



**IJCSIS Vol. 19 No. 6, June 2021**  
**ISSN 1947-5500**

# **International Journal of Computer Science & Information Security**

**© IJCSIS PUBLICATION 2021**  
**Pennsylvania, USA**

Indexed and technically co-sponsored by :



AUