IJCSIS Vol. 13 No. 9, September 2015
ISSN 1947-5500

International Journal of Computer Science & Information Security

Pennsylvania, USA

Cornell University Library

Cogprints

Google scholar

.docstoc
find and share professional documents

ScientificCommons

View my documents on
Scribd

BASE
Bielefeld Academic Search Engine

scirus
search engine for science

SciRate.com

CiteSeerx beta

dblp.uni-trier.de
Computer Science
Bibliography

Q·Sensei BETA

DOAJ DIRECTORY OF
OPEN ACCESS
JOURNALS

EBSCO
HOST

ProQuest

IJCSIS

ISSN (online): 1947-5500

Please consider to contribute to and/or forward to the appropriate groups the following opportunity to submit and publish original scientific results.

CALL FOR PAPERS
International Journal of Computer Science and Information Security (IJCSIS)
January-December 2015 Issues

The topics suggested by this issue can be discussed in term of concepts, surveys, state of the art, research, standards, implementations, running experiments, applications, and industrial case studies. Authors are invited to submit complete unpublished papers, which are not under review in any other conference or journal in the following, but not limited to, topic areas.
See authors guide for manuscript preparation and submission guidelines.

Indexed by Google Scholar, DBLP, CiteSeerX, Directory for Open Access Journal (DOAJ), Bielefeld Academic Search Engine (BASE), SCIRUS, Scopus Database, Cornell University Library, ScientificCommons, ProQuest, EBSCO and more.

Deadline: **see web site**
Notification: see web site
Revision: see web site
Publication: see web site

Context-aware systems
Networking technologies
Security in network, systems, and applications
Evolutionary computation
Industrial systems
Evolutionary computation
Autonomic and autonomous systems
Bio-technologies
Knowledge data systems
Mobile and distance education
Intelligent techniques, logics and systems
Knowledge processing
Information technologies
Internet and web technologies
Digital information processing
Cognitive science and knowledge
Agent-based systems
Mobility and multimedia systems
Systems performance
Networking and telecommunications
Software development and deployment
Knowledge virtualization
Systems and networks on the chip
Knowledge for global defense
Information Systems [IS]
IPv6 Today - Technology and deployment
Modeling
Software Engineering
Optimization
Complexity
Natural Language Processing
Speech Synthesis
Data Mining

For more topics, please see web site https://sites.google.com/site/ijcsis/

For more information, please visit the journal website (https://sites.google.com/site/ijcsis/)

Editorial
Message from Managing Editor

*The **International Journal of Computer Science and Information Security** (IJCSIS) a monthly, peer reviewed, online open access journal that publishes articles which contribute new results and theoretical ideas in all areas of Computer Science & Information Security. The editorial board is pleased to present the September 2015 issue. The core of the vision is to publish and disseminate new knowledge and technology for the benefit of all, ranging from academic research and professional communities to industry professionals in a range of topics in computer science and information security in general. It also provides a publication place for high-caliber researchers, practitioners and PhD students to present ongoing research and development in these areas. We are glad to see variety of articles focusing on the major topics of innovation and computer science; big data analytics; Biometric security; mobile computing; network security and IT applications. This scholarly resource endeavors to provide international audiences with the highest quality research manuscripts and accounts of the constant evolution of information science and technology in whole. Researchers, academicians, practitioners and doctoral students will find this journal as a critical source of reference.*

Over the last years, we have revised and expanded the journal scope to recruit papers from emerging areas of green & sustainable computing, cloud computing security, forensics, mobile computing and big data analytics. IJCSIS archives all publications in major academic/scientific databases and is indexed by the following International agencies and institutions: Google Scholar, CiteSeerX, Cornell's University Library, Ei Compendex, Scopus, DBLP, DOAJ, ProQuest, ArXiv, ResearchGate and EBSCO.

We thank and congratulate the wonderful team of editorial staff members, associate editors, and reviewers for their dedicated services to select and publish high quality papers for publication. In particular, we would like to thank the authors for submitting their papers to IJCSIS and researchers for continued support to IJCSIS by citing papers published in IJCSIS. Without their continued and unselfish commitments, IJCSIS would not have achieved its current premier status.

"We support researchers to succeed by providing high visibility & impact value, prestige and excellence in research publication."

*For further questions please do not hesitate to contact us at **ijcsiseditor@gmail.com**.*

A complete list of journals can be found at:
http://sites.google.com/site/ijcsis/

IJCSIS Vol. 13, No. 9, September 2015 Edition

ISSN 1947-5500 © IJCSIS, USA.

Journal Indexed by (among others):

Google scholar
ScientificCommons
CiteSeerx beta
SCIRUS search engine for science
DOAJ DIRECTORY OF OPEN ACCESS JOURNALS
INDEX COPERNICUS INTERNATIONAL
ProQuest® Start here.

Bibliographic Information
ISSN: 1947-5500
Monthly publication (Regular Special Issues)
Commenced Publication since May 2009

Editorial / Paper Submissions:
IJCSIS Managing Editor
(ijcsiseditor@gmail.com)
Pennsylvania, USA
Tel: +1 412 390 5159

IJCSIS EDITORIAL BOARD

TABLE OF CONTENTS

Ngu Wah Win, University of Computer Studies, Yangon, UCSY
Thandar Thein, University of Computer Studies, Yangon, UCSY

Abstract — Big data analytics technologies are to extract value from very large data volume, variety of data, and highly rate of data stream. With the fast deployment of cloud services with mobile devices, big data analytics is shifting from personal computer to mobile devices. But, significant limitations of mobile devices are less storage amount and processing power. This paper proposes a big data analytic platform on mobile cloud computing with efficient query execution time by developing MapReduce Transformation Process and query operation based on input query's complexity level. Furthermore, this paper presents the process of RESTful web service for providing seamless connectivity between mobile devices and cloud storage, where store the data and all of necessary processing steps are done by cloud backend. This proposed platform is evaluated by using Census dataset and compared the result with other traditional high level query languages, such as Pig, Hive, and Jaql.

Keywords- big data analytic; mobile cloud computing; Hadoop MapReduce; RESTful web serivce

Jagadeesh H S, Dept. of Electronics and Communication Engineering, APSCE, Bangalore, India
Suresh Babu K, Dept. of Electronics and Communication Engineering, UVCE, Bangalore, India
K B Raja, Dept. of Electronics and Communication Engineering, UVCE, Bangalore, India

Abstract — Real time challenges are eternal for verification and recognition of a person using face biometric. In this paper, we propose an efficient algorithm using Extended Directional Binary codes (EDBC) with Discrete Wavelet Transform (DWT) and Singular Value Decomposition (SVD) with Discrete Cosine Transform (DCT). In preprocessing, the face images are refined to make them suitable for feature extraction. The Approximate (LL) band is extracted by applying DWT. One hundred EDBC features are extracted using LL sub band. Additionally, DCT is applied on pre-processed image and one hundred SVD features are extracted from DCT output. Final one hundred distinct features are derived by fusing each of one hundred EDBC and SVD features. The features comparison is performed using Euclidean Distance (ED) measure to produce the results. Performance on JAFFE and ORL face datasets shows that the proposed algorithm is superior in different metrics compared to other existing methods.

Keywords- Discrete wavelet transform; Euclidean distance; Extended directional binary codes; Face biometric; Singular value decomposition.

Agus Sihabuddin, Subanar, Dedi Rosadi, Edi Winarko
Computer Science Graduate Program, Faculty of Mathematics and Natural Science, Gadjah Mada University, Yogyakarta – Indonesia

Abstract — This paper evaluates whether the variable-length moving average (VMA) as input in NARX outperform the univariate exchange rate forecasting performance. Six major rates of monthly data from January 1975 to April 2014 (USDAUD, USDCAD, USDEUR, USDGBP, USDJPY and USDCHF) are used to test the proposed model with a (1,5,0) VMA rule. We evaluate that the VMA can be used as input for NARX model and the forecasting accuracy is outperform the NAR univariate model with 19.97% improvement on Dstat and 3.17% improvement on MSE.

Keywords— forecasting, major exchange rates, VMA, NAR, NARX

4. Paper 31081527: Implementing the Database Users Privilege Model: Effects of possible successful SQL Injection attack in web applications (pp. 19-21)

Gem Ralph Caracol, Soomi Yang
Information Security Department, Suwon University, Hwaseong City, South Korea

Abstract — For more than a decade, many solutions and detection mechanisms have been proposed to prevent web applications from SQL Injection attacks. However, according to the 2013 OWASP 10, SQL Injection is still a top threat and attackers can find evasive ways to exploit this vulnerability. We implemented the proposed database level Database Users Privilege Model of [6]. Our findings suggest that by implementing the model, it does not detect SQL Injection attacks but with the necessary recommendations, it can prevent the attacker from fully compromising the database and the database server.

Keywords-SQL Injection, Database Users Privilege Model, OWASP, Database Security, Web Application

5. Paper 31081528: Security Issues and Solutions for Android-based Mobile Devices (pp. 22-27)

Klever R. P. Cavalcanti, Edejair Viana
Department of Statistics and Informatics, Federal Rural University of Pernambuco, Pernambuco, Brazil
Fernando A. A. Lins, Department of Statistics and Informatics, Federal Rural University of Pernambuco, Pernambuco, Brazil

Abstract — Currently, mobile devices are being widely used by of a considerable number of people. The need to be connected 24 hours a day is becoming a reality, because users need to make online purchases, make payments, access social networks, surf the Internet, check e-mails and so on. In this context, users with mobile devices, especially smartphones, using the Internet to connect to specific applications and safety issues may arise because, for example, sensitive data may be sent over an insecure channel (Internet). The aim of this paper is to present an overview of current security risks and security solutions related to smartphones based on the Android platform. Security risks have been divided into five categories, and these risks are presented and detailed on the corresponding categories. In addition, still stand out security solutions that are currently available on Android stores and these solutions can be used to eliminate or mitigate the risks.

Keywords- Android; Mobile; smartphone; security; Application.

6. Paper 31081534: Intrusion Detection and Prevention Systems (IDPS) State of Art (pp. 28-35)

Homam Reda El-Taj, Community College Univesity of Tabuk, Tabuk, Saudi Arabia

Abstract — Over the past few years, we have witnessed an ever-increasing rampant battle between network managers & computer criminals which led to many developments in the tools used by both parties i.e. " legitimate computer professionals & computer criminals". Recently, interruption exposure & avoidance systems have earned increasing appreciation due to their more frequent involvement in the security domain since they allow security analysts to make fast reactions and thus take quick decisions to prevent any possible damage. This underlines the significance of upgraded detection & prevention processes, taking into consideration the competitive and dynamic network environment these days. Most commercial and government information systems are connected through the internet, which will expose them to possibilities of spasms. The increasing number of computer users marks it precise, ever since computers have become a necessary device in our lives. This article covers the IDPS state of art and discusses the IDPS challenges.

Keywords- component; Network, IDS, IPS, Security, IDS Myths, IDS Alerts.

7. Paper 31081520: Improving the Quality of Composite Services Through Improvement of Cloud Infrastructure Management (pp. 36-44)

Olga Shpur, Department of Telecommunication, Lviv Polytechnic National University, Lviv, Ukraine
Mykhailo Klymash, Department of Telecommunication, Lviv Polytechnic National University, Lviv, Ukraine
Marian Seliuchenko, Department of Telecommunication, Lviv Polytechnic National University, Lviv, Ukraine
Bogdan Strykhaliuk, Department of Telecommunication, Lviv Polytechnic National University, Lviv, Ukraine
Orest Lavriv, Department of Telecommunication, Lviv Polytechnic National University, Lviv, Ukraine

Abstract — For improving the quality of composite services in cloud infrastructure this paper proposes an integrated control architecture using the NVF technology that provides load balancing with estimation of available system resources. The aim of our proposed algorithms is to assess existing physical and virtual, resources of telecommunication system. The analysis is based on the maximum value of integral resources index of each physical machine. Maximum values of available virtual and physical resources are transferred to Orchestrator, which provides the migration of service components to less loaded servers if necessary. Performance analysis of the proposed approach shows that load balancing by implementing integrated management architecture based on NVF technology allows to reduce the duration of service requests by 3 times.

Keywords – cloud infrastructure management; load balancing; NVF; analysis cloud resources; duration of service requests

8. Paper 31081502: Service-Oriented Architecture for Secure Service Discovery and Selection in Specialized Mobile Networks (pp. 45-71)

M. Adel Serhani, College of Information Technology, UAE University, Al-Ain, UAE
Yasser Gadallah, The American University in Cairo, Egypt
Ezedin Barka, College of Information Technology, UAE University, Al-Ain, UAE

Abstract – Special operations such as emergency response as well as military missions are usually characterized by the limited resources available to handle generally large-scale operations. Precise resource discovery and allocation thus becomes an important factor for the success of such operations. This task has been recognized as a challenging research issue. This is due to the dynamic nature of the emergency response elements e.g., personnel and equipment. One of the important requirements of these operations is achieving the security of the communications involved in the resource discovery and allocation tasks. Security ensures the confidentiality, integrity, and availability of the communicated information. Therefore, solutions that are intended for selecting best matching service(s) should not only rely on the functional properties of the service but also on level of security under which this service is provided. In this study, we propose a secure multicast service discovery architecture that is based on a mobile ad hoc network (MANET) of operation participants. The main objective is to locate, select, reserve and assign certain resources to parties that are in need of these resources. The involved communications are designed to be secure multicast-based, utilizing features of the Role-Based Access Control (RBAC) Model. We describe the details of the proposed communication protocol. We then qualitatively compare our architecture to other alternative MANET-based service discovery architectures. The comparison highlights the merits of the proposed architecture. Finally, we conduct and present the results of a set of experiments to evaluate key features of our proposed architecture.

Keywords: Service-Oriented Architecture, Secure Service Discovery, MANET, Special Operations, Access Control, Service Selection.

9. Paper 31081511: Vehicle Segmentation Using K-Means with Fuzzy Logic (pp. 72-77)

(1) Shakila basher, (2) Purushothaman S., and (3) Rajeswari P.
(1) Department of MCA, VELS University, Chennai, India.
(3) Department of Electrical and Computer Science Engineering
(2,3) Institute of Technology, Haramaya University, DireDawa, Ethiopia

Abstract - This paper presents methods for vehicle segmentation. The camera can be fixed or moving which can be used to capture the moving vehicle. During this process, the orientation of the vehicle captured can be in any direction. Many segmentation methods available. However, K-Means with Fuzzy logic can be still more appropriate in segmenting the vehicles moving on the road.

10. Paper 31081513: Effective feature selection in multi-label classification problems using genetic algorithms (pp. 78-82)

Somayeh Fattahi Ferdowsi, Department of computer, Zanjan Branch, Islamic Azad University, Zanjan, Iran

Abstract- Designing a classifier in a multiple-label classification issue in which the number of features used for describing each sample is high and the number of samples is low, is faced with many problems. The features describing each sample can be divided into three categories: relevant, irrelevant and redundant. Redundant and irrelevant features could seriously influence the accuracy of classification in such issues. In spite of works carried out, the issue of feature selection in multiple–label classification issues is still considered as a challenge. For this reason, the issue of feature selection has been discussed in this paper. The aim of feature selection problem is finding a subset of features in order to modify and improve the accuracy of estimation without loss of accuracy that classifier using the selected features performs the classification of data. This study was aimed to enhance the efficiency of classification through decreasing the error and to increase classification speed through selecting a subset of effective features in classification of multi-label data as well as using mutual information, Genetic Algorithm and Rank SVM classification The performance of proposed method has been evaluated on three data collections including Emotions, Scene and Yeast that are available on Mulan website.

Keywords: feature selection, multi-label classification, genetic algorithms and classification Rank SVM

11. Paper 31081515: Vehicle Tracking Using Locally Weighted Projection Regression Method (pp. 83-89)

(1) Shakila basher, (2) Purushothaman S., and (3) Rajeswari P.
(1) Department of MCA, VELS University, Chennai, India.
(3) Department of Electrical and Computer Science Engineering
(2,3) Institute of Technology, Haramaya University, DireDawa, Ethiopia

Abstract - This paper presents the method of tracking vehicle in video frames using Locally weighted projection regression (LWPR). The coordinates of the segmented vehicle image are presented to the LWPR. Based on the coordinates of the previous video frames, the LWPR estimates the next position of the vehicle. The LWPR is trained with coordinates of the vehicle obtained from few frames. Based on the learned information the next movement of the vehicle is estimated without processing next few video frames.

12. Paper 31081518: Multilevel Extensible and Dynamic of Mobile Establishment Concepts (pp. 90-91)

Ammar Es-Said, University Hassan II/ Faculty of Science Ben M'sik, Casablanca Morocco
Labriji El Houssine, University Hassan II/ Faculty of Science Ben M'sik, Casablanca Morocco

Abstract -- Mobile establishment of masts is an exclusive competence a control power, basically regarding town planning, mobility characterizes what could move or be moved, which can change place, this multilevel extensible, dynamic notion intuitive the activity however by three different aspects, and as many approaches, 'nomadisme', ubiquity, the sensitive system in context, nevertheless the use of these devices remains immersive, these devices requires all the attention, independently from this one. This approach is often called 'nomasime', although this term can take different significance in other fields to find proximity, In ray of influence that remains to be determined, mobility is in fact related to features of the increasing data of the computing mobile.

Keywords -- mobility, extensible, mobile devices, WPAN, mobile failures, wired, Mobile Technology

13. Paper 31081530: Forensic Investigation of User's Web Activity on Google Chrome using Open-source Forensic Tools (pp. 92-100)

Narmeen Shafqat, Baber Aslam
Dept of Information Security, MCS, National University of Science and Technology, Rawalpindi, Pakistan

Abstract — Cyber Crimes are increasing day by day, ranging from confidentiality violation to identity theft and much more. The web activity of the suspect, whether carried out on computer or smart device, is hence of particular interest to the forensics investigator. Browser forensics i.e forensics of suspect's browser history, saved passwords, cache, recent tabs opened etc. , therefore supply ample amount of information to the forensic experts in case of any illegal involvement of the culprit in any activity done on web browsers. Owing to the growing popularity and widespread use of the Google Chrome web browser, this paper will forensically analyse the said browser in windows 8 environment, using various forensics tools and techniques, with the aim to reconstruct the web browsing activities of the suspect. The working of Google Chrome in regular mode, private "Google Incognito Mode" and portable modes of operation is discussed at length in this paper.

Keywords—Browser forensics, Private web browsing, Chrome Incognito, Chrome forensics, Portable browser forensics, Chrome artifacts.

14. Paper 31081532: Natural Language Processing and Machine Learning: A Review (pp. 101-106)

Fateme Behzadi, Computer Engineering Department, Bahmanyar Institute of Higher Education, Kerman, IRAN

Abstract — Natural language processing emerges as one of the hottest topic in field of Speech and language technology. Also Machine learning can comprehend how to perform important NLP tasks. This is often achievable and cost-effective where manual programming is not. This paper strives to Study NLP and ML and gives insights into the essential characteristics of both. It summarizes common NLP tasks in this comprehensive field, then provides a brief description of common machine learning approaches that are being used for different NLP tasks. Also this paper presents a review on various approaches to NLP and some related topics to NLP and ML.

Keywords- Natural Language Processing, Machine learning, NLP, Ml.

15. Paper 31081533: A User-Aware Approach to Provide Context Aware Web Service Composition (pp. 107-120)

Sihem Cherif, MIRACL, ISIMS, Cité El Ons, Route de Tunis Km 10, Sakiet Ezziet 3021, Sfax, Tunisia
Raoudha Ben Djemaa, MIRACL, ISIMS, Cité El Ons, Route de Tunis Km 10, Sakiet Ezziet 3021, Sfax, Tunisia
Ikram Amous, MIRACL, ISIMS, Cité El Ons, Route de Tunis Km 10, Sakiet Ezziet 3021, Sfax, Tunisia

Abstract — Web services Compositions are rapidly gaining acceptance as a fundamental technology in the web fields. They are becoming the cutting edge of communication between the different applications all over the web. With the need for the ubiquitous computing and the pervasive use of mobile devices, the context aware web service composition becomes a hot topic. This later aims to adapt the web service composition behavior according to the user's context such as his specific work environment, language, type of Internet connection, devices and preferences. Many solutions have been proposed in this area. Nevertheless, the adaptation was carried out only at the runtime and it partially covered the user's general context. In this paper, we introduce a new context-aware approach that provides dynamic adaptation of service compositions. Our approach allows to express requirements by taking into account potential user's context in addition to the functional one.

Keywords-component; UDDI, AAWS-WSDL, Dynamic context, SABPEL, CAC-WSR

16. Paper 31071533: Analysis and Detection of the Zeus Botnet Crimeware (pp. 121-135)

Laheeb Mohammed Ibrahim, Software Engineering, Mosul University, Collage of Computer Sc. & Math., Mosul, Iraq
Karam H. Thanon, Software Engineering, Mosul University, Collage of Computer Sc. & Math., Mosul, Iraq

Abstract — The raised significant evolution of the Internet next to the development of the high prevalence of computers, smart phones and the Internet on a large scale in most of the trends of life, but this use leads to network attacks. with a large use of e-commerce, they needs websites on the Internet. E-commerce represents a good reason for criminals or attackers to be diverted to profit law. Recently, the attackers used botnets to achieve their goals. A comprehensive study of botnet is done in this paper , study a life cycle of botnet, the attack on the behavior, topologies and technologies of botnet, studied of Zeus robots (An ethical penetration operation has been done using Zeus botnet version 1.2.7.19 and using Zeus version 2.0.8.9) were is done in in detail to determine its characteristics, and be able to detect it in the computers on the Internet. Host Botnet Detection Software (HBD's) is designed and implemented to detect Zeus botnet in user's computers. The HDB's depends on information obtained from studying Zeus in addition to information obtained from analysis (an analysis of Zeus bot has been done by using reverse engineering tool (Ollydbg reverse engineering tool)) and penetration operation. In order to remove Zeus botnet from victim computers.

Keywords - Zeus, Host Botnet Detection Software (HBDS), Botnet, Ollydbg reverse engineering tool, Zeus botnet version 1.2.7.19 and using Zeus version 2.0.8.9

17. Paper 31081525: Security and Cryptography on World Wide Web (pp. 136-141)

Okal Christopher Otieno, Department of Information Technology, Mount Kenya University, Nairobi, Kenya
Magati Steve Biko, Department of Information Technology, Mount Kenya University, Nairobi Kenya

Abstract – Security has been a major concern for internet users regarding the potential for harm that a breach in their systems can present to the landscape. The world is evolving towards an internet dependent computing architecture considering the advancements in cloud computing and other such technologies. They promise various benefits mostly relating to the cost of operation for the businesses and personal Internet users. This investigation has the intention of determining the role that cryptography plays in ensuring the safety of the systems and the information that people share over the internet. The paper looks at the types of cryptography that are in broad use in the field of information technology and how they enable the protection that the users need. There are important protocols of protection including Internet Protocol Security Standard (IPSec) and Field Programmable Gate Arrays (FPGAs) that use cryptographic techniques. The investigation concludes that cryptography is an important contributor to Internet security through the implementation of such procedures.

18. Paper 31081521: LDA-PAFI: Linear Discriminate Analysis Based Personal Authentication using Finger Vein and Face Images (pp. 145-152)

Manjunathswamy B E, Dr Thriveni J, Dr Venugopal K R
Department of Computer Science and Engineering, University Visvesvaraya College of Engineering, Bangalore, India

Abstract — Biometric based identifications are widely used for individuals personnel identification in recognition system. The unimodal recognition systems currently suffer from noisy data, spoofing attacks, biometric sensor data quality and many more. Robust personnel recognition can be achieved considering multimodal biometric traits. In this paper the LDA(Linear Discriminate analysis) based Personnel Authentication using Finger vein and Face Images (LDA-PAFF) is introduced considering the Finger Vein and Face biometric traits. The Magnitude and Phase features obtained from Gabor Kernels is considered to define the biometric traits of personnel. The biometric feature space is reduced using Fischer Score and Linear Discriminate Analysis. Personnel recognition is achieved using the weighted K-nearest neighbor classifier. The experimental study presented in the paper considers the (Group of Machine Learning and Applications, Shandong University-Homologous Multimodal Traits) SDUMLA-HMT multimodal biometric dataset. The performance of the LDA-PAFF is compared with the existing recognition systems and the performance improvement is proved through the results obtained.

Keywords-SDUMLA_HMT; LDA-PAFF; Phase; Magnitude; fisher Score

19. Paper 31081516: The Socio-Political Influences of the Globalization of the IT Industry (pp. 153-157)

Okal Christopher Otieno
Department of Information Technology, Mount Kenya University, Nairobi, Kenya

Abstract - This paper seeks to establish the sociopolitical impacts that the globalization of the information technology industry has in different societies. The review focuses on defining the two concepts of IT and Globalization and later outlines the relationship that exists between them. IT is an important contributor to the process of globalizing different communities and economies. While most people might view the relationship as unidirectional, it is untrue since globalization also impacts how the IT industry develops through various markets. The paper focuses on the two objectives of IT that are automation of processes for better efficiency and integrating people by promoting communication between them. These goals match the definition of globalization that describes their connection. Globalizing IT has different impacts on the politics and policy implementations of various locations through the flow of information that influences the people in governments. Other effects include the formation of trade blocs that are influential on the performance of the IT industry.

An Efficient Big Data Analytics Platform for Mobile Devices

Ngu Wah Win
University of Computer Studies, Yangon, UCSY
nguwahwin@ucsy.edu.mm

Thandar Thein
University of Computer Studies, Yangon, UCSY
thandartheinn@gmail.com

Abstract— *Big data analytics technologies are to extract value from very large data volume, variety of data, and highly rate of data stream. With the fast deployment of cloud services with mobile devices, big data analytics is shifting from personal computer to mobile devices. But, significant limitations of mobile devices are less storage amount and processing power. This paper proposes a big data analytic platform on mobile cloud computing with efficient query execution time by developing MapReduce Transformation Process and query operation based on input query's complexity level. Furthermore, this paper presents the process of RESTful web service for providing seamless connectivity between mobile devices and cloud storage, where store the data and all of necessary processing steps are done by cloud backend. This proposed platform is evaluated by using Census dataset and compared the result with other traditional high level query languages, such as Pig, Hive, and Jaql.*

Keywords-big data analytic; mobile cloud computing; Hadoop MapReduce; RESTful web serivce

I. INTRODUCTION

The Internet generates the largest amount of data and it has exceeded the zetabyte levels. Processing the high volume of data is beyond the computational capabilities of traditional data warehouses, giving rise the term Big Data [3, 4]. Cloud computing is the powerful platform because of their well-known services. It can give many advantages to users by allowing them to use infrastructure, platforms and software by cloud providers at low cost and elastically in an on demand fashion [1]. After the number of mobile phone usage is many times the number of personal computers, these small portable devices that can access information are already part of everyday life for hundreds of millions of people in the developed world. Mobile devices need to borrow storage and computing power from the cloud because of their limited resources. When mobile devices try to access a shared pool of computing resources, cloud computing becomes mobile and accessing data in the cloud from mobile devices is becoming a basic need.

Because of this stream of technology requirements, many researches emphasize to integrate mobile device and big data analysis to gain the business facilities by using mobile web services. Mobile web services allow deploying, discovering and executing of web services in a mobile communication environment using standard protocol. Web service can be classified into two main categories: RESTful and SOAP-based web services. On the other hand, Hadoop is becoming the core technology in big data analytic to solve the business problem for large organizations with MapReduce programming model. The server level architecture for Big Data consists of parallel computing platforms that can handle the associated volume and speed. Clusters or grids are types of parallel and distributed systems, where a cluster consists of a collection of interconnected stand-alone computers working together as a single integrated computing resource, and a grid enables the sharing, selection, and aggregation of geographically distributed autonomous resources dynamically at runtime. A commonly used architecture for Hadoop consists of client machines and clusters of loosely coupled commodity servers that serve as the HDFS distributed data storage and MapReduce distributed data processing.

The MapReduce is the programming model for data processing [9, 10, 11, 12, 13]. It operates via regular computer that uses built-in hard disk, not a special storage. Each computer has extremely weak correlation where expansion can be hundreds and thousands of computers. Since many computers are participating in processing, system errors and hardware errors are assumed as general circumstances, rather than exceptional. With a simplified and abstracted basic operation of Map and Reduce, many complicated problems can solve. Programmers who are not familiar with parallel programs can easily perform parallel processing for data. It supports high throughput by using many computers. As the core technology of the Hadoop is the MapReduce parallel processing model, all of the high level query languages that run on Hadoop are the MapReduce based query languages such as Hive, Pig, and JAQL. This paper presents a big data analytic platform for mobile device with different OS and concludes with experimental results based on query execution time.

II. RELATED WORK

There are many types of existing big data analytic platforms for large scale data. Most of them based on MapReduce, distributed file system, and no-SQL indexing. Tableau [2] is known for its strong visualization features, which can support exploratory or discovery analytics. Analytics aside, Tableau is also used as an all-purpose BI platform, applied to either enterprise or departmental needs. The visual approach seen in Tableau enables high ease of use so that – with simple drag-and-drop methods – an analyst or other user can interact directly with the visualization and other visual controls to form queries, reports, and analyses. If the user knows the basics of enterprise data, he or she doesn't need to wait for assistance from IT. With a few mouse-clicks, a user can access a database, identify data structures of interest, and bring big data into server memory for reporting or analysis – all in a self-service manner.

The Vertica Analytics platform has a high-speed, relational SQL DBMS purpose-built for analytics and business intelligence. Vertica has helped over 300 customers monetize their data in unique ways, including Zynga, JP Morgan, Verizon, Comcast, Vonage, Blue Cross Blue Shield, and others. The Vertica Analytics platform offers a shared-nothing, MPP column-oriented architecture, and has been benchmarked by many customers as being on average 10x to 200x faster than other solutions. It also uses compression very aggressively, both of data on disk and on data “in motion” during queries, which further enhances query speed while enabling cost-effective storage management. The Vertica Analytics Platform runs on clusters of inexpensive, industry-standard Linux servers and requires limited resources up front for setup and performance configuration. Unlike most solutions in this space, Vertica was purposely built from the ground up for today’s most demanding analytics challenges.

Teradata Database is famous for supporting large and mostly centralized Enterprise Data Warehouse (EDWs) that yield scalability and fast performance, despite the fact that they’re supporting concurrent mixed workloads, such as those for standard reports, performance management, OLAP, advanced analytics, and real-time or streaming data. Furthermore, Teradata’s support for third normal form and in-database analytic processing makes it a good platform for managing and analyzing detailed big data. The centralized EDW has distinct advantages. Yet, some Teradata customers need analytic databases outside the main Teradata System. In response, Teradata introduced a line of data warehouse appliances and acquired Aster Data. Since then, Aster Data has received a patent on its native SQL integration with MapReduce called SQL-MapReduce (with Hadoop lacks). And Teradata continues to improve support for partnering analytic tools and platforms.

Our big data analytic platform for mobile devices provides a solution to reduce the query processing time based on complexity of query that requested by mobile users with MapReduce Transformation Process and query mode operation. To achieve the seamless connectivity between mobile and cloud storage, we used RESTful web service technology. By using this platform, users send a request from their mobile device and get back the results without noticeable amount of time.

III. MOBILE CLOUD COMPUTING AND BIG DATA ANALYTICS CONCEPT

A. *Mobile Cloud Computing*

Mobile cloud computing (MCC) at its simplest, refers to an infrastructure where both the data storage and data processing happen outside of the mobile device. Mobile cloud applications move the computing power and data storage away from the mobile devices and into powerful and centralized computing platforms located in clouds, which are then accessed over the wireless connection based on a thin native client. Improving data storage capacity and processing power: it enables mobile users to store/access large data on the cloud and helps to reduce the running cost for computation intensive applications [7].

B. *Big Data Analytic*

Big data analytics requires massive performance and scalability - common problems that old platforms can’t scale to big data volumes, load data too slowly, respond to queries too slowly, lack processing capacity for analytics and can’t handle concurrent mixed workloads [5, 6].

There are two main techniques for analyzing big data: the store and analyze, and analyze and store. The store and analyze integrates source data into a consolidated data store before it is analyzed. The advantages of this are improved by data integration and data quality management, plus the ability to maintain historical information. The disadvantages are additional data storage requirements and the latency introduced by the data integration task.

Analyze and store technique analyzes data as it flows through business processes, across networks, and between systems. The analytical results can then be published to interactive dashboards and published into data store for user access, historical reporting and additional analysis. This can also be used to filter and aggregate big data before it is brought into a data warehouse.

C. *Hadoop Distributed File System and MapReduce*

The Hadoop distributed file system (HDFS) [19] is designed to store very large data sets reliably, and to stream those data sets at high bandwidth to user applications. HDFS stores file system metadata and application data separately. As in other distributed file system, HDFS stores metadata on a dedicated server. All servers are fully connected and communicate with each other using transmission control protocol (TCP) based protocols. The following figure shows the Hadoop distributed file system architecture.

Hadoop MapReduce is a software framework for easily writing applications which process vast amounts of data in parallel on large clusters of commodity hardware in a reliable, fault-tolerant manner. The framework sorts the outputs of the map, which are then input to the reduce tasks. Typically, both the input and the output of the jobs are stored in a file system. The framework takes care of scheduling tasks, monitoring them and re-executing the failed tasks.

D. *RESTful Web Service*

REST stands for Representational State Transfer: it is a resource oriented technology and it is defined by Fielding in [15] as an architectural style that consists of a set of design criteria that define the proper way for using web standards such as HTTP and URIs. Although REST is originally defined in the context of the web, it is becoming a common implementation technology for developing web services. RESTful web services are implemented with web standards (HTTP, XML and URI) and REST principles. REST principles include addressability, uniformity, connectivity and stateless. RESTful web services are based on uniform interface used to define specific operations that are operated on URL resources.

E. MapReduce based High Level Query Languages

A number of HLQLs have been constructed on top of Hadoop to provide more abstract query facilities than using the low-level Hadoop Java based API directly. Pig, Hive, and JAQL are all important HLQLs. Programs written in these languages are compiled into a sequence of MapReduce jobs; to be executed in the Hadoop MapReduce environment. Apache Hive [14, 15, 16] is an open-source data warehousing solution built on top of Hadoop. Hive provides an SQL dialect, called Hive Query Language (HiveQL) for querying data stored in a Hadoop cluster. Apache Pig [17, 18] provides an engine for executing data flows in parallel on Hadoop. It includes a language, PigLatin, for expressing these data flows. PigLatin includes operators for many of the traditional data operations, as well as the ability for users to develop their own functions for reading, processing, and writing data. Jaql [8] is a declarative scripting language for analyzing large semistructured datasets in parallel using Hadoop's MapReduce framework. It consists of a scripting language and compiler, as well as a runtime component for Hadoop. It is extremely flexible and can support many semistructured data sources such as JSON [9], XML, CSV, flat files and more.

IV. PROPOSED BIG DATA ANALYTIC PLATFORM

Big data analytics involves analyzing large amounts of data of a variety of types to uncover hidden patterns, unknown correlations and other useful information. In this paper, we proposed a big data analytics platform for mobile device and improve the query execution time of user request. In our proposed platform consists of four layers: storage layer, processing layer, web service layer (for data transmission) and application layer.

- *Storage layer*: storage layer is to store the data in DataNode of Hadoop distributed file system. When a file is placed in HDFS it is broken down into blocks, 64MB block size by default. The default replication is 3, i.e. there will be 3 copies of the same block in the cluster. Hadoop follows the master-slave architecture. The slave machines run dataNode to store data with distributed architecture that supported by Hadoop.
- *Processing layer*: processing layer is to work together with storage layer. The main components of this layer are TaskTracker and JobTracker. After the JobTracker receive a request from client, it assigns TaskTracker which task to be performed. Normally, JobTracker is run on master machine and it tries to connect with salve machine, to execute the data, where DataNodes are running. TaskTracker is a daemon that accepts tasks (Map and Reduce) from the JobTracker and sends progress/status information of Map and Reduce tasks to the JobTracker.

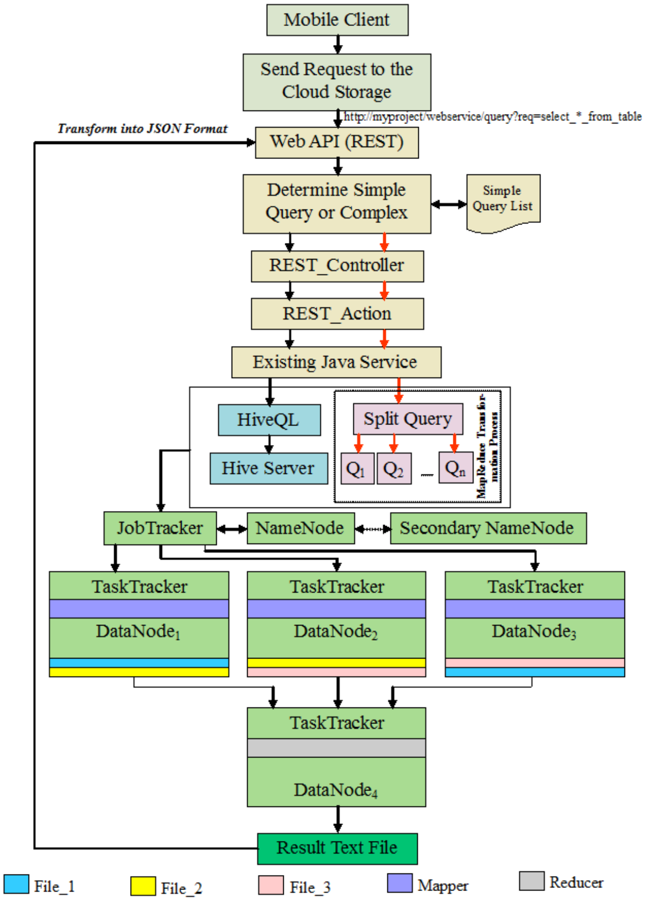


Figure 1. Sysem flow of the proposed big data analytic platform

- *Web service layer*: web service layer is responsible for providing seamless connection between client mobile device and cloud storage. At the same time, it reduces the complexity of result from cloud storage to become a light-weight data transfer.
- *Application layer*: application layer which operates the user request by using Pig, Hive and Jaql. This proposed platform combined MapReduce Transformation Process to perform user requested simple queries.

A. System Flow of Proposed Platform

Firstly, mobile user sends request from mobile device and this request pass to the cloud storage by using RESTful web service. After web service receiving the request, it determines whether the request is simple query or not by matching local simple query list. If the incoming request is simple query type, it will work through red arrow line and if it was a complex query, it will work through black arrow line.

For the simple query request, we developed a MapReduce Transformation Process which perform ad-hoc simple query by using Map and Reduce function. In this stage, it breaks the query into sub-queries according to the query decomposition rules. These sub-queries work with multiple Mapper classes and Reducer class which produces the final output result. All of these Mappers and Reducer are Map and Reduce tasks of the TaskTracker nodes.

For the complex query request, the platform will work with traditional query processing language, HiveQL, is more efficient than other high level query languages, Pig and Jaql. After testing above query languages, we can conclude that HiveQL is three times faster than other two languages. HiveQL extract data from DataNodes with hive server and hadoop-hive driver. In these two mechanisms, the query processing time of the proposed platform is faster when it used MapReduce Transformation Process when they run same queries. Because, HiveQL is need to transform query into MapReduce form to combine with Hadoop Distributed File System. But the proposed MapReduce Transformation Process is not need to transform MapReduce form and processing time of sub-queries is effectively reduce the overall query processing time. The output result of the Reducers from both query engines is the text file format and this text file is transformed into JSON format to be a light weight message for mobile user. The RESTful web service returns the JSON output to the mobile user and the mobile devices need to develop a convenient data visualization application that can change the received JSON output to become a user friendly graphical representation form. By developing this platform, mobile user can applied big data analytic process on cloud infrastructure with efficient query processing time.

B. Experiment Environment

We implement the mobile platform for big data analytic and evaluate on different Operating Systems and different high level query languages. To build a storage cluster, we created 16 VMs for NameNode, Secondary NameNode, DataNode, JobTracker and TaskTracker.

TABLE I. EXPERIMENT PARAMETERS

Parameters	Specification
OS	- Ubuntu 14.04 Linux, - Red Hat Enterprise Linux 6.4
Host Specification	Intel ® Core i7-2600 CPU @ 3.40GHz, Intel ® Core i7-3770 CPU @ 3.40GHz, 8GB Memory, 1TB Hard Disk
VMs Specification	1GB RAM, 50 GB Hard Disk
Mobile Device Specification	Huawei G730-U00, Android OS version 4.2.2 (Jelly Bean), Quad-core 1.3 GHz Cortex-A7, 4GB internal memory
Software Component	- Hadoop 1.1.2 - Hive 0.14.0, Pig 0.12.1, Jaql 0.5.1
Data Set	US census dataset [20], -114 GB in size

The specification of devices and necessary software components used in mobile cloud infrastrue, and dataset ued in MapReduce processing are described in table 1.

C. Result Discussion

In this platform, we test many queries and record the query processing time of traditional query languages and proposed MapRedcue Transformation Process on both operating systems, Red Hat and Ubuntu. The following figure shows the one of the tested query.

The **HiveQL** (Hive Query Language) is

```
hive> create table population (ID int, FILEID string,
STUSAB string, CHARITER string, CIFSN string,
LOGRECNO string, POPCOUNT int) row format
delimited fields terminated by '\,' stored as textfile;

hive> load data inpath '/user/root/Rec250000.csv'
overwrite into table population;

hive> select STUSAB, sum(POPCOUNT) from
population group by STUSAB;
```

The **PigLatin** is

```
grunt> population = load '/user/root/families.csv' using
PigStorage(',') as (ID: int, FILEID:

chararray, STUSAB: chararray, CHARITER: chararray,
CIFSN: chararray, LOGRECNO: chararray,
POPCOUNT: int);

grunt>grouped = group population by STUSAB;

grunt> result = foreach grouped generate group,
SUM(population.POPCOUNT);

grunt> dump result;
```

The **Jaql** is

```
jaql>$ population = read(del("/user/root/families.csv", {
schema: schema { ID: long, FILEID: string, STUSAB:
string, CHARITER: string, CIFSN: string, LOGRECNO:
string, POPCOUNT: long} }));

jaql> $population -> group by $STUSAB={$.STUSAB}
into {$STUSAB, total:sum($[*].POPCOUNT)};
```

Figure 2. Sample query of Pig, Hive, Jaql and MapReduce transformation process

Figure 3 shows the query processing time of different query languages on different operating system by varying workloads.

According to this figure, other query languages take a large amount of time to execute a query. From a querying point of view, we can conclude that Hive query language and MapReduce Transformation Process of proposed platform is better than other query language on both OS and MapReduce Transformation Process is faster than Hive query language on Red Hat and Ubuntu also. From the operating system point of view, we can also conclude that the Red Hat OS is more convenient than Ubuntu OS for this proposed platform.

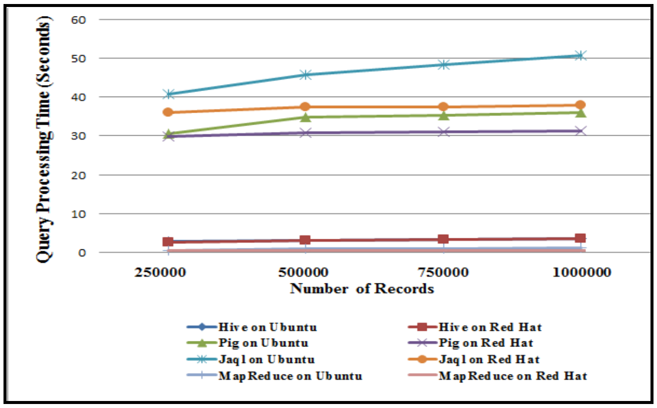


Figure 3. Comparison of query processing time on different OS

V. Conclusion

In this paper, we implement a big data analytic platform for mobile deivces. This platform operates with RESTful web service technology to provide seamless connectivity between mobile device and cloud storage. To improve the query performance, we developed a MapReduce Transformation Process to transform users' requests into MapReduce form. To control the complex query request, we implement a traditional querying method, HiveQL, in this platform. The analytical result is transferred to the mobile by using RESTful web service technology. As a result, performance evaluations are conducted to prove that the proposed platform provides three times faster than other high level query languages in both operating systems.

References

[1] D. Talia, "Clouds for Scalable Big Data Analytics", Computer, vol.46, no. 5, pp. 98-101, May 2013, doi:10.1109/MC.2013.162.

[2] A. Nandeshwar, “Tableau Data Visualiztion Cookbook”, Packt Publishing Ltd., August 26, 2013.

[3] S. Kaisler, F. Armour, A. Espinosa, "Introduction to Big Data: Scalable Representation and Analytics for Data Science Minitrack", HICSS, 2013, 2014 47th Hawaii International Conference on System Sciences, 2014 47th Hawaii International Conference on System Sciences 2013, pp. 984, doi:10.1109/HICSS.2013.292.

[4] S. Kaisler, F. Armour, J. A. Espinosa, "Introduction to Big Data: Challenges, Opportunities, and Realities Minitrack", HICSS, 2014, 2014 47th Hawaii International Conference on System Sciences (HICSS), 2014 47th Hawaii International Conference on System Sciences (HICSS) 2014, pp. 728, doi:10.1109/HICSS.2014.97.

[5] A. B. Waluyo, D. Taniar, B. Srinivasan, "The Convergence of Big Data and Mobile Computing", NBIS, 2013, 2013 16th International Conference on Network-Based Information Systems (NBiS), 2013 16th International Conference on Network-Based Information Systems (NBiS) 2013, pp. 79-84, doi:10.1109/NBiS.2013.15.

[6] K. Ebner, T. Buhnen, N. Urbach, "Think Big with Big Data: Identifying Suitable Big Data Strategies in Corporate Environments", HICSS, 2014, 2014 47th Hawaii International Conference on System Sciences (HICSS), 2014 47th Hawaii International Conference on System Sciences (HICSS) 2014, pp. 3748-3757, doi:10.1109/HICSS.2014.466.

[7] C. Chung, D. Egan, A. Jain, N. Caruso, C. Misner, R. Wallace, "A Cloud-Based Mobile Computing Applications Platform for First Responders", SOSE, 2013, 2013 IEEE Seventh International Symposium on Service-Oriented System Engineering, 2013 IEEE Seventh International Symposium on Service-Oriented System Engineering 2013, pp. 503-508, doi:10.1109/SOSE.2013.26.

[8] K.S. Beyer, V.Ercegovac, R.Gemulla, A.Balmin, “Jaql: A Scripting Language for Large Scale Semistructured Data Analysis”, In Proceedings of the VLDB Endowment, Vol.4, No.12, 2011, pp. 1272-1283.

[9] C. T. Chu, S. K. Kim, Y. A. Lin, Y. Yu, et al., “Map-Reduce for Machine Learning on Multicore”, Advances in Neural Information Processing System (NIPS’ 06), MIT Press,2006, pp.281-288.

[10] J. Dean and S. Ghemawat, “MapReduce: A Flexible Data Processing on Large Clusters”, Proc. “6th Symposium on Operating Systems Design and Implementation, San Francisco, CA, USA, December 6-8, 2004, pp.137-149.

[11] J. Dean and S. Ghemawat, “MapReduce: A Flexible Data Processing Tool”, Communications of the ACM, Vol.53, No.1, January 2010, pp.72-77.

[12] J. Ekanayake, S. Pallickara, and G. Fox, “MapReduce for Data Intensive Scientific Analyses”, Proc. “IEEE 4th International Conference on eScience (eScience’08), Washington, DC, USA, December 7-12, 2008, pp.277-284.

[13] J.Lin, “Brute Force and Indexed Approaches to Pariwise Document Similartiy Comparisons with MapReduce”, Proc. “32nd Annual International ACM SIGIR Conference on Research and Development in Information Retrieval (SIGIR 2009), Boston, Massachusetts, July 19-23, 2009, pp. 155-162.

[14] J.Rutherglen, D.Wampler and E.Capriolo, “Programming Hive”, O’Reilly Media, Inc., October 2012.

[15] A.Thusoo, J.S.Sarma, N.Jain,Z.Shao, ”Hive-A Petabyte Scale Data Warehouse Using Hadoop”, In Proceedings of the 26th International Conference on Data Engineering, Long Beach, CA, USA, March 1-6, 2010, pp.996-1005.

[16] A.Thusoo, J.S.Sarma, N.Jain,Z.Shao, ”Hive-A Warehousing Solution Over a Map-Reduce Framework”, In Proceedings of VLDB Endowment, Vol.2, Issue. 2, August 2009, pp. 1626-1629.

[17] A. Gates, “Programming Pig”, O’Reilly Media, Inc., October 2011.

[18] C.Olston, B.Reed, U.Srivastava, R.Kumar, “Pig Latin: A Not-So-Foreign Language for Data Processing”, In Proceedings of the 2008 ACM SIGMOD International Conference on Management of Data (SIGMOD 2008), Vancouver, BC, Canada, June 9-12, 2008, pp. 1099-1110..357670.

[19] K.Shvachko, H.Kuang, S. Radia and R.Chansler, “The Hadoop Distributed File System”, In Proceedings of the 2010 IEEE 26th Symposium on Mass Storage Systems and Technologies, Incline Village, NV, USA, May3-7, 2010, pp.1-10.

[20] http://www2.census.gov/census_2010/04-Summary_File_1

Face Recognition based on Spatial and Transform domain techniques

Jagadeesh H S
Dept. of Electronics and Communication Engineering
APSCE, Bangalore, India

Suresh Babu K
Dept. of Electronics and Communication Engineering
UVCE, Bangalore, India

K B Raja
Dept. of Electronics and Communication Engineering
UVCE, Bangalore, India

Abstract *— Real time challenges are eternal for verification and recognition of a person using face biometric. In this paper, we propose an efficient algorithm using Extended Directional Binary codes (EDBC) with Discrete Wavelet Transform (DWT) and Singular Value Decomposition (SVD) with Discrete Cosine Transform (DCT). In preprocessing, the face images are refined to make them suitable for feature extraction. The Approximate (LL) band is extracted by applying DWT. One hundred EDBC features are extracted using LL sub band. Additionally, DCT is applied on pre-processed image and one hundred SVD features are extracted from DCT out put. Final one hundred distinct features are derived by fusing each of one hundred EDBC and SVD features. The features comparison is performed using Euclidean Distance (ED) measure to produce the results. Performance on JAFFE and ORL face datasets shows that the proposed algorithm is superior in different metrics compared to other existing methods***.

Keywords- Discrete wavelet transform; Euclidean distance; Extended directional binary codes; Face biometric; Singular value decomposition.

I. INTRODUCTION

National security issues have to be paid highest priority than others in the present scenario. Threats through territory interfaces such as land, naval and airports cannot be neglected. Human beings has major role in creating these threats, hence person identification is the critical stage in any technological implementation. Applications using biometrics have deployed enough to recognize humans. Biometrics are either physical structure of organs or any behavioral trait associated with human beings. Hand geometry, fingerprint, face, iris are some physiological biometric parameters normally extracted directly [1] and the activities such as typing style, voice, gait are few behavioral parameters. Each biometric parameter has its own advantage and disadvantage in different applications. Face biometric has distinct advantage of non intrusive and captured without the cooperation of humans also. Facial expression recognition [2] is an augmented part any approach.

A general Face Recognition (FR) system accepts face images as input and processed in different steps to give decisions e.g. known/ unknown person, any details of the same person. Major steps of FR are preprocessing, feature extraction and matching. The performance of a FR system is influenced by resolution of input images, methods and tools used at different steps. If the input contains low resolution [3] images or having variation in illumination, pose [4] and expression [5], they are improved in its quality through preprocessing. Principal Component Analysis (PCA) is used to handle the data corrupted by error [6] and it reduces the dimension [7] of input data also. Pose is another vital factor which affects on the appearance of image and in-turn on the performance of recognition algorithm [8]. Many tools such as Discrete Cosine Transform (DCT) [9], Discrete Wavelet Transform (DWT), Local Binary Patterns (LBP) [10], Singular Value Decomposition (SVD) and many others are used to derive unique features. Directional Binary Codes (DBC) [11] on Hong Kong Polytechnic University Near Infra Red (Poly-U NIR) face database have promising performance. Then DBC with DWT combination used in [12], have shown an improvement in recognition accuracy. The accuracy varies for expression and poses variation with different databases. The Extended DBC (EDBC) proposed in our work extracts precise texture features in all directions contributes to improve efficiency. The energy efficient DCT with SVD join hands towards distinct features extraction and to boost performance. Access control [13], surveillance, law enforcement, driving licenses, ATMs for bank [14], tele-medicine, information security, and forensics [15] applications uses biometrics.

Contribution: DE-DS FR algorithm is proposed to recognise the face of a person, which uses EDBC and SVD to extract features. Face cropping and resizing are performed as pre-processing. Euclidean distance measure is used for matching.

Organization: Rest of the paper is organized as follows; survey of related work is in section II; DE-DS FR model and algorithm is in section III and IV respectively. Performance is discussed in section V and inferred in section VI.

II. RELATED WORK REVIEW

Rasber D Rashid et al., [16] proposed a feature extraction algorithm for face recognition problem using Local Binary Patterns (LBP) and wavelets. LBP histograms are derived from the approximation sub band of wavelets. The face image is represented by single histogram. Results using Euclidean distance matching on Yale and ORL databases are better compared to other LBP based methods. Radhey Shyam and Yogendra Narain Singh, [17] presented augmented local binary patterns for face recognition in uncontrolled environments. The proposed method works on uniform and non-uniform patterns locality, then computes Bray Curtis dissimilarity metric. Performance is substantially improved on Yale A and Extended Yale B database. Yang Zhao et al., [18] proposed completed robust local binary pattern and weighted local gray level for texture classification. The proposed scheme replaces central pixel by average gray level of 3*3 dimensions. It is immune to noise and illumination variants. Experimental results on texture databases such as Outex database, UIUC database, CUReT database, and XU_HR database achieves better classification accuracy.

Jianfeng Ren et al., [19] proposed a Transformation for converting LBP feature appropriate to Gaussian distribution. Asymmetric principal component analysis is used to remove the unreliable dimensions. Euclidean distance with nearest neighbor classifier is used as the baseline algorithm. The proposed algorithm is evaluated for face recognition, dynamic texture recognition, and protein cellular classification. The performance is consistent on 8 different datasets. Di Huang et al., [20] presented a 3D face representation scheme using multi-scale extended local binary patterns with SIFT feature matching. The discriminative power of proposed approach for recognition and verification of face is proved better on FRGC v2.0 database. Khoa Luu et al., [21] introduced an age-determination technique using hybrid facial features with Kernel Spectral Regression (KSR). The input image is preprocessed using logarithmic non sub sampled contourlet transform. Uniform local ternary patterns are the local features and holistic features are extracted by active appearance model. The combination of local and holistic features yields hybrid facial features. Feature set`s inter class distances are minimized and intra class distances are maximized using KSR. The efficacy of proposed approach yields promising results on FGNET, PAL and Vietnamese Longitudinal Face database.

Fujin Zhong et al., [22] proposed discriminant locality preserving projection method for face recognition problem. It uses L-1 norm for preserving dispersion between classes and within a class. The proposed method is feasible and robust to outliers by overcoming the small sample size problem. The experimental results on artificial, Binary Alpha digits, FERET face and Poly U palm print dataset have demonstrated the effectiveness of the proposed method. Bing-Kun Bao et al., [23] proposed Corruptions Tolerant Discriminant Analysis (CTDA) algorithm to capture the features with high amount of similarity within class. CTDA can handle well the gross corruptions existing in the training data. Experiments on CMU PIE, FERET, and AR face data sets and Pittsburgh food image dataset object recognition data set show that CTDA outperforms compared to other related algorithms.

Sumit Shekhar et al., [24] proposed a sparse representation method for multimodal biometrics recognition. Alternative direction method is used to solve the optimization problem and data nonlinearity is handled by kernelizing the algorithm. Recognition accuracy is improved on AR face database and WVU multimodal data set. Meng Yang et al., [25] presented a regularized coding model with iterative feature for robust face recognition. The maximum posterior estimation solves coding problem and weights are assigned based on coding residuals of each pixel iteratively. Results are better on AR, Extended Yale B and Multi-PIE databases compared with other state of the art methods. Zizhu Fan et al., [26] proposed Weighted SRC (WSRC) method for representation and classification problem. It computes the weight for a training sample according to the distance or similarity relationship. WSRC concentrates those training samples which are similar to the test sample. The experiments on AR, Georgia Tech (GT), CMU PIE, and Labeled Faces in the Wild face data sets show that the proposed algorithm can achieve desirable recognition performance.

Yunlian Sun and Massimo Tistarelli, [27] presented Coarse to fine sparse representation technique for the recognition of faces. The coarse phase determines an individual dictionary for each test sample to produce the least residual with nearest neighbours. The experimental results on Extended Yale B, AR and ORL face databases shows competitive performance in comparison with other state-of-the-art techniques. JunYing Gan et al., [28] designed a real-time face recognition system based on IP camera and SRC algorithm using OpenCV and C++ programming. The algorithm has reconfigured to process the video frame also. AdaBoost algorithm is used to detect face in each frame, and then LBP is used to extract the textual features. The results show that the system can deal with real-time video and is robust to illumination. Xingjie Wei et al., [29] proposed Dynamic Image to Class Warping (DICW) algorithm for the recognition of occluded faces. Dynamic programming technique is used to compute the image to class distance for classification. Experiments on the FRGC, AR, The face we make and LFW face databases show that DICW achieves promising performance on various types of occlusions.

Jian Zhang et al., [30] presented Nearest Orthogonal Matrix Representation (NOMR) for face recognition. The specific individual subspace of each image is estimated and represented uniquely by singular value decomposition. The proposed NOMR is more robust for alleviating the effect of illumination and powerful in handling the small sample size problem. Performance on Extended Yale B, CMU-PIE, FRGCv2, AR and CUHK Face Sketch databases demonstrated encouraging performance compared with the state-of-the-art methods. Dapeng Tao et al., [31] proposed human behaviour recognition scheme for wireless sensor networks using hamming sensing, Rank Preserving Discriminant Analysis (RPDA) and a nearest neighbour classifier. RPDA encodes local rank information of within class samples and discriminative information of the between class using patch alignment framework. Performance on the SCUT Naturalistic 3D acceleration based activity dataset demonstrate the effectiveness of RPDA for human behaviour recognition. Jing Wang et al., [32] proposed Adaptive Sparse Representation-Based Classification (ASRC) framework, in which sparsity and correlation are jointly considered. For the samples with low correlation, ASRC selects the most discriminative samples for representation, like SRC; when the training samples are highly correlated, ASRC selects most of the correlated and discriminative samples for representation, rather than choosing some related samples randomly. Experiments on UCI repository data sets verify the robustness of the proposed algorithm by comparing it with the state-of-the art methods.

III. PROPOSED WORK

The definitions for performance analysis and the block diagram of the proposed DWT - EDBC and DCT- SVD based Face Recognition with (DE - DS FR) model are discussed in this section.

A. *Definitions*

- False Acceptance Rate (FAR): It is the ratio between the number of unauthorized persons accepted to total number of un-authorized persons.
- False Rejection Rate (FRR): It is the ratio between the number of authorized persons rejected to total number of authorized persons in the database.
- Total Success Rate (TSR) or Recognition Rate (RR) [17]: It is the ratio between number of persons recognized correctly to total number of persons in database.
- Equal Error Rate (EER) : It is a point at which the value of FRR is same as FAR value.
- Error Rate (ER): It is the redundancy associated with RR and given by ER= 1-RR.

B. *Block Diagram*

Explanation for the proposed DE - DS FR model shown in Figure 1 is as follows.

1) *Datsbases*

The performance of proposed work is evaluated on Japanese Female Facial Expression (JAFFE), and Olivetti Research Laboratory (ORL) face databases. The JAFFE [33], database consists of 10 Japanese female subjects with 20 images per subject of 7 facial expressions. The horizontal and vertical resolution of each image is 100 dpi (dots per inch) with 8 bits depth and the size is 256*256. JAFFE database samples of a person with different expressions are as shown in Figure 2.

The ORL face database [34], has 40 different subjects each with 10 images. The images captured at different times with varying lighting intensities. In addition, facial expression variations such as opening or closing of eyes, smiling or non-smiling face images and wearing or without wearing glasses facial images are also present in the data base. All the subjects are in up-right, frontal position and the images are acquired against a dark homogeneous background. All images are in JPEG format with each image of size 92*112 size and represented by 8-bit grey levels. The horizontal and vertical resolution of each image is 96 dpi. Figure 3 shows the sample of images of different persons in ORL face database.

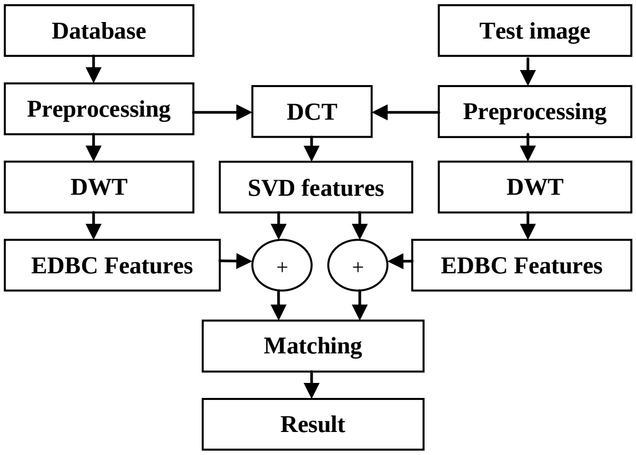


Figure 1. Block diagram of the proposed DE - DS FR model

2) *Pre-processing*

To make appropriate for feature extraction, the database and test images are refined in pre-processing. The gray scale images are converted to binary before applying following two steps.

a) *Face cropping*

The details such background and any redundant part in input image has no impact in person identification. Hence, more precise portion of face is elicited in cropping and then it is divided into two parts. Each part is scanned horizontally and vertically to identify and remove redundant area in the image.

b) *Image resizing*

The dimension of all cropped images may not be same; hence all cropped images are uniformly resized to 100*100. Figure 4 shows the effect of pre-processing on ORL data base face image.

Figure 2: JAFFE database image samples of a person

Figure 3: ORL database image samples of three persons

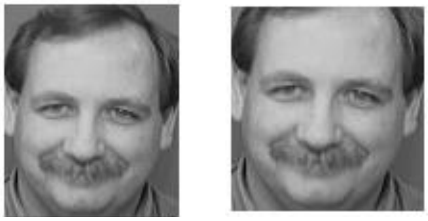

(a) (b)

Figure 4: Pre-processing effect (a) Original image (b) Pre-processed image

3) Feature extraction

The vital facial features of each image are elicited using Extended Directional Binary codes (EDBC) and Singular Value Decomposition (SVD) separately and fused. In addition with existing DBC (4-DBC), which extracts four directional information, eight directional infromation is extracted and named as EDBC (8-DBC). The one level DWT with Haar wavelet [35], is used to decompose preprocessed image. Output of DWT contains approximation and detail components such as LL, HL, LH, HH sub bands, where LL is approximate, and HL, LH, HH are horizontal, vertical, diagonal sub bands respectively. The output size of each sub band is reduced to half compared with input size, which makes processing time faster. LL sub band is used to extract features as it contains more appropriate details compared to remaining three sub bands.

EDBC is applied on LL sub band of DWT output to extract the eight directional details. EDBC determines spatial relationship in all eight directions associated with eight different neighborhood pixels. The LL band of size 50*50 is partitioned into 100 cells each with 5*5 size. For each cell, first order derivative $I'_{\alpha,d}$ is computed, where $\alpha = 0^0, 45^0, 90^0, 135^0, 180^0, 225^0, 270^0, 315^0$ and d is the distance between the given point and its neighboring point. The eight directional derivatives $(I'_{\alpha,d})$ at a point $z_{i,j}$ are calculated using Equations from 1 to 8. Equation 9 converts derivative form to binary form. Only central 9 values out of 25 values of a 5*5 matrix of each cell, forms 9 bit binary code as shown in Figure 5 and the sequence of reading is given in Equation 10.

	$I_{i-1,j-1}$	$I_{i-1,j}$	$I_{i-1,j+1}$	
	$I_{i,j-1}$	$I_{i,j}$	$I_{i,j+1}$	
	$I_{i+1,j-1}$	$I_{i+1,j}$	$I_{i+1,j+1}$	

*Figure 5. A 5*5 cell with bolded 3*3 central mask*

The computed EDBCs along 0^0, 45^0, 90^0, 135^0, 180^0, 225^0, 270^0, and 315^0 directions with corresponding decimal values (inside bracket) are given by: $EDBC_{0,1}$ = 110000110 (390), $EDBC_{45,1}$ = 110001101 (397), $EDBC_{90,1}$ = 100010111 (279), $EDBC_{135,1}$ = 101111000 (376), $EDBC_{180,1}$ = 111101100 (492), $EDBC_{225,1}$ = 111011100 (476), $EDBC_{270,1}$ = 101011000 (344), $EDBC_{315,1}$ = 110010111 (407). Figure 6 depicts the complete process of EDBC features extraction.

$$I'_{0,d}(z_{i,j}) = I(z_{i,j}) - I(z_{i,j+d}) \tag{1}$$
$$I'_{45,d}(z_{i,j}) = I(z_{i,j}) - I(z_{i-d,j+d}) \tag{2}$$
$$I'_{90,d}(z_{i,j}) = I(z_{i,j}) - I(z_{i-d,j}) \tag{3}$$
$$I'_{135,d}(z_{i,j}) = I(z_{i,j}) - I(z_{i-d,j-d}) \tag{4}$$
$$I'_{180,d}(z_{i,j}) = I(z_{i,j}) - I(z_{i,j-d}) \tag{5}$$
$$I'_{225,d}(z_{i,j}) = I(z_{i,j}) - I(z_{i+d,j-d}) \tag{6}$$
$$I'_{270,d}(z_{i,j}) = I(z_{i,j}) - I(z_{i+d,j}) \tag{7}$$
$$I'_{315,d}(z_{i,j}) = I(z_{i,j}) - I(z_{i+d,j+d}) \tag{8}$$

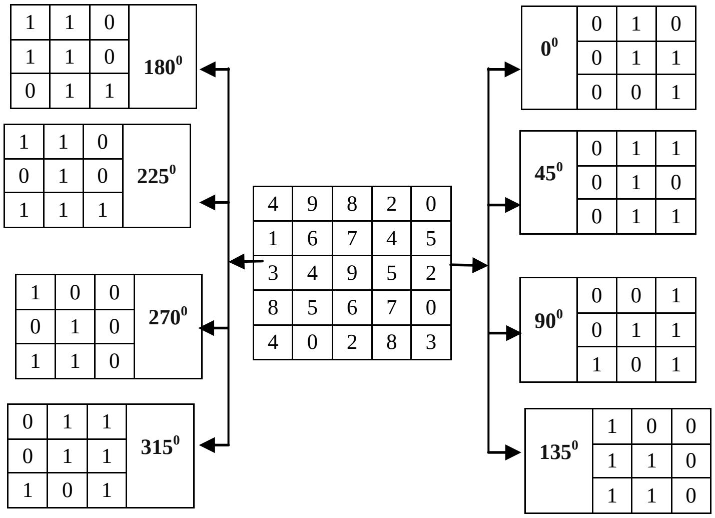
$$f\left(I'_{\alpha,d}(z)\right) = \begin{cases} 0, & I'_{\alpha,d}(z) \le 0 \\ 1, & I'_{\alpha,d}(z) > 0 \end{cases} \tag{9}$$

$$EDBC_{\alpha,d}(z_{i,j}) = \{ f(I'_{\alpha,d}(z_{i,j})), f(I'_{\alpha,d}(z_{i-d,j})), f(I'_{\alpha,d}(z_{i-d,j-d})), f(I'_{\alpha,d}(z_{i,j-d})), f(I'_{\alpha,d}(z_{i+d,j-d})), f(I'_{\alpha,d}(z_{i+d,j})), f(I'_{\alpha,d}(z_{i+d,j+d})), f(I'_{\alpha,d}(z_{i,j+d})), f(I'_{\alpha,d}(z_{i-d,j+d})) \} \tag{10}$$

On the other side, Discrete Cosine Transform (DCT) is applied on the preprocessed image to produce energy compacted image. The basis function of DCT is real and easy to compute. SVD is computed on DCT output image, which retains textual features. SVD is a process of factorizing a given matrix in to three parts, consisting of Left Singular Vectors (LSV), singular values and Right Singular Vectors (RSV). SVD [36] of a matrix A with M*N dimension is given in Equation 11.

$$A = USV^T \tag{11}$$

Where, U (LSV) is a M*M orthogonal matrix contains Eigen vectors as columns of AA^T, V (RSV) is a N*N orthogonal matrix whose columns are the Eigen vectors of A^TA, and S is a M*N diagonal matrix contains singular values in decreasing magnitudes till, r = rank (A).



4	9	8	2	0
1	6	7	4	5
3	4	9	5	2
8	5	6	7	0
4	0	2	8	3

180⁰

1	1	0
1	1	0
0	1	1

225⁰

1	1	0
0	1	0
1	1	1

270⁰

1	0	0
0	1	0
1	1	0

315⁰

0	1	1
0	1	1
1	0	1

0⁰

0	1	0
0	1	1
0	0	1

45⁰

0	1	1
0	1	0
0	1	1

90⁰

0	0	1
0	1	1
1	0	1

135⁰

1	0	0
1	1	0
1	1	0

Figure 6. EDBC along 8- directions

The diagonal elements of S are square roots of the Eigen values of A^TA named as singular values of A and are always real in nature. Even matrices U and V are also real, when matrix A is real. Consider an image of JAFFE database with size 256*256 as shown in Figure 7. Resized matrix of the same image of size 10*10 is represented in matrix Equation 12 and corresponding ten singular values of matrix A are [1106.27, 247.48, 213.11, 94.56, 42.80, 32.39, 25.6, 12.05, 10.64, 5.22]. SVD is applied on the DCT output of size 100*100 to generate 100 singular values; these are fused with 100 EDBC features to yield final 100 features.

4) *Matching*

Final step of the proposed work is to produce the results. The system has to verify and decide whether test image is in database or not, and also to validate correct recognition of a person. Euclidean Distance (ED) measure is used to generate the result. Let $I(p_1,q_1)$ and $J(p_2,q_2)$ are any two points on a given 2D plane, then ED is calculated by Equation 13. The ED value between feature vectors of a test image and feature vectors of all images in the database are computed. Image number and the corresponding Person in the database are identified based on minimum ED value. Finally, ED values of all images are compared with entire threshold range varied from 0 to 1 in steps of 0.1 or still precise.

RR is calculated based on correct matching count of persons. Correct matching count is incremented when ED value is less than the threshold and also the queried person should be same as database person. On the other hand, mismatch occurs if the ED value is less than the threshold and person from the database and test image of a person are different. FRR is a count incremented when the ED value is greater than threshold, infers that the person in the database is falsely rejected.

Figure 7: JAFFE database image

$$B=\begin{pmatrix} 127 & 148 & 164 & 147 & 114 & 131 & 163 & 160 & 149 & 138 \\ 128 & 140 & 91 & 14 & 0 & 8 & 56 & 126 & 145 & 142 \\ 117 & 104 & 4 & 4 & 58 & 69 & 14 & 61 & 130 & 132 \\ 116 & 75 & 0 & 62 & 176 & 189 & 119 & 33 & 124 & 130 \\ 113 & 66 & 17 & 91 & 132 & 144 & 92 & 72 & 129 & 130 \\ 100 & 64 & 62 & 128 & 142 & 154 & 148 & 127 & 140 & 135 \\ 92 & 84 & 64 & 161 & 154 & 155 & 189 & 147 & 142 & 141 \\ 97 & 80 & 22 & 93 & 95 & 107 & 136 & 135 & 133 & 135 \\ 90 & 70 & 42 & 45 & 54 & 69 & 108 & 123 & 120 & 132 \\ 77 & 101 & 135 & 145 & 77 & 137 & 173 & 149 & 129 & 121 \end{pmatrix} \quad (12)$$

$$ED\ (I, J) = \sqrt{((p_1-p_2)^2 + (q_1-q_2)^2\ )} \qquad (13)$$

For FAR calculation, the test images are taken from out of database and ED value is compared for all images of database. FAR count is incremented by one when the ED value is less than threshold, which conveys that even the image is not there in database, but falsely accepting. Lastly, if the ED value is higher than threshold, it is considered as mismatch and to conclude that the system is correctly rejecting.

IV. ALGORITHM

Problem definition: Identification of a person is made by using EDBC and SVD based Face Recognition system with DWT & DCT (DE - DS FR). The objectives are as follows:

- To improve the RR
- To reduce FRR and FAR.

The proposed DE-DS FR model algorithm is shown in Table I.

V. PERFORMANCE ANALYSIS

The proposed algorithm is tested on JAFFE and ORL face database.

A. *Performance analysis using JAFFE database*

JAFFE database consists of 10 persons with 20 images per person. For 8 persons each with 18 images are considered for database and remaining images are used for testing. The experiments are conducted to observe performance of EDBC with SVD (without DCT) by varying number of images used for database. Table II compares %FRR, %FAR and %RR for 12, 15 and 18 images used for database. As the number of trained images are increasing, the % RR is also increasing e.g. % RR is 37.5, 50 and 62.5 at 0.4 threshold and reaches to maximum of 87.5, 100 and 100 respectively for the 3 cases.

The performance on JAFFE database is tested for both DBC and EDBC with SVD (without DCT). The Table III compares %FRR, %FAR and %RR for different values of threshold on JAFFE database. The %RR is 25 % higher in EDBC with SVD compared with DBC with SVD at 0.5 threshold value.

TABLE I. ALGORITHM OF PROPOSED DE-DS FR MODEL

Input: Database and Probe images of face
Output: Identification / Refutation of a person.

1. Preprocessing involves resizing an image to 100*100 after face cropping.
2. Approximate band of 50*50 size is considered by applying DWT.
3. Approximate band is divided into 100 cells with each cell of 5*5 size.
4. Computation of 8 - directional derivatives for each cell.
5. 9-bit code generated from each cell along 8- directions & converted into its decimal equivalent.
6. One decimal value per cell in all directions correspondingly averaged to constitute 100 features.
7. DCT of preprocessed image is performed.
8. SVD is computed on DCT output & fused with 100 co-efficient features of step 6.
9. Euclidean Distance between database and test image feature vectors is computed.
10. Matching is decided for an image with minimum distance.

TABLE II. PERFORMANCE OF EDBC WITH SVD ON JAFFE DATABASE (WITHOUT DCT)

Threshold	Case-1 : 12 images database			Case-2 : 15 images database			Case-3 : 18 images database		
	% FRR	% FAR	% RR	% FRR	% FAR	% RR	% FRR	% FAR	% RR
0.0	100	0	0	100	0	0	100	0	0
0.1	100	0	0	100	0	0	100	0	0
0.2	100	0	0	100	0	0	100	0	0
0.3	75	0	25	100	0	0	100	0	0
0.4	62.5	0	37.5	50	0	50	37.5	0	62.5
0.5	37.5	50	62.5	0	50	100	0	50	100
0.6	0	50	87.5	0	50	100	0	50	100
0.7	0	100	87.5	0	100	100	0	100	100
0.8	0	100	87.5	0	100	100	0	100	100
0.9	0	100	87.5	0	100	100	0	100	100
1.0	0	100	87.5	0	100	100	0	100	100

TABLE III. PERFORMANCE COMPARISON ON JAFFE DATABASE (WITHOUT DCT)

Thres hold	DBC with SVD			EDBC with SVD		
	% FRR	% FAR	% RR	% FRR	% FAR	% RR
0.0	100	0	0	100	0	0
0.1	100	0	0	100	0	0
0.2	100	0	0	100	0	0
0.3	87.5	0	12.5	100	0	0
0.4	62.5	0	37.5	37.5	0	62.5
0.5	25	0	75	0	50	100
0.6	0	100	100	0	50	100
0.7	0	100	100	0	100	100
0.8	0	100	100	0	100	100
0.9	0	100	100	0	100	100
1.0	0	100	100	0	100	100

The plot of FAR and FRR versus threshold on JAFFE database using SVD with DBC and EDBC (without DCT) is in Figure 8 and 9 respectively. Optimum %RR on JAFFE database is obtained at EER i.e. when both %FRR and %FRR are same.

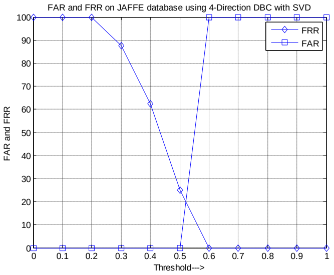


Figure 8: FAR & FRR versus threshold on JAFFE database using DBC with SVD (Without DCT)

TABLE IV.
PERFORMANCE COMPARISON OF SVD WITH DBC & EDBC ON JAFFE DATABASE (WITHOUT DCT)

Method	EER	Optimum % RR	Maximum %RR
DBC with SVD	20	80	100
EDBC with SVD	22	87.5	100

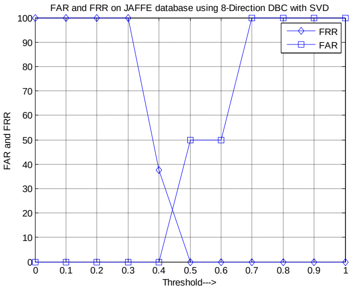


Figure 9: FAR & FRR versus threshold on JAFFE database using EDBC with SVD (Without DCT)

Table IV compares EER, Optimum %RR and Maximum % RR for DBC with SVD and EDBC with SVD. Individual effect of EDBC, SVD (with DCT) and the combination of both for different values of threshold is observed. Table V depicts the results of EDBC with DWT, DCT–SVD combination and features fusion of both combinations. Results reveal that the fusion has improved the performance against to individual performances.

TABLE V. PERFORMANCE COMPARISON OF SVD WITH DBC & EDBC ON JAFFE DATABASE (WITH DCT)

Threshold	EDBC			SVD			EDBC with SVD		
	% FRR	% FAR	% RR	% FRR	% FAR	% RR	% FRR	% FAR	% RR
0.0	100	0	0	100	0	0	100	0	0
0.1	100	0	0	25	0	75	100	0	0
0.2	100	0	0	0	100	87.5	25	50	75
0.3	100	0	0	0	100	87.5	0	100	100
0.4	37.5	0	62.5	0	100	87.5	0	100	100
0.5	0	50	100	0	100	87.5	0	100	100
0.6	0	50	100	0	100	87.5	0	100	100
0.7	0	100	100	0	100	87.5	0	100	100
0.8	0	100	100	0	100	87.5	0	100	100
0.9	0	100	100	0	100	87.5	0	100	100
1.0	0	100	100	0	100	87.5	0	100	100

Compared to other approaches such as [37], [38], and [39], our proposed algorithm has better %RR on JAFFE database as in Table VI.

TABLE VI. RECOGNITION RATE COMPARISION ON JAFFE DATABASE (WITH DCT)

Method	Maximum % RR
DSNGE +SVM [37]	68.85
PCA based GA [38]	96
GABOR - SVD [39]	98
Proposed DE-DS FR model	100

B. Performance analysis using ORL database

The performance is tested on ORL face database, consisting of 40 persons with 10 images per person. For 36 persons each with 9 images is considered for database and remaining images are used for testing. Table VII compares %FRR, %FAR and %RR using both DBC and EDBC with SVD (without DCT) for 0 to 1 threshold variation. The %RR attains maximum of 82.85 and 88.57 for both DBC and EDBC with SVD respectively. The plot of FAR and FRR versus threshold on ORL face database for both DBC and EDBC with SVD is in Figure 10 and 11 respectively. Table VIII compares EER, optimum %RR and Maximum % RR using SVD with DBC and EDBC (without DCT).

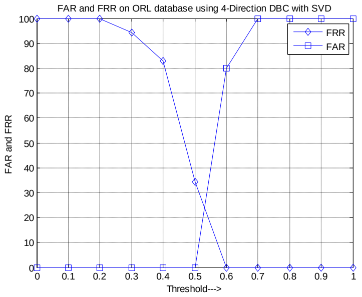


Figure 10: FAR & FRR versus threshold on ORL database using DBC with SVD (Without DCT)

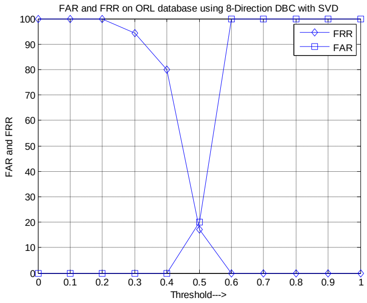


Figure 11: FAR & FRR versus threshold on ORL database using EDBC with SVD (Without DCT)

TABLE VII. PERFORMANCE COMPARISON OF SVD WITH DBC & EDBC ON ORL DATABASE (WITHOUT DCT)

Thres hold	DBC with SVD			EDBC with SVD		
	% FRR	% FAR	% RR	% FRR	% FAR	% RR
0.0	100	0	0	100	0	0
0.1	100	0	0	100	0	0
0.2	100	0	0	100	0	0
0.3	94.28	0	5.71	94.28	0	5.71
0.4	82.85	0	17.14	80	0	20
0.5	34.28	0	60	17.14	20	74.28
0.6	0	80	82.85	0	100	88.57
0.7	0	100	82.85	0	100	88.57
0.8	0	100	82.85	0	100	88.57
0.9	0	100	82.85	0	100	88.57
1.0	0	100	82.85	0	100	88.57

TABLE VIII. PERFORMANCE COMPARISON ON ORL DATABASE (WITHOUT DCT)

Method	EER	Optimum %RR	Maximum %RR
DBC with SVD	25	60	82.5
EDBC with SVD	20	74.28	88.57

TABLE IX. PERFORMANCE COMPARISON OF SVD WITH DBC & EDBC ON ORL DATABASE (WITH DCT)

Threshold	EDBC			SVD			EDBC with SVD		
	% FRR	% FAR	% RR	% FRR	% FAR	% RR	% FRR	% FAR	% RR
0.0	100	0	0	100	0	0	100	0	0
0.1	100	0	0	34.28	0	57.14	100	0	0
0.2	100	0	0	0	80	74.28	100	0	0
0.3	94.28	0	5.71	0	100	74.28	94.44	0	5.56
0.4	80	0	20	0	100	74.28	80.56	0	19.44
0.5	17.14	20	74.28	0	100	74.28	19.44	25	72.22
0.6	0	100	88.57	0	100	74.28	0	100	88.89
0.7	0	100	88.57	0	100	74.28	0	100	88.89
0.8	0	100	88.57	0	100	74.28	0	100	88.89
0.9	0	100	88.57	0	100	74.28	0	100	88.89
1.0	0	100	88.57	0	100	74.28	0	100	88.89

Further the algorithm is tested to observe rationale of individual components such as DWT-EDBC and DCT-SVD separately, then the combined effect of both on ORL face database. The results are in Table IX, which justifies that features fusion yields improved performance. Table X compares the maximum %RR with other algorithms such as [40], [41] and the Error Rate is compared in Table XI with [42]. It is clear that the proposed algorithm has superior results compared to existing algorithms.

The major reasons for results improvement are; the LL band coefficients of DWT have significant information and compressed version of the original image. Using texture features of LL band which are derived using EDBC, yields less recognition rate, as the edge information of the original image is neglected. The SVD is applied on DCT compressed coefficients results in less recognition rate, but SVD reduces the effect of noise due to illumination variation [39]. Singular values of SVD are invariant to translation and rotation. The arithmetic addition of EDBC and SVD is used in fusion technique to generate final set of features has better performance compared to EDBC and SVD alone.

TABLE X. RECOGNITION RATE COMPARISION ON ORL DATABASE (WITH DCT)

Method	Maximum % RR
Local Features + Bayesian classifier [40]	78.75
DWT with FKNN classifier [41]	87
Proposed DE-DS FR model	88.89

TABLE XI. COMPARISON OF % ERROR RATE ON ORL DATABASE (WITH DCT)

Method	% Error Rate
Schur faces [42]	15
Proposed DE-DS FR model	11.11

VI. CONCLUSION

Verification and recognition of persons using biometrics have no ideal solutions in real time. An efficient method using DWT-EDBC and DCT-SVD combination for face recognition is proposed. In preprocessing scanning and cropping of the vital part of face is performed and then it is resized to 100*100. The LL band of DWT with size 50*50 is used. EDBC is applied on LL band to elicit one hundred features. Concurrently the preprocessed image is transformed using DCT and SVD is applied on DCT output to generate another one hundred features. Finally both EDBC and SVD features are fused to yield one hundred distinct features. The matching results based on ED measure is are computed. The performance on JAFFE and ORL face datasets are better compared with other existing algorithms.

REFERENCES

[1] Juhi Malhotra and Netra Raina, “Biometric Face Recognition and Issues,” Second IEEE International Conference on Computing for Sustainable Global Development, pp. 1239- 124, March 2015.

[2] Thiago H.H. Zavaschi, Alceu S. Britto Jr. Luiz E.S. Oliveira, Alessandro L. Koerich, “Fusion of feature sets and classifiers for facial expression recognition,” ELSEVIER International journal on Expert Systems with Applications, Vol. 40, Issue 2, pp. 646–655, February 2013.

[3] Soma Biswas, Gaurav Aggarwal, Patrick J. Flynn, and Kevin W. Bowyer, “Pose-Robust Recognition of Low-Resolution Face Images,” IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol. 35, No. 12, pp. 3037- 3049, December 2013.

[4] Ramzi Abiantun, Utsav Prabhu, and Marios Savvides, “Sparse Feature Extraction for Pose-Tolerant Face Recognition,” IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol. 36, No. 10, pp. 2061 – 2073, October 2014.

[5] Jiwen Lu, Venice Erin Liong, Gang Wang, and Pierre Moulin, “Joint Feature Learning for Face Recognition,” IEEE Transactions on Information Forensics and Security, Vol. 10, No. 7, pp. 1371 -1383, July 2015.

[6] Bing-Kun Bao, Guangcan Liu, Changsheng Xu and Shuicheng YanKai, “Inductive Robust Principal Component Analysis,” IEEE Transactions on Image Processing, Vol. 21, No. 8, pp. 3794- 3800, August 2012.

[7] Huu-Tuan Nguyen and Alice Caplier, “Local Patterns of Gradients for Face Recognition,” IEEE Transactions on Information Forensics and Security, Vol. 10, No. 8, pp. 1739 – 1751, August 2015.

[8] Changxing Ding, Chang Xu, and Dacheng Tao, “Multi-task Pose-Invariant Face Recognition,” IEEE Transactions on Image Processing, Vol. 24, No. 3, pp. 980 – 993, March 2015.

[9] Mehran Kafai, Kave Eshghi, and Bir Bhanu “Discrete Cosine Transform Locality-Sensitive Hashes for Face Retrieval,” IEEE Transactions on Multimedia, Vol. 16, No. 4, pp. 1090 -1103, June 2014.

[10] Loris Nanni, Alessandra Lumini, and Sheryl Brahnam, “Survey on LBP based texture descriptors for image classification,” ELSEVIER International Journal on Expert Systems with Applications, Vol. 39, Issue 3, pp. 3634-3641, February 2012.

[11] Baochang zhang, Lei zhang, David zhang and Linlin shen, “Directional Binary Code with Application to PolyU Near-Infrared Face Database,” ELSEVIER Pattern Recognition Letters, Vol. 31, Issue 14, pp. 2337- 2344, October 2010.

[12] Jagadeesh H S, Suresh Babu K and Raja K B, “DBC based Face Recognition using DWT,” An International Journal in Signal & Image Processing, Vol.3, No.2, pp. 115 – 130, April 2012.

[13] Giovanni Betta, Domenico Capriglione, Mariella Corvino, Consolatina Liguori, and Alfredo Paolillo, “Face Based Recognition Algorithms: A First StepToward a Metrological Characterization,” IEEE Transactions on Instrumentation and Measurement, Vol. 62, No. 5, pp. 1008 -1016, May 2013.

[14] Kai Yang and Eliza Yingzi Du, “Consent Biometrics,” IEEE International Workshop on Computational Intelligence in Biometrics and Identity Management, pp. 78 – 83, April 2011.

[15] Anil K. Jain, Brendan Klare, and Unsang Park, “Face Recognition: Some Challenges in Forensics,” IEEE International Conference on Automatic Face & Gesture Recognition and Workshops, pp. 726-733, March 2011.

[16] Rasber D. Rashid, Sabah A. Jassim, Harin Sellahewa, “LBP Based On Multi Wavelet Sub-Bands Feature Extraction Used For Face Recognition,” IEEE International Workshop on Machine Learning for Signal Processing, pp. 1-6, September 2013.

[17] Radhey Shyam and Yogendra Narain Singh, “Face Recognition using Augmented Local Binary Pattern and Bray Curtis Dissimilarity Metric,” second IEEE International Conference on Signal Processing and Integrated Networks pp. 779 – 784, February 2015.

[18] Yang Zhao, WeiJia, Rong-XiangHu, HaiMin, “Completed robust local binary pattern for texture classification,” ELSEVIER International Journal on Neurocomputing, Volume 106, pp. 68–76, March 2013.

[19] Jianfeng Ren, Xudong Jiang, and Junsong Yuan, A Chi-Squared-Transformed Subspace of LBP Histogram for Visual Recognition, IEEE Transactions on Image Processing, Vol. 24, No. 6, pp. 1893-1904, June 2015.

[20] Di Huang, Mohsen Ardabilian, Yunhong Wang, and Liming Chen, “A Novel Geometric Facial Representation based on Multi-Scale Extended Local Binary Patterns,” IEEE International Conference on

Automatic Face & Gesture Recognition and Workshops, pp. 1-7, March 2011.

[21] Khoa Luu, Tien Dai Bui, and Ching Y. Suen, "Kernel Spectral Regression of Perceived Age from Hybrid Facial Features," IEEE International Conference on Automatic Face & Gesture Recognition and Workshops, pp. 1-6, March 2011.

[22] Fujin Zhong, Jiashu Zhang, and Defang Li, "Discriminant Locality Preserving Projections Based on L1-Norm Maximization," IEEE Transactions on Neural Networks and Learning Systems, Vol. 25, No. 11,pp. 2065 -2074, November 2014.

[23] Bing-Kun Bao, Guangcan Liu, Richang Hong, Shuicheng Yan, and Changsheng Xu, "General Subspace Learning With Corrupted Training Data Via Graph Embedding," IEEE Transactions on Image Processing, Vol. 22, No. 11, pp. 4380- 4393, November 2013.

[24] Sumit Shekhar, Vishal M. Patel, Nasser M. Nasrabadi, and Rama Chellappa, "Joint Sparse Representation for Robust Multimodal Biometrics Recognition," IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol. 36, No. 1, pp. 113 – 126, January 2014.

[25] Meng Yang, Lei Zhang, Jian Yang, and David Zhang, "Regularized Robust Coding for Face Recognition," IEEE Transactions on Image Processing, Vol. 22, No. 5, pp. 1753- 1766, May 2013.

[26] Zizhu Fan, MingNi, QiZhu, and ErgenLiu, "Weighted sparse representation for face recognition," ELSEVIER Neurocomputing letters, Vol. 151, Part 1, pp. 304-309, March 2015.

[27] Yunlian Sun and Massimo Tistarelli, "Robust Coarse-to-Fine Sparse Representation for Face Recognition," Springer-Verlag Berlin Heidelberg - Seventeenth International Conference on Image Analysis and Processing, Part II, Lecture Notes in Computer Science, Vol. 8157, pp. 171–180, September 2013.

[28] JunYing Gan, XiaoJie Liang, YiKui Zhai, Lei Zhou, and Bin Wang, "A Real-Time Face Recognition System Based on IP Camera and SRC Algorithm," Springer International Publishing Switzerland - Ninth Chinese Conference on Biometric Recognition, Lecture Notes in Computer Science, Vol. 8833, pp. 120–127, November 2014.

[29] Xingjie Wei, Chang-Tsun Li, Zhen Lei, Dong Yi, and Stan Z. Li, "Dynamic Image-to-Class Warping for Occluded Face Recognition," IEEE Transactions on Information Forensics and Security, Vol. 9, No. 12, pp. 2035- 2050, December 2014.

[30] Jian Zhang, JianYang, JianjunQian, and JiaweiXu, "Nearest orthogonal matrix representation for face recognition," ELSEVIER Neurocomputing letters, Vol. 151, pp. 471-480, 2015.

[31] Dapeng Tao, Lianwen Jin, Yongfei Wang, and Xuelong Li, "Rank Preserving Discriminant Analysis for Human Behavior Recognition on Wireless Sensor Networks," IEEE Transactions on Industrial Informatics, Vol. 10, No. 1, pp. 813 -823, February 2014.

[32] Jing Wang, Canyi Lu, Meng Wang, Peipei Li, Shuicheng Yan, and Xuegang Hu, "Robust Face Recognition via Adaptive Sparse Representation," IEEE Transactions on Cybernetics, Vol. 44, No. 12, pp. 2368- 2378, December 2014.

[33] http://www.kasrl.org/jaffe.html

[34] http://www.cl.cam.ac.uk/research/dtg/attarchive/facedatabase.html

[35] Nilanjan Dey, Anamitra Bardhan Roy, Sayantan Dey," A Novel Approach of Color Image Hiding using RGB Color planes and DWT," International Journal of Computer Applications, Vol. 36– No.5, pp. 19- 24, December 2011.

[36] Miao Cheng, Bin Fang, Yuan Yan Tang, Taiping Zhang, and Jing Wen, "Incremental Embedding and Learning in the Local Discriminant Subspace With Application to Face Recognition," IEEE Transactions on Systems, Man, and Cybernetics—Part C: Applications and Reviews, Vol. 40, No. 5, pp. 580 – 591, September 2010.

[37] Hsin-Wen Kung, Yi-Han Tu, and Chiou-Ting Hsu, "Dual Subspace Nonnegative Graph Embedding for Identity-Independent Expression Recognition," IEEE Transactions on Information Forensics and Security, Vol. 10, No. 3, pp. 626 – 639, March 2015.

[38] Firoz Mahmud, Md. Enamul Haque, Syed Tauhid Zuhori, and Biprodip Pal, "Human Face Recognition Using PCA based Genetic Algorithm," IEEE International Conference on Electrical Engineering and Information & Communication Technology, pp. 1 – 5, April 2014.

[39] Lim Song Li and Norashikin Yahya "Face Recognition Technique using Gabor Wavelets and Singular Value Decomposition," IEEE International Conference on Control System, Computing and Engineering, pp. 455 – 459, November 2014.

[40] Wael Ouarda,Hanene Trichili, Adel M. Alimi, and Basel Solaiman, "Combined Local Features Selection for Face Recognition Based on Naive Bayesian Classification," IEEE International Conference on Control System, Computing and Engineering, pp. 455 – 459, November 2013.

[41] Thamizharasi Ayyavoo and Dr. Jayasudha J S, "Face Recognition using Enhanced Energy of Discrete Wavelet Transform," Thirteenth IEEE International Conference on Hybrid Intelligent Systems, pp. 240 – 245, December 2013.

[42] Gheorghita Ghinea, Rajkumar Kannan, and Suresh Kannaiyan, "Gradient-Orientation-Based PCA Subspace for Novel Face Recognition," IEEE OPEN ACCESS Journal, Vol. 2, pp. 914 – 920, August 2014.

AUTHORS PROFILE

Jagadeesh H S awarded the B.E degree in E & C Engineering from Bangalore University and M.Tech degree in Digital Electronics and Communication Systems from Visvesvaraya Technological University, Belgaum. He is pursuing his Ph.D. in Electronics and Communication Engineering of Jawaharlal Nehru Technological University Hyderabad, India under the guidance of Dr. K. Suresh Babu. He has two research publications in refereed International Journal and Conference Proceedings. He is currently an Assistant Professor, Dept. of Electronics and Communication Engineering, A P S College of Engineering, Bangalore, India. His research interests include Image processing and Biometrics. He is a life member of Indian Society for Technical Education, New Delhi, India.

K Suresh Babu working as Professor, Dept. of Electronics and Communication Engineering, University Visvesvaraya College of Engineering, Bangalore University, Bangalore, India. He obtained his BE and ME in Electronics and Communication Engineering from University Visvesvaraya College of Engineering, Bangalore. He was awarded Ph.D. in Computer Science and Engineering from Bangalore University. He has over 27 research publications in refereed International Journals and Conference Proceedings. His research interests include Image Processing, Biometrics, Signal Processing.

K B Raja working as Professor, Dept. of Electronics and Com-munication Engineering, University Visvesvaraya College of Engineering, Bangalore University, Bangalore, India. He obtained his BE and ME in Electronics and Communication Engineering from University Visvesvaraya College of Engineering, Bangalore. He was awarded Ph.D. in Computer Science and Engineering from Bangalore University. He has over 134 research publications in refereed International Journals and Conference Proceedings. His research interests include Image Processing, Biometrics, VLSI Signal Processing, Computer networks.

Exchange Rates Forecasting Using Variable Length Moving Average - NARX

Agus Sihabuddin, Subanar, Dedi Rosadi, Edi Winarko

Computer Science Graduate Program, Faculty of Mathematics
and Natural Science, Gadjah Mada University, Yogyakarta - Indonesia

***Abstract*— This paper evaluates whether the *variable-length moving average (VMA)* as input in NARX outperform the univariate exchange rate forecasting performance. Six major rates of monthly data from January 1975 to April 2014 (USDAUD, USDCAD, USDEUR, USDGBP, USDJPY and USDCHF) are used to test the proposed model with a (1,5,0) VMA rule.**

We evaluate that the VMA can be used as input for NARX model and the forecasting accuracy is outperform the NAR univariate model with 19.97% improvement on D_{stat} and 3.17% improvement on MSE.

***Keywords*— forecasting, major exchange rates, VMA, NAR, NARX**

I. INTRODUCTION

Exchange rate forecasting has proved to be predictable using univariate model and it gives a good forecast accuracy[1]. In some cases, univariate specifications are limited that the market could be efficient and it can only be driven from outside indicators; the available time series are too short for significant technical analysis with the chosen forecasting horizon[2], and for some exchange rates, univariate model does not provide a good forecast [3].

Technical analysis studies patterns in historical exchange rate series those are generated by time-to-time market activities, which aim to predict future market movements. The key information used by technical analyst is volume and price. Two technical trading rules were firstly tested extensively on DJIA during period of 1897 to 1986[4]. These two technical indicators are *variable moving average* (VMA) and trading range break-out. The additional research on this method is extensively done for many stock index data or single stock data [5]–[16]. VMA on exchange rate forecasting is used to filter the signal [17]. The use of VMA on exchange rates forecasting is still rare.

Nonlinear Autoregressive with eXogenous Inputs (NARX) that has been used for exchange rate forecasting with good result [18]–[20] can accommodate the VMA indicator as an input.

II. RELATED WORK

The study of Moving Average with trading range breakouts has predictive ability for financial market [4], [6] with long sufficient data [15].

The profitability of VMA method has been tested on a costly trading environment like in UK data[6].

Recent literature on VMA has concluded that this method is technically more successful in the emerging market of Malaysia, Thailand and Taiwan but less powerfull in more developed countries like Hongkong and Japan [7]. [9].

The recent research shows that this method is not good as its historical sample tested out of sample over period of 1987 to 2011 and [16].

III. VMA-NARX METHOD

A VMA consists of comparison of two simple moving average, a longer- and a shorter- periods. Signals are generated by the short-term moving average crossing above or below the longer-term moving average [7], [15]. The rule of moving average period often uses the convention of 5-20 periods, 20-60 periods and 100-200 periods to detect short-, medium-, and long-term cycles of price movements, respectively. It depends on the economics circumstances and investors' behaviors differ [16]. The short- and long-period of moving avergae are described below [8].

$$Sp = \frac{\sum_{s=1}^{S} R_{i,t}}{S} ; Lp = \frac{\sum_{l=1}^{L} R_{i,t-l}}{L}$$

Where $R_{i,t}$ is daily return in short-period of S, and $R_{i,t-l}$ is the return in long-period of L.

A trading range break-out (TRB) is used to filter the buy (sell) signal when the price penetrates the resistance level (local maximum or minimum). A buy (sell) signal is generated when price rises above (below) the resistance area. A 50, 150, 200 days of maximum (minimum) is often used as the resistance level and with or without 1% band break-out [4].

An important class of discrete-time nonlinear system is the NARX model and this model is well suited for modelling nonlinear system [21] .

$$y(t) = f(u(t-n_u), \dots, u(t-1), u(t), y(t-n_y), \dots, y(t-1)) \quad (1)$$

Where *u(t)* and *y(t)* represent input and output of the network at time *t*, n_u and n_y are the input and output order and *f* is a nonlinear function.

VMA can be used as input to an artificial neural network especially NARX [22] like other trading indicators. Technical indicator is still valuable to trading decision because at least 90% of the respondent placed some weight on technical analysis for decisioon making [23].

The research goal were sets whether the VMA as input in NARX outperform the univariate exchange rate forecasting performance. The method is described as follows:

1. Compute the VMA of monthly six major exchange rates
2. Use the VMA value as external input for the NARX model
3. Calculate the forecasting performance
4. Compare with NAR forecasting performance from previous work

IV. Experiment and Results

A. Data

The exchange rates data used here are monthly six major exchange rates from January 1975 until April 2014. The major exchange rates used here are USDAUD, USDCAD, USDJPY, USDGBP, USDEUR and USDCHF which are the major exchange rates in the foreign exchange market and 65.2% of exchange market liquidity in April 2013 [24]. Each data contains 472 records which is divided into 80% (377 data) for training, 5% (24 data) for validation, and 15% (71 data) for testing. This data partition is similar to[25]–[28].

The external input or external variable for NARX is exchange rate that has been processed with VMA.

B. Methodology

The selected variable moving average for short-, long-periods and band in this exchange rates forecasting is (1,5,0) similar to [17]. The short period is 1 because it is a monthly data and it is equal to about 24 daily data. The long periods is 5 and since it is a monthly data it is long enough and equal to about 120 daily data. It is still in the range of its original rule [4] and the consensus value [16]. We do not test trading range breakout since there is no major differences in efficacy of trading model in presence of trading band [8].

Once the data calculated with VMA (1,5,0) then it is processed by NARX algorithm with preprocessing first, network training, network testing and performance measurement as shown in Fig 1.

C. Forecast Measure

In order to evaluate the forecast accuracy of the models, two forecast error measurements are used: *Mean Square Error (MSE)* and *directional statistics* (D_{stat}). MSE is defined as follows [29]:

$$MSE = \sum_{t=1}^{n} \frac{e_t^{\ 2}}{n} \qquad (2)$$

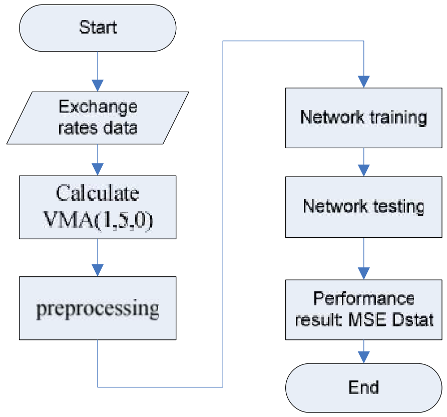


Fig. 1. Forecasting Process

D_{stat} is defined as follows [3]:

$$D_{stat} = \frac{1}{N}\sum_{t=1}^{N} at * 100\% \qquad (3)$$

where *at=1 if* $(x_{t+1} - x_t)(\hat{x}_{t+1} - x_t) \geq 0$;
otherwise 0.

D_{stat} is more preferable in financial instruments forecasting because it gives the correctness of gradient prediction [3].

D. Result

The proposed method is tested by using 10 experiments for each exchange rate pair. NAR algorithm result is used to get the univariate exchange rate forecasting and collected from the previous study [30] and used as a benchmark data. The best experiment results is presented in Table I for the MSE parameter.

TABLE I. Forecasting performance VMA NARX on MSE

Method	USD AUD	USD CAD	USD EUR	USD GBP	USD JPY	USD CHF
NAR	3,587[1]	1,138[1]	6,670[2]	3,260[2]	7.565	1,375[1]
VMA-NARX	3,239[1]	1,110[1]	6,520[2]	3,259[2]	7.229	1,373[1]
MSE Dec.(%)	-9.70	-2.46	-2.25	-0.03	-4.45	-0.15

1= $*10^{-3}$; 2=$*10^{-4}$

The VMA-NARX on MSE parameter gives the best derease of MSE for USDAUD (-9.70%) and the worst for USDGBP (-0.03%) with average of -3.17%.

The results for D_{stat} accuracy parameter is more promising in VMA-NARX model with the best accuracy improvement for USDGBP (37.84%) and the worst is USDEUR (4.66%) and the average of 19.97% for all exchange rates. The result is summarized in Table II.

TABLE II. FORECASTING PERFORMANCE VMA NARX ON D_{STAT}

Method	USD AUD	USD CAD	USD EUR	USD GBP	USD JPY	USD CHF
NAR (%)	57.75	47.89	60.56	52.11	47.89	57.75
VMA-NARX (%)	66.2	60.56	63.38	71.83	60.56	63.38
D_{stat} Inc. (%)	14.63	26.46	4.66	37.84	26.46	9.75

The summary result for proposed method showed that VMA-NARX gives improvement for MSE and D_{stat} parameters for all exchange rates forecasting. With the average improvements of 3.17% for MSE and 19.97% for D_{stat}, it can be conclude that VMA can be used as input for NARX algorithm and the performance of proposed method outperform the NAR method for six major exchange rates pairs.

V. CONCLUSIONS.

The VMA could be applied as external input for a NARX algorithm and gives a better result compared to a univariate NAR algorithm for six major exchange rates. The proposed model gives 19.97% improvement on average for D_{stat} and 3.17% improvement on average for MSE.

The accuracy performance could be improved by adding more variables to the models or combining with other models for further research.

REFERENCES

[1] G. P. Zhang, "Time Series Forecasting using A Hybrid ARIMA and Neural Network Model," *Neurocomputing*, vol. 50, pp. 159–175, 2003.

[2] B. R. Setyawati, R. C. Creese, and M. Jaraiedi, "Neural Networks for Univariate and Multivariate Time Series Forecasting," *Proceeding 2003 IIE Annu. Conf.*, 2003.

[3] J. Yao and C. L. Tan, "A Case Study on Using Neural Networks to Perform Technical Forecasting of Forex," *Neurocomputing*, vol. 34, no. 1–4, pp. 79–98, Sep. 2000.

[4] W. Brock, J. Lakonishok, and B. LeBaron, "Simple Technical Trading Rules and The Stochastic Properties od Stock Returns," *J. Finance*, vol. 47, no. 5, pp. 1731–1764, 1992.

[5] R. Sullivan, A. Timmermann, and H. White, "Data-Snooping , Technical Trading Rule Performance , and the Bootstrap," *J. Finance*, vol. 54, no. 5, pp. 1647–1691, 1999.

[6] R. Hudson, M. Dempsey, and K. Keasey, "A NOte on The Weak Form Efficiency of Capital Markets: The Application of Simple Technical Trading Rules to UK Stock Prices - 1935 to 1994," *J. Bank. Financ.*, vol. 20, pp. 1121–1132, 1996.

[7] H. Bessembinder and K. Chan, "Market Efficiency and the Returns to Technical Analysis," *Financ. Manag.*, vol. 27, no. 2, pp. 5–17, 1998.

[8] M. Ratner and R. Leal, "Tests of Technical Trading Strategies in the Emerging Equity Markets of Latin America and Asia," *J. Bank. Financ.*, vol. 23, no. May, pp. 1881–1905, 1999.

[9] A. Parvez, K. Beck, and E. Goldreyer, "Can Moving Average Technical Trading Strategies Help in Volatile and Declining Markets ? A Study of Some Emerging Asian Markets," *Manag. Financ.*, vol. 26, no. 6, pp. 49–62, 2000.

[10] S. Achutan and R. Anubhai, "Effectiveness of Variable Length Moving Average (VMA) Trading Rules in the Indian Stock Mark," *Financ. India*, vol. 19, no. 4, pp. 1375–1391, 2005.

[11] B. M. Cai, C. X. Cai, and K. Keasey, "Market Efficiency and Returns to Simple Technical Trading Rules: Further Evidence from U.S., U.K., Asian and Chinese Stock Markets," *Asia-Pacific Financ. Mark.*, vol. 12, no. 1, pp. 45–60, Jul. 2006.

[12] M. D. Mckenzie, "Technical Trading Rules in Emerging Markets and the 1997 Asian Currency Crises Technical Trading Rules in Emerging Markets and the 1997 Asian Currency Crises," *Emerg. Mark. Financ. Trade*, vol. 43, no. 4, pp. 46–73, 2007.

[13] C. Lonnbark and A. Soultanaeva, "Profitability of Technical Trading Rules on the Baltic Stock Markets," *Umea Econ. Study*, vol. 761, pp. 1–5, 2008.

[14] H. Yu, G. V. Nartea, C. Gan, and L. J. Yao, "Predictive ability and profitability of simple technical trading rules: Recent evidence from Southeast Asian stock markets," *Int. Rev. Econ. Financ.*, vol. 25, pp. 356–371, Jan. 2012.

[15] N. H. Hung and Y. Zhaojun, "Profitability of Applying Simple Moving Average Trading Rules for the Vietnamese Stock Market," *J. Bus. Manag.*, vol. 2, no. 3, pp. 22–31, 2013.

[16] J. Fang, B. Jacobsen, and Y. Qin, "Predictability of The Simple Technical Trading Rules: An out-of-sample Test," *Rev. Financ. Econ.*, vol. 23, no. 1, pp. 30–45, Jan. 2014.

[17] C. J. Neely and P. A. Weller, "Lessons from the Evolution of Foreign Exchange Trading Strategies," *Work. Pap. 2011-021D Res. Div. Fed. Reserv. Bank St. Lois*, 2013.

[18] P. C. Soman, "An Adaptive NARX Neural Network Approach for Financial Time Series Prediction," *Thesis, State Univ. New Jersey*, 2008.

[19] E. Diaconescu, "The use of NARX Neural Networks to predict Chaotic Time Series," *WSEAS Trans. Comput. Res.*, vol. 3, no. 3, 2008.

[20] C. Jiang and F. Song, “Sunspot Forecasting by Using Chaotic Time-series Analysis and NARX Network,” *J. Comput.*, vol. 6, no. 7, pp. 1424–1429, Jul. 2011.

[21] H. T. Siegelmann, B. G. Horne, C. L. Giles, and S. Member, “Computational Capabilities of Recurrent NARX Neural Networks,” *IEEE Trans. Syst. MAN, Cybern. PART B Cybern.*, vol. 27, no. 2, pp. 208–215, 1997.

[22] B. Vanstone and G. Finnie, “Combining Technical Analysis and Neural Networks in the Australian Stockmarket,” *Work. Pap. Bond Univ.*, 2006.

[23] B. J. Vanstone, G. Finnie, and B. Vanstone, “An Empirical Methodology For Developing Stockmarket Trading Systems Using Artificial Neural Networks An Emperical Methodology For Developing Stockmarket Trading Systems Using Artificial Neural Networks,” *Work. Pap. Bond Univ.*, 2009.

[24] Bank for International Settlements, “Triennial Central Bank Survey Foreign Exchange Turnover in April 2013 : Preliminary Global Results,” 2013.

[25] K. Kim and W. B. Lee, “Stock Market Prediction Using Artificial Neural Networks with Optimal Feature Transformation,” *Neural Comput. Appl.*, vol. 13, pp. 255–260, 2004.

[26] I. Kaastra and M. Boyd, “Designing A Neural Network for Forecasting Financial and Economic Time Series,” *Neurocomputing*, vol. 10, pp. 215–236, 1996.

[27] M. Al Mamun and K. Nagasaka, “Artificial Neural Networks Applied to Long-term Electricity Demand Forecasting,” in *Proceedings of the Fourth International Conference on Hybrid Intelligent Systems (HIS’04)*, 2004, pp. 0–5.

[28] A. M. Oyewale, “Evaluation of Artificial Neural Networks in Foreign Exchange Forecasting,” *Am. J. Theor. Appl. Stat.*, vol. 2, no. 4, pp. 94–101, 2013.

[29] B. Abraham and J. Ledolter, *Statistical Methods for Forecasting*. New Jersey: Wiley-Interscience, 1983.

[30] A. Sihabuddin, Subanar, D. Rosadi, and E. Winarko, “A Second Correlation Method for Multivariate Exchange Rates Forecasting,” *Int. J. Adv. Comput. Sci. Appl.*, vol. 5, no. 7, pp. 30–33, 2014.

Agus Sihabuddin received his Bachelor and Master degree from Computer Science, Gadjah Mada University, pursuing a doctoral at the same university. He is currently a lecturer in the Department of Computer Science and Electronics, Faculty of Mathematics and Natural Science, Gadjah Mada University. His research interests include time series forecasting, mobile applications and their applications.

Subanar, he hold his doctoral (Ph.D) in statistics from University of Wisconsin, Madison, United States in 1976. He is currently a lecturer and professor in the Faculty of Mathematics and Natural Science, Gadjah Mada University. His research interests include Mathematic Statistics, Neural Network and Bootstrap Method.

Dedi Rosadi, received the B.Sc., M.Sc. and Dr.rer.nat. degrees from Gadjah Mada University, Indonesia in 1996, University of Twente, the Nedherlands, in 1999, and Vienna University of Technology, Austria, in 2004 respectively. Since 2013, He is a professor at the Department of Mathematics, Gadjah Mada University. Dedi Rosadi is a regular member of ISI and ISAC. His research areas include time series analysis and computational statistics, including application for finance.

Edi Winarko, lecturer at the Department of Computer Science and Electronics, Faculty of Mathematics and Natural Science, Gadjah Mada University. He holds his B.Sc. degree in Statistics Study Program, Gadjah Mada University, M.Sc. degree from Computer Science of Queen’s University Canada, and Ph.D. degree in Computer Science from Flinders University Australia. His research interests covers Data Warehousing and Data Mining, Information Retrieval.

Implementing the Database Users Privilege Model

Effects of possible successful SQL Injection attack in web applications

Gem Ralph Caracol, Soomi Yang
Information Security Department
Suwon University
Hwaseong City, South Korea

Abstract—**For more than a decade, many solutions and detection mechanisms have been proposed to prevent web applications from SQL Injection attacks. However, according to the 2013 OWASP 10, SQL Injection is still a top threat and attackers can find evasive ways to exploit this vulnerability. We implemented the proposed database level Database Users Privilege Model of [6]. Our findings suggest that by implementing the model, it does not detect SQL Injection attacks but with the necessary recommendations, it can prevent the attacker from fully compromising the database and the database server.**

Keywords-SQL Injection, Database Users Privilege Model, OWASP, Database Security, Web Application

I. Introduction

Injection is still number 1 in the OWASP top 10 list of the most critical web application security flaws. Injection flaws occur when an application sends untrusted data to an interpreter. Injection flaws are very prevalent, particularly in legacy code. They are often found in SQL, LDAP, Xpath, or NoSQL queries; OS commands; XML parsers, SMTP Headers, program arguments, etc. Injection flaws are easy to discover when examining code, but frequently hard to discover via testing [1][13]. A successful injection when the database is not well defended, an attacker can gain full access to the database and even the database server itself.

In a SQL Injection, the root cause of its vulnerabilities is insufficient input validation and the solution for eliminating these vulnerabilities is to apply defensive coding practices [7][11]. Solutions have been proposed and recommended mostly in the code level by creating parameterized interface and / or escaping special characters of the unsafe input data [1][2][4][7][14]. Scanners and fuzzers systems like Intrusion Detection Systems that detects possible SQL Injection flaws that are in web applications [3][4][5][7][8][9][11][12]. While these code level solutions and detection systems may make web applications safer, attackers can still find evasive ways to attack. It is also best to be able have another level of protection in case of a successful SQL injection. A Users Privilege Model has been proposed as another level of protection in the database level [6].

In this paper we implemented a database level protection based on [6] to identify the level of protection of the database server in an event of a successful SQL Injection. Section 2 shows the Implementation of the Database Users Privilege Model. Section 3 discusses the findings of a successful SQL Injection attack in each user privilege. Finally, Section 4 concludes the paper.

II. ImplementATION OF THE Database Users Privilege Model

Reference [6] proposed the Database Users Privilege Model as shown in table 1.

TABLE I. Database Users Privilege Model

Username	Privileges
viewer_user	SELECT
editor_user	SELECT, INSERT, UPDATE, DELETE
structure_user	CREATE, ALTER, DROP, EXECUTE
super_user	CREATE, GRANT, RELOAD, CREATE USER

Table 2 shows the implementation of the above model in a mysql database (db). The asterisk (*) represents all.

TABLE II. Database Users Privilege Model Implementation

Username	Privileges

viewer_user	CREATE USER 'viewer_user'@'localhost' IDENTIFIED BY 'viewer_pass';
	GRANT SELECT ON db.* ON 'viewer_user'@'localhost';

editor_user	CREATE USER 'editor_user'@'localhost' IDENTIFIED BY 'editor_pass';
	GRANT SELECT, INSERT, UPDATE, DELETE ON db.* ON 'editor_user'@'localhost';

structure_user	CREATE USER 'structure_user'@'localhost' IDENTIFIED BY 'structure_pass';
	GRANT CREATE, ALTER, DROP, EXECUTE ON db.* ON 'structure_user'@'localhost';

super_user	CREATE USER 'super_user'@'localhost' IDENTIFIED BY 'super_pass';
	GRANT CREATE, GRANT, RELOAD, CREATE_USER ON db.* ON 'super_user'@'localhost';

Table 3 shows a simplified PHP Language Connection based on table 2.

TABLE III. PHP LANGUAGE CONNECTION

connection.php

```
<?php

class DBConnection {
  // db user variables
  private $viewer_user = “viewer_user”;
  private $viewer_pass = “viewer_pass”;
  private $editor_user = “editor_user”;
  private $editor_pass = “editor_pass”;
  private $structure_user = “structure_user”;
  private $structure_pass = “structure_pass”;
  private $super_user = “super_user”;
  private $super_pass = “super_pass”;

  //database variable for the database connection
  private $database = “db”;

  //host variable
  private $host = “localhost”;

  //connection variable
  private $con;

public function db_connect($login_status){
   switch($login_status){
               case 1: $user = $viewer_user; $pass = $viewer_pass; break;
               case 2: $user = $editor_user; $pass = $editor_pass; break;
               case 3: $user = $structure_user; $pass = $structure_pass; break;
               case 4: $user = $super_user; $pass = $super_pass; break;
               default: $user = “”; $pass=””
   }
    $this->con = @mysql_connect($this -> host, $this -> user, $this -> pass));
}
?>
```

III. FINDINGS, DISCUSSIONS & RECOMMENDATIONS

Results of a successful SQL Injection on the Database Users Privilege Model are shown here together with the discussions and recommendations

A typical database for a web application contains the users table, and the data tables relevant to the function of a web application.

A. *Viewer User*

The “viewer_user” has a privilege of SELECT only. Meaning it has the capability of retrieving records from the database.

User Example: A typical example of a user that has this privilege is guest in online shop where just goes on viewing the public pages.

Effect: Once a successful SQL Injection attack, it can only get records from the database. While it cannot modify or change any data, the users table is also available for viewing. The attacker can now try to brute force the password and log into any user he wants. Even if the attacker doesn’t know or cannot brute force the password, a successful SQL Injection attack in the login page may also make the attacker any user he wants.

Recommendation: This type of user must not have a SELECT access to the users table.

B. *Editor User*

The “editor_user” has a privilege of SELECT, INSERT, UPDATE, and DELETE. Meaning it has the capability of adding, updating retrieving, and deleting records from the database.

User Example: A typical example of a user that has this privilege is a customer in an online shop where he can modify his personal information, make or cancel an order and so on.

Effect: Once this user logs in or his account is hijacked and does a successful SQL Injection attack, it can do all the damage to all tables by modifying the content of the tables and even deleting all the records.

Recommendation: This type of user must not have any privilege to the users table as well as tables that he has nothing to do with.

C. *Structure User*

The “structure_user” has a privilege of CREATE, ALTER, DROP, EXECUTE. Meaning it has the capability of creating, altering and dropping tables, indexes and views and executing stored routines.

User Example: A typical example of a user that has this privilege is the DB admin in an online shop where he can modify the structure of the database.

Effect: Once a successful SQL Injection attack, it can also do all the damage to all tables in the database much more than the structured user by erasing all the tables and views

Recommendation: Most of the DB Admin pages are for these types of functions that are considered out of reach from the public. Caution in implementing the use of this type of database connection in web applications.

D. *Super User*

The “super_user” has a privilege of CREATE, GRANT, RELOAD, CREATE_USER. Meaning it has the capability of creating, tables and indexes. It also has a capability of creating new users and can grant privileges to mysql database users and can do mysqladmin commands.

User Example: A typical example of a user that has this privilege is also the DB admin in the overall Database Server where he can manage the server.

Effect: Once a successful SQL Injection attack, it can also do whatever he wants to do of the database server.

Recommendation: The functions of this user are for managing the DBMS and must be out of reach from the public. Caution in implementing the use of this type of database connection in web applications.

IV. CONCLUSION

There are a lot of proposed solutions as well as detection mechanisms to combat SQL Injection attacks however the attackers still manages to find ways to exploit the injection vulnerabilities in web applications. In the 2013 OWASP Top 10, SQL Injection still ranks as the top vulnerability. The implementation of the Database Users Privilege Model of [6] with the necessary recommendations shows that it cannot detect or fully eliminate SQL Injection attacks but it may prevent the attacker from fully compromising the database server.

Web Application developers must still follow the best practices to prevent SQL injections attacks. They may implement the Database Users Privilege Model of [6] with the necessary recommendations to provide another level of security of the database and the database server.

REFERENCES

[1] "OWASP Top 10 - The ten most critical web application security risks," Open Web Application Security Project (OWASP), 2013.

[2] "OWASP Top 10 - The ten most critical web application security risks," Open Web Application Security Project (OWASP), 2010.

[3] A. Saxena, S. Sengupta, P. Duraisamy, V. Kaulgud and A. Chakraborty, "Detecting SQL injection vulnerabilities in Sales Force applications," Proceeding of the International Conf on Advances in Computing, Communications and Informatics (ICACCI)., Mysore,KA, 2013, pp. 489-493.

[4] A. Kumar and K.Reddy, "Constructing Secure Web Applications With Proper Data Validations," IEEE International Conference on Recent Advances and Innovations in Engineering (ICRAIE-2014),May 09-11, 2014, Jaipur, India

[5] S. Amirmohammad, M. Zamani, and A.A. Manaf. "A Taxonomy of SQL Injection Detection and Prevention Techniques," In Informatics and Creative Multimedia (ICICM), 2013 International Conference on, pp. 53-56. IEEE, 2013.

[6] S. Amirmohammad, M. Zamani, and A.A. Manaf. " SQL Injection is Still Alive:A Study on SQL Injection Signature Evasion Techniques," In Informatics and Creative Multimedia (ICICM), 2013 International Conference, pp. 265-268. IEEE, 2013.

[7] WG Halfond, J Viegas, and A Orso, "A Classification of SQL Injection Attacks and Countermeasures," Proc. IEEE Int',l Symp. Secure Software Eng., Mar. 2006.

[8] G. Buja, K.B.A. Jalil, F.B.H.J. Ali, and T.F.A. Rahman, "Detection Model for SQL Injection Attack:An Approach for Preventing a Web Application from the SQL Injection Attack," IEEE Symposium on Computer Applications & Industrial Electronics (ISCAIE),April 7-8, 2014, Penang Malaysia.

[9] A. Pramod, "SQLI detection system for a safer web application," Advance Computing Conference (IACC), 2015 IEEE International, pp. 237-240, June 12-13, 2015, Bangalore, India.

[10] Shar, L.K.; Hee Beng Kuan Tan, "Defeating SQL Injection," Computer , vol.46, no.3, pp.69,77, March 2013.

[11] Y.S. Jang and J.J. Choi, "Detecting SQL injection attacks using query result size," Computers & Security, Volume 44, July 2014, Pages 104–118

[12] I. Lee, S. Jeong, S. Yeo, and J. Moon, "A novel method for SQL injection attack detection based on removing SQL query attribute values," Mathematical and Computer Modelling Volume 55, Issues 1–2, January 2012, Pages 58–68

[13] L.K. Shar and H.B.K. Tan, ″Predicting SQL injection and cross site scripting vulnerabilities through mining input sanitization patterns," Information and Software Technology Volume 55, Issue 10, October 2013, Pages 1767–1780

[14] V. Karakoidas, D. Mitropoulos, P. Louridas, and D. Spinellis, "A type-safe embedding of SQL into Java using the extensible compiler framework J%," Computer Languages, Systems & Structures Volume 41, April 2015, Pages 1–20

International Journal of Computer Science and Information Security (IJCSIS),
Vol. 13, No. 9, September 2015

Security Issues and Solutions for Android-based Mobile Devices

Klever R. P. Cavalcanti, Edejair Viana
Department of Statistics and Informatics
Federal Rural University of Pernambuco
Pernambuco, Brazil

Fernando A. A. Lins
Department of Statistics and Informatics
Federal Rural University of Pernambuco
Pernambuco, Brazil

Keywords-* *(Android; Mobile; smartphone; security; Aplication).

Abstract— **Currently, mobile devices are being widely used by of a considerable number of people. The need to be connected 24 hours a day is becoming a reality, because users need to make online purchases, make payments, access social networks, surf the Internet, check e-mails and so on. In this context, users with mobile devices, especially smartphones, using the Internet to connect to specific applications and safety issues may arise because, for example, sensitive data may be sent over an insecure channel (Internet). The aim of this paper is to present an overview of current security risks and security solutions related to smartphones based on the Android platform. Security risks have been divided into five categories, and these risks are presented and detailed on the corresponding categories. In addition, still stand out security solutions that are currently available on Android stores and these solutions can be used to eliminate or mitigate the risks.**

I. Introduction

Currently, mobile devices are undoubtedly present in the daily routine of a considerable part of the community. The need to be connected twenty four hours a day is apparent because users need to shop online, perform payments, access social networks, surf the Internet, check emails and so on. By the end of this year (2015), the number of smartphones worldwide will reach almost 7 billion, close to the number of inhabitants on the planet, according to data released by the International Telecommunication Union (ITU-T) [10]. The entry of new phones will reach 96% worldwide by December, thanks to emerging countries, which represent almost 78% of all phones in use around the globe. Currently, two of three Internet users are located in developing countries [7].

In this context, considering that users with mobile devices, especially smartphone, utilize the Internet to connect to specific applications, security issues may arise, because sensitive data may be sent over this unsecure channel. On the current days, more than three billion mobile devices suffer all kind of attacks. In a recent study conducted by the Chinese company Cheetah Mobile, it is possible to observe that in the last 12 months the number of malwares for Android devices increased 600% [5]. Based on this and other facts, it is imperative to consider security measures and mechanisms in the mobile applications use and development.

The main objective of this work is to present, describe and categorize the current most relevant security issues and solutions for Android-based mobile devices (especially Android-based smartphones). To achieve that, five categories of security issues are proposed and detailed, and they can be used to reason about available security attacks.

This paper is structured as follows. Section II presents relevant basic concepts that help to understand this work. Section III introduces the proposed five categories, in which security issues are described and detailed. Section IV details current solutions for security in Android-based mobile devices. Finally, Section V presents the conclusions and future work.

II. Basic Concepts

A. Android Architecture

Android is an operating system that was developed based on UNIX and it was designed to be used in mobile devices. Usually, applications for this operation system are developed using the Java programming language, which are then deployed in a specific virtual machine named Dalvik. The Android architecture is basically composed by five layers, which are described as follows.

- **Applications.** The main purpose of this layer is to provide the basic functions of the device for high-level users. These applications may come available on the smartphone (eg e-mail, calendar, web browser and organizer) and also be downloaded by users on specific online shops.
- **Application Framework**. This layer is developed mostly in Java, and interfaces with Android applications. It provides a set of libraries to access the various features of the device such as the graphical interface, locator (GPS), persistent database storage on the SD card and so on.

- **Libraries**. Composed of several native libraries built for specific mobile device architectures and provide many different features, such as screen graphical access, web rendering engine, internal database access, SSL / TLS channel establishment and so on.
- **Android Runtime**. Its main role is to support the applications execution. Basically, the programs are written in Java and then converted into machine code called bytecode, an intermediate step between the source code and code readable by the hardware. These bytecodes can be executed by a specific virtual machine called Dalvik.
- **Linux Kernel**. Based on the fact that Android uses a modified version of the 2.6 Linux kernel, it provides some important services, such as security and memory management, and also an abstraction layer for hardware utilization.

B. Security Overview

Security is a topic that has been well discussed by the community in past years [20]. Due to that, some security basic concepts are being widely used and are briefly highlighted in this section.

Confidentiality. The information should not be made available or disclosed to unauthorized individuals, entities or processes. For example, confidential information sent over the Internet (such as credit card number) should not be accessed by unauthorized users.

Availability. The information should be accessible and useable, even considering periods with high demand. For example, the loss of connectivity of a relevant server can impact the system availability, because this system may become unavailable to external users.

Integrity. Consists of protecting information against non-authorized modification without the permission of the information owners.

Authentication. Property that ensures that the information was originated by the expected source and that there was not any in the communication process by unauthorized users.

Access control. The main objective is to prevent unauthorized users from accessing the system and its functionalities. For example, it is important to ensure that unauthorized users will not access specific wireless networks.

III. COMMOM ISSUES AND VULNERABILITIES IN ANDROID-BASED ENVIRONMENTS

This section presents and details current security issues and vulnerabilities that appear when using mobile application and devices in Android-based platforms. For didactic reasons, they were classified into five categories: Device Loss, Unsecure Communication Environment, Usage of Programs from Suspicious Sources, Vulnerabilities in the Mobile Application Development and User Misconfiguration.

A. Device Loss

When a mobile device is lost, not only the hardware is committed, but also its internal information (for example, photos, personal documents and settings). For example, a malicious user can put a USB cable on a smartphone and have access to all the information that is available on the device. This section aims to focus on relevant issues of security that appears in this context.

We focus primarily on five security issues: USB-exposure, loss of information, blackmail, SIM exposure and exposure of internal data.

In the case of security problem "USB-Exposure", the main risk is based on the fact that an unauthorized user can access private data of the device by connecting to the USB port of your smartphone. Based on this, this user will have access to private photos and data files. One possible solution for this problem is the usage of a password on the smartphone and to use encryption on the smartphone memory card.

Other relevant issue is "Loss of Information", and is relevant because the device owner will lose access to the internal data of this device if preventive measures were not taken. For example, if the owner did not made a backup of the more important files, this owner may no longer have access to these files.

Another relevant security problem related to the device loss is related to the fact that a malicious user can require specific actions or recompense in order to return the lost device or to not use and disseminate its content. This security issue is known as "Blackmail". One possible countermeasure for this situation is to install specific security applications that are able to remotely access the mobile device and take actions such as to format it.

Another source of security issues is based on the fact that the SIM card is the subscriber identification module for the phone operator. Malicious users can use list SIM cards for a diversity of actions. The SIM card protection is a very important practice. However, a considerable number of users does not put a password on the SIM card because they have already put a password on the home screen of the mobile device.

Finally, another risky situation is to have the data card violated without user consent. This security issue is referred to as "Internal data exposure" and is somehow related to other security issues that were previously introduced in this section. However, the focus at this point is how to protect the contents of the data itself. One possible and commonly used approach is the adoption of encryption mechanisms to prevent unauthorized users from understanding the stolen data. The main objective is to transform the user's mobile data such as email and photos, in a set of characters that are very difficult to understand. Even if an unauthorized user has access to the encrypted information, that person will not be able to retrieve the information in a readable format, because this user does not have access to the decryption key.

B. *Unsecure Communication Environment*

Currently, mobile users are having to an increasing number of wireless networks (especially Wi-Fi), which offer fast and efficient connection to mobile devices. However, eventually it becomes an unsafe environment in which the user does not know, for example, who is managing the network. Based on that, some security issues may arise. For example, an unauthorized person can have access to the information that is being sent across the network. Several security issues exist in a non-secure communication environment. This category focuses on security issues related to the use of open Wi-Fi networks. More specifically, three points should be analyzed in the context of users from accessing open networks: web pages capturing, obtaining the credentials of an FTP server and reports abduction.

An user that accesses web pages on the mobile device connected to an open Wi-Fi network could suffer an attack considering that a malicious user can scan the open network and view all traffic that are going through the network using computational resources such as a packet capture program. Another concern appears if an user uses an application to connect to the mail server without using encryption. It this case, the attacker is able to access the login details of the user and/or device.

Kidnapping accounts or accessing unauthorized user information occurs not only in personal computers, but also in mobile devices. In this type of attack, an attacker with a computer running a malicious application can access personal data or accounts on popular services such as Gmail, LinkedIn, Yahoo and Facebook. To protect against attacks on data over a wireless Internet network, the best way is to avoid access social networks, internet banking and other sites that may have access to user data.

Some security mechanisms and strategies can be used to avoid security problems. More specifically, the utilization of cryptographic algorithms has being widely adopted to secure the communication process in this case. Some of these algorithms are:

WEP. This is one of the first encryption algorithms to be used. Currently, it is considered not strong and therefore its use should be avoided.

WPA. This algorithm was proposed in order to address some of the weaknesses of the WEP mechanism. Considering the current state of the art, it is more suitable in comparison to WEP.

WPA-2. This algorithm is similar to WPA, but is considered stronger in terms of encryption complexity. It is recommended mechanism.

C. *Usage of Programs from Suspicious Sources*

In this category, the focus is on the use of programs and applications that are obtained from suspected sources (or, at least, not well known sources). Basically, this section present attacks that are based on the use of programs with suspicious sources.

Initially, viruses such as malware or trojan horse can come disguised as official insurance programs on Google Play stores. Despite the claim that Google Bouncer program is a service that checks applications for evidence of malware in the Android Market, it is known that there are a number of malicious software in these stores [9].

With the variety of applications for mobile devices, a considerable number of users download other programs from unofficial stores, and therefore are susceptible to attacks. These applications are, for example, malwares that turn users' mobile devices into botnets, which is a malicious software that is capable of turning the mobile device in a bot (which is also known as zombie). When this event occurs, the device can run automated tasks over the Internet without the user knowledge and authorization. Figure 1 illustrates this scenario.

Figure 1- Using Programs from suspicious sources

As mentioned, with the large number of mobile devices in the world and the users' inexperience in their secure utilization, these users may download applications without knowing its origin, leading to the possibility of Botnet attacks. A Bot-Net is a collection of software robots (called bots) that are executed automatically and can compromise multiple computers or mobile devices that were invaded by malicious programs such as worms, Trojan horses and so on. They are executed under a common control infrastructure. They serve several purposes, including denial of service attacks, often without the user's knowledge. Its main objective is to have the largest number of infected mobile devices, because the total computational power of these devices have enough bandwidth and processor speed to cause significant damages in high-scale attacks.

Another important point is to download programs that are not connected to the official stores. In this case, the user does not know the origin of the program and thus taking a considerable risk of downloading a malware. It is worth noting that even downloading a program or application in the official stores is always recommended to have an antivirus. The amount of programs and applications that are placed daily in official stores are analyzed to detect the presence of malwares. More specifically, Google recently added a new layer of security to the Android Market named Bouncer that scans new and existing applications automatically for malware evidences. However, this is not enough, and the user should check the source of the program and other related information to guarantee the program safety.

One of the most important relevant risks involved in downloading programs from suspicious sources is the malware infection. Malware is any type of unwanted software installed without user consent. Viruses, worms and Trojans are examples of malicious software that are often grouped together and called collectively malware. According to the survey conducted by Kaspersky Lab [13] Android is still the main target of malicious attacks considering all mobile platforms. 98,05 % of the malicious programs for mobile devices that were discovered in 2013 are directed related to the Android platform, and this fact helps to understand the need for security measures considering Android-based programs and devices.

Considering the attacks described in this section, some actions can be taken to mitigate or even avoid their occurrence. Before downloading any application, it is important to check the latest comments from other users about the application. In addition, it is also relevant to avoid downloading applications or programs outside of official store shops, because the amount of malware and viruses that usually comes in other sources are comparatively higher.

D. *Vulnerabilities in the Mobile Application Development*

The mobile programs itself can be source of attack risks. To develop mobile applications without considering security risks and measures is other relevant commom issue currently in Android-based programs and devices. Three situations appears with relevance in this context: poor security knowledge of the development team, indirect attack and applications that require advanced permissions on Android.

Insufficient security knowledge of the application development team is a major concern, because many applications are placed daily in official stores without considering basic security concepts and tools. Usually, developers creates simpler applications, without considering security requirements in the development process. This fact contributes to the existence of security risks and threats.

Another relevant point is the indirect attack, where Android applications have some certificates previously recorded by developers, giving them special access and privileges within the operating system without going through the chain of the certificate validation process. For example, Adobe is giving certificates to their applications. This process exists to allow other applications to stop using the plug-in Adobe Flash Player. One possible situation is that an attacker can validate a malicious application with a certificate that appears to have been validated by the prerecorded code from Adobe, but actually is not. Also, while the Adobe certificate is present in the application's certificate chain, the system accepts code released by this application and inject in other applications.

Finally, there are risks associated to the applications permissions. To install an application, is necessary for the user to accept some permissions. For example, the user may downloads an application which requires the user permission to use the camera, to the GPS and other relevant function. By doing that, the user may become more vulnerable, because this application can use these permissions for other purposes that were not mentioned in the installation process. Figure 2 presents an example in which an application requests some permissions for its installation.

The acceptance of the permissions request can generate unpleasant consequences, such as theft of personal data. The problem becomes even more relevant when permissions are combined, because to review all the permissions is exhausting, and usually the user just accepts the request without performing a significant review. A preventive measure is to not install an application that requires too much permission, except if they are considered essential. Unfortunately, usually it is not possible to accept only a subset of these permissions.

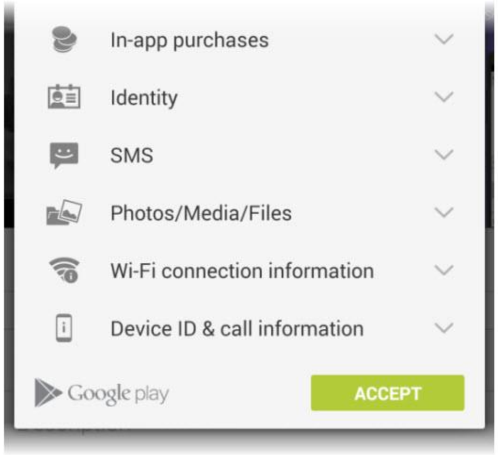


Figure 2- Example of an application requiring Android permissions.

E. *User Misconfiguration*

A considerable number of security attacks occurs based on the poor security knowledge of the high-level user. This type of user is generally not fully aware of what is being done when some actions are performed in the mobile device. Based on that, this last category is named "User Misconfiguration", and focus on some common user misconfigurations that can produce relevant security risks.

The first possible misconfiguration is related to the use of Bluetooth and GPS. Many users utilize mobile devices on a daily basis and do not care if the Bluetooth or GPS are active (even without using them) all the time. If the Bluetooth is active, an attacker could obtain sensitive data such as user information without the proper consent. In the case of GPS, leaving it active can makes possible to an attacker locate the current position of the user and use this information against the user desire. In addition, to leave this resources turned on all the time infers in more energy consumption, which impacts on the availability of the device.

Another type of attack occurs when there is not any password in the main screen of the mobile device. To use a mobile device without password in the initial screen causes the user to be vulnerable to various attacks. For example, a physical attack on the device can occur, in which a malicious user with access to the device may access its internal data.

Finally, another type of attack is based on the fact that it is very common for users that need to access the Internet via notebook share their Internet connection of his mobile device by creating a Wi-Fi network. This procedure is known as a portable Wi-Fi router or anchorage. If not configured properly, this network is susceptible to attacks, in which an attacker may have access non-authorized information. This unsecured share of the smartphone Internet with the active router function can cause, for example, theft of documents, images and video files, installation of malicious software and passwords theft.

IV. General Solutions for the Security Improvement of the android device

It was highlighted in the previous sections how users are susceptible to security risks due to malicious user attacks, mobile loss, negligence developers, mobile user configuration errors and so on.

The focus of this section is to introduce relevant initiatives that propose general strategies to check and/or improve the general status of the device security.

A. Academic Initiatives

In [24], the author shows the creation of an application called Android Security Test, and one of its main features is to identify and classify threats considering its associated risks. The goal is to analyze the application settings and user applications in order to identify potential threats. The use of the system can be considerably simpler; the user must first download the application, and then click the "Test Your Phone" feature, which collects various information about the mobile settings to check the level of the current mobile security. Thereafter, applications send the information (security level), in the form of a report to the user.

In addition, the Android Security Testing Initiative [24] analyzed the data that was collected from more than 375,000 users who downloaded the application from November 2010 to March 2011. The data collected include information on the device, general settings and application permissions. In resume, this data shows three important facts. Firstly, most users are not using the security mechanisms that are available for use on the Android device such as to use password in the initial screen, to encrypt the memory card and so on. Secondly, due to its open nature, operating system updates and security patches cannot be generated and distributed from a single source. Finally, the Android security permission mechanism is poorly documented and prone to misuse by developers.

Another interesting work, named LeakMiner [24], consists on an application that controls the security of Android mobile device. Most applications for PC and Android application deal with personal information, such as contacts and SMS messages, and the leakage of such information can cause significant damage for Android users [25]. Recent approaches to Android leak detection are focused on the dynamic analysis of the user's location, based on the fact that the leakage requires more runtime overhead. LeakMiner focused on the detection of confidential information leakage in Android with static analysis rather than dynamic approaches. Based on this fact, LeakMiner can detect information leaks before applications are distributed to users. LeakMiner detects three activities in the loss of information.

B. General solutions available on the Android Market

Focusing on the Android user’s safety, companies and institutes have created several applications to minimize the risk of malware attacks and threats in the system.

In a recent survey conducted by AV-Test [3], an independent security institute, malware detection tests were performed in 30 applications available on Google Play. 14 of these applications were able to detect any kind of malware: Antiy AVL [1], Avira [2], Bitdefender [4], GData [8], Ikarus [11], Kaspersky [13], Kingsoft [14], KSMobile CMS [15], McAfee [17], Norton [18], Qihoo 360 [19], Trend Micro [21] and TrustGo [22].

Considering the security applications submitted to the AV-Test Institute, the applications that stand out were: Avira, Bitdefender, Kaspersky, McAfee, Quick Heal Mobile Security and Norton [9]. Each one of these has its relevance, but Ikarus, Quick Heal Mobile Security and Trend Micro has specific features that will be described at this point.

Ikarus antivirus [12] protects mobile giving reliability to the user against malware and Internet applications, yet finds and removes viruses, Trojans, spyware, adware and other malware. Developers ensure that this security application does not consume a lot of battery and memory. An interesting advantage of this solution is the automatic monitoring of infection [9].

The solution developed by Trend Micro, called Trend Micro Mobile Security [21], is a security application that has anti-phishing, download protection and a specific filter for unwanted messages. One of its main features is to block malware that may come in the application downloaded from Google Play. Another important feature is to protect user privacy finding lost phones or tablets, and also performs backup of photos and videos with 50 MB of storage in the cloud.

Finally, the Quick Heal Mobile Security application [22] is available for the Android operating system and has the function of protecting the mobile device against malware and also against theft or loss. This solution also has security filters that can block numbers and also unknown numbers starting and ending with a certain numbers. This security application also has the function of notifying the user of programs that can affect the user privacy, and guides this user on settings that can improve the security of the device. In addition, the user can manage the mobile device via the management portal.

V. Conclusions and Future Work

This paper aimed to present and analyze current security vulnerabilities and solutions focused on Android-based mobile devices. The main objective is to present an updated set of security risks, vulnerabilities and applications focused on the Android platform. One of the most important strategies presented on this work is based on the search of risky settings made by the high-level user. To search, identify and mitigate these risks is very important because a considerable number of attacks are based on the user misconfiguration.

As future work, we intend to implement a specific solution to search for possible user misconfiguration and to suggest corrections to the high-level user in order to increase the device security level. Thus, this solution will be able to reduce the number of vulnerability points caused by poor user configuration, increasing the security level of the mobile device.

References

[1] Antiy Avl. Available in http://www.antiy.net/. Last visit: 24/03/2015.

[2] Avira. Available in http://www.avira.com/pt-br/index/x-c-channel/AW/awc/5659_1441673668_8b0e98602de0696bd20f3d117b0e6aaf. Last visit: 24/03/2015.

[3] AV-Test. Available in http://www.av-test.org/en/news/news-single-view/av-test-media-coverage-iv2014/. Last visit: 07/02/2015.

[4] Bitdefender. Avaliable in http://www.bitdefender.com/?c=1. Last visit: 24/03/2015.

[5] Cheetah Mobile. CM Security Research Lab July Security Report: Smartphone vulnerabilities summary. Available in http://www.cmcm.com/blog/en/security/2014-08-15/370.html. Last visit: 04/11/2014.

[6] Computer World . 98% of mobile malware targets Android platform. . Available in http://www.computerworld.com/article/2475964/mobile-security/98--of-mobile-malware-targets-android-platform.html. Last visit: 12/03/2015.

[7] D. Akiyo Yomoah. Should access to the internet be a human right?. Avaliable in http://africanarguments.org/2013/09/12/ should-access-to-the-internet-be-a-human-right-by-doreen-akiyo-yomoah/. Last Visit: 02/11/2014.

[8] Gdata. Available in https://www.gdatasoftware.com/. Last visit: 24/03/2015.

[9] Hubert Nguyen. Google Bouncer to fight Android malware. Available in http://www.ubergizmo.com/2012/02/google-bouncer-to-fight-android-malware/. Last visit: 07/01/2015.

[10] ITU- World in 2013: ICT Facts and Figures. Available in http://www.itu.int/net/pressoffice/press_releases/2013/05.aspx#.VQsaDY7F_hA. Last visit: 01/11/2014.

[11] Google Play. Ikarus mobile.security. Available in https://play.google.com/store/apps/details?id=com.ikarus.mobile.security Last visit: 20/04/2014

[12] Ikarus Mobile Security. Available in http://www.ikarussecurity.com/at/. Last visit: 24/03/2015.

[13] Kaspersky Mobile Security. Available in http://usa.kaspersky.com/?sitepref=US. Last visit: 25/03/2015.

[14] Kingsoft Mobile Security. Available in http://m.duba.com/. Last visit: 25/03/2015.

[15] KSMobile CMS. Available in http://www.cmcm.com/pt-pt/. Last visit 25/03/2015.

[16] Lukas Jeter, Shivakant Mishra. Identifying and quantifying the android decide users security risk exposure. International Conference on Computing. 2013.

[17] McAfee Mobile Security. Available in http://affiliates.digitalriver.com/z/343316/CD133407/ieao58lsmk00ypei009sf/. Last visit: 25/03/2015

[18] Norton Mobile Security. Available in http://br.norton.com/. Last visit: 25/03/2015.

[19] Qihoo 360 Mobile Security. Available in http://www.360.cn/. Last visit: 25/03/2015.

[20] Security Architecture for open systems Interconnection for ccit apolications. Smartphone vulnerabilities summary. Avaliable in http://www.cmcm.com/blog/en/security/2014-08-15/370.html. Acess in 03/12/2014.

[21] Trend Micro Security Mobile. Available in http://www.trendmicro.com/us/index.html. last visit 25/03/2015.

[22] TrustGo Mobile Security. Available in http://www.baidu.com/search/error.html. Last visit 25/03/2015.

[23] Quick Heal Mobile Security. Available in http://www.quickheal.co.in/home-users/quick-heal-mobile-security. Last visit: 07/02/2015.

[24] Zhemin Yang, Min Yang. LeakMiner: Detect Information Leakage on Android with Static Taint Analysis. Third World Congress on, 2012.

[25] Zhemin Yang, Min Yang, Yuan Zhang, Guofei Gu, Peng Ning, X. Sean Wang. AppIntent: Analyzing Sensitive Data Transmission in Android for Privacy Leakage Detection. 2011.

Intrusion Detection and Prevention Systems (IDPS) State of Art

IDPS Challenges

Homam Reda El-Taj
Community College
Univesity of Tabuk
Tabuk, Saudi Arabia

***Abstract*— Over the past few years, we have witnessed an ever-increasing rampant battle between network managers & computer criminals which led to many developments in the tools used by both parties i.e. " legitimate computer professionals & computer criminals". Recently, interruption exposure & avoidance systems have earned increasing appreciation due to their more frequent involvement in the security domain since they allow security analysts to make fast reactions and thus take quick decisions to prevent any possible damage. This underlines the significance of upgraded detection & prevention processes, taking into consideration the competitive and dynamic network environment these days. Most commercial and government information systems are connected through the internet, which will expose them to possibilities of spasms. The increasing number of computer users marks it precise, ever since computers have become a necessary device in our lives. This article covers the IDPS state of art and discusses the IDPS challenges.**

Keywords-component; Network, IDS, IPS, Security, IDS Myths, IDS Alerts.

I. Introduction

Before we go into the challenges of IDPS we need to highlight & understand each term that concerns the IDPS starting with IDS, IPS and Threats.

A. Intrusion Detection System (IDS)

Intrusion detection can be defined as the method to identify “any set of actions that attempt to compromise the integrity, confidentiality, or availability of a resource” [1, 2, 3]. IDS generally monitors any system held in three phases: the collection of audit data, the analysis of collected data and finally the release of an alert when a threat is detected [4, 5]. IDS can be classified in many different ways; the major classifications are: Active and Passive IDS, Network Intrusion detection systems (NIDS) and host Intrusion detection systems (HIDS), and finally, Knowledge-based (Signature-based) IDS and behavior-based (Anomaly-based) IDS [4 – 7].

1) Active and passive IDS

An active Intrusion Detection System (IDS) is also known as the Intrusion Detection and Prevention System (IDPS)[8]. Intrusion Detection and Prevention System (IDPS) is constructed to automatically block suspected attacks without any interference required by an operator. Intrusion Detection and Prevention System (IDPS) has the benefit of providing real-time corrective action in response to an attack [2, 4, 8].

A passive IDS system is assembled just to monitor and analyze network traffic activity and alert an operator to possible vulnerabilities and attacks. A passive IDS is not capable of performing any protective or corrective functions on its own.

1) Network Intrusion detection systems (NIDS) and Host Intrusion detection systems (HIDS)

A Network Intrusion Detection System (NIDS) usually consists of a network appliance (or sensor) with a Network Interface Card (NIC) operating in promiscuous modes and which has a separate management interface; NIDS normally runs at the gateway of a network to capture and examine network packets that go through the network hardware interface [9, 10].

A Host Intrusion Detection System (HIDS) relies on operating system audit data to monitor and analyze the events generated by programs or users on the host that may cause any intrusion attempts on critical servers. HIDS monitors the operating system and write data to log files and/or trigger alerts. HIDS can only monitor the individual workstations on which the HIDS are installed and it cannot monitor the entire network [10].

2) Knowledge-based (Signature-based) IDS and behavior-based (Anomaly-based) IDS

A knowledge-based (Signature-based) Intrusion Detection System (IDS) references a database of previous attack signatures and known system vulnerabilities. IDS is documented evidence of an intrusion or attack. Each intrusion leaves a footprint behind (e.g., nature of data packets, failed attempt to run an application, failed logins, file and folder access etc.). These footprints are called signatures and can be used to identify and prevent the same attacks in the future. Based on these signatures Knowledge-based (Signature-based) IDS systems identify intrusion attempts.

Some of Signature-based IDS disadvantages of are: Signature database must be constantly updated and continued, and Signature-based Intrusion Detection Systems (IDS) may fail to identify matchless attacks [5-8, 11, 12].

A Behavior-based (Anomaly-based) Intrusion Detection Systems (IDS) references a baseline or learned pattern of normal system activity to identify active intrusion attempts. Deviations from this baseline or pattern cause an alarm to be triggered. Higher false alerts are often related with Behavior-based Intrusion Detection Systems (IDS) [11-14].

B. Intrusion Prevention System

Intrusion prevention system (IPS) is a network device/software that works similar to a firewall in order to recognize and block network threats, by evaluating each packet based on the network protocols in the application layer. Since Intrusion prevention came out of research on the short comings of intrusion detection (Prevention after Detection), so it got the same categories or types based on the methodology used (Signature base or Anomaly base), and that is the reason why in some article they write (IDPS) to refer to IPS [8, 13, 20].

2) Myths About Intrusion Prevention

There are a diverse number of superstitions about Intrusion Prevention. The IDS marketing system caused most of this disinformation, or the unawareness of the proper way to operate a well-designed in-line IPS device, and the lack of information about its capabilities [21]. Let's examine a few of the most common myths:

a) MYTH 1: Each one of the detection & prevention of intrusion methods has a single solution.

At the time being, this is the case. The limitations of integral performance have caused to design IPS products with a very limiting signature set on board, and a little space to increase it without affecting performance seriously. A limited number of exploits could be prevented, and these are mostly the most serious; it undeniably means that a little space is available to the security administrator, to nip out the product for his own environment. it means as well that because the detection capabilities of the IPS product are so restricted, in order to alert on those exploits that aren't covered, an extra IDS product is compulsory overdue it. Intrusion prevention products that are designed from bottom to top should be capable of providing a far-reaching signature set that allows them to operate in either or both IDS and IPS modes.

The most supple IPS appliance will make it possible to initiate in passive IDS mode, while possibly attached to a wide port or network tap device in order to permit the administrator to determine how successful it can be in detecting an extensive variety of exploits and (just as importantly in the case of an IPS) how prone it is to false positives.

When the signature set is adjusted, switching to in-line mode and starting to block some or all detected suspicious packets and flows, is a simple procedure for the administrator. Good Intrusion Prevention is actually an extension of IDS, not something completely separate [21].

b) MYTH 2: Intrusion Prevention Is ALL or NOTHING

As shown in the previous myth, this is obviously false when the right kind of appliance is deployed. It is possible to have it block only a subsection of exploits, even where an IPS product can only operate in an in-line mode, and even as most packets are passed through as normal. Behind the IPS device, you'll have a traditional passive-mode IDS, which does most of the detection and alerting on suspicious traffic. Obviously, this is not a case of all-or-nothing; however, the use of two separate tools will undoubtedly cause implementation and management problems. This can be enhanced significantly with a device that has been designed from the ground up as an IDS as well as an IPS. As it has been shown in Myth #1, it is possible to structure an appliance that offers both IDS and IPS functions at the same time, providing an unassailable migration path from pure detection to prevention. Now imagine a device with several network ports, with each port capable of supporting SPAN, tap or in-line mode. Now you overcome the "all or nothing" concept and adopt a truly combined IDS/IPS solution in a single box. One pair of ports can be joint to provide an in-line prevention feature (say on the private LAN), while another pair of ports can be selected as a passive-mode IDS (say on the DMZ), providing full detection and alerting features. Now the administrator can deploy both technologies using a single appliance controlled by a single management interface. The management and configuration capabilities are also important if we are to avoid the "all or nothing" notion. Previously, network sensors have often used a monolithic approach to setting intrusion policy and response, with the response being fixed according to the signature. Modern IDS/IPS sensors, however, should be capable of permitting the administrator to adjust the response according to a per-signature or per-signature group basis perhaps port scans are given abnormally low significance in one particular environment, while IIS Web server exploits are blocked and the administrator paged. Utilizations are dissimilar, and so the IDS/IP device should demonstrate enough flexibility to allow the administrator to configure the alerts and responses to his or her specific needs [21].

c) MYTH 3: Intrusion Prevention Is TCP Kills/Resets or Modify Firewall Rules by IDS

One can easily see where this myth came from. Quickly review the marketing literature of many traditional IDS products today, and you may well see claims that they offer "Intrusion Prevention" features. Only one kind of prevention can be delivered by a passive IDS device i.e. to send TCP Resets to both ends of the connection when a doubtful packet has been detected, or maybe to reconfigure an external firewall or router device to ensure that the rest of the flow is blocked at the network borderline. Nevertheless, the problem here is that unless the invader is operating on a 2400 baud modem, the probability is that by the time the IDS has detected the unlawful packet, raised an alert, and transmitted the TCP Resets, and especially by the time the two ends of the connection have received the Reset packets and acted on them (or the firewall or router has had time to activate new rules to block the remainder of the flow), the load of the exploit has long since been conveyed. We believe that there are not many offenders using 2400 baud modems these days. A true IPS device, however, is sitting in-line all the packets have to pass through; therefore, as soon as a suspicious packet has been detected and before it is passed to the internal interface and on to the protected network, it can be aborted. Moreover; as the flow has been identified as suspicious, all subsequent packets that are part of that session can also be aborted with minimum extra processing. It is also possible to send TCP Resets or ICMP Unreachable messages to the attacking host [21].

d) MYTH 4: Intrusion Prevention Is Losing Control Over Intrusion Detection and Response

To this point, hopefully we have made it clear that this is simply not true. The IPS device has been designed properly and, in the way of intrusion detection and response, it offers more than any basic IDS product. If carefully designed, typically involving custom hardware and ASICS for the highest levels of performance when operating in in-line mode, the IPS device can provide remarkable detection capabilities that are equal to the best passive IDS. In addition, only an in-line IDS can block all IP/ICMP/TCP/UDP based malicious traffic from reaching the intended target hosts with complete reliability and/or scrub non-conforming packets to defeat many DoS or reconnaissance attempts. Most customers wish to use the IDS in the Intrusion Detection Mode (sniffing mode) initially and then migrate to the Intrusion Prevention mode (in-line mode) [21].

C. Computer Security Threats

Based on Techopedia; "a threat, in the context of computer security refers to anything that has the potential to cause serious harm to a computer system. A threat is an action that has the potential to cause serious damage. Threats can lead to attacks on computer systems, networks and more. Also, they can turn potential vulnerabilities into attacks [22]. They can put individuals' computer systems and business computers at risk; therefore, vulnerabilities have to be fixed so that attackers cannot infiltrate the system and cause damage. Threats can include everything from viruses, trojans, and back doors to outright attacks from hackers. Generally speaking, the term blended threat is more precise, as the majority of threats comprise multiple exploits. For example, a hacker might use a phishing attack to gain information about a network and break into a network [15, 23].

1) Trojan:

Trojan is one of the most intricate threats of all. The Trojan family such as Zeus and SpyEye comprise most of the banking threats. It can hide itself from antivirus detection and take important banking data to compromise your bank account. Furthermore, if the Trojan is really powerful, it can take over your entire security system as well. Consequently, a Trojan can cause numerous types of damage to your own computer and to your online account [24].

2) Virus:

10 years back, Virus was widespread. It is a malicious program where it duplicates itself and aims only to destroy a computer. The ultimate goal of a virus is to guarantee that the victim's computer will never be able to function properly or even at all. Today, It is not common because Malware today is designed to earn money over destruction. Accordingly, Virus is only used by people who want to take revenge on their adversaries [24].

3) Worms:

It is program designed only to spread and thus it is one of the most harmless threats. It does not change your system, but it can spread from one computer to another within a network or even through the internet. The computer security risk here is that it will consume your computer hard disk space due to the duplication and will take up most of your bandwidth as a result of its spreading [24].

4) Spyware:

This Malware is intended to spy on the victim's computer. When infected with it, the daily activity or a certain activityby the computer user will be spied by the spyware which will find a way to contact the host of this malware. Typically, this spyware is used to know what the daily activity of the computer user is so that the attacker can make use of his data. For instance, if you browse on sex toys every day for a week, the attacker will try to come out with a sex toy scam to rip off your money [24].

5) Scareware:

Scareware is something that you plant into your system and instantly it will notify you that you have hundreds of infections which you don't have. It tries to trick you into purchasing a false anti-malware that claims to eliminate those threats. It is all about ripping off your money through scaring you to buy the malware [24].

6) Keylogger:

It keeps a record of every keystroke you made on your keyboard. . It is a sub-function of a powerful Trojan that threatens to steal people's login credential such as username and password [24].

7) Adware:

Adware is a form of threat where your computer will start popping out a lot of advertisement. These advertisements can be anything from non-adult materials to adult materials as any type of ads will make the host some money. It is not really a harmful threat but it can be really annoying [24].

8) Backdoor:

Backdoor is not really a Malware but rather a method where once a system is exposed to it, the attacker will be able to bypass all the regular verification service. It is usually installed before any virus or Trojan infection because having a backdoor installed will facilitate the transfer of those threats [24].

9) Wabbits:

Is another self-replicating threat but it does not work like a Virus or Worms. It does not harm your system like a Virus and it does not replicate via your LAN network like Worms. An example of Wabbit's attack is the fork bomb, a form of DDoS attack [24].

10) Exploit:

Exploit is a software specifically designed to attack a certain vulnerability. For instance, if your web browser is vulnerable to some outdated vulnerable flash plugin, Exploit will work only on your web browser and plugin. The way to avoid Exploit is to always patch your stuff because the function of software patches is to fix vulnerabilities [24].

11) Botnet:

Botnet is installed by a BotMaster to take hold of all the computer bots via the Botnet infection. It mostly infects through drive-by downloads or even Trojan infection. The result of this threat is the victim's computer, which is the bot will be used for a large scale attack like DDoS [24].

12) Dialer:

This threat is no longer common today, but looking at the technology 10 years back or more when we used to access the internet by means of a dial-up modem, it was quite a popular threat back then. What it does is that it makes use of your internet modem to dial international numbers which are pretty expensive. Today, this type of threat is more popular on Android as it can make use of the phone call to send SMS to premium numbers [24].

13) Dropper:

As the name suggests, a Dropper is designed to drop into a computer and install something beneficial to the attacker such as Malware or Backdoor. There are two types of Dropper: the first type immediately drops and gets installed to avoid Antivirus detection. The second type only drops a small file which will auto trigger a download process to download the Malware [24].

14) Fake AV:

Fake Antivirus threat became a very popular threat among Mac users about 10 months ago. Because Mac users rarely face a virus infection, scaring them with message which tells them that their computer is infected with virus is pretty useful as it results into them purchasing a bogus antivirus which does nothing [24].

15) Phishing:

Creating a false website designed to look exactly like the actual website where the users are tricked into entering their username and password into the fake login form which is used to steal the identity of the victims. Every form sent out from the phishing site will not go to the actual server, but to the attacker controlled server [24].

16) Cookies:

Cookies are not really a Malware as such. It is used by most websites to store data into your computer. It is used because it has the ability to store things into your computer and track your activities within the site. If you really don't like the presence of cookies, you can choose to disable them for some of the sites which you do not know [24].

17) Bluesnarfing:

Bluesnarfing is having an unauthorized access to specific mobile phones, laptops, or PDA via Bluetooth connection. By having such unauthorized access, personal stuff such as photos, calender, contacts and SMS will all be revealed and probably even stolen [24].

18) Bluejacking:

Bluejacking also uses the Bluetooth technology, but it is not as serious as Bluesnarfing. What it does is that it connects to your Bluetooth device and sends a message to another Bluetooth device. It does not damage your privacy or device system compared to the Bluesnarfing threat [24].

19) DdoS:

This is one of the most well-known activities done by Anonymous attackers where millions of traffic is sent to a single server to cause the system to disable a certain security feature so that the anonymous attackers can do their data stealing. This kind of trick which is to send a lot of traffic to a machine is known as Distributed Denial of Service, also known as DDoS [24].

20) Boot Sector Virus:

It is a virus that places its own codes into computer DOS boot sector. It is also known as the Master Boot Record. It will only start if there it is injected during the boot up period where the damage is high but difficult to infect. The victim needs to do if he realizes there is a boot sector virus is to remove all the bootable drive so that this particular virus will not be able to boot [24].

21) Browser Hijackers:

A browser hijacker uses the Trojan Malware to take control of the victim's web browsing session. It is extremely dangerous especially when the victim is trying to send some money via online banking because the hijacker can alter the destination of the bank account and even the amount [24].

22) Chain Letters:

When I was small, I got tricked with chain letters written by my friend. But chain letters do not stop at that era. Even adults, like to send chain letter. Chain letters like Facebook account delete letters which say if you don't forward that particular message or email to 20 people or more, your account will be deleted, are simply not real, yet people really believe them [24].

23) Virus Document:

Nowadays, Virus can be spread through document files especially PDF document files. In the past, people would only advice you simply not to execute an EXE file, but in today's world with today's technology, document file should also be avoided. It is best if you use an online virus scanner to scan any suspicious file before opening it [24].

24) Mousetrapping:

I am not sure if you had encountered a Mousetrapping Malware before where it traps your web browser to a particular website only. If you try to type another website, it will repeatedly redirect you back. If you try clicking forward/backward of the navigation button, it will also redirect you back. If you try to close your browser and re-open it, it will set the homepage to that website and you can never get out of this threat unless you remove it [24].

25) Obfuscated Spam:

In actual fact, obfuscated Spam is a spam mail. It is obfuscated in the way that it does not look like any spamming message so that it can trick the potential victim into clicking it [24]. Spam mail today looks very genuine and if you are not careful, you might just be attracted to what they are offering [24].

26) Pharming:

Pharming works more or less like phishing but in a more complicated way. There are two types of pharming: one is DNS poisoning where your DNS is being compromised and all your traffic will be redirected to the attacker's DNS. The other type of pharming is to edit your HOST file where even if you typed www.google.com on your web browser, it will still redirect you to another site. Both types are equally dangerous [24].

27) Crimeware:

Crimeware is a form of Malware which takes control of your computer to make you commit a computer crime on behalf of the attacker. Instead of the hacker himself committing the crime, it plants a Trojan or whatever the Malware is called to order you to commit a crime instead. This will make the hacker himself clean from whatever crime that he had done [24].

28) SQL Injection:

SQL injection does not damage the end users directly. It aims to infect a vulnerable website. What it does is that it gains unauthorized access to the database and the attacker can recover all the valuable information stored in the database [24].

II. IDPS Challenges

IDPS as any other system got some challenges that require additional research.

A. IDS rules got different format

One of the challenges in IDS rules' analysis is the absence of the common format. [25]. IDS rule are different from firewall rules in the following areas:

1) Firewall rules often have a common format but IDS rules don't.

2) Firewall rules usually have a small set of actions such as (allow, deny) whereas IDS rules got different responses.

3) Rule ordering plays essential role in firewall rules while it is not necessarily in IDS rules.

B. Current IDPS doesn't support mobile ad-hoc environment

Compared with wired networks; traffic monitoring is usually done at switches, routers and gateways, the mobile ad-hoc environment does not have such traffic concentration points where the IDPS can collect audit data for the entire network. Therefore, the only available audit trace will be limited to communication activities taking place within the radio range, and the intrusion detection algorithms must be made to work on this partial and localized information [1, 26, 27].

C. The amount of alerts generated by IDS

After turning on the typical intrusion detection system for the first time, the IDS station will get spammed. Intrusion detection systems regularly give off over 10,000 alerts a day. For sure not those entire alerts map to real intrusions. A separation process is needed to get value out of an intrusion detection system; separation process "tuning process" is very expensive upfront cost. And, even after tuning, there can be a significant ongoing cost to look at alerts that you might want to review [28-30].

D. Network Architecture Issues

This challenge is for the NIDS solution since it listens to all traffic of the network. Switches are an issue for a NIDS (switch forwards traffic to the ports that have devices involved in a given conversation). Using switches in networks led to many advantages such as (eliminate collisions, reduce processing power required on terminating devices and they make malicious packet sniffing much more difficult). The last advantage of switching is a problem for a NIDS [4, 10, 23, 31].

E. High Speed Networks

The network speed increases ahead of the processing power available to process every packet off the network. Current high-end systems should be able to cope with a marginally loaded gigabit network, but will not be able to come close to coping with a fully loaded 10G network [31].

F. Type of IDS alerts

Alerts are the reason for having and IDS. Without them you simply have a complex sniffer. There are two types of alerts that IDS triggers either true alerts or false alerts. IDS generates thousands of alerts per day, analyzing these alerts will cost the organization time and effort which causing tension to the system analysts. Most system analysts consider these alerts as false positive alerts while they can be normal noise caused by the IDS (login failure on a password authentication server) [10]. There are four types of IDS alerts: (*false positive alerts, false negative alerts, true positive alerts and true negative alerts*), keeping in mind that positive = identified and negative = rejected, therefore: (True positive = correctly identified, False positive = incorrectly identified, True negative = correctly rejected, False negative = incorrectly rejected).

1) False positive:

Is a mystery term that describes a situation where the IDS trigger an alert when there is a malicious activity in simple words (IDS makes a mistake). When an IPS has a false positive, the primary concern is that legitimate traffic will be blocked. IPS false positive is a much more serious matter than an IDS false positive, if an IPS blocks legitimate traffic a few times; blocking legitimate traffic consider as much more serious problem than generating a false alert. The difference between IDS and IPS false positives also means that some types of filters that are appropriate for IDS are not appropriate for IPS. IDS filters leads on suspicious activity intended for a human to follow, while IPS filters are used for automatic action such as blocking traffic or quarantining an endpoint. There are many reasons behind the false positive such as:

a) If the training stage (in IDS anomaly base) was not trained enough, this will make the running stage got so many false positive alerts.

b) If IDS rules are (in IDS signature base) framed and adjusted; several of similar false positive alerts will be generated by IDS. IDS rules should detect intrusions based on pre-defined rules, tuning these rules will led to minimizing the amount of alerts which will kill a huge number of false positive alerts. This method is effective in IDS (An IDS false positive is an alert that did not result in an intrusion.) but it so dangerous in the IPS. Since the primary concern is that legitimate traffic will be blocked, and blocking such traffic will led to yank it out of the network.

c) There are different research papers was introduced to reduce the false positive alerts, these papers stated that there is two different ways to study the false positive reduction either by studying the false alert reduction at the sensor level or at the log alert file (after intrusion accrued) [13].

2) False Negative:

Is a genuine attack that had not been noticed (Missed Alerts). False negatives are hard to quantify (it's difficult to figure out what you don't know). False negative create two problems (there are missed attacks that will not be discovered, false negatives give a false sense of security) [30]. There are many reasons behind the false negative such as:

a) Traffic encryption: Encrypted traffic does not trigger alerts because the signature patterns don't match.

b) Faulty signatures: It may be that a signature is written incorrectly (in IDS with misuse detection method) and are not watching for the correct attack signature.

c) Any environment relying on anomaly detection method should be relying on file changes, the assumption must be that at the time of training the network or system was not compromised. If this is not true there will be false negatives for any already exploited conditions.

d) Poor change management: Mostly there are no separate departments in most organizations to handle network administration, and security, which causes a lack in the signature updates.

e) Snort sensor administration problems: (Snort is a popular IDS) [30] tuning the Snort rule set to control false positives, while eliminates an important rule may cause an attack or probe to be unnoticed [31].

c) An overloaded IDS will drop packets potentially causing false negatives.

3) True Positive Alerts

A legitimate attack which the IDS triggers an alert for it, there is no much in the web about this type of alerts since it should be about how the IDS works [32].

4) True Negative Alerts

Is the state of IDS where there is no attack has taken place and no alert is triggered. This will happened when all the rules, tools and signatures have evaluated the packet/ log and found nothing to match. True negative alerts are an important term that should be considered when tuning up the IDS, since bad tuning will affect the sensitivity of security system, and correlating these alerts will make the IDS alerts more significance [33].

III. Conclusion

IDPS as any exciting system needs to be improved, this article discusses IDS and IPS, the threats that IDS is trying to catch, the myths behind these two systems, the challenges that IDS faces and the types of alerts that IDS triggers.

This article helps network security researchers know the state of art stage that the IDPS reaches, so they can start from that point to build their own research. By the finding of this article the researcher came out with: *1- A proof that IDS and IPS are not the same system. 2-The type of threats are defined and categorized. 3-There is a lack of researches to cover IDS true positive alerts and true negative alerts*,

Acknowledgment

The author would like to acknowledge financial support for this work, from the deanship of Scientific Research (DSR), University of Tabuk, Tabuk, Saudi Arabia, under grant no. 0222-1436.

References

[1] A. Fourati and K. Al Agha, 'An IDS First Line of Defense for Ad Hoc Networks', 2007 IEEE Wireless Communications and Networking Conference, 2007.

[2] P. Zanna, B. O'Neill, P. Radcliffe, S. Hosseini and M. Ul Hoque, 'Adaptive threat management through the integration of IDS into Software Defined Networks', 2014 International Conference and Workshop on the Network of the Future (NOF), 2014.

[3] Salour and X. Su, 'Dynamic Two-Layer Signature-Based IDS with Unequal Databases', Fourth International Conference on Information Technology (ITNG'07), 2007.

[4] danielowen.com, 'NIDS in the Small-Midsize Business', 2015. [Online]. Available: http://danielowen.com/files/NIDS_in_the_Small-Midsize_Business.pdf. [Accessed: 14- Sep- 2015].

[5] Z. Fadlullah, H. Nishiyama, N. Kato and M. Fouda, 'Intrusion detection system (IDS) for combating attacks against cognitive radio networks', IEEE Network, vol. 27, no. 3, pp. 51-56, 2013.

[6] G. Victor, D. Rao and D. Venkaiah, 'Intrusion Detection Systems - Analysis and Containment of False Positives Alerts', International Journal of Computer Applications, vol. 5, no. 8, pp. 27-33, 2010.

[7] Homam El-Taj, Firas Najjar, Hiba Alsenawi, Mohannad Najjar, "Intrusion Detection and Prevention Response based on Signature-Based and Anomaly-Based: Investigation Study" (IJCSIS) International Journal of Computer Science and Information Security, Vol. 10, No. 6, June 2012.

[8] Manusankar, S. Karthik and T. Rajendran, 'Intrusion Detection System with packet filtering for IP Spoofing', Communication and Computational Intelligence (INCOCCI), 2010 International Conference on, pp. 563-567, 2010.

[9] Sans.org, 'SANS: Intrusion Detection FAQ: What is network based intrusion detection?', 2015. [Online]. Available: https://www.sans.org/security-resources/idfaq/network_based.php. [Accessed: 14- Sep- 2015].

[10] O. Abouabdalla, H. El-Taj, A. Manasrah and S. Ramadass, 'False positive reduction in intrusion detection system: A survey', 2009 2nd IEEE International Conference on Broadband Network & Multimedia Technology, 2009.

[11] B. Shwetha Nayak, 'Research on application of intrusion detection system in data mining', National Conference on Challenges in Research & Technology in the Coming Decades (CRT 2013), 2013.

[12] D. Mudzingwa and R. Agrawal, 'A study of methodologies used in intrusion detection and prevention systems (IDPS)', 2012 Proceedings of IEEE Southeastcon, 2012.

[13] G. Chen, H. Yao and Z. Wang, 'An Intelligent WLAN Intrusion Prevention System Based on Signature Detection and Plan Recognition', 2010 Second International Conference on Future Networks, 2010.

[14] excITingIP.com, 'An overview of IPS - Intrusion Prevention System and types of Network Threats', 2009. [Online]. Available: http://www.excitingip.com/626/an-overview-of-ips-intrusion-prevention-system-and-types-of-network-threats/. [Accessed: 14- Sep-2015].

[15] K. Haslum, A. Abraham and S. Knapskog, 'DIPS: A Framework for Distributed Intrusion Prediction and Prevention Using Hidden Markov Models and Online Fuzzy Risk Assessment', Third International Symposium on Information Assurance and Security, 2007.

[16] D. Stiawan, A. Abdullah and M. Yazid Idris, 'The trends of Intrusion Prevention System network', 2010 2nd International Conference on Education Technology and Computer, 2010.

[17] Ubiquity.acm.org, 'Ubiquity: Intrusion prevention systems', 2015. [Online]. Available: http://ubiquity.acm.org/article.cfm?id=1071927. [Accessed: 14- Sep- 2015].

[18] D. Mudzingwa and R. Agrawal, 'A study of methodologies used in intrusion detection and prevention systems (IDPS)', 2012 Proceedings of IEEE Southeastcon, 2012.

[19] M. Chen, K. Chien, C. Huang, B. Cheng and Y. Chu, 'An ASIC for SMTP Intrusion Prevention System', 2009 IEEE International Symposium on Circuits and Systems, 2009.

[20] mcafee.com, 'Intrusion Prevention: Myths, Challenges, and Requirements Whitepaper', 2015. [Online]. Available: http://www.mcafee.com/japan/products/pdf/intrusionprevention_whitepaper_en.pdf. [Accessed: 14- Sep- 2015].

[21] Techopedia.com, 'What is a Threat in Computing? - Definition from Techopedia', 2015. [Online]. Available: https://www.techopedia.com/definition/25263/threat. [Accessed: 14-Sep- 2015].

[22] G. Hashimoto, P. Rosa, E. Filho and J. Machado, 'A Security Framework to Protect against Social Networks Services Threats', 2010 Fifth International Conference on Systems and Networks Communications, 2010.

[23] IT Security Column, '28 Types of Computer Security Threats and Risks', 2015. [Online]. Available: http://www.itscolumn.com/2012/03/28-types-of-computer-security-threats-and-risks/. [Accessed: 14- Sep- 2015].

[24] Integration, T. zyer, K. Kianmehr, M. Tan and S. Wien, 'Recent Trends in Information Reuse and Integration | Tansel zyer | Springer', Springer.com, 2015. [Online]. Available: http://www.springer.com/us/book/9783709107379. [Accessed: 14- Sep-2015].

[25] Yongguang Zhang, Wenke Lee, Yi-An Huang, "Intrusion detection techniques for mobile wireless networks" Wireless Networks, Volume 9 Issue 5, September 2003, Pages 545 – 556

[26] B. Sun, L. Osborne, Y. Xiao and S. Guizani, 'Intrusion detection techniques in mobile ad hoc and wireless sensor networks', IEEE Wireless Commun., vol. 14, no. 5, pp. 56-63, 2007.

[27] John Viega, "The Myths of Security: What the Computer Security Industry Doesn't Want You to Know 1st Edition", O'Reilly Media, Inc, 2009.

[28] kaspersky.com, 'Statistical Analysis of Snort Alerts.', 2015. [Online]. Available: http://www.kaspersky.com/images/remi-omosowon,_o._b._-_statistical_analysis_of_snort_alerts.pdf. [Accessed: 14- Sep- 2015].

[29] Snort.org, 'Snort.Org', 2015. [Online]. Available: https://www.snort.org/. [Accessed: 14- Sep- 2015].

[30] Books.gigatux.nl, '9.2 False Negatives (Missed Alerts)', 2015. [Online]. Available: http://books.gigatux.nl/mirror/snortids/0596006616/snortids-CHP-9-SECT-2.html. [Accessed: 14- Sep- 2015].

[31] Manish Kumar, M. Hanumanthappa, T. V. Suresh Kumar, "Intrusion Detection System - False Positive Alert Reduction Technique" ACEEE Int. J. on Network Security, Vol. 02, No. 03, July 2011.

[32] Google Books, 'Designing and Building Security Operations Center', 2015. [Online]. Available: https://books.google.com.sa/books?id=2GpzAwAAQBAJ&printsec=frontcover&dq=Designing+and+Building+Security+Operations+Center&hl=ar&sa=X&redir_esc=y#v=onepage&q=Designing%20and%20Building%20Security%20Operations%20Center&f=false. [Accessed: 14- Sep-2015].

AUTHORS PROFILE

Homam Reda El-Taj finished his Bachelor degree in Computer Science (CSCIS) from Philadelphia University Jordan in 2003, then he continued his graduate studies in Universiti Sains Malaysia (USM), he finished his master degree on distributed systems, and PhD on the Network Security.

Homam works as visiting researcher in National Advanced IPv6 Center of Excellence (NAv6) during his work as an assistant professor in University of Tabuk (UT), before that he was working as an assistant professor in Fahad Bin Sultan University (FBSU). Homam published several articles on Computer Networks field to cover subjects as:

Real time Network Security (Botnets/Worms/viruses), Intelligent Techniques in Detecting Network threats, Advanced Networking Mechanisms and protocols, Intrusion Detection of DOS & DDOS, Intrusion Anomaly Detection Methods, Intrusion Prevention Techniques, Intrusion Prevention, Decision Making, Intrusion Prevention Threats Behavior, Application Network traffic tracing, Network users and misuse detection, Intrusion Detection on QR Code, and Overlay Network.

Currently Homam is supervising some PhD students who are working on fields of Intrusion Detection & Prevention Systems (IDPS) and on the Intrusion Detection on QR Code.

Improving the Quality of Composite Services Through Improvement of Cloud Infrastructure Management

Olga Shpur
Department of Telecommunication
Lviv Polytechnic National University
Lviv, Ukraine

Mykhailo Klymash
Department of Telecommunication
Lviv Polytechnic National University
Lviv, Ukraine

Marian Seliuchenko
Department of Telecommunication
Lviv Polytechnic National University
Lviv, Ukraine

Bogdan Strykhaliuk
Department of Telecommunication
Lviv Polytechnic National University
Lviv, Ukraine

Orest Lavriv
Department of Telecommunication
Lviv Polytechnic National University
Lviv, Ukraine

***Abstract*— For improving the quality of composite services in cloud infrastructure this paper proposes an integrated control architecture using the NVF technology that provides load balancing with estimation of available system resources. The aim of our proposed algorithms is to assess existing physical and virtual, resources of telecommunication system. The analysis is based on the maximum value of integral resources index of each physical machine. Maximum values of available virtual and physical resources are transferred to Orchestrator, which provides the migration of service components to less loaded servers if necessary. Performance analysis of the proposed approach shows that load balancing by implementing integrated management architecture based on NVF technology allows to reduce the duration of service requests by 3 times.**

Keywords – cloud infrastructure management; load balancing; NVF; analysis cloud resources; duration of service requests

I. Introduction

Nowadays permanent traffic growth in the World Wide Web is observed. This is resulted from the fact that users strive to remotely operate with data regardless of location instead of store data locally. This concept requires increasing the performance of hardware and software of the provider's infrastructure as well as users' equipment improvement. However, increasing of computing capabilities may be unreasonable due to the high cost deployment. Therefore, providers prefer automated services based on the cloud technology instead of straightforward hardware enhancement. This approach provides three basic service models: infrastructure as a service (IaaS), platform as a service (PaaS) and software as a service (SaaS). These models require a good scalability and flexibility of existing hardware resources. The key technology that provides effective utilization of avaliable resources is virtualization [1]. Virtualization enables more efficient servers utilization that allows to decrease the amount of necessary hardware resources. Virtualization also provides live migration, especially when the server is overloaded and a copy of operating system with its applications can be moved to another less loaded server.

Load balancing increases the performance of cloud computing systems in terms of data flows distribution within the set of interacting hosts [2,3]. The aim of such a system is to prevent overloading of physical servers and distribute overall workload between available physical servers as even as possible.

Typically, the decision to migrate a virtual machine is taken based on the current workload of servers: available bandwidth of logical and physical channels, available computing resources (memory, CPU, etc.) [4]. In this paper, we propose a new approach for the evaluation of these parameters that allows to increase the effectiveness of load balancing by introducing an integrated control architecture based on the NVF (Network Function Virtualization) technology..

II. Recent work

The problem of available resources estimation in data centers is of great interest for both industry and academia [5-8]. Many researches have been published so far on the problem of resources availability at different levels of a cloud system. .

In [5], Soares et al. have studied the availability of physical servers in dynamic deployment of virtual machines.. Their approach is to develop Cloud4NFV (Cloud for NFV) platforms with VNF (Virtual Network Functions). Proposed platform includes the simulation of virtualized network functions as infrastructure resources. However, proposed platform and designed algorithm does not take into account available hardware and software resources of each physical machine.

Another approach proposed by Ma et al. [6] is to analyze the availability of complex applications based on the service-oriented architecture. The load balancing model was developed using TOPSIS (Technique for Order of Preference by Similarity to Ideal Solution) method. Authors claim that proposed system can achieve better load balancing in a large-scale cloud computing environment with less number of virtual machines migrations. However, proposed approach is not reliable for scenarios with dynamic variations of data centers parameters due to distance vector routing base. Alternative approach in [7] provides adaptive dynamic migration of virtual machines by implementation ofdistributed load balancing algorithm. Proposed algorithm is based on a selective tracking of migrations between VLANs (Virtual Local Area Networks) to simplify the control plane and reduce reconfiguration time of the data center. The simple model has been implemented that allows to decrease the time of virtual machines migration between data centers by converting them into Red Hat Cluster service. However, the implementation of proposed algorithm requires significant hardware resources and does not estimate the status of other physical machines. Therefore, it is necessary to develop a new approach to evaluate the performance of available resources and to increase the effectiveness of load balancing. In this paper, we develop an integrated control architecture using the NVF technology that provides load balancing with estimation of available system resources. The aim of our proposed algorithms is to assess existing physical and virtual, resources of telecommunication system. The analysis is based on the maximum value of integral resources index of each physical machine.

III. Proposed control plane architecture based on NVF functions

We propose the control plane architecture (Fig. 1) that includes:

- Virtual Infrastructure Manager (VIM), which is responsible for NFV resources management;

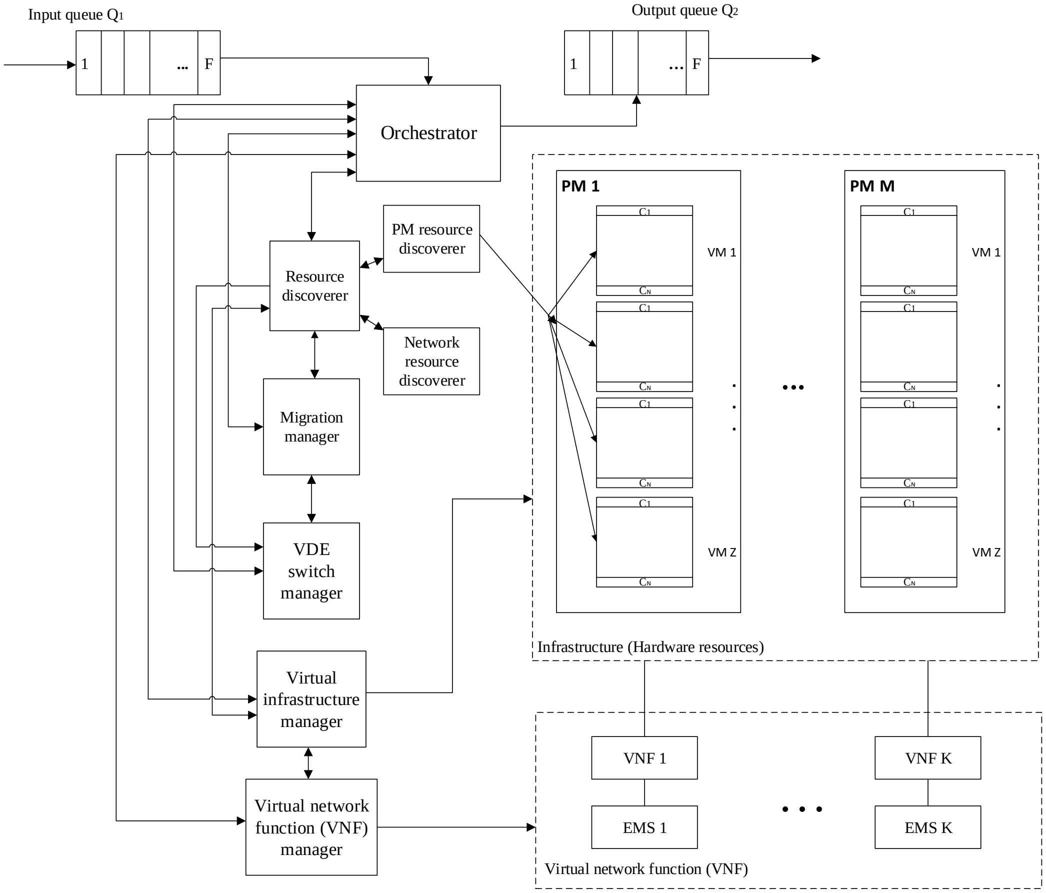


Figure 1. Conceptual model of management system for cloud-service provision.

- VNF manager – responsible for managing the lifecycle of VNF instances including copying, configuring, updating, up/down scaling). VNF manager is responsible for the entire life cycle of VNF providing the middleware between virtualized fuctions and Orchestrator. For example, VNF manager provides installing and configuring of software components;
- Resource discoverer (RD) – responsible for analysis of system resources. Its responsibilities include assessment of existing physical and virtual, computing resources as well as throughput. Based on the available bandwidth and availability of service components, the Orchestrator makes a decision to provide the service, or to migrate service components to a less loaded server in order to provide load balancing and optimal resources utilization;
- Migration manager – is responsible for the migration of virtual machines and informs the VDE (Virtual Distributed Ethernet) switch manager about VM (Virtual Machine) new location (number of VLAN, port, , etc.);
- VDE switch manager – supports and manages VDE switches allowing combination of virtual machines in VLANs to simplify their management.
- VDE switch is a virtual analogue of conventional Ethernet-switch. All virtual devices connected to VDE have the opportunity to interact with each other in a way like conventional devices interact in the real Ethernet network. VDEs also able to perform fast network reconfiguration regardless of ports quantity and without influence on the input queue . This feature is important to minimize end to end delays of the data transmission . VDE switch allows to control the data flow by adjusting the number of packets between electronic buffers of input and output ports.
- Orchestrator – responsible for orchestration and management of NFV resources and provides services basen on NFVI (Network Function Virtualization Infrastructure). Orchestrator handles following functions:
  - monitoring and control of service provision by using a common interface;
  - processing the system data of information services;
  - making the decision and informs Migration manager about necessity of VM migration by using information from Resource discoverer and informs VDE switch manager to change the location of VMs;
  - interacting with VIM and various VNF managers;
  - accessing services and infrastructure of VNF module, which contains information about priorities of services.

In our model, we suppose that cloud-system is requested to provide a service. The intensity of incoming request is a random variable with exponential distribution. The request of each service is putted into the input queue. Orchestrator provides instructions to Resource discoverer to check whether all components of required services are available, to wit there is enough computing capacity of physical and consequently virtual machine to process and provide all service components. While Resource discoverer checks the availability of free PM (Physical Mashine) resources, Network discoverer checks the status of physical and logical channels determining the optimal transmission for components exchanging of using the least loaded channel. If the Resource discoverer or Network discoverer reports about the lack of computing power or lack of necessary bandwidth, Resource discoverer informs the Orchestrator and sends information about available resources to Migration Manager, which makes a choice of PM and transfer the available component of service (conducts VM migration) in collaboration with VDE switch manager. VDE switch manager determines which VLAN is overloaded by VM requests and which VLAN is underutilized by VM requests. Then,a VDE switch performs switching of logic service components and provides system reconfiguration in accordance with the changes (i.e upgrades routing tables). The whole process of migration and operation in the system is conducted by the control of Orchestrator and Virtual Infrastructure Manager. If number of requests for a particular component sequentially increases Virtual Infrastructure Manager runs NFV technology. NFV allows to create a software abstraction of any physical device and process requests for service provision based on this device.

A. Principle of resources analysis

As mentioned above, Resource discoverer is responsible for analysis of system resources. Its responsibilities include assessment of existing physical and virtual computing and bandwidthresources. This analysis will be based on the maximum value of integral resources index of each physical machine. In order to determine this value it is necessary to control available hardware resources and their accessibility. Accessibility means availability of both computing resources of VM and bandwidth resources of communication channels. Computing parameters of VM, which hosts M_i components, are defined as following:

$$CPU_{pr} = \frac{\sum_{i=1}^{k} M_i \times CPU_i}{\sum_{i=1}^{k} M_i}, \tag{1}$$

$$RAM_{pr} = \frac{\sum_{i=1}^{k} M_i \times RAM_i}{\sum_{i=1}^{k} M_i}, \tag{2}$$

where M_i – the number of applications (components) in i-th VM; CPU_i – CPU (Central Processing Unit) clock speed of VM used by the i-th component; RAM_i – RAM of VM, used by the i-th component; k – the VMs quantity of one PM in a cloud system.

We propose a new algorithm to estimate the avaliable resources of cloud system (Fig.2). Proposed algorithm provides fast requests processing and analyzes degree of utilization for each machine by using the information about the processing power of each node (in our case –VM). Proposed algorithm is described below.

Let $z=\overline{1,Z}$ is a VM, which hosts $i=\overline{1,K}$ component of service $j=\overline{1,S}$, and $m=\overline{1,M}$ – a PM, which hosts $Z_m=\overline{1,Z}$ VMs. We denotesets of routes:

$$\begin{aligned} &P=\{P_1,\ldots,P_n,\ldots P_N\},\\ &n=\overline{1,N},\ P_n=\{e_1,\ldots e_l,\ldots e_L\},\\ &l=\overline{1,L}, \end{aligned}$$

where N – number of paths between components i and $i+1$, L – number of edges in the route n, which connect VM_z with VM_{z+1}. First, the input requests queue is checked for service components. If queue contains $f=\overline{1,F}$ requests for a particular component of the j^{th} service, the analyzer determines which resources are needed to maintain the service. Thus, a table of available CPU, RAM and bandwidth resources is forming to ensure access to the component within the time $t<t_{\max}$ and to determine VM type for each component of the composite service. Simultaneously, algorithm checks whether the i^{th} component of j^{th} service is available. Each component of service uses resources (CPU, RAM) of physical and virtual machines on which it is hosted. Resource discoverer checks if z^{th} VM has enough hardware resources to provide another instance of the i^{th} component to the user. If the amount of resources is enough, algorithm verifies that necessary channel resources are available to establish a reliable connection for components transmission to end users.

$$C_{P_n}>R_{i,j}\ , \tag{3}$$

where $R_{i,j}$ - information flow rate, which generate i^{th} component of j^{th} service. All parameters, which will be available at the moment of network status checking by Resource discoverer, will be stored in the array $\overline{A}$ that generates service queue. The enough channel bandwidth to provide component of a service will be also stored in $\overline{A}$. Then, Resource discoverer informs the Orchestrator to transferthe component to the output queue Q_2.

Network discoverer checks the status of the channels and determines an optimal path for components transmission and exchanging by using the least loaded channel. Because, cloud system receives queries of services components, whichare transmitted by different routes, we can determine the proportion of channel bandwidth occupation by each component relative to the total number of routes through this channel. Above mentioned procedure provided as following. First, we define the weight coefficient of information flow rate for the i^{th} component of j^{th} service relative to the total traffic that transmitted by l^{th} channel:

$$k_{i,j|l}=\frac{R_{i,j|l}}{\sum_{i,j}R_{i,j|l}} \tag{4}$$

Then, the proportion of unoccupied bandwidth for l^{th} channel is calculates as:

$$k_{0|l}=1-\frac{\sum_{i,j}R_{i,j|l}}{C_l} \tag{5}$$

where C_l denotes the bandwitdh of l^{th} channel.

The value the occupation part of $\Pr_{i,j|l}$ bandwidth is expressed proportionally to $k_{i,l}$ and calculated as following:

$$\Pr_{i,j|l}=k_{i,j|l}\cdot\left(1-k_{0|l}\right)\cdot 100\% \tag{6}$$

We assume that $\Pr_{i,j|l}$ meets the priorities of components in relation to others, traffic of which is transmitted by l^{th} channel. It means that the largest bandwidth will be released when current component will be successfully transferred, which in turn will make possible to serve all requests with the highest efficiency.

We also assume that the bandwidth of certain route is used ineffectively when $\min\left(k_{0|l}\mid \mathrm{P}_n\right)$ has the maximum value. Then, VDE switcher manager and Migration Manager provide up loading of the less loaded band and is bandwidth reallocation between components with higher needs.

If during the evaluation of free resources we find out that there are not enough resources for another instance of the component or the next component, i.e:

$$CPU_{available}(z)>CPU(i,j) \tag{7}$$

$$RAM_{available}(z)>RAM(i,j) \tag{8}$$

$$C_{P_n}\min\left(k_{0|l}\mid \mathrm{P}_n\right)>R_{i,j}\mid P_n\ , \tag{9}$$

then the replication of z^{th} virtual machine to another physical machine PM_m is performed. .

Information about the necessity of component migration is sent to Orchestrator and Migration Manager, which moves overloaded VM_z in collaboration with VDE switcher manager. If migration is not possible, denial of service will happen and RD starts again the process of resources analysis.

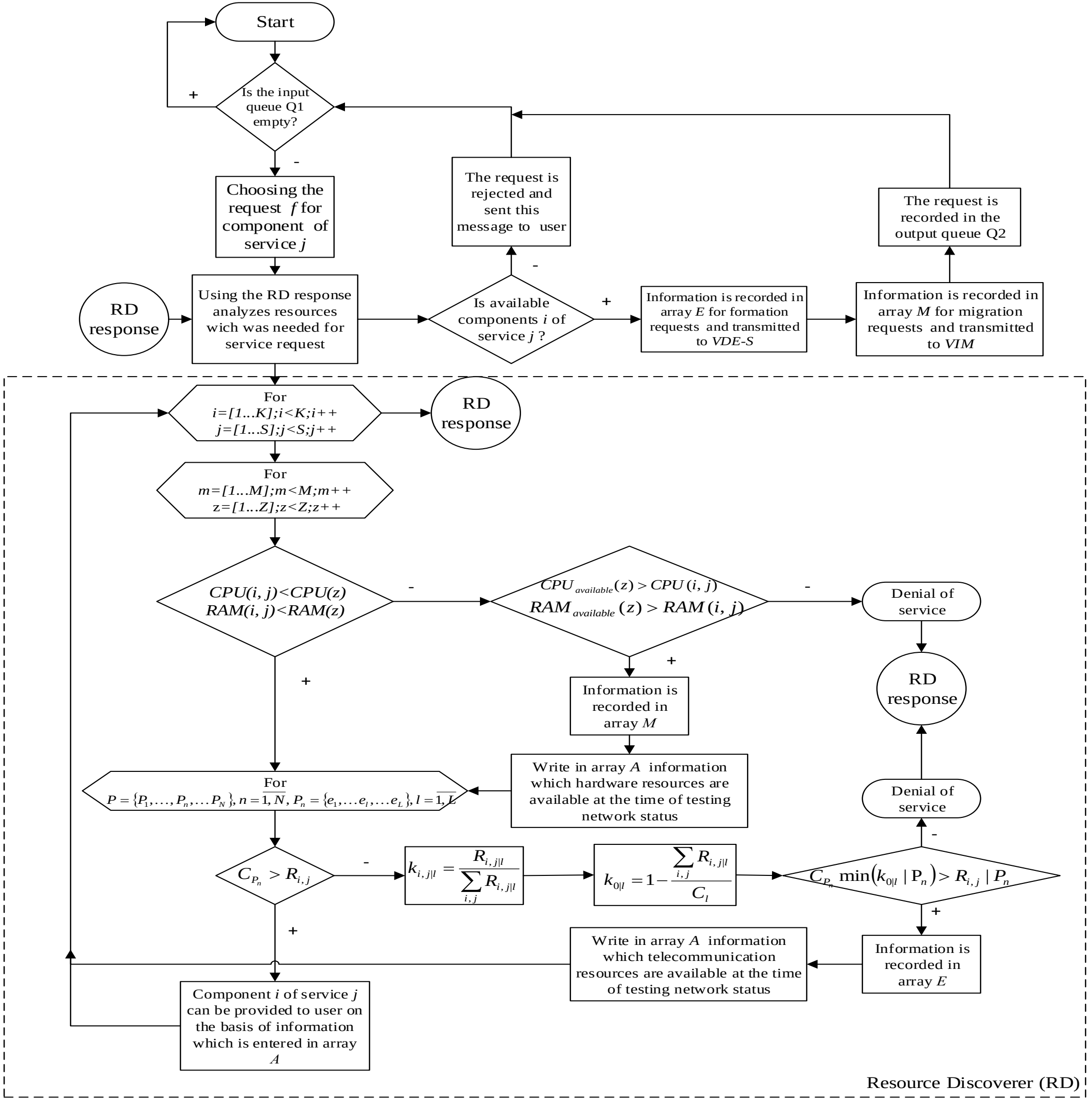

Start
Is the input queue Q1 empty?
+
-
Choosing the request f for component of service j
The request is rejected and sent this message to user
The request is recorded in the output queue Q2
RD response
Using the RD response analyzes resources wich was needed for service request
Is available components i of service j ?
+
-
Information is recorded in array E for formation requests and transmitted to VDE-S
Information is recorded in array M for migration requests and transmitted to VIM
For i=[1...K];i<K;i++ j=[1...S];j<S;j++
RD response
For m=[1...M];m<M;m++ z=[1...Z];z<Z;z++
CPU(i, j)<CPU(z) RAM(i, j)<RAM(z)
-
+
$CPU_{available}(z) > CPU(i, j)$ $RAM_{available}(z) > RAM(i, j)$
-
+
Denial of service
RD response
Information is recorded in array M
Write in array A information which hardware resources are available at the time of testing network status
For $P = \{P_1,\ldots,P_n,\ldots P_N\}, n=\overline{1,N}, P_n = \{e_1,\ldots e_l,\ldots e_L\}, l=\overline{1,L}$
Denial of service
$C_{P_n} > R_{i,j}$
-
+
$k_{i,j|l} = \frac{R_{i,j|l}}{\sum_{i,j} R_{i,j|l}}$
$k_{0|l} = 1 - \frac{\sum_{i,j} R_{i,j|l}}{C_l}$
$C_{P_n} \min(k_{0|l} \mid P_n) > R_{i,j} \mid P_n$
-
+
Write in array A information which telecommunication resources are available at the time of testing network status
Information is recorded in array E
Component i of service j can be provided to user on the basis of information which is entered in array A
Resource Discoverer (RD)

Figure 2. The algorithm to estimate the avaliable resources of cloud system

Maximum values of free virtual and channel resources will be transferred to the Orchestrator, which will provide the migration of applications to the less loaded PM if necessary.

IV. Simulation and Performance Analysis

We develop the simulation model of cloud infrastructure to analyse the efficiency of proposed approaches. Conventional simulation models operate on the principle of discrete events that does not reflect peculiarities of processes in the real network. In difference to existing models, our model is based on the deployment of virtual machines on the physical servers and service provision. The UML (Unified Modeling Language) diagram of developed model is shown in Fig. 3.

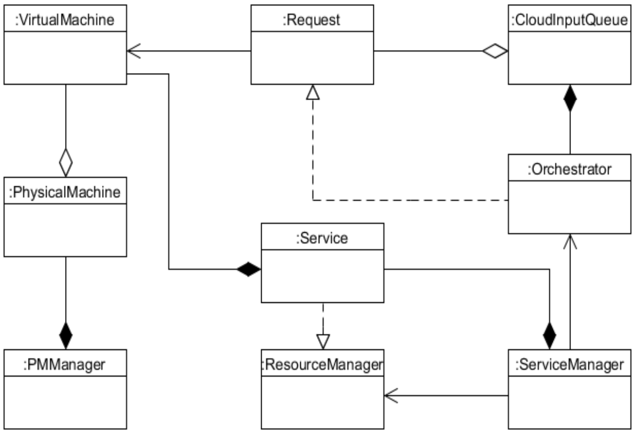


Figure 3. The block diagram of simulation model based on Unified Modeling Language

The conceptual model of service provision to the user based on proposed management system and balancing method for the cloud infrastructure is described in Fig. 4.

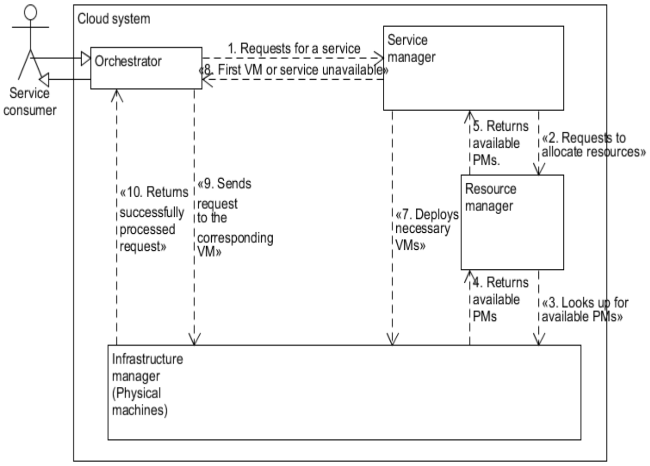
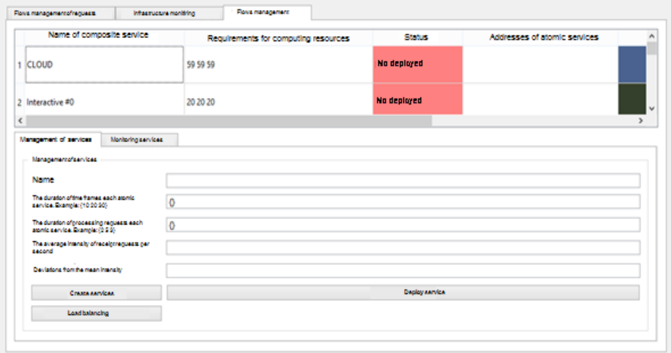

Cloud system
Service consumer
Orchestrator
1. Requests for a service
«8. First VM or service unavailable»
Service manager
5. Returns available PMs.
«2. Requests to allocate resources»
Resource manager
«10. Returns successfully processed request»
«9. Sends request to the corresponding VM»
«7. Deploys necessary VMs»
4. Returns available PMs
«3. Looks up for available PMs»
Infrastructure manager (Physical machines)

Figure 4. The conceptual model of service provision based on the cloud infrastructure

Based on the proposed simulation model we develop a software tool by using the Qt5.4 programming environment. Our tool allows to create an infrastructure with any configuration and parameters. In our case, we use following parameters: number of physical servers, hardware resources allocated to deploy each component, number of services and their type. All elements of infrastructure can be configured independently, but initially have the same configuration. The connection between them is formed by random filling of the adjacency matrix. The dialog window for network configuration and simulation process control of developed tool is shown in Fig. 5.



	Name of composite service	Requirements for computing resources	Status	Addresses of atomic services
1	CLOUD	59 59 59	No deployed	
2	Interactive #0	20 20 20	No deployed	

Name

The duration oftime frames each atomic service. Example: (10 20 30) 0

The duration ofprocessing requests each atomic service. Example: (3 5 5) 0

The average intensity ofreceiptrequests per second

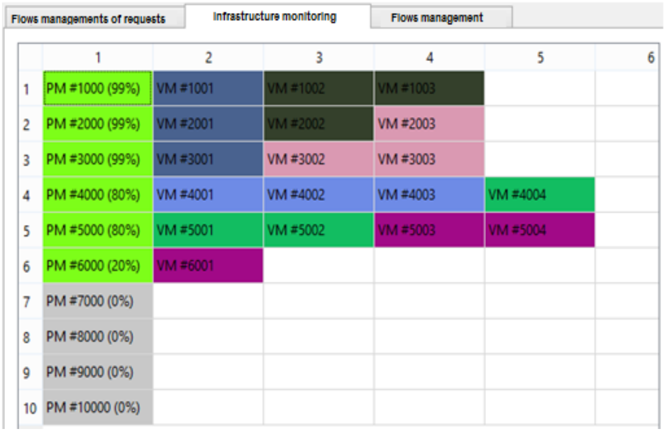
Deviations from the mean intensity

Figure 5. Dialog window for network configuration

We create a set of services, which are deployed based on designed infrastructure. The system infrastructure is represented as a matrix: rows define the number of physical servers, and columns define virtual machines, which are deployed on each server. Service parameters for our simulation are presented in Table 1. Designed infrastructure and VMs allocation is shown in Fig. 6.

TABLE I. PARAMETERS OF SERVICES FOR SIMULATION

Name of composite service	Color	Requirements for computing resources	Addresses of atomic services
1	Blue	{59, 59, 59}	Instance 1 {1001, 2001, 3001}
2	Black	{20, 20, 20}	Instance 2 {1002, 1003, 2002}
3	Purple	{20, 20, 20}	Instance 3 {2003, 3002, 3003}
4	Azure	{20, 20, 20}	Instance 4 {4001, 4002, 4003}
5	Green	{20, 20, 20}	Instance 5 {4004, 5001, 5002}
6	Lilac	{20, 20, 20}	Instance 6 {5003, 5004, 6001}



	1	2	3	4	5	6
1	PM #1000 (99%)	VM #1001	VM #1002	VM #1003		
2	PM #2000 (99%)	VM #2001	VM #2002	VM #2003		
3	PM #3000 (99%)	VM #3001	VM #3002	VM #3003		
4	PM #4000 (80%)	VM #4001	VM #4002	VM #4003	VM #4004	
5	PM #5000 (80%)	VM #5001	VM #5002	VM #5003	VM #5004	
6	PM #6000 (20%)	VM #6001				
7	PM #7000 (0%)					
8	PM #8000 (0%)					
9	PM #9000 (0%)					
10	PM #10000 (0%)					

Figure 6. The infrastructure of cloud system

To generate traffic we are using lognormal distribution for interval between requests and exponential traffic intensity distribution. This combination allows to reflect properties of the real traffic in the cloud network.

All services and traffic generators are active simultaneously. The duration of virtual machines existence is not limited. Simulation is conducted in three stages.

In the first stage, an analysis of the network functioning is conducted while operate in accordance with the existing architecture and principles of cloud network. At this stage the resources utilization is analyzed and compared among existing physical servers. In addition, end to end delays of packets transmissionandnumbers of processed/unprocessed requests are calculated. Special attention is given to service with the largest number of uprocessed requests.

In the second stage a monitoring of cloud system infrastructure is provided and durations of service requests are determined. Using the integrated architecture enables the control of available hardware and software resources.

In the third stage the load balancing algorithm is started for services with the largest duration of service requests processing. Coordinated operation between load balancing algorithms and integrated management infrastructure promises to reduce the duration of service requests processing and delay of packet transmission. This allows to increase network productivity and reliability as well as to decrease the server load.

We simulate two scenarios: conventional cloud system and cloud system with our implemented solutions. Simulation results of service requests duration for different types of service are shown in Fig. 7. Switching from conventional system to our proposed system decreases the duration of service requests and enables resources control for each server.

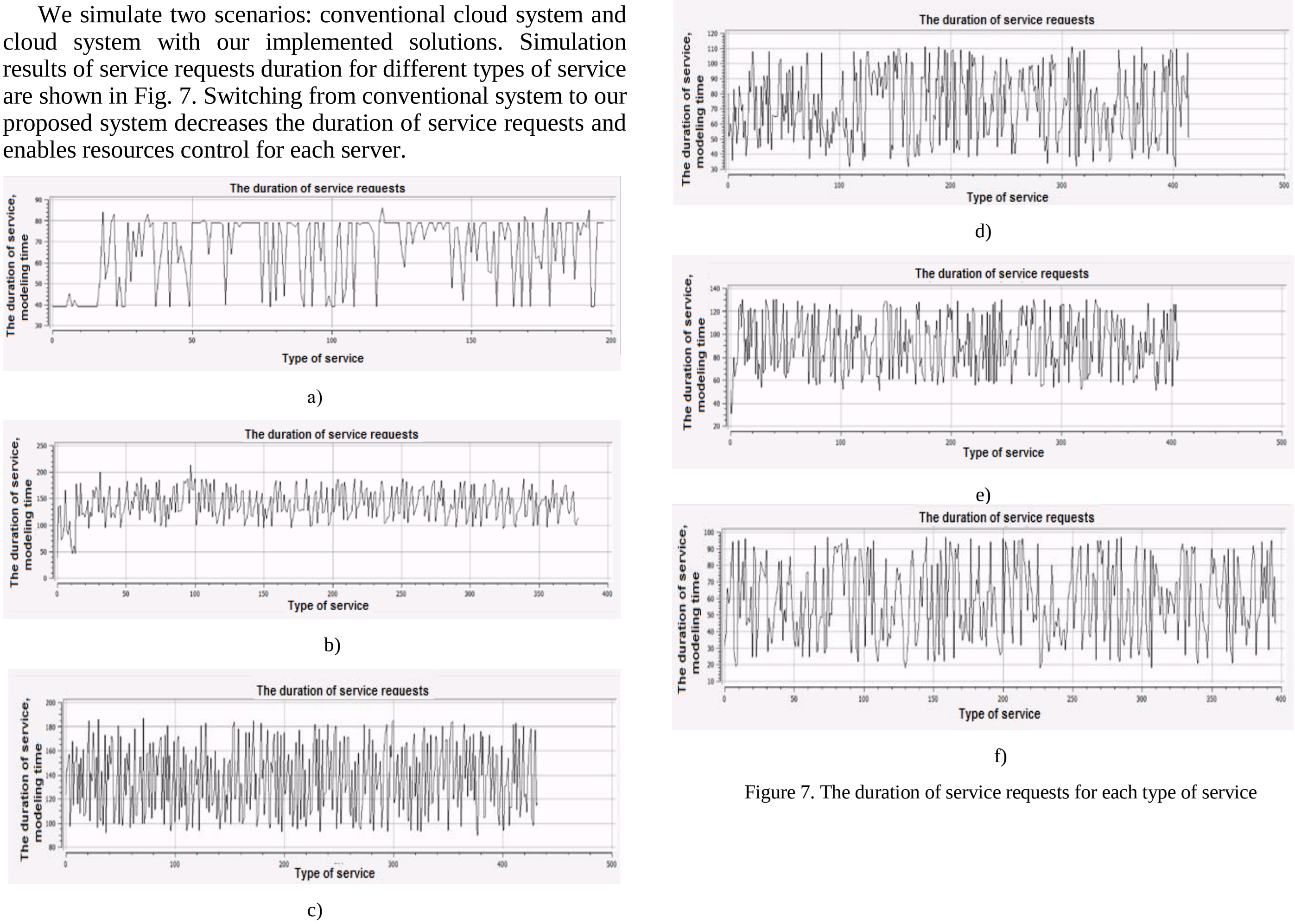
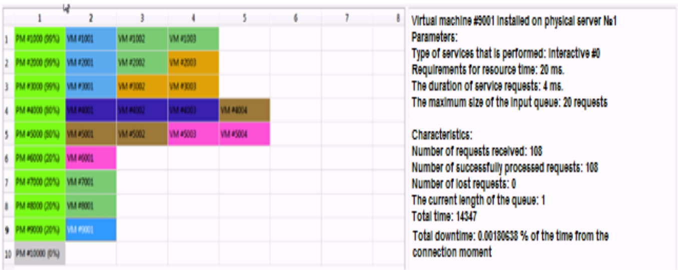


Figure 7. The duration of service requests for each type of service

TABLE II. PARAMETERS OF SERVICES BEFORE AND AFTER TURNING LOAD BALANSING ALGORITHM

Name of compo-site service	Addresses of atomic services	The duration of service requests	The total number of requests received to be processed into the system	Number of successfully processed requests	The duration of service requests after migration	The total number of requests received to be processed into the system after migration	Number of successfully processed requests after migration
1	Instance 1 {1001, 2001, 3001}	70 mod.sec.	212	212	70 mod.sec	407	407
2	Instance 2 {1002, 1003, 2002}	150 mod.sec.	394	391	50 mod.sec	739	739
3	Instance 3 {2003, 3002, 3003}	130 mod.sec.	367	365	130 mod.sec	711	706
4	Instance 4 {4001, 4002, 4003}	80 mod.sec.	405	404	80 mod.sec	695	692
5	Instance 5 {4004, 5001, 5002}	90 mod.sec.	374	372	90 mod.sec	732	728
6	Instance 6 {5003, 5004, 6001}	60 mod.sec.	332	332	60 mod.sec	740	740

Results in Fig. 7 show that majority of requests are assigned to the second service with average processing duration of 150 seconds in modeling time. Note than one second in modeling time is equal to the one microsecond in the real system. Accordingly, there are not enough hardware and software resources to provide additional component of the second service, because buffers of virtual machines are overloaded by requests. In this case, Orchestrator takes the decision to migrate service components of to another physical server. Fig. 8 shows the network infrastructure after migration and load balancing.



	1	2	3	4	5	6	7	8
1	PM #1000 (99%)	VM #1001	VM #1002	VM #1003				
2	PM #2000 (99%)	VM #2001	VM #2002	VM #2003				
3	PM #3000 (99%)	VM #3001	VM #3002	VM #3003				
4	PM #4000 (80%)	VM #4001	VM #4002	VM #4003	VM #4004			
5	PM #5000 (80%)	VM #5001	VM #5002	VM #5003	VM #5004			
6	PM #6000 (20%)	VM #6001						
7	PM #7000 (20%)	VM #7001						
8	PM #8000 (20%)	VM #8001						
9	PM #9000 (20%)	VM #9001						
10	PM #10000 (0%)							

Virtual machine #9001 installed on physical server №1
Parameters:
Type of services that is performed: Interactive #0
Requirements for resource time: 20 ms.
The duration of service requests: 4 ms.
The maximum size of the input queue: 20 requests

Characteristics:
Number of requests received: 108
Number of successfully processed requests: 108
Number of lost requests: 0
The current length of the queue: 1
Total time: 14347
Total downtime: 0.00180638 % of the time from the connection moment

Figure 8. The network infrastructure of after migration and load balancing

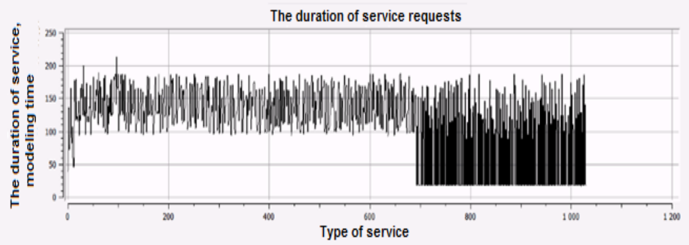


Figure 9. The duration of requests maintenance for the second type of service by using proposed solutions

By analyzing obtained results we observe that load balancing by implementing integrated management architecture based on NVF technology allows to reduce the duration of service requests processing approximately by 3 times. Thanks to the integrated estimation of bandwidth and software-hardware resources, proposed solutions allow to reduce the delay of the service provision to end users and decrease load of most loaded servers. This is especially important in a situation where large number of services is available and large amount of data is transferred in the network.

Quality of service monitoring results shows that after migration of service components, average duration of request processing decreases almost three times, from 150 to 55 microseconds (Fig.9).

V. Conclusion

The paper proposes a new approach to solve the problem of load balancing by means of integrated management architecture based on NVF functions. This analysis is based on the maximum integral resources index of physical machine. Maximum values of available virtual and physical resources are transferred to Orchestrator, which provides the migration of service components to less loaded servers if necessary. Performance analysis of the proposed approach shows that load balancing by implementing integrated management architecture based on NVF technology allows to reduce the duration of service requests by 3 times. Proposed integrated estimation of bandwidth, software and hardware resources reduces the time delay of the service provision to end users and unloads the most loaded server. Simulation results show that migration of service components decrease the average duration of requests processing from 150 to 55 microseconds.

References

[1] Mykola Beshley, SOA quality management subsystem on the basis of load balancing method using fuzzy sets // Mykola Beshley, Mykhailo Klymash, Bohdan Strykhalyuk, Olga Shpur, Bugil Bohdan, Igor Kagalo // International Journal of Computer Science and Software Engineering (IJCSSE). – 2015 - Volume 4 - Issue 1 – P.10-21

[2] Klymash M. The model of provide services on the basis of the adaptation logical structure in cloud-system / Klymash M.M., Strykhalyuk B.M., Shpur O. M., Beshley M. I./ Scientific proceedings of Ukrainian research institute of communications. – 2014. – №5(33) c. 27-36

[3] Strykhalyuk B., Service provisioning by using a structure stability algorithm in a virtualized data center based on cloud technology // Bogdan Strykhalyuk, Olga Shpur, Andriy Masiuk // Computational Problems of Electrical Engineering. - 2014.- vol. 4. - №1. - P.83-88

[4] Strykhalyuk B. Virtualization mobile communication systems based on technology NFV and models of cloud-services // Strykhalyuk B.M., Shpur O.M., Masyuk A.R.// Modern problems of telecommunications and training in the field of telecommunications: materials of the conference (30 Oct. – 02 Nov 2014 p. Lviv), 2014p. - P.21-24,

[5] Soares J. Cloud4NFV: a platform for virtual network functions / J. Soares, M. Dias, J. Carapinha, B. Parreira, S. Sargento // Proceedings of the 3rd International conference on cloud networking.- 2014, - P.288-293

[6] Fel Ma Distributed load balancing allocation of virtual machine in cloud data center / Fel Ma, Feng Liu та Zhen Liu // Proceedings of the 3rd International conference on software engineering and service science (ICSESS), 2012. - P.20-23.

[7] Yi Zhao Adaptive distributed load balancing algorithm based on live migration of virtual machines in cloud / Yi Zhao, Wenlong Huang // Fifth International joint conference on INC, IMS and IDC, 2009. - P.170-175

[8] Clark C. Live migration of virtual machines / C.Clark, K.Fraser, S Hand, J Hansen, and E Jul // Proceedings of the 2nd ACM/USENIX Symposium on Networked Systems Design and Implementation (NSDI). 2014 - P. 273-286

AUTHORS PROFILE

Olga Shpur is now PhD student at Telecommunications department, Lviv Polytechnic National University, and received his M.S. degree in information communication networks from Lviv Polytechnic National University in 2013. Here research interests: include design features and operation of networks based on service-oriented architecture, mesh- and cloud-technology.

Mykhailo Klymash is now the Chief of Telecommunication Department, Lviv Polytechnic National University, Ukraine. He received his PhD in optical data transmission, location and processing systems from Bonch-Bruevich Saint-Petersburg State University of Telecommunications, Saint Petersburg, Russia, in 1994 Honored member of Ukrainian Communications Academy . The topics of his current interest of research include distributed networks, cloud computing, convergent mobile networks, big data, software defined networks and 5G heterogeneous networks.

Marian Selyuchenko is now PhD student at Telecommunications department, Lviv Polytechnic National University, and received his M.S. degree in information communication networks from Lviv Polytechnic National University in 2013. His research interests include 5G wireless communication networks, cloud computing, SDN, design aspects of network-assisted device-to-device communications for opportunistic cellular spectrum re-utilization.

Bohdan Stryhalyuk PhD, Telecommunications department, Lviv Polytechnic National University. He received his PhD in telecommunication systems and nets from Lviv Polytechnic National University in 2009. Scientific interests: theoretical foundations of telecommunications networks analysis and synthesis on the basis of Cloud technologies, efficiency increasing for multiservice traffic management, efficiency increasing for wireless communications.

Orest Lavriv PhD, is now Senior Lecturer at Telecommunications department, Lviv Polytechnic National University. He received his PhD in telecommunication systems and networkss from Lviv Polytechnic National University in 2012. Scientific interests: theoretical foundations of telecommunications networks analysis and synthesis on the basis of Cloud technologies, efficiency increasing for multiservice traffic management, efficiency increasing for wireless communications

Service-Oriented Architecture for Secure Service Discovery and Selection in Specialized Mobile Networks

M. Adel Serhani[1], Yasser Gadallah[2], Ezedin Barka[1]
[1] College of Information Technology, UAE University, Al-Ain, UAE
[2] The American University in Cairo, Egypt

***Abstract* – Special operations such as emergency response as well as military missions are usually characterized by the limited resources available to handle generally large-scale operations. Precise resource discovery and allocation thus becomes an important factor for the success of such operations. This task has been recognized as a challenging research issue. This is due to the dynamic nature of the emergency response elements e.g., personnel and equipment. One of the important requirements of these operations is achieving the security of the communications involved in the resource discovery and allocation tasks. Security ensures the confidentiality, integrity, and availability of the communicated information. Therefore, solutions that are intended for selecting best matching service(s) should not only rely on the functional properties of the service but also on level of security under which this service is provided. In this study, we propose a secure multicast service discovery architecture that is based on a mobile ad hoc network (MANET) of operation participants. The main objective is to locate, select, reserve and assign certain resources to parties that are in need of these resources. The involved communications are designed to be secure multicast-based, utilizing features of the Role-Based Access Control (RBAC) Model. We describe the details of the proposed communication protocol. We then qualitatively compare our architecture to other alternative MANET-based service discovery architectures. The comparison highlights the merits of the proposed architecture. Finally, we conduct and present the results of a set of experiments to evaluate key features of our proposed architecture.**

Key words: Service-Oriented Architecture, Secure Service Discovery, MANET, Special Operations, Access Control, Service Selection.

I. Introduction

Mobile ad hoc networks (MANETs) can play a significant role in facilitating the allocation of resources to the spots of need while conducting special operations such as search and rescue, forest fire fighting and military combat missions. In these operations, participants and equipment can be thought of as resources, each with specific attributes and capabilities. For example, in disaster relief operations we may have participants of different types e.g., medical personnel, ambulance workers and heavy equipment operators. These participants provide services to individuals or parties in need such as trapped or injured persons. Since MANETs can be assembled and operated hastily and without the need for any existing network infrastructure, they present a good candidate communications solution to use in such situations.

Different service discovery architectures have been proposed. These approaches rely mainly on the service functional attributes (e.g., medical personnel) for service selection. However, non-functional properties, e.g., security levels, of selected services are crucial in contexts such as that of military operations because of the mobility of involved participants and the confidentiality of exchanged information.

Let us consider the following scenario, which deals with an operations field where we have several groups engaged in one or more operation. A group could be responsible for a certain geographical area of the operations theatre or it could be responsible for a specific task of the mission. Each group has a commander who is responsible for overseeing the progress of the task that is assigned to his/her group. This responsibility includes locating and assigning resources to operation participants at their request. Considering a specific group, we can classify group members into different types of job functions/specialties (roles).

The scenario can therefore be described as follows:

1. A party in need of a service issues a request to the commander of the group.
2. The commander decides on the type of needed help.
3. It consequently dispatches a multicast message to all suitable units (service providers).
4. The providers, which could satisfy the request, respond back to the commander with their service attributes.
5. The commander evaluates the different responses and selects the one that best satisfies the request.
6. In the event that no suitable provider is available to service the request, the commander communicates with commanders of other groups to seek help from their available resources. However, the group-to-group communication is beyond the scope of this paper. We only focus on intra-group communications within this study.
7. Once the right service provider is found, it gets requested to move to address the request.

Based on this scenario, and depending on the requested help, the commander can confidentially find and allocate the requested help on the basis of best available matching attributes to what has been requested as well as other additional information such as the provider's proximity to the requester. Figure 1 gives an illustration of the scenario.

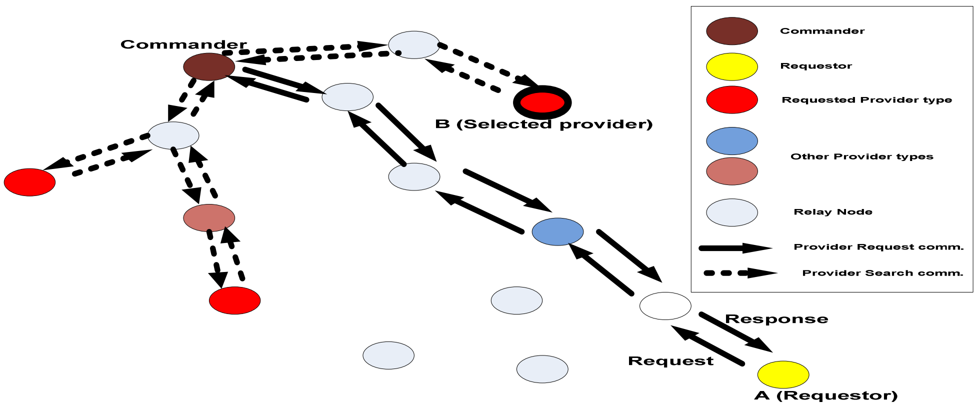


Figure 1: Targeted Scenario of Operation

This study addresses the following system elements:

- A comprehensive service discovery, selection and reservation system architecture that we design for use in special operations. This includes the service provider discovery and management system.
- A role-based secure communication scheme for connecting the network elements of the architecture.
- A customized multicast protocol.
- The security structure of system interactions.

Consequently, we determine the way the selection of the required service providers is done and how the calculations in this regard are made. We also determine the security scheme by which the information exchanges are governed. For service selection, we build an algorithm that evaluates different candidate services using a utility function calculated based on a set of weighted non-functional attributes such as service availability, proximity and delivery time.

The rest of this paper is organized as follows. Section II summarizes the related work on service discovery in special operations. Section III discusses the security issues in MANET and describes how our approach addresses these issues. Section IV illustrates the network infrastructure design including the communication infrastructure, protocol base operations, and packet structure. Section V details the service discovery and reservation architecture. Section VI describes the experimental scenarios, which we use to evaluate the effectiveness of our technique using a set of specific metrics. In addition, it provides a comparative study of several service discovery approaches based on a set of criteria that we defined. Finally, Section VII concludes the paper and suggests future research directions.

II. Related Work

Several studies have dealt with the use of service discovery in special and emergency operations. These works can be classified into two categories: (1) research architectures and approaches for non-secure service discovery and (2) research architectures and approaches for secure service discovery. For non-secure service discovery, several techniques have been proposed. These techniques differ in many aspects including the service discovery methodology and the underlying architecture.

The studies in [1], [3], [4], [7] and [8] propose middleware, framework or general infrastructure to handle emergency response operations. The studies deal with data flow and management issues but did not address security issues within the system. In [2], a system called EmerLoc was proposed for location-aware medical applications that use a wireless body area network (WBAN) and an A* algorithm for service routing and navigation. Some security considerations have been implemented and were based on the Public Key Infrastructure (PKI). In [5], the study introduces an emergency management architecture that relies on an agent-based resource discovery in which agents cooperate to monitor and respond to environmental emergency situations. In [6], the authors propose a long-distance multimedia wireless mesh network for collaborative disaster emergency responses to enable communications under the constraints of limited network bandwidths and high network latencies. In [11], a multicast-based service discovery protocol for MANET is proposed. The protocol is based on the ODMRP multicast algorithm [12]. Any node that needs a service will have to send the request to the multicast group address of the server that provides this service. In [13], the authors link service availability to specific areas in which they can be accessed. Service discovery is therefore done on the basis of geographical proximities to the available services of each region. In [14], an SLP-based service discovery protocol for MANET is proposed. This technique enables the user to discover appropriate service providers and also keeps the user informed of the existence and properties of alternative providers. None of the previous works addressed security issues in service discovery environments.

As far as secure service discovery approaches are concerned, many studies have been conducted with emphasis on aspects such as the security properties, security implementation and enforcement and the underling security architecture. In [15], the authors focus on access control for sensor nodes in Wireless Sensor Networks (WSNs). They address the issue of expanding node conciliation in sensor nodes through broadcast and propose a sensor node security approach using T-RBAC. They claim that even if a network node is compromised, it can increase the whole network availability as it increases a number of available nodes. They have presented a design and implementation. Their security analysis and comparison to other approaches indicated the feasibility of their approach. In [16], the issues of privacy and security in MANET are addressed. A combination of an access control mechanism and a privacy policy is used to ensure that the privacy and security of personal data is protected accordingly. In this paper, the authors defined MANET as a temporary network structure, which is set up by a group of existing rescue personnel such as policemen, firemen, an army or paramedics during emergency services. Nodes in the groups are initially configured before the actual network is established. They enhanced access control, through the utilization of Group-Based Access Control (GBAC), by incorporating the privacy policies together with the access policy. The goal was to achieve privacy with regards to sensitive data such as PII or PHI. In [17], the focus is on the security issues in the semi-infrastructured and ad hoc network, which is a wireless MANET sub-network connected to a structured backbone network (LAN). These types of networks are gaining popularity but their security is considered as a major obstacle in their advances due to their uncontrolled medium access, dynamically changing topology and mobility of the hosts.

The studies in [18] and [19] focus on devising XML-based security-aware architectures and infrastructures. This type of architecture is relatively heavy for use in limited bandwidth wireless environments where simple handheld devices are usually used for communications. In [20], the authors focus mainly on providing a scalable solution for securing the service discovery mechanisms based on a new concept of Attribute Based Encryption, which is derived from the Identity Based Encryption schemes. In [21], the authors propose a service discovery protocol with security features, named a Secure Pervasive Discovery Protocol (SPDP). It is based on an anarchy trust model, which provides the location of trusted services, as well as a protection of confidential information, secure communications or access control. The authors in [22] present their implementation of a system that provides a communication and security infrastructure to enable clients to access and utilize services in heterogeneous networks. In [23], the author proposes a trust-aware routing protocol called TARP that focuses more on the trusted availability and quality of trust as important factors in securing Ad Hoc networks. In [24], the authors propose a new service discovery model called Splendor that emphasizes security and supports privacy. Location awareness is integrated for location-dependent service discovery and is used to lower service discovery network infrastructure requirements. In [25], the authors present a deep review and analysis of service discovery protocols in multi-hop mobile ad hoc networks including a suitability assessment of these protocols based on architecture, mobility and network size. In [26], a trust-based dynamic secure service discovery model has been proposed to measure the trust value of a service requestor based on SOA. In [27], the study presents a cross-layer service discovery solution tailored for use in MANETs. The solution integrates Web services Dynamic Discover (WS-Discovery) and an interoperability gateway to enable service discovery across network boundaries thus connecting mobile solution systems and deployed tactical systems. In [28], the paper proposes a proactive service discovery approach for pervasive environments relying on a formal context model called Hyperspace Analogue to Context, which effectively captures the dynamics of the context and the relationship between services and context. In [29], the authors propose ubiquitous bindings for Service Component Architecture applications that modularize the discovery elements thus promoting the sharing of the common discovery functionalities and simplifying the integration of discovery protocols.

In [30], the authors describe a model for dynamic monitoring in ad hoc networks, which serves as the trust-base. The model requires some trusted nodes to play the role of the authentication server and the policy rules enforcement server when the previous servers leave the network. The paper in [31] proposes a secure access architecture that integrates an access control model to ensure that data travel among groups of rescuers is secure and the data integrity is preserved. An access control model is used to specify access policies. Cryptographic protocols, has functions and digital signatures are used for confidentiality, integrity and authentication of participating members.

Our study offered an architecture that aims at managing emergency response operations via the use of secure role-based service discovery over multicast. This enables hierarchical access to information among operation participants. The hierarchy is constructed on the basis on the operation participants' rank. This is done while we address the issue of non-existent or hard-to-access network infrastructure via the use of MANET. We also ensure the efficient use of the available bandwidth through the use of multicast as the underlying communication technique. To the best of our knowledge, we are the first to provide such a comprehensive architecture to the secure special operations problem.

III. SECURITY THREATS DISCUSSION

The nature of MANET networks, which are infrastructureless and consist of different types of mobile devices, and the lack of centralized administration, makes this ubiquities environment very vulnerable to security attacks. In this section, we discuss some of the expected security threats to MANET networks, in general, and to our service discovery scheme in particular. We define the security requirements for system protection. Finally, we introduce some techniques to mitigate the risk posed by these threats and attacks.

Security threats against MANET exist at different layers of the TCP/IP protocol stack. They range from eavesdropping, to replication, and modification of data exchanged among nodes on the MANET network. This is due to the vulnerable nature of MANET, which can be described as follows:

- Dynamic topology: Due to the fact that each node can join and leave the network independently, this introduces the possibility for malicious nodes that can harm the network.
- Lack of clear line of defense: MANET has no clear lines of defense available, which makes it possible to attack the network from any direction.
- Wireless links: Due the wireless interconnection interfaces in MANET, attacks against links can be very effective.
- Ubiquitous resources such as different device types "e.g., laptops, desktops, and mobile phones", which require different connectivity and have different storage capacities and different processing capabilities. This encourages more sophisticated attacks.

Attacks against MANET can take the form of passive and/or active attacks. While passive attacks do not disrupt the operation of the network as they only tap on the lines, listen and gather information, active attacks, on the other hand, are more disruptive and can render the network dysfunctional.

Active attacks include, but not limited to, the following:

- Flooding Attacks, such as the HELLO flood attack where the attacker node floods the network with a high quality route with a powerful transmitter.
- Dropping attacks: which force compromised nodes to drop all packets that are not destined for them, which leads to the denial of service.
- Modification attacks: these attacks (also known as sinkhole attacks) can modify routing information in packets, which can disrupt the entire network.
- Fabrication attacks: in this type of attacks, adversaries can inject fake packets into the network or send fake responses to legitimate requests.
- Network Layer attacks: examples of such attacks are the reply attacks, blackhole attacks, sinkhole attacks, and Sybil attacks.

A. Security requirements of the proposed architecture

The key architectural requirements in order to secure service discovery in MANET are as follows:

- Confidentiality: This requirement ensures service discovery data secrecy.
- Integrity: this requirement protects against any unauthorized alteration of service discovery data.
- Availability: which makes sure that the system resources are available when needed.
- Authentication: especially in such an open and dynamic environment. This requirement ensures the authenticity of the communicating entities involved in service discovery.
- Non-repudiation: this resolves any disputes that result from one entity denying doing the action.

- Resilience to attacks: this is critical because it ensure continuity of service discovery operations in cases when some the key infrastructures are down or compromised.

B. Risk Mitigation

There are many approaches and techniques discussed in the literature to address the security attacks on MANET. However, in this paper in order to achieve security and privacy, we focus on access control policies to control the access to system resources. For this purpose, we utilize the feature of the public key infrastructure "public/private keys and public key certificates" to enforce these access control policies as well as to address the issues of confidentiality, integrity, authentication, and non-repudiation.

The proposed solution therefore consists of the following elements:

- Access control: to control access to system resources, we utilize the features of the well-known Role-Based Access Control (RBAC), which defines all the job functions on the network as roles. It then assigns some permissions/access to these job functions to accomplish their task. Finally, it assigns users to roles so that they can gain the permissions assigned to their respective roles.
- In our approach, a global access policy is specified by network owners and can be enforced using a designated role in RBAC (usually the group leader) to serve as the global access policy management server (GPMS). Furthermore, due to the mobility nature of MANET, an agent node is also designated to assume the role of the GPMS in case that role leaves the network. The processes and the functional steps of granting access to the multicast group to the data are elaborated further in subsequent sections of this paper.
- PKI and Certificates: we utilize PKI (X.509), which already exists in most operating systems today e.g., Windows built-in PKI, for confidentiality, authentication, integrity and digital signature for non-repudiations. We also establish public directories, i.e., LDAP; to store all public keys, public key certificates and public key revocation lists.

IV. Architecture Design

In this section, we introduce the architecture of the proposed system. We also provide the details of each element of this architecture with emphasis on the communication elements that serve the secure service discovery goals of the system.

A. Architecture Overview

Figure 2, describes the architecture of the proposed secure service discovery based multicast communication system. The architecture is composed of three layers, namely, the Communication Layer, the Access Control and Security Layer, and the Service Application Layer. Interfaces between layers represent the communications between components of the different layers. The scheme illustrates the details of the main components involved in the secure multicast service discovery, selection, and reservation processes. However, it does not specify the proper sequence of events within the same layer and between layers. For example, security attributes usually come before access control. So, access control is implemented jointly within both the group access protocol and the data access protocol. Likewise, service discovery results in the application layer are used by the service selection whose result is used as an input to service reservation. Each component at each layer is briefly described next and will be further discussed, along with the sequence of events, in the subsequent sections.

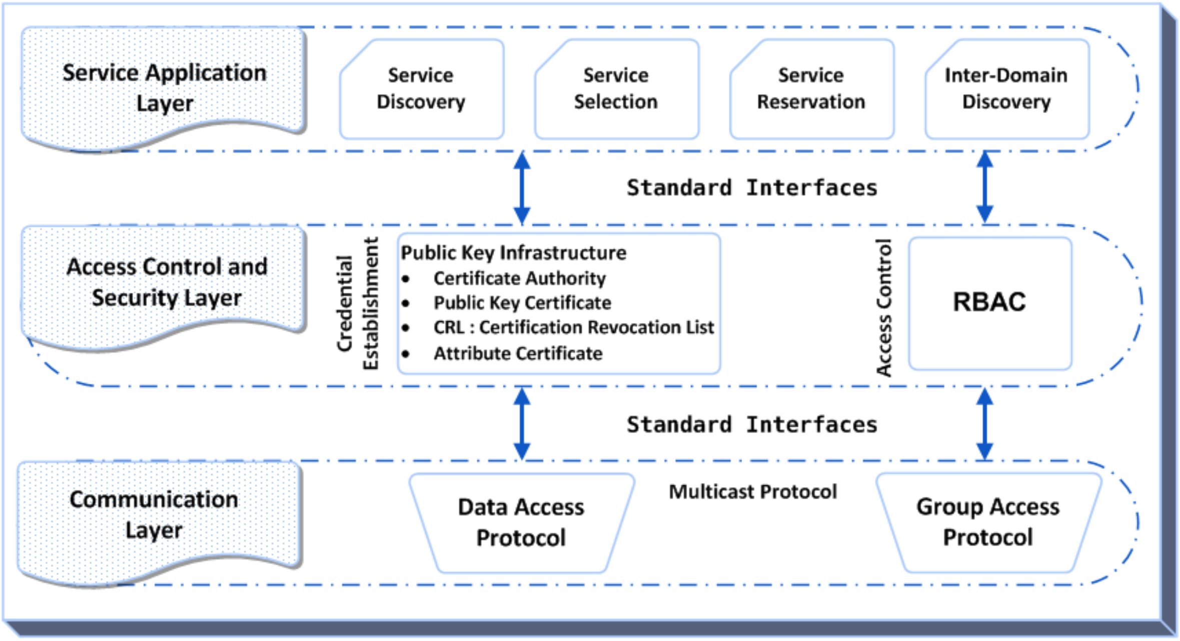


Figure 2: Overall Architecture

- ***Communication Layer***: provides the needed communication protocols used to support communication (e.g., service discovery) among involved parties in emergency operations. The used protocol is based on the multicast protocol and is comprised of two main elements, namely, the group access protocol, and the data access protocol.
- ***Access Control and Security Layer***: secures the communications provided by first layer by providing the necessary security measures which include credential establishment based on public and private keys and access control mechanism, which is implemented using public key certificates, that provide authentication of who is allowed to join the multicast group and who will subsequently be allowed or denied to view the multicast data. It also manages the role-privileges relationship.

Figure 3 depicts the concept of access control architecture, it is based on a client/server environment, where the client is the group member requesting a service and the server is the group leader accepting or rejecting the request from the group member. The group leader then acts as a client when it requests the service from the server provider on behalf of the requesting member.

The figure shows that when a group leader “a server” receives a request from a group member “a client”, it checks the client’s credentials and uses three access control components to make a decision on whether to allow or deny access to the resource. The resource is made available to the group leader after the group leader requests and gets granted access to the resource by the service provider. In the latter case, the group leader acts as a client of the service provider.

The authentication module of the access control components verifies the identity of the requestor using his public key certificate. The authorization module consults the access control policy, specified by RBAC, to make sure that role of the group member (i.e. the client) has the proper permissions to access these resources.

The cryptographic module ensures the confidentiality of the communicated information. It also provides a digital signature capability for ensuring authentication and non-repudiation.

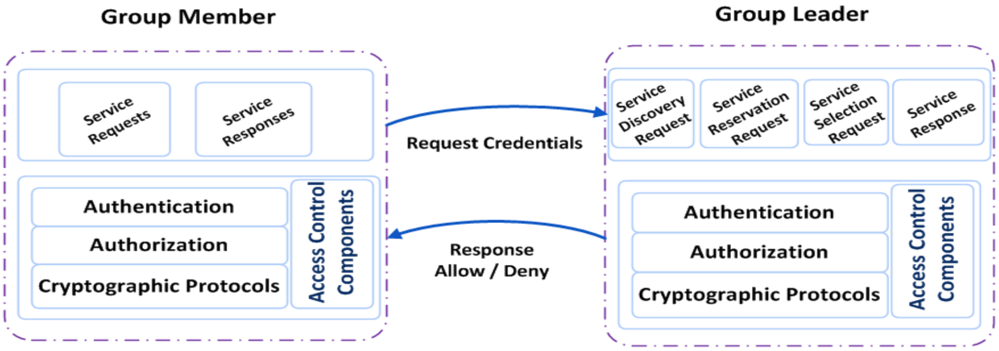


Figure 3: Access control Architecture

- ***Service Application Layer***: relies on the first two layers to provide secure service discovery, selection and reservation, as well as inter-domain discovery.

As seen in Figure 3, each node includes only the elements of the architecture that are needed by its functionality. Therefore, the architecture elements that are implemented on the group leader node are generally different from those supported on a group member.

B. Communication Layer Details

The communications protocol that is used for the different interactions for the service discovery process includes provisions for the base operation and security parameters establishment and exchange. The operation of the protocol depends on creating one multicast group for all operation participants. Any member who is part of the operation can join the multicast (MC) group. The members, however, are classified in a hierarchical manner based on their role in the operation and possibly their rank, if applicable. This role (or rank) is usually determined and programmed within the node prior to the operation. Depending on the nature of the operation at hand, several roles may be assigned to a node, each with its own credentials. That is, the user may choose to activate a specific role, depending on the nature of the current task, and provide the right credentials for the active role while communicating within the network. Based on the role, a member node may or may not be able to:

1. Grant other nodes access to the MC group.
2. Access some of the communication content being exchanged within the group.

Having one MC group for all members and granting access to information on the basis of participants' roles has many advantages over having a separate MC group for each participant's role. For instance, having one group provides the following merits:

- This arrangement saves the overhead of members trying to join several groups for which they are allowed to access the data according to their rank/role.
- Once we establish one group, which all members can join, there is no need for creating new groups as the need arises, and hence saving the delay in doing so.
- Data sharing is easier and more efficient for members who can access data that belong to different roles (e.g., high ranking personnel). This is not the case when using several MC groups, one for each role.

The core operation of the underlying multicast communication protocol is based on the study of [27]. The establishment and maintenance of the multicast group is composed of the following main tasks:

- Credential establishment
- Group formation and access
- Data access process

The multicast group formation and member access are done on the basis of node roles and the privileges that are assumed by these roles. The entire security arrangement is described in detail in the following sub sections.

1) Credential Establishment

This phase is used to establish the security capabilities that will be associated with all entities involved in the multicast communications. It includes authentication, confidentiality and data integrity. The establishment of the security capabilities includes the following:

- Establishing public key infrastructure: a centralized architecture that comprises a certificate authority that issues and distributes a public key certificate, which binds the name with the corresponding public key, and attribute certificate that can be used to enforce the implementation of RBAC. Also, directory service (i.e. LDAP) can be established to host public key certificates, certificate revocation lists (CRLs), attribute certificates (ADs), which are made available to everybody to retrieve public keys and other key information of others. Finally, this infrastructure requires the existence of certificate validation authority and authorization servers that store access control lists to enforce access control. This is usually accomplished using a customized version of the ISO reference monitor. It is worth noting that the proposed infrastructure can be housed on the operations command center, which acts as the centralized server. All MANET nodes can access this server either directly or via multi-hop communications. Alternatively, a high-ranking group member node can be used to house this infrastructure, with the possibility of having backup nodes to replace it in case of failure.

- Secret “shared” keys are also pre-established between the commander and the members of each role. These keys distributed using the public keys in order to protect the data that are exchanged communicated between the commander and the group members.
- The public key and the secret key cryptosystems are assumed to be used in the following processes:
  - Service registration and deregistration: during this process, a mutual authentication between directories and providers is ensured.
  - Service discovery: in this process, confidentiality, using secret keys or public keys, is used to ensure that only authorized clients are allowed to discover services.
  - Service delivery: here integrity, using public keys/digital signatures, is achieved to protect against malicious tampering or accidental modifications.

2) *Group formation and access*

As we discussed above, it is assumed that each node has been preprogrammed with its role and rank within the operation at hand. The group and data access will therefore be based on these preconfigured roles of the network nodes.

a) Group formation process

Group formation is handled by an authorized entity, e.g., a commanding officer or the command center. This is due to the fact that accepting members into the group will depend on the keys that these members have and are authenticated mainly by this authorized entity.

The group formation is announced with the list of initial members. This list is included in the initial group announcement message. Initial member nodes, which are included in this message, must respond to the announcing Multicast Group Leader (MCGL) and include their credentials for verification by the MCGL. The MCGL can then distribute the proper keys to the different members on the basis of their roles and hierarchy in the group. These keys will be used by the right members for both data access and further authorization to other group members to join this multicast group.

b) Group access process

The group access process deals with any subsequent node that wishes to join the multicast group. In this work we propose the well-known Role-based Access Control Model to control who can join the multicast group as well as who can have access to the encryption key that can be used to decrypt and subsequently retrieve the multicast message. Role-based Access Control (RBAC) has received considerable attention as a promising alternative to traditional discretionary and mandatory access control [28]. In RBAC, a role is a semantic construct forming the basis for the access control policy. Also, in RBAC, permissions are associated with roles. Users are made members of appropriate roles based on their responsibilities and qualifications, thus acquiring the permissions of these roles. In RBAC, users can easily be reassigned from one role to another. Roles can also be granted new permissions as the need arises, and permissions can be revoked as needed. This simplifies the security management process significantly [25]. Group access is therefore performed as follows:

- Any node that joins the group may be assigned, in addition to its functional role, the privilege to authorize other nodes that have a lower role to join the group. A node that becomes a member of the group is termed as Multicast Group Member (MCGM)
- Any node that wishes to join the group sends an encrypted Route Request (RREQ) using the address of the MCGL. This message is encrypted with the MCGL public key. The node includes its initial role (default node role) in the RREQ message. It also includes its authentication credentials for verification purposes by authorizing nodes
- The RREQ propagates according to the original protocol [27]. However, when a relay node that is not a member of the multicast group gets the RREQ, it cannot return a Route Reply (RREP) immediately. Instead, it has to keep propagating it up the tree towards the MCGL until it either reaches the MCGL itself, or a MCGM that both has a role that is superior to that of the requesting node and has been authorized by the MCGL to grant group memberships.
- When an authorized node gets the RREQ and verifies the credentials of the requesting node, it sends back a RREP authorizing that node to join the Multicast (MC) group. This RREP message includes an authorization for this node to grant other nodes access to the MC group, if its role is high enough for this. The RREP is encrypted with the public key of the requestor.
- If the requesting node does not have a suitable role, or its credentials could not be verified, the authorizing node sends back a Negative Acknowledge (NACK) message denying it access to the group.

Figure 4 illustrates the process of group access in the proposed protocol. The figure shows two cases of nodes that wanted to join the MC group, node A and node B. Node A sends its RREQ message which travels towards the MCGL until it finds another node that has a role that is superior to that of A's role. This node therefore sends node A the RREP allowing it to join the group. On the other hand, when node B sends its RREQ, it does not find a node whose role is higher in the hierarchy than its own role. The RREQ of node B therefore travels all the way until it reaches the MCGL. When the MCGL finds that a node B is not eligible to join the group, its sends it a "NACK" denying it access to the group.

In the event that a node wishes to leave the group, it sends a Leave Request (LREQ) message to the MCGL, which will in turn, ensures that this node gets removed from the list of MC group members so that it does not receive any other communications. When the MCGL, however, decides that a node should move to another group, e.g., to add extra support to that group, it will have to transfer this node's credentials to the commander of this group so that it can take care of adding it to its group.

In the following section, we describe how data access is handled. This mainly depends on the underlying security arrangement as described in subsequent sections.

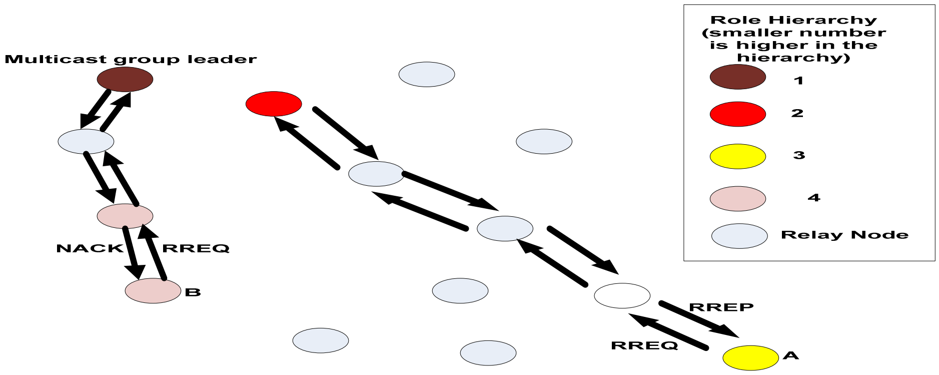


Figure 4: Illustration of group access technique

3) *Data access process*

Data access strategy determines which Multicast Group Member (MCGM) can access a specific data item that is flowing within the MC group. By data, we mean any information that gets exchanged within the MC group, other than requests to join the group.

The data access capabilities of a certain network node are determined as follows:

- When a node joins the MC group, it gets an encryption key that is based on its rank and/or role within the operation. This key helps the node decrypts the data that is supposed to access only.
- When some data packets are sent, they are encrypted in such a way that only a group of nodes with specific privileges within the MC are able to access these data.
- Any packet that gets sent has a flag that specifies the role of the node that can access the data of this packet. This feature speeds up the processing of the packet. If a node is not authorized to access this data, it simply drops the packet.

A node that tries to maliciously access the data of a packet, regardless of the role flag, will fail, as the key that it has for data decryption will not enable it to access these data.

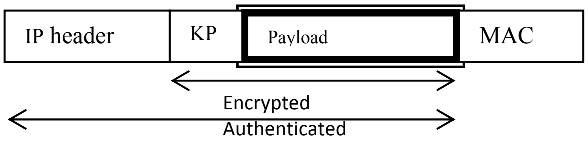
If the multicast group formation and member access are done on the basis of node roles and the privileges that are assumed by these roles, then the discovery scheme will be conducted based on the pre-formed group.

The packet structure as well as the detail of the above service operations is described in the following sub-sections.

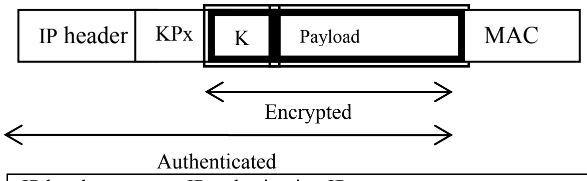
C. *Packet Structure*

Figure 5 describes the base packet structure as supported by the proposed protocol.

1. Requester ⟶ Commander



2. Commander → All Group members with the same role



IP header = source IP + destination IP
Ks = secret “shared” key used to encrypt the message “payload”.
KPc= commander’s public key
KRc= Commander’s private Key
KPx = other role members public key (x is a variable represents the selected role member)
KRx = other role members private key (x is a variable represents the selected role member)
Payload = information been exchanged between requester and commander
MAC = Message authentication code used for message integrity

Figure 5: Packet Structure

All nodes use a standard way to advertise their services. Service description is to be understood by all nodes requesting these services. Table 1 shows the main elements of a discovery packet structure.

Table 1: Discovery packet structure

Attributes	Description
S_CAT	Service Category
REQ_ID	Request ID
S_Requestor	ID of requestor
S_Provider	ID of provider
SN	Service Name
SA	Service Attributes
NFA	Non-Functional Attributes
R_LOC	Location of service requestor (x,y)
P_LOC	Location of service provider (x,y)

The protocol supports the following packet types:

- **Service Request (SREQ):** Sent by a requestor to seek a certain service. The main structure of the packet is as follows: *SREQ (S_Requestor, REQ_ID, S_CAT, SN, R_LOC, SA, NFA)*
- **Service Reply (SREP):** Sent by service providers that are available to help, in response to a service discovery request. The main structure of this packet is as follows:
  SREP (S_Provider, REQ_ID, SN, S_CAT, P_LOC, SA, NFA)
- **Service Reservation (SRESV):** Sent by the commander to the provider to inform it that its services are required. The main structure of this packet is as follows: *SRESV (S_Requestor, REQ_ID, SN, NFA)*
- **Service Provider Acknowledgement (SACK):** Sent by the service provider as a response to an SRESV packet informing that it can service the request. The main structure of this packet is as follows:
  SACK (S_Provider, REQ_ID, SN, P_LOC)
- **Service Provider not available (SNACK):** Sent by the service provider as a response to an SRESV packet to inform that it can no longer service the request. The main structure of this packet is as follows:
  SNACK (*S_Provider, REQ_ID, SN*)

- **Group Access Request (RREQ):** Sent by the service provider who wishes to join a group. The main structure of this packet is as follows: *RREQ* (*Public Key, S_Provider, S_CAT, SN, SA, P_Loc)*
- **Group Access Response (RREP):** Sent by the MCGL or the MCGM in response to a Group Access Request to grants MC group access to the requester. The main structure of this packet is as follows: *RREP* (*Authorization, Secret key of the MC Group*)
- **Group Access Denial (NACK):** sent by the MCGL or the MCGM in response to a Group Access Request to denying it access to the MC group. The main structure of this packet is as follows: *NACK* (*Denial to access MC Group*)

V. SERVICE DISCOVERY SCHEME

Network participants include commander nodes, service requestor nodes and service provider nodes. Figure 6 shows an example of the interactions that take place between the different network nodes. The service discovery scheme is conducted by executing the following operations:

- Service discovery operation: it is based on the node's role and its authorization to view the communication. This includes the service discovery within the same group as well as discovering services that belong to other groups. Also, in this case it requires communication between commanders of different groups to support service discovery. The security in this case is achieved through the data access control described above. If a requestor node is not authorized to view the data it is requesting, the request will be denied.
- Service selection operation: it is conducted by the commander node who considers some heuristics to select the appropriate service provider. In addition to service attributes, it considers the non-functional attributes of the service (e.g., service provider proximity).
- Service reservation operation: this includes service reservation within the same group as well as service reservation from other group, which is performed via the two group commanders.

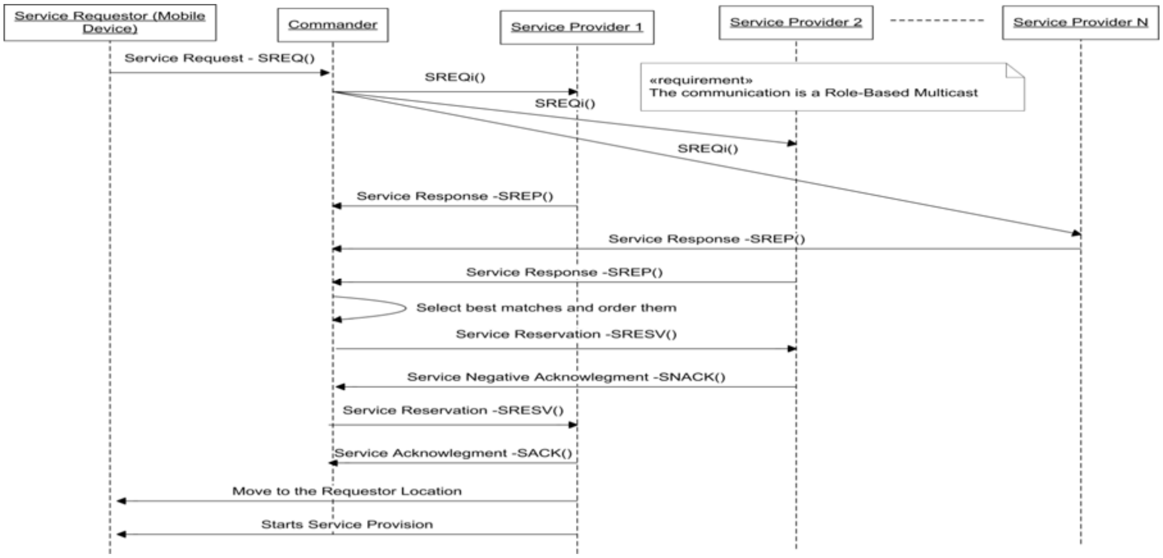

Service Requestor (Mobile Device)
Commander
Service Provider 1
Service Provider 2
Service Provider N
Service Request - SREQ()
SREQi()
SREQi()
«requirement»
The communication is a Role-Based Multicast
SREQi()
Service Response -SREP()
Service Response -SREP()
Service Response -SREP()
Select best matches and order them
Service Reservation -SRESV()
Service Negative Acknowlegment -SNACK()
Service Reservation -SRESV()
Service Acknowlegment -SACK()
Move to the Requestor Location
Starts Service Provision

Figure 6: Service Discovery and Reservation Scenario

A. *Secure Service Discovery Operation*

When a station needs a certain service, it issues an SREQ message directly to its commander. The commander re-issues an SREQ message to its multicast group including the service-required parameters as well as is non-functional attributes and it waits for a response. If any of the service providers is available to provide the service with the required parameters and the non-functional attributes, it responds back with an SREP message. Otherwise responds with a "Service NACK" message. In these types of communications, security, through the encryption of messages among service requesters and commanders, plays a big role in keeping the exchanged information between the communicating parties confidential. Also, security, through the group and data access controls, ensures that only MCGMs can view and respond to the SREQ from the commander.

B. *Service Selection Algorithm*

Service selection operation is carried out after the service discovery operation is completed. A list of potential service providers who responded to the service discovery request is retrieved and classified by the commander. These available service providers can supply the same service. Therefore, a decision should be made by the commander as to which provider to select on the basis on the best match to the requestor's requirements. One of the important criteria for service selection is considering the non-functional attributes of the service under consideration.

1) *Non-Functional Attribute Description*

There is a variety of non-functional attributes that are used in discovering services in the context of emergency operations. Non-functional properties of a service are qualitative attributes that evaluate the quality of service that a given service is providing e.g., service provider availability, and service delivery time. In our study, we consider only attributes that we see as most important in differentiating among providers who offer the same services. The following is a brief description of these properties:

- ***Provider Proximity***: the provider proximity is determined in relation to the service requestor; it is the GPS coordinates of the provider. This information is collected and stored in the commander node and updated whenever a provider changes its location.
- ***Service Availability****:* is the percentage of service responsiveness. It is calculated as the total number of responses to the commander reservation requests over the total number of reservation requests during a given period of time.
- ***Service Delivery Time (SDT)***: it is the time the provider takes to deliver the service to the intended requestor.

2) *Non-Functional Attributes Measurement*

Each of the above mentioned non-functional attributes should be measured and maintained continuously as they might change over the time. As for the "availability" attribute, the commander periodically measures the availability of each service provider. It is measured as the degree of service responsiveness to the commander requests which includes both discovery and reservation requests. For the measurement of service proximity attribute the operation is triggered on-demand whenever it is required to select a given service provider by a commander. However, for the measurement of service delivery time, the commander records the average time each provider spent in delivering a given service and updates it whenever the provider and/or the client receive an updated SDT. This may also include the effectiveness of the provider in servicing the client, the time spent in offering the services, and the quality of the provided service. Using the stored values of availability, service delivery time and proximity of all service providers allows the commander to differentiate among providers who offer the same services and select the best match.

To protect against data tampering (unauthorized modification of data while in transit) or eavesdropping, our protocol utilizes digital signatures by the sender to provide data integrity and authentication of origin, and uses the shared secret keys between the providers and the commander for canceling the data.

The following is a description of the selection algorithm and its main features. Consider the utility function F_x that is associated with a service provider, *X*:

$$F_x = \sum_{n=1}^{N} \left(W_n * \frac{(Q_x^n - \mu^n)}{\sigma^n} \right), \qquad (1)$$

where, Q_x is an atomic non-functional attribute of a service S_x, N is the number of non-functional attributes provided by a service S_x, W_n is the weight assigned for each non-functional attribute in the client request ($0<W_n< 1$, $\sum_{n=1}^{m} W_n = 1$), μ is the average of the non-functional attribute values of a candidate service and σ is the standard deviation of the non-functional attribute values of a candidate service.

The ultimate goal of the commander is to select the service provider, which maximizes the utility function F_x.

C. A Service Selection Example

We now present an illustrative example of service selection based on the utility function of (1),to select the best request matching service from the list of service candidates. We use three service categories mainly medical personnel, Rescue workers, and Ambulances. Note that the number of service candidates within each category can be different. The commander node relies on three non-functional properties, namely, availability, service delivery time, and proximity, in selecting the best match service provider. Table 2 presents, for three categories of services, the values of the non-functional parameters used to calculate the utility function of each candidate service. The resulting utility functions are used to differentiate among services in order to select the service that maximizes the value of the utility function of these competing services.

The non-functional requirements of client *X* may be expressed by a weighted vector for a service S_i as follows,.

$$NRF_i = \alpha\, P + \sigma\, SDT + \ \varphi\, AV \qquad (2)$$

where *P* represents the service proximity, *SDT* represents the Service Delivery Time, *AV* describes the service availability and α, σ and φ are the weights assigned by a client *X* to each quality property per each request. These weights are governed by the following relationship,

$$\alpha\ + \sigma\ +\ \varphi = 1 \qquad (3)$$

The non-functional requirements of the client and the weights (α, σ and φ) assigned to each property include:

- Proximity ≤ 10, $\alpha = 0.4$ (weight assigned to proximity property)
- Service Delivery Time ≥ 4 (it is defined as a scale between 0 and 5), $\sigma = 0.2$
- Availability ≥ 85%, $\varphi = 0.4$

The above weights are defined by the service consumer. They are selected based on the importance given to each of these properties. For instance a service consumer might give a high weight to the service proximity if he/she is in a very critical situation, and give a low weight to the other properties if they are not as important. In many situations the consumer's opinion might be subjective. Therefore some correctives measures to adjust these weights could be considered. An appropriate way of deciding about these weights in this situation might include, in addition to the consumer rating, applying a fundamental theory for decision making problem that could adjust and average both resulted weights.

The optimal selection of a service among candidate services is the one who maximizes the utility function value. In this sample, there are a total of nine Service candidates, each of which has different utility and non-functional attribute values.

Table 2: Available service categories and their non-functional attributes

Service Categories	Medical personnel Services			Rescue Services		Ambulance Services			
Service Candidate	New Medics	Gulf Medics	MEDEC	Life Rescue	Vital Rescue	SOS AMB	Fast AMB	AMBD	Insure AMB
Availability (%)	0.95	0.99	0.88	0.78	0.97	0.93	0.86	0.96	0.92
SDT (Hours)	4	4	5	3	5	5	4	5	5
Proximity (Mile)	5	8	10	2	11	6	13	7	3
Utility (F_x)	0.75	0.82	0.79	0.76	0.9	0.89	0.72	0.92	0.93
Selected Services	**0.82**			**0.9**		**0.93**			

The results we see from Table 2 show how our service selection scheme is able to differentiate between services based on the calculated utility function, which relies on the set of non-functional properties and their weights. For example, as shown in Table 2, among the medical personnel Services, the Gulf Medics service is selected as the best match service that maximizes the utility function (0.82). The same applies to Rescue and Ambulance Services where the Vital Rescue service and Insure AMB services were selected as best match services since they maximize the value of utility function of these two services to take the values 0.9 and 0.93, respectively.

D. Service Reservation Operation

Once the service discovery phase is completed successfully, the commander node assesses all the received responses in order to make its selection based on the response that best matches the requestor's needs as well as other selection non-functional parameters. When it makes its selection, it issues an SRESV message directly to the best matching service provider. If the provider is still available to provide the service according to the required parameters, it responds back with a "service acknowledgement" (SACK) message, which would conclude this phase. However, if this provider is no longer available by the time it gets the reservation message, it responds with a "service NACK" (SNACK) message. If the commander node gets an SNACK message, it tries the next best provider on its list and so on. Finally, if it does not find any of them available anymore, it will have to restart the service discovery process. As in the service discovery and selection, communications between the commander and the matching service provider in the services reservation process (SRESV, SACK, and SNACK) are all protected by encryption to ensure confidentiality and by digital signature to ensure authenticity and integrity.

The sequence diagram shown in Figure 5 describes an example scenario of the main interactions conducted to discover and reserve a service provider to fulfill a requestor's need. The scenario assumes that the MCGM is established and the credential infrastructure is in place. It also assumes a situation where at least one suitable provider is available to handle the request.

VI. Evaluation

To evaluate the performance of the proposed solution, we conduct a series of experiments. We developed a simulator specifically for this purpose, and we used the multicast communication scheme that we presented before. To ensure the validity of simulation results, we replicated the same experiments 5 times using the same setup and configurations for all experiments scenarios.

A. Environment Setup

We extended the DisSERV simulator we have developed in [8] and we implemented a role-based multicast communication protocol within the DisSERV simulator. For mobile nodes, the random waypoint mobility model [26] is used in the experiments.

The following are the default simulation parameters:

- Simulation area is 1000 × 1000 square meters.
- The size of the request packet is 128 bytes.
- Service provider and requestor device communication range is 250 meters.
- Network nodes are initially uniformly distributed over the simulation area.
- We set the number of groups as following: "Surgeon", "Nurse", "Ambulance", "FireWorker", "Worker", "Police", "medical", "rescue", "Supply System- Electricity".
- Processing time for each service: {50, 100, 100, 100, 100, 135, 50, 50, 100, 130, 150}
- Each service provider node moves at a speed of value that is randomly selected in the range of 1 to 6 m/s. It follows the random waypoint movement scheme.
- The service requesting nodes are stationary.
- The commander node is stationary.
- The simulation experiment time is 2400 seconds.

B. Experiment Description and Performance Metrics

To evaluate main features of our solution we have conducted a series of simulations that measure specific metrics, as indicated in Table 3. We use the following metrics in our evaluation:

- Discovery success: This metric measures the ratio between the services that were actually reserved (i.e., fulfilled requests) and the total number of unique service requests.
- Request delivery ratio: This metric measures the ratio between the number of providers who received a certain request to the total number of providers who are expected to get it.
- The success in controlling access to the group: This is done using two measures:

- The ratio of the number of denials to the total number of RREQs
- The ratio of the number of allowed access to the total number of RREQs

- The success in getting access permission: This is measured by the ration between the total number of unique access requests (by all roles) to the total number of access permissions.
- The delay in getting access permission versus the different ranks (i.e. average delay per requestor rank).

Table 3: Experiment description and used metrics

Experiment Description	Used Metric	Formula
The experiment tests whether a service-requesting node was able to find a service provider that meets its conditions located and reserved successfully.	Discovery Success (DS).	$DS = \frac{\sum_{i=1}^{N} SDREV_i}{\sum_{i=1}^{N} SREQ_i}$
This experiment measures the ratio of the delivered requests to the total number of sent requests.	Request Delivery Ratio.	$PDR = \frac{\sum_{k=1}^{N} SPR_k}{\sum_{l=1}^{M} TPM_l}$ SPR: Number of Service Provider actually got the Service discovery Request (SREQ) TPM: Total number of Service providers who should get the message.
Fraction of successful Denials and Fraction of successful Allowed Access.	Success in controlling access to the group.	PD = number of denials/ Total number of RREQ PAA = number of allowed access/ Total number of RREQ $PD = \frac{\sum_{i=1}^{N} NACK_i}{\sum_{i=1}^{N} PREQ_i}$ $PAA = \frac{\sum_{i=1}^{L} NACK_i}{\sum_{i=1}^{L} PREQ_i}$
1. We randomly generate nodes with different permissions (roles). 2. We generate group access requests (RREQ) using different roles 3. Over the duration of the experiment, we count the number of RREPs vs. the generated RREQs (the repeated RREQs should not be counted) 4. The success ratio is RREPs/RREQs, where RREQs can be repeated after timeouts. The repeated RREQs should NOT be considered in the calculations.	Success in getting access permission.	PA = # of RREP's / (# of RREQ – repeated RREQ) $PA = \frac{\sum_{i=1}^{N} RREP_i}{\sum_{i=1}^{N} PREQ_i - \sum_{i=1}^{S} RRREQ_i}$ RRREQ: Repeated RREQ.

1. We randomly generate nodes (roles) with different permissions. 2. We select a specific role. We generate RREQs from the members of this role. We count the average time it takes for the RREP to be received. 3. Repeat #1 above for the other roles. 4. As the role of the requestor gets higher, we should expect the average time for receiving the RREP to increase. 5. If we get different results than what we expected in #4, we should investigate why.	Time it takes to get access permission versus the rank of the requestor.	TAP = average time (Time (RREQ) – Time (RREP)) per role T_{RREQ} : Time stamp when the RREQ request was sent. T_{RREP} : Time stamp when the RREP response was received r is a role of given service provider T_r Total time of getting access permission of a role r. $TAP_r = \frac{\sum_{i=1}^{k} T_{RREP\,i} - \sum_{i=1}^{S} T_{RREQ_i}}{T_r}$

C. *Results and Discussion*

1) *Service Discovery/Reservation success rate*

In this experiment, we evaluate the ability of the proposed technique to locate and reserve required service providers (i.e. finding providers). We set the number of available providers within each multicast group to be less than the generated requests. We gradually increase the number of generated requests to different groups and we verify if the discovery success is maintained. Figure 7 shows that the requestors are able, through the help of the commander node, to discover service providers with a very high discovery success percentage that reaches 92%. Also, an average of around 83% of discovered requests were reserved. The remaining requests, about 17%, fail to have a provider reserved. Obviously, not all discovered services would be reserved since some providers will become busy between the time they were discovered and the time they were sent a reservation request. Also, some reservation requests might fail to reach the providers since these providers might be moving frequently. According to Figure 8, as the number of requests increases, the gap between discovered services and reserved services increase gradually. This can be explained as follow. As more requests are generated, the processing and reservation process takes a longer time. During this period some of the providers may become busy due to other demand on their services, therefore some requests might be rejected or delayed until the provider becomes available.

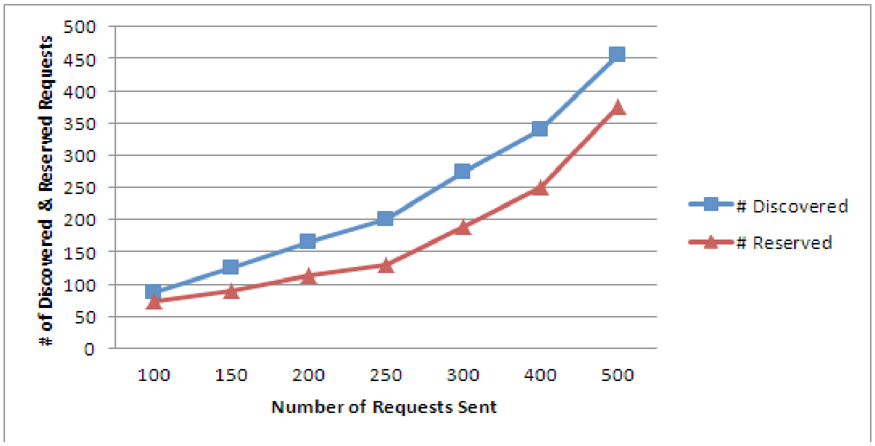


Figure 7: Service Discovery and Reservation Success vs. the Number of Requests

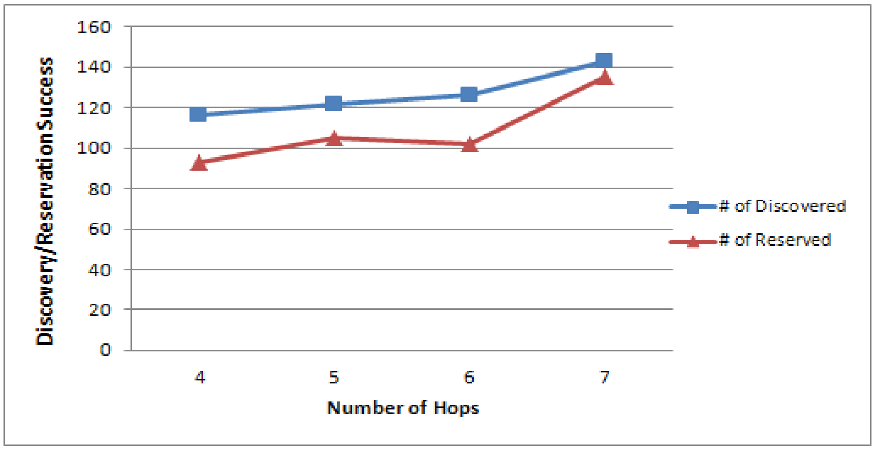


Figure 8: Service Discovery and Reservation Success vs. the Number of Hops

In another experiment we change the discovery search diameter (i.e. search distance in number of hops) and we measure the service discovery/reservation success rate. Figure 8, shows that, as the number of hops increases, the percentage of successful provider discovery and reservation increases. This is intuitive since as we increase the area of search we should be able to find and reserve more resources and it shows that the proposed technique performs as expected.

2) Request Delivery Ratio

In the second experiment, we evaluate the ability of the proposed technique to maintain a good level of packet delivery ratio while varying the number of discovery requests. Figure 9 shows that the packet delivery ratio is around 0.9 with a number of requests relatively small (less than 100). Then, it decreases slightly and remains stable despite the increased number of requests. This proves that our solution maintains very high packet delivery ratio and packet losses are very small. These results demonstrate that the discovery packets will usually reach their destinations, which will not affect the discovery success of our solution.

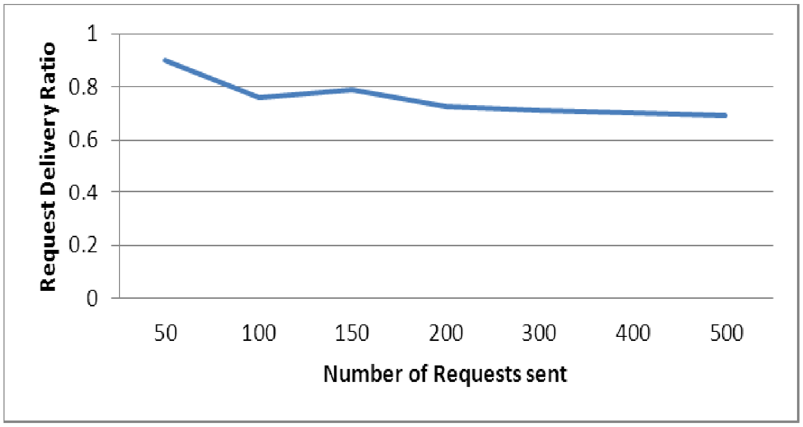


Figure 9: Request Delivery Ratio over the Number of Requests

3) *Controlling Access to Multicast Groups*

In these experiments, we evaluate:

- The ability of our access control scheme to grant access permissions to the different nodes (roles) that are willing to join four categories of groups, and,
- The average time it takes to get access permissions for members belonging to each group.

For both experiments we randomly generate a number of RREQs, in the range of 20 to 80 requests. We then measure the PA and the TAP ratios as described in Table 3. We run each experiment five times and we use the average of the results of all runs. Figure 10, shows the access permission success ratio of four groups, namely, the commander, head of unit, medical, and rescuer groups. The graph illustrates that the ratio of successful group access permission is high for the RREQ requests that are issued to join the rescuer group, which has the lowest role in the hierarchy. This is due to the fact that RREQs for lower roles can be approved by many more members of the team than RREQs for higher roles.

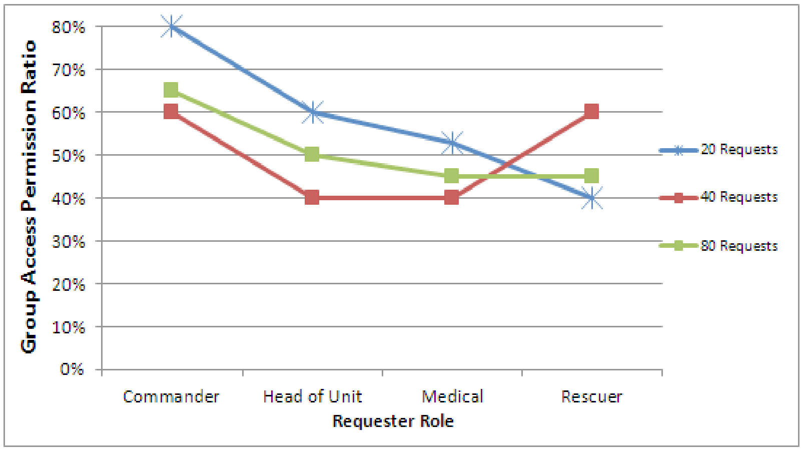


Figure 10: Success ratio in controlling access to each group

As for the average time that it took to process the requests to join different groups, the experiments showed that the average time increases, as the level of the group gets higher. The reason is that when, for example, the lowest level group access is required, and all members of groups above this group can give access to it. The number of members who can give access to a group decreases as the level of the group increases. This is reflected directly on the time it takes for granting access. Figure 11 illustrates the trend followed in this case. It is clear from the figure that the time increases as the group level increases as we discussed.

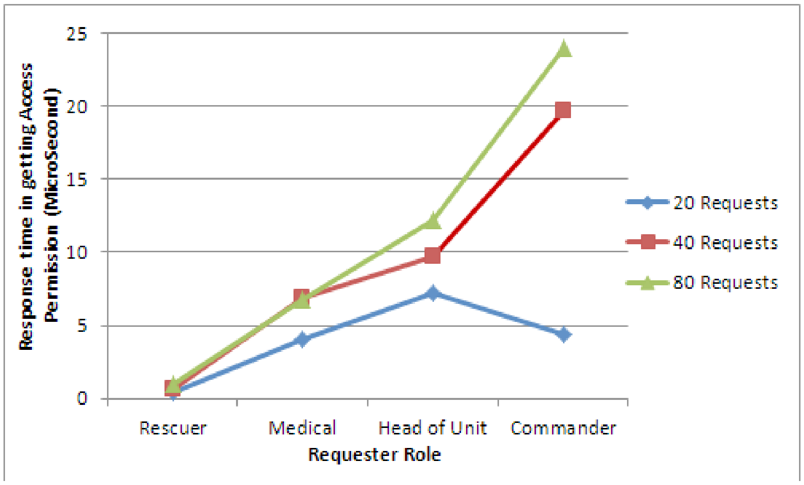


Figure 11: Response time in granting access (Join) the each group

Figure 12, illustrates the response time measured as the difference between sending a service request (SREQ) and receiving a service response (SREP). We average this measure for each number of generated requests and number of nodes in the network. The graph shows clearly that the response time values are considerably low and relatively stable even with the increased number of requests/nodes. They increase slightly and then stabilize around a constant value. This proves that our service discovery scheme maintains a prompt service delivery time while scaling with the number of requests and number of nodes deployed on the network.

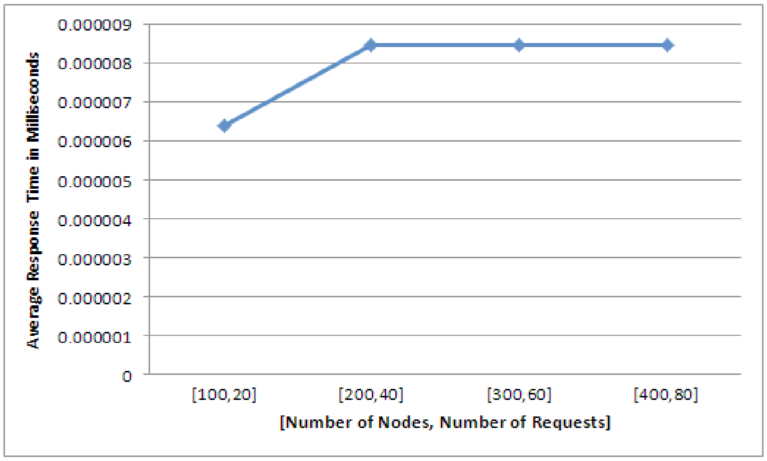


Figure 12: Average response time versus number of requests and number of nodes in the network

D. Qualitative Comparison of different Service Discovery Architectures

We study in this section few examples of existing architectures [2], [3], [8] that addressed the issue of service discovery and selection in specialized mobile networks. This comparison is based on a set of properties that are relevant to service discovery in special military operations e.g., security, reliability, scalability, mobility, and discovery success. The table below details the results of this comparison.

Table 3. Qualitative comparison of service discovery architectures based MANET

Service discovery solutions	Reliability (in terms of discovery success)	Security features (confidentiality, authentication)	Scalability (in terms of number of requests)	Communication protocol used	Mobility	Suitability for Military operations
Our proposed technique	High Service Discovery success.	Security is fully implemented at different levels (e.g., communication, discovery, etc.)	Highly scalable as it allows request/services delegation.	Multicast based wireless communications.	Addressed	Highly suitable; designed specifically for military interventions.
EmerLOC [2]	No service discovery is involved.	Security is partially addressed by using Public Key Infrastructure (PKI) and making use of LDAP.	Not considered.	Wireless, GPRS/GSM based.	Addressed	Not designed specifically for Military operations.
CodeBlue [3]	Data and naming discovery.	Partially addressed using a decentralized security scheme.	Scalability is evaluated by number of sensors.	Wireless Communication.	Addressed	Not designed specifically for military operations
DisSERV [8]	High service discovery success.	Not considered.	Considered.	TCP/IP based protocols.	Addressed	Not designed specifically for Military operations.

The above comparison shows that our proposed architecture for service discovery fulfills all the qualitative requirements for special military operations unlike the other architectures that are not designed specifically for this purpose. The completeness of our architecture relies on its adaptability to the context of military operations as it ensures the confidentiality and integrity of communicated information as well as the access control and management. For example, with regards to security, our architecture maintains it at different levels, as it ensures confidentiality and integrity of data in addition to the access control feature.

VII. CONCLUSION

Emergency response and military operations are of critical nature in terms of the time constraints for delivering help to parties in need. As such, managing the discovery and allocation of resources in a timely efficient and secure manner is of utmost importance when planning and conducting such missions. In this paper, we introduced a comprehensive secure role-based service discovery system to use in special operations. The system ensures that service requests are allowed for operation members with the right permissions only. The system uses a MANET multicast communications system thus conserving on the communications overhead while overcoming the likely situation of the lack of networking infrastructure. The elements of the system include credential establishment, access control, data and group access, service discovery and service selection and reservation components.

The results of system evaluation showed high discovery and reservation success rate. The results also show that the security arrangements, as established within our architecture, ensure secure data delivery and integrity. We also qualitatively compared our architecture to other architectures for special operations, which illustrated the merits of our proposed system.

REFERENCES

[1]. A Meissner, T Luckenbach, T Risse, T Kirste, H Kirchner, “Design Challenges for an Integrated Disaster Management Communication and Information System”, 1st IEEE Workshop on Disaster Recovery Networks (DIREN), pp. 1-7, New York, USA 2002.

[2]. I. Maglogiannis, S. Hadjiefthymiades, “EmerLoc: Location-based services for emergency medical incidents”, International Journal of Medical Informatics Vol. 76, Issue 10, pp. 747-759, October 2007.

[3]. D Malan, T Fulford-Jones, M Welsh, S Moulton, “CodeBlue: An Ad Hoc Sensor Network Infrastructure for Emergency Medical Care”, International Workshop on Wearable and Implantable Body Sensor Networks, New York, USA 2004.

[4]. D. Bottazzi, A. Corradi, and R. Montanari, “Context-Aware Middleware Solutions for Anytime and Anywhere Emergency Assistance to Elderly People”, IEEE Communications Magazine, pp. 82-90, April 2006.

[5]. K. F.R. Liu, “Agent-based Resource Discovery Architecture for Environmental Emergency Management,” Expert Systems with Applications, Vol. 27, pp. 77-95, 2004.

[6]. K. Kanchanasut, A. Tunpan, M. A. Awal, T. Wongsaardskul, D. Das, and Y. Tsuchimoto, “Building A Long-distance Multmedia Wireless Mesh Network for Collaborative Disaster Emergency Reponses”, intERLab Technical Report, Asian Institute of Technology, Thailand, April 2007.

[7]. T. Catarci, M. Leoni, A. Marrella, B. Salvatore, G. Vetere, S. Dustdar, L. Juszczyk, A. Manzoor, and H. Truong, “Pervasive Software Environments for Supporting Disaster Responses,” IEEE Internet Computing, pp. 26-37, January 2008.

[8]. Y. Gadallah, M. A. Serhani, Nader, M. “Middleware Support for Service Discovery in Special Operations Mobile Ad Hoc Networks”, Elsevier’s Journal of Network and Computer Applications, Vol.33, Issue 5, pp. 611-619, March 2010.

[9]. L. Cheng, “Service Advertisement and Discovery in Mobile Ad hoc Networks”, Workshop on Ad hoc Communications and Collaboration in Ubiquitous Computing Environments, November, New Orleans, Louisiana, USA, 2002.

[10]. S. Lee, M. Gerla, and C. Toh, “On-demand multicast routing protocol (ODMRP) for ad hoc networks”, Internet Draft, June 1999.

[11]. R. Meier, V. Cahill, A. Nedos, and S. Clarke, “Proximity-Based Service Discovery in Mobile Ad Hoc Networks”, Lecture Notes in Computer Science, the 5th IFIP International Conference on Distributed Applications and Interoperable Systems, Springer-Verlag, pp. 115 – 129, Athens, Greece, 2005.

[12]. S. Penz, “SLP based Service Management for Dynamic Ad hoc Networks”, the 3rd International Workshop on Middleware for Pervasive and Ad-Hoc Computing, pp. 1-8, November, Grenoble, France, 2005.

[13]. S. Czerwinski, B Y. Zhao, T. Hodes, A. Joseph, and R. Katz, “Architecture for a secure service discovery service” Journal of Systems and Software, Vol.76, No.1, pp.45-54.

[14]. Y. Yuan and A. Agrawala, “A Secure Service Discovery Protocol for MANET”, 14th IEEE Proceedings on Personal, Indoor and Mobile Radio Communications, pp. 2218 – 2222, Vol. 3, Finland 2003.

[15]. Moon, Misun, Dong Seong Kim, and Jong Sou Park. "Toward Modeling Sensor Node Security Using Task-Role Based Access Control with TinySec." Computational Intelligence and Security. Springer Berlin Heidelberg, 2007. 743-749.

[16]. Bakar, Asmidar Abu, Azimah Abdul Ghapar, and Roslan Ismail. "Access control and privacy in MANET emergency environment." Computer and Information Sciences (ICCOINS), 2014 International Conference on. IEEE, 2014.

[17]. Maity, Soumya, P. Bera, and S. K. Ghosh. "An access control framework for semi-infrastructured Ad hoc networks." Computer Technology and Development (ICCTD), 2010 2nd International Conference on. IEEE, 2010.

[18]. S. Trabelsi and Y. Roudier "Enabling Secure Service Discovery with Attribute Based Encryption", Research Report RR-06-164, EURECOM, France.

[19]. C. Campo, F. Almenarez, D. Diaz, C. Garcia-Rubio, and A. Marin Lopez. "Secure Service Discovery based on Trust Management for ad-hoc Networks" Journal of Universal Computer Science, Vol. 12, Issue 3, 2006

[20]. F. Zhu, M. Mutka, and L. Splendor, "A Secure, Private and Location-Aware Service Discovery Protocol Supporting Mobile Services," 1st International Conference on Pervasive Computing and Communication, ACM Press, pp. 235–242, 2003.

[21]. Mohsen Guizani, "Security and Trust in Mobile Ad Hoc Networks", 4th Annual Communication Networks and Services Research Conference, pp.4-5, Moncton, Canada, 2006.

[22]. E. Barka and Y. Gadallah, "A Role-based Protocol for Secure Multicast Communications in Mobile Ad Hoc Networks", the 6th International Wireless Communications, Networking, and Mobile Computing Conference, China, June 2010.

[23]. R. Sandhu, E. Coyne, H. Feinstein, and C. Youman, "Role-based access control models," IEEE Computer, Vol. 29, No. 2, pp. 38-47, February 1996.

[24]. R. S. Sandhu and P. Samarati, "Access control: principle and practice," IEEE Communication. Magazine, Vol. 32, No. 9, pp. 40–48, 1994.

[25]. Mian, A.N, Baldoni, R., Beraldi, R. "A Survey of Service Discovery Protocols in Multihop Mobile Ad Hoc Networks", IEEE Pervasive Computing, Vol. 8, Issue 1, pp. 66-74, 2009.

[26]. Fang Shen, Qingqi Pei, Shu-po Bu "A Trust-based Dynamic Secure Service Discovery Model for Pervasive Computing" 7th International Conference on Computational Intelligence and Security (CIS), pp. 630-634, China, 2011.

[27]. Johnsen, F.T., Flathagen, J., Hafse, T. "Pervasive service discovery across heterogeneous tactical networks", IEEE Military Communications Conference, pp. 1-8, Norway 2009.

[28]. Katharina R., Fei L., Sanjin S., Rassul A., Schahram D. "Context-driven personalized service discovery in pervasive environments", World Wide Web, Special Issue on Mobile Services on the Web, Vol. 14, No. 4, pp. 295-319, 2011.

[29]. Daniel R., Romain R., Lionel S.; Pierre C. "Service Discovery in Ubiquitous Feedback Control Loops" International Conference on Distributed Applications and Interoperable Systems, LNCS 6115, pp. 112-125, Netherlands 2010.

[30]. Araghi, Tanya Koohpayeh, et al. "An Access Control Framework in an Ad Hoc Network Infrastructure." Advanced Computer and Communication Engineering Technology. Springer International Publishing, pp.747-754, 2015.

[31]. Bakar, A., et al. "Ensuring Data Privacy and Security in MANET: Case in Emergency Rescue Mission." Proceedings of the International Conference on Information and Knowledge Management (ICIKM), Kuala Lumpur, Malaysia. 2012.

VEHICLE SEGMENTATION USING K-MEANS WITH FUZZY LOGIC

[1]Shakila basher, [2]Purushothaman S., and [3]Rajeswari P.
[1]Research Scholar, Department of MCA, VELS University, Chennai, India.
[2]Associate Professor,
[3]Lecturer, Department of Electrical and Computer Science Engineering,
[23]Institute of Technology, Haramaya University, DireDawa, Ethiopia

Abstract:

This paper presents methods for vehicle segmentation. The camera can be fixed or moving which can be used to capture the moving vehicle. During this process, the orientation of the vehicle captured can be in any direction. Many segmentation methods available. However, K-Means with Fuzzy logic can be still more appropriate in segmenting the vehicles moving on the road.

1. Introduction

Vehicle segmentation is an important process in the image processing domain. Only after proper segmentation of the vehicle from the road and other sceneries background, the segmented image can be further used for template matching, tracking and identifying the type of vehicle.

Kong, 1998, implement the motion segmentation algorithm based on Galilean wavelets. These wavelets behave as matched filters and perform minimum mean-squared error estimations of velocity, orientation, scale and spatio-temporal positions. This information is finally used for tracking and segmenting the objects. They claimed that the algorithm is robust, it can deal with temporary occlusions and by tuning a threshold it can estimate the number of moving objects in the scene.

Tsai et al, 2007, implement a color transform model to detect vehicles using color and edges. The color transform model identifies the pixels from the background and the corner, edge map. The wavelet transforms construct an cascade multichannel classifier. This approach eliminates most background pixels in advance to make easy to detect the vehicles.

Chen, 2006, exploit the wavelet decomposition in order to reduce the typical noise problem of image difference based approaches. The image difference is computed on the low frequency sub-image of the third level of the discrete wavelet transform (DWT). On the extracted blobs they perform morphological operations and extract the color and some spatial information. Each blob is associated with a descriptor that is used to track the objects through the sequence.

Ahad Karimi Moridani et al., 2015, present a powerful algorithm of computer vision methods to traffic flow monitoring, vehicle detection and traffic analysis, which intend to develop the vehicle count system using an image processing technique in CCTV video outputs. This software-based vehicle counter can detect all vehicles through images instead of using expensive electronic sensors or cameras embedded in the sidewalks. This system processes captured video, detects vehicles in each frame, classifies the vehicles into four types and counts all of them, all by image/video processing techniques.

2. Problem statement

Many image processing techniques still find difficulties in segmentation of images. The segmentation is becomes clear only when the image is taken in a controlled condition. However, in case of vehicle tracking, there is no controlled condition of lighting, and hence a clear image is always a difficult job. It is difficult task to segment such image clearly.

3. System setup

a. Acquire image

b. Create contrast in the image

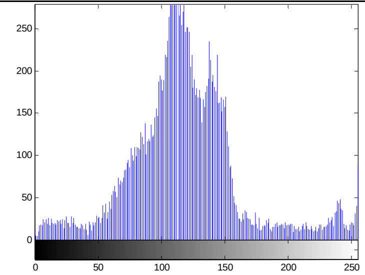
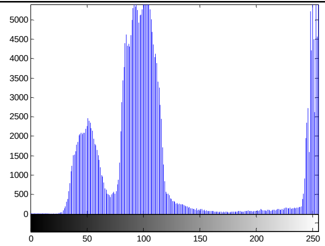
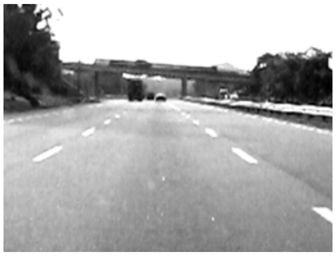
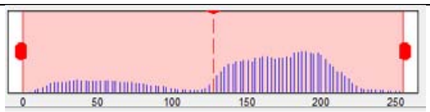
c. Segment the image using K-Means with Fuzzy Logic

d. Compare with the template and identify the type of vehicle.

4. Description and Results

a) Acquiring image: Image has to be acquired with good quality camera. The various information in the image has to be separated from the background of the image. In order to achieve this, there should be a clear contrast among objects against the background in the image. Mostly a clear contrast does not present in the image. Hence, contrast has to be created in the image.

b) Contrast: A contrast in the image can be changed by first obtaining the histogram of the image horizontally and vertically.

a.		
b.		
		

In the table shown the first row has an image with good contrast where in the vehicle object is clearly visible against the background. The histogram image is properly bell shaped and the major portion of the histogram is cantered. However for the image shown in the second row, the image is not having good contrast. Hence the corresponding histogram has three locations where the intensities are concentrated. This has to be contrast enhanced so that, the objects are clearly visible against the background. The image is contrast adjusted and presented in the third row. The corresponding change in the histogram is shown.

C) K-means algorithm

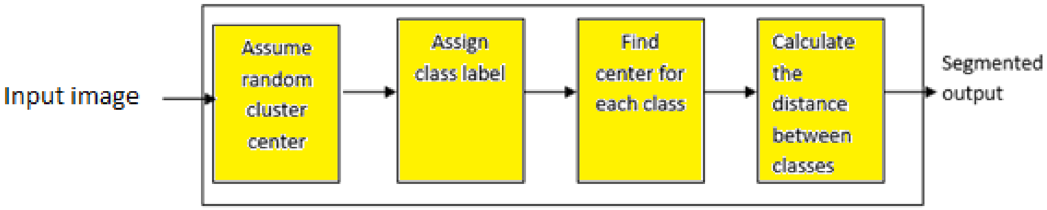

Input image
Assume random cluster center
Assign class label
Find center for each class
Calculate the distance between classes
Segmented output

Fig.1 K-Means algorithm

K-Means is a statistical method that uses distance concept in clustering group of adjacent pixels with very close similar intensity values. In general, the intensity values and their pixel locations are considered for grouping. A manual centre initialization procedure is used for segmenting the image. Only when the number of group of objects and the object centres are clearly known in advance, then a better segmentation can be achieved.

D) Fuzzy logic with K-Means (FLKM)

Vehicle images have different brightness and contrast and different clarity. These variations are considered to be fuzzy and hence, the pixels representing the objects are considered fuzzy. Hence, fuzzy logic with K-Means has been combined to segment the image.

Fuzzy Logic (FL) is a multi-valued logic that allows intermediate values to be defined between conventional evaluations like true/false, yes/no, high/low. Fuzzy systems are an alternative to traditional notions of set membership and logic.

The training and testing fuzzy logic with K-Means is to map the input pattern with target output data. For this, the inbuilt function has to prepare membership table and finally a set of number is stored. During testing, the membership function is used to test the pattern.

Figure 2 presents a schematic architecture for training and testing FLK-Means or segmenting a texture image. Training FLKM involves inputting feature patterns from CC and target values for segmenting texture image. The sugeno type inference system available in the Matlab software generates inference rules using subtractive clustering. The final sets of trained values are stored in a file. In the testing process of FLKM, the image is input to FLKM module. The final weights are processed with features and an output is obtained. This output is compared with a threshold to assign segmentation values to the image.

Training FLKM

Step 1: Input the k-Means segmented image.

Step 2: Create Fuzzy membership function.

Step 3: Create clustering using K-Means algorithm.

Step 4: Process with target values.

Step 5: Obtain final weights.

Testing FLKM for texture segmentation

Step 1: Input the k-Means segmented image.

Step 2: Process with Fuzzy membership function.

Step 3: Find the cluster to which the pattern belongs.

Step 4: Obtain estimated target values.

Step 5: Segment the image

RADII specifies the range of influence of the cluster centre for each input and output dimension, assuming the data falls within a unit hyperbox (range [0 1]). Specifying a smaller cluster radius will usually yield more, smaller clusters in the data, and hence more rules. When RADII is a scalar it is applied to all input and output dimensions.

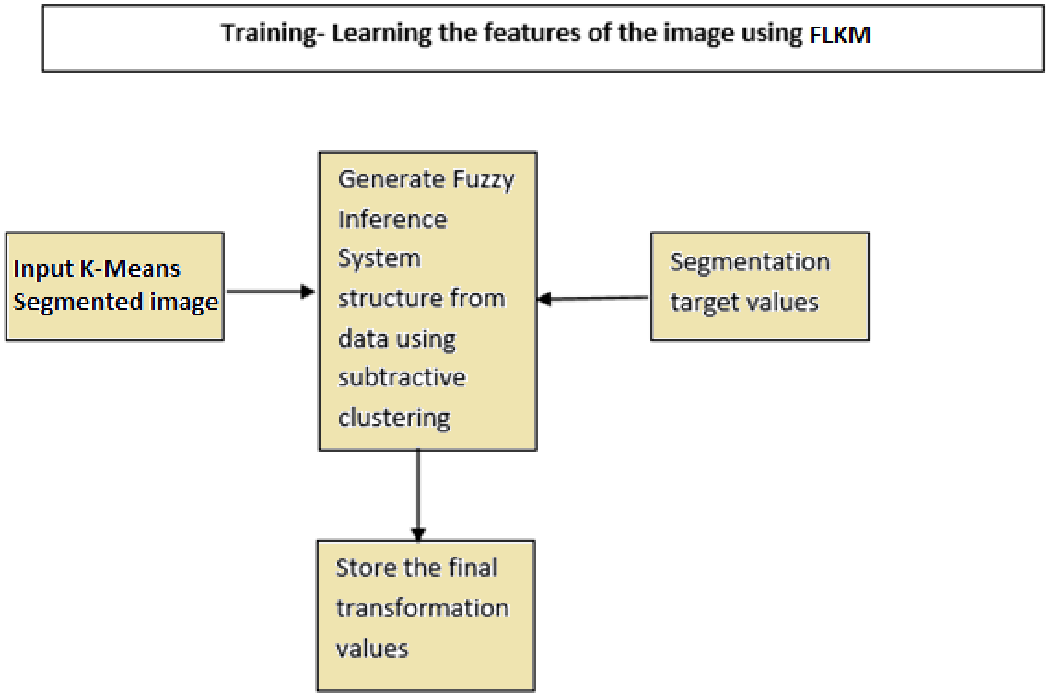

Training- Learning the features of the image using FLKM
Input K-Means Segmented image
Generate Fuzzy Inference System structure from data using subtractive clustering
Segmentation target values
Store the final transformation values

Fig.2a Training and Testing FLKM for segmenting the image

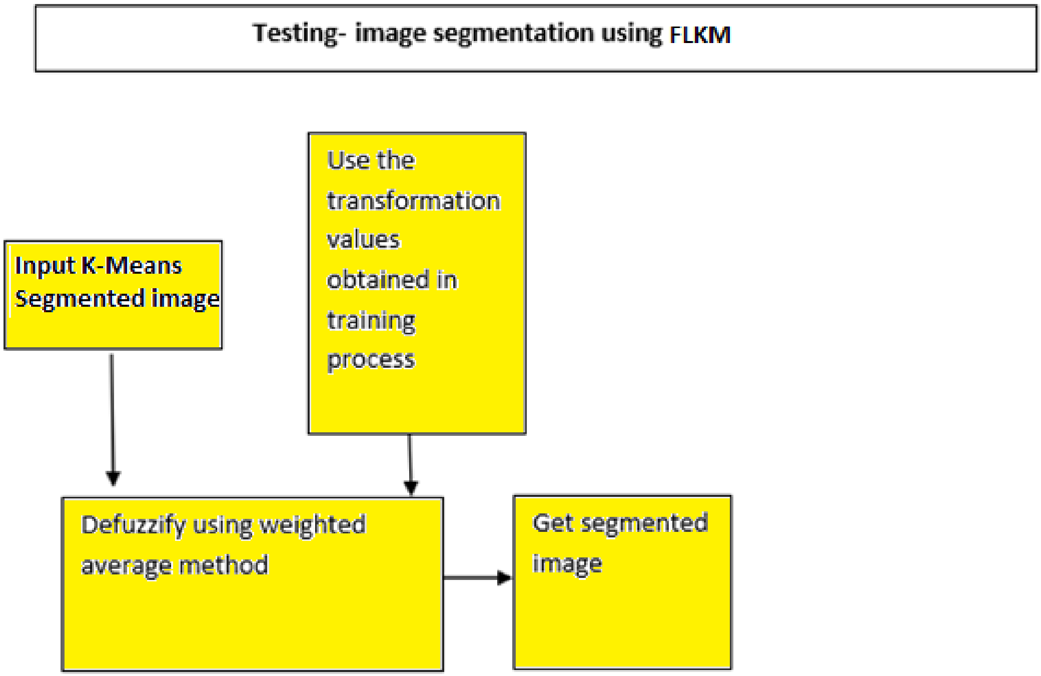
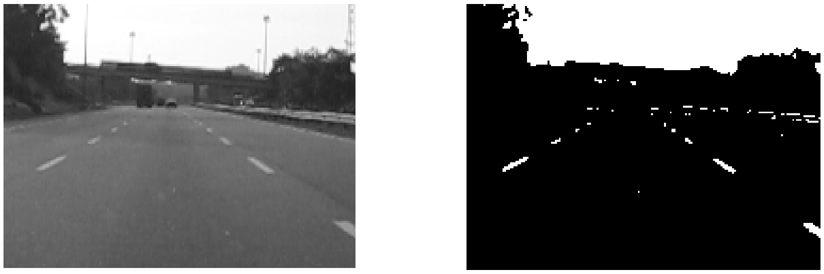

Testing- image segmentation using FLKM
Input K-Means Segmented image
Use the transformation values obtained in training process
Defuzzify using weighted average method
Get segmented image

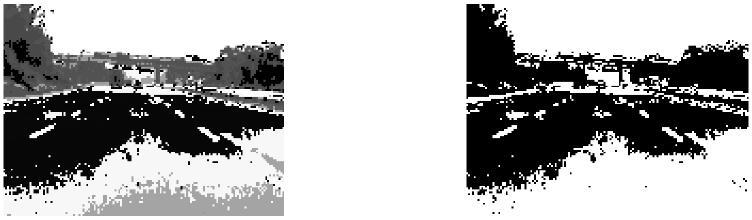
Fig.2b Training and Testing FLKM for segmenting the image



input

FCKM segmented image

Fig.3 Uncontrasted image segmented



input

FCKM segmented image

Fig.4 Contrasted image segmented

Figure 3 shows the vehicle image (less contrast) segmented by FCKM. There is no clear visibility of the vehicle in the segmented image. Figure 4 presents the well contrasted image. The segmented image shows the presence of a vehicle.

5. Conclusion

This paper presents methods of normalizing and segmenting vehicle images with better clarity. K-Means algorithm is used for initial segmentation of the vehicle image. Subsequently, the segmented image is input to the Fuzzy logic module for getting the final segmented image. From the segmented image, the presence of a vehicle is identified using template matching.

References

[1] Ahad Karimi Moridani, et al., 2015, Vehicle Detection and Tracking in Roadway Traffic Analysis using Kalman Filter, International Journal of Imaging and Robotics, Vol,15; Issue No.2,

[2] Chen C.E., Wang H., Ali A., Hudson R.E., and Yao K., 2006, Particle filtering approach to localization and tracking of a moving acoustic source in a reverberant room, IEEE, pp.849-852.

[3] Kong M., Leduc J.P., Ghosh B., and Wickerhauser V., 1998, Spatio-temporal continuous wavelet transforms for motion-based segmentation in real image sequences, Proceedings of the International Conference on Image Processing, Vol.2, pp.662-666.

[4] Tsai L.W., Hsieh J.W., and Fan K.C., 2007, Vehicle detection using normalized color and edge map, IEEE Transactions on Image Processing, Vol.16, No.3, pp.850–864.

Effective feature selection in multi-label classification problems using genetic algorithms

Somayeh Fattahi Ferdowsi

Department of computer
Zanjan Branch, Islamic Azad University
Zanjan, Iran

***ABSTRACT-* Designing a classifier in a multiple-label classification issue in which the number of features used for describing each sample is high and the number of samples is low, is faced with many problems. The features describing each sample can be divided into three categories: relevant, irrelevant and redundant. Redundant and irrelevant features could seriously influence the accuracy of classification in such issues. In spite of works carried out, the issue of feature selection in multiple–label classification issues is still considered as a challenge. For this reason, the issue of feature selection has been discussed in this paper. The aim of feature selection problem is finding a subset of features in order to modify and improve the accuracy of estimation without loss of accuracy that classifier using the selected features performs the classification of data. This study was aimed to enhance the efficiency of classification through decreasing the error and to increase classification speed through selecting a subset of effective features in classification of multi-label data as well as using mutual information, Genetic Algorithm and Rank SVM classification The performance of proposed method has been evaluated on three data collections including Emotions, Scene and Yeast that are available on Mulan website.**

Keywords: feature selection, multi-label classification, genetic algorithms and classification Rank SVM

I. Introduction

Numerous studies have been carried out about single label. However, every record might correspond with some classes in real world that is called multi-labels. In single-label classification, each sample is related to a label, but in multi-label classification to one or more labels. In other words, in multi-label classifications, the class of each sample is determined by a vector of labels. In many real applications, the data is also multi-label one. Multi-label classification is a special supervised learning issue, in which any single instance could be possibly associated with several classes simultaneously and thus the classes are no longer mutually exclusive. Recently, it has been paid more attention to than before due to lots of real-world applications, e.g., text categorization, scene and video annotation, bioinformatics, and music emotion categorization [1].The actual data set reduces significantly the degree of precision and accuracy due to the large number of irrelevant and redundant features. In addition, the more the number of labels, the more difficult learning multi-label data. Accordingly, the problem with features arises. Features are divided into the three categories: related, unrelated and redundant [2]. Related features are counted as the features influencing the output; there is a correlation between these features and class label, determining class label, selecting efficient features to be classified. Unrelated features do not express any information about the class label. In other word, there is no affiliation between these features and class label, so they should not be affected in classification. Redundant features are the ones which do not provide additional useful information to selected features available, so they can be removed from the existing feature set, because there are a number of other features in the subset that can express the same information. In the selection feature problem, the aim is to find one subset of the features to correct and recover the accuracy and precision estimates, without loss of accuracy, which the classifier classifies the data using selected features of classification. In this article, the attempts were made to select a subset of the features of the multi-label data classification to improve the performance classification by reducing errors and to increase the speed of classification.

II. Topics studied in this article

A. *Feature Selection*

The problem of feature selection is considered as one of the issues that is proposed in machine learning discussions and statistical pattern recognition. This is of high importance in many applications (such as classification), for there are a lot of irrelevant and redundant features which contain little information, removing them does not cause a problem, but increase the computational load. In addition, this makes a lot of useless information to be stored along with useful data.

B. *Feature selection algorithms*

In this section we peruse different methods of selecting a subset of features.

1) *Filter method*

In filter algorithms, the search process is independent of any classification algorithm. The goodness of feature subsets are evaluated based on a certain criterion like distance measure, information measure and consistency measure [3].

2) *Wrapper method*

In a wrapper model, the feature selection algorithm exists as a wrapper around a classification algorithm and the classification algorithm is used as a "black box" by the feature selection algorithm. The performance of the classification algorithm is used in the evaluation function to evaluate the goodness of feature subsets and guide the search [3].

C. *Genetic algorithm*

Artificial intelligence research within the computer science field produced GA, a heuristic search tool designed to mimic the natural process of evolution. This heuristic, or so called meta-heuristic, is commonly used to generate useful solutions for optimization and search problems, often employing the natural techniques of evolution, such as inheritance, mutation, selection and crossover. John Holland developed the formal theory of GA in the 1970s, and continued improvements to the price and performance value have made GA attractive for many problem-solving optimization methods [4].Genetic algorithms are a type of optimization algorithm, meaning they are used to find the optimal solution(s) to a given computational problem that maximizes or minimizes a particular function [5]. GA has been shown to perform well in mixed (continuous and discrete) combinatorial problems. Although GA easily become trapped in local optima, they are computationally expensive and a probabilistic one. A GA begins with a set of solutions represented by a group of chromosomes called the population. A new population can be generated by borrowing solutions from the current population or by applying genetic operators such as selection, crossover, and mutation to current population. The new population must be better than the old one.

The function of genetic operators warrants more detailed attention. The selection operator picks two parent chromosomes from the population based on their fitness to participate in the next operations, crossover and mutation. These steps are considered the most important in a GA because they have a positive impact on the overall performance. First, parents form new offspring (children) through crossover probability. Shortly after, the mutation operator randomly exchanges alleles, as occurs in nature. To work well, GA require the definition of three important aspects: the objective function, the genetic representation and its implementation, the genetic operators and their implementation.[4]

D. *SVM algorithm*

Let a binary i.i.d. training set of size l be $\{(x_1, y_1), \dots, (x_i, y_i), \dots, (x_l, y_l)\}$ where $x_i \epsilon X$ and $y_i \in \{+1, -1\}$ denote the ith training instance vector and its binary label.

In the original space, a linear discriminant function is defined as $f(x) = w^t x + b$ .where w and b are the weight vector and bias term respectively. The primary problem of SVM for the nonlinearly separable case is formulated as

$$\text{Min}\frac{1}{2}w^T w + C\sum_{i=1}^{l}\xi_i, \qquad s.t. y_i(w^T x_i + b) \geq 1 - \xi_i, \xi_i \geq 0\,,$$
$$i = 1, \dots, l \qquad (1)$$

where C>0 denotes a regularization constant to control the tradeoff between classification errors and model complexity, and $\xi_{imn} \geq 0$ are slack variables to indicate misclassification errors.

E. *Rank SVM algorithm*

In classification for multi-label data using Rank SVM algorithm [6,7] in the original input space, q linear discriminant functions are defined as

$$f_k(x) = {w_k}^T x + b_k\,, k = 1, \dots, q \quad (2)$$

Where w_k and b_k denote the weight vector and bias term of the k^{th} class respectively. Therefore, in Rank-SVM, the relative relationship between any relevant label and any irrelevant one for some training instance xi, is described using the following pairwise constraint:

$$f_m(x_i) - f_n(x_i) = (w_m - w_n)^T x_i + (b_m - b_n) \geq 1 - \xi_{imn}, (m, n) \in \left(L_i \times \overline{L_i}\right) \qquad (3)$$

Where the slack variable $\xi_{imn} \geq 0$ is added to force the difference to be equal to or more than 1.

As shown in Fig. 1 for$\rho = 1$, there exist three possible cases:

(a) $f_m(x_i) - f_n(x_i) \geq 1\ and\ \xi_{imn} = 0$, which is a perfect situation

(b) $0 < f_m(x_i) - f_n(x_i) < 1\ \ and\ \ 0 < \ \xi_{imn} < 1$

(c) $f_m(x_i) - f_n(x_i) \leq 0\ and\ \xi_{imn} \geq 1$

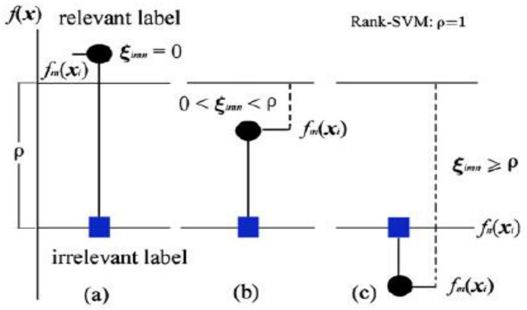


Figure 1. Three possible relative relationships between a pair of labels in Rank-SVM ($\rho = 1$).[1]

III. The proposed method

In this paper, the genetic algorithm was considered to solve the problem of feature selection in the field of multi-label sample classification, within the framework of the wrapper. In this case, prediction of multi-label samples is made through an appropriate threshold t(x). Since the evaluation of a multi-label algorithm is more complex than that of a single-label Algorithm, three evaluation criteria were applied in the present study: one-error, average precision and ranking loss. Multi-label support vector machine was used to classify the data, and establish relative relationship between each related label and each unrelated label.

To select the features using a genetic algorithm, the following procedure was followed:

- Creating random population with n_{pop} size and evaluating them
- Selecting parents and combining them to create a population of children as n_{c}
- Selecting members of the population for enforcing mutation and creating mutant population as n_{m}
- Integrating the original population, children and mutants, and creating new original one.

In the present study, the probability of selection was calculated by the use of $\mathrm{P_i} = \mathrm{e}^{-\beta \mathrm{C_i}}$ in which β was selective pressure as parameter and $\mathrm{C_i}$ was the cost of ith selection. The three cross over ways (i.e., single-point crossover, two-point crossover and uniform crossover) were adapted to be used and through roulette wheel selection (RWS), the parents were selected from the main population. To do so, it is attributed to each of these ways probability which were considered here as follows:

$pSinglePoint = 0.1;$
$pDoublePoint = 0.2;$
$pUniform = 1 - pSinglePoi - pDoublePoint$

To enforce the mutation, an element was randomly selected from the input vector, being completed (one was changed to zero and zero to one).

Suppose there is an original population with a number of $\mathrm{n_{pop}}$ members from which the population of children is selected according to$0 \leq \mathrm{p_c} \leq 1$, $\mathrm{n_c} = \mathrm{p_c}\mathrm{n_{pop}}$, the population must be paired, and then $\mathrm{n_c}$ can be rewritten as $\mathrm{n_c} = 2\left\lceil \frac{\mathrm{p_c}\mathrm{n_{pop}}}{2} \right\rceil$ and crowd of mutants was selected as$\mathrm{n_m}$. All these members were integrated together so that it equaled $\mathrm{n_{pop}} + \mathrm{n_c} + \mathrm{n_m}$. It was ordered, and due to elitism, $\mathrm{n_{pop}}$ was selected as the best choice from the beginning of the population. In this case, the new generation and the population were organized.

Let $\mathrm{X} \in \mathrm{R^d}$ be a d-dimensional input space with l features and C set of all output classes, find out the subset $\mathrm{S} \subseteq \mathrm{X}$ with k features and $\mathrm{Q} = \{1,2, \dots, \mathrm{q}\}$ a finite set of class labels, where q is the number of class labels. Further, assume that each instance xϵX can be associated with a set of relevant labels $\mathrm{L} \subseteq 2^{\mathrm{Q}}$. At the same time, the complement of L, i.e., $\overline{\mathrm{L}} = \mathrm{Q} \setminus \mathrm{L}$, is referred to as a set of irrelevant labels of x. Given a training data set of size l drawn identically and independently from an unknown probability distribution (i.i.d.) on $\mathrm{X} \times 2^{\mathrm{Q}}$, i.e., $\{(\mathrm{x_1}, \mathrm{L_1}), \dots, (\mathrm{x_i}, \mathrm{L_i}), \dots, (\mathrm{x_l}, \mathrm{L_l})\}$. Given some instance xi, its q discriminant function values and predicted set of relevant labels from some multi-label classification algorithm are denoted by $\mathrm{f_k^p}(\mathrm{x_i}), \mathrm{k} = 1, \dots, \mathrm{q}$ and $\mathrm{L_i^p} \subseteq 2^{\mathrm{Q}}$ respectively.

Also any relevant label should be ranked higher than any irrelevant one [7]. In this case, the multi-label prediction can be fulfilled through a proper threshold t(x),

$$\mathrm{f(x)} = \{\, \mathrm{k} \mid \mathrm{f_k(x)} > \mathrm{t(x)}\, ,\ \mathrm{k} = 1, \dots, \mathrm{q}\} \qquad (4)$$

IV. The evaluation and compare results

To evaluate the proposed method we use data sets in Table (2) which includes three data sets Emotions, Scene and Mulan Yeast, which have been published in the database [8].

TABLE I. Data sets used in our experiments.

Datas et	***Domain***	***Instances***		***Features***	***Classes***
		Train	***Test***		
Emotion	Music	391	202	72	6
Scene	Scene	1200	800	294	6
Yeast	Biology	1500	917	103	14

Since the proposed method is based on the classification labels. Therefore, the measures contained in the multi-label data classification criteria of an error, a drop in ratings and an average accuracy of classification based on the methods used order to assess their use [1].

The one error: evaluates how many times that the top-ranked label is not one of relevant labels:

$$\text{One error} = \frac{1}{m}\sum_{i=1}^{m}\left|\{k \notin L_i | f_k^p(x_i) = \max_{k' \in Q} f_{k'}^p(x_i)\}\right| \in [0,1]\} \qquad (5)$$

The ranking loss: calculates the average fraction of labels pairs (a relevant label versus an irrelevant one) that are not correctly ordered for the instance:

$$\text{Ranking loss} = \frac{1}{m}\sum_{i=1}^{m}\left(\frac{1}{|L_i||\bar{L}_i|}\left|\{(k,k') \in (L_i \times \bar{L}_i) | f_k^p(x_i) \leq f_{k'}^p(x_i)\right|\right) \in [0,1] \qquad (6)$$

The average precision: compute the average fraction of labels ranked above a specific relevant label kALi , which actually are in Li, i.e

$$\text{Average precision} = \frac{1}{m}\sum_{i=1}^{m}\left(\frac{1}{|L_i|}\sum_{k \in L_i}\frac{\left|\{k' \in L_i | f_{k'}^p(x_i) \geq f_k^p(x_i)\}\right|}{\left|\{k' \in Q | f_{k'}^p(x_i) \geq f_k^p(x_i)\}\right|}\right) \in [0,1] \qquad (7)$$

It is favorable that a multi-label algorithm should achieve a larger value for the average precision, and smaller values for the other four measures.

The process for evaluating the proposed method is that each dataset was tested separately in MATLAB in terms of each criterion by using the proposed method (FSS Rank SVM), and characteristics of each dataset was reduced by the use of proposed method.

TABLE II. Number of features obtained by test proposed method (Fss Rank svm)

measure / Dataset	*Features*	*Feature selection by Ranking Loss*	*Feature selection by One Error*	*Feature selection by Average Precision*
Emotion	72	34	30	45
Scene	294	93	115	102
Yeast	103	64	63	61

Then a new dataset was obtained through feature selection based on genetic algorithm to each criterion. (For each dataset, given that the three criteria have been used, 3 new datasets were produced). In the second process, each of the three primary datasets was tested with Rank SVM for multi-label classification, and the errors of the three evaluation criteria were obtained. Then, each reduced dataset was tested again by Rank SVM, and results were compared with the results of the primary dataset. The results of the tests carried out for each dataset have been recorded in a separate table as following.

TABLE III. Compare the results Rank svm for Yeast dataset and new dataset with reduced features using proposed method

measures / Data set	*Ranking Loss*	*One Error*	*Average Precision*	*cost* *Feature selection*
Rank Svm by **103** feature	0.1703	0.2366	0.7508	......
64 feature with Feature selection by Ranking loss	**0.1644**	0.2116	**0.7635**	0.1644
63 feature with Feature selection by One error	0.1712	0.2137	0.7578	0.2137
61 feature with Feature selection by Average Precision	0.1675	**0.2105**	0.7620	0.7620

TABLE IV. Compare the results Rank svm for Scene dataset and new dataset with reduced features using proposed method

measures / Data set	*Ranking Loss*	*One Error*	*Average Precision*	*Cost Feature selection*
Rank Svm by **294** feature	0.3533	0.6421	0.5588	......
93 feature with Feature selection by Ranking loss	**0.0820**	0.2485	**0.8549**	0.0820
115 feature with Feature selection by One error	0.0980	**0.2349**	0.8509	0.2349
102 feature with Feature selection by Average Precision	0.0931	0.2425	0.8507	0.8507

TABLE V. Compare the results Rank svm for Emotions dataset and new dataset with reduced features using proposed method

measures ***Data set***	***Ranking Loss***	***One Error***	***Average Precision***	***cost*** ***Feature selection***
Rank Svm by **72** feature	0.3937	0.5842	0.5747	………
34 feature with Feature selection by Ranking loss	0.2573	0.4025	0.7099	0.17552
30 feature with Feature selection by One error	**0.2464**	**0.4000**	**0.7141**	0.23762
45 feature With Feature selection by Average Precision	0.4758	0.5750	0.5533	0.5747

Comparing the results, it was concluded that in the proposed method, since the proposed algorithm reduces the number of features, cost classification is reduced in general by reducing the number of features.

V. Conclusion

In a multi-label classification problem, where the number of attributes used to describe each sample is a lot and the sample size is small, numerous problems are to be faced to design a classifier. Features describing each sample can be categorized under three heads of related, unrelated and redundant features. Redundant and irrelevant features may strongly have an effect on the accuracy of classification in such problems. In this article the problem of feature selection in the multi-label classification problems were discussed. In the feature selection problem, it is aimed at finding one subset of features to correct and recover precision and accuracy of estimates, without reducing the accuracy of the classification accuracy which enables the classifier to classify data using selected features. In this study, using genetic algorithms and Rank SVM classification, a subset of the features effective on multi-label data classification have been selected, so that the efficiency has been increased by reducing error. Performance of the proposed method was assessed on three datasets Emotions, Scene and Yeast. Comparing the results, it was concluded that in the proposed method, since the proposed algorithm reduces the number of features, cost classification is reduced in general by reducing the number of features. It is proposed for future study to make use of other Meta-heuristic Algorithms in feature selection on multi-label data.

References

[1] Xu , Jianhua ,"Fast multi-label core vector machine" ,Pattern Recognition 46,2013, 885–898.

[2] B. Bonev," FEATURE SELECTION BASED ON INFORMATION THEORY", Robot Vision Group Department of Computer Science and Artificial Intelligence UNIVERSITY OF ALICANTE , PH.D. THESIS, 2010, paper 24.

[3] Bing Xue, "Particle Swarm Optimization for Feature Selection in Classification" , A thesis submitted to the Victoria University of Wellington in fulfillment of the requirements for the degree of Doctor of Philosophy in Computer Science , 2014, paper 26-28.

[4] Abu-Srhan .A , Al Daoud .E, "A Hybrid Algorithm Using a Genetic Algorithm and Cuckoo Search Algorithm to Solve the Traveling Salesman Problem and its Application to Multiple Sequence Alignment ", International Journal of Advanced Science and Technology Vol.61, 2013 , pp.29-38.

[5] Jenna Carr, "An Introduction to Genetic Algorithms" , 30 May 2014.

[6] Tsoumakas, I.Katakis, I. Vlahavas, "Mining Multi-label Data" , 2010, pp 667-685.

[7] A. Elisseeff, J. Weston, "A kernel method for multi-labelled classification", in: Proceedings of the 14th Conference on Neural Information Processing Systems (NIPS2001), Vancouver, British Columbia, Canada, 2001, pp. 681-687.

[8] Tsoumakas, Multi-label data sets, 2009 /http://mulan.sourceforge.net/datasets.htmlS.

VEHICLE TRACKING USING LOCALLY WEIGHTED PROJECTION REGRESSION METHOD

[1]Shakila basher, [2]Purushothaman S., and [3]Rajeswari P.
[1]Research Scholar, Department of MCA, VELS University, Chennai, India.
[2]Associate Professor,
[3]Lecturer, Department of Electrical and Computer Science Engineering,
[23]Institute of Technology, Haramaya University, DireDawa, Ethiopia

Abstract

This paper presents the method of tracking vehicle in video frames using Locally weighted projection regression (LWPR). The coordinates of the segmented vehicle image are presented to the LWPR. Based on the coordinates of the previous video frames, the LWPR estimates the next position of the vehicle. The LWPR is trained with coordinates of the vehicle obtained from few frames. Based on the learned information the next movement of the vehicle is estimated without processing next few video frames.

1. Introduction

Vehicle tracking is an important area that is very much useful for tracking vehicles from helicopters, tracking the movement of objects from remote sensing, tracking the movement of vehicles on the road in a crowded traffic environment. To achieve, the tracking pre-processing of images have to be carried out. This includes identifying the presence of vehicles in a frame, identifying frames that do not have vehicles images, identifying non-vehicle images that can be anything from the road to post lamp. Image processing plays an important role in processing the frames of the video, and proving with the presence of the vehicle in a frame.

2. Related work

The object tracking in video processing is an important step to tracking the moving objects in visual-based surveillance systems and represents a challenging task for researchers [Porikli and Yilmaz, 2012]. To track the physical appearance of moving objects such as the vehicles and identify it in dynamic scene, it has to locate the position, estimate the motion of these blobs and follow these movements between two of consecutive frames in video scene

[Rhee, 2004]. Several vehicle tracking methods have been illustrated by several researchers for different issues; it consists of:

1). Region-Based Tracking Methods.

2). Contour Tracking Methods.

3) 3D Model-Based Tracking Methods.

4). Feature-Based Tracking Methods.

5). Color and Pattern-Based Methods.

Gupte et al., 2002, introduced a model-based automobile recognizing, tracking and classification that is efficiently working under most conditions. The model provides position and speed knowledge for each vehicle as long as it is visible, also, this model works on series of traffic scenes recorded by a stable camera for automobiles monocular images. The processing algorithms of this model represent of three levels: raw images, region level, and vehicle level.

Jin-Cyuan, 2010, introduced a traffic criterions assessment such as vehicles numbering and classification involving with a suggested traffic observation scheme. The scheme demonstrated in its work the feature ratio and density to classify vehicles, also, it used the geometric traits to eliminate the false regions and for more accurate segmentation process is used the shades elimination algorithm.

Koller, 1994, stated that contour tracking methods depend on contours of the vehicle in tracking vehicle process. Ambardekar, 2008, used real-time traffic supervision approach that employs optical movement and uncalibrated camera parameter knowledge to detect a vehicle pose in the 3D world. The approach uses two techniques: color contour based matching and gradient-based matching, and it showed results when it tested for tracking, foreground object detection, vehicle recognition and vehicle speed assessment methods.

A real-time vehicles tracking and classification technique on the highway is useful. A few traffic criterions are extracted by the above technique. Also, the technique supports the occlusion detection and tracking that cause from multiple vehicles poses in the crowding situation. The method uses the Kalman filter, background [Monnet, 2003] differencing methods and morphological operations for extraction and recognition vehicle's contour.

In the 3D Model-Based Tracking Methods, Yung and Lai, 1998 presented an occlusion detection approach based on the generalized deformable model. The occlusion of vehicles detection process use a 3D solid cuboid form with up to six vertices, and this cuboid used to fit any different types and sizes of vehicle images by changing the vertices for the best fit.

Hsieh, 2006, used feature-based tracking methods using a linearity feature technique, which is a line-based shade method that uses lines groups to remove all undesirable shades. The method undertakes well the occlusion resulting from shades. This method represented an automatic vehicle tracking and classification traffic observation system.

In color and pattern-based tracking method Mao-Chi and Shwu-Huey, 2004, analyzed colors of image series in traffic supervision. The technique uses the YCrCb color space for the construction preliminary background, segmenting foreground, vehicle location, vehicle tracking, shade elimination, and background updating algorithms that used the system.

The limitation of the camera in vehicle tracking is as follows:

1. The camera can cover only small distance because of factors such as road configuration (e.g., elevation changes, curvature, and overhead or under pass structures), congestion level, vehicle mix, and inclement weather vertical and lateral viewing angles.
2. The number of lanes observed.
3. Stability with respect to wind and vibration, and image quality.

3. Methodology

LWPR involves projection regression to find mapping of input data with output data. Locally Weighted Projection Regression (LWPR) is an algorithm that achieves nonlinear function approximation in high dimensional spaces even in the presence of redundant and irrelevant input dimensions. At its core, it uses locally linear models, spanned by a small number of univariate regressions in selected directions in input space. This nonparametric local learning system

i) learns rapidly with second order learning methods based on incremental training,

ii) uses statistically sound stochastic cross validation to learn,

iii) adjusts its weighting kernels based on local information only,

iv) has a computational complexity that is linear in the number of inputs, and

v) can deal with a large number of-possibly redundant & irrelevant–inputs.

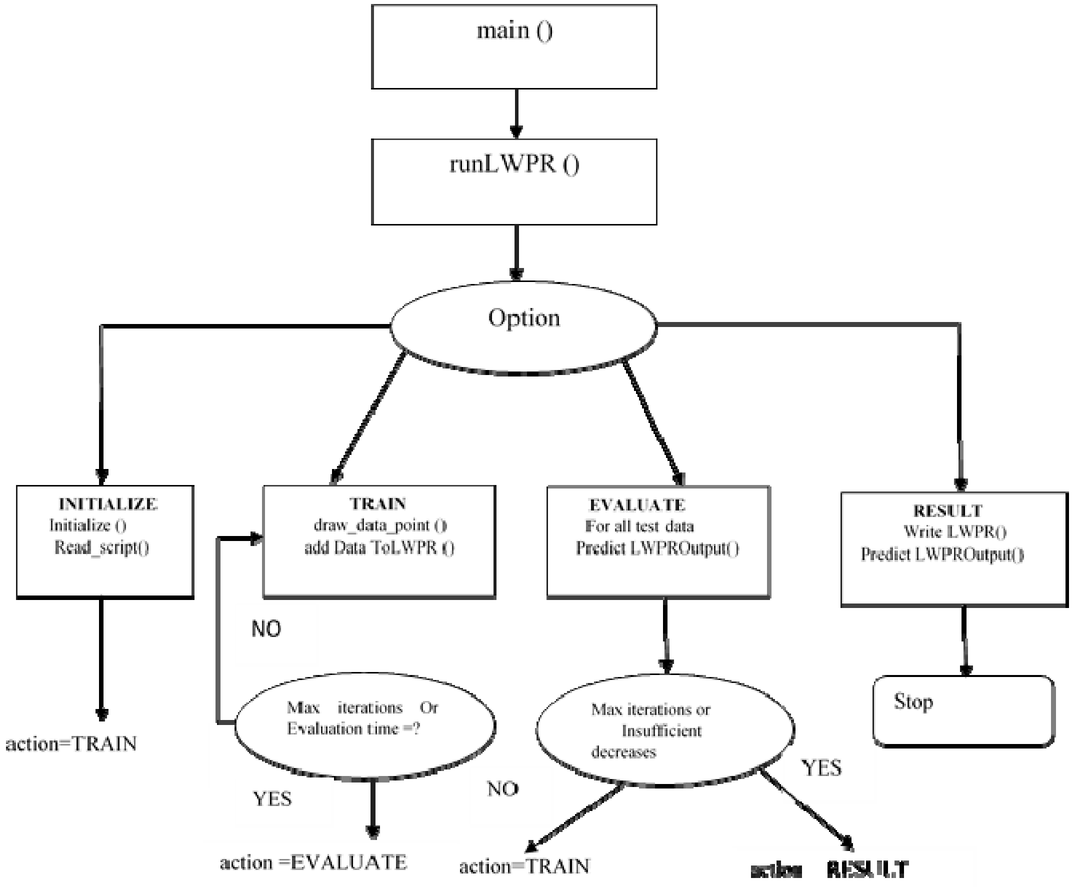


Fig.1 Flowchart of Locally Weighted Projection Regression

Figure 1 indicates general flow chart for implementing the LWPR algorithm.

4. Results and discussions

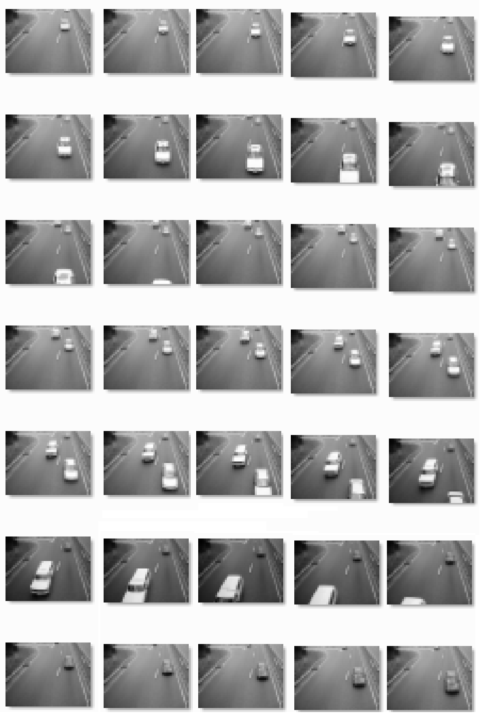


Fig.2 Sample video frames

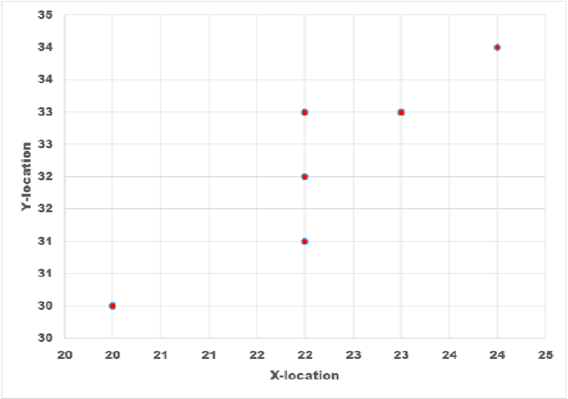


Fig.3 x-y coordinates of a vehicle

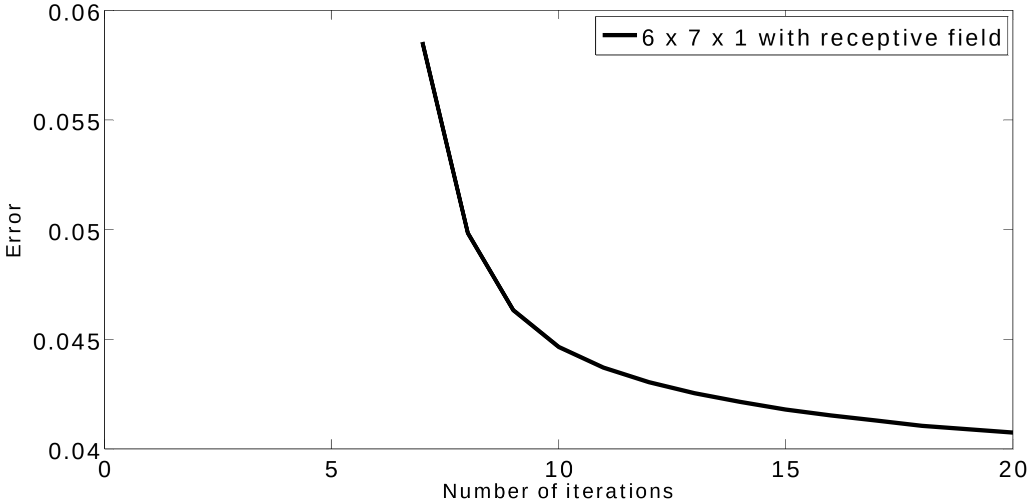


Fig.4 Error for learning x-y coordinates error

Figure 4 shows error while training the LWPR for x-y-difference vector. The convergence rate comes close to 0.022 in more than 25 iterations.

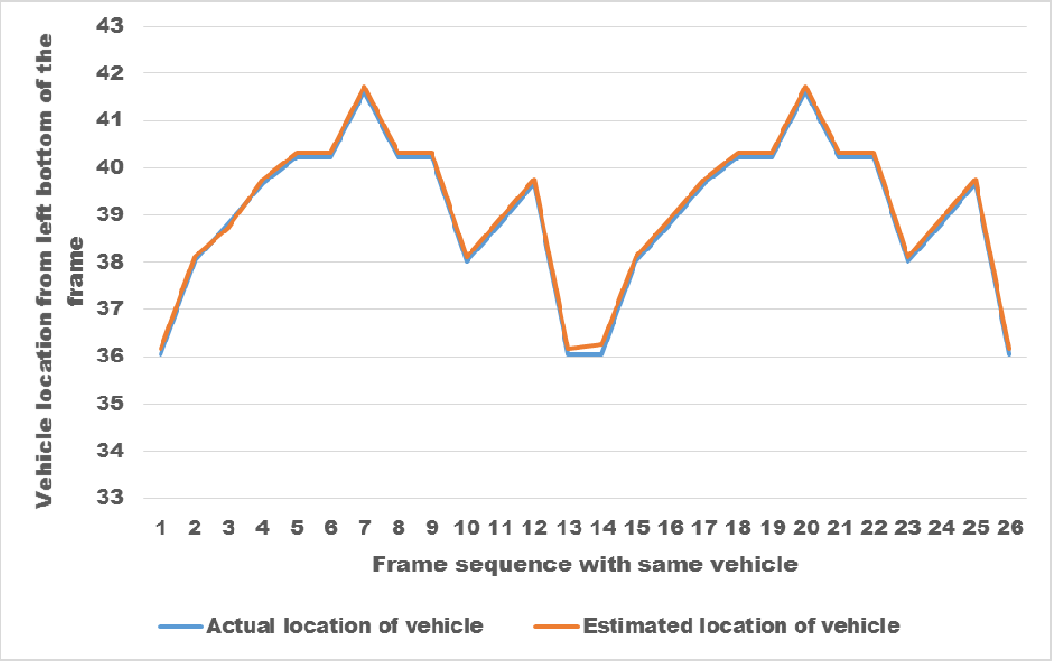


Fig.5 Estimation of vehicle location by LWPR

Figure 5 presents the actual location of the vehicle in the frame and the estimated location by LWPR. In this limited frames, the LWPR performs best in estimation.

5. Conclusion

In this work, the segmented vehicle images are considered. The x,y coordinates of the frames were used as input data for training the LWPR algorithm. The final weights obtained after training the LWPR has been used for estimating the next vehicle position the subsequent vide frames.

References

[1] Ambardekar A., 2008, Efficient Vehicle Tracking and Classification for an Automated Traffic Surveillance System, in International Conference on of Signal and Image Processing, pp.1-6.

[2] Gupte S., Masoud O., Martin R.F.K., and Papanikolopoulos N.P., 2002, Detection and classification of vehicles, IEEE Transactions on Intelligent Transportation Systems, Vol.3, No.1, pp.37–47.

[3] Hsieh J.W., 2006, Automatic traffic surveillance system for vehicle tracking and classification, Intelligent Transportation Systems, IEEE Transactions on, Vol.7, pp.175-187.

[4] Jin-Cyuan L., 2010, Image-based vehicle tracking and classification on the highway, International Conference in Green Circuits and Systems (ICGCS), 2010, pp.666-670.

[5] Koller D., 1994, Towards robust automatic traffic scene analysis in real-time, in Decision and Control, Proceedings of the 33rd IEEE Conference on, Vol.4, pp.3776-3781.

[6] Mao-Chi H., and Shwu-Huey Y., 2004, A real-time and color-based computer vision for traffic monitoring system, in Multimedia and Expo, 2004. ICME '04. 2004 IEEE International Conference on, Vol.3, pp.2119-2122.

[7] Monnet A., 2003, Background Modeling and Subtraction of Dynamic Scenes, presented at the Proceedings of the Ninth IEEE International Conference on Computer Vision – Vol.2.

[8] Porikli F., and Yilmaz A., 2012, Object Detection and Tracking, Springer Berlin Heidelberg in Video Analytics for Business Intelligence. Vol.409, pp.3-41.

[9] Rhee S., 2004, Vehicle Tracking Using Image Processing Techniques, in Rough Sets and Current Trends in Computing, Vol.3066, S. Tsumoto, et al., Eds., ed: Springer Berlin Heidelberg, pp.671-678.

[10] Yung N.H.C. and Lai A.H.S., 1998, Detection of vehicle occlusion using a generalized deformable model, in Circuits and Systems, ISCAS '98. Proceedings of the 1998 IEEE International Symposium on, Vol.4, pp.154-157.

Multilevel Extensible and Dynamic of Mobile Establishment Concepts

AMMAR ES-SAID
University Hassan II/ Faculty of Science Ben M'sik,
Casablanca Morocco
Department of Mathematics and Computer,

LABRIJI EL HOUSSINE
University Hassan II/ Faculty of Science Ben M'sik,
Casablanca Morocco
Department of Mathematics and Computer,

***Abstract* -- Mobile establishment of masts is an exclusive competence a control power, basically regarding town planning, mobility characterizes what could move or be moved, which can change place, this multilevel extensible, dynamic notion intuitive the activity however by three different aspects, and as many approaches, 'nomadisme', ubiquity, the sensitive system in context, nevertheless the use of these devices remains immersive, these devices requires all the attention, independently from this one.**

This approach is often called 'nomasime', although this term can take different significance in other fields to find proximity, In ray of influence that remains to be determined, mobility is in fact related to features of the increasing data of the computing mobile.

***Keywords* -- mobility, extensible, mobile devices, WPAN, mobile failures, wired, Mobile Technology**

I. INTRODUCTION

The mobile establishment carried out in wireless networking and the mobile terminals arouses Growing interest in computing .Moreover, the human being is characterized by his nomadisme, He seems to be the first to have left his original land and gradually inhabited the different continents .We do not want to return to the history of humanity, but just to underline that the human being is by nature nomad. Nowadays, this ambition of nomadisme is not only related to a burning desire of social advancement but also a new professional version. In matter in fact, in his professional entourage the human being uses daily different *, thus a new paradigm appeared, known by the name of mobile computing.

Mobile computing offers a flexible mechanism of communications between users and an access to the group of services normally available in a classical environment through a network, independently from physical (geographical) localization and the user's movements.

II. MOBILE COMPUTING PROBLEMS

The problems related to the mobile computing, and more specifically the once related to wireless networks and to mobile terminals. We try to characterize the impact of these problems on the applications distributed, the algorithm and the protocols from a network and system point of view. We limit ourselves to major mobile computing problems by demonstrating that all these problems converge toward the problem of disconnection which is the object of this thesis.

Mobile computing is particularly influenced by the limitation of the variation of the bandwidth,

These two characteristics introduce deadlines of data transition in the network. These deadlines degrades the performance of the applications we have, for example, the time constraints such as the multimedia interactive of the videoconferencing type, in the mobile environments, the variety of the bandwidth can be ,for example, the result of a change of the network at the time of the passage of a high-speed wireless network toward a network a very low flow, this variety can also be a result of the degradation of the signal because of obstacles (building, tunnels…).

The applications distributed risk never functioning correctly in the presence of disconnection unfortunately the disconnections are frequent events in the mobile environment and should not be treated like failures and the applications distributed must function in the presence of disconnections as normally as possible, this requires mechanisms that must bring an added value that differentiates the applications and the systems for mobiles environment compared to those conceived for the telegraphic environment

Otherwise, the mobile terminals become increasingly powerful in terms of resources offered, however these resources present performances which are far from reaching the performances of the fixes terminals ,in fact for a terminal to be mobile it must be light and in a small size, these characteristics limit the of storage capacity ,of the treatment and visualization.

III. THE STRONG POINTS IN MOBILE TECHNOLOGY

Wireless networks: in which at least two terminals can communicate without telegraphic connection, The wireless networks are based on a connection that uses radio waves instead on ordinary cables, the installation of such networks does not demand heavy installations of the existing

Google scholar
https://sites.google.com/site/ijcsis/
ISSN 1947-5500

infrastructure as in the case of the telegraphic networks (trenching to convey the cables, equipment of buildings in wiring ,chutes and connectors) which was worth the fast development of this kind of technologies.

The geographical perimeter defining the extent of wireless net wors make it possible to distingu is sevral categories, the wireless networks, personal, local, metropolitan extended set

Wireless personnel network (WPAN): Concerning the wireless networks with a weak range (about a few tens of meters).this type mainly used to connect peripherals to a computer without a telegraphic connections ,several technologies are used for the WPAN which the principal of is the Bluetooth technology ,having the advantage of being far from greedy in terms of energy use, which make it adaptable for a use with small peripherals

IV. Mobiles terminals

The first mobile terminals were introduced with a CT technology, to replace telegraphic telephones; these terminals were in reality the beginning of a technology that does not only influence the telephones but also the personal computers ,the mobiles terminals are characterized with the resources offered, the obstruction, autonomy and the possible extensions, these characteristics allow choosing mobile terminals ,a voluminous mobile terminal offers more resources, but it consumes more energy which induces a weak autonomy, on the other side a smaller and lighter mobile terminal offers less resources but allows a good autonomy the extensions represent a considerable factor to the choice of a terminal mobile, thus, several configuration and architectures can contribute to improve their liability of the mobile terminals with the aim of meeting the requirements with the end-users on the market

V. Conclusion

The concept of mobile computing the use of wireless communication technologies, allowed the appearance of new systems of communication that offers more advantages compared to the classical systems, the new systems do no compel the user with a fixed localization, but it allows him a free mobility.

The mobile environments are characterized by the variability of the band-width network and the restrictions on the resources uses, especially if all the users of the system are mobile.

REFERENCES:

[1] Y. Zhu, T. Chen, S. Liu, “Models and Analysis of Trade-offs in Distributed Network Management Approaches”, ISBN 0-7803-6719-7 IEEE 2001. pp 391-404.

[2] Josep L. Marzo, Pere Vilà , Lluís Fàbrega, Daniel Massaguer, “A Distributed Simulator for Network Resource Management Investigation”, In Computer Communications Journal - Special issue on Recent Advances in Communications Networking, Volume 26, Issue 15 , September 2003, Pages 1782-1791

[3] N.R. Jennings, “An Agent-Based Approach for building complex software systems”, Communications of the ACM, Vol.44 No.4, pp.35-41, 2001.

[4] Bigham J., Cuthbert L.G., Hayzelden A.L.G., Luo Z., “Multi-Agent System for Network Resource Management”, International Conference on Intelligence in Services and Networks, IS&N'99, Barcelona (Spain), April 1999.

[5] ASAKA, M., OKAZAWA, S., TAGUCHI, A. AND GOTO, S., A method for tracing intruders by use of mobile agents, INET’99, June 1999.

[6] WANG, W., BEHERA, S. R., WONG, J., HELMER, G., HONAVAR, V., MILLER, L., LUTZ, R., AND SLAGEL, M., Towards the Automatic Generation of Mobile Agents for Distributed Intrusion Detection System, Journal of Systems and Software, 79 2006, pp. 1–14

[7] Chen, H., Finin, T., Joshi, A.: An Ontology for Context-Aware Pervasive Computing Environments. Special Issue on Ontologies for Distributed Systems, Knowledge Engineering Review (2003)

Forensic Investigation of User's Web Activity on Google Chrome using Open-source Forensic Tools

Narmeen Shafqat
Dept of Information Security, MCS
National University of Science and Technology
Rawalpindi, Pakistan

Baber Aslam
Dept of Information Security, MCS
National University of Science and Technology
Rawalpindi, Pakistan

Abstract— **Cyber Crimes are increasing day by day, ranging from confidentiality violation to identity theft and much more. The web activity of the suspect, whether carried out on computer or smart device, is hence of particular interest to the forensics investigator. Browser forensics i.e forensics of suspect's browser history, saved passwords, cache, recent tabs opened etc. , therefore supply ample amount of information to the forensic experts in case of any illegal involvement of the culprit in any activity done on web browsers.**

Owing to the growing popularity and widespread use of the Google Chrome web browser, this paper will forensically analyse the said browser in windows 8 environment, using various forensics tools and techniques, with the aim to reconstruct the web browsing activities of the suspect. The working of Google Chrome in regular mode, private "Google Incognito Mode" and portable modes of operation is discussed at length in this paper.

Keywords—**Browser forensics, Private web browsing, Chrome Incognito, Chrome forensics, Portable browser forensics, Chrome artifacts.**

I. Introduction

Internet has become the need of hour today. According to the Internet Live Stats (2015), 40% of the world's population uses internet daily for a couple of tasks involving browsing internet for information or entertainment, social networking, email, e-commerce, gaming, blogging, banking etc. With such large number of internet users throughout the world, the number of cyber criminals has also come to a rise. Where the good guys benefit a lot from the internet, the bad guys also use it to carry out cyber-attacks, communicate with their peers, search for attack methods, preparing themselves for the crime etc.

It is interesting to note that, from the websites visited, to the items downloaded, every web activity of the user gets stored on his device. Even a single word searched by the user leaves its trace somewhere in his computer and thus can be obtained by the forensic analyst if he/she carries out forensic analysis of the suspect's browser. Thus, browser forensics supply ample amount of information to the forensic experts in case of illegal involvement of the culprit in any activity done on web browsers.

Forensic Experts should therefore have full grasp on not only the forensic analysis of well-known and well acknowledged browsers like Internet Explorer, Google Chrome, Mozilla Firefox, Safari, Opera etc. but should also have hands on experience of less popular web browsers like Erwise, Arena, Cello, Netscape, iCab, Cyberdog etc. Not only this, the forensic experts should also know how to find artifacts of interest from older versions of well-known web browsers; Internet Explorer, Chrome and Mozilla Firefox atleast, because he might experience a case where the suspected person is using older versions of these browsers.

According to StatCounter Global market share for the web browsers (2015), Google Chrome, Mozilla Firefox and Microsoft's Internet Explorer make up 90% of the browser usage.

Owing to the growing popularity of the Google Chrome web browser, having 48.71% of the web browser share alone, this paper will move around this web browser. The forensic analysis of Google Chrome, as carried out on HP Pavilion laptop running Windows 8 OS, in normal/regular, private (incognito) and portable modes of operation is discussed at length in this paper, to help the forensic investigators in investigations relating to web browsers.

Various open-source forensic tools have been used throughout the research to provide maximum amount of human readable information to the forensic investigator/ practitioner, as retrieved from the Google Chrome's default files and folders. The results have been tested with different forensic softwares/ tools to ensure the validity and accuracy of the obtained forensic results.

II. Literature Review

Current research in the field of browser forensics targets the stored files of widely used web browsers notably Google Chrome, Internet Explorer, Mozilla Firefox, Safari and Opera to extract data of interest. Emphasis nowadays is also laid on the structural analysis of internet log files from a forensic point of view to gather traces of the internet habits of the suspect under investigation.

Where the web browser vendors endeavor to provide safe and secure browsing features to its customers, the forensic researchers are trying hard to dig out methods to combat these anti-forensics attempts on the web browsers and reveal more and more internet activity of the user that gets stored on the disk even in the private or portable web browsing mode of operation.

A number of freeware tools exist on the internet for carrying out the forensic analysis of the web browser's history, cache, cookies, login data files etc. Most of the tools however, target only a single web browser and cannot create a real picture of the case if the culprit uses more than one web browser on his device.

Since the scope of the research is confined to the forensic analysis of Google Chrome only, we assume that the suspect uses only Chrome on his computer, and thus the available open source Chrome analysis tools are sufficient to analyze the case forensically.

A. *Basics of Google Chrome*

Google Chrome, is the fastest and most used web browser in the world today. For Windows 8, Chrome stores its files and database in the following default locations in C drive. C:\Users\[USERNAME]\AppData\Local\Google\Chrome\UserData\Default.

The folder contains files of our interest i.e. Bookmarks, Cookies, Current Tabs, History, Last tabs, Login Data, Preferences, Top Sites and Web Data. These web browsing artifacts are stored in SQLite, SNSS (Session Saver) and JSON (Java Script Object Notation) formats. The structure of the DB file is quite different from that of other renowned browsers e.g. Mozilla Firefox. (Russ Taylor, 2014).

Google Chrome stores the timestamps in Webkit format i.e. number of microseconds passed since 00:00:00 UTC of Jan 1, 1601. (Junghoon, Seungbong & Sangjin, 2011). However, some of the Chrome files have also been observed to follow a flavor of the Windows File time, which is basically 100 nano-second intervals since January 1, 1601 UTC, divided by factor 10. For examination, any Chrome time decoder e.g. DCode etc. can be used by the forensic investigator to convert the timings given in history files to the desired format.

B. *Google Chrome's Web Browsing Mode*

Chrome web browser works in the following modes:

- Regular Mode: It is the default mode that is most commonly used. It stores entire user's activity on disk.
- Private Mode: This mode is designed to give user privacy while surfing the Internet. It does not keep a track of all of the user's activity.
- Portable Mode: The mode allows user to install a portable web browser on a USB or cloud media, and run it on any PC. It provides the user portability to keep his browser files, websites' passwords etc. with him all the time.

III. Chrome Browser Forensics: Preparation and Procedure

Forensic research in this paper is carried out on HP Pavilion laptop running Windows 8. Chrome 40 was installed on the PC for experimenting with regular and private mode of operation. It was made sure that Chrome is in use for more than one week, so that abundant amount of information is present to carry out its forensic analysis. However, for portable mode forensics, Goggle Chrome Portable Application was installed in USB and the experiment was repeated.

In general, the investigation methodology depends largely on the OS installed on suspected PC, the web browser under investigation, the type of evidence etc. One way to analyze the browser forensically is to take the image of the hard drive, select some user's search words from the history file, and use FTK Live Search option to search those keywords in the imaged drive. The data can then be authenticated using CRC (cyclic redundancy check), SHA-1 (Secure Hash Algorithm) or MD-5 (Message Digest Algorithm).

The second approach for browser forensics is to open each file present in the Default Chrome folder and analyze it separately for internet evidences using various forensic tools and techniques. Then, validate all the results with alternative open source tools too, if proprietary softwares have not been used in the investigation. This subsection however attempts to find artifacts using the second method. However, methodology 1 has also been used in the paper.

Well for any methodology, it is important for the forensic team to know where he can find the data of his interest, for reconstructing the culprit's web browsing activity, as shown in Table 1.

TABLE 1. WHERE TO FIND CHROME CONTENTS

Content	Found in (File/ Folders)
Websites visited	History, Cache, Cookies, Recovery Folders, Suggested Sites
Visit count	History
Visit time	History, Cookie, Cache, Recovery Folders
Search Words	Auto Complete, Cache
Downloads	Downloads, Cache
Sites saved	Bookmarks

The forensic investigator must be equipped with a good collection of various open-source and proprietary browser forensics tools before starting the investigation. Table 2 below enlists the softwares that will be used for forensic analysis of Google Chrome in this paper.

TABLE 2. WEB BROWSER FORENSIC TOOLS

Forensics Tool	Contents analyzed
Phrozen Browser Forensics Tool	Scans browser's history and keywords
History Viewer	History, Top sites, Cookies, Keyword, Downloads,
MyLastSearch	Search queries
ChromeCookie View	Cookies
Chrome Password Decryptor	Decrypts password
ChromeCache View	Cache
Internet Evidence Finder	Internet artifacts from unallocated space, default folders, pagefile.sys, hiberfil.sys
Cookie Cutter	Google Analytics cookies, Search terms
Chrome Analysis	History, Bookmarks , Cookies, Search words, Downloads

Chrome Session Parser	Current and last sessions and tabs
Web Historian	History

The forensic investigator while investigating any case involving web browser or any other illegal internet activity, should proceed with the following steps. (Newman, 2007).

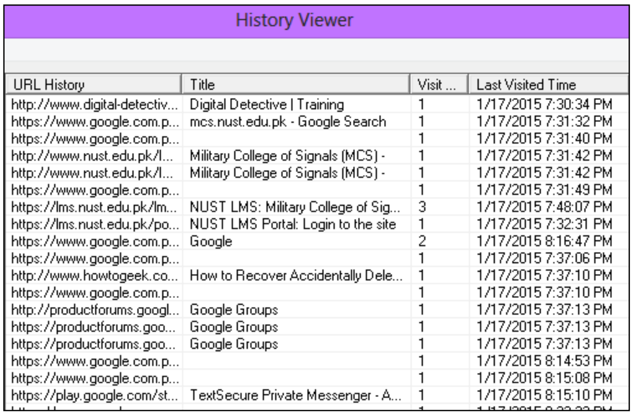
- Precisely define the scope of the investigation,
- Maintain a detailed log of investigation activities,
- Secure the computer/ laptop under investigation, Document the peripherals attached, hardware and software configurations of the system,
- Connect a software or hardware write blocker to the PC, to prevent accidental damaging of any kind of potential evidence. Take snapshot or print any result that shows internet-abuse,
- Preserve any data opened on PC, and the time stamps,
- Run "Phrozen Browser Forensics Tool" to identify the web browser that the suspect uses most. This tool scans the history of widely known web browsers and provides statistics according to the browser usage,
- If the browser is opened, check whether you can view Incognito sign or recent tabs in the Chrome Menu. Presence of sign and absence of recent tabs both indicate that the private mode has been enabled. In that case first collect the evidence from Chrome's own settings bar before the session expires. Also collect Chrome's default files and folder for further analysis. However, incase the browser is running in regular/ normal mode, simply collect all the default files and folders and analyze them using forensic tools.
- If browser is closed, simply collect files from the default folder. The absence of URL name for even some of the results, indicate the usage of private web browsing mode by the suspect. Else it is evident that the user uses Chrome in normal/ regular mode,
- Check registry entries for the USB devices connected to the computer so far and determine whether portable mode was enabled or not. If Chrome has been used in portable mode, trace the residual artifacts in the computer,
- Also search File slack space, Swap Files, Pagefile.sys, Hyberfil.sys, $Logfile, Volume shadow copies, Unpartitioned space, Uninitialized file area, Unallocated clusters, $mft, etc. for trace of Internet activity.
- Validate all results with alternative open source tools, if proprietary softwares have not been used in the investigation,
- Present your findings.

IV. Chrome's Forensics in Regular Mode

This section will discuss the analysis of the artifacts stored on disk in the Regular Browsing mode from the forensic point of view. Chrome version 40 was installed on the laptop running Windows 8. This section covers the forensic analysis of Google Chrome by opening the files present in the Default Chrome folder i.e. History, Cookies, Bookmarks, Top Sites, WebData, Shortcuts etc., separately in various forensic tools and analyzing them for required internet evidences.

A. History:

The History file found in the ../Chrome/Default/History folder is basically a database file that contains record of user's all web history. It contains tables for downloads, visits, urls, segment_usage, keyword_search_terms, meta, presentation, and segments, that provide useful information to the forensic experts about the victim's web activity. The forensic investigator can simply use History Viewer tool to open the History file present in the Chrome Default folder. The software makes search easy for the investigator as seen in the Figure 1 below.

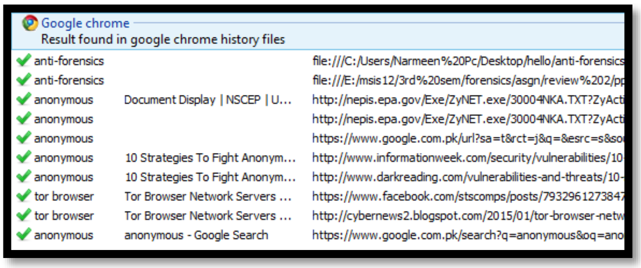


History Viewer

URL History	Title	Visit ...	Last Visited Time
http://www.digital-detectiv...	Digital Detective | Training	1	1/17/2015 7:30:34 PM
https://www.google.com.p...	mcs.nust.edu.pk - Google Search	1	1/17/2015 7:31:32 PM
https://www.google.com.p...		1	1/17/2015 7:31:40 PM
http://www.nust.edu.pk/l...	Military College of Signals (MCS) -	1	1/17/2015 7:31:42 PM
http://www.nust.edu.pk/l...	Military College of Signals (MCS) -	1	1/17/2015 7:31:42 PM
https://www.google.com.p...		1	1/17/2015 7:31:49 PM
https://lms.nust.edu.pk/lm...	NUST LMS: Military College of Sig...	3	1/17/2015 7:48:07 PM
https://lms.nust.edu.pk/po...	NUST LMS Portal: Login to the site	1	1/17/2015 7:32:31 PM
https://www.google.com.p...	Google	2	1/17/2015 8:16:47 PM
https://www.google.com.p...		1	1/17/2015 7:37:06 PM
http://www.howtogeek.co...	How to Recover Accidentally Dele...	1	1/17/2015 7:37:10 PM
https://www.google.com.p...		1	1/17/2015 7:37:10 PM
http://productforums.googl...	Google Groups	1	1/17/2015 7:37:13 PM
https://productforums.goo...	Google Groups	1	1/17/2015 7:37:13 PM
https://productforums.goo...	Google Groups	1	1/17/2015 7:37:13 PM
https://www.google.com.p...		1	1/17/2015 8:14:53 PM
https://www.google.com.p...		1	1/17/2015 8:15:08 PM
https://play.google.com/st...	TextSecure Private Messenger - A...	1	1/17/2015 8:15:10 PM

Figure 1. History file opened in History Viewer

To speed up the investigation, instead of looking for evidences in whole history file, forensic investigator can use *Browser Forensic* tool, to make up a list of keywords that he needs to search for in the history and start scan. Figure. 2 below shows part of keyword list generated for a sample search.



Google chrome
Result found in google chrome history files

✓	anti-forensics		file:///C:/Users/Narmeen%20Pc/Desktop/hello/anti-forensics
✓	anti-forensics		file:///E:/msis12/3rd%20sem/forensics/asgn/review%202/pp
✓	anonymous	Document Display | NSCEP | U...	http://nepis.epa.gov/Exe/ZyNET.exe/30004NKA.TXT?ZyActi
✓	anonymous		http://nepis.epa.gov/Exe/ZyNET.exe/30004NKA.TXT?ZyActi
✓	anonymous		https://www.google.com.pk/url?sa=t&rct=j&q=&esrc=s&so
✓	anonymous	10 Strategies To Fight Anonym...	http://www.informationweek.com/security/vulnerabilities/10
✓	anonymous	10 Strategies To Fight Anonym...	http://www.darkreading.com/vulnerabilities-and-threats/10-
✓	tor browser	Tor Browser Network Servers ...	https://www.facebook.com/stscomps/posts/793296127384
✓	tor browser	Tor Browser Network Servers ...	http://cybernews2.blogspot.com/2015/01/tor-browser-netw
✓	anonymous	anonymous - Google Search	https://www.google.com.pk/search?q=anonymous&oq=ano

Figure 2. Search Results for specific keywords searched

Since open source tool has been used for the research, the forensic investigator can also view user's web history details and download information in *Chrome Analysis* tool to verify his results. The problem for the forensic investigator while investigating history files is that Google keeps each web history artifact for a period of three months only, after which it automatically gets deleted. The artifacts however do not get wiped off from the drive and are kept in archived history database. The forensic investigator can get the URL and download information from there, while the visit time gets expire. Hence it is difficult for the investigator to prepare timelines for evidences of cases more than three months old. (Craig Wilson, 2014)

B. *Search Keywords*

It is important for the forensic examiner to understand that the words searched by the user, on the web browser, simply get stored in the URL. Thus, if for instance, he comes across a URL say, http://www.google.com/search?hl=en&source=hp&q=chrome&aq=f&oq=&aqi=g10 then it means that the suspect used Google.com host to search for the variable q i.e. *Chrome* in this case. (Junghoon, Seungbong & Sangjin, 2011).

The recent search words of the suspect can be viewed by opening the Default Chrome folder in tool like MyLastSearch, History Viewer etc.

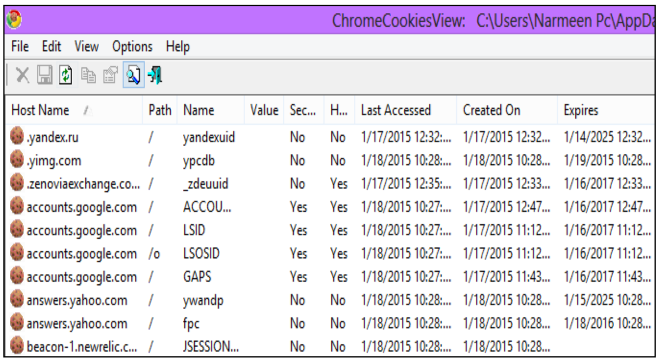
C. *Cookies*

Cookies are basically the SQL files, that websites create to store the users' browsing information such as his/her site preferences, location or personal profile information etc. Cookies also help analyze web traffic and are often necessary for website's functionality. The cookies are of two types; first party (set by site domain) and third party cookies (comes from sources that display items or adds on that particular page.)

Google Chrome stores its cookies in ../Chrome/ User Data/ Default folder. The users are given 5 options for cookies; allow, block, delete, make exception list, or keep cookies until the browser is open. Users, who do not wish to be tracked, must disable cookies. To view the cookies from Google Chrome, go to Chrome Menu > Settings > Show advance settings > Privacy section > All cookies and site data. This will open up the cookie console. Any cookie value when clicked opens up the dialog box showing name, content, domain, path, time of creation and expiration. For forensic investigator, detail as small as a cookie even helps progress the investigation because cookies prove that the user accessed that website at some time.

Since there is no fixed structure for cookies, forensic investigator may face problem analyzing them. The best solution for that is to use any cookie viewing tool like Cookie Spy or Chrome Cookie Viewer. Figure 3 below shows a snapshot of the Chrome Cookie Viewer when run on the target PC. It provides the name of the cookie, host name, path, HTTP use, creation date, last access date, expiry date and whether security feature is enabled or not.

Many websites nowadays, however use Google Analytics (GA) cookies. GA cookies are more structured than the standard HTTP cookies, and hence provides more authentic information regarding the user of that website, insight on how he found/ accessed that particular site, how many pages did he view and whether the user had established active session with the site before closing Google Chrome or not. (Nelson, 2012)



Host Name	Path	Name	Value	Sec...	H...	Last Accessed	Created On	Expires
.yandex.ru	/	yandexuid		No	No	1/17/2015 12:32:...	1/17/2015 12:32...	1/14/2025 12:32...
.yimg.com	/	ypcdb		No	No	1/18/2015 10:28:...	1/18/2015 10:28...	1/19/2015 10:28...
.zenoviaexchange.co...	/	_zdeuuid		No	Yes	1/17/2015 12:35:...	1/17/2015 12:33...	1/16/2017 12:33...
accounts.google.com	/	ACCOU...		Yes	Yes	1/18/2015 10:27:...	1/17/2015 12:47...	1/16/2017 12:47...
accounts.google.com	/	LSID		Yes	Yes	1/18/2015 10:27:...	1/17/2015 11:12...	1/16/2017 11:12...
accounts.google.com	/o	LSOSID		Yes	Yes	1/18/2015 10:27:...	1/17/2015 11:12...	1/16/2017 11:12...
accounts.google.com	/	GAPS		Yes	Yes	1/18/2015 10:27:...	1/17/2015 11:43...	1/16/2017 11:43...
answers.yahoo.com	/	ywandp		No	No	1/18/2015 10:28:...	1/18/2015 10:28...	1/15/2025 10:28...
answers.yahoo.com	/	fpc		No	No	1/18/2015 10:28:...	1/18/2015 10:28...	1/18/2016 10:28...
beacon-1.newrelic.c...	/	JSESSION...		No	No	1/18/2015 10:28:...	1/18/2015 10:28...	

Figure 3. Cookies opened in Chrome Cookie View

D. *Login Data*

This file in the ../Chrome/Default folder stores the login credentials of user for various websites. The file stores the URL of website, username, password, actual name, date of creation in plain text as record.

It is to be noted that Google Chrome leaves it upon the OS to secure the saved passwords. In most cases, the passwords will be stored in plain text. Figure 4 below shows the Login Data file present in ../Chrome/ UserData/ Default folder opened in a freely available SQLite DB browser.

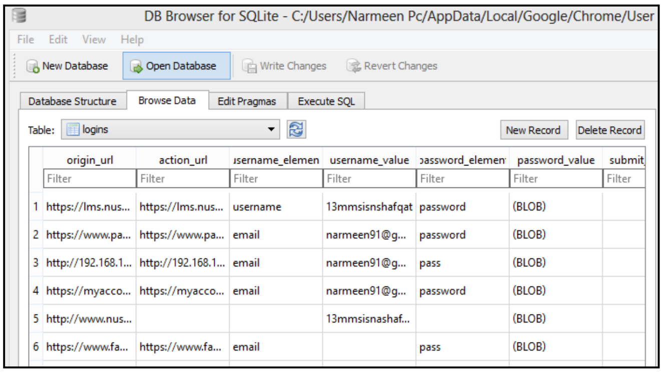
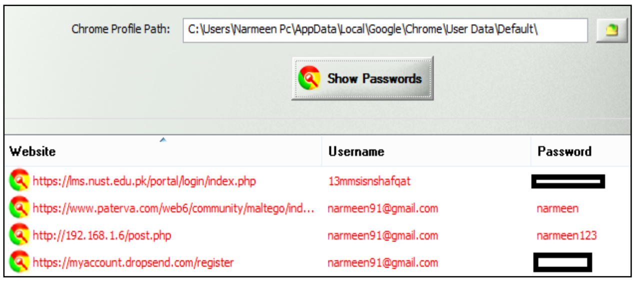


Table: logins

	origin_url	action_url	ısername_elemen	username_value	ɔassword_elemen	password_value	submit
	Filter	Filter	Filter	Filter	Filter	Filter	Filter
1	https://lms.nus...	https://lms.nus...	username	13mmsisnshafqat	password	(BLOB)	
2	https://www.pa...	https://www.pa...	email	narmeen91@g...	password	(BLOB)	
3	http://192.168.1...	http://192.168.1...	email	narmeen91@g...	pass	(BLOB)	
4	https://myacco...	https://myacco...	email	narmeen91@g...	password	(BLOB)	
5	http://www.nus...			13mmsisnashaf...		(BLOB)	
6	https://www.fa...	https://www.fa...	email		pass	(BLOB)	

Figure 4. Login Credentials opened in SQLite Viewer

However in some cases, the user's password is encrypted with triple DES algorithm, with the seeding input as the user's own login password. The user is prompted to type his master password to view the Chrome passwords. Figure 5 as seen below, shows part of Chrome Password Decryptor, that the forensic analyst may use to decrypt the encrypted Chrome password. (Securityxploded, n.d).



Chrome Profile Path: C:\Users\Narmeen Pc\AppData\Local\Google\Chrome\User Data\Default\

Website	Username	Password
https://lms.nust.edu.pk/portal/login/index.php	13mmsisnshafqat	[redacted]
https://www.paterva.com/web6/community/maltego/ind...	narmeen91@gmail.com	narmeen
http://192.168.1.6/post.php	narmeen91@gmail.com	narmeen123
https://myaccount.dropsend.com/register	narmeen91@gmail.com	[redacted]

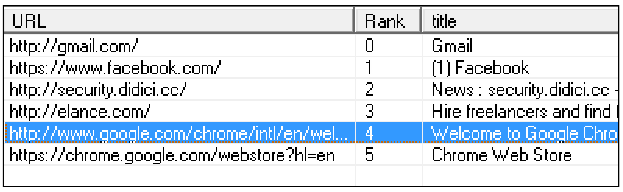
Figure 5. Chrome Password Decryptor

E. Shortcuts

The shortcuts are the guess words that might help the user while typing his search keyword in the URL bar. They will appear as suggestion to him, like fac for facebook.com, gm for gmail.com etc. The Shortcuts file can be viewed in SQLite DB Browser to reveal the shortcuts.

F. Top Sites

Top sites, or the sites most visited by the user can be viewed by opening the ../UserData/Default/Top Sites file in DB Browser for SQLite. It provides URL along with data_count etc. for the most viewed sites. However, "History Viewer" software can also show these details, as seen in Figure 6.



URL	Rank	title
http://gmail.com/	0	Gmail
https://www.facebook.com/	1	(1) Facebook
http://security.didici.cc/	2	News : security.didici.cc -
http://elance.com/	3	Hire freelancers and find
http://www.google.com/chrome/intl/en/wel...	4	Welcome to Google Chro
https://chrome.google.com/webstore?hl=en	5	Chrome Web Store

Figure 6. Top Sites file opened in History Viewer

G. Web Data

The Web Data Chrome file stores the login credentials and auto fill data of the Chrome users.

- The login credentials are only stored for the websites that the user has permitted to store the credentials for.

- The auto fill data is the data with which the user has already filled any web form with. Chrome stores this data for user's ease so that it may auto suggest the stored input when the user is about to fill the form. (Sarah, 2010)

Figure 7 shows snapshot of the WebData file from ../Chrome/UserData/Default folder opened in SQLite DB Browser.

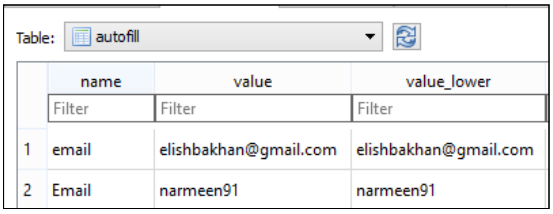


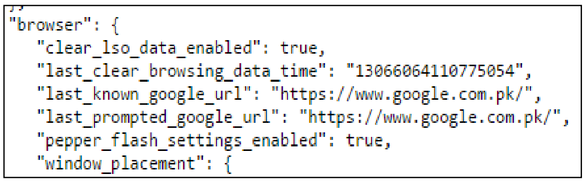
Table: autofill

	name	value	value_lower
	Filter	Filter	Filter
1	email	elishbakhan@gmail.com	elishbakhan@gmail.com
2	Email	narmeen91	narmeen91

Figure 7. WebData file opened in SQLite DB Viewer

H. Preferences

The Preferences file present in the ..Chrome/UserData/Default folder indicates the user's preferred settings for the Google Chrome web browser. The forensic investigator can simple open it in Chrome by double clicking on the file in the folder. Figure 8 shows part of the data of the Preferences file.



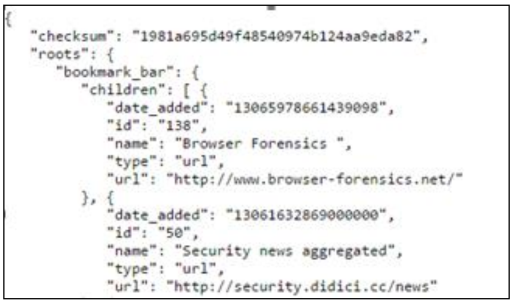
```
"browser": {
   "clear_lso_data_enabled": true,
   "last_clear_browsing_data_time": "13066064110775054",
   "last_known_google_url": "https://www.google.com.pk/",
   "last_prompted_google_url": "https://www.google.com.pk/",
   "pepper_flash_settings_enabled": true,
   "window_placement": {
```

Figure 8. Snapshot of Preferences file

I. Bookmarks

Bookmarks are URI's (Universal Resource Identifiers) that are basically the shortcuts to the favorite or saved pages. If the website has been bookmarked, the user doesn't need to remember the URL for opening it. Thus these bookmarks provide the forensic investigator idea of what kind of data or website does the user deems important. Bookmarked sites can be opened from the Chrome Menu > Bookmarks.

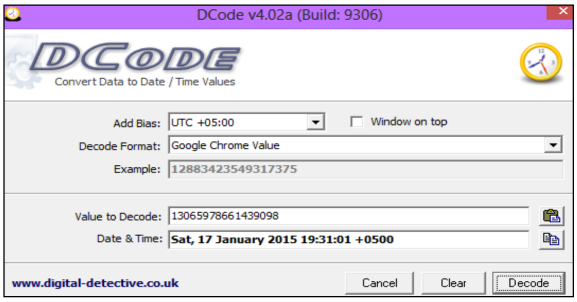
Bookmarks tab only shows the URL of the websites that the user has bookmarked. This information is insufficient for a forensic analyzer to determine which bookmarks are recent. He may therefore open the bookmarks file located in Chrome/ UserData/ Default folder in notepad or chrome to see other bookmark's parameters such as time of bookmarking, URL, type etc., as seen in Figure 9.



```
{
   "checksum": "1981a695d49f48540974b124aa9eda82",
   "roots": {
      "bookmark_bar": {
         "children": [ {
            "date_added": "13065978661439098",
            "id": "138",
            "name": "Browser Forensics ",
            "type": "url",
            "url": "http://www.browser-forensics.net/"
         }, {
            "date_added": "13061632869000000",
            "id": "50",
            "name": "Security news aggregated",
            "type": "url",
            "url": "http://security.didici.cc/news"
```

Figure 9. Chrome Bookmarks opened in Chrome

To interpret the date_added field as seen in figure 13, the forensic investigator may use Dcode Time decoder, or any other freely available decoder. Figure 10, shows the first date_added value converted to Pakistan standard time i.e. GMT+05.



DCode v4.02a (Build: 9306)

Convert Data to Date / Time Values

Add Bias: UTC +05:00

□ Window on top

Decode Format: Google Chrome Value

Example: 12883423549317375

Value to Decode: 13065978661439098

Date & Time: **Sat, 17 January 2015 19:31:01 +0500**

Figure 10. Chrome Time Decoding

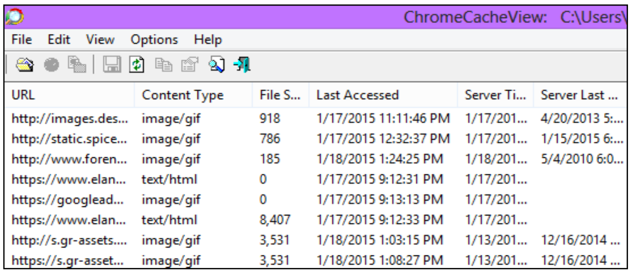
J. Bookmarks.bak

Bookmarks.bak file contains the recent backup of the Chrome bookmarks, since the user last launched it. It overwrites this backup every time the user launches the Google Chrome web browser.

Incase the suspect has deleted the bookmarks before running away from the crime scene, the forensic investigator can restore them by deleting the bookmarks file present in ../Chrome/UserData/Default folder and renaming the Bookmarks.bak file to Bookmarks. All previously deleted bookmarks will be restored to the bookmarks bar and can be viewed upon opening the web browser.

K. Cache

Cache transparently stores website's data so that future requests for that data can be served faster. The Chrome's Cache folder consists of an index file, four data files and another hex file. Figure 11 below shows the view of cache folder, as seen from the Chrome Cache Viewer tool.



URL	Content Type	File S...	Last Accessed	Server Ti...	Server Last ...
http://images.des...	image/gif	918	1/17/2015 11:11:46 PM	1/17/201...	4/20/2013 5:...
http://static.spice...	image/gif	786	1/17/2015 12:32:37 PM	1/17/201...	1/15/2015 6:...
http://www.foren...	image/gif	185	1/18/2015 1:24:25 PM	1/18/201...	5/4/2010 6:0...
https://www.elan...	text/html	0	1/17/2015 9:12:31 PM	1/17/201...	
https://googlead...	image/gif	0	1/17/2015 9:13:13 PM	1/17/201...	
https://www.elan...	text/html	8,407	1/17/2015 9:12:33 PM	1/17/201...	
http://s.gr-assets....	image/gif	3,531	1/18/2015 1:03:15 PM	1/13/201...	12/16/2014 ...
https://s.gr-asset...	image/gif	3,531	1/18/2015 1:08:27 PM	1/13/201...	12/16/2014 ...

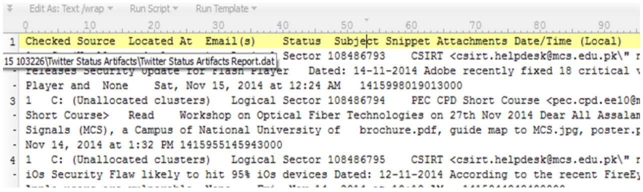
Figure 11. Cache file opened in Chrome Cache View

Clicking on them, open up a dialog box, revealing more information regarding the cached object, for instance URL, content type, file size, last accessed date and time, server time, expire time, server response, eTag, Cache Control etc.

L. Other Internet Artifacts

Part of the memory of computer's PC also stores artifacts/ message traces of web mailing and social networking sites like Facebook, Gmail, Yahoo etc. Therefore, the investigator must also look upon the pagefile.sys, hyberfil.sys, unallocated space, etc. for their artifacts too.

The *Internet Evidence Finder* software can be used by the forensic investigator to find traces of social networking apps, webmail services, mapping queries, instant messaging applications, cloud based services etc. from different memory locations including the pagefile.sys, hiberfil.sys, $mft, unallocated clusters etc. A search summary and scan, was conducted as part of research using the Internet Evidence Finder tool to find the left over internet artifacts. The results of the search summary can be seen in the figure 12 below.

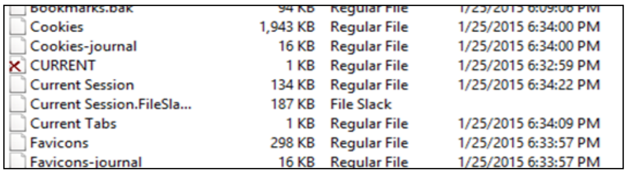


```
1  Checked Source  Located At  Email(s)    Status  Subject Snippet Attachments Date/Time (Local)
15 103226\Twitter Status Artifacts\Twitter Status Artifacts Report.dat Sector 108486793    CSIRT <csirt.helpdesk@mcs.edu.pk\" r
-  releases Security Update for Flash Player   Dated: 14-11-2014 Adobe recently fixed 18 critical v
-  Player and  None    Sat, Nov 15, 2014 at 12:24 AM   1415998019013000
3  1   C: (Unallocated clusters)   Logical Sector 108486794    PEC CPD Short Course <pec.cpd.ee10@m
-  Short Course>   Read    Workshop on Optical Fiber Technologies on 27th Nov 2014 Dear All Assalam
-  Signals (MCS), a Campus of National University of   brochure.pdf, guide map to MCS.jpg, poster.p
-  Nov 14, 2014 at 1:32 PM 1415955145943000
4  1   C: (Unallocated clusters)   Logical Sector 108486795    CSIRT <csirt.helpdesk@mcs.edu.pk\" r
-  iOs Security Flaw likely to hit 95% iOs devices Dated: 12-11-2014 According to the recent FireEy
```

Figure 12. IEF Scan Results

M. Deleted Chrome Data

If however the culprit/user deletes the browsing history from the Chrome Menu> Clear History, all the history files present in the memory gets deleted. However, the downloads, cookies, and cache files are initialized to zeroes. (Junghoon, Seungbong & Sangjin, 2011). The default folder when opened in Access Data FTK Imager showed deleted files with a red cross, as seen in the Figure 13 below.



Bookmarks.bak	94 KB	Regular File	1/25/2015 6:09:06 PM
Cookies	1,943 KB	Regular File	1/25/2015 6:34:00 PM
Cookies-journal	16 KB	Regular File	1/25/2015 6:34:00 PM
☒ CURRENT	1 KB	Regular File	1/25/2015 6:32:59 PM
Current Session	134 KB	Regular File	1/25/2015 6:34:22 PM
Current Session.FileSla...	187 KB	File Slack	
Current Tabs	1 KB	Regular File	1/25/2015 6:34:09 PM
Favicons	298 KB	Regular File	1/25/2015 6:33:57 PM
Favicons-journal	16 KB	Regular File	1/25/2015 6:33:57 PM

Figure 13. Deleted File shown in FTK Imager

In short, we observe that Google Chrome really stores a wealth of internet artifacts on the user's drive. Among all the files, the history file alone provides sufficient information to the forensic investigator to reconstruct the timeline of user's activity or at the least get the idea of his intention. The cached web pages not only provides user content of the sites visited by the suspect but also proves that the user has visited those particular sites. This observation is important in cases of child pornography, electronic fraud, non-repudiation cases etc. Moreover, the forensic investigator must also analyze the cookie's file to get the session ID of the user, top sites file to look for suspect's most visited sites, login data file to note suspect's credentials for various websites, etc. In terms of privacy, the regular mode of operation is not at all secure, since it stores almost all the surfing activity of the user on the hard drive. However, with the availability of various browser forensics tools in the market, the forensic investigation of web browsers has been made quite easy for the forensic investigators.

V. GOOGLE INCOGNITO (PRIVATE WEB BROWSER) FORENSICS

Like Chrome, other well-known web browsers also allow user to surf internet in Private mode. The private browsing feature of web browsers gives the user freedom of browsing the internet, without keeping any record of his browsing history, cookies, temporary Internet files, usernames/passwords, form data etc. The feature also helps prevent him from third party websites that usually track user's browsers activity. Thus, these types of browsing features tend to make the job of forensic expert or forensic investigator hard. (Donny & Narasimha, 2013)

For the user to start the private browsing in Chrome, press Chrome Menu > New Incognito window. Alternatively incognito window can be opened from Ctrl+Shift+N shortcut. The user can enjoy private browsing unless he himself turns it off.

A. Google Incognito providing false sense of security

From a logical view point, it does make sense that for the browser to function normally, even in the private mode, it needs to write some amount of useful data or commands/instruction to a portion of disk. Where is it written, and whether it gets deleted or not, is a million dollar question because Google do not provide any public specification document on Google Chrome's Incognito Mode Implementation. (Jessica, n.d).

Google Chrome does not store any web activity of the user who has enabled private browsing mode in his browser, but it certainly doesn't stop the operating system, websites and the router from keeping account of what the user do. Thus in reality, these web browsers give a false sense of security to the users, and do not completely guarantee the secrecy and privacy of the user's browsing activities.

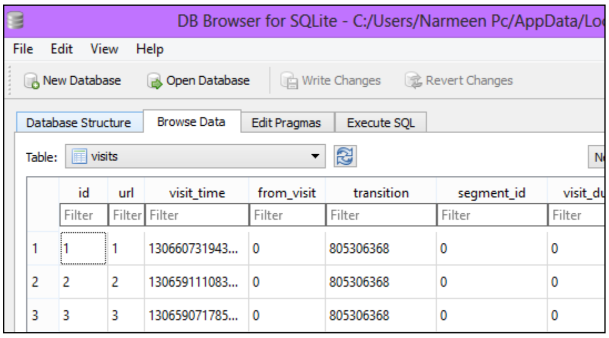
B. *Detecting private mode:*

Since the evidence extraction for private mode of operation is slightly different from the regular mode the forensic examiner needs to know whether the suspect uses private mode or not. A simple indication for private mode on an opened browser is the presence of Incognito sign and the absence of Recent tabs bar. But if the browser if closed, the forensic examiner can run Chrome Cross-mode Interference inspector application on the suspect's PC to see when the private mode was enabled and where was the data stored.

The subsection that follows gives brief forensic analysis of the Google Chrome's Incognito mode. Before this experiment, Google Chrome was fully uninstalled and then reinstalled so as not to confuse between the artifacts obtained from regular and private modes of Chrome. The chrome was opened in private incognito mode and some browsing, downloading and surfing was done to check whether private browsing mode keeps artifacts or not. The results of the research are:

1. *Web Activity*

Private browsing mode though enabled keeps track of user internet activity. The History file, present in the default Chrome Folder, when opened in SQLite browser after closing the browser, as proved by the snapshot in Figure 14 below, shows that Chrome does store visit time but not the actual URL of the page visited. However using BelkaSoft RAM capturer, the analysis of the captured RAM indicates the presence of browsed websites in the RAM. (Noorulla, 2014)

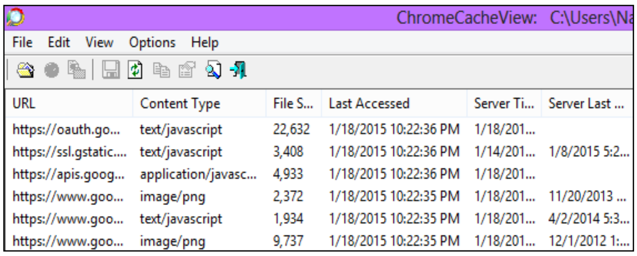


	id	url	visit_time	from_visit	transition	segment_id	visit_du
	Filter	Filter	Filter	Filter	Filter	Filter	Filter
1	1	1	130660731943...	0	805306368	0	0
2	2	2	130659111083...	0	805306368	0	0
3	3	3	130659071785...	0	805306368	0	0

Figure 14. SQLite DB (History file after browser was closed)

2. *Cache*

Like regular browsing mode, private browsing mode stores cache files in the Temporary Internet Files folder of Google Chrome. Snapshot shown in Figure 15 below shows the cache files viewed in Chrome Cache Viewer, after the browser was closed.



URL	Content Type	File S...	Last Accessed	Server Ti...	Server Last ...
https://oauth.go...	text/javascript	22,632	1/18/2015 10:22:36 PM	1/18/201...	
https://ssl.gstatic....	text/javascript	3,408	1/18/2015 10:22:36 PM	1/14/201...	1/8/2015 5:2...
https://apis.goog...	application/javasc...	4,933	1/18/2015 10:22:36 PM	1/18/201...	
https://www.goo...	image/png	2,372	1/18/2015 10:22:35 PM	1/18/201...	11/20/2013 ...
https://www.goo...	text/javascript	1,934	1/18/2015 10:22:35 PM	1/18/201...	4/2/2014 5:3...
https://www.goo...	image/png	9,737	1/18/2015 10:22:35 PM	1/18/201...	12/1/2012 1:...

Figure 15. Cache file opened in Chrome Cache Viewer

3. *Cookies*

In private browsing mode, the cookies are associated with a session time, and hence expire once the browser closes. They can thus only be copied, if the browser is left open.

4. *Bookmarks*

They can be easily seen, by just clicking the Bookmarks file present in Default folder, even after session expires. Thus, bookmarks need to be manually deleted by user.

5. *Third Party Websites*

Private browsing may temporarily hide the data from someone, trying to search for browsing activity in browser history, but the third party websites are still able to trace the IP, track user's activity and send malwares via links/pop-ups.

6. *Downloads*

The download list is cleared after the browser closes, but the downloads can still be seen in the downloads window and needs to be manually deleted.

7. *Other Observations*

WebData and Shortcut files when viewed in SQLite Viewer gave no data. Neither Chrome gives suggestions when typing URL/ form data nor it saves any user credentials.

Though data is deleted at the expiry of the session in private web browsing but this data certainly does not get wiped off the drive. The forensic examiner should therefore know all places and folders where the internet activity of the user and browser preferences gets stored. He may use any forensic tool e.g. FTK Toolkit etc. to view the deleted data. (DFIRninja, 2014)

VI. GOOGLE CHROME'S PORTABLE WEB BROWSER FORENSICS

Operating in Portable mode means that the user installs the portable version of web browser i.e. "Google Chrome Portable" on a portable medium (e.g. a removable hard disk) or cloud service and uses it on any PC. Since the browser has been installed on the portable medium, the artifacts get stored in the same installation folder too.

The portable feature allows the user to keep his data including downloads, bookmarks, saved videos, music, browser extensions etc. with him, all the time, in his portable drive. This not only loads the webpages faster but also provides greater privacy to the user by storing the browser related data in portable drive.

Bad guys can use it in corporate computers where no browser is installed/ allowed. Portable browser however, is a great challenge for forensic investigators, because if the removable media is unplugged by the suspect/criminal, the artifacts are out of the reach of the forensic examiner. (Divyesh & Nagoor, 2014). Essentially all the browsing history, cookies, cache files, downloads, auto fill data was required to be stored in the removable disk from which the browser was running, but it was interesting to note that Chrome's portable mode of operation also leaves artifacts like browsing history, images, downloads, credentials, etc. on the host system in the NTFS Allocated and Unallocated space, Pagefile.sys, Memdump, System32/Winevt/logs etc. (Donny & Narasimha, 2013). Hence the objective of this research was to find any artifacts of user's activity in Google Chrome Portable that might have got stored in his PC.

Another problem that forensic investigator faces while handling cases of portable web browsing is that there is no way to determine whether any web browser was used in portable mode or not. In such criminal cases, where the forensic analysis of web browser in portable media is required, the forensic analyzer must first check the list of portable/ removable media attached to the computer, by analyzing the Windows Pre-fetch files or the Windows' registry via regedit command. He should then check locations where Portable Chrome might save artifacts, and then conclude his observations.

Experiment involves downloading the Google Chrome Portable browser in Kingston 16 GB USB and installing it. Google Chrome application present in USB was then run on HP Pavilion laptop. For traces to be available in Chrome folder and other memory locations, surfing was done for quite some time and then changes in the default Chrome Folder were noted. As part of research, other important drive locations were also searched for internet evidences.

The image of both hard drive and USB were taken via FTK Imager and then the search keywords were analyzed via FTK Search function. It was revealed that part of the browsing data was stored in GoogleChromePortable/data/profile/Default folder and free space in USB. However browsing history, cookies, cached websites, saved passwords etc., also got stored in the ../LocalSettings/Temp/GoogleChromePortable folder in the C drive, and remained there even after the USB, containing Portable Chrome application, was detached. Although the artifacts retrieved from the drive in this experiment were less than the artifacts found in normal Chrome browsing session, they are sufficient for the forensic investigator to reconstruct the browser session. Thus, Google Chrome Portable version also provides a false sense of security to the users.

A. *Forensics of Chrome Portable Incognito mode*

The private web browsing mode also exists within the portable Chrome browser. This Portable Incognito mode is even safer than the normal Incognito or portable mode of operation. Same experiment was conducted, but with Incognito mode enabled in Google Chrome Portable web browser. The results obtained from the FTK Live Search indicate that web browsing data get stored in the free disk space of USB. The incognito mode, despite its claim to rarely leave any trace on computer's disk, leaves abundant internet artifacts in the virtual swap file. (Marrington, I, 2012). The wealth of artifacts, however, varies according to the amount of PC's RAM, number of active processes, and size of swap file. Since this virtual swap file is quite frequently overwritten, the investigator can only extract data for the most recent portable browsing sessions only.

VII. Summary of Preliminary Changes

The working of Google Chrome in all three modes of operation is quite different. Table 3 below, summarizes the forensic analysis of Google Chrome in normal, private and portable mode of operation.

TABLE 3. SUMMARY OF CHROME MODE OF OPERATION

Mode	Forensic Analysis
Normal Mode	• Browsing history, cached websites, cookies, downloads, saved passwords etc. are stored in ..\Chrome\User Data Directory in C drive
Private Mode	• Cookies, Bookmarks, History etc. gets stored in the Default Chrome folder • Browsed websites can be seen in RAM • New timestamp replaces chrome_shutdown_ms.txt on session expiry • User credentials and videos not stored
Portable mode	Forensic artifacts were found in • **Drive:** Data is stored in../LocalSettings/Temp/ GoogleChromePortable folder in C drive • **USB:** Data gets stored in GoogleChromePortable/data/profile/Default folder and also in free space in USB
Portable Incognito mode	Forensic artifacts were found in • **USB:** Data gets stored in free space in USB • **Drive:** Data gets stored in pagefile.sys

IX. Future Trends

Web Browser forensics has become an important field of research for the forensic researchers. Today, most of the Web browser Forensic tools target any specific web browsers, and those few that are able to analyze multiple web browsers, lacks the accurate artifacts extraction. In order to address this issue, a methodology should be designed to analyze multiple browsers simultaneously with one tool, and integrate their data according to the timestamps for integrated artifact analysis. Based on this designed methodology, a forensic tool should be developed for the forensic experts, to speed up their process of investigation. Moreover, since the web browsers are updated frequently, forensic analysts must be able to forensically analyze the newer versions too.

Like regular browsing mode stores a lot of data pertaining to the user's web activity on the drive, the private and portable web browsing modes that though claim to provide privacy to users are not really secure. Before accepting claims of privacy of portable and private modes of other web browsers i.e. Mozilla Firefox, Internet Explorer, Opera etc., the forensic examiners need to forensically analyze them too and find a way to trace the internet artifacts efficiently. Browser forensics should similarly be conducted on other Operating systems too.

Artifacts of web mail, instant messaging and social media applications like Facebook, Gmail, Yahoo, Twitter, MySpace etc., as discussed in the paper, gets stored mostly in the hyberfil.sys and pagefill.sys. Thus these system files must also be forensically analyzed in depth for more details.

However, since the trend of computer is gradually shifting towards the smartphone, the forensic investigator must also thoroughly carry out browser forensic of smart phones.

X. Conclusion

No user can browse safely on the internet. Whether the user has enabled the privacy mode or is working on a portable browser application, the browser tends to store a large amount of data regarding the user's surfing activity, his username passwords, downloads, temporary files, cache, form data and other browser specific data on the user's hard disk, and that is from where the forensic examiner can collect the artifacts from, to reconstruct the timeline of user's web activity.

Browser Forensic Tools are the best source for the forensic experts to find the artifacts from web browser, in case of any suspected illegal Internet activity. The forensic experts can therefore utilize the efficiency of these forensic tools to find internet artifacts from various different locations in the computer's memory. Though the stored web data can be traced down to the exact folder, the deletion of any evidence by the culprit can seriously affect the progress of the case.

REFERENCES

[1] Noora Al Mutawa, Ibrahim Baggili, Andrew Marrington, "Forensic Analysis of Social Networking Applications on Mobile Devices", 12th Annual Digital Forensics Research Conference (DFRWS'12), Washington DC, August 2012

[2] Junghoon, Seungbong Leeb, Sangjin Leea. (2011) *Advanced evidence collection and analysis of web browser activity*. 11th Annual Digital Forensics Research Conference: volume 8.

[3] Christopher Soghoian. (2010). *Why Private Browsing Modes Don't Deliver Real Privacy*. Google Scholar Citation.

[4] D. Ohana; N. Shashidhar. (2013). *Do Private and Portable Web Browsers Leave Incriminating Evidence?* IEEE Symposium on Security and Privacy Workshops 2013. (pp. 135-142)

[5] Divyesh G, Nagoor A R. (2014). *Forensic Evidence Collection by Reconstruction of Artifacts in Portable Web Browser*. International Journal of Computer Applications. vol. 91, issue 4. (pp. 32-35)

[6] Marrington, I Baggili, Talal Ali. (2012). *Portable Web Browser Forensics: A forensic examination of the privacy benefits of portable web browsers.* 2012 International Conference on Computer Systems and Industrial Informatics (ICCSII), (pp. 1-6).

[7] Satvat, Forshaw, Hao, Paper: *On the Privacy of Private Browsing - A Forensic Approach*. Journal of Information Security and Applications. Volume 19, Issue 1. (pp. 88-100)

[8] Sandeep Kumar Khanikekar. (2010). *Web Forensics*. Graduate Thesis, A&M University, Texas.

[9] Emad Sayed Noorulla (2014). *Web Browser Private Mode Forensics Analysis*, Graduate Thesis, Rochester Institute of Technology

[10] DFIRninja (2014). In-Private Browsing: Not so private anymore. Retrieved from http://malwerewolf.com/2014/06/inprivate-browsing-private-anymore/

[11] Kristinn (2010). Google Chrome Forensics. SANS Digital Forensics and Incident Response Blog. Retrieved from http://digital-forensics.sans.org/blog/2010/01/21/google-chrome-forensics/

[12] Craig Wilson (2014). Google Chrome History Backend. Retrieved from http://kb.digital-detective.net/display/BF/Google+Chrome+HistoryBackend

[13] Free Forensic Tools, Retrieved from https://forensiccontrol.com/resources/free-software/

[14] Exposing the password secrets of Google Chrome. Retrieved from http://securityxploded.com/googlechromesecrets.php

[15] Jessica Riccio. Can You Browse Internet in Secrecy? Retrieved from http://burgessforensics.com/Browse_Web_Secret.php

[16] Gaurang Patel (2014). Anti-forensics techniques for browsing artifacts. Retrieved from http://www.slideshare.net/gaurang17/anti-forensicstechniquesforbrowsing-artifacts

[17] Jon S. Nelson (2012). Google Analytics Cookies and the Forensic Implications. Retrieved from http://www.forensicmag.com/articles/2012/02/google-analytics-cookies-and-forensic-implications

[18] Russ Taylor (2014). Chrome Basics. Retrieved from http://hatsoffsecurity.com/ 2014/06/25/chrome-basics/

[19] Herrmann (2012). Chrome Forensics. Retrieved from http://forensir.blogspot.com/2012/03/chrome-forensics.html

[20] John Lehr (2011). Google Chrome Download History. Retrieved from http://linuxsleuthing.blogspot.com/2011/06/google-chrome-download-history.html

[21] Sarah Holmes (2010). How Google Chrome stores Web History. Retrieved from http://www.lowmanio.co.uk/blog/entries/how-google-chrome-stores-web-history/

[22] Internet Live Stats for number of Internet Users (2015). Retrieved from http://www.internetlivestats.com/internet-users/

[23] StatCounter Global Stats - Top 5 Desktop, Tablet and Console Browsers (2015). Retrieved from http://gs.statcounter.com/

[24] DCode. [Software]. Available from http://www.digital-detective.net/digital-forensic-software/free-tools/

[25] Robert C. Newman (2007). *Computer Forensics: Evidence Collection and Management*. In Computer Abuse Investigation (pp. 66)

[26] PhrozenSoft. (2013). Browser Forensic Tool (version 2.0.) [Software]. Available from http://phrozenblog.com/?p=38

[27] History Viewer (version 5.1). [Software]. Available from http://www.historyviewer.net/

[28] Nir Sofer. MyLastSearch (version 1.63). [Software]. Available from http://www.nirsoft.net/utils/my_last_search.html

[29] Nir Sofer. ChromeCookiesView (version 1.11). [Software]. Available from http://www.nirsoft.net/utils/chrome_cookies_view.html

[30] Securityxploded. Chrome Password Decryptor. Google Chrome Login Password Recovery Software. Available http://securityxploded.com/chromepassworddecryptor.php

[31] Nir Sofer. ChromeCacheView for Google Chrome Web browser. (version 1.65) [Software]. Available from http://www.nirsoft.net/utils/chrome_cache_view.html

[32] Internet Evidence Finder by Magnet Forensics. [Software]. Available from http://www.magnetforensics.com/mfsoftware/internet-evidence-finder/

[33] DB Browser for SQLite. [Software]. Available from http://sqlitebrowser.org/

(IJCSIS) International Journal of Computer Science and Information Security,
Vol. 13, No. 9, September 2015

Natural Language Processing and Machine Learning: A Review

Fateme Behzadi

Computer Engineering Department, Bahmanyar Institute of Higher Education
Kerman, IRAN

***Abstract*—Natural language processing emerges as one of the hottest topic in field of Speech and language technology. Also Machine learning can comprehend how to perform important NLP tasks. This is often achievable and cost-effective where manual programming is not. This paper strives to Study NLP and ML and gives insights into the essential characteristics of both. It summarizes common NLP tasks in this comprehensive field, then provides a brief description of common machine learning approaches that are being used for different NLP tasks. Also this paper presents a review on various approaches to NLP and some related topics to NLP and ML.**

Keywords-Natural Language Processing, Machine learning, NLP, Ml.

I. INTRODUCTION

A. Natural Language Processing

Natural Language Processing is a hypothetically driven range of calculative techniques for analyzing and representing naturally texts at one or more levels of linguistic analysis in order to achieve human-like language processing for a range of tasks or applications [1].

The term Natural Language Processing surrounds a wide set of techniques for automated generation, manipulation and analysis of natural or human languages. NLP techniques are affected by Linguistics and Artificial Intelligence, Machine Learning, Computational Statistics and Cognitive Science. Here is introduction of some basic terminology in NLP that will be avail [2]:

- *Token:* Linguistic units of an input text, such as words, punctuation, numbers or alphanumerics.
- *Sentence:* An ordered sequence of tokens.
- *Tokenization:* The process of separating a sentence into its component tokens.
- *Corpus:* A body of text, ordinarily containing a large number of sentences.
- *Part-of-speech (POS) Tag:* A symbol stands for a lexical category, like NN(Noun), VB(Verb), JJ(Adjective), AT(Article).
- *Parse Tree:* Describes the syntactic structure of the sentence as defined by a formal grammar.

Now let's consider some common NLP tasks:

- *POS Tagging:* Assigning POS tags to each word in the sentence.
- *Computational Morphology:* Discovery and analysis of the internal structure of words using computers.
- *Parsing:* Constructing the parse tree given a sentence.
- *Machine Translation (MT):* Translating the given text in one natural language to fluent text in another language with a computer, without any human in the loop.

For more information, an overview of NLP tasks is provided below [3]:

- *Low-level NLP tasks:* Sentence boundary detection, Tokenization, POS tagging, Morphological decomposition of compound words, Shallow parsing (chunking), Problem-specific segmentation.
- *High-level NLP tasks:* Spelling/grammatical error identification and Recovery, Named entity recognition (NER), Word sense disambiguation (WSD), Negation and uncertainty identification, Relationship extraction, Temporal inferences/relationship extraction, Information extraction (IE).

A brief description about NLP, is shown in tables I and II. Table I illustrates some of NLP characteristics [1]. Table II presents levels of NLP [4].

TABLE I. SOME OF NLP CHARACTERISTICS

Origins	Computer Science; Linguistic; Cognitive Psychology.
Divisions	Language Processing; Language Generation.
Approaches to NLP	Symbolic Approach; Statistical Approach; Connectionist Approach.
NLP Applications	Information Retrieval (IR); Information Extraction (IE); Question-Answering; Summarization; Machine Translation (MT); Dialogue Systems.

TABLE II. LEVELS OF NLP

Levels Of NLP	Definition
Phonetics And Phonology	Knowledge About Linguistic Sounds.
Morphology	Knowledge Of The Meaningful Components Of Words.
Syntactic	Knowledge Of The Structural Relationships Between Words.
Semantic	Knowledge Of Meaning.
Pragmatics	Knowledge Of The Relationship Of Meaning To The Intentions Of The Speaker.
Discourse	Knowledge About Linguistic Units Larger Than A Single Utterance.

B. Progression of NLP Research

There are three different areas for progression of NLP research which will finally lead NLP research to grow into natural language understanding. The areas are the following [5]:

- *Syntax-centered NLP:* Manage tasks such as information retrieval and extraction, auto-categorization, topic modeling, etc. Categories of this area are keyword spotting, lexical affinity, statistical methods.
- *Semantics-based NLP:* Focuses on the inherent meaning associated with natural language text. Categories of this area are techniques that leverage on external knowledge or semantic knowledge bases, methods that exploit only intrinsic semantics of documents.
- *Pragmatics-based NLP:* Attempt to understand narratives by leveraging on discourse structure, argument-support hierarchies, plan graphs, and common-sense reasoning.

C. Machine Learning

With advances in computer technology, we presently have the ability to store and process enormous amounts of data, and likewise to access it from physically far locations over a computer network. Most data acquisition devices are digital now and record dependable data. There is a process that explains the data that is observed.

Though the details of the process underlying the generation of data are unknown, it may not be feasible to identify the process entirely, but it can construct a good and helpful approximation. Though identifying the complete process may not be possible, it can still be suitable to detect specific patterns or regularities. This is the role of machine learning. Such patterns can help to comprehend the process, or use those patterns to make predictions.

Application of machine learning methods to large databases is called data mining. In data mining, a large volume of data is processed to construct a simple model with valuable use. But machine learning is not just a database problem; it is also a part of artificial intelligence. To be intelligent, a system that is in a changing environment should have the ability to learn. If the system can learn and adapt to these changes, the system designer needs no predict and provides solutions for all proper situations. Machine learning also helps to find solutions for many problems in vision, speech recognition, and robotics.

Machine learning is programming computers to optimize a performance criterion using example data or past experience. There is a model defined up to some parameters, and learning is the execution of a computer program to optimize the parameters of the model using the training data or past experience. The model may be predictive to make predictions in the future, or descriptive to obtain knowledge from data, or both.

Machine learning uses the theory of statistics in building mathematical models, because the core task is making inference from a sample. The role of computer science is divided into two parts: First, in training, it is required the effective algorithms to solve the optimization problem, and also to store and process the enormous amount of data. Second, once a model is learned, its representation and algorithmic solution for inference needs to be efficient too. In particular applications, the effectiveness of the learning or inference algorithm, namely, its space and time complexity, perhaps are as significant as its predictive accuracy [6].

II. MACHINE LEARNING IN NATURAL LANGUAGE PROCESSING

Natural Language Processing (NLP) deals with real text element processing. The text element is transformed into machine format by NLP.

A system capable of obtaining and combining the knowledge automatically is referred as machine learning [7]. Machine learning systems automatically learn programs from data [8]. Here are shown some machine learning methods [9]:

- *Classifiers:* Document classification, Disambiguation.
- *Structured models:* Tagging, Parsing, Extraction.
- *Unsupervised learning:* Generalization, Structure induction.

The application of machine learning to natural language processing is constantly increasing. Spam filtering is one where spam generators on one side and filters on the other side keep finding more and more talented ways to surpass each other. Perhaps the most striking would be machine translation. After decades of research on hand-coded translation rules, it has become apparent lately that the most favorable way is to provide a very large number of example pairs of translated texts and have a program understand automatically the rules to map one string of characters to another[6].

A. Machine Learning Models

Machine-learning models can be widely classified as either generative or discriminative [3]. These models are briefed here:

- *Generative methods:* Create rich models of probability distributions; like Naive Bayes classifiers and hidden Markov models (HMMs).
- *Discriminative methods:* Directly estimating succeeding probabilities based on observations; like Logistic regression and conditional random fields (CRFs), Support vector machines (SVMs).

B. Some Statistical Machine Learning Approaches

There are a wide variety of learning forms in the machine learning literature. However, the learning approaches other than the HMMs have not been used so widely for the POS tagging problem. However, all well-known learning forms have been applied to POS tagging in some degree. The list of these approaches is here. The interested reader can refer to them in the companion wiki for further details.

- Support vector machines (SVM)
- Neural networks (NN)
- Decision trees (DT)
- Finite state machines
- Genetic algorithms
- Fuzzy set theory
- Machine translation (MT)ideas
- Others: Logical programming, dynamic Bayesian networks and cyclic dependency networks, memory-based learning, relaxation labeling, robust risk minimization, conditional random fields, Markov random fields, and latent semantic mapping [10].

III. Classical Approaches to Natural Language Processing

Text Preprocessing: text preprocessing is the task of converting a raw text file, basically a sequence of digital bits, into a well-defined sequence of linguistically definable units. Text preprocessing is a main part of any NLP system, since the characters, words, and sentences identified at this stage are the fundamental units passed to all more processing stages, from analysis and tagging components, such as morphological analyzers and part-of-speech taggers, through applications, such as information retrieval and machine translation systems.

Text preprocessing can be divided into two stages: document triage and text segmentation. Document triage is the process of transforming a set of digital files into well-defined text documents. Text segmentation is the process of converting a well-defined text corpus into its component words and sentences.

Lexical Analysis: Words are the building blocks of natural language texts. The techniques and mechanisms for performing text analysis at the level of the word, is lexical analysis. A basic task of lexical analysis is to relate morphological variants to their lemma that lies in a lemma dictionary bundled up with its invariant semantic and syntactic information. The mapping of string to lemma, as the only one side of lexical analysis, is the parsing side. The other side is mapping from the lemma to a string, morphological generation.

Syntactic Parsing: This approach presents basic techniques for grammar-driven natural language parsing, that is, analyzing a string of words (typically a sentence) to determine its structural description as a formal grammar. In most conditions, this is not an aim in itself but rather an intermediary step for the goal of additional processing, such as the assignment of a meaning to the sentence. Finally, the requested output of grammar-driven parsing is typically a hierarchical, syntactic structure appropriate for semantic interpretation. The string of words comprising the input will usually have been processed in separate phases of tokenization and lexical analysis, which is therefore not part of parsing proper.

Semantic Analysis: In general linguistics, semantic analysis refers to analyzing the meanings of words, fixed expressions, whole sentences, and utterances in context. In practice, this means translating original expressions into some kind of semantic meta-language. There is a traditional division made between lexical semantics, which involves itself with the meanings of words and fixed word combinations, and supra-lexical (combinational, or compositional) semantics, which involves itself with the meanings of the unclearly large number of word combinations-phrases and sentences-allowable under the grammar.

Natural Language Generation: Natural language generation (NLG) is the process by which thought is rendered into language. It has been studied by philosophers, neurologists, psycholinguists, child psychologists, and linguists. The people who look at it from a computational perspective study the generation in the fields of artificial intelligence and computational linguistics. From this viewpoint, the generator -the equivalent of a person with something to say- is a computer program.

Its work begins with the initial intention to communicate, and then on to determining the content of what will be said, selecting the wording and rhetorical organization and fitting it to a grammar, by way of formatting the words of a written text or establishing the prosody of speech. The process of generation is usually divided into three parts, often executed as three distinct programs:

1) Identifying the goals of the expression.
2) Planning how the goals may be achieved by evaluating the situation and available communicative resources.
3) Realizing the plans as a text [10].

IV. Some Empirical and Statistical Approaches to Natural Language Processing

Corpus Creation: A corpus can be defined as a collection of machine-readable reliable texts (including official copies of spoken data) that is sampled to be representative of a certain natural language or language variety. Corpora provide a material basis and a test bed for building NLP systems. On the other hand, NLP research has contributed considerably to corpus development, especially in corpus annotation, for example, part-of-speech tagging, syntactic parsing. Some issues in corpus creation are such as corpus size, representativeness, balance and sampling, data capture and copyright, markup and annotation, multilingual and multimodal corpora.

Treebank Annotation: The main use of tree-bank is in the area of NLP, most often and significantly statistical parsing. Tree-banks are used as the training data for supervised machine learning (which might contain the automatic extraction of grammars) and as test data for evaluating them. Corpus annotation is not a self-contained task: it serves, among other things, as:

1) A testing and training data resource for NLP.

2) An inestimable test for linguistic theories on which the annotation schemes are based.

3) A resource of linguistic information for the build-up of grammars and lexicons.

Part-of-Speech Tagging: One of the earliest steps within this sequence is part-of-speech (POS) tagging. It is usually a sentence based approach and given a sentence formed of a sequence of words, POS tagging tries to label (tag) each word with its correct part of speech (also named word category, word class, or lexical category).

This process can be considered as a simplified form (or a sub process) of morphological analysis. Whereas morphological analysis involves finding the internal structure of a word (root form, affixes, etc.), POS tagging only deals with assigning a POS tag to the given surface form word.

Nevertheless, Part-of-Speech problems are ambiguous words and unknown words. POS tagging approaches are rule-based approaches, Markov model approaches, and maximum entropy approaches.

Statistical Parsing: Statistical parsing means techniques for syntactic analysis that are based on statistical inference from samples of natural language. Statistical inference perhaps invoked for different aspects of the parsing process but is mainly used as a technique for disambiguation, that is, for selecting the most proper analysis of a sentence from a larger set of possible analyses.

The task of a statistical parser is to map sentences in natural language to their preferred syntactic representations, either by providing a ranked list of candidate analyses or by selecting a single optimal analysis.

Multiword Expressions: Languages are made up of words, which combine via morpho-syntax to encode meaning in the form of phrases and sentences. While it may appear relatively harmless, the question of what constitutes a "word" is an unexpectedly vexed one. To be able to regain the semantics of these expressions, they must have lexical status of some form in the mental lexicon, which encodes their specific semantics. Expressions such as these that have surprising properties not predicted by their unit words are referred to as multiword expressions (MWEs). Types of MWEs are Nominal MWEs, Verbal MWEs, and Prepositional MWEs [10].

V. Components of Learning Algorithms

A classifier is a system that inputs a vector of discrete and/or continuous feature values and outputs a single discrete value, the class. The three components of learning algorithms are [8]:

- *Representation:* A classifier should be represented in some formal language that the computer can handle.
- *Evaluation:* An evaluation function (also called objective function or scoring function) is needed to differentiate good classifiers from bad ones.
- *Optimization:* A method is needed to search among the classifiers in the language for the highest-scoring one.

A. Machine Learning Algorithms for Sentiment Classification

Sentiment classification or Polarity classification is the binary classification task of labeling an opinionated document as declaring either a totally positive or a totally negative opinion and a technique for analyzing subjective information in a large number of texts. A standard approach for sentiment classification is to use machine learning algorithms.

One of the machine learning algorithms is taxonomy based depending on result of the algorithm or type of input available. Description of these algorithms is summarized here [7]:

Supervised learning: Creates a function which maps inputs to expected outputs also named as labels, like Nave Bayes classification, and support vector machines. Supervised learning learns classification function from hand-labeled instances.

Unsupervised learning: Unsupervised learning is learning without a teacher. This learning Models a set of inputs, like clustering, labels are not familiar during training. As an explanation, one basic thing that you might want to do with data is to visualize it. Sadly, it is difficult to visualize things in more than two (or three) dimensions, and most data is in hundreds of dimensions (or more). Dimensionality reduction is the problem of taking high dimensional data and embedding it in a lower dimension space. Another thing you might want to do is automatically derive a partitioning of the data into clusters [11].

Semi-supervised learning: One idea is to try to use the unlabeled data to learn a better decision boundary. In a discriminative setting, you can accomplish this by trying to find decision boundaries that don’t pass too closely to unlabeled data. In a generative setting, you can simply treat some of the labels as observed and some as hidden. This is semi-supervised learning [11]. Semi-supervised learning Generate an appropriate function or classifier in which both labeled and unlabeled examples are combined.

B. Domain Adaptation Algorithms

The concept of domain adaptation is almost related to transfer learning. Transfer learning is a public term that refers to a class of machine learning problems that include different tasks or domains.

There are three general types of domain adaptation algorithms [12]. It could be understood easily when represented in a tabular form as given in table III:

TABLE III. COMPARISON OF THREE CLASSES OF ALGORITHMS

	Class1 (FST)	**Class2 (PBA)**	**Class3 (ISW)**
Name	Feature Space Transformation	Prior Based Adaptation	Instance Selection/ Weighting
Level	Feature	Model	Instance
Dependency	Moderate	Strong	Weak
Domain Gap	Large	Large	Small
Extendability of Domains	Strong	Strong	Weak

VI. WORD SENSE DISAMBIGUATION IN BRIEF

Word Sense Disambiguation (WSD) is mainly a classification problem. Suppose a word in a sentence and an inventory of possible semantic tags for that word; which tag is suitable for each individual instance of that word in context. In many implementations, these labels are major sense numbers from an online dictionary, but they may also match to topic or subject codes, nodes in a semantic hierarchy, a set of feasible foreign language translations, or even assignment to an automatically induced sense partition. The nature of this given sense inventory significantly determines the nature and complexity of the sense disambiguation task [10].

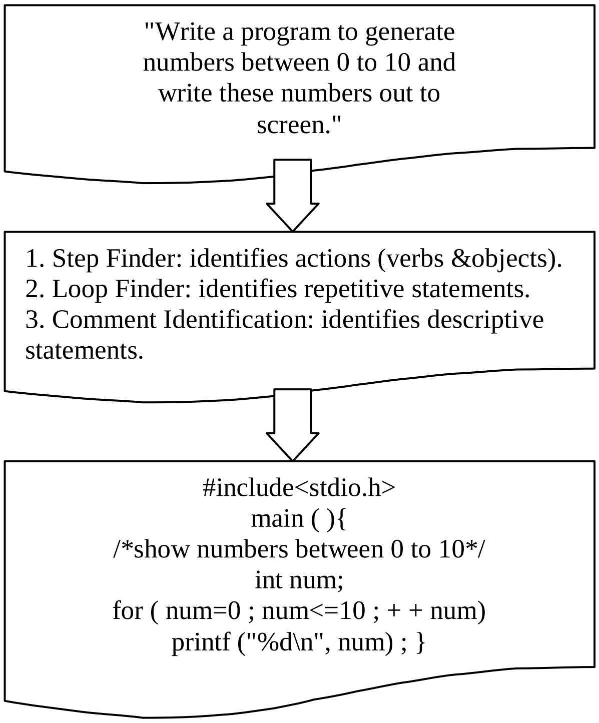
Also applications of word sense disambiguation are applications in machine translation and applications in information retrieval.

An amount of robust disambiguation systems with more simple requirements have been developed over the years. These systems are designed to operate in a standalone mode and make minimal hypothesizes about what information will be attainable from other processes. In machine learning approaches, systems are trained to do the task of word sense disambiguation. In these approaches, what is learned is a classifier that can be used to assign invisible examples, until now, to one of a fixed number of senses [4].

VII. NLP (NATURAL LANGUAGE PROCESSING) FOR NLP (NATURAL LANGUAGE PROGRAMMING)

Natural Language Processing and Programming Languages are both based areas in the field of Computer Science. A computer program is usually composed of sequences of action statements that point out the operations to be performed. Although they are both focused on a common idea -languages-, through the years, there has been only little communication between them. Here, the example below, tries to show how to convert natural language text into computer programs [13].

Starting with the natural language text, "Write a program to generate numbers between 0 to 10 and write these numbers out to screen", the system is analyzing the text with the goal of breaking it down into steps as the one shown below:



"Write a program to generate numbers between 0 to 10 and write these numbers out to screen."

1. Step Finder: identifies actions (verbs &objects).
2. Loop Finder: identifies repetitive statements.
3. Comment Identification: identifies descriptive statements.

```
#include<stdio.h>
main ( ){
/*show numbers between 0 to 10*/
int num;
for ( num=0 ; num<=10 ; + + num)
printf ("%d\n", num) ; }
```

Figure 1. The natural language (English) and programming language (C) expressions for the same problem

VIII. BIONLP: BIOMEDICAL NLP

BioNLP, also known as biomedical language processing or biomedical text mining, is the application of natural language processing techniques to biomedical data. The biomedical domain presents a number of unique data types and tasks, but concurrently has many aspects that are of interest to the "mainstream" natural language processing community. Moreover, there are moral issues in BioNLP that force an attention to software quality assurance beyond the normal attention that is paid to it in the mainstream academic NLP community [10].

There are two basic user communities for BioNLP, and many different user types within those two communities. The two main communities are the clinical or medical community on the one hand, and the biological community on the other.

IX. CONCLUSION

Natural Language Processing is widely considered to be the area of research and application, as compared to other information technology approaches. There have been adequate successes that propose NLP-based technologies will continue to be a great area of research and development in information systems now and in the future. Also Machine Learning is a significant application in NLP that can never be ignored. ML is truly a very important and elaborate, however a necessary task in the NLP development applications.

The article is initiated with a brief review of Natural Language Processing and Machine learning. Machine learning models and approaches are defined in section II. There are numerous possible benefits from utilizing every model. Some classical and statistical approaches to NLP are introduced in section III and IV.

Domain adaptation approaches in NLP tasks are presented in section V that are dispersed to various classes. WORD sense disambiguation is declared briefly in section VI. In section VII, it is believed NLP for programmers will become main technology in their information life. It will be a great event in the ML history. NLP for NLP, appears to be a promising model especially focusing on standardizing APIs, working on large databases like calling functions just by speaking of humans to machine, and improving IDEs for complex services. Hence there is a scope for further research in these areas. At last, BioNLP is showed in short.

ACKNOWLEDGMENT

The author would like to express her sincere thanks to Dr.Khosravi for his valuable comments and his assistance on this paper.

REFERENCES

[1] Liddy, E. D, "Natural language processing",In Encyclopedia of Library and Information Science, 2nd Ed,NY, Marcel Decker, Inc., 2001.

[2] Madnani, Nitin,"Getting started on natural language processing with python". Vol 13, pp. 1–3, 2013.

[3] Nadkarni, Prakash M, Ohno-Machado, Lucila, and Chapman, Wendy W. "Natural language processing: an introduction", Published by group.bmj.com, pp. 545-547, 2011.

[4] Jurafsky, D. and Martin, J. H., "Speech and Language Processing: An Introduction to Natural Language Processing, Speech Recognition, and Computational Linguistics", 2nd edition. Prentice-Hall, Upper Saddle River, NJ, 2008.

[5] Cambria, Erik and White, Bebo. "Jumping nlp curves: A review of natural language processing research" . IEEE Computational Intelligence Magazine, pp. 51-55, 2014.

[6] Alpaydın, Ethem., "Introduction to Machine Learning", 2nd edition, The MIT Press, Massachusetts Institute of Technology, 2010.

[7] Buche, Arti., Chandak, Dr. M. B., and Zadgaonkar, Akshay. "Opinion mining and analysis: A survey",International Journal on Natural Language Computing (IJNLC), Vol. 2, No.3,pp. 41, 2013.

[8] Domingos, Pedro. "A few useful things to know about machine learning", communications of the ACM magazine vol.55,issue.10,pp 78-79,2012.

[9] Pereira, Fernando. "Machine Learning in Natural Language Processing",University of Pennsylvania, pp. 3, 2002.

[10] Indurkhya, Nitin and Damerau, Fred J. , "Handbook Of Natural Language Processing", second edition, Chapman & Hall/CRC press, 2010.

[11] Daumé III, Hal ,"A Course in Machine Learning", Published by TODO,2014

[12] Li, Qi." Literature survey:domain adaptation algorithms for natural language processing", Department of Computer Science The Graduate Center, The City University of New York, pp. 8-10, 2012.

[13] Mihalcea, Rada, Liu, Hugo, and Lieberman, Henry. "Nlp (natural language processing) for nlp (natural language programming)",pp. 323–325, Springer-Verlag Berlin Heidelberg, 2006.

AUTHOR PROFILE

Fateme Behzadi is a MSC student in software engineering in bahmanyar institute of higher education of kerman.she has two accepted papers in 2th National Conference on New Approaches in Computer Engineering, which will be held in Islamic Azad University of Roudsar.

A User-Aware Approach to Provide Context Aware Web Service Composition

Sihem Cherif
MIRACL, ISIMS, Cité El Ons,
Route de Tunis Km 10,
Sakiet Ezziet 3021, Sfax,
Tunisia

Raoudha Ben Djemaa
MIRACL, ISIMS, Cité El Ons,
Route de Tunis Km 10,
Sakiet Ezziet 3021, Sfax,
Tunisia .

Ikram Amous
MIRACL, ISIMS, Cité El
Ons,
Route de Tunis Km 10,
Sakiet Ezziet 3021, Sfax,
Tunisia

Abstract— Web services Compositions are rapidly gaining acceptance as a fundamental technology in the web fields. They are becoming the cutting edge of communication between the different applications all over the web. With the need for the ubiquitous computing and the pervasive use of mobile devices, the context aware web service composition becomes a hot topic. This later aims to adapt the web service composition behavior according to the user's context such as his specific work environment, language, type of Internet connection, devices and preferences. Many solutions have been proposed in this area. Nevertheless, the adaptation was carried out only at the runtime and it partially covered the user's general context. In this paper, we introduce a new context-aware approach that provides dynamic adaptation of service compositions. Our approach allows to express requirements by taking into account potential user's context in addition to the functional one.

Keywords-component; UDDI, AAWS-WSDL, Dynamic context, SABPEL, CAC-WSR

I. INTRODUCTION

A characterizing feature of SOA-based systems is their high dynamicity in selecting the functions that satisfy user requirements. Service composition plays a fundamental role in this kind of software systems. So far, many researchers have investigated different techniques to support the automatic generation of service compositions from a set of published services (domain), given a specific goal to reach (problem).

SOA suffers from a number of limitations and weaknesses in the context of composition on demand; hence web services adaptation to context remains essential to better exploit services.

Web Services Composition based on 'context' can give a personalized behavior to the client by utilizing information about the client. The information can be anything, such a profile of the person, which includes name, country, language, his current location or it can also be the device on which he intends to invoke the service. For e.g., if the client wants to access a web page on his mobile device, then the page needs to be modified or customized so that it can fit into the requirements of the mobile device, the memory to be used.

In addition, most of the existing Web services compositions are not originally developed to be adaptable. Essentially, tools and mechanisms are required to describe and publish adaptable atomic Web service and composite web service. In fact, current web service standards WSDL, UDDI and BPEL are limited to functional view and do not support context information.

Eventhough previous solutions take into account non-functional properties of Web service, they are limited to atomic web service. Moreover, most of researches focus only on the publishing of adaptable atomic service description level; they did not deal with the publishing issue of the adaptable service composition.

In the following, we propose a possible extension of WSDL and called it AAWS-WSDL (Adaptive Atomic Web Service Web Service Description Language).

On the other hand, we propose an UDDI extension that supports context aware service composition based on the AAWS-WSDL and SABPEL [3]. In addition, we extend the BPEL description with the context properties related to the users. We propose a new registry called context aware composition web service registry (CAC-WSR) that publishes adaptable composition web services and allows users to select composite services according to their profiles.

The remainder of our article is organized as follows. Section 2 describes adaptable service composition framework (ASCF), Section 3 describes modelling layer. Section 4 describes the description layer. Section 5 describes publication layer. Section 6 describes the CAC-WSR experimentation. Section 7 discusses some related works. and finally section 8 concludes the paper.

II. ASCF: ADAPTABLE SERVICE COMPOSITION FRAMEWORK

In order to reach the full potential of Web services, they can be combined to achieve specific functionalities. If the implementation of Web service business logic involves the invocation of other Web services, it is called a composite service. The process of assembling a composite service is called service composition. Web services run in a context (e.g. their operating computing infrastructure). In an ideal scenario, Web service operations would do their job smoothly. But, several exceptional situations may arise in the complex, heterogeneous, and changing contexts where they run.

For example, one of the partner services may go down, it may be updated to require new policies, etc. When such situations occur, the composite web service will not operate appropriately and runtime faults will be thrown. Most available web service orchestration engines do not provide automated support for detecting and reacting to such situations and handling them can be done through manual human intervention, i.e., the fault must be detected, the web service based process that threw the fault needs to be undeployed, certain changes should be applied either to the process itself or to its deployment configuration (e.g., replacing the faulty partner service, changing the setting of the interactions to be secure, etc), and then restarting the composite service. Such an approach is inappropriate because the operation of the composite service is discontinued, because certain processes may be interrupted in the middle of a business transaction, and also because of the huge administrative overhead.

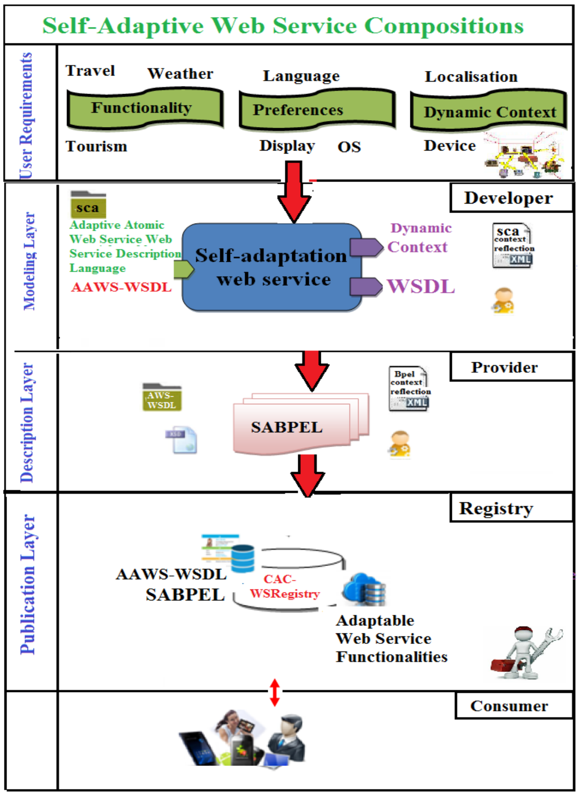


Fig.1: Adaptable web Service Composition main Layers

The need of managing adaptive services composition impels the incorporation of facilities to deal with user's context in all the services composition life cycle. We define the user's context as a set of context information composed of device characteristics, connection, location and a set of preferences in terms of content and presentation.

To achieve this objective, we propose in this section a framework that supports the development, the description and the publication of adaptive service composition (ASC). Our goal is to offer relevant and suitable information depending on the user's particular profile. Therefore, developers have to integrate software facilities dealing with the context characteristics. Then, context annotations must be used to extend BPEL descriptions. Moreover, UDDI must be extended to include contextual information of the service composition in addition to the atomic web service information and the composite web service information currently stored in UDDI registries. Our framework is organized in a layered architecture and it consists mainly of four layers providing specification, modeling, description and publication solutions.

Figure 1 illustrates an overview of our framework's main layers. Each one describes our proposal to a given stage of the Web service life cycle.

- Modeling layer: It focuses on the design of the application behind the atomic service and composite service. In fact, in this layer we propose a modeling tool called SCA (Service Component Architecture). The SCA allows to provide a programming model for designing applications and SCA solutions based on a Service Oriented Architecture (SOA). It is based on a series of services, which are assembled together to manipulate solutions that serve a particular business need. These composite applications contain both business function from existing systems and applications and also new services created specifically for the application, reused as part of the composition.
- Description layer: It concentrates on the annotation of the BPEL description document with contextual information managed by the composite service. The adaptable description named SABPEL [3] is automatically generated from the service implementation using our SABPEL generator.
- Publication layer: It gathers atomic web services features, composite web service and context supported on a UDDI extended registry named CAC-WSR [18].

The following sections will concentrate on a detailed description of each layer.

III. Modeling Layer

The SCA specifications concentrate on the task of describing the assembly and the configuration of the components that compose an SOA application. This assembly is used as input to initialize and instantiate the application. But, the SCA specifications do not address the runtime management of the application, which typically includes reconfiguration and monitoring.

Furthermore, the SCA specification does not address either the run-time management of the platform itself. Yet, these properties are almost mandatory for modern SOA platforms in order to be able to adapt to changing operating conditions, to support online evolution, and to be deployed in dynamically changing environments (e.g., ubiquitous environments) [3].

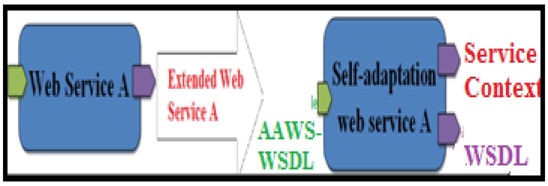


Fig.1: SCA component A extended with management interfaces

In this section, we present the design of the self-adaptation Web service which addresses these problems.

Our solution relies on the addition of the reflection mechanisms. Namely, we use these mechanisms to provide self-adaptable service using ReMoSSA reference model [3] in dynamic context. In fact, we envision separate components for monitoring context. These components are attached to each self-adaptation web service. From an external point of view, we added, at design phase, a set of additional interfaces to web service A. In fact, we transformed the Web service A into Self-adaptation Web service A, as shown in Figure 2. The general structure of our conception is shown for an individual web service A in Figure 3.

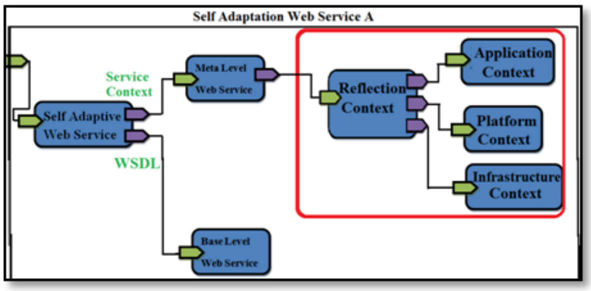


Fig. 3: Extended SCA component A with all its attached reflective components

Web service A is extended with component for service context and component for each task of reflection mechanism.

So, the original "service" and "reference" interfaces of Web service A are promoted to the interface of Self-adaptation web service A, so that, from a functional point of view, this self-adaptation web service A can be employed in the same way as the original Web service A.

In our architecture, we integrate reflection mechanisms as self-adaptation mechanism that can be used to adapt dynamically the behavior of applications. A reflection mechanism provides the ability of the service-based applications to observe and to modify its computation.

This layer supports adaptive context-awareness capabilities. It is designed to offer runtime adaptation to dynamic environments.

We introduce this mechanism in this layer for dynamically adapting the service and composing in two levels:

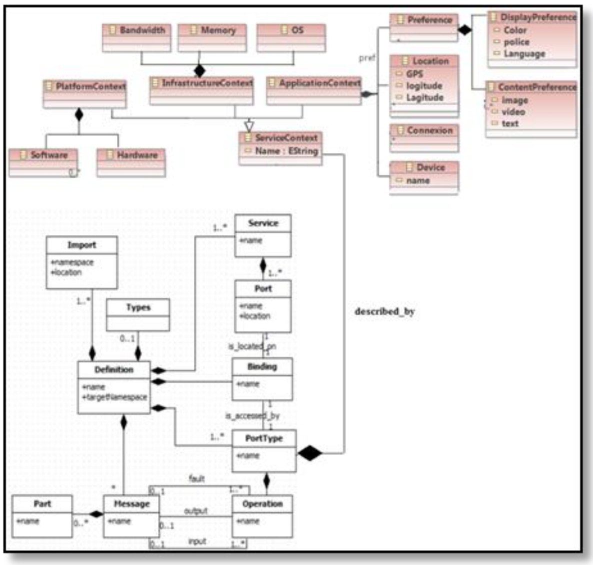


Fig. 4: Metamodel of the AAWS-WSDL

A base-level subservice provides the system's domain functionality (i.e., application logic). It composed by interceptor components as architecture pattern. Interceptors use for changing services transparently during runtime, adapt services for fault tolerance (e.g., failure of servers), and adapt services according to capacity and load of resource (e.g., distribute the load between servers).

The second level is the reflective subservice (meta-level); it defines the context the web service (the platform context, the infrastructure context and the application context).

IV. DESCRIPTION LAYER

In order to allow the provider to publish adaptation criteria on the one hand and to allow the consumer to choose from a list of published Web services compositions the most appropriate description according to his needs and profile on the other hand , we suggest additional information in the description file. We therefore propose an extension of the two standard WSDL and BPEL having the ability to describe composite and atomic service profile information. Our extension, named AAWS-WSDL and SABPEL, is detailed in [4]. The SABPEL document is the output of our description layer.

The SABPEL is obtained through a model transformation from the adaptive design described in the previous section.

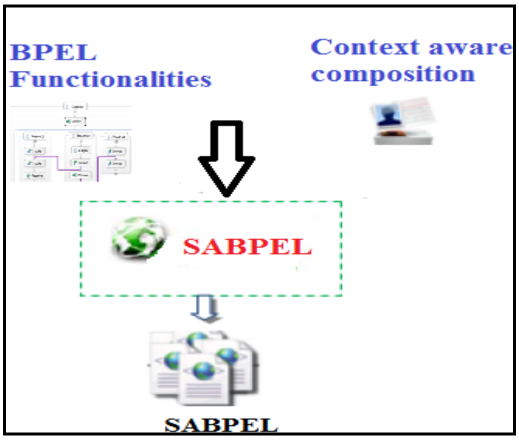


Fig. 2: Description Layer of the ASCF

Figure 5 illustrates the transformation process in the description layer.

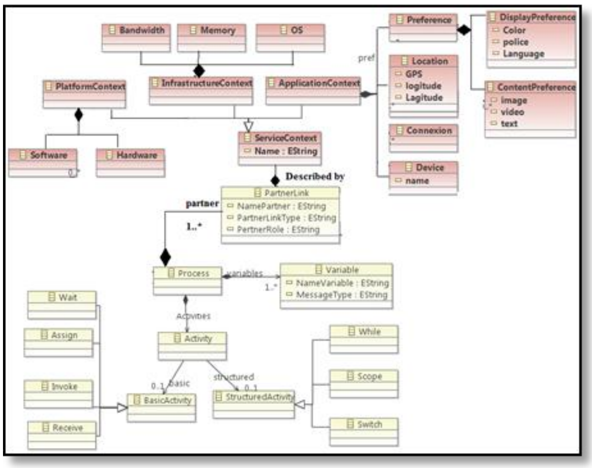


Fig. 3: Metamodel of the SABPEL

A. *Context-aware Service Composition: Intersection of atomic Web service context*

For our study, we present composite context information concept as shown in Figure. 6.

First of all, we have to define the composite context information's concept for our research.

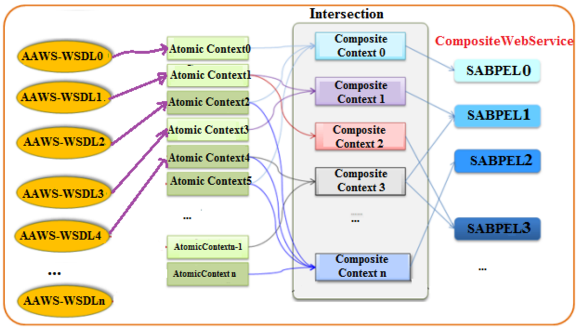
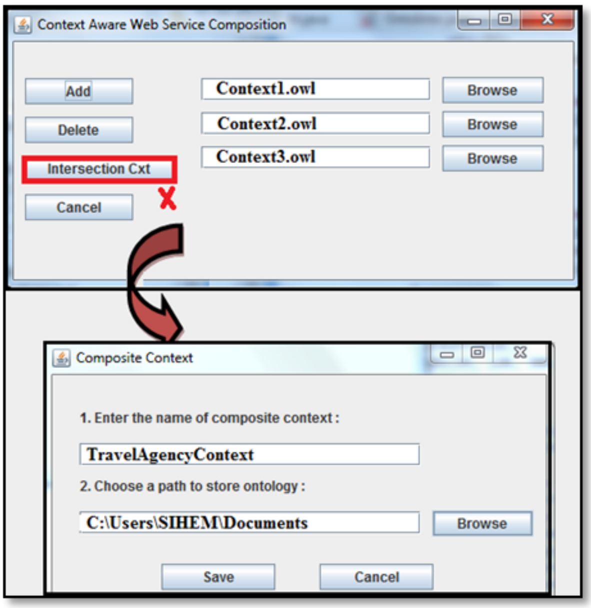


Fig. 4 : Composite context information concept

We define the composite context information that is "Enhanced high level context information by integration context information related with atomic service for decide or supply the context aware service composition of application. In order to provide composite contextual service, context ontology is constructed.



Context1.owl
Context2.owl
Context3.owl

1. Enter the name of composite context :
TravelAgencyContext
2. Choose a path to store ontology :
C:\Users\SIHEM\Documents

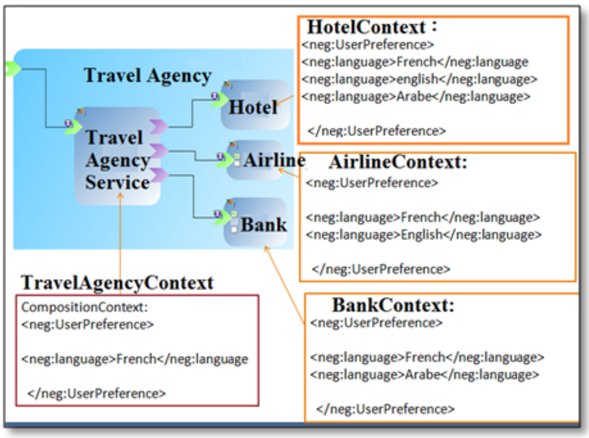
Fig. 5 : Intersection of atomic Web service context

Each elementary web service has atomic context ontology which is stored in OWL file. This atomic context ontology is automatically generated from AAWS-WSDL description file. Figure 8 shows an example of composite context intersection using three atomic contexts:

- Context1.owl describes the context of hotel service (as shown in figure.8).
- Context2.owl describes the context of airline service (as shown in figure.8).

- Context3.owl describes the context of bank service (as shown in figure.8).

In fact, figure. 8 shows a composite context of travel agency service. This later uses three atomic contexts (Hotelcontext, AirlineContext and BankContext. The hotel service uses three languages as user's preference (French, English and Arabic); The Airline service uses two languages as user's preference (French, and English); and the bank service uses two languages as user's preference (French and Arabic). Therefore, the composite context of travel agency uses one language (French) that is an intersection of the three atomic contexts.



HotelContext :
```
<neg:UserPreference>
<neg:language>French</neg:language
<neg:language>english</neg:language>
<neg:language>Arabe</neg:language>

 </neg:UserPreference>
```

AirlineContext:
```
<neg:UserPreference>

<neg:language>French</neg:language>
<neg:language>English</neg:language>

 </neg:UserPreference>
```

BankContext:
```
<neg:UserPreference>

<neg:language>French</neg:language>
<neg:language>Arabe</neg:language>

 </neg:UserPreference>
```

TravelAgencyContext
```
CompositionContext:
<neg:UserPreference>

<neg:language>French</neg:language

 </neg:UserPreference>
```

Fig. 6 : Example of Composite Context

B. *Context-aware Semantic Service Design*

To support design and composition of context-aware services we propose: an OWL ontology (OWL-SABPEL), supporting the description of sets of contexts in specific domains and an extension of the OWL-S ontology for services.

Context-aware semantic descriptions can be exploited during the service composition process to automatically generate compositions better-tuned to the requestor's behaviors and preferences and to the particular situation of the environment.

Figure. 10 shows OWL-SABPEL, an extensible OWL ontology for describing contexts according to AAWS-WSDL, described in Section 2. Profile, Context, Preferences are the main concepts in this ontology

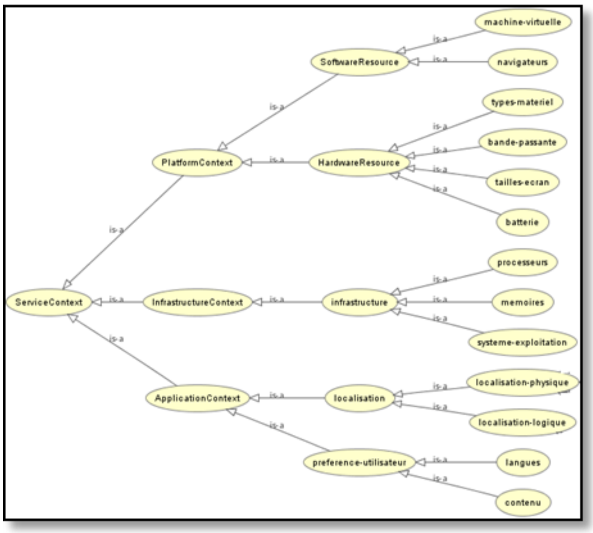


Fig.7 : OWL-SABPEL: ontology language

.

We can distinguish a Context as a composite or an atomic. Differently from an Atomic context, a Composite context can be further intersection in one or more atomic context that can be helpful for a better characterization of the associated context aspect.

V. PUBLICATION LAYER

A service provider publishes its service at a service registry using a publishing interface. The public interfaces and binding information of the registered services are clearly defined in the WSDL standard language. A registry organizes the published services and provides a query interface that enables a service consumer to search for a needed service, and obtain its provider's location information.

A service consumer then interacts with a service provider through the SOAP protocol. The most known registry is UDDI which is an XML-based standard that was proposed for allowing providers to publish their web services, so that they can be located afterwards by consumers. A UDDI registry is structured into three components: BusinessEntity or white pages, BusinessService or yellow pages and BindingTemplate or green pages. These components allow the search for a suitable web service in the

UDDI[1] registry according to the three data types. Unfortunately, web service discovery through UDDI-based registries is insufficient to carry out consumer adaptation requirements. This necessity is increasing every day with the emergence of portable devices and various users preferences. Hence, the provider and the consumer want to have a registry providing a fairly precise publishing and search capabilities to render the use of user-aware web services more efficient. To overcome these needs, we propose a web service registry offering the ability to save adaptation criteria of atomic web service and adaptation criteria of composite web service. The registry is called context aware composition web service registry (CAC-WSR) and it supports the publication of the SABPEL description presented in section 4.

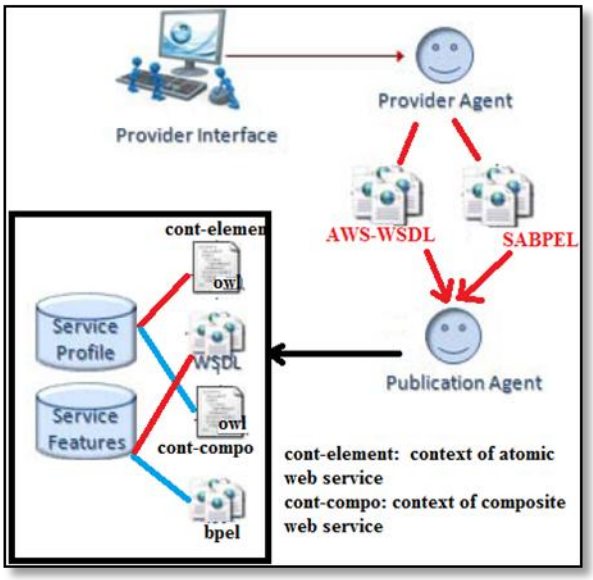


Fig. 8: Publication process in the CAC-WSR Registry

We extend the UDDI data structure by an atomic AdaptationCriteria element which makes reference to the item UserProfile in the description file AAWS-WSDL. In addition, we extend the UDDI data structure by an composite AdaptationCriteria element which makes reference to the item UserProfile in the description file SABPEL. When a supplier requests the publication of his service at the registry, an analyzer module retrieves the AAWS-WSDL description file and the SABPEL description file. Then features and access points description will be transferred to the Services features database and those corresponding to the adaptation criteria will be transmitted to the Service Profile database.

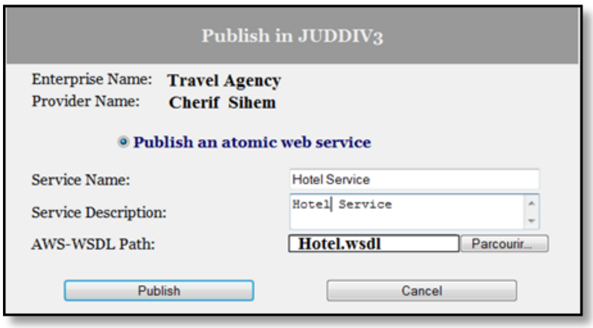
To implement our registry, we propose an extension of the JuddiV3[2] API.

Therefore, we use the apache Tomcat as a web server and the MySQL to implement the UDDI data Base. We offer a user-interface allowing the provider to specify atomic and composite service information and to load the description file of its service. Then, a parser analyzes two files (the AAWS-WSDL file ans SABPEL file). It allows the extraction of the functional description carried out by the elements (types, portype, message, binding, service) and stores it in the database ServiceProfile.

Then it extracts the profile description contained in the element UserProfile and saves it in the database ServiceFeature. The db–atomic-context table stores the profile of the atomic web service. This table refers to the binding – template table that stores atomic web service instances.

The db–bpel-context table stores the profile of the composite web service. This table refers to the binding – template table that stores composite web service instances.

Our extended registry is compatible with the basic UDDI and both of them could coexist in the same environment. Publication process is shown in figure 11.To publish AAWS-WSDL description of the the atomic web service in CAC-WSR. The definition document which is associated with the supported profile is chosen by the provider via the publishing interface illustrated in figure 12. The provider have to specify the enterprise information, the service information, the web server and the description file.



Publish in JUDDIV3

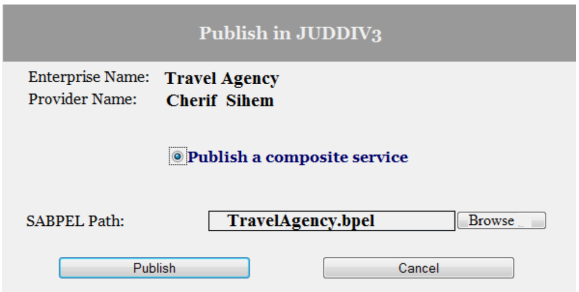
Enterprise Name: Travel Agency
Provider Name: Cherif Sihem

● Publish an atomic web service

Service Name: Hotel Service
Service Description: Hotel Service
AWS-WSDL Path: Hotel.wsdl

Fig. 9: Publish AAWS-WSDL description of the the atomic web service

The CAC-WSR registry contains also a query analyzer module used in the selection and discovery phase. This module communicates with the database Web service Functionalities and ServiceProfile in order to select the suitable list of Web services meeting user's query in terms of functionality and adaptation. The query analyzer allows the customer to:



Publish in JUDDIV3

Enterprise Name: Travel Agency
Provider Name: Cherif Sihem

● Publish a composite service

SABPEL Path: TravelAgency.bpel

Fig. 10: Publish SABPEL description of the the composite web service

- Extract the needs in terms of functionality through keywords,
- Extract the needs in terms of adaptation through a comparison between the user's profile and the service profile stored in the CAC-WSRegistry. The user's profile is automatically detected by a detection module named WEDM (WildCat Extension Detected module) which is an extension of the WildCat API and it is stored in an XML file.

Composite service finding process over CAC-WSRegistry is depicted by figure 14.

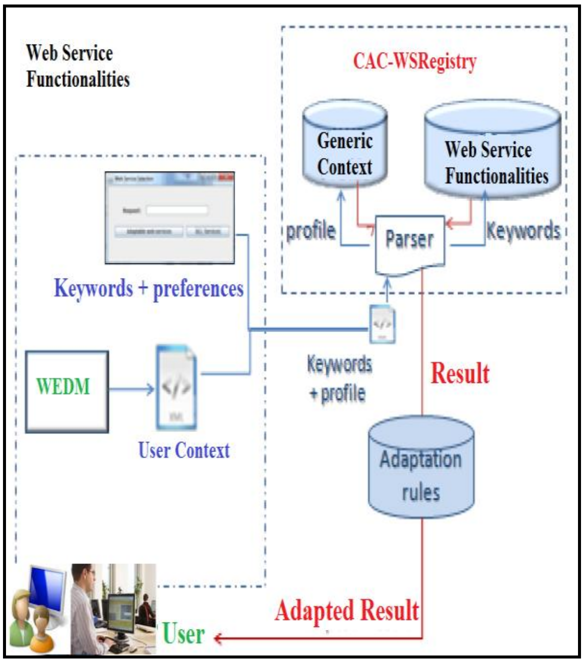


Fig. 11: Finding composite service process in the CAC-WSRegistry

VI. Illustration of Use

In this section, we illustrate the feasibility of our proposed framework ASCF through the example of a *Travel Agency composite* web service. The service client wants to book a room in a hotel on the basis of his profile characteristics. We provide corresponding solution to each layer.

A. *Modeling layer*

This layer's focus is on the design of the *Travel Agency* web service features as well as the Web service adaptation ability. Figure 16 shows an extract of the SCA diagram in eclipse.

Figure 15 shows the generation of AAWS-WSDL hotel service using SCA diagram. The reflection model allowing to represent the supported content and presentation preferences of the hotel service. This component is necessary to generate the AAWS-WSDL file for web service.

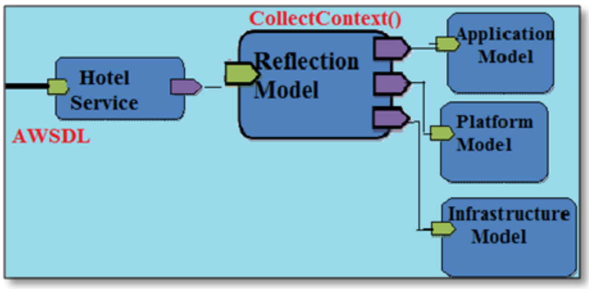
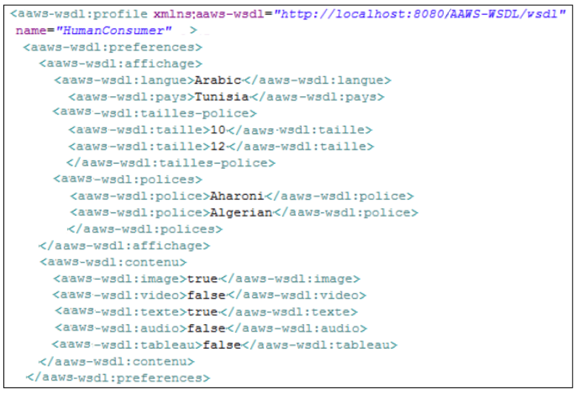


Fig. 12:Generation of AAWS-WSDL Hotel Service

In our case study we configure the preferences of the human consumer hotel service. Clearly, for a chosen element, we can select multiple choices. For instance, police size could be ”10” or ”12”. Also, we can add new values in the proposed textfields. A temporary file is associated to every configured view. Then, they are gathered into the AAWS-WSDL description final document. An extract of the generated description file is illustrated in figure 16.



```
<aaws-wsdl:profile xmlns:aaws-wsdl="http://localhost:8080/AAWS-WSDL/wsdl"
 name="HumanConsumer"  >
  <aaws-wsdl:preferences>
    <aaws-wsdl:affichage>
      <aaws-wsdl:langue>Arabic</aaws-wsdl:langue>
        <aaws-wsdl:pays>Tunisia</aaws-wsdl:pays>
      <aaws-wsdl:tailles-police>
        <aaws-wsdl:taille>10</aaws-wsdl:taille>
        <aaws-wsdl:taille>12</aaws-wsdl:taille>
        </aaws-wsdl:tailles-police>
      <aaws-wsdl:polices>
        <aaws-wsdl:police>Aharoni</aaws-wsdl:police>
        <aaws-wsdl:police>Algerian</aaws-wsdl:police>
        </aaws-wsdl:polices>
    </aaws-wsdl:affichage>
    <aaws-wsdl:contenu>
      <aaws-wsdl:image>true</aaws-wsdl:image>
      <aaws-wsdl:video>false</aaws-wsdl:video>
      <aaws-wsdl:texte>true</aaws-wsdl:texte>
      <aaws-wsdl:audio>false</aaws-wsdl:audio>
      <aaws-wsdl:tableau>false</aaws-wsdl:tableau>
    </aaws-wsdl:contenu>
  </aaws-wsdl:preferences>
```

Fig. 13: Extract from the Hotel description file

In this example, we have a HotelService component corresponding to the *BookingHotel* main feature provided to all kind of users, a FlightService component corresponding to the *BookingFlight* main feature provided to all kind of users and a BankService component corresponding to the payment main feature provided to all kind of users. In addition, we add the EventBD component to retrieve the list of promotions or to add the travel agency service to its list of activities.

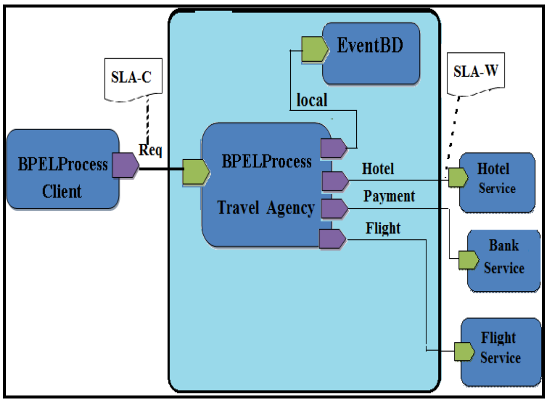
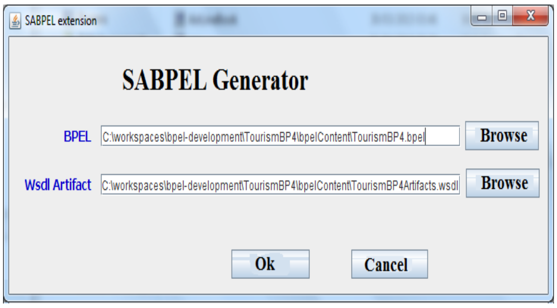


Fig. 14: Travel Agency web service

We can distinguish the travel agency component which invokes the hotel service, bank service and the flight service.

B. *Description layer*

The Travel Agency web service modeled above using our tool SCA diagramm is then implemented in Java. The next step is to generate the SABPELdescription file gathering all needed information about the available functionalities, access links and supported profiles. Figure 18 illustrates the SABPEL generator interfaces.

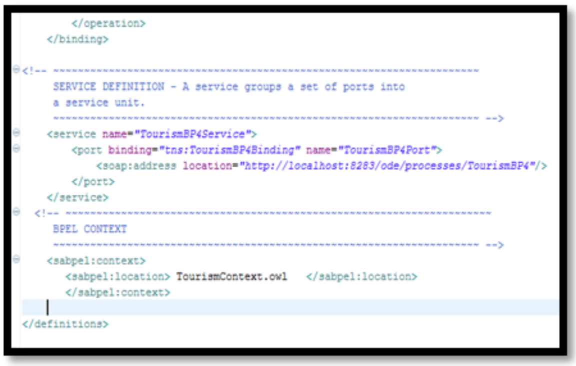


BPEL C:\workspaces\bpel-development\TourismBP4\bpelContent\TourismBP4.bpel

Wsdl Artifact C:\workspaces\bpel-development\TourismBP4\bpelContent\TourismBP4Artifacts.wsdl

Fig. 15: The SABPEL generator GUI interfaces

As input, we provide the BPEL and the WSDL of the composition of the Travel Agency adaptable service. Then the provider could select, through the plug-in Interface, the composite context of travel agency (as shows in figure 8). This later is an intersection of three atomic context (the context of hotel service, bank service and flight). This composite context is included in the BPEL description file.



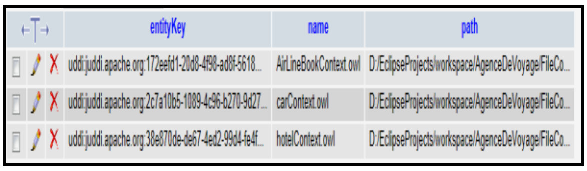
```
        </operation>
    </binding>

<!-- ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
     SERVICE DEFINITION - A service groups a set of ports into
     a service unit.
     ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~ -->
    <service name="TourismBP4Service">
        <port binding="tns:TourismBP4Binding" name="TourismBP4Port">
            <soap:address location="http://localhost:8283/ode/processes/TourismBP4"/>
        </port>
    </service>
  <!-- ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
     BPEL CONTEXT
     ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~ -->
    <sabpel:context>
       <sabpel:location> TourismContext.owl   </sabpel:location>
       </sabpel:context>

</definitions>
```

Fig. 16: Extract from the Travel Ageny description file

An extract of the generated description file (SABPEL) is illustrated in figure 19.

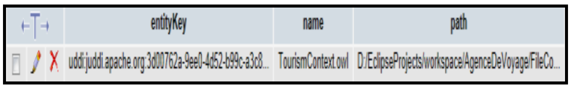
C. Publication layer

Next step is to publish the SABPEL description of the composite service in our CAC-WSR registry. The provider has to specify the enterprise information, the service information, the web server and the description file to load. The BPEL document enriched with the supported profile is saved in the db-bpel-context table (cf figure 20).



←T→	entityKey	name	path
□ ✎ ✗	uddi:juddi.apache.org:172eefd1-20d8-4f98-ad8f-5618...	AirLineBookContext.owl	D:/EclipseProjects/workspace/AgenceDeVoyage/FileCo...
□ ✎ ✗	uddi:juddi.apache.org:2c7a10b5-1089-4c96-b270-9d27...	carContext.owl	D:/EclipseProjects/workspace/AgenceDeVoyage/FileCo...
□ ✎ ✗	uddi:juddi.apache.org:38e870de-de67-4ed2-99d4-fe4f...	hotelContext.owl	D:/EclipseProjects/workspace/AgenceDeVoyage/FileCo...

Fig. 17: juddi Publication of the Flight and hotel web service in the CAC-WSRegistry



←T→	entityKey	name	path
□ ✎ ✗	uddi:juddi.apache.org:3d00762a-9ee0-4d52-b99c-a3c8...	TourismContext.owl	D:/EclipseProjects/workspace/AgenceDeVoyage/FileCo...

Fig. 18: Publication of the Travel agency web service in the CAC-WSRegistry

Below, we expose experiment results of the publication process in our CAC-WSR registry:

1. The first experiment determined the performance of the standard UDDI by measuring the speed of the publishing function dealing with BPEL document.
2. The second experiment determined the performance of the CAC-WSR registry by measuring the speed of the publishing function dealing with SABPEL document. Figure 21 demonstrates a comparison between the span of time taken to publish BPEL description and the one taken to publish SABPEL description. BPEL documents used in these experiments were taken from the webservicex portal.

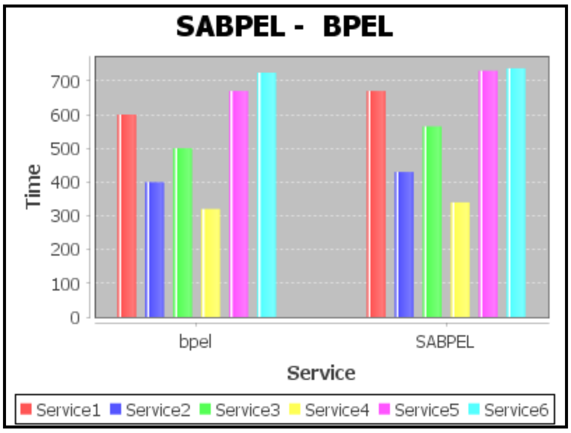


Fig. 21: Execution time required to publish web services on the CAC-WSRegistry

VII. RELATED WORKS

In this section, we take a look at some research works interested in the possibilities of integrating the self-adaptive in the Web Service Composition. We provide an overview of some of these works.

Portchelvi and al. [25] proposed a Goal-Directed Orchestration (GDO) approach which employs an orchestration engine to provide flexibility in responding to the changes in dynamic services environment. In GDO Process, the user request for service is given to the engine and the composition request generator generates an abstract goal tree and concrete goal tree. The Abstract goal tree is mapped to abstract task tree and the concrete goal tree is mapped to the concrete task tree and thereby a composition plan is generated with abstract service descriptions. If services are not available to construct a composition plan then the goal cannot be achieved and it leads to goal failure. This failure is reported back to the composition requestor and an alternate sub-goal for the failed sub-goal is found and given to the composition plan generator. However, the authors need to formalize this goal-directed approach using formal methods.

Martin [24] deals with the problem of the flexible composition by automated planning for which he proposes a model. The sequence and the choice operators are defined and used to characterize flexible plans. Two other operators are then derived from the sequence and the choice operators : the interleaving and the iteration operators. The author refers to this framework in order to define the flexibility produced by my planner, Lambda-GraphPlan (LGP), which is based on the planning graph. The originality of Lambda-GraphPlan is to produce iterations. Martin [24] shows that Lambda-GraphPlan is very efficient on domains that allow the construction of iterative structures.

Vukovic [22] proposed a framework for building context aware applications on-demand, as dynamically composed sequences of calls to services. She presents the design and implementation of a system, which employs goal-oriented inferencing for assembling composite services, dynamically monitors their execution, and adapts applications to deal with contextual changes. To handle composition failures, the author introduces GoalMorph, a system which transforms failed composition requests into alternative ones that can be solved.

Ashraf Butt [23] proposed a Trend-based Service Discovery Protocol (TRENDY), a new compact and adaptive registry-based Service Discovery Protocol with context awareness for the Internet of Things (IoT), with more emphasis given to constrained networks. TRENDY's service selection mechanism collects and intelligently uses the context information to select appropriate services for user applications based on the available context information of users and services. In addition, TRENDY introduces an adaptive timer algorithm to minimise control overhead for status maintenance, which also reduces energy consumption. Its context-aware grouping technique divides the network at the application layer, by creating location-based groups. This grouping of nodes localises the control overhead and provides the base for service composition, localised aggregation and processing of data.

Grati and al. [8] proposed a QoS monitoring framework QMoDeSV for composite Web services implemented using the BPEL process and deployed in the Cloud environment. The proposed framework is composed of three basic modules to: collect low and high level information, analyze the collected information, and take corrective actions when SLA violations are detected. This framework provides for a monitoring approach that modifies neither the server nor the client implementation. In addition, its monitoring approach is based on composition patterns to compute elementary QoS metrics for the composed Web service.

El Haddad and al. [19] presents a QoS aware selection method for Web services composition called TQoS (Transactional QoS-Driven Web Services Composition). The service selection is realized based on QoS and transactional requirements. Quality requirement is described as a set of weights over QoS criteria. Transactional requirement is expressed by a risk notion that denotes if the results could be compensated or not. In [19], five QoS criteria (execution price, execution duration, reputation, successful execution rate and availability) are used and a local optimization method for service selection is proposed. The authors also present and formally analyze a service selection algorithm based on the workflow patterns and the transactional properties of the component services.

The ASWSCC Method [11] (Adaptation of Semantic Web Service Composition to Context) is a model which ensures, on the one hand, this model allows management and taking into account the user context that makes composition process adaptable to different instances of use context, which may change during the same session. On the other hand, web services matching during composition process by using domain ontology as lexical database, its purpose is to identify, classify and relate in different ways semantic content and lexical language.

Furno and al. [7] presented a design approach based on a semantic model for context representation. It is an extension of the OWL-S ontology aimed at enriching the expressiveness of each section of a typical OWL-S semantic service description, by means of context conditions and adaptation rules. The model proposed by the authors allows to use context-awareness expressions in semantic service descriptions and their adoption during composition.

Hermosillo and al. [9] described CEVICHE, a framework that combines Complex Event Processing (CEP) and Aspect Oriented Programming (AOP) to support dynamically adaptable business processes. The adaptation logic is defined as aspects (reconfiguration component), and adaptation situations are specified by CEP rules (monitoring component). However, the decision- making is not specified as component in this framework. It is integrated into the defined aspects.

As we have shown, work on adaptation at service composition modeling is prolific. Different scopes are defined as well as different mechanisms for achieving such adaptations.

Cheng and al. [4] presented an automatic Web service composition method that deals with both input/output compatibility and behavioral constraint compatibility of fuzzy semantic services. First, user input and output requirements are modeled as a set of facts and a goal statement in the Horn clauses, respectively. A service composition problem is transformed into a Horn clause logic reasoning problem. Next, a Fuzzy Predicate Petri Net (FPPN) is applied to model the Horn clause set, and T-invariant technique is used to determine the existence of composite services fulfilling the user input/output requirements. Then, two algorithms are presented to obtain the composite service satisfying behavioral constraints, as well as to construct an FPPN model that shows the calling order of the selected services.

Madkour and al. [17] proposed a three-phases adaptation approach: firstly they select the suitable services to the current context and we recommend them to the adaptation process, in the service adaptation phase they perform adaptation by using fuzzy sets represented with linguistic variables and membership degrees to define the user's context and the rules for adopting the policies of implementing a service. Finally they deal with the complex requirements of the user by the composition of the obtained adaptable atomics services.

A variety of techniques have been proposed in literature which integrates existing services based on several pieces on information. Although a rich landscape in adaptation related researches, a complete and generic context-aware composition approach is still missing. Table 1 summarises the comparison of context aware service composition works. Nor all of the identified features are present in a single work, as they focused on different research problems. Most surveyed architectures employ a centralized composition model. They address dynamism in the composition, primarily from the perspective of unavailability of selected Web services, and deal with the issues of how to replace them with other equally capable Web services to perform the desired task.

Context aware service composition frameworks should support the following features:

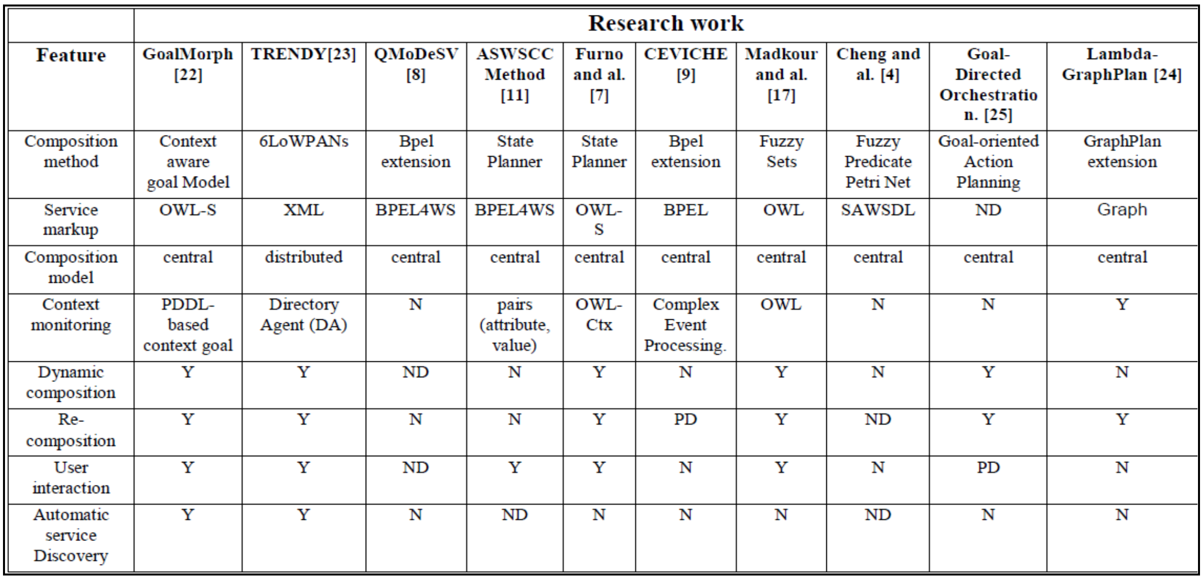
1. The dynamic composition. Static service composition involves pre-compilation of the composite service prior to a user's request. Dynamic composition is essential for exploiting the current state of available services and making adaptations based on run time parameters, such as bandwidth and the cost of executing the various services.
2. Re-composition. As composite services may be executed in a dynamic environment, the context may change and services may become unavailable. Therefore it is necessary to have some means of recomposing the service on the fly.
3. User interaction. Whilst service composition is an automated process, it is necessary to allow users to provide feedback when they so wish or moreover be integrated in the composition process. For example, aside from providing

input parameters, users may need to guide the composition, by selecting the services and re-defining the goals or guide the failure recovery process.

4. Automatic service discovery. Working with a limited domain of services or predefined service types limits the potential of service composition. Moreover, new services, possibly with new capabilities, may become available or existing ones may change their functionality. Having an automated means of service discovery is therefore an essential feature.

5. Context monitoring. For the purpose of supporting dynamic adaptations, software should be aware of changes in its context. Context-aware systems are concerned with the acquisition of context, the abstraction and understanding of context, and applicationbehavior based on the recognized context.

TABLE 1: Main research challenges and features of automatic Web service composition



	Research work									
Feature	**GoalMorph [22]**	**TRENDY[23]**	**QMoDeSV [8]**	**ASWSCC Method [11]**	**Furno and al. [7]**	**CEVICHE [9]**	**Madkour and al. [17]**	**Cheng and al. [4]**	**Goal-Directed Orchestration. [25]**	**Lambda-GraphPlan [24]**
Composition method	Context aware goal Model	6LoWPANs	Bpel extension	State Planner	State Planner	Bpel extension	Fuzzy Sets	Fuzzy Predicate Petri Net	Goal-oriented Action Planning	GraphPlan extension
Service markup	OWL-S	XML	BPEL4WS	BPEL4WS	OWL-S	BPEL	OWL	SAWSDL	ND	Graph
Composition model	central	distributed	central	central	central	central	central	central	central	central
Context monitoring	PDDL-based context goal	Directory Agent (DA)	N	pairs (attribute, value)	OWL-Ctx	Complex Event Processing.	OWL	N	N	Y
Dynamic composition	Y	Y	ND	N	Y	N	Y	N	Y	N
Re-composition	Y	Y	N	N	Y	PD	Y	ND	Y	Y
User interaction	Y	Y	ND	Y	Y	N	Y	N	PD	N
Automatic service Discovery	Y	Y	N	ND	N	N	N	ND	N	N

Y-Done; N-Not Done; P- Partially Done; PD-Partially Discussed; ND-Not Discussed.

VIII. Conclusions and Future Work

The composition of services can meet the needs increasingly complex of user, by a combination of web services within a single business process. However, despite this widespread adoption of Web services, many obstacles prevent their reconciliation in the composition, or may occur within a BPEL process in a state change, the context for example. To solve this problem of the Web service adaptation invoked in a BPEL process and to satisfy the client context and web service context. In this paper, we proposed an adaptable Web service registry called CAC-WSR. Our solution based on SABPEL and AAWS-WSDL to publish a context aware composition. It supports saving and searching atomic and composite Web services according to adaptation criteria together with functional needs. We detailed our registry data structure and implementation. Our extension shows the importance of context-awareness in Web Service composition.

For future work, we will extend our approach to be used in the open world, in which the service composition should react to continuous and unanticipated changes in complex and uncertain contexts. We will continue to enhance our approach in the categories of context modeling, service discovery, service adaptation, and service composition. We are currently working on a prototype system to evaluate our approach by conducting more experiments to examine performance metrics including efficiency of service composition

IX. References

[1] B. Benatallah, R. Dijkman, M. Dumas and Z. Maamar, “Service Composition?: Concepts, Techniques, Tools and Trends,” In: Z. Stojanovi and A. Dahanayake, Eds., Service-Oriented Software System Engineering: Challenges and Practices, Idea Group, pp. 48-66, 2005.

[2] Cherif Sihem. R, Ben Djemaa, R., Amous. I. "ReMoSSA: Reference Model for Specification of Self-adaptive Service-Oriented-Architecture", ADBIS’2013, June 2013, Genoa, Italy.

[3] Cherif Sihem. R, Ben Djemaa, R., Amous. I. " SABPEL: Creating Self-Adaptive Business Processes", ICIS 2015: 619-626, June 2015, Las-Vigas, USA.

[4] Cheng. J, Liu. C, MengChu Zhou, Qingtian Zeng, Antti Yla-Jaaski, “Automatic Composition of Semantic Web Services Based on Fuzzy Predicate Petri Nets”, Automation Science and Engineering, IEEE Transactions on (Volume:12 , Issue: 2), 2015.

[5] El Hog C., Ben Djemaa R., Amous I., “A User-Aware Approach to Provide Adaptive Web Services”. The Journal of Universal Computer Science (JUCS’14), Vol. 20, No. 7, 2014. PP 944-963.

[6] Erl, T. SOA Design Patterns (The Prentice Hall Service-Oriented Computing Series). January 2009.

[7] Furno. A, Zimeo. E, “Context-aware Composition of Semantic Web Services”, Journal: Mobile Networks and Applications, Volume 19, Issue 2, pp 235-248, 2014.

[8] Grati.R., Boukadi.K., Ben-Abdallah.H,. A QoS Monitoring Framework for Composite Web Services in the Cloud. ADVCOMP 2012: The Sixth International Conference on Advanced Engineering Computing and Applications in Sciences. 2012.

[9] Hermosillo. G, L. Seinturier, L. Duchien, “Using Complex Event Processing for Dynamic Business Process Adaptation” in Proceedings of the 7th IEEE 2010 International Conference on Services Computing (SCC 2010), Miami, Florida : United States, 2010 .

[10] Koning. M, C.-a. Sun, M. Sinnema, and P. Avgeriou, “Vxbpel:Supporting variability for web services in bpel,” Inf.Softw.Technol., vol. 51, no. 2, pp. 258–269, 2009.

[11] Mcheick. H, Hannech. A, « Semantic Web Services Adaptation and Composition Method», ICIW 2013 : The Eighth International Conference on Internet and Web Applications and Services. 2013.

[12] Maamar. Z, Wives. L.K, Y. Badr, S. Elnaffar, K. Boukadi and N. Faci, “LinkedWS: A novel Web services discovery model based on the Metaphor of ”social networks”,” Simulation Modelling Practice and Theory, vol 19, 2011,pp.121-132,doi:10.1016/j.simpat.2010.06.018.

[13] Tigli, J.-Y., Lavirotte, S., Rey, G., Hourdin, V., Riveill, M. “Lightweight Service Oriented Architecture for Pervasive Computing” IJCSI International Journal of Computer Science Issues, Vol. 4, No. 1, ISSN (Online): 1694-0784, ISSN (Print): 1694-0814. September 2009.

[14] UDDI Spec Technical Committee Draft, http: //uddi.org/pubs/uddiv3.html.

[15] Azmeh, Z.: “A web Service Selection Framework for an Assisted SOA”; Thesis, (2011).

[16] Hafiddi, H., Baidouri, H., Nassar, M. , Kriouile, A.: “Context-Awareness for Service Oriented Systems”; CoRR, abs/1211.3229, (2012) .

[17] Madkour. M, el ghanami. I, maach. A “Context-Aware Service Adaptation: An Approach Based on Fuzzy Sets and Service Composition”. Journal of information science and engineering 29, 1-16. 2013.

[18] Cherif Sihem. R, Ben Djemaa, R., Amous. I. “Adaptable Web Service Registry for Publishing Context Aware Service Composition”. iiWas. 2015 (to appear).

[19] El Haddad. J, Manouvrier. M, Rukoz M, TQoS: transactional and QoS-aware selection algorithm for automatic Web service composition, IEEE Trans. Serv. Comput. 3 (1) (2010) 73–85.

[20] Ardagna. D, Baresi. L, Comai. S, Comuzzi. M, Barbara Pernici, A service-based framework for flexible business processes, IEEE Softw. 28 (2) (2011) 61–67.

[21] Yu. J, Han. J, Quan Z. Sheng, Steven O. Gunarso, PerCAS: an approach to enabling dynamic and personalized adaptation for context-aware services,in: Proceedings of the 10th International Conference on Service-Oriented Computing-(ICSOC-2012),-Springer-Verlag, Berlin, Heidelberg, 2012, pp. 173–190.

[22] Vukovic. M. “Context aware service composition”. Technical Report number 700.UCAM-CL-TR-700-ISSN-1476-2986. 2007.

[23] Ashraf Butt. T. “Provision of Adaptive and Context-Aware Service Discovery for the Internet of Things “.Doctoral Thesis. Loughborough University. 2013.

[24] Martin. C. “Composition flexible par planification automatique “, Doctoral Thesis. University Joseph Fourier, Laboratory of Informatics of Grenoble. France. 2013.

[25] Portchelvi. V. Venkatesan. P. “A Goal-Directed Orchestration Approach for Agile Service Composition”. I.J. Information Technology and Computer Science, 03, 60-67. 2015.

Analysis and Detection of the Zeus Botnet Crimeware

Laheeb Mohammed Ibrahim
Software Engineering
Mosul University, Collage of Computer Sc. & Math.
Mosul , Iraq

Karam H. Thanon
Software Engineering
Mosul University, Collage of Computer Sc. & Math.
Mosul , Iraq

***Abstract*— The raised significant evolution of the Internet next to the development of the high prevalence of computers, smart phones and the Internet on a large scale in most of the trends of life, but this use leads to network attacks. with a large use of e-commerce, they needs websites on the Internet. e-commerce represents a good reason for criminals or attackers to be diverted to profit law. Recently, the attackers used botnets to achieve their goals.**

A comprehensive study of botnet is done in this paper , study a life cycle of botnet, the attack on the behavior , topologies and technologies of botnet, studied of Zeus robots (An ethical penetration operation has been done using Zeus botnet version 1.2.7.19 and using Zeus version 2.0.8.9) were is done in in detail to determine its characteristics, and be able to detect it in the computers on the Internet.

Host Botnet Detection Software (HBD's) is designed and implemented to detect Zeus botnet in user's computers. The HDB's depends on information obtained from studying Zeus in addition to information obtained from analysis (an analysis of Zeus bot has been done by using reverse engineering tool (Ollydbg reverse engineering tool)) and penetration operation. In order to remove Zeus botnet from victim computers.

Keywords - Zeus, Host Botnet Detection Software (HBDS), Botnet, Ollydbg reverse engineering tool, Zeus botnet version 1.2.7.19 and using Zeus version 2.0.8.9

I. Introduction

Internet users have been attacked continuously by widespread E-mail viruses and worms. However, in recent years, a major virus or worm outbreak causing great loss has not been seen. This is not because the internet is much more secure, but more likely because attackers have shifted their attention to compromising and controlling victim computers; an attack scheme which provides more potential for personal profit and attack capability. This lucrative attack theme has produced a large number of botnets in the current internet [21].

Botnet now represents a great and dangerous digital crime for computer network and internet. Botnet challenges fall into two categories, First, botnet can be remote access by botmaster to run any command come from botmaster in victim computer and return results to him. Second, Botnet can be run in victim computer (user's computers) without user consent. So, many users may have bots run in their computers but they did not know anything about it.

According to Trend Micro, the first bot to appear was in 1999 and was named PrettyPark. PrettyPark bot implements a way of controlling malicious program remotely using IRC networks [26][32]. At the start of 2000, many sites such as Yahoo, eBay, Amazon, and CNN have been attacked by a Canadian hacker. During 2002, new communication protocols for bots/botnets were developed. From 2003, bots used different techniques to spread. Nowadays, bots can be delivered by most of the ways that current malware can. Today, bots are used for extortion, spam and phishing, identity theft, and malware seeding [14] [22] [32].

Zeus botnet is one of the dangerous botnets nowadays. It steals banking accounts for large money profits and it can steal any account (user name and password) typed in user computer infected by Zeus bot such as mails accounts or social websites accounts, etc. Zeus is a family of malicious software that focuses on stealing passwords for financial institutions, and includes several rootkit components to provide stealth capabilities. The Zeus malware, which originated in Russia has been in existence since 2007, and was continuously being updated and widespread in 2009. It is one of the largest botnets in existence, affecting approximately 75,000 computers in over 200 countries. It is possible to purchase a Zeus "bot-maker" kit on underground Internet forums, which can be used to generate malware that is distributed to victims via drive-by downloads or spam email campaigns [27].

The primary goal of the Zeus malware is to steal passwords and sensitive information for web-based financial accounts, which are then used to transfer stolen money to criminals [18] [24]. Zeus is known by many names (ZBOT due to its botnet capabilities, WSNPoem, PRG), and others—but its use has been particularly criminal [27].

Zeus is a malware package that is readily available for sale and also traded in underground forums. The package contains a builder that can generate a bot executable and Web server files (PHP, images, SQL templates) for use as the command and control server. While Zbot is a generic back door that allows full control by an unauthorized remote user, the primary function of Zbot is financial gain—stealing online credentials such as FTP, email, online banking, and other online passwords [4] [16] [33].

So, the main contribution is to paper, analyze, detect, and remove Zeus bot in computer networks and internet.

II. Related works

Binkley J. et.al. (2006), present an anomaly-based algorithm for detecting internet relay chat (IRC)-based botnet meshes. The algorithm combines an IRC mesh detection component with TCP scan detection heuristic called the TCP work weight. They discussed how to combine TCP-based anomaly detection with IRC tokenization and IRC message statistics to create a system that can clearly detect client botnets. Their system is deployed in their network and works well [2] [7] [9] [30].

"Peer-to-Peer Botnets: Overview and case" study was a research title from Grizzard J. B. *et al.* in 2007, where they present an overview of peer-to-peer botnets. Their case study of the Trojan. Peacomm bot demonstrates one implementation of peer-to-peer functionality used by a botnet [11] [29].

Gu G. et. al. presented in 2007 a prototype system, BotSniffer, that can capture spatial-temporal correlation in network traffic and utilize statistical algorithms to detect botnets with theoretical bounds on the false positive and false negative rates. They evaluated BotSniffer using many real-world network traces. The results show that BotSniffer can detect real-world botnets with high accuracy and has a very low false positive rate [5] [15] [31].

In 2008, Gu G. et. al. presented a general detection framework that is independent of botnet C&C protocol and structure, and required no a priori knowledge of botnets (such as captured bot binaries and hence the botnet signatures, and C&C server names/addresses). In their experimental evaluation on many real-world network traces, BotMiner showed excellent detection accuracy on various types of botnets (including IRC-based, HTTP based, and P2P-based botnets) with a very low false positive rate on normal traffic [4] [8] [17].

In 2008 Erbacher R. et. al. designed a multi-layered architecture for the detection of a wide range of existing and new botnets. The key advantage of the architecture is that it allows for the integration of wide ranging techniques. By allowing algorithms from other researchers to be integrated through the open architecture, they allow for the greatest possible detection strategy [19].

"Salvador P. et. al. presented in 2009 a new approach, based on neural networks, that is able to detect Zombie PCs based on the historical traffic profiles presented by "licit" and "illicit" network applications. The evaluation of the proposed methodology relies on traffic traces obtained in a controlled environment and composed by licit traffic measured from normal activity of network applications and malicious traffic synthetically generated using the SubSeven backdoor. The results obtained the proposed methodology was able to achieve good identification results [18][20**].**

Binsalleeh H. et. al. presented an analysis of the Zeus botnet Crimeware Toolkit in 2010. Their analysis aims to uncover the various obfuscation levels and shed light on the resulting code. In addition, they detail a method to extract the encryption key from the malware binary and use that to decrypt the network communications and the botnet configuration information. They present a detailed reverse engineering analysis of the Zeus crimeware toolkit to unveil its underlying architecture and enable its mitigation and designed a tool to automate the recovery of the encryption key and the extraction of the configuration information from the binary bot executable [6][27].

Al-Hammadi Y. presented in 2010 a framework as a host-based botnets /bots detection system. The detection of botnets or bots on the infected machine is performed by correlating bots' behavioral attributes. His framework is applied to various bots command and control structures such as IRC bots and P2P bots. An evaluation of the framework showed success in detecting malicious behaviors on the system [32].

Zang X. et. al. in 2011 presented a research in order to counter the escalation of the botnets evolution. The mining based detection methods operated on the flow level internet traffic have demonstrated some promising performances. A preliminary experiment has been conducted in this paper observing the discriminating capabilities of the Hierarchical and K mean clustering algorithms and exploring a RTT adjustment procedure to mix the botnet trace with the background internet traffic [30].

In 2011, Wang S. et. al. worked on Tracking Botnets using NetFlow and PageRank, where NetFlow related data is correlated and a host dependency model is leveraged for advanced data mining purposes. They extended the popular linkage analysis algorithm PageRank with an additional clustering process in order to efficiently detect stealthy botnets using peer-to-peer communication infrastructures .The key conceptual component in this approach is to analyze communication behavioral patterns and to infer potential botnet activities [6] [10].

In 2012, Nair H. et. al. presented a paper to discuss some of the botnet detection techniques and compare their advantages, disadvantages and features used in each technique. The botnet detection techniques can be classified into three types, namely honeypot, passive anomaly analysis and based on traffic application [13]**[** 23 **]**.

In 2012 Alomari E. et. al. presented a comprehensive study to show the danger of Botnet-based DDoS attacks on application layer, especially on the Web server and the increased incidents of such attacks that have evidently increased recently. Incidents around the world and revenue losses of famous companies and government Web sites are also described; indicating that extreme care should be taken and a further study should be conducted to assess the size of the problem and then derive an optimal solution [3] [18].

III. What is zeus

Zeus is a financial malware. It infects consumer PCs, waits for them to log onto a list of targeted banks and financial institutions, and then steals their credentials and sends them to a remote server in real time. Additionally, it may inject HTML into the pages rendered by the browser, so that its own content is displayed together (or instead of) the genuine pages from the bank's web server. Thus, it is able to ask the user to divulge more personal information, such as payment card number and PIN, one time passwords and TANs, etc. [28].

Zeus has two perspectives:

- From a technical perspective, it is a crime ware tool primarily used to steal money.
- From another perspective, it signals a new wave in online criminal business enterprise wherein many different organizations cooperate with one another to perpetrate outright online theft and fraud.

Fig. 1 shows how a typical Zeus infection takes place [27]. When a victim visits a targeted site, the bot steals the credentials that are entered by the victim. Afterward, it posts the encrypted information to a drop location that is meant to store the bot update reports. This server decrypts the stolen information and stores it into a database [6] [27]. The communication protocol used is HTTP, specifically HTTP POST requests to send stolen data and retrieve commands from the C&C server. All data packets are encrypted using RC4 encryption to avoid detection [1] [15][31].

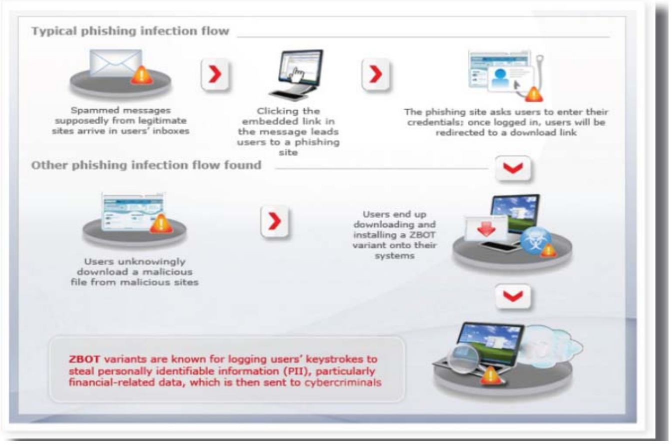

Typical phishing infection flow
Spammed messages supposedly from legitimate sites arrive in users' inboxes
Clicking the embedded link in the message leads users to a phishing site
The phishing site asks users to enter their credentials; once logged in, users will be redirected to a download link
Other phishing infection flow found
Users unknowingly download a malicious file from malicious sites
Users end up downloading and installing a ZBOT variant onto their systems
ZBOT variants are known for logging users' keystrokes to steal personally identifiable information (PII), particularly financial-related data, which is then sent to cybercriminals

Figure 1. Zeus Infection Diagram [27]

IV. Zeus Functions

Zeus bot has many functions to do. Some functions are related to the victim computer information that Zeus deals with, and others are related to the operating system.

Zeus functions are functions on victim computer information have main tasks and additional tasks; all of them are explained below :

1. **Main tasks :** The main purpose of Zeus is to steal online credentials as specified by the hacker. Zeus performs four main actions (Gathering system information, Stealing protected storage information, Stealing online credential information as specified by a configuration file, Contacting the command and control server for additional tasks to perform [16].
2. **Additional Tasks :** The Zeus has multiple built-in commands that can be executed as additional tasks. The execution of these commands can be created as tasks in the command and control server. When the bot connects to the server, the server will see if any active tasks should be sent to the bot for execution [16].

V. Zeus functions's on operating system of victim computer

Because Zbot is a package that is readily available, vectors of infection vary widely, with popular methods including drive-by download and SPAM. SPAM runs of Zbot are a regular occurrence using social engineering tactics, impersonating organizations such as the FDIC, IRS, MySpace, Facebook, and Microsoft. Once the bot is executed, the following actions take place [16][24].

- It adds a process to the path "system32\sdra64.exe".
- It sets the previous path to: "HKEY_LOCAL_MACHINE\Software\Microsoft\WindowsNT\winlogon\userinit", so that winlogon.exe spawns the process at startup time.
- It looks for winlogon.exe, increases its privileges, injects its code and a string table into this process, and creates a thread to execute this code.
- The main bot executable terminates.
- The injected code in winlogon injects additional code into svchost.exe.
- It also creates a folder named System \lowsec and puts two files inside: local.ds and user.ds. Local.ds is the latest dynamic configuration file downloaded from the server. User.ds contains stolen credentials and other information to be transmitted to the server.
- The code inside svchost is responsible for network communication and third-party process injection required to hook Internet-related APIs in order to inject or steal information to/from banking sites
- The communication between these various injected components is done with mutexes and pipes, maliciously named _AVIRA_x, where x is a number (eg: x=2109 in winlogon.exe, x=2108 in svchost.exe) [16].

If Zeus is run by using an account that does not have Administrator privileges, code will not be injected into winlogon.exe, but instead into explorer.exe. Also, instead of copying itself to the System folder, the bot will copy itself to UserProfile \Application Data\sdra64.exe, and create the folder UserProfile \Application Data\lowsec. Finally, the bot will create a load point under the registry key:

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\"userinit"=" UserProfile \Application Data\sdra64.exe" [16].

Once Zeus is installed, the malware waits until a user logs into a financial website that is specified in the configuration file. It then injects predetermined code into the browser to include additional textboxes for the user to enter sensitive information . The configuration file can be customized based on the user's location and language. An example of this injection is shown in Fig. 2. The malware logs the sensitive information and transmits it to the botmaster via encrypted network traffic [24].

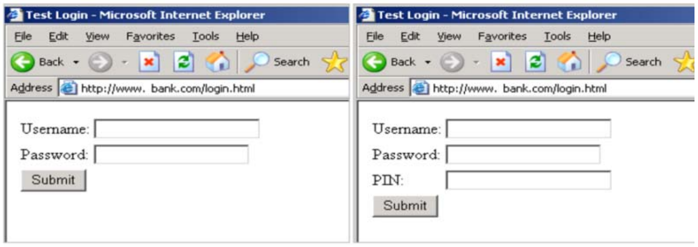

Test Login - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search
Address http://www. bank.com/login.html
Username:
Password:
Submit
Test Login - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search
Address http://www. bank.com/login.html
Username:
Password:
PIN:
Submit

Figure 2 Zeus/Zbot Login Form Injection [24]

Now an explanation of Zbot's general behavior after it has infected a system. Most of Zbot's data stealing logic is driven by the hooks it places inside processes. Here is a quick run-down of typical Zbot API hook as seen in table I [12].

The ntdll.dll hooks are intended to ensure that the Zbot memory resident component is injected into new processes and the new process's API's are hooked. Most of the rest are intended to monitor and steal data that those API's are used to send [12]

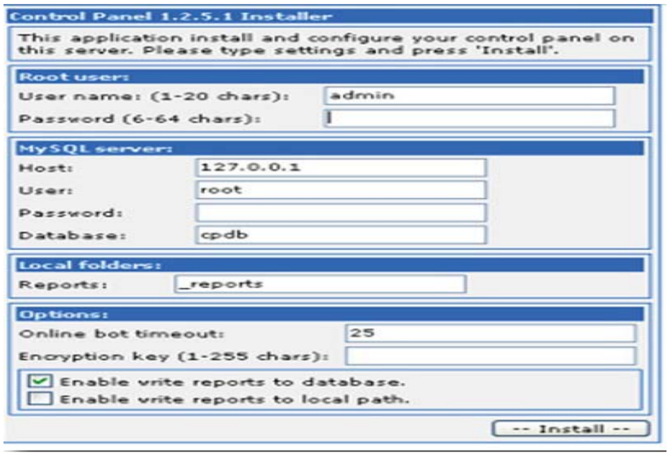
VI. Components of Zeus

The Zeus crimeware toolkit is a set of programs which have been designed to setup a botnet over a high-scaled networked infrastructure. Generally, the Zeus botnet aims to make machines behave as spying agents with the intent of getting financial benefits. The Zeus malware has the ability to log inputs that are entered by the user as well as to capture and alter data that are displayed into web-pages [25]. These components are:

1. **Control panel (server):** The Zeus Server is also remarkably simple to configure. A cybercriminal simply drops the Web server files onto his/her machine, looks for the install page, and fills in some very basic settings. Once set up, this server will receive all of the data Zeus bots steal. It also has many other features such as keeping tabs on how many infected users there are (based on OS, geographical location, and others) and running scripts on infected machines, just to name a few as shown in Fig. 3 [27].
2. **Configuration file:** All Zeus botnets are built based on a highly versatile configuration file. This file contains settings such as the botnet's name, the times it will send stolen information back, and the server the malware should connect to. More importantly, however, it contains a list of banks for Zeus to target. Zeus has the ability not only to gather all the banking login credentials and passwords users enter but also to directly inject extra form components into users' banking website view as mentioned earlier [27]. It is divided up into sections that start with "entry" with the two main being "entry 'StaticConfig'" and "entry 'DynamicConfig'". These two sections deal with the settings that will be hardcoded into the binary and the settings that will be written into the configuration file and downloaded at runtime.

TABLE I. TYPICAL ZBOT API HOOK

Dll Name	Api Name	Dll Name	Api Name
ntdll.dll	NtCreateThread (pre Vista)	user32.dll	BeginPaint
ntdll.dll	NtCreateUserProcess (Vista and later)	user32.dll	EndPaint
ntdll.dll	LdrLoadDll	user32.dll	GetDCEx
kernel32.dll	GetFileAttributesExW	user32.dll	GetDC
wininet.dll	HttpSendRequest	user32.dll	GetWindowDC
wininet.dll	HttpSendRequestEx	user32.dll	ReleaseDC
wininet.dll	InternetCloseHandle	user32.dll	GetUpdateRect
wininet.dll	InternetReadFile	user32.dll	GetUpdateRgn
wininet.dll	InternetReadFileEx	user32.dll	GetMessagePos
wininet.dll	InternetQueryDataAvailable	user32.dll	GetCursorPos
wininet.dll	HttpQueryInfo	user32.dll	SetCursorPos
ws2_32.dll	Closesocket	user32.dll	SetCapture
ws2_32.dll	Send	user32.dll	ReleaseCapture
ws2_32.dll	WSASend	user32.dll	GetCapture
user32.dll	OpenInputDesktop	user32.dll	GetMessage
Dll Name	**Api Name**	**Dll Name**	**Api Name**
user32.dll	SwitchDesktop	user32.dll	PeekMessage
user32.dll	DefWindowProc	user32.dll	TranslateMessage
user32.dll	DefDlgProc	user32.dll	GetClipboardData
user32.dll	DefFrameProc	crypt32.dll	PFXImportCertStore
user32.dll	DefMDIChildProc	nspr4.dll	PR_OpenTCPSocket
user32.dll	CallWindowProc	nspr4.dll	PR_Close
user32.dll	RegisterClass	nspr4.dll	PR_Read
user32.dll	RegisterClassEx	nspr4.dll	PR_Write


Control Panel 1.2.5.1 Installer

This application install and configure your control panel on this server. Please type settings and press 'Install'.

Root user:
User name: (1-20 chars): admin
Password (6-64 chars):

MySQL server:
Host: 127.0.0.1
User: root
Password:
Database: cpdb

Local folders:
Reports: _reports

Options:
Online bot timeout: 25
Encryption key (1-255 chars):
☑ Enable write reports to database.
☐ Enable write reports to local path.

Figure 3. Zeus Server Installation Page

The static options include timing options (how long to wait between attempting to download the config file etc...), the URL from which the configuration file is downloaded, and a URL that is used to check the external IP address that the bot is phoning home from. These will be written into the binary when it is distributed [12].

The dynamic options mainly centre on what particular web addresses the bot owner wants to target but there are also several housekeeping entries, including:

- A URL from which a new Zbot executable will be downloaded.
- A URL to which stolen data is sent back.
- A URL at which a further configuration file can be downloaded.

The other dynamic options include:

- A set of URL masks that enable or disable logging for those URLS.
- A set of URL pairs where one URL is redirected to the other URL.
- A group of URL's from which TAN's (Transaction Authentication Number) will be harvested.
- A set of IP/domain pairs that will be written into the hosts file to hijack DNS requests.
- A set of URL masks each with a corresponding block of HTML that will be injected into any page whose request matches the URL mask (Web Injects) [20].

3. **Encrypted configuration file:** *Zeus Builder* then takes this configuration file and encrypts it. All Zeus bots regularly dial home and download the encrypted configuration file to see if they have already received new orders, which, of course, make security researchers' jobs more difficult. Receiving a copy of an encrypted configuration file does not tell researchers anything unless we can also extract the encryption key from the corresponding Zeus binary[18].

   Criminals who use Zeus now take both the encrypted configuration file and the Zeus binary, which they created with *Zeus Builder*, and place them on a Web server. Zeus allows either each component to be placed on a separate Web server or all of its components on a single Web server.

4. **Binary file:** when user's system is infected by the binary, it will apply the latest version of its configuration settings and begin stealing the user's personally identifiable information (PII). After only a few mouse clicks, cybercriminals can get access to a fully functional banking Trojan or botnet [18].

   The executable can be built with the "Build loader" button. The Builder will embed the information needed to retrieve and decrypt the configuration file into the Zbot binary before packing it with its own custom run-time packer. Generally speaking, Zeus customers will then pack the executable again with some other packer [20].

5. **Zeus builder:** *Zeus Builder* is one of the key parts of the Zeus toolkit. It is responsible for creating the binary file used to make the botnet as well as the configuration file that stores all of the botnet's settings. When a criminal first runs *Zeus Builder*, they are presented with a simple screen that shows information about the Zeus version they purchased. Interestingly, however, Zeus also checks if the local system is currently already infected by the Zeus malware, which gives the user an opportunity to remove it practical implementation. [27]

VII. Practical IMplementation

Zeus is very difficult to detect even with up-to-date antivirus software. This is the primary reason why its malware family is considered the largest botnet on the internet. Security experts are advising that businesses continue to offer training to users to prevent them from clicking hostile or suspicious links in emails or on the web while also keeping up with antivirus updates. Symantec claims its Symantec Browser Protection can prevent "some infection attempts" but it remains unclear if modern antivirus software is effective to prevent all of its variants from taking root [33]. Removal of the Zeus rootkit was confirmed by rebooting and performing subsequent scans of corroborating tools, as well as observing the lack of certain behaviors, such as the hiding of the System32/lowsec directory [24].

Fig. 4 represents a flow chart that explains the general scheme of the work, starting with botmaster who creates Zeus bot using Zeus builder, then this bot used in penetration, analysis, detection, removal operations. The penetration operation uses Zeus bot and depends on the study. So it results in Zeus database creation at the botmaster's command and control. The analysis process analyzes Zeus bot and creates a report with many information about Zeus bot such as CPU, registers, and memory information etc... The detection process depends on penetration and analysis information besides to our paper to give a report that is explains if the user computer infected or not. Finally The removal process uses all above process information to have the ability to remove Zeus bot from user computer and give a report presented to user that Zeus has been removed successfully.

A. *Penetration process*

At this stage, penetration processes are done to a victim computer by server computer because Zeus botnet work as client –server model using http protocol to communicate between botmaster and any bot at victim computer.

To do this, a suitable configuration and installation must be done for C&C server which the botmaster uses to control botnet network that it manages at server side.

Fig. 5 explains the main steps for penetration operation using windows XP operating system (O.S) and using windows seven operating system (O.S) besides to two different versions of Zeus bot. Zeus bot version 1.2.7.19 and Zeus bot version 2.0.8.9.

To penetration windows XP operating system Botmaster needs the following steps to configure and prepare its computer to have the ability to run its command and control:

1. Penetration windows XP operating system

Botmaster needs the following steps to configure and prepare its computer to have the ability to run its command and control:

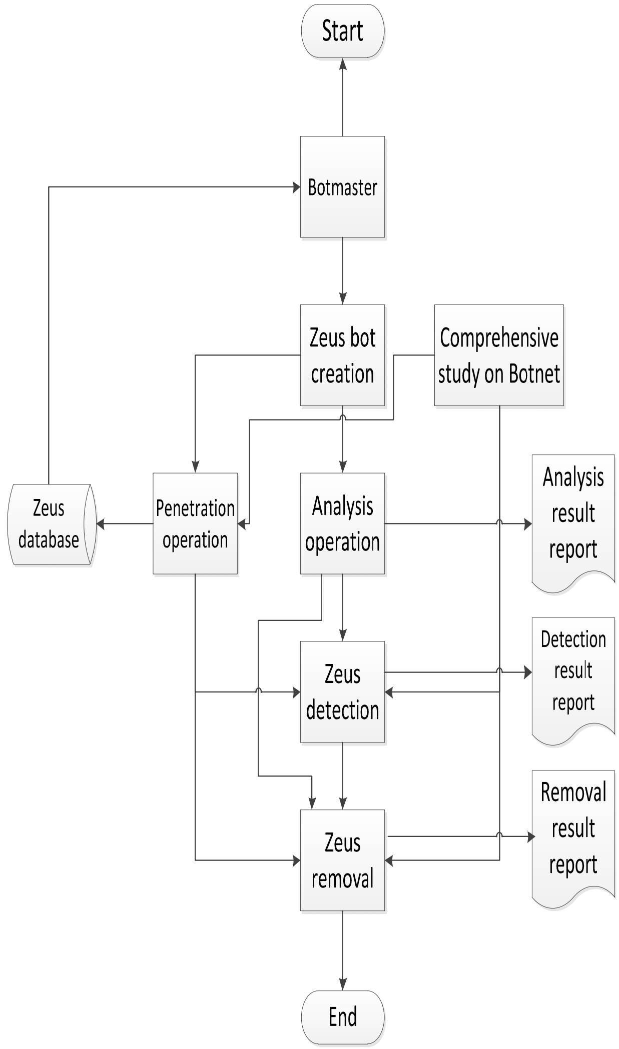


Figure 4. General Scheme Of Practical Implementation And Analysis

a) Installing a program that makes any computer as (web server) needed. There are many programs to do this, such as (Appserv) or (Xampp). In this paper, Xampp is used with version 1.7.3 to enable us to do this work. **Appendix A-1** explains the main window for Xampp program.

b) At this step, the server computer of botmaster must Listen to a specific IP that represents the server computer IP and port number which should be listen to, and which is (80) here and represents http protocol port that Zeus bot used, after Zeus bot infects the victim computer, it sends any collected information to the botmaster through command and control run at botmaster server's computer. So, server computer must listen to have the ability to get and save the information received from victim computer bot. To do this, an edit process will be done to some information in the file named (httpd.conf) by adding botmaster server computer IP with port number (80). This file exists at this path:
"C: \ xampp \ appserv \ conf \". **Appendix A-2** shows an example of this configuration file.

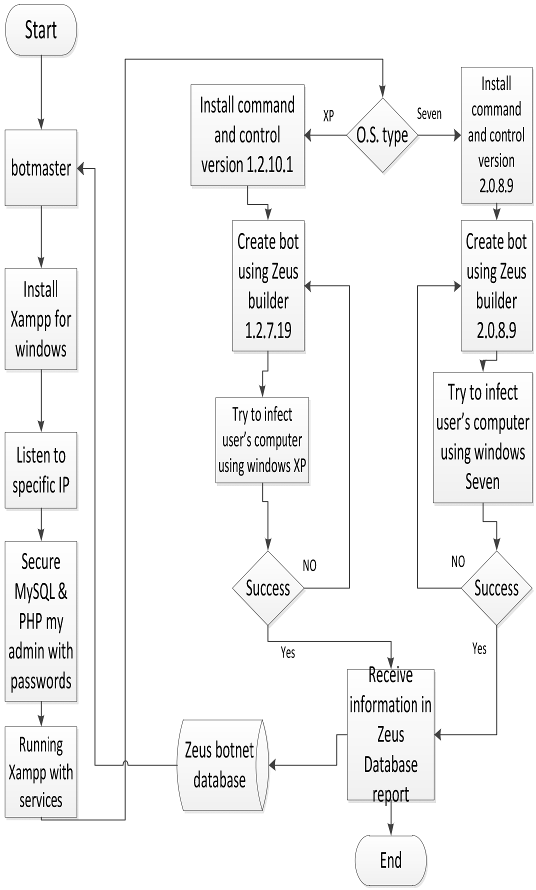

Start
botmaster
Install Xampp for windows
Listen to specific IP
Secure MySQL & PHP my admin with passwords
Running Xampp with services
O.S. type
XP
Seven
Install command and control version 1.2.10.1
Install command and control version 2.0.8.9
Create bot using Zeus builder 1.2.7.19
Create bot using Zeus builder 2.0.8.9
Try to infect user's computer using windows XP
Try to infect user's computer using windows Seven
Success
NO
Yes
Success
NO
Yes
Receive information in Zeus Database report
Zeus botnet database
End

Figure 5. Penetration Operation Scheme

c) In order to manipulate Zeus command and control and run it by botmaster at a server computer, a copy of a command and control files must be transferred to this path:
"c:\xampp\htdocs\xampp". Also a suitable folder name for these (.php) files such as (botnetserver) must be selected because it will be useful later to access Zeus command and control by internet explorer. **Appendix A-3** shows the content of Zeus command and control version 1.2.7.19 files.

d) Running Xampp program by using control panel which belongs to Xampp is next step. Two services must be activated to work in a right manner as shown in **Appendix A-4**. These services are first Appserv which enables to implement the programming code related with command and control written in PHP language. Second is to run MySQL service which will help to manipulate Zeus botnet Database. Then, an internet browser must be run, and then entered to Xampp program through address line. After this, a strong password for MySQL must be chosen with the super user (root) as a user name because this user name has the full permissions to manage database such as (add, edit or delete).

e) The next step is to select "phpmyadmin" from Xampp program which represents a graphical user interface (GUI) to give facilities when working with databases instead of writing instructions and line commands using MySQL. The great benefit here is to create a database for Zeus botnet which will contain any information that comes from bot to botmaster as shown **Appendix A-5.**

f) All above steps prepare a suitable environment to install Zeus command and control on botmaster server computer and use it. In order to do that, this line is written in the address line of the internet browser:
"Your IP\xampp\botnetserver\install\index.php". As a result, Zeus command and control will be displayed as shown in **Appendix A-6.** So the fields must be filled and then the install is chosen.

After that, Zeus command and control will be ready for use as shown in **Appendix A-7**. At this point, the installation process for Zeus command and control at botmaster computer is finished.

g) In order to build and create Zeus bot, Zeus builder toolkit with version 1.2.7.19 will be used. **Appendix A-8** Shows Zeus builder window. When select "builder" to build Zeus bot as shown **in Appendix A-9**, a suitable configuration to Zeus bot configure file must be done by "Edit config" option in the builder window, then "build config" option will create Zeus configuration file (cfg.bin). **Appendix A-10** shows a sample of Zeus bot configuration file. This file contains the information needed for Zeus bot after penetrate victim's computer to connect with botmaster in a right manner, besides a list of websites that Zeus dealt with. "Build loader" option creates bot execution file (bot.exe) which is used to penetrate victim computer by botmaster.

h) After user's computer was penetrated and infected, botmaster must notice a change on his server computer at the option (Total bots) in the command and control window, this number represent the number of Zeus bot which can the botmaster managed at this time. So botmaster can manipulate with these bots and managed them and give them any command he wants from any of Zeus commands. **Appendix A-11**shows Zeus control panel with total bots =1 which means successful penetration operation.
The operating system of the victim's computer can be shown at botmaster C&C. when botmaster select "OS" option at his C&C; he can know victim computer operating system. In this penetration operation, victim computer's operating system is windows XP professional service pack 3 as shown in **Appendix A-12.**

2. Penetration windows seven operating system

Zeus Builder version 2.0.8.9 can build a bot that can penetrate windows seven operating system and steals passwords from victim computers that's used this operating system.

Botmaster needs the following steps to configure and prepare his computer in order to penetrate windows seven operating system victim computers.

a) Executing the first five steps explained previously in section (**Penetration windows XP operating system**). These steps include a complete configuration for botmaster computer to run as a server and communicate with the bot successfully.

b) Opening Zeus 2.0.8.9 control panel installer window by typing this line in the address line of your browser.
"Your IP/Xamp/botnetserver/install/index.php".

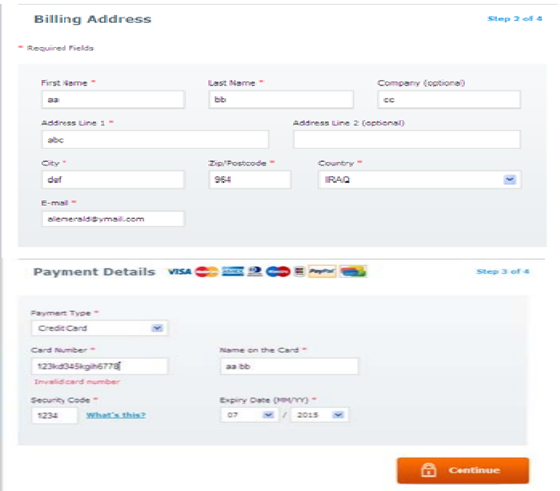
3. Penetration experiments and results

Three main types of experiments were done ethically on victim's computer to get results in botmaster computer, these types are financial sites experiments, social sites experiments and experiments using virtual keyboard.

a) **Financial site experiments**: When user tries to buy his needs using internet, he must pay online. Many experiments are done, one of them, a user tries to buy an antivirus program online, the program's site presents some field that must filled to buy the software such as name, address, payment type and card number etc. as shown in Fig. 6. After user finish, Zeus bot works and send all the information to the botmaster. In order to get this information by botmaster he must select "search database" option from command and control then open the site and get a report from bot. Total number of reports always increased by one every time bot sends information to botmaster. Fig. 7 shows the report at botmaster C&C which explains all information that user entered previously at financial site.

b) **Social sites experiments**: Many experiments are done on Google mail, Facebook, twitter social site.

c) **Experiment using virtual keyboard**: Virtual keyboard are supplied by windows operating system and some website to enter username and passwords in their site without using computer‘s keyboard. For example a situation when user tries to sign in in the bank of Baghdad which provide embedded virtual keyboard as shown in Fig. 8 The result is found in a report added to Zeus database at botmaster's command and control. Fig. 9 shows this report in database with all information about victim computer.



Billing Address — Step 2 of 4

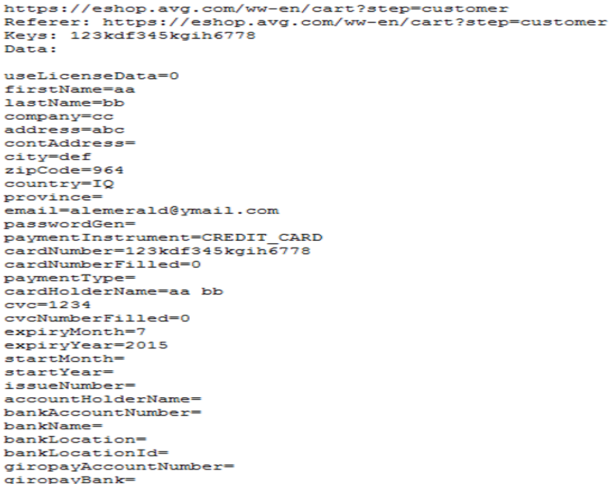
* Required Fields

First Name *: aa	Last Name *: bb	Company (optional): cc
Address Line 1 *: abc	Address Line 2 (optional):	
City *: def	Zip/Postcode *: 964	Country *: IRAQ
E-mail *: alemerald@ymail.com		

Payment Details — Step 3 of 4

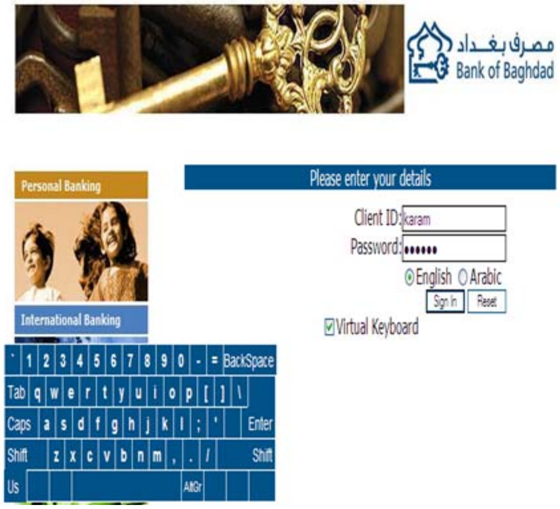
Payment Type *: Credit Card	
Card Number *: 123kd345kgih6778 Invalid card number	Name on the Card *: aa bb
Security Code *: 1234	Expiry Date (MM/YY) *: 07 / 2015

Figure 6. Online Payments On A Website



```
https://eshop.avg.com/ww-en/cart?step=customer
Referer: https://eshop.avg.com/ww-en/cart?step=customer
Keys: 123kdf345kgih6778
Data:

useLicenseData=0
firstName=aa
lastName=bb
company=cc
address=abc
contAddress=
city=def
zipCode=964
country=IQ
province=
email=alemerald@ymail.com
passwordGen=
paymentInstrument=CREDIT_CARD
cardNumber=123kdf345kgih6778
cardNumberFilled=0
paymentType=
cardHolderName=aa bb
cvc=1234
cvcNumberFilled=0
expiryMonth=7
expiryYear=2015
startMonth=
startYear=
issueNumber=
accountHolderName=
bankAccountNumber=
bankName=
bankLocation=
bankLocationId=
giropayAccountNumber=
giropayBank=
```

Figure 7. Database report of financial site

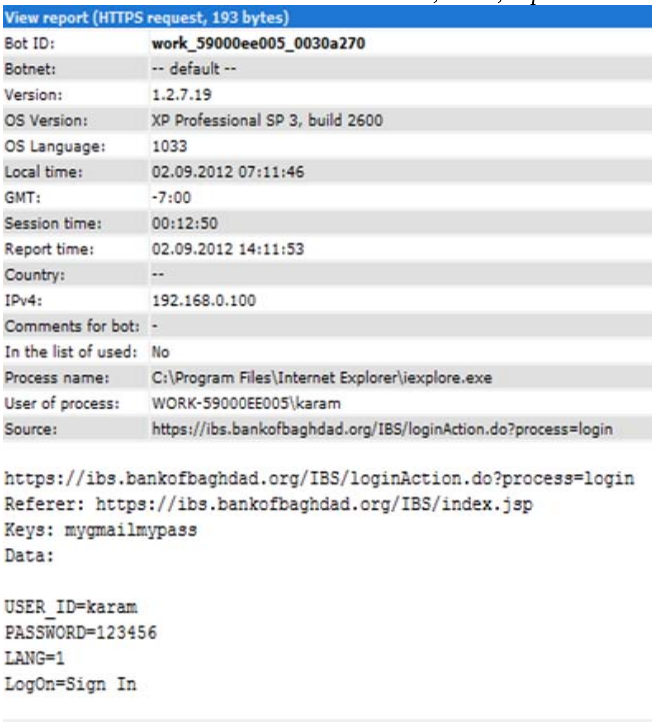


مصرف بغداد
Bank of Baghdad
Personal Banking
International Banking
Please enter your details

Client ID: karam
Password: ••••••
○ English ○ Arabic

Sign In
Reset
☑ Virtual Keyboard
` 1 2 3 4 5 6 7 8 9 0 - = BackSpace
Tab q w e r t y u i o p [ ] \
Caps a s d f g h j k l ; ' Enter
Shift z x c v b n m , . / Shift
Us AltGr

Figure 8. Bank Of Baghdad Sign In Window



View report (HTTPS request, 193 bytes)

Bot ID:	work_59000ee005_0030a270
Botnet:	-- default --
Version:	1.2.7.19
OS Version:	XP Professional SP 3, build 2600
OS Language:	1033
Local time:	02.09.2012 07:11:46
GMT:	-7:00
Session time:	00:12:50
Report time:	02.09.2012 14:11:53
Country:	--
IPv4:	192.168.0.100
Comments for bot:	-
In the list of used:	No
Process name:	C:\Program Files\Internet Explorer\iexplore.exe
User of process:	WORK-59000EE005\karam
Source:	https://ibs.bankofbaghdad.org/IBS/loginAction.do?process=login

```
https://ibs.bankofbaghdad.org/IBS/loginAction.do?process=login
Referer: https://ibs.bankofbaghdad.org/IBS/index.jsp
Keys: mygmailmypass
Data:

USER_ID=karam
PASSWORD=123456
LANG=1
LogOn=Sign In
```

Figure 9 Bank Of Baghdad Sign In Report In Zeus Database

B. *Zeus bot analysis using reverse engineering tool*

It is very difficult to analyze bots without using reverse engineering tools. The analysis operation using reverse engineering tool is useful for programmers and professionals whose work is with network security research field or work in security institutes and security labs. In order to analyze Zeus bot, software for reverse engineering tool called “olly debug” will be used. Fig. 10 presents the main stages of Zeus bot analysis using ollydbg reverse engineering tool.

In order to analyze Zeus, just select open and select Zeus bot which is created previously using Zeus builder version 1.2.7.19. Fig. 11 explains Ollydbg window after opening Zeus bot (bot.exe). As seen, there are many windows that appear in this program. Each of them represents some information about Zeus bot such as CPU window, memory map window etc… Each one of them will be explained in this section Opening the bot (bot.exe) results in:

- New process with Id 00000A90 is created. So this process is “sedra64.exe” which the Zeus bot adds to the path “C:\windows\system32”. When the host botnet detection program for Zeus is designed, this important point must be taken to detect Zeus bot.
- Main thread with Id 00000AB0 is created. This is a thread added to winlogin.exe process and created when Zeus bot is executed in the victim computer. Then the log data window shows a group of (.dll files) that is loaded when opening Zeus bot for analysis such as kernal32.dll, ntdll.dll and user32.dll. This process creation and thread creation operation must be deal with when removing Zeus

bot from victim computer or preventing Zeus bot from infected users' computers.

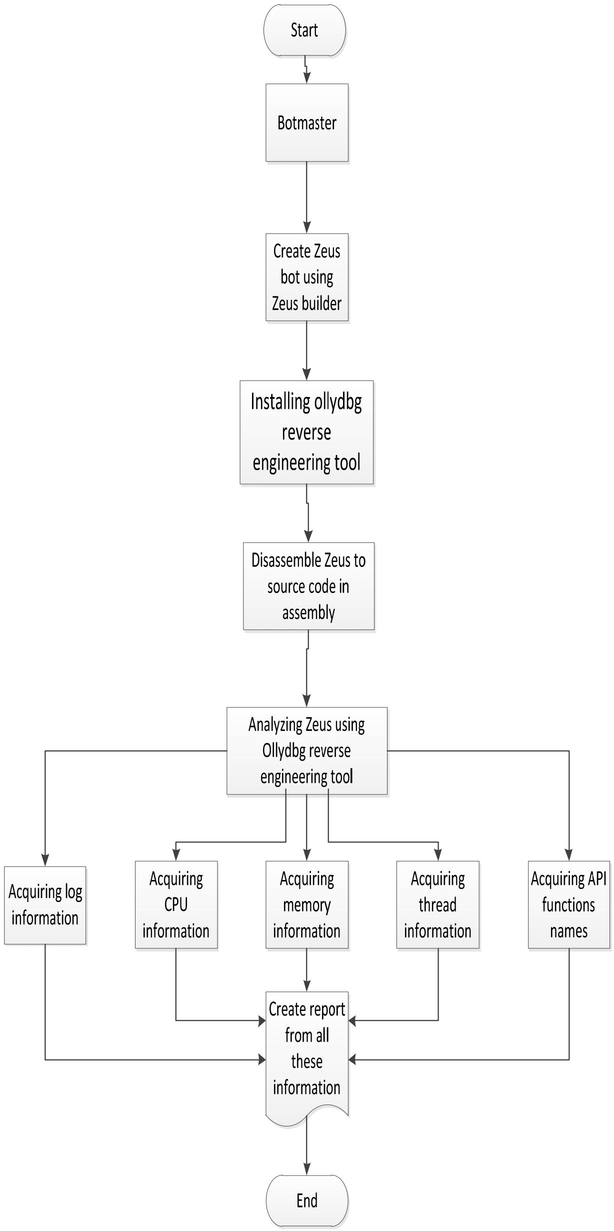

Start
Botmaster
Create Zeus bot using Zeus builder
Installing ollydbg reverse engineering tool
Disassemble Zeus to source code in assembly
Analyzing Zeus using Ollydbg reverse engineering tool
Acquiring log information
Acquiring CPU information
Acquiring memory information
Acquiring thread information
Acquiring API functions names
Create report from all these information
End

Figure 10. Analysis Operation Scheme

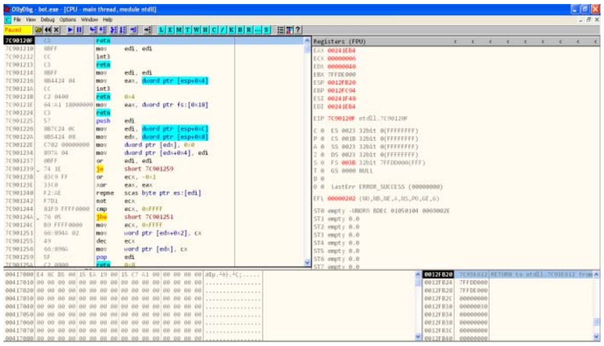
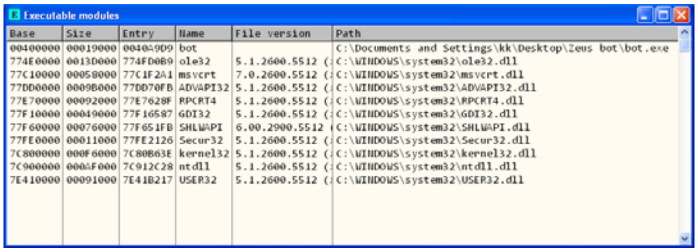


Figure 11. Ollydbg Window After Opening Zeus Bot

Executable modules window which is shown in Fig. 12 presents executable run. The first line Zeus bot is shown with the base address 00400000 in Hexadecimal with size 19000 byte, with name bot and path which was opened from it previously in addition to Zeus bot entry point 0040A9D9. This information gives us Zeus base address in memory with the total size and entry point address that Zeus uses when it implements in victim's computers. The rest of the information in executable modules is about DLL windows used into the system with their paths, versions and entry points for each windows DLL system file that has been used.



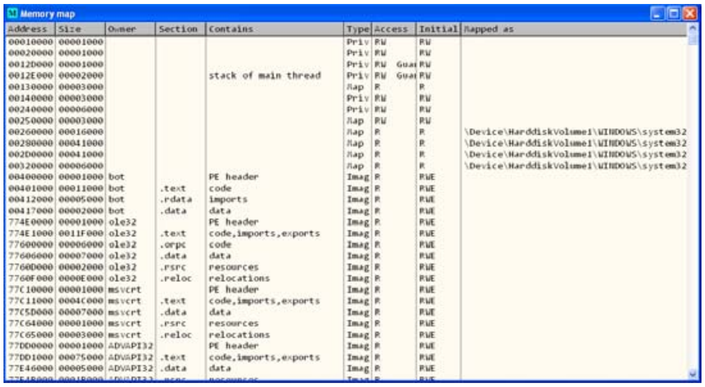
```
Executable modules
Base     Size     Entry    Name     File version      Path
00400000 00019000 0040A9D9 bot                        C:\Documents and Settings\kk\Desktop\Zeus bot\bot.exe
774E0000 0013D000 774FD0B9 ole32    5.1.2600.5512 (  C:\WINDOWS\system32\ole32.dll
77C10000 00058000 77C1F2A1 msvcrt   7.0.2600.5512 (  C:\WINDOWS\system32\msvcrt.dll
77DD0000 0009B000 77DD70FB ADVAPI32 5.1.2600.5512 (  C:\WINDOWS\system32\ADVAPI32.dll
77E70000 00092000 77E7628F RPCRT4   5.1.2600.5512 (  C:\WINDOWS\system32\RPCRT4.dll
77F10000 00049000 77F16587 GDI32    5.1.2600.5512 (  C:\WINDOWS\system32\GDI32.dll
77F60000 00076000 77F651FB SHLWAPI  6.00.2900.5512 ( C:\WINDOWS\system32\SHLWAPI.dll
77FE0000 00011000 77FE2126 Secur32  5.1.2600.5512 (  C:\WINDOWS\system32\Secur32.dll
7C800000 000F6000 7C80B63E kernel32 5.1.2600.5512 (  C:\WINDOWS\system32\kernel32.dll
7C900000 000AF000 7C912C28 ntdll    5.1.2600.5512 (  C:\WINDOWS\system32\ntdll.dll
7E410000 00091000 7E41B217 USER32   5.1.2600.5512 (  C:\WINDOWS\system32\USER32.dll
```

Figure 12. Executable Modules by Zeus

Memory map can be seen in Fig. 13 which explain Zeus memory map in four lines:

- At the address 00400000, there is PE header which means bot header with size 1000 byte.
- At the address 00401000, there is code of Zeus which is (.text) of the size 11000 byte.
- At the address 00412000, there is 5000 byte size of data containing imports function that Zeus uses.
- Finally, the rest of the data of Zeus bot begins at 00417000-00419000.

All these sections have the permission to read and write at corresponding memory locations explained above.



```
Memory map
Address  Size     Owner    Section Contains               Type Access    Initial Mapped as
00010000 00001000                                         Priv RW        RW
00020000 00001000                                         Priv RW        RW
0012D000 00001000                                         Priv RW   Gua  RW
0012E000 00002000                  stack of main thread   Priv RW   Gua  RW
00130000 00003000                                         Map  R         R
00140000 00003000                                         Priv RW        RW
00240000 00006000                                         Priv RW        RW
00250000 00003000                                         Map  RW        RW
00260000 00016000                                         Map  R         R       \Device\HarddiskVolume1\WINDOWS\system32
00280000 00041000                                         Map  R         R       \Device\HarddiskVolume1\WINDOWS\system32
002D0000 00041000                                         Map  R         R       \Device\HarddiskVolume1\WINDOWS\system32
00320000 00006000                                         Map  R         R       \Device\HarddiskVolume1\WINDOWS\system32
00400000 00001000 bot              PE header              Imag R         RWE
00401000 00011000 bot      .text   code                   Imag R         RWE
00412000 00005000 bot      .rdata  imports                Imag R         RWE
00417000 00002000 bot      .data   data                   Imag R         RWE
774E0000 00001000 ole32            PE header              Imag R         RWE
774E1000 0011F000 ole32    .text   code,imports,exports   Imag R         RWE
77600000 00006000 ole32    .orpc   code                   Imag R         RWE
77606000 00007000 ole32    .data   data                   Imag R         RWE
7760D000 00002000 ole32    .rsrc   resources              Imag R         RWE
7760F000 0000E000 ole32    .reloc  relocations            Imag R         RWE
77C10000 00001000 msvcrt           PE header              Imag R         RWE
77C11000 0004C000 msvcrt   .text   code,imports,exports   Imag R         RWE
77C5D000 00007000 msvcrt   .data   data                   Imag R         RWE
77C64000 00001000 msvcrt   .rsrc   resources              Imag R         RWE
77C65000 00003000 msvcrt   .reloc  relocations            Imag R         RWE
77DD0000 00001000 ADVAPI32         PE header              Imag R         RWE
77DD1000 00075000 ADVAPI32 .text   code,imports,exports   Imag R         RWE
77E46000 00005000 ADVAPI32 .data   data                   Imag R         RWE
```

Figure 13. Zeus Memory Map

C. *Zeus detection software*

Host botnet detection software is designed and implemented using C# programing language. This detection process is done after studying Zeus botnet in details as shown previously in chapter three. Ethical penetration process is implemented on computers on internet besides the useful information obtained from analyzing Zeus botnet. Fig. 14 shows a scheme about Zeus bot detection system.

The main goal of this (HBDS) is to detect Zeus bot in computer network and internet. The two important ideas in this software are searching for Zeus botnet files in two main locations (windows folders and windows registry).

After the computer has become a victim and is infected by botmaster using Zeus bot, the modification to windows XP operating system folders and its registry are explained in Fig. 15 and 16 respectively. Just scan the computer, and the HBDS will work and give a message that explains if this computer is infected with Zeus bot or not. If the computer is not infected, an advice is given to the user to protect his computer and information. If the result of the HBDS is that the computer is infected, advice is given to the user to firstly use our removal operation steps to clean up his computer.

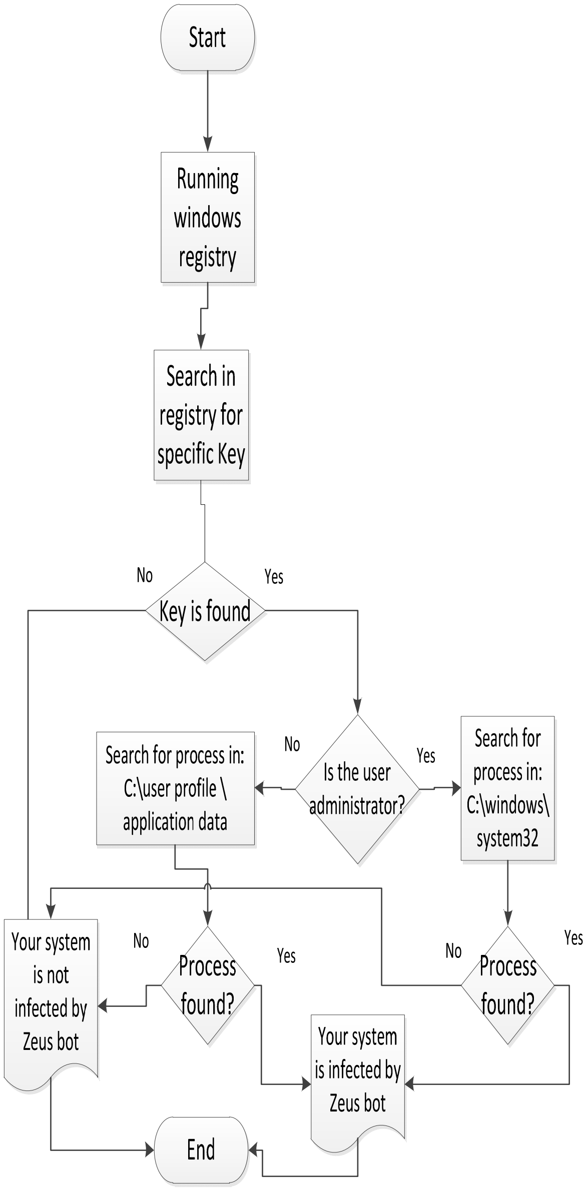
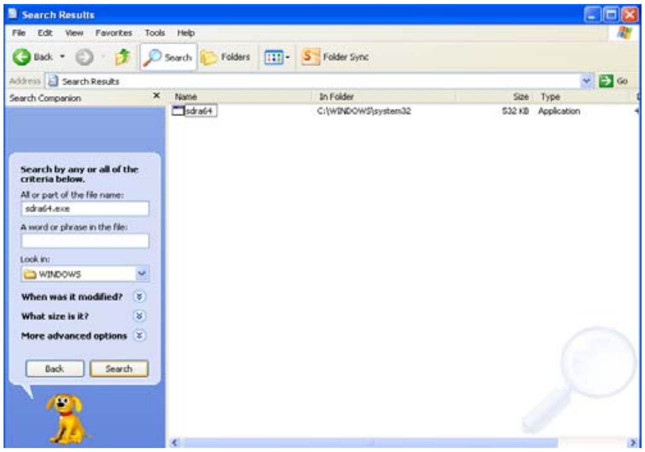

Start
Running windows registry
Search in registry for specific Key
No
Yes
Key is found
Search for process in: C:\user profile \ application data
No
Is the user administrator?
Yes
Search for process in: C:\windows\ system32
Your system is not infected by Zeus bot
No
Process found?
Yes
No
Process found?
Yes
Your system is infected by Zeus bot
End

Figure 14. Zeus Bot Detection Operation Scheme



Address: Search Results

Name	In Folder	Size	Type
sdra64	C:\WINDOWS\system32	532 KB	Application

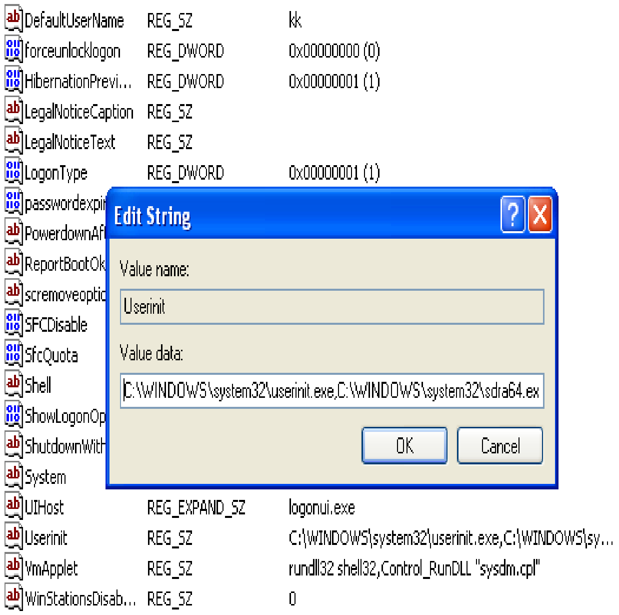
Search by any or all of the criteria below.

All or part of the file name: sdra64.exe

A word or phrase in the file:

Look in: WINDOWS

Figure 15. Infected Windows XP Operating System By Zeus



DefaultUserName	REG_SZ	kk
forceunlocklogon	REG_DWORD	0x00000000 (0)
HibernationPrevi...	REG_DWORD	0x00000001 (1)
LegalNoticeCaption	REG_SZ	
LegalNoticeText	REG_SZ	
LogonType	REG_DWORD	0x00000001 (1)
passwordexpi		
PowerdownAf		
ReportBootOk		
scremoveoptic		
SFCDisable		
SfcQuota		
Shell		
ShowLogonOp		
ShutdownWith		
System		
UIHost	REG_EXPAND_SZ	logonui.exe
Userinit	REG_SZ	C:\WINDOWS\system32\userinit.exe,C:\WINDOWS\sy...
VmApplet	REG_SZ	rundll32 shell32,Control_RunDLL "sysdm.cpl"
WinStationsDisab...	REG_SZ	0

Edit String

Value name: Userinit

Value data: C:\WINDOWS\system32\userinit.exe,C:\WINDOWS\system32\sdra64.ex

OK Cancel

Figure 16. Infected Windows Registry By Zeus

D. Zeus bot removal process

After detecting the Zeus bot in a victim computer that uses internet, a suitable reactive process that represents the user action after knowing that his computer was infected will be needed. Fig. 17 shows the main steps that is must be followed to remove Zeus bot from user's computers.

First, Zeus bot must be stopped from working then, it must be delete from the victim computer. In order to stop and remove Zeus bot, an assistance program will be needed to perform this action. The program "process explorer" is used in our work. This program is like a task manager with windows operating system, but the process explorer shows every task running at a time with all threads running and belonging to specific process. The Process Explorer is described as an advanced process management utility that picks up where Task Manager leaves off. It will show you detailed information about a process including its icon, command-line, full image path, memory statistics, user account, security attributes, and more. When you zoom in on a particular process, you can list the DLLs it has loaded or the operating system resource handles it has opened. A search capability enables you to track down a process that has a resource opened, such as a file, directory or Registry key, or to view the list of processes that have a DLL loaded. Fig. 18 shows process explorer program's window.

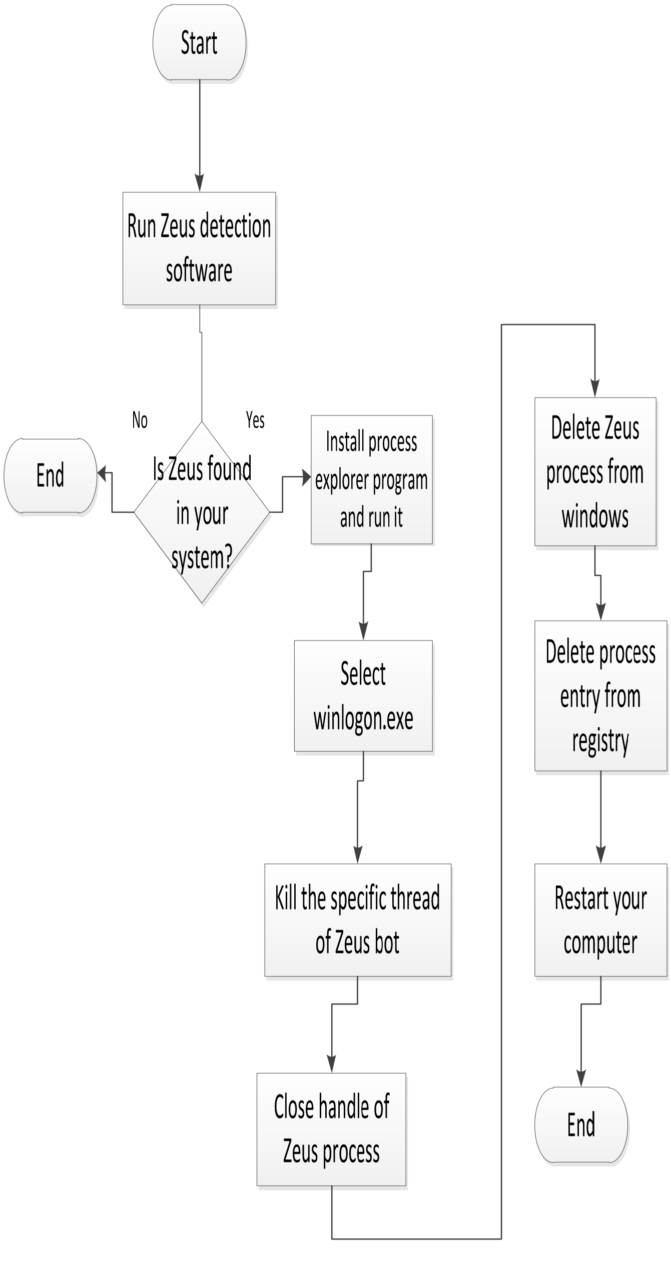
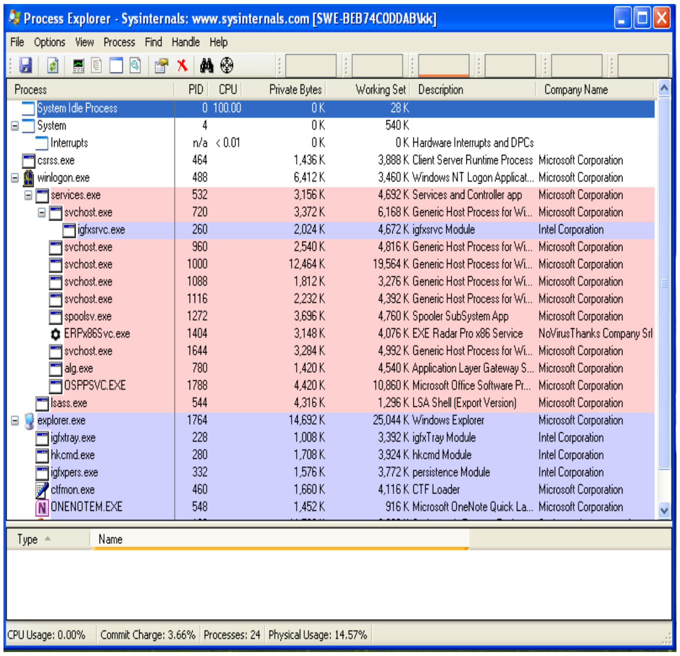

Start
Run Zeus detection software
Is Zeus found in your system?
No
Yes
End
Install process explorer program and run it
Select winlogon.exe
Kill the specific thread of Zeus bot
Close handle of Zeus process
Delete Zeus process from windows
Delete process entry from registry
Restart your computer
End

Figure 17. Removal Operation Scheme


Process Explorer - Sysinternals: www.sysinternals.com [SWE-BEB74C0DDAB\kk]
File
Options
View
Process
Find
Handle
Help

Process	PID	CPU	Private Bytes	Working Set	Description	Company Name
System Idle Process	0	100.00	0 K	28 K		
System	4		0 K	540 K		
Interrupts	n/a	< 0.01	0 K	0 K	Hardware Interrupts and DPCs	
csrss.exe	464		1,436 K	3,888 K	Client Server Runtime Process	Microsoft Corporation
winlogon.exe	488		6,412 K	3,460 K	Windows NT Logon Applicat...	Microsoft Corporation
services.exe	532		3,156 K	4,692 K	Services and Controller app	Microsoft Corporation
svchost.exe	720		3,372 K	6,168 K	Generic Host Process for Wi...	Microsoft Corporation
igfxsrvc.exe	260		2,024 K	4,672 K	igfxsrvc Module	Intel Corporation
svchost.exe	960		2,540 K	4,816 K	Generic Host Process for Wi...	Microsoft Corporation
svchost.exe	1000		12,464 K	19,564 K	Generic Host Process for Wi...	Microsoft Corporation
svchost.exe	1088		1,812 K	3,276 K	Generic Host Process for Wi...	Microsoft Corporation
svchost.exe	1116		2,232 K	4,392 K	Generic Host Process for Wi...	Microsoft Corporation
spoolsv.exe	1272		3,696 K	4,760 K	Spooler SubSystem App	Microsoft Corporation
ERPx86Svc.exe	1404		3,148 K	4,076 K	EXE Radar Pro x86 Service	NoVirusThanks Company Srl
svchost.exe	1644		3,284 K	4,992 K	Generic Host Process for Wi...	Microsoft Corporation
alg.exe	780		1,420 K	4,540 K	Application Layer Gateway S...	Microsoft Corporation
OSPPSVC.EXE	1788		4,420 K	10,860 K	Microsoft Office Software Pr...	Microsoft Corporation
lsass.exe	544		4,316 K	1,296 K	LSA Shell (Export Version)	Microsoft Corporation
explorer.exe	1764		14,692 K	25,044 K	Windows Explorer	Microsoft Corporation
igfxtray.exe	228		1,008 K	3,392 K	igfxTray Module	Intel Corporation
hkcmd.exe	280		1,708 K	3,924 K	hkcmd Module	Intel Corporation
igfxpers.exe	332		1,576 K	3,772 K	persistence Module	Intel Corporation
ctfmon.exe	460		1,660 K	4,116 K	CTF Loader	Microsoft Corporation
ONENOTEM.EXE	548		1,452 K	916 K	Microsoft OneNote Quick La...	Microsoft Corporation

Type	Name

CPU Usage: 0.00% | Commit Charge: 3.66% | Processes: 24 | Physical Usage: 14.57%

Figure 18 Process Explorer Program Window

Users have Zeus bot in their computers must follow these steps to remove Zeus from their computers:

1- First, the user must run the "process explorer", then select winlogon.exe from left pane on process explorer and open it.

2- From winlogon.exe properties windows, the user must select threads and "Kernal32.dll" thread then press kill. So Zeus thread may be stopped by killing it as explained above. This process stops the thread that makes Zeus work. After killing this thread

3- From process explorer window, select "find" then type "Sdra64.exe", then press "search". After that, select "sdra64.exe" process, then right click "select" close handle, Zeus bot is completely stopped from working in the user computer.

4- The final step is to remove sdra64.exe from the path where it exists when it infects victim computer. So, go to the path "c:\windows\system32" and select sdra64 and press .Then delete sdra64 key from registry from the path:

"HKEY_LOCAL_MACHINE\Software\Microsoft\WindowsNT\winlogon\userinit".

Now, Zeus is completely stopped and removed from the user computer. Users must now try to secure their computers by using protection system to disallow hackers from penetrating the computer.

VIII. Conclusions

Botnet is considered one of the large criminal nowadays; this is because we cannot keep our computers and their operating systems secure enough. Also, many users of computer networks and internet do not have enough knowledge about malicious codes foundation and existence. So they need great awareness about network attacks and their dangerous activities. Others who know that there are many malicious codes do not use the proper tool to secure their operating systems.

The conclusions we have arrived at are as follows:

1. In order to begin with an idea to design a Zeus botnet detection system, a penetration process has been performed and implemented as a botmaster and as a victim. A network was configured as client-server network and penetration operation was implemented successfully where a botmaster can get anything typed in victim computer such as user name and passwords of visa card, PayPal websites, yahoo mail accounts, Google mail accounts and Facebook accounts, etc... .
2. After the penetration process, all effects that Zeus bot has done to the victim user computer are known. Examples are Zeus effect on windows operating system in windows XP and windows Seven, effects on windows registry, Zeus effect on important dynamic link libraries (.DLL), and other files which created or affected by Zeus botnet.

IX. Future works

Botnet are new methods which attackers use to infect computer networks and internet for some different gains and reasons. It may be developed rapidly with the revolution of internet and its propagation at last years. According, our suggestions for future works are: Implementing a multilayer botnet detection system depending on the cooperation process between our host botnet detection system and the suggested network botnet detection system, designing a botnet prevention system and implementing it by speed hardware devices in order to take action before bots can infect user's computer in internet. Here new technology with (FPGA) devices is useful to implement this idea.

References

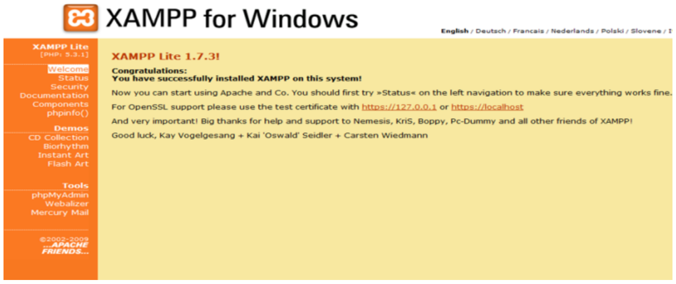
1. A. Shaikh, "Botnet Analysis And Detection System", Napier University , School Of Computing - UK Matriculation No: 06015008, 2010.
2. C. Hyunsang , L. Hanwoo , L. Heejo, K. Hyogon , "Botnet Detection by Monitoring Group Activites in DNS Traffic" , Computer and Information Technology, 2007. CIT 2007. 7th IEEE International Conference on , 2007.
3. E. Alomari, S. Manickam, "Botnet-Based Distributed Denial Of Service (DDOS) Attacks On Web Servers: Classification And Art", International Journal Of Computer Applications (0975 – 8887) Vol. 49, PP:24-32, 2012.
4. G. Gu, R. Roberto, "Botminer: Clustering Analysis Of Network Traffic For Protocol- And Structure-Independent Botnet Detection", In Proceedings Of The 17th USENIX Security Symposium (Security'08), San Jose, CA, USA, 2008.
5. G. Gu, J. Zhang, "Botsniffer: Detecting Botnet Command And Control Channels In Network Traffic", In *Proceedings Of The 15th Annual Network And Distributed System Security Symposium (NDSS 2008)*, San Diego, CA,USA, 2008.
6. H. Binsalleeh, T. Ormerod, "On The Analysis Of The Zeus Botnet Crimeware Toolkit", IEEE, Privacy Security and Trust (PST), Eighth Annual International Conference, Canada, PP: 31 – 38, 2010.
7. H.R . Zeidanloo, M.J.Z. Shooshtari, P.V. chniqueAmoli, M. Safari, " A Taxonomy of Botnet Detection Techniques", Computer Science and Information Technology (ICCSIT), 2010 3rd IEEE International Conference on (Volume:2), Pp. 158 – 162, 2010.
8. H. Zhiyong, "Detecting and Blocking P2P Botnets Through Contact tracing Chains",International Journal of Internet Protocol Technology, Vol. 5, Nos. 1/2 2010
9. J. Binkley, S. Singh, "An Algorithm For Anomaly-Based Botnet Detection" Proc. USENIX Sruti'06, PP: 43–48, 2006.
10. J. François, S. Wang, "Bottrack: Tracking Botnets Using Netflow And PageRank", In Proc. Networking (1), PP.1-14. Interdisciplinary Centre For Security, Reliability And Trust (Snt) -University Of Luxembourg - Campus Kircherg, L-1359 Luxembourg, 2011.
11. J. Grizzard, V. Sharma, " Peer- to-peer botnets: Overview and case study". In HotBots 07 conference, PP:1, Berkeley, CA, USA. USENIX Association, 2007.
12. J. Wyke, "What Is Zeus?", Threat Researcher, Sophoslabs Uk. A Sophoslabs Technical, Boston, USA | Oxford, Uk , Copyright Sophos Ltd, 2011.
13. K. Engin, "Worldwide Observatory Of Malicious Behaviors And Attack Threats", Workpackage Wp5 - Threats Intelligence, Seventh Framework Programmem, Seventh Framework Programme (FP7/2007-2013), 2013 http://www.ijsrp.org/print-journal/ijsrp-apr-2012-print.pdf.
14. K. H. Thanon, "Analysis and Detection of the Zeus Botnet Crimewre", PhD. Thesis, university of Mosul, college of computer Sciences & math. , 2013.
15. L. M. Ibrahim, K. H. Thanon, " Detection of Zeus Botnet in Computers Networks and Internet ", International Journal of Information Technology and Business Management, Vol. 6, No. 1, 2012.
16. N. Falliere, E. Chien, "Zeus: King Of The Bots", Symantec Security Response. Symantec Corporation World Headquarters, 20330 Stevens Creek Blvd. Cupertino, CA 95014, USA, 2009, www.symantec.com.
17. N. Sang-Kyun. "Detecting P2P Botnets Using a Multi-phased Flow Model", Third International Conference on Digital Society, /2009.
18. P. Salvador, A. Nogueira, "Framework For Zombie Detection Using Neural Networks", The Fourth International Conference On Internet Monitoring and Protection (ICIMP 2009), Venice, Italy. Doi:10.1109/ICIMP.2009.10 University Of Aveiro / Instituto De Telecomunicac, ˜oes - Aveiro Pole, 3810-193 Aveiro, Portugal, 2009.
19. R. Ebacher, A. Cutler, "A Multi-Layered Approach To Botnet Detection", International Conference on Security and Management (SAM'08), USA, 2008.
20. R. Eduardo . "Can Multiscale Traffic Analysis be Used to Differentiate Internet Applications?", Telecommunication Systems, Volume 48, 2010
21. R. Joshi, A. Sardana, "Honeypots A New Paradigm To Information Security", Published By Science Publishers, P.O. Box 699, Enfi Eld, NH 03748, USA. An Imprint Of Eden bridge Ltd., British Channel Islands, ISBN 978-1-57808-708-2, 2011.
22. Symantec Inc., 2005 "The Evolution of Malicious IRC bots". Symantec Security Response. In proceedings of the VB2005 Conference.
23. S. Haritha., S. Vinodh, "A Study On Botnet Detection Techniques", International Journal Of Scientific And Research Publications, Volume 2, Issue 4, 1 ISSN 2250-3153, 2012.
24. T. Arnold, "A Comparative Analysis Of Rootkit Detection Techniques", Thesis at The University Of Houston-Clear Lake, 2011.
25. T. Holz, M. Engelberth, "Learning more about the underground economy: A case-study of keyloggers and dropzones", Computer Security ESORICS 2009, PP: 1–18, 2009.
26. Trend Micro Inc., "Taxonomy of botnet threats", A Trend Micro report, http://www.trendmicro.com, 2006.
27. Trend Micro Inc., "Zeus: A Persistent Criminal Enterprise", Trend Micro, Incorporated Threat Research Team, Trend Micro Inc, 2010.
28. Trusteer Inc., "Measuring The In-The-Wild Effectiveness Of Antivirus Against Zeus", Trusteer Inc.142 Wooster St. NewYork, Ny 10012 Sales 646.247.5669 www.trusteer.com, 2009.
29. W. HaiLong, H. Jie, " Botnet Detection Architecture Based on Heterogeneous Multi-sensor Information Fusion", Journal Of Networks, Vol. 6, No. 12, 2011. http://www.wombat-project.eu/WP5/FP7-ICT-216026-Wombat_WP5_D12_V01_RCATechnical-survey.pdf
30. X. Zang, A. Tangpong, "Botnet Detection through Fine Flow Classification", CSE Dept Technical Report on Report No. CSE11-001.
31. X. Lei, X. XiaoLong and Yue Z. "P2P Botnet Detection Using Min-Vertex Cover", Journal of Networks, VOL. 7, NO. 8, 2012.

32. Y. Al-Hammadi, “Behavioural Correlation for Malicious Bot Detection”, thesis at University of Nottingham for the degree of Doctor of Philosophy, 2010.

33. http://en.wikipedia.org/wiki/Zeus_(trojan_horse),2011

AUTHORS PROFILE

First Author :**Dr. laheeb M. Alzubaidy**, have BSc. In 1987, MSc. In 1992 And PhD in 2002, in computer Sc. From Dept. of computer Sc, university of Mosul, Iraq. Associative professor in 2003, Head of Dept of Computer Sc. In 2003, visiting lecturer in Isra private university in 2004, head of Dept of Software Engineerinh in 2007, Visiting lecturer in USM university , NAV6 center/ Malaysia in 2009, Now: Associative prof. in Software Eng. Dept. /college of computer sciences & Math./ university of Mosul –Iraq, interested research fields are in Artificial Intelligent technique, network security, image processing**,** pattern recognition, software eng



XAMPP for Windows

XAMPP Lite 1.7.3!

Congratulations:
You have successfully installed XAMPP on this system!

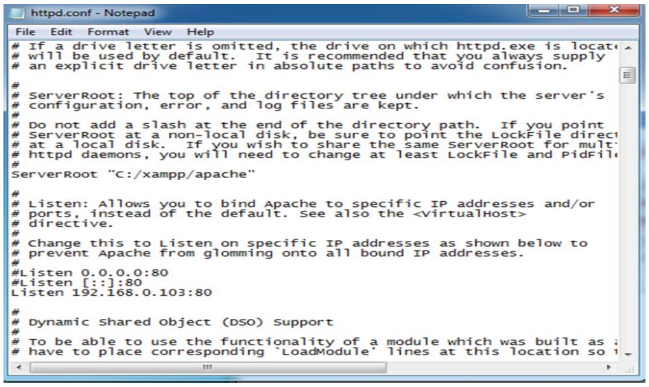
Now you can start using Apache and Co. You should first try »Status« on the left navigation to make sure everything works fine.

For OpenSSL support please use the test certificate with https://127.0.0.1 or https://localhost

And very important! Big thanks for help and support to Nemesis, KriS, Boppy, Pc-Dummy and all other friends of XAMPP!

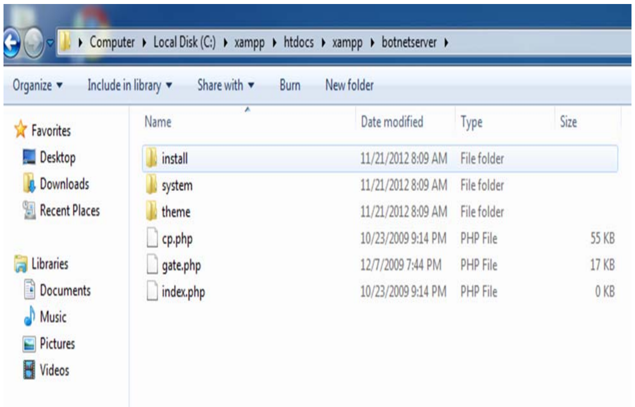
Good luck, Kay Vogelgesang + Kai 'Oswald' Seidler + Carsten Wiedmann

Figure A-1 Xampp program windows for windows



```
# If a drive letter is omitted, the drive on which httpd.exe is locat
# will be used by default.  It is recommended that you always supply
# an explicit drive letter in absolute paths to avoid confusion.

#
# ServerRoot: The top of the directory tree under which the server's
# configuration, error, and log files are kept.
#
# Do not add a slash at the end of the directory path.  If you point
# ServerRoot at a non-local disk, be sure to point the LockFile direct
# at a local disk.  If you wish to share the same ServerRoot for mult
# httpd daemons, you will need to change at least LockFile and PidFil
#
ServerRoot "C:/xampp/apache"

#
# Listen: Allows you to bind Apache to specific IP addresses and/or
# ports, instead of the default. See also the <VirtualHost>
# directive.
#
# Change this to Listen on specific IP addresses as shown below to
# prevent Apache from glomming onto all bound IP addresses.
#
#Listen 0.0.0.0:80
#Listen [::]:80
Listen 192.168.0.103:80

#
# Dynamic Shared Object (DSO) Support
#
# To be able to use the functionality of a module which was built as
# have to place corresponding `LoadModule' lines at this location so i
```

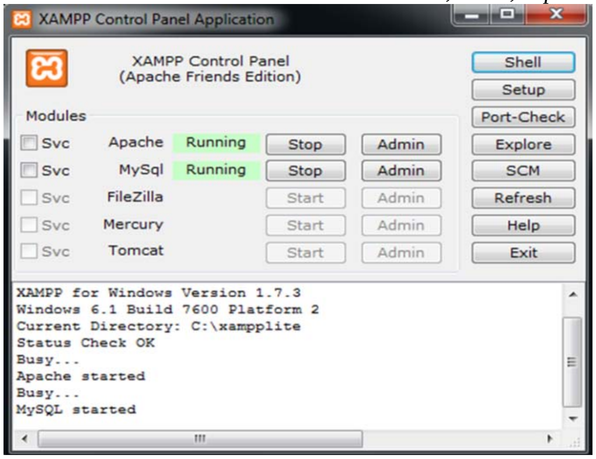
Figure A-2 Xampp configuration file



Computer ▸ Local Disk (C:) ▸ xampp ▸ htdocs ▸ xampp ▸ botnetserver ▸

Name	Date modified	Type	Size
install	11/21/2012 8:09 AM	File folder	
system	11/21/2012 8:09 AM	File folder	
theme	11/21/2012 8:09 AM	File folder	
cp.php	10/23/2009 9:14 PM	PHP File	55 KB
gate.php	12/7/2009 7:44 PM	PHP File	17 KB
index.php	10/23/2009 9:14 PM	PHP File	0 KB

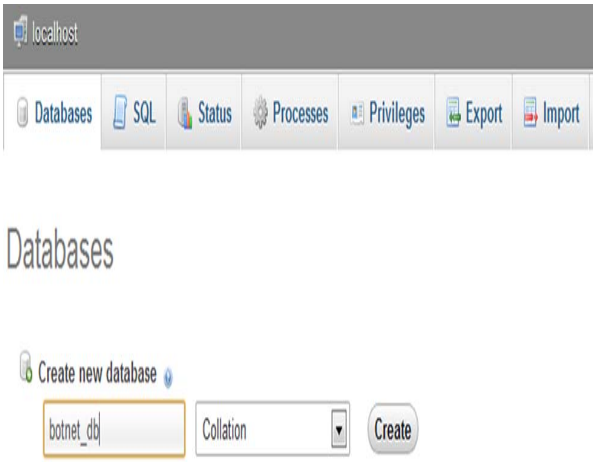
Figure A-3 Zeus Command And Control Contents



□ Svc	Apache	Running	Stop	Admin
□ Svc	MySql	Running	Stop	Admin
□ Svc	FileZilla		Start	Admin
□ Svc	Mercury		Start	Admin
□ Svc	Tomcat		Start	Admin

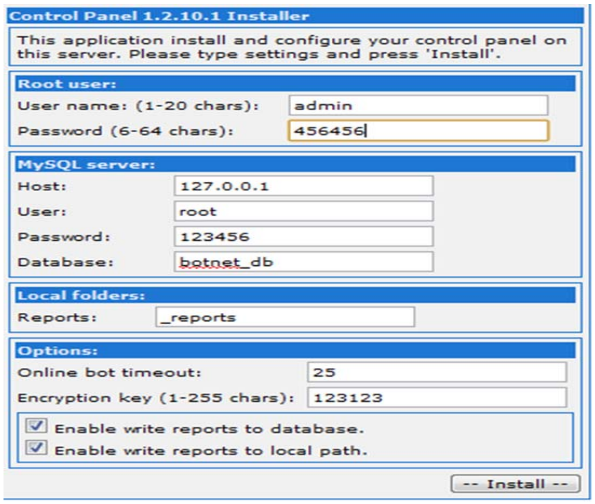
```
XAMPP for Windows Version 1.7.3
Windows 6.1 Build 7600 Platform 2
Current Directory: C:\xampplite
Status Check OK
Busy...
Apache started
Busy...
MySQL started
```

Figure A-4 Xampp Control Panel Window



Create new database: botnet_db

Figure A-5 Creation Of Zeus Database



Control Panel 1.2.10.1 Installer

This application install and configure your control panel on this server. Please type settings and press 'Install'.

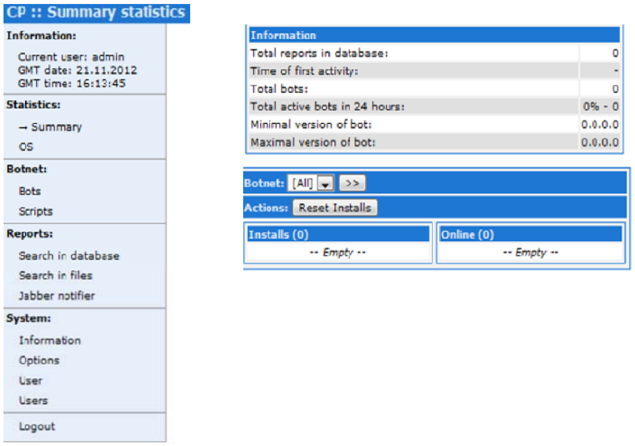
Root user:
User name: (1-20 chars): admin
Password (6-64 chars): 456456

MySQL server:
Host: 127.0.0.1
User: root
Password: 123456
Database: botnet_db

Local folders:
Reports: _reports

Options:
Online bot timeout: 25
Encryption key (1-255 chars): 123123
☑ Enable write reports to database.
☑ Enable write reports to local path.

Figure A-6 Control Panel Install Window



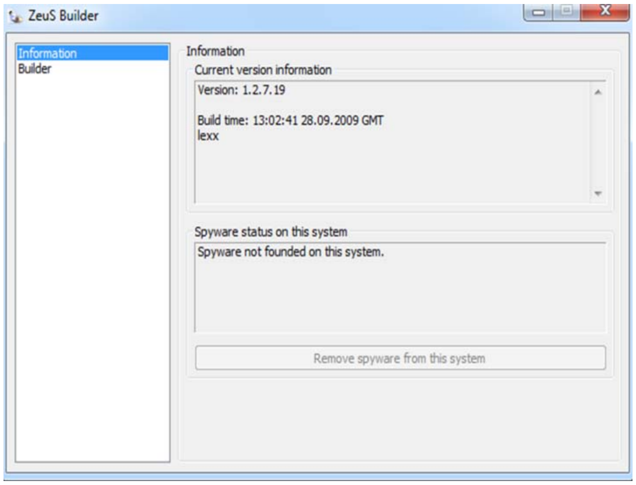
Current user: admin
GMT date: 21.11.2012
GMT time: 16:13:45

Information	
Total reports in database:	0
Time of first activity:	-
Total bots:	0
Total active bots in 24 hours:	0% - 0
Minimal version of bot:	0.0.0.0
Maximal version of bot:	0.0.0.0

Installs (0)
-- Empty --

Online (0)
-- Empty --

Figure A-7 Ready Zeus Command and Control

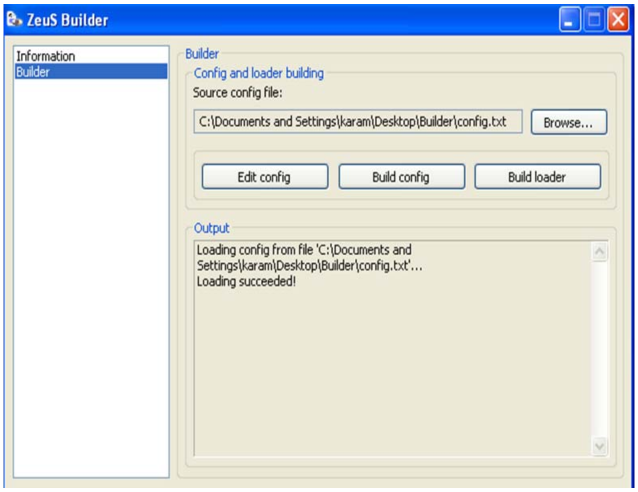

ZeuS Builder
Information
Builder
Information
Current version information
Spyware status on this system
Remove spyware from this system

Version: 1.2.7.19

Build time: 13:02:41 28.09.2009 GMT
lexx

Spyware not founded on this system.

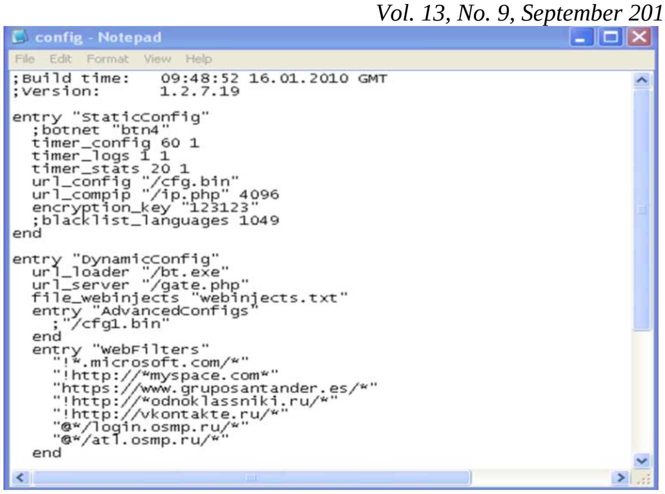
Figure A-8 Zeus Builder Window



Source config file: C:\Documents and Settings\karam\Desktop\Builder\config.txt

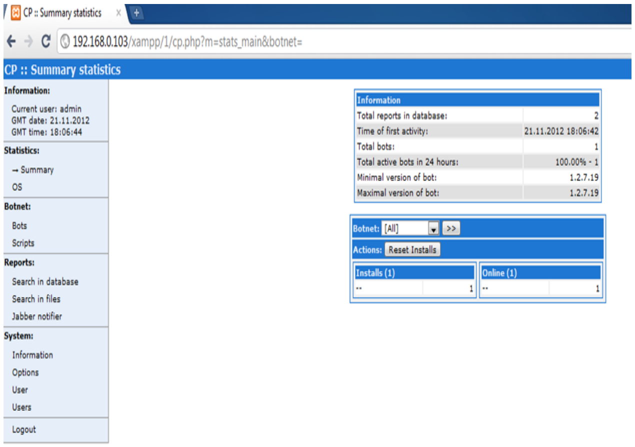
```
Loading config from file 'C:\Documents and
Settings\karam\Desktop\Builder\config.txt'...
Loading succeeded!
```

Figure A-9 Builder Window Of Zeus Bot



```
;Build time:    09:48:52 16.01.2010 GMT
;Version:       1.2.7.19

entry "StaticConfig"
  ;botnet "btn4"
  timer_config 60 1
  timer_logs 1 1
  timer_stats 20 1
  url_config "/cfg.bin"
  url_compip "/ip.php" 4096
  encryption_key "123123"
  ;blacklist_languages 1049
end

entry "DynamicConfig"
  url_loader "/bt.exe"
  url_server "/gate.php"
  file_webinjects "webinjects.txt"
  entry "AdvancedConfigs"
    ;"/cfg1.bin"
  end
  entry "WebFilters"
    "!*.microsoft.com/*"
    "!http://*myspace.com*"
    "https://www.gruposantander.es/*"
    "!http://*odnoklassniki.ru/*"
    "!http://vkontakte.ru/*"
    "@*/login.osmp.ru/*"
    "@*/atl.osmp.ru/*"
  end
```

Figure A-10 Configuration File Sample



192.168.0.103/xampp/1/cp.php?m=stats_main&botnet=

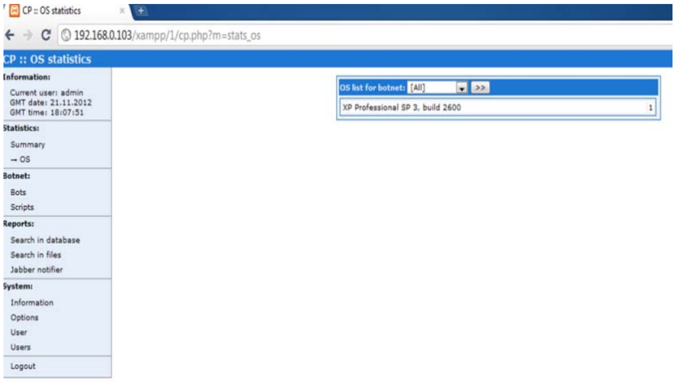
Current user: admin
GMT date: 21.11.2012
GMT time: 18:06:44

Information	
Total reports in database:	2
Time of first activity:	21.11.2012 18:06:42
Total bots:	1
Total active bots in 24 hours:	100.00% - 1
Minimal version of bot:	1.2.7.19
Maximal version of bot:	1.2.7.19

Installs (1)	
--	1

Online (1)	
--	1

Figure A-11 Zeus control panel with total bots =1



CP :: OS statistics

192.168.0.103/xampp/1/cp.php?m=stats_os

CP :: OS statistics

Information:

Current user: admin
GMT date: 21.11.2012
GMT time: 18:07:51

OS list for botnet: [All]

XP Professional SP 3, build 2600	1

Figure A-12 Victim Operating System Window

Security and Cryptography on World Wide Web

Okal Christopher Otieno
Department of Information Technology
Mount Kenya University
Nairobi, Kenya

Magati Steve Biko
Department of Information Technology
Mount Kenya University
Nairobi Kenya

ABSTRACT – Security has been a major concern for internet users regarding the potential for harm that a breach in their systems can present to the landscape. The world is evolving towards an internet dependent computing architecture considering the advancements in cloud computing and other such technologies. They promise various benefits mostly relating to the cost of operation for the businesses and personal Internet users. This investigation has the intention of determining the role that cryptography plays in ensuring the safety of the systems and the information that people share over the internet. The paper looks at the types of cryptography that are in broad use in the field of information technology and how they enable the protection that the users need. There are important protocols of protection including Internet Protocol Security Standard (IPSec) and Field Programmable Gate Arrays (FPGAs) that use cryptographic techniques. The investigation concludes that cryptography is an important contributor to Internet security through the implementation of such procedures.

INTRODUCTION

The Internet and the World Wide Web (WWW) have brought different advantages in the field of information technology that have consequently enhanced significant processes in that area. The two technologies have presented the ability of people to share information through different platforms in communication and other exercises. They are an enabler for people to exchange information and other procedures with more efficiency in terms of accuracy and speed. More developments on the internet and the web have allowed users to store data and other forms of information on the technologies using such avenues as cloud computing.

Using the internet and the web to complete certain tasks has advantages that come with it including a reduction in operational costs ([6]). They lower the requirement of particular hardware and Infrastructure for the users by providing a virtual environment that facilitates their activities in various ways. For example, cloud computing eliminates the need for storage devices by providing the virtual space for the users to store their data and launch their programs. Despite reducing the cost of purchasing the hardware, it also eliminates the expenditure on maintenance schedules [20]. More benefits associate with the use of these technologies that have enabled them to replace most traditional requirements in the computing arena.

Security of the information on the internet platforms has been a major concern in the recent past to the users and almost overshadows the benefits they present ([27]). There is a global increase in the number of people that wish to use the internet and the web to handle different tasks ranging from research to education and professional practice [13]. Other individuals with malicious intent are taking advantage of the increase in traffic and raising havoc on the users through various cyber attack techniques [1]. There has been an engagement of different researchers and developers in information technology into the objective of developing security procedures that can enable the users to protect their information from these predators. The growth of networks to share data between users increases the risks for the participants as they may have differing objectives and some of them malicious. The techniques that the developers make today need to evolve each time and advance in their implementation to adjust to the problems of the future [15]. The evolution is necessary because the threats keep changing and violating the protocols through their innovations.

Security has been a primary concern for different users of the Internet and the World Wide Web due to the dangers that the breaches in their information can present. Various businesses have termed the safety of their data as the central concern and limiter for taking advantage of the benefits that the two technologies present. They have to ensure the protection of that information because its impact can spill over and affect their clients and other persons. The users will be liable to more people due to the breaches and prefer to abstain from availing their data on the internet platforms. This research will take a look at the issue of security on the World Wide Web and the situation around the globe. The main area of concern is the protocols of transferring and storing information and data over the internet that are the primary enablers of communication and cloud computing. The research will investigate the role of cryptography on the web and network security. The procedure has different angles of approach that may be good or wrong for the safety of the users. Therefore, the study will establish the contexts of application of cryptographic techniques, and their benefits and disadvantages on the internet.

LITERATURE REVIEW

What is Cryptography?

Cryptography is an ancient technique that did not begin with the computing age. The applications in the area of information technology derive from the classical communication between two parties who used different techniques to conceal their messages [3]. It involves the use of certain codes to hide the meaning of the message from other parties besides the sender and the recipient [11]. The method was in widespread use during periods of wars when different warriors and commanders would use it to protect their information from their opponents and other opposing sympathizers. It is the cornerstone of security protocols in modern times with applications in computing. Most users apply the techniques to protect their information and data from people who use it without permission from the implementers. The technology is necessary for both open and closed networks to safeguard the processes of data transmission. A modern definition of cryptography is a technique that uses algorithms to conceal the context of a message from other parties outside the sender and receiver ([8]). Therefore, it is a form of secret communication between two parties that prevents unintentional access to particular information.

Modern cryptography uses sophisticated mathematical and programming algorithms to attain its objectives of concealing messages from the wrong audiences. There are various components that the techniques will apply. So, the algorithms are one of them, and the others include digital signatures that the users implement to notify the recipients of the messages that are pertinent to them [21]. The components of cryptographic procedure are necessary to ensure the efficiency of the communications and their security. Take the example where one party sends a secret message, another person with the ability to retrieve it can deduce the meaning and perform an action they do not intend. Therefore, they need techniques that can help them differentiate their communication to ensure the measures that follow are relevant. Some other components include hash key functions and ciphers. In summary, the elements begin with the plain text or direct message that the communication under cryptography is carrying. The plaintext goes through an encryption algorithm that turns it into a secret communication called a cipher [23]. The algorithm uses a secret key that is a set of codes that defines their hidden messages and transforms the plaintext into the cipher. The understanding of the secret keys is necessary to retrieve the messages from the cipher in a process called decryption using various techniques and algorithms. It is this action that presents a security challenge in most cases. Most people breach the ciphers by identifying weaknesses that they exploit to decrypt the message and abuse its application to the recipients, senders, or other participants.

The various procedures that people use to develop secret codes and retrieve their means have the name cryptanalysis [4]. Cryptanalysis is the study of techniques and principles that develop codes of encrypting communications and breaking them to retrieve the messages [9]. The letters that go through these coding processes are called ciphers, and they need the person to practice with the relevant cryptographic technique for retrieval of the communications they have. There are different procedures for retrieving the ciphers including decryption that are at the disposal of the particular person regarding their training and practice. Combining the aspects of cryptography and cryptanalysis presents another concept called cryptology. Therefore, the whole process of practicing cryptographic techniques and breaking the codes has an umbrella term that is cryptology.

Types of Cryptography in Internet Security

There are two main techniques of cryptography; Symmetric and Asymmetric encryption [7]. Their primary difference lies in the manner of encrypting and decrypting the messages that the developers input into the communication. The next section discusses the two types of cryptography and their applications.

(1) Symmetric Encryption

Symmetric encryption is a secure communication procedure that uses a single secret key to developing the encryption method and decrypts the message from the ciphers [14]. Therefore, the sender and their recipient will share the secret keys and use similar methods of decoding the message in their secure communication. The primary goal of using this technique between two parties is to ensure that there are high levels of privacy for the information they share because there are only two ends with access to it. The technique presents the benefit of reducing the probability of breaches by eliminating the existence of third parties that can access the communication they launch between them [2]. The two sides in the transmission will also share a key-generation algorithm that dictates both of them on how to encrypt and decrypt their information. This form of cryptography is the most conventional form that has seen broad applications in different fields including espionage in the ancient periods. The nature of the symmetric encryption procedure implies that it has three algorithms that all the users implement to ensure secure connections between them. The first is the key-generation algorithm that gives them the method of hiding and retrieving the message. It then opens up to the encryption algorithm that informs the sender on the method they will use to turn their message into a cipher. The third is the decryption algorithm that tells the receiver the procedure that will enable them to get the plain message from the cipher that they get from the sender.

One of the interesting facts is that users have to share the same secret keys of encryption and decryption if their number increases in the channel of communication [17]. They will not develop different keys when the number goes beyond one sender and receiver respectively. It implies that those on the recipient side will share the same decryption key and those on the sending one will distribute the encryption algorithm as well. The sharing makes the system more susceptible because it presents an obvious procedure to more parties. An interception on the communication is much easier since an access to one decryption key leaves all recipients vulnerable as the interceptor can now access any information. It is among the weaknesses of a symmetric communication strategy between parties. The challenge implies that if a person has access to any of the algorithms, they can transmit messages from any of the genuine participants and infect their channels. They can input misleading information to them and impact their protocols adversely.

One of the most common techniques using the symmetric approach is the Data Encryption Standard (DES) that IBM developed for the government of the United States [19]. The procedure uses a 56-bit key and a 64-bit lock in its communication strategy. The level of security for this process was susceptible to various interceptions that led to an ease of decryption. One of the system's susceptibilities is that it is open to brute force techniques of cracking. Here, a person uses all the possible combinations of letters and numbers to gain access to the system. The authorities engaged designers into developing a system that would increase the number of combinations that the system required to reduce the susceptibility. One of the newer techniques that were safer than the DES is the Advanced Encryption Standard (AES) that requires 128, 192 and 256-bit keys in its system [12]. The older DES system has more vulnerability for data that needs high security; therefore, most developers recommend against it. The strength of the secret algorithm is still susceptible due to its small combination requirements and procedures. The use of a similar key for encrypting and decrypting is the main challenge because someone who has access to either can control the activities of the system.

(2) Asymmetric Encryption

Asymmetric Encryption advances from the symmetric approach by developing different keys for encrypting and decrypting a system message [25]. This provision makes it better than the symmetric system of communication that is more susceptible to breaches. The use differing keys in the creation of the cipher and retrieving the messages, the technique reduces the probability of someone using either of them to outline the objective of any of them. For example, an unauthorized person cannot use the encryption key to retrieve the message in the communication. Therefore, the system stays secure from interceptions as a person with the ability to develop one of the two keys cannot control the system using their strategy. The requirement for implementing a communication is that one needs to obtain a secret key that helps them to generate a cipher and sends it to somebody else. The recipient also has another secret key that is pertinent to the authorizations of the communication channel that will allow them to retrieve the message and use it. Any other person cannot use their key to get the message if it is not for them as only those that the encryption algorithm authorizes can access the plain message from the cipher.

The main advantage that this strategy presents is that a sender can develop a key that is unique to them and uses it to generate messages and control who reads them [24]. The sender can define the exact recipients by limiting the access of that information to a particular recipient by selecting the specific algorithms about the key of the consignee. Therefore, the receiver of that communication also has a unique decryption key that eliminates any external access to the communications that come to them. Therefore, the messages in the channel have a one-way approach since the keys that the sender has cannot decrypt the message from the cipher that they develop [5]. They cannot tamper with the original communication in that particular piece of information unless they develop another one. Their encryption key has no control over any messages that they have developed from their systems. This move further reduces the susceptibility of the communication channel. Besides reducing the probability of interceptions, the interceptors have no control over the information that is in the message.

When using an asymmetric approach to communication, there are two types of keys that the system needs. They are the private and public keys. The sender has to visit a directory that contains the public keys that are the identifiers of the recipients they wish to contact [22]. They encrypt their messages and place them in the directory to reach the receiver through their public identifier algorithms. The recipients of the communication have private keys that are unique to them and are not allowed to disclose them to any other persons [16]. They use those secret keys to access the message that comes to them, and the algorithm retrieves the information that it contains. No other person can receive the message and get the information out of the cipher because it is unique to only one receiver. Even the sender has no ability to retrieve that information because they do not have the private algorithm that the systems accept to decrypt it. Any person that intercepts the communication must have access to the private key to enable them to retrieve the connection. Therefore, it is harder to use such techniques as brute force to guess the cipher's decryption strategy as there are no hints from the sender's side that can help. It widens the number of guesses one has to make to achieve their objective. It is like trying to get three factors of a product of numbers when they are more than two and one does not have any of them to begin with during the process. It is important to note that there is a link between the public and private keys in their algorithms that enable them to work together. That connection in their models allows them to differentiate between each other to avoid contact with the wrong persons in the communication.

The Role of Cryptography in Internet and Network Security

Cryptography is an important provision for ensuring security over networks that users intend to use for sharing information. If the data and information are in motion over the networks, then they are susceptible to interceptions from people outside the legitimate parties in the channel [10]. There are different implementations that developers and users utilize to secure their transmissions over the internet. The large traffic that is available on the internet and the vast size of information that is on the World Wide Web present various safety challenges to both creators and users. The automation of computing processes to perform particular tasks can further the problem by leaving the control open to any person in the event of an interception on the networks. Cryptography plays different significant roles in preventing unauthorized access to computing systems aiming to protect the users from the harm a breach may intend to bring. The applications of the two techniques are important to secure the information that people share over the internet using methodologies that prevent access to it until the recipient gets it. Other strategies have the objectives of lowering the susceptibility of unauthorized access to the computing systems and in turn protecting the information on them.

Password-Authenticated Key (PAK) Exchanges are one of the methodologies that developers use to protect internet users from unauthorized access to their systems and databases ([18]). Cryptography proposes different solutions to the problems that pertain to the use of such problems by making the information that they share unique to the senders and receivers. PAK procedures just protect people from accessing the whole system but do not promise any security on the information in the event that an unauthorized party gets. Cryptography presents a further protection from the superficial hindrance that passwords present to the users ([18]). The passwords are a primitive approach towards cryptography but are susceptible to attacks due to the different advancement people have made in computing. Therefore, they will require an extra step to prevent an illegal use of the information that the adversary accesses after the attack.

There are other security protocols that the World Wide Web utilizes that apply the principles and techniques of cryptography to achieve the security goal. Among the strategies are the Internet Protocol Security Standard (IPSec) and Field Programmable Gate Arrays (FPGAs) that ensure the safety of the transmissions that users make over the internet. They both use the cryptographic approach to ensure that the access to the databases on the Web is under the authority of the vendors and report any malicious activity [28]. They enable the initiation of security procedures to protect the information on the internet and inform the users about the threats to take further protective measures. They are a progressive advancement of the primitive preventive strategies by offering the extra alert features that can enable the users to protect their information once an outsider tries to breach the systems. Therefore, cryptography is significant in two levels of implementation for internet users [26]. The first area is through the protocols of transmission that enable the users to access the internet and the databases that are available on the web. The second level is ensuring the protection of the databases by controlling the access to the users by limiting certain information to particular parties alone.

CONCLUSION

Cryptography is an important art and science for ensuring the security of different protocols and infrastructure that users implement on the internet and the World Wide Web. The increasing attention towards the potential of the internet is motivating more people into its utilization. The increase in traffic presents a challenge to different vendors especially concerning the safety of the information that the users share and store on the Web. There is an increase in the security interest because the growing utility also presents the problem of growing cybercrime on the platforms with different intentions behind its motivation. The security procedures have to evolve on a regular basis to catch up with the changing face of the intruders on the systems and their innovation in malicious techniques. Cryptography presents a solution to this problem by allowing the developers to make protocols and mechanisms that can enable uniqueness in the access of information through the internet. They aim to differentiate the users by developing techniques that can enable the system administrators to detect any malicious activity and its location. The cryptographic techniques also present an important layer of protection that allows authorization procedures by preventing illegal access and use of information. With the various advancements in the computing industry, more protective strategies are a sure promise for the future. As much as it is almost impossible to prevent a cyber attack, the future looks towards a system where the users have a notification of an ongoing breach to enable them to protect their information.

REFERENCES

[1] A. Bartoli, J. Hernández-Serrano, M. Soriano, M. Dohler, A. Kountouris, & D. Barthel. “Security and Privacy in Your Smart City.” *Proceedings of the Barcelona Smart Cities Congress*. 2011.

[2] A. Boldyreva, J. Degabriele, K. Paterson & M. Stam. “On Symmetric Encryption with Distinguishable Decryption Failures.” *Fast Software Encryption*. Springer Berlin Heidelberg, 2014.

[3] B. Lang. “People's Secrets: Towards a Social History of Early Modern Cryptography”. *Sixteenth century journal: the journal of Early Modern Studies,* 2. Pp. 291-30. 2014.

[4] B. Schneier. “A self-study course in block-cipher cryptanalysis.” *Cryptologia*, 24(1). Pp. 18-33. 2000.

[5] D. Brown, R. Gallant, S. Vanstone, & M. Struik. “Trapdoor One-Way Functions on Elliptic Curves and Their Application to Shorter Signatures and Asymmetric Encryption.” U.S. Patent No. 8,782,400. 15 Jul. 2014.

[6] S. Dorogovtsev, & J. Mendes. “*Evolution of networks: From biological nets to the Internet and WWW*.” Oxford University Press, 2013.

[7] E. Fujisaki & O. Tatsuaki. “Secure Integration of Asymmetric and Symmetric Encryption Schemes.” *Crypto,* 99(32). 1999.

[8] E. Schaefer. “An introduction to cryptography and cryptanalysis.” *California's Silicon Valley: Santa Clara University*. 2009.

[9] H. Heys. “A tutorial on linear and differential cryptanalysis.” *Cryptologia,* 26(3). Pp. 189-221. 2002.

[10] H. Suo, J. Wan, C. Zou, & J. Liu. “Security in the Internet of Things: A Review.” *Computer Science and Electronics Engineering (ICCSEE), 2012 International Conference*. IEEE, 2012.

[11] J. Coron. “What is cryptography?” *Security & Privacy, IEEE,* 4(1). Pp. 70-73. 2006.

[12] J. Daemen & V. Rijmen. *The Design of Rijndael: AES-The Advanced Encryption Standard*. Springer Science & Business Media, 2013.

[13] J. Vitak, J. Crouse, & R. LaRose. "Personal Internet Use at Work: Understanding Cyberslacking." *Computers in Human Behavior*, 27(5). Pp. 1751-1759. 2011.

[14] K. Krishnan. “Computer Networks and Computer Security.” 2004.

[15] L. Wang, A. Massimiliano & S. Jajodia. *Network Hardening: An Automated Approach to Improving Network Security*. Springer, 2014.

[16] M. Agrawal, & M. Pradeep. “A Comparative Survey on Symmetric Key Encryption Techniques.” *International*

Journal on Computer Science and Engineering (IJCSE) 4(5). Pp. 877-882. 2012.

[17] M. Bellare, K. Paterson, & P. Rogaway. “Security of Symmetric Encryption against Mass Surveillance.” *Advances in Cryptology–CRYPTO 2014*. Springer Berlin Heidelberg, 2014. 1-19.

[18] M. Nguyen. “The Relationship between Password-Authenticated Key Exchange and Other Cryptographic Primitives.” *Theory of Cryptography*. Springer Berlin Heidelberg, 2005. Pp. 457-475.

[19] O. Verma, R. Agarwal, D. Dafouti, & S. Tyagi. “Performance Analysis of Data Encryption Algorithms.” *Electronics Computer Technology (ICECT), 2011 3rd International Conference on*, 5. IEEE, 2011.

[20] P. Dembla, F. Charles, & S. Petter. “Extending the DeLone and McLean IS Success Model to Cloud Computing.” 2015.

[21] R. Anderson. *Security Engineering: A Guide to Building Dependable Distributed Systems*. 2001.

[22] S. Farah, Y. Javed, A. Shamim, & T. Navaz. “An Experimental Study on Performance Evaluation of Asymmetric Encryption Algorithms.” *Recent Advances in Information Science, Proceeding of the 3rd European Conf. of Computer Science, (EECS-12)*. 2012.

[23] S. Goyat. “Cryptography Using Genetic Algorithms (GAs).” *IOSR Journal of Computer Engineering (IOSRJCE),* 1(5). 2012.

[24] S. Heyse, & T. Güneysu. “Towards One Cycle per Bit Asymmetric Encryption: Code-Based Cryptography on Reconfigurable Hardware.” *Cryptographic Hardware and Embedded Systems–CHES 2012*. Springer Berlin Heidelberg. Pp. 340-355. 2012.

[25] S. Sasi, D. Dixon, J. Wilson, & P. No. “A General Comparison of Symmetric and Asymmetric Cryptosystems for WSNs and an Overview of Location Based Encryption Technique for Improving Security.” *IOSR Journal of Engineering* 4(3). 2014.

[26] S. Strom. “Importance of Cryptography in Network Security 2D1441 Seminars in Theoretical Computer Science.” 2013.

[27] S. Subashini & V. Kavitha. “A Survey on Security Issues In Service Delivery Models of Cloud Computing.” *Journal of network and computer applications,* 34(1). Pp. 1-11. 2011.

[28] V. Prasanna & D. Andreas. “FPGA-Based Cryptography for Internet Security.” *Online Symposium for Electronic Engineers*. 2000.

LDA-PAFF: Linear Discriminate Analysis Based Personal Authentication using Finger Vein and Face Images

Manjunathswamy B E$_1$, Dr Thriveni J $_1$, Dr Venugopal K R$_1$
$_1$Department of Computer Science and Engineering, University Visvesvaraya College of Engineering,
Bangalore, India

Abstract— **Biometric based identifications are widely used for individuals personnel identification in recognition system. The unimodal recognition systems currently suffer from noisy data, spoofing attacks, biometric sensor data quality and many more. Robust personnel recognition can be achieved considering multimodal biometric traits. In this paper the LDA(Linear Discriminate analysis) based Personnel Authentication using Finger vein and Face Images (LDA-PAFF) is introduced considering the Finger Vein and Face biometric traits. The Magnitude and Phase features obtained from Gabor Kernels is considered to define the biometric traits of personnel. The biometric feature space is reduced using Fischer Score and Linear Discriminate Analysis. Personnel recognition is achieved using the weighted K-nearest neighbor classifier. The experimental study presented in the paper considers the (Group of Machine Learning and Applications, Shandong University-Homologous Multimodal Traits) SDUMLA-HMT multimodal biometric dataset. The performance of the LDA-PAFF is compared with the existing recognition systems and the performance improvement is proved through the results obtained.**

Keywords-SDUMLA_HMT; LDA-PAFF; Phase; Magnitude; fisher Score

I. Introduction

The use of biometrics to identify personnel is widely adopted in our day-to-day scenario. A biometric recognition system identifies an each personnel using one or more specific physiological characteristics possessed by the individuals [1]. If one physiological characteristics is considered for recognition then they are termed as unimodal recognition systems. When multiple or a combination of personnel biometrics are considered then they are termed as multimodal biometric recognition systems. Enrollment and verification of authorized personnel are the important functions of the recognition systems. The recognition systems enroll authorized personnel based on the data provided from the biometric sensors and store the data for future verification or matching. During verification the recognition systems validates with the existing whether the biometric data presented is valid or invalid. Predominantly unimodal systems are adopted for personnel identification [2].

Key challenges in unimodal biometic systems:

The unimodal biometric recognition systems currently used in day-to-day activities suffers from large number of drawbacks [2][3][4]. Biometric recognition systems solely rely on the data provided in the biometric sensors. The data input provided to the recognition systems from the sensors are generally noisy in nature which can affect the verification results and also cause faulty enrollment techniques. The illumination variation for face recognition systems is one such example. Interpersonal biometric similarities is another drawback of unimodal biometric systems [4]. Unimodal biometric recognition system presented in the research work using the finger print [5] it clearly illustrates the biometric similarity problem. Spoofing attacks are the common causes in unimodal recognition systems. Spoofing attacks are commonly noticed when biometrics like signature, voice, face and finger prints are considered [2] in the recognition system.

Motivation:

Multimodal biometric recognition systems is used to overcome the drawbacks of the unimodal recognition systems and have proved to be successful [6][7]. The LDA-PAFF is a multimodal recognition system. Limited work has been carried out by researchers considering a comprehensive set of biometric traits of personnel. The research work carried out by other researchers considers either the magnitude features [8][9][10][11] or the phase features[12][13][14][15].

Contribution:

Considering the research findings, a LDA based Personnel Authentication using Finger vein and Face Images (LDA-PAFF) are introduced in this paper. The state of art work presented by Shekar et al., [7] considers the Iris, Finger print and Face biometrics for recognition. In LDA-PAFF the finger vein and face biometric is considered for recognition. In LDA-PAFF, the personnel are identified on the basis of the Gabor kernel features extracted. To enable efficient feature extraction and recognition the biometric data obtained from the sensors are pre processed to obtain the region of interest(ROI) for the considered biometric traits. On obtaining the ROI, data feature extraction is performed using Gabor kernels. The novelty of LDA-PAFF is that both the phase features and magnitude feature are considered.

Organization:

The manuscript is organized as follows. Section 2 discusses the related work. The background is discussed in Section 3. The LDA-PAFF proposed is presented in Section 4. The penultimate section of the manuscript discusses the experimental work and results obtained. The conclusions are drawn in the last section.

2. Related Work

Many number of researches have been done till these days for human traits based biometric identification system where some are emphasized for multi model consideration while taking into account of performance and classification accuracy as prime objectives. Some of them are as follows:

Monwar M et al., [13] develop a multimodal biometric system using Fisher Extraction Scheme on the basis of PCA and Fisher's linear discriminant (FLD) approach which do employs face, ear and signature for identification. They employed rank-level fusion process and used Borda count paradigm (combination of ranks for individual model) and logistic regression technique. This system exhibited that the fusion of varied models could lead to performance enhancement.

Dinakardas C et al., [14] in their system developed a multimodal face recognition system using fusion of results from PCA, fisherface as well as minutia extraction with LBP feature extraction for varied biometric traction. The authors emphasized system optimization for accuracy of recognition.

Jihyeon Jang et al., [15] developed a multiple biometric system taking into consideration of non-linear classifiers and derived varied score vectors which was classified using SVM, Kernel Fisher Discriminant (KFD) and further by Bayesian Classifier. They exhibited their system functional efficiently with multi-model architecture.

Jian Yang et al., [16] emphasized their research for projection using unsupervised discriminant projection (UDP) scheme for reducing dimensionality of high-dimensional data in certain defined small sample size cases. The uniqueness of this system was that it (UDP) characterizes the local scatter factor as well as the available nonlocal scatter, requiring estimation of certain data projection which could optimize the nonlocal scatter simultaneously. They employed this system with face and palm based biometric identification. The authors advocated their system to be used for real time biometrics utilities.

3. Background Work

This is the fact that a number of researcher have made effort to enhance the system performance and among them Jiwen Lu et al., [22] have employed cost sensitive analysis paradigm for face recognition. In general the traditional subspace oriented face identification approaches need lower dimensional feature subspaces for accomplishing higher accuracy of classification[24][25][26][27]. In fact such kind of assumptions could not possess effectiveness in varied circumstances. In [22], the developed system employs a cost matrix factor which specifies varied cost factors in relation with different types of misclassification, and for this the author have taken discriminative subspace analysis approach into consideration, of which was further devised into the cost-sensitive linear discriminant analysis (CSLDA). Later a cost-sensitive marginal fisher analysis (CSMFA) approach was employed for accomplishing the value of minimum identification loss by exhibiting identification with learned low-dimensional subspaces.

In order to enhance the system by exploiting complementary details from multiple extracted features they proposed a multi-view cost sensitive subspace analysis scheme that needs a common feature subspace for fusing multiple features. In fact this work was an enhanced form of [23] which has already employed certain cost-sensitive PCA and LPP (CSLPP) approach for face identification. On the other hand generic PCA and LPP approaches are unsupervised and author enhanced it with supervised, which resulted into better results. In their work they have enriched the system with two discriminative subspace analysis approach called (LDA and marginal Fisher analysis (MFA). Some other works such as [14][15][21] have also emphasized their system for multimodal biometric application and have tried to function on reduced dimensionality with linear subspaces.

This is the matter of fact that the existing approaches have performed better, but taking into consideration of varied critical human traits and associated real time circumstances such as lighting, contrast and orientation, major systems gets limited to exhibit better. On the contrary the implementation of traditional LDA doesn't ensure optimal results. Therefore these requirements become a motivation for this present research and we have proposed a highly robust and efficient system employing phase congruency with Gabor extraction, fisher matrix enriched with LDA paradigm and the system has been further optimized with K-nearest neighbor classification system which makes the system optimal in terms of accuracy, efficiency and overall performance.

4. Proposed Model

The proposed architecture for LDA based personal authentication using finger vein and face images is LDA-PAFF as shown in Fig.1.

Let us consider a multimodal biometric dataset of $\mathcal{P}$ personnel. There exists a classification problem of $\mathcal{P}$ personnel to be identified based on their $\mathbb{B}$ biometric feature set. The biometric feature set consisting of Finger Vein and Face can be defined as

$$\mathbb{B} = \{\mathbb{V}^g \cup \mathbb{F}^g\} \qquad (1)$$

Where $\mathbb{V}^g$ is the phase features for the finger vein and $\mathbb{F}^g$ represents the feature set of the face biometric.

The LDA-PAFF proposed in this paper considers primarily Two biometric features of $\mathcal{P}$ personnel namely the finger vein $(\mathbb{V})$ and frontal face $(\mathbb{F})$. Pre-processing is adopted on all the raw biometric images to obtain the regions of interest $(\mathcal{ROI})$. The $\mathcal{ROI}$ identification procedures adopted is discussed in the future section of the paper. The $\mathcal{ROI}$ identified for finger vein and face are represented as $\mathcal{V},\mathcal{F}$ in the remaining manuscript. The use of Gabor kernels is considered for phase congruency feature extraction i.e. $\mathbb{V}^g,\mathbb{F}^g$

.

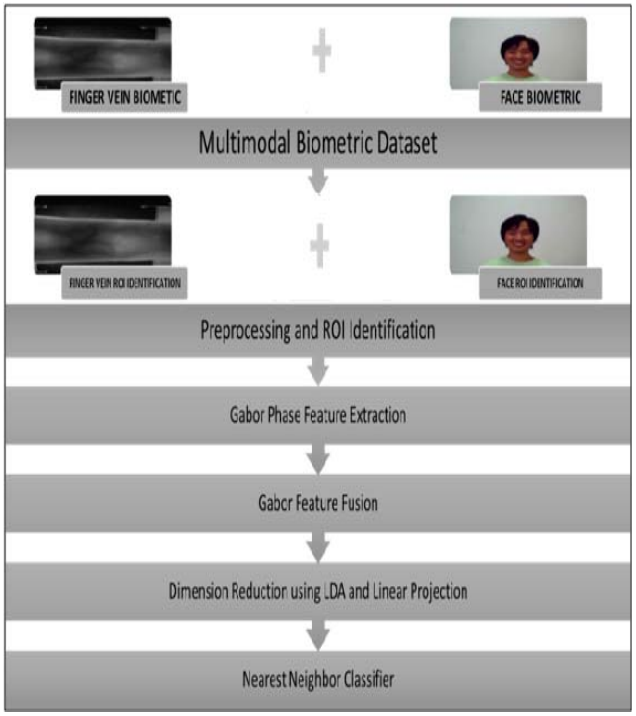

FINGER VEIN BIOMETIC
FACE BIOMETRIC
Multimodal Biometric Dataset
FINGER VEIN ROI IDENTIFICATION
FACE ROI IDENTIFICATION
Preprocessing and ROI Identification
Gabor Phase Feature Extraction
Gabor Feature Fusion
Dimension Reduction using LDA and Linear Projection
Nearest Neighbor Classifier

Fig. 1. System Architecture

4.1. Finger Vein Biometric F-ROI Identification

The finger vein biometric image set v can be represented as

$$v = \{v_1, v_2, v_3 \dots v_P\} \quad (2)$$

For precise ROI extraction of finger veins, in LDA-PAFF grey scaling, edge detection, ROI area normalization and greyscale normalization techniques are adopted. The grey scaling $_{LDA-PAFF}^{G\_Scale}PP(v_n)$ operation[16] for an image $v_n \in v$ can be defined as

$$_{LDA-PAFF}^{G\_Scale}PP(v_n) = \sum^{i=a}\sum^{j=b}([0.2989 \times R(v_n(i,j))] + A + B) \quad (3)$$

A=$[0.5870 \times G(v_n(i,j))]$, B=$[0.11400 \times B(v_n(i,j))]$

Where $R(v_n(i,j)), G(v_n(i,j))$ and $B(v_n(i,j))$ represent the red, green and blue channel values on the pixel at the location (i,j). The dimensions of the image v_x are represented as $a \times b$ .We have employed the Sobel operator for edge detection on the $_{LDA-PAFF}^{G\_Scale}PP(v_n)$ image with a masking scale of 3×3. The $_{LDA-PAFF}^{Sobel\_Mask}PP$ mask utilized is

$$_{LDA-PAFF}^{Sobel\_Mask}PP = \begin{bmatrix} -1 & 0 & 1 \\ -2 & 0 & 2 \\ -1 & 0 & 1 \end{bmatrix} \quad (4)$$

The Edge detected images vary in size. To normalize the size of the image to 128×128, bilinear interpolation is adopted [17].

4.2. Face Biometric F-ROI Identification

In LDA-PAFF, the ROI of the face is identified by localization, image segmentation, face region classification and non-face region classifications techniques. The face image dataset f of P number of personnel can be defined as

$$f = \{f_1, f_2, f_3 \dots\dots f_P\} \quad (5)$$

Consider an image $f_n \in f$ represented as a vector $b = \{b_1, b_2, \dots, b_p\}$, where b_i is the color of i^{th} pixel and p is the total number of pixels. To obtain the face ROI image the vector $A = \{a_1, a_2, \dots, a_p\}$ needs to be computed, where a_i represents the level to which the particular pixel i^{th} is assigned to. The variable a_i accepts values from the level set $X = \{x_1, x_2, \dots, x_n\}$. The level set X comprises only two possible levels, either Face or Non-face. The subsequent probability for a for the given b is represented as $L(a|b)$ and is computed using

$$L(a|b) = \frac{L(b|a) + L(a)}{L(b)} \infty L(b|a)l(a) \quad (6)$$

Using the probability $L(a|b)$ the energy facto (EF) for a face or non-face level is

$$EF(a) = (-\log L(a|b) + K) = (\emptyset(a,b) + \psi(a) + K) \quad (7)$$

Where $\emptyset(a,b) = -\log L(a|b)$, $\psi(a) = \log L(a)$ and K represents a constant.

The greyscale face ROI dataset constructed is defined as

$$F = \{F_1, F_2, F_3 \dots\dots F_P\} \quad (8)$$

4.3. Multimodal Biometric Feature Extraction Using Gabor Filters and Fusion Set Creation

The use of Gabor kernels for feature extraction have proved to be robust and efficient in personnel biometrics identification systems [18]. In LDA-PAFF the use of Gabor kernels for feature extraction from the multimodal ROI image datasets of Finger Vein and Face is adopted. The magnitude features and the phase features have been considered to define the ROI images. The Gabor kernels are complex band limited filters that enable fine grained localization in the frequency and spatial domain [19]. For a confined frequency band the Gabor kernels enable robust feature extractions in terms of spatially local features, orientation features and multi resolutional features. The Gabor features extracted efficiently negate the varied environmental conditions changes occurring due to illumination, intensity, position and orientations. The Gabor kernels relate to the simple cells of the mammalian visual cortex and are thus are relevant from the biological point of few as well [20].

Let us consider an ROI image represented as $I^{ROI}(a, b)$ where $I^{ROI} \in \mathbb{V} \parallel \mathbb{F}$. If the orientation is θ_o, center frequency is f_s then the Gabor kernel is represented by $\mathcal{K}_{s,o}(a, b)$. The feature extraction process in LDA-PAFF is achieved by performing the filtering operation on $I^{ROI}(a, b)$, utilizing the kernel function of size s and orientation o represented as $\mathcal{K}_{s,o}(a, b)$. The feature extraction function ${}_{LDA-PAFF}^{g}FE(\mathbb{D}_n) | \mathbb{D}_n \in \mathbb{V} \parallel \mathbb{F}$ can be defined as

$$ {}_{LDA-PAFF}^{g}FE(\mathbb{D}_n) = \mathcal{G}_{s,o}(a, b) = I^{ROI}(a, b) * \mathcal{K}_{s,o}(a, b) \quad (9)$$

The features obtained $\mathcal{G}_{s,o}(a, b)$ are complex in nature and consist of the real and imaginary components defined as

$$\mathcal{G}_{s,o}^{r}(a, b) = Re[\mathcal{G}_{s,o}(a, b)] = Re[I^{ROI}(a, b) * \mathcal{K}_{s,o}(a, b)] \quad (10)$$

$$\mathcal{G}_{s,o}^{i}(a, b) = Im[\mathcal{G}_{s,o}(a, b)] = Im[I^{ROI}(a, b) * \mathcal{K}_{s,o}(a, b)] \quad (11)$$

It can be observed that the feature vectors obtained for the finger vein and face biometric possess same dimensions and a simple union method is adopted in the LDA-PAFF to create the feature fusion set. The feature fusion set $\mathbb{B}$ can be defined as

$$\mathbb{B} = \sum_{n=1}^{m} (\mathbb{V}_n^{\mathbb{F}} \cup \mathbb{F}_n^{\mathbb{V}}) \quad (12)$$

4.4. Feature Sub Space Dimensional Reduction

The fusion datasets $\mathbb{B}$ consists of a large number of h data points. The large dimensions of the set $\mathbb{B}$ induce huge computational and space requirements for personnel classification in the LDA-PAFF. The data available in the set $\mathbb{B}$ is considered to encompass g points in c clusters. Each cluster represents a personnel $p \in \mathcal{P}$ and is a subspace in the space $\mathbb{B}^h$. Each data point can be represented as

$$\{(g_k, c_k)\} \forall k \in h \quad (13)$$

Where g_k is the Gabor feature and $g_k \in \mathbb{B}^h$. The class assignment variable is represented as $c_k \in \mathcal{P}$. The Gabor Feature matrix $\mathcal{G} \in \mathbb{B}^{h \times p}$ can be represented as

$$\mathcal{G} = \{g_1, g_1, g_2, \cdots g_h\} \quad (14)$$

To reduce the dimensions of the subspace projection the use of Fisher Scores and Linear Discriminate Analysis is considered in the LDA-PAFF. The Fischer scores [21] enable dimensional reduction. In addition the Fischer Scores optimize the subspace projections by increasing the inter cluster distances and reducing the intra cluster distances. The Linear Discriminate Analysis assists in feature combinations and enables accurate projections of the subspaces [22].

4.5. Classification Using K-Nearest Neighbor

Let the set $T = \{t_1, \cdots, t_p\} \subset \mathbb{B}^{p \times r}$ represent the training set. The training vector $t_z = \{(g_z, p_z)\} \forall z \in \mathcal{P}$ where g_z is the Gabor feature set representing the $p \in \mathcal{P}$ class. The training set T is considered as the dataset of the registered $\mathcal{P}$ personnel enrolled in the LDA-PAFF. Let $U = \{u_1, \cdots, u_p\} \subset \mathbb{B}^{p \times r}$ represent the unknown or testing dataset and $U \not\subset T$. Similar to the training set the testing set vector can be represented as $u_v = \{(g_v, p_v)\} \forall v \in \mathcal{Y}$ with the class variable p_v is treated as an unknown. The Gabor feature set of the training or testing sets is represented as $g_x = \{g_{1x}, g_{2x}, g_{3x}, \cdots g_{rx}\}$.

To identify the unknown class in the test data U the use of Weighted K Nearest Neighbor Classifier is adopted in the LDA-PAFF . To classify the vectors $u_v \in U$ the Weighted K Nearest Neighbor ranks the Gabor features of the test vector amongst the Gabor features of the training vectors. Using the rank and the known $\mathcal{P}$ classes of the train data the classifier predicts the unknown personnel class of the test vector using the personnel classes of the similar neighbors. The similarity amongst the test and train vectors u_p, t_p is computed using

$$\underset{LDA-PAFF}{\overset{Classify}{}}Sm(u_p, t_p, w_p) = \left(\sum_{f=1}^{r}\{w_{pf} \times t_{pf} \times u_{pf}\}\right) \times \left(\left(\sqrt{\sum_{f=1}^{r}(u_{pf})^2}\right)\left(\sqrt{\sum_{f=1}^{r}(t_{pf})^2}\right)\right)^{-1} \tag{15}$$

Where w is the weight vector, r represents the total number of Gabor Kernel features of the biometric feature under consideration.

A weighing or scoring operation is performed to identify the nearest neighbors of the test vector using the similarity matrix.

$$\underset{LDA-PAFF}{\overset{Classify}{}}Sc(u_p, \mathcal{P}_p, w_p) = \sum_{t_p \in \underset{LDA-PAFF}{\overset{Classify}{}}nn(u_p)} \underset{LDA-PAFF}{\overset{Classify}{}}Sm(u_p, t_p, w_p) \underset{LDA-PAFF}{\overset{Classify}{}}CI(t_p, \mathcal{P}_p) \tag{16}$$

Where $\underset{LDA-PAFF}{\overset{Classify}{}}nn(u_p)$ is the nearest neighbors of the unknown test vector u_p, $\underset{LDA-PAFF}{\overset{Classify}{}}CI(t_p, \mathcal{P}_p)$ is the classification index of the train vector t_p with respect to the personnel class $\mathcal{P}_p$.

5. EXPERIMENTAL STUDY

To evaluate the performance of the LDA-PAFF use of the SDUMLA-HMT multimodal biometric dataset [23] is considered. The SDUMLA-HMT data set consists of five biometric traits namely finger vein, iris, face, fingerprint and gait. The SDUMLA-HMT encompasses biometric traits of 106 personnel. A total of 45 female and 61 males aged between 17 and 31 are the personnel considered in the dataset. To evaluate the performance the use of Finger Vein and Face biometric data from the SDUMLA-HMT dataset is considered. The finger vein data provides data about the ring finger, index finger and middle finger collected over six sessions.

A total of 84 face images per personnel are provided. Personnel accessories, phase and expression variations are considered in the face data. Environmental illumination variations considered data is also provided in the face dataset.

The dataset available is split into training and testing data i.e. T, V. Equal number of train and test images are considered in the finger vein and face data. The dataset used and the construction of the test and train data is summarized in Table 1.

Table 1: SDUMLA-HMT DATA SET PARAMETERS CONSIDERD

Biometric Feature	No of Personnel	Biometric Data Per Personnel	Total Number of Images	Training Data Size	Testing Data Size
Finger Vein	106	36	3816	1908	1908
Face	106	84	8904	4452	4452

The ROI images extracted from the raw train and test data are converted to greyscale images and down sampled to 128×128. The Gabor kernel considered in the LDA-PAFF is constructed using 8 orientations i.e. $o = \{0,1,2,\ldots,6,7\}$ and 5 scales i.e. $s = \{0,1,\ldots,4\}$ resulting in 40 complex filters. The feature fused data is obtained is dimensionally reduced using the $\underset{LDA-PAFF}{}{}^{DR}F\_Feat$ function. A dimensional reduction of about 77% is achieved. The performance evaluation is carried out using Mat lab 2013b on an Intel i5 system.

The Cumulative Match Characteristic(CMC) are computed for the Proposed System and Existing System. The results obtained considering 106 p personnel or ranks is shown in Fig 2 . From Fig 2 it is observed that the Proposed System exhibits a better recognition rate. The CMC analysis is also used to compute the multimodal biometric system recognition rate. The CMC analysis results are summarized in Table 2. The cumulative system recognition rates for the Proposed system and Existing systems is shown in Fig 3.

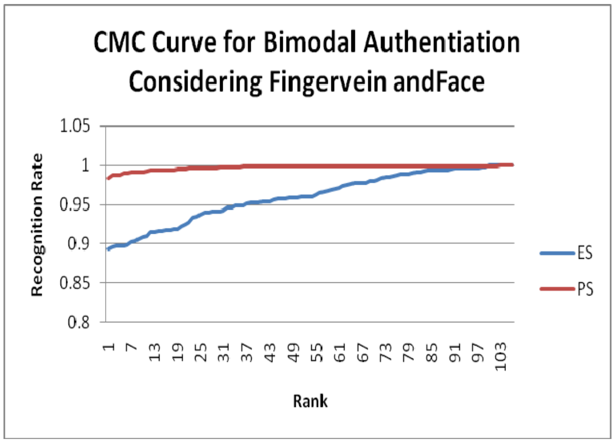


Fig. 2. Performance comparison considering CMC analysis for Bimodal biometric verification

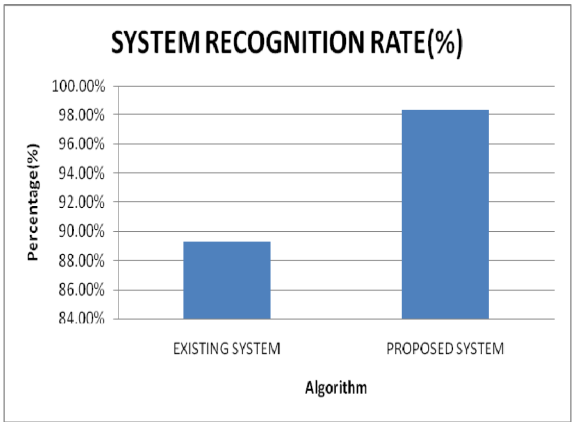


Fig.3. CMC Analysis – Cumulative System Recognition Rate Comparison

Table 2. CMC Analysis Results

ALGORITHM	NO OF PERSONNEL/RANKS	SYSTEM RECOGNITION RATE
Existing System	106	89.31%
Proposed System	106	98.43%

To evaluate the performance of the Proposed system and Existing System receiver operating characteristics (ROC) were computed. The ROC curves obtained is shown in Fig 4 of this paper. From the figure the performance improvement considering the proposed Bimodal is evident considering the vein and face dataset. The average recognition rate of Proposed system is around 92.89 and of the Existing is around 90.83 as shown in Fig 5. The ROC computation results are summarized in Table 3 of this paper.

The classification error statistics computed is graphically displayed in Fig 6. The receiver operating characteristics analysis can also be used to compute the verification rate normalized between 0-1 and the False Acceptance Rate. The false acceptance rate results are shown Fig 7. The performance improvement considering the Proposed System is clear from the results shown.

Table 3. ROC computation results of Proposed System and *Existing system*

ALGORITHM	ROC CLASSIFICATION ERROR (%)	ROC AVERAGE RECOGNITION RATE(%)	ROC FALSE ACCEPTANCE RATE (FAR %)
Existing System	5.13	90.83	5.12
Proposed System	0.74	92.89	0.74

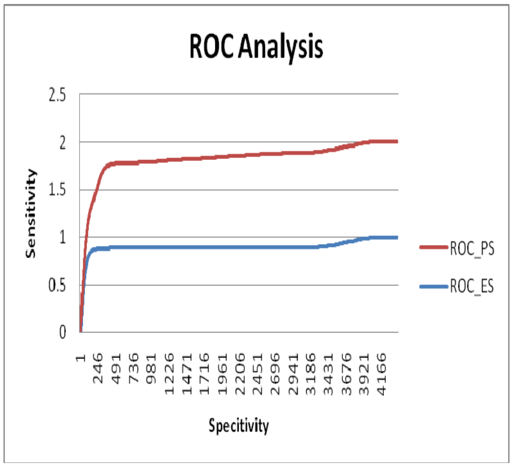


Fig .4. ROC Analysis Comparison Considering SDUMLA-HMT Dataset

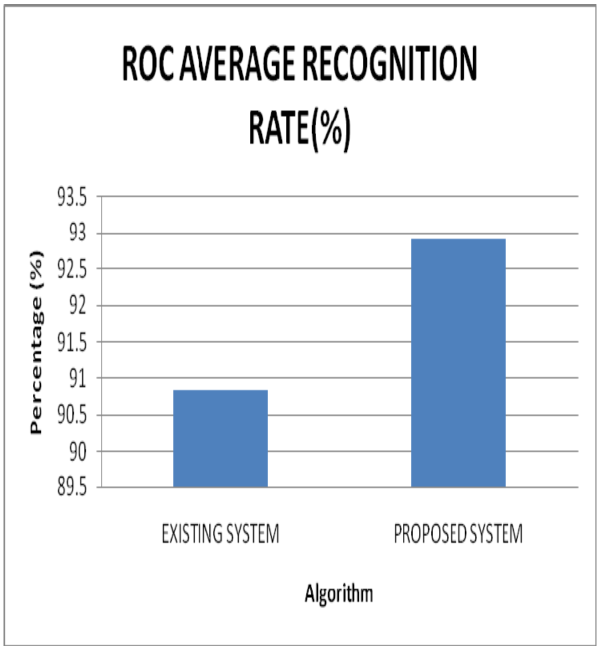


Fig.5.ROC Analysis – Average Recognition Rate Comparison

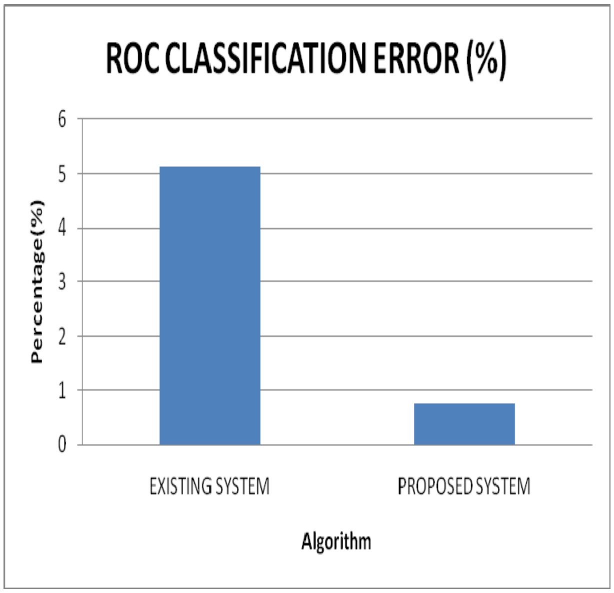


Fig.6.ROC Analysis – Classification Error Comparison

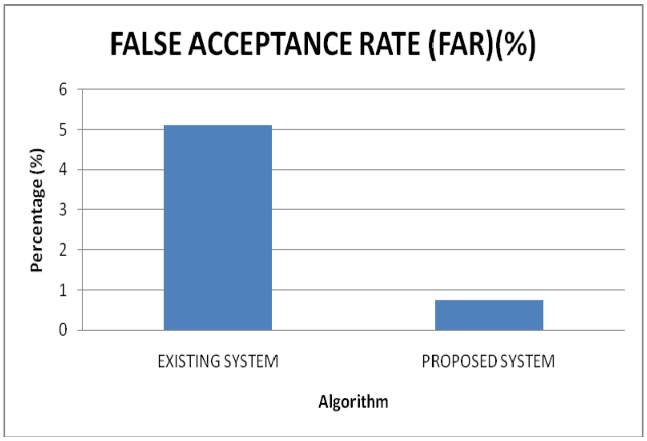


Fig.7.ROC Analysis – False Acceptance Comparison

The EPC analysis is used to compute the unbiased estimates of verification performance of the Existing System and Proposed System . The results obtained is shown in Fig. 8. The average Half total error rate considering the proposed system is 0.004% compared to the half total error rate of 0.051% observed considering the existing system. Based on the analysis carried out and the results presented it can be concluded that the proposed is robust and exhibits better user verification when compared to the existing mechanism.

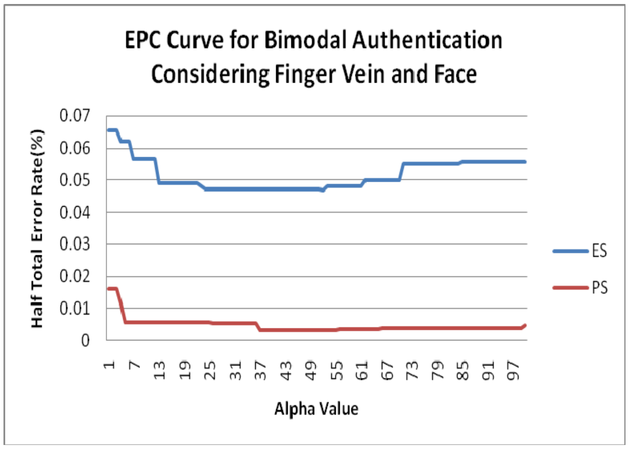


Fig. 8. Performance comparison considering EPC analysis for Bimodal Authentication

6. Conclusions

The use of biometrics for personnel identification is very common. The unimodal biometric recognition systems suffer from a number of drawbacks discussed in this paper. To over-come these drawbacks the LDA-PAFF is introduced in this paper. The LDA-PAFF considers the finger vein and face biometric traits for enrolment and recognitions of personnel into the system. The raw data obtained from the biometric sensors are preprocessed to obtain the relevant ROI'S. The use of Gabor Kernels is considered for feature extraction. The magnitude and phase features are considered. Limited work is carried out considering both these features for extraction in multimodal biometric systems. Fischer score and linear discriminate Analysis is considered for dimensional reduction. Feature dimension reduction of 77% is achieved using this methodology. For personnel verification the weighted k-nearest neighbor classifier is used. SDUMLA-HMT multimodal biometric dataset is used for performance evaluation.

The future of the work presented in this paper is consideration of additional biometric traits and additional biometric trait combinations for building robust and reliable recognition systems for personnel identification.

REFERENCES

[1]. Monwar M and Gavrilova, M.L., "Multimodal Biometric System Using Rank-Level Fusion Approach," IEEE Transactions on Systems, Man, and Cybernetics, Part B: Cybernetics, vol. 39, no. 4, pp. 867-878, Aug 2009.

[2] A. Ross and A. K. Jain, "Multimodal biometrics: an overview," Proc.European Signal Processing Conference, pp. 1221-1224, Vienna, Austria, Sept 2004.

[3] A. Ross, K. Nandakumar, and A. K. Jain, Handbook of Multibiometrics, Springer, 2006.

[4] Golfarelli, M. Maio, D. Malton, D., "On the error-reject trade-off in biometric verification systems," IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 19, no. 7, pp. 786-796, July 1997.

[5] P. Krishnasamy, S. Belongie, and D. Kriegman, "Wet fingerprint recognition:Challenges and opportunities," International Joint Conference on Biometrics, Washington DC, USA, pp. 1-7, Oct 2011.

[6] L. Hong, A. K. Jain, and S. Pankanti, "Can multibiometrics improve performance," in Proceedings AutoID'99, (Summit(NJ), USA), pp. 59-64, Oct 1999.

[7] Shekhar S. Patel V.M. Nasrabadi N.M. Chellappa R., "Joint Sparse Representation for Robust Multimodal Biometrics Recognition," IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 36, no. 1, pp. 113-126, Jan 2014.

[8] Chengjun Liu, Wechsler H, "Gabor feature based classification using the enhanced fisher linear discriminant model for face recognition," IEEE Transactions on Image Processing, vol. 11, no. 4, pp. 467-476, Apr 2002.

[9] Struc, V, Vesnicer B,Pavesic, N, "The Phase-based Gabor Fisher Classifier and its application to face recognition under varying illumination conditions," 2nd International Conference on Signal Processing and Communication Systems, ICSPCS 2008., pp. 1,6, 15-17 Dec 2008.

[10] S. Gundimada, V. K. Asari, and N. Gudur, "Face recognition in multi-sensor images based on a novel modular feature selection technique," Information Fusion, vol. 11, no. 2, pp.124-132, 2010.

[11] Laiyun Qing, Shiguang Shan,Xilin Chen, Wen Gao, "Face Recognition under Varying Lighting Based on the Probabilistic Model of Gabor Phase," 18th International Conference on Pattern Recognition, ICPR 2006, vol.3, pp.1139-1142, 2006.

[12] SÌŒ. Vitomir P. Nikola et al, "The complete gabor-fisher classifier for robust face recognition," EURASIP Journal on Advances in Signal Processing, 2010.

[13] Zhenhua Chai, Zhenan Sun, Mendez-Vazquez, H, Ran He, Tieniu Tan, "Gabor Ordinal Measures for Face Recognition," IEEE Transactions on Information Forensics and Security, vol. 9, no. 1, pp.14-26, Jan. 2014.

[14] Nicolo, F, Schmid, N.A, "Long Range Cross-Spectral Face Recognition: Matching SWIR Against Visible Light Images," IEEE Transactions on Information Forensics and Security, vol. 7, no. 6, pp.1717-1726, Dec. 2012.

[15] Faten bellakhdhar, Mossaad ben ayed, Kais loukil,Faouzi bouchhima and Mohamed abid."Multimodal biometric identification system based on face and fingerprint", Proceedings Engineering & Technology, vol. 3, pp. 219-222, 2013.

[16] Ruksar Fatima, Mohammed Zafar Ali Khan, A. Govardhan and Kashyap D Dhruve. *"Computer Aided Multi-Parameter Extraction System to Aid Early Detection of Skin Cancer Melanoma"*, International Journal of computer Science & Network Security, vol. 12 ,no. 10, pp. 74-86, Oct2012.

[17] De Oliveira, J.J., Jr.; Veloso, L.R.; de Carvalho, J.M., *"Interpolation/decimation scheme applied to size normalization of character images,"* 15th International Conference on Pattern Recognition, vol. 2, pp.577-580,2000.

[18] Weitao Li, Kezhi Mao, Hong Zhang, Tianyou Chai, *"Selection of Gabor filters for improved texture feature extraction,"* 17th IEEE International Conference on Image Processing (ICIP), pp.361-364, 26-29 Sept. 2010.

[19] Chengjun Liu, Wechsler H, *"Gabor feature based classification using the enhanced fisher linear discriminant model for face recognition,"* IEEE Transactions on Image Processing, vol.11, no.4, pp.467-476, Apr 2002.

[20] J. G . Daugman, *"Uncertainty relation for resolution in space, spatial frequency, and orientation optimized by two-dimensional visual cortical filters"*, JOSA A, 2(7):1160–1169, July 1985.{R11}

[21] Fukunaga K," *Introduction to statistical pattern recognition (2nd ed.)",*. Academic Press Professional, Inc., San Diego, CA, USA (1990).

[22] R. O. Duda P E H, Stork D G, Pattern Classification. Wiley-Interscience Publication-2001.

[23] Yilong Yin, Lili Liu and Xiwei Sun ,"SDUMLA-HMT: A Multimodal Biometric Database", LNCS 7098, pp. 260–268, 2011.

[24] Manjunathswamy B E, Thriveni J, K. R. Venugopal, L. M. Patnaik, "Efficient Iris Retrieval Using Neural Networks", IEEE NUICONE 2012, at Nirma University Ahemedabad, India, December 06-08, 2012.

[25] Manjunathswamy B E, Appaji M Abhishek, Thriveni J, K. R. Venugopal, L. M. Patnaik, "Multimodel Biometrics Using ECG and Fingerprint", International Conference on Advances in Communication Network and Computing-CNC, at Chennai, India, February 21-22, 2014.

[26] Manjunathswamy B E, Thriveni J, K. R. Venugopal, L. M. Patnaik, "MultiModel Personal Authentication Using Finger Vein and Iris Images(MPAFII)", Fifth International Conference on Advances in Computer Engineering-ACE, at Kochi, India, December 26-27, 2014.

[27] Manjunathswamy B E, Thriveni J, K. R. Venugopal, L. M. Patnaik, "MultiModel Personal Authentication Using Finger Vein and Face Images(MPAFFI)", Third International Conference on Parallel, Distributed and Grid Computing-PDGC, at Waknaghat, Solan, Himachal Pradesh, India, December 11-13, 2014.

AUTHORS PROFILE

Manjunathswamy B E

has Graduated in Telecommunication Engineering from Visvesavaraya Technological University, Belgaum, Masters degree in Information Technology from UVCE, Bangalore University, Bangaluru. He is a Research Scholar in Department of computer Science and Engineering, Bangalore University. He has 9 years of teaching experience. Currently he is working in Department of Information Science and Engineering, Alpha College of Engineering Bangalore. His area of interest includes Image Processing, Signal Processing , and Network Security.

Thriveni J

has completed Bachelor of Engineering, Masters of Engineering and Doctoral Degree in Computer Science and Engineering. She has 4 years of industrial experience and 20 years of teaching experience. Currently she is an Associate Professor in the Dept. of CSE, University Visvesvaraya

College of Engineering, Bangalore. She has over 50 research papers to her credit. she has produced one doctorate student and guiding 10 Ph.D Students. Her research interests include Networks, Data Mining and Biometrics.

Venugopal K R

is presently Special Officer, DVG Bangalore University and Principal, University Visvesvaraya College of Engineering, Bangalore University, Bangalore. He received his Bachelor of Engineering from University Visvesvaraya College of Engineering. He obtained his Masters degree in Computer Science and Automation from Indian Institute of Science Bangalore. He was awarded Ph.D. in Economics from Bangalore University and Ph.D. in Computer Science from Indian Institute of Technology, Madras. He has a distinguished academic career and has degrees in Electronics, Economics, Law, Business Finance, Public Relations, Communications, Industrial Relations, Computer Science and Journalism. He has authored and edited 54 books on Computer Science and Economics, which include Petrodollar and the World Economy, C Aptitude, Mastering C, Microprocessor Programming, Mastering C++ and Digital Circuits and Systems etc.. During his three decades of service at UVCE he has over 450 research papers to his credit. He was a Post Doctoral Research Scholar at University of Southern California, USA. His research interests consists of Computer Networks, Wireless Sensor Networks, Parallel and Distributed Systems, Digital Signal Processing and Data Mining.

The Socio-Political Influences of the Globalization of the IT Industry

Okal Christopher Otieno
Department of Information Technology
Mount Kenya University
Nairobi, Kenya

Magati Steve Biko
Department of Information Technology
Mount Kenya University
Nairobi Kenya

Abstract - This paper seeks to establish the socio-political impacts that the globalization of the information technology industry has in different societies. The review focuses on defining the two concepts of IT and Globalization and later outlines the relationship that exists between them. IT is an important contributor to the process of globalizing different communities and economies. While most people might view the relationship as unidirectional, it is untrue since globalization also impacts how the IT industry develops through various markets. The paper focuses on the two objectives of IT that are automation of processes for better efficiency and integrating people by promoting communication between them. These goals match the definition of globalization that describes their connection. Globalizing IT has different impacts on the politics and policy implementations of various locations through the flow of information that influences the people in governments. Other effects include the formation of trade blocs that are influential on the performance of the IT industry.

INTRODUCTION

Globalization refers to a process that allows the interaction and integration of different societal entities especially regarding business investments and international trade [16]. Researchers argue that this is not a new trend but rather a continuation of traditional conventions and developments [14]. The trend has brought with it a lot of enhancements in the trading environments with influences on both private and public sectors of the economies around the globe. There are frequent arguments that information technology and globalization turn on the same page, others state that they are separate concepts that just influence one another from different dimensions [24]. There has been a widespread study on the two concepts and how they impact businesses through their relationship in every market in the world.

This research will delve into the socio-political influences that the notion of globalization and the industry of information technology have on the business environment. The primary concern of the investigation is to determine how the globalization of the information technology sector impacts the societies that are in participation. The two areas are already experiencing much attention as the main influences on the economies of the world by enabling business transaction in many ways [4]. The paper will then focus on the different factors that make the globalization of the technological and communication platforms a significant contributor to the society. The information will come from previous research findings on how the two concepts relate and then determine the effects they create with a particular focus on empowering the economy.

LITERATURE REVIEW

What is Globalization?

The basic definition of globalization is that it is a process that enables the interdependence of economies and territories by integrating and increasing the integration of the people [1]. The idea of globalization has gained popularity in recent periods with different factors contributing to the acceleration of its growth. The motivation behind the concept was to expand the markets that each business had to explore by engaging more people in the activities [22]. This objective required that most of the ventures move to indulge in newer areas that would promise larger audiences for market products and also as a source of new items [26]. The territories aim to acquire equitable distribution of resources by eliminating the factors that hinder international trade, such as policies, to achieve the intentions of globalization in the market [27].

There are different factors that impact the trends of globalization, and one of them is the liberalization of trading by implementing flexible policies across the platform [7]. Most countries are developing towards a situation that allows the equal participation of both foreign and local products in their markets to increase competition. Most of them even fail to protect their industries from the competitive pressure to achieve a common ground that allows them to take part in international activities [7]. Some argue that these development gives their local producers an opportunity in the foreign areas as well which is a justification for their move to allow external traders in their markets. The second factor that enables globalization is the technological advancement that the business industry is witnessing. The developments in information technology reduce the costs of communication and transport and make the processes quicker [19]. The second aspect has had the significant influence on the whole process of integrating the people around the world and their activities in different ways. There are other areas that have received the impact of technology such as better production techniques that are a competitive advantage among the communities.

Defining Information Technology

IT refers to the use of computing and telecommunications systems to transmit, retrieve, and store data and information [2]. Information t plays a very significant role in the lives of humans especially in providing the content they require at their fingertips using electronic structures to outline its objectives [5]. There have been rapid developments in this field in the recent years with systems improving their capacities to assist human thinking in different ways. The trend looks to put information and communication technology in a spectrum that is integral to various activities that people do around the world. There are improvements in the capabilities of the devices that enhance the speed and efficiency of the different process in the world, for example, through robotics.

Information technology is an influential factor in developing intelligent systems and infrastructure that are essential to worldwide economies [17]. An example is the transport network that employs IT in different aspects to ensure efficiency and the creation of sufficient infrastructure. They allow the movement of commodities and services providers through various regions with ease [9]. They include the enhancement of vehicles, for example, that are easier to handle through implement IT devices into their operations and using other technologies to monitor the road transit processes. The progress in this area also promises to improve the way communities do business by empowering inclusive models through the networking strategies that it presents to them [28]. Therefore, IT is an important contributor to economic growth in many ways that include doing business in the field itself. The aspects of networking that result from the use of IT in businesses is among the factors that contribute to the globalization of the different territories and their socio-political attributes.

Objectives of the Information Technology Industry

The primary goal that the IT industry seeks to achieve is the automation of processes to make them quicker, more accurate and efficient [5]. The objective covers all areas of other industries including the manufacturing activities as well as communication and transport. These empowerments in businesses are significant as they impact the aspects of cost efficiency and process improvements. They can promise the better performance of different aspects of society by reducing human effort and in turn enabling people to focus on more activities [8]. There is wide criticism that most industry players in the field of IT only concentrate on the primary objective of developing and installing the systems [5]. They fail to follow up to other stages that are beyond the installation such as improving on particular aspects. They prefer to develop newer strategies instead of improving those that are currently in use.

The second most prominent objective of the development in Information Technology is the integration of people and communities [21]. The globalization of IT strategies and methods ensures that societies can connect with one another around the world through the processes of sharing information. Businesses are the biggest beneficiaries of this goal as they can use it for decision-making about different regions around the globe. For example, the can tell which areas are the best producers and which ones can save them production costs for their operations.

Components of Information Technology

There are five elements that enable the efficiency of IT in various applications. Their combinations develop the systems that define information technology and its utilization [5]. They are Hardware, Software, Procedures, Data, and People. These are the internal components of the system that enable its functionality regardless of their environment. Therefore, each of them has to be present to define a complete system that operates efficiently implying that they are interdependent in this context. Another important component that falls in this category is the network that enables a connection between independent systems between the regions. It is the core descriptor of the communication strategies that allow the people to share information through different media bases.

Hardware refers to the machinery and physical attributes of the system that are tangible and the users apply them to implement the other components [5]. Software refers to the intangible parts of a computer that are the programs and applications that initiate and complete the procedures of the machines. Data is the essential aspect that the two components above use to deliver a communication between two systems. It develops in the two aspects in the form of databases that store particular information that is relevant to an activity of interest for the communities [10]. There are different sources of data that include the systems themselves through the information they store and also the observations and collection exercises that people undertake and input their findings into them. Procedures define the general processes of operating the technology and the other components by implementing the three parts of hardware, software and data. People in this context refer to the users of the systems that enable their operation and define their utility to others who are interested in the particular procedures.

External aspects of Information Technology include those that relate to the people and their structures of governance and Association [15]. The most significant factor, in this case, is the governance methodologies and structures that different authorities implement regarding the field of IT. They are an influential contribution to its efficient use and attainment of its various objectives of the operation. They can impact the use of technology according to the preferences and perceptions of a particular community and their authorities. These factors are also important determining the opportunities that the industry has in the different locations and how users can perform its strategic alignments to the objectives.

The advancement of information technology is dependent on consistent innovation in the industry that aims to improve the systems to support various activities of a particular operation [18]. After the development of individual devices, the developers seek to make improvements on them or bring new ideas to the landscape. They have to clear every challenge they face in their industry by implementing new machines and procedures that are more efficient than the current technology. With the amount of competition growing in the industry, every producer struggles to come up with innovative solutions to gain an advantage in the markets. It is beneficial to consumers as it promises better outcomes each time.

Relationship between Globalization and the Information Technology Industry

It is important to establish the connection that exists between the information technology industry and the aspect of globalization. Most arguments place IT as an enabler of globalization in different ways [24]. There is a focus on how much IT has impacted the participation of developing countries in global economic development [23]. The IT industry’s development in such areas has allowed them to have a say on the same platforms as other nations in the implementation of international trade. The primary objective of globalization is to create an integration of people, and they share this with information technology. Therefore, it is easier to conclude that IT is an enabler of globalization. As much as this is true, the relationship does not go one way. There are many influences of globalization that impact the IT industry as well. Some of them include governance on the production and use of technology in various territories that can control the consumption of IT.

Socio-Political Influences of Globalizing the Information Technology Industry

Migration counts among the most prominent outcomes of intensive globalization as people go to explore new markets and opportunities in foreign areas [11]. The impact of globalizing the industry of IT also promises to encourage the same trend as the producers will venture into new areas to promote their businesses. There is the creation of jobs through the industry that can also motivate the migration of people from different regions to take this opportunity. The ease of movement and communication around the globe by most important is another area that information technology has enabled [12]. People can now access information about a particular place and its opportunities using such media as the Internet and organization their immigrations as well through it. The trend has led to the integration of different locations by bringing in new actors either for business or other purposes as a result of globalizing the industry of information technology. There is also a pattern that shows the willingness of every country to encourage research and development on the aspects of technology and it implies a future devolution of developers to every state. These circumstances may increase traffic flow between the territories to ensure the exploration of all ventures and opportunities. There are concerns that each local community will feel the threat from external participants on the flow of labor, capital, and information. Most of them encourage the regulation of the migrations to protect the indigenous people from these threats [20].

Globalization has led to the creation of trade blocs which reduces the significance of nation states [6]. The collective strategies to address regional issues eliminate the absolute sovereignty that most countries used to practice. It enables them to achieve a universal objective by pooling their resources and strategies that are an impact to the traditional political system that relied on the sovereign rule. Most of the economies develop legislations that touch on different aspects of their politics to ensure they comply with the agreements that they make in the unions. The impact of international trade on such economies can get the influence of the IT industry as it seeks to expand to newer regions. The businesses will try to indulge in areas that are politically stable with democracy as the primary factor of concern for them [6]. This requirement from the enterprises of the IT industry can influence the way most states practice their governance to allow them to be a participative market.

There is another influence that results from the abilities of the internet and social media to connect people around the world on their politics. They bring the possibility of people across the oceans to make commentaries about the political situations of other countries that have an influence on how governments implement their policies (Weare). It has also enabled the empowerment of nongovernmental organizations and the civil society in participating in different forums through social and mass media [6]. The participation of the country's citizens has also gained significant improvement because they now have a platform that enables others to hear their voice in governance. The globalization of the Internet to more regions means that each action has a wider audience and consequentially more influence even from foreign places. Most civil society players use the internet as an avenue to hold campaigns that are in support or against particular political activities in their states. Another political aspect that has received influence from the development in IT is the empowerment of women around the globe [25].

There is an increasing convergence between mass media and information technology resulting from the globalization of the latter industry [13]. The industry of information technology sector plays a significant role in the spread of information and producers of the media have sought to take advantage of the capabilities. There are two impacts that will result from this development, and the first is the liberalization of international trade [21]. The trend will promote the focus on improving multinational corporations as there is a focus on how each country reacts to them by the media. Among the enterprises that will benefit from this are the players in the IT industry as they now experience flexible market regimes. They also have a direct market for their products as the mass media producers will use them to outline their objectives. The second effect of the converging trend between IT and media regards multilateral cooperation between different societies through integration [21]. The availability of information through these two components of communication will encourage the association between communities as they now have clarity on the similarities and differences between their cultures. It facilitates the efficient implementation of the policies and regulations of international trade that are a significant influence on the business structures. They are also an actor that allows the confidence to explore foreign markets as there is sufficient knowledge about the environments and the nature of trading.

CONCLUSION

The paper reveals the significance of globalization and how it impacts various industries and among them information technology. The relationship between the two concepts also shows that they are interdependent with each having a way of limiting or empowering the other. IT is the factor that has increased the processes of globalizing different communities and their economies. It makes IT an important contributor in ways such as the creation of employment and enabling quick communications that facilitate business efficiency. The globalization of the IT industry has different impacts on the integration of communities as well as an influence on the structures of governance. It also affects migration patterns depending on the information that people get about particular regions and their business environments. It affects the way that civil societies and nongovernmental organizations perform their activities as well by enabling the spread of knowledge and information about a particular territory.

REFERENCES

[1] A. Deese. Globalization: causes and effects. Boston: Ashgate, 2012.

[2] B. Björk. "Information technology in construction–domain definition and research issues." 1999.

[3] C. Weare and J. W. Stanley. "The effects of internet use on political participation: evidence from an agency online discussion forum." Administration & Society (2003): 503-27.

[4] D. Wolfe. "Globalization, information and communication technologies and local and regional systems of innovation." Transition to the knowledge society: Public policies and private strategies. Vancouver: UBC Press (Institute for European Studies), 2000.

[5] E. Zalzadeh. "The use of information technology in academic departments of library and information science in Iranian universities." 2012.

[6] F. Mehlika. "Globalization and its social-cultural-political and economic impacts." Tata Institute of Social Science, 2015.

[7] G. Shangquan. "Economic globalization: trends, risks and risk prevention." Economic & Social Affairs, CDP Backround Paper 1, 2000.

[8] J. A. Garavaglia. "Full automation in live-electronics: advantages and disadvantages." 2009.

[9] J. Falcocchio and Z. Rae. "The importance of information technology (IT) for transportation security." 2015.

[10] J. Ranjan. "Business intelligence: Concepts, components, techniques and benefits." Journal of Theoretical and Applied Information Technology, 9.1, 60-70, 2009.

[11] K. Orozalieva. "Impact of globalization on socio-economic and political development of the Central Asian countries." 2010.

[12] L. J. Lau. "Economic globalization and the information technology revolution." Economic Globalization: China and Asia," a conference of the National Committee of the Chinese People's Political Consultative Conferences, Beijing, June. Vol. 15. 2000.

[13] L. K. Kelegai and R. M. Middleton. "Information technology education in Papua New Guinea: Cultural, economic and political influences." Journal of Information Technology Education, 1.1, 11-23, 2002.

[14] M. Mrak. "Globalization: trends, challenges and opportunitess for countries in transition." UNIDO, 2000.

[15] M. Ridley. "Information Technology (IT) Governance." A position paper, 2006.

[16] N. Al-Rodhan, and S. Gérard. "Definitions of globalization: a comprehensive overview and a proposed definition." Program on the Geopolitical Implications of Globalization and Transnational Security 6, 2006.

[17] N. Singh. Information technology and its role in India's economic development: A review. No. 718. Working Papers, UC Santa Cruz Economics Department, 2014.

[18] R. D. Atkinson and M. S. Andrew. "Digital prosperity: understanding the economic benefits of the information technology revolution." Available at SSRN 1004516, 2007.

[19] R. K. Lee. "Impacts of information technology on society in the new century." 2002.

[20] S. Berger. "Globalization and politics." Annual Review of Political Science 3.1, 43-62, 2000.

[21] S. O. Siochrú. "Social consequences of the globalization of the media and communication sector: some strategic considerations." 2004.

[22] S. Reich. "What is globalization." Four Possible Answers, Kellog, 1998.

[23] S. Schmitt, A. Dinesh, V. Gumadi & M. Tegtmeyer. "IT services in developing nations." 2010.

[24] S. Sunrano. "Globalization and information technology: forging new partnerships in public administration." Asian Review of Public Administration, XIII 2, 2001.

[25] Secretariat, UN ICT Task Force. "Information and communication technologies and their impact on and use as an instrument for the advancement and empowerment of women." 2002.

[26] Staff, I. M. F. "globalization: a brief overview." Int. Monetary Fund Issues Brief 2, 2008.

[27] U. Beck. "What is globalization?" Soziologie, 2000.

[28] W. Kramer, B. Jenkins, and R. Katz. "The role of the information and communications technology sector in expanding economic opportunity." Cambridge, MA: Kennedy School of Government, Harvard University, 2007.

IJCSIS REVIEWERS’ LIST

Assist. Prof. Monika Bhatnagar, TIT, India

Prof. Gaurang Panchal, Charotar University of Science & Technology, India

Prof. Anand K. Tripathi, Computer Society of India

Prof. Jyoti Chaudhary, High Performance Computing Research Lab, India

Assist. Prof. Supriya Raheja, ITM University, India

Dr. Pankaj Gupta, Microsoft Corporation, U.S.A.

Assist. Prof. Panchamukesh Chandaka, Hyderabad Institute of Tech. & Management, India

Prof. Mohan H.S, SJB Institute Of Technology, India

Mr. Hossein Malekinezhad, Islamic Azad University, Iran

Mr. Zatin Gupta, Universti Malaysia, Malaysia

Assist. Prof. Amit Chauhan, Phonics Group of Institutions, India

Assist. Prof. Ajal A. J., METS School Of Engineering, India

Mrs. Omowunmi Omobola Adeyemo, University of Ibadan, Nigeria

Dr. Bharat Bhushan Agarwal, I.F.T.M. University, India

Md. Nazrul Islam, University of Western Ontario, Canada

Tushar Kanti, L.N.C.T, Bhopal, India

Er. Aumreesh Kumar Saxena, SIRTs College Bhopal, India

Mr. Mohammad Monirul Islam, Daffodil International University, Bangladesh

Dr. Kashif Nisar, University Utara Malaysia, Malaysia

Dr. Wei Zheng, Rutgers Univ/ A10 Networks, USA

Associate Prof. Rituraj Jain, Vyas Institute of Engg & Tech, Jodhpur – Rajasthan

Assist. Prof. Apoorvi Sood, I.T.M. University, India

Dr. Kayhan Zrar Ghafoor, University Technology Malaysia, Malaysia

Mr. Swapnil Soner, Truba Institute College of Engineering & Technology, Indore, India

Ms. Yogita Gigras, I.T.M. University, India

Associate Prof. Neelima Sadineni, Pydha Engineering College, India Pydha Engineering College

Assist. Prof. K. Deepika Rani, HITAM, Hyderabad

Ms. Shikha Maheshwari, Jaipur Engineering College & Research Centre, India

Prof. Dr V S Giridhar Akula, Avanthi's Scientific Tech. & Research Academy, Hyderabad

Prof. Dr.S.Saravanan, Muthayammal Engineering College, India

Mr. Mehdi Golsorkhatabar Amiri, Islamic Azad University, Iran

Prof. Amit Sadanand Savyanavar, MITCOE, Pune, India

Assist. Prof. P.Oliver Jayaprakash, Anna University,Chennai

Assist. Prof. Ms. Sujata, ITM University, Gurgaon, India

Dr. Asoke Nath, St. Xavier's College, India

Mr. Masoud Rafighi, Islamic Azad University, Iran

Assist. Prof. RamBabu Pemula, NIMRA College of Engineering & Technology, India

Assist. Prof. Ms Rita Chhikara, ITM University, Gurgaon, India

Mr. Sandeep Maan, Government Post Graduate College, India

Prof. Dr. S. Muralidharan, Mepco Schlenk Engineering College, India

Associate Prof. T.V.Sai Krishna, QIS College of Engineering and Technology, India

Mr. R. Balu, Bharathiar University, Coimbatore, India

CALL FOR PAPERS
International Journal of Computer Science and Information Security

IJCSIS 2015
ISSN: 1947-5500
http://sites.google.com/site/ijcsis/

International Journal Computer Science and Information Security, IJCSIS, is the premier scholarly venue in the areas of computer science and security issues. IJCSIS 2011 will provide a high profile, leading edge platform for researchers and engineers alike to publish state-of-the-art research in the respective fields of information technology and communication security. The journal will feature a diverse mixture of publication articles including core and applied computer science related topics.

Authors are solicited to contribute to the special issue by submitting articles that illustrate research results, projects, surveying works and industrial experiences that describe significant advances in the following areas, but are not limited to. Submissions may span a broad range of topics, e.g.:

Track A: Security

Access control, Anonymity, Audit and audit reduction & Authentication and authorization, Applied cryptography, Cryptanalysis, Digital Signatures, Biometric security, Boundary control devices, Certification and accreditation, Cross-layer design for security, Security & Network Management, Data and system integrity, Database security, Defensive information warfare, Denial of service protection, Intrusion Detection, Anti-malware, Distributed systems security, Electronic commerce, E-mail security, Spam, Phishing, E-mail fraud, Virus, worms, Trojan Protection, Grid security, Information hiding and watermarking & Information survivability, Insider threat protection, Integrity
Intellectual property protection, Internet/Intranet Security, Key management and key recovery, Language-based security, Mobile and wireless security, Mobile, Ad Hoc and Sensor Network Security, Monitoring and surveillance, Multimedia security ,Operating system security, Peer-to-peer security, Performance Evaluations of Protocols & Security Application, Privacy and data protection, Product evaluation criteria and compliance, Risk evaluation and security certification, Risk/vulnerability assessment, Security & Network Management, Security Models & protocols, Security threats & countermeasures (DDoS, MiM, Session Hijacking, Replay attack etc,), Trusted computing, Ubiquitous Computing Security, Virtualization security, VoIP security, Web 2.0 security, Submission Procedures, Active Defense Systems, Adaptive Defense Systems, Benchmark, Analysis and Evaluation of Security Systems, Distributed Access Control and Trust Management, Distributed Attack Systems and Mechanisms, Distributed Intrusion Detection/Prevention Systems, Denial-of-Service Attacks and Countermeasures, High Performance Security Systems, Identity Management and Authentication, Implementation, Deployment and Management of Security Systems, Intelligent Defense Systems, Internet and Network Forensics, Large-scale Attacks and Defense, RFID Security and Privacy, Security Architectures in Distributed Network Systems, Security for Critical Infrastructures, Security for P2P systems and Grid Systems, Security in E-Commerce, Security and Privacy in Wireless Networks, Secure Mobile Agents and Mobile Code, Security Protocols, Security Simulation and Tools, Security Theory and Tools, Standards and Assurance Methods, Trusted Computing, Viruses, Worms, and Other Malicious Code, World Wide Web Security, Novel and emerging secure architecture, Study of attack strategies, attack modeling, Case studies and analysis of actual attacks, Continuity of Operations during an attack, Key management, Trust management, Intrusion detection techniques, Intrusion response, alarm management, and correlation analysis, Study of tradeoffs between security and system performance, Intrusion tolerance systems, Secure protocols, Security in wireless networks (e.g. mesh networks, sensor networks, etc.), Cryptography and Secure Communications, Computer Forensics, Recovery and Healing, Security Visualization, Formal Methods in Security, Principles for Designing a Secure Computing System, Autonomic Security, Internet Security, Security in Health Care Systems, Security Solutions Using Reconfigurable Computing, Adaptive and Intelligent Defense Systems, Authentication and Access control, Denial of service attacks and countermeasures, Identity, Route and

Location Anonymity schemes, Intrusion detection and prevention techniques, Cryptography, encryption algorithms and Key management schemes, Secure routing schemes, Secure neighbor discovery and localization, Trust establishment and maintenance, Confidentiality and data integrity, Security architectures, deployments and solutions, Emerging threats to cloud-based services, Security model for new services, Cloud-aware web service security, Information hiding in Cloud Computing, Securing distributed data storage in cloud, Security, privacy and trust in mobile computing systems and applications, **Middleware security & Security features:** middleware software is an asset on

its own and has to be protected, interaction between security-specific and other middleware features, e.g., context-awareness, **Middleware-level security monitoring and measurement:** metrics and mechanisms for quantification and evaluation of security enforced by the middleware, **Security co-design:** trade-off and co-design between application-based and middleware-based security, **Policy-based management:** innovative support for policy-based definition and enforcement of security concerns, **Identification and authentication mechanisms:** Means to capture application specific constraints in defining and enforcing access control rules, **Middleware-oriented security patterns:** identification of patterns for sound, reusable security, **Security in aspect-based middleware:** mechanisms for isolating and enforcing security aspects, **Security in agent-based platforms:** protection for mobile code and platforms, Smart Devices: Biometrics, National ID cards, Embedded Systems Security and TPMs, RFID Systems Security, Smart Card Security, Pervasive Systems: Digital Rights Management (DRM) in pervasive environments, Intrusion Detection and Information Filtering, Localization Systems Security (Tracking of People and Goods), Mobile Commerce Security, Privacy Enhancing Technologies, Security Protocols (for Identification and Authentication, Confidentiality and Privacy, and Integrity), Ubiquitous Networks: Ad Hoc Networks Security, Delay-Tolerant Network Security, Domestic Network Security, Peer-to-Peer Networks Security, Security Issues in Mobile and Ubiquitous Networks, Security of GSM/GPRS/UMTS Systems, Sensor Networks Security, Vehicular Network Security, Wireless Communication Security: Bluetooth, NFC, WiFi, WiMAX, WiMedia, others

This Track will emphasize the design, implementation, management and applications of computer communications, networks and services. Topics of mostly theoretical nature are also welcome, provided there is clear practical potential in applying the results of such work.

Track B: Computer Science

Broadband wireless technologies: LTE, WiMAX, WiRAN, HSDPA, HSUPA, Resource allocation and interference management, Quality of service and scheduling methods, Capacity planning and dimensioning, Cross-layer design and Physical layer based issue, Interworking architecture and interoperability, Relay assisted and cooperative communications, Location and provisioning and mobility management, Call admission and flow/congestion control, Performance optimization, Channel capacity modeling and analysis, Middleware Issues: Event-based, publish/subscribe, and message-oriented middleware, Reconfigurable, adaptable, and reflective middleware approaches, Middleware solutions for reliability, fault tolerance, and quality-of-service, Scalability of middleware, Context-aware middleware, Autonomic and self-managing middleware, Evaluation techniques for middleware solutions, Formal methods and tools for designing, verifying, and evaluating, middleware, Software engineering techniques for middleware, Service oriented middleware, Agent-based middleware, Security middleware, Network Applications: Network-based automation, Cloud applications, Ubiquitous and pervasive applications, Collaborative applications, RFID and sensor network applications, Mobile applications, Smart home applications, Infrastructure monitoring and control applications, Remote health monitoring, GPS and location-based applications, Networked vehicles applications, Alert applications, Embeded Computer System, Advanced Control Systems, and Intelligent Control : Advanced control and measurement, computer and microprocessor-based control, signal processing, estimation and identification techniques, application specific IC's, nonlinear and adaptive control, optimal and robot control, intelligent control, evolutionary computing, and intelligent systems, instrumentation subject to critical conditions, automotive, marine and aero-space control and all other control applications, Intelligent Control System, Wiring/Wireless Sensor, Signal Control System. Sensors, Actuators and Systems Integration : Intelligent sensors and actuators, multisensor fusion, sensor array and multi-channel processing, micro/nano technology, microsensors and microactuators, instrumentation electronics, MEMS and system integration, wireless sensor, Network Sensor, Hybrid

Sensor, Distributed Sensor Networks. Signal and Image Processing : Digital signal processing theory, methods, DSP implementation, speech processing, image and multidimensional signal processing, Image analysis and processing, Image and Multimedia applications, Real-time multimedia signal processing, Computer vision, Emerging signal processing areas, Remote Sensing, Signal processing in education. Industrial Informatics: Industrial applications of neural networks, fuzzy algorithms, Neuro-Fuzzy application, bioInformatics, real-time computer control, real-time information systems, human-machine interfaces, CAD/CAM/CAT/CIM, virtual reality, industrial communications, flexible manufacturing systems, industrial automated process, Data Storage Management, Harddisk control, Supply Chain Management, Logistics applications, Power plant automation, Drives automation. Information Technology, Management of Information System : Management information systems, Information Management, Nursing information management, Information System, Information Technology and their application, Data retrieval, Data Base Management, Decision analysis methods, Information processing, Operations research, E-Business, E-Commerce, E-Government, Computer Business, Security and risk management, Medical imaging, Biotechnology, Bio-Medicine, Computer-based information systems in health care, Changing Access to Patient Information, Healthcare Management Information Technology. Communication/Computer Network, Transportation Application : On-board diagnostics, Active safety systems, Communication systems, Wireless technology, Communication application, Navigation and Guidance, Vision-based applications, Speech interface, Sensor fusion, Networking theory and technologies, Transportation information, Autonomous vehicle, Vehicle application of affective computing, Advance Computing technology and their application : Broadband and intelligent networks, Data Mining, Data fusion, Computational intelligence, Information and data security, Information indexing and retrieval, Information processing, Information systems and applications, Internet applications and performances, Knowledge based systems, Knowledge management, Software Engineering, Decision making, Mobile networks and services, Network management and services, Neural Network, Fuzzy logics, Neuro-Fuzzy, Expert approaches, Innovation Technology and Management : Innovation and product development, Emerging advances in business and its applications, Creativity in Internet management and retailing, B2B and B2C management, Electronic transceiver device for Retail Marketing Industries, Facilities planning and management, Innovative pervasive computing applications, Programming paradigms for pervasive systems, Software evolution and maintenance in pervasive systems, Middleware services and agent technologies, Adaptive, autonomic and context-aware computing, Mobile/Wireless computing systems and services in pervasive computing, Energy-efficient and green pervasive computing, Communication architectures for pervasive computing, Ad hoc networks for pervasive communications, Pervasive opportunistic communications and applications, Enabling technologies for pervasive systems (e.g., wireless BAN, PAN), Positioning and tracking technologies, Sensors and RFID in pervasive systems, Multimodal sensing and context for pervasive applications, Pervasive sensing, perception and semantic interpretation, Smart devices and intelligent environments, Trust, security and privacy issues in pervasive systems, User interfaces and interaction models, Virtual immersive communications, Wearable computers, Standards and interfaces for pervasive computing environments, Social and economic models for pervasive systems, Active and Programmable Networks, Ad Hoc & Sensor Network, Congestion and/or Flow Control, Content Distribution, Grid Networking, High-speed Network Architectures, Internet Services and Applications, Optical Networks, Mobile and Wireless Networks, Network Modeling and Simulation, Multicast, Multimedia Communications, Network Control and Management, Network Protocols, Network Performance, Network Measurement, Peer to Peer and Overlay Networks, Quality of Service and Quality of Experience, Ubiquitous Networks, Crosscutting Themes – Internet Technologies, Infrastructure, Services and Applications; Open Source Tools, Open Models and Architectures; Security, Privacy and Trust; Navigation Systems, Location Based Services; Social Networks and Online Communities; ICT Convergence, Digital Economy and Digital Divide, Neural Networks, Pattern Recognition, Computer Vision, Advanced Computing Architectures and New Programming Models, Visualization and Virtual Reality as Applied to Computational Science, Computer Architecture and Embedded Systems, Technology in Education, Theoretical Computer Science, Computing Ethics, Computing Practices & Applications

Authors are invited to submit papers through e-mail ijcsiseditor@gmail.com. Submissions must be original and should not have been published previously or be under consideration for publication while being evaluated by IJCSIS. Before submission authors should carefully read over the journal's Author Guidelines, which are located at http://sites.google.com/site/ijcsis/authors-notes .

ISSN 1947 5500
http://sites.google.com/site/ijcsis/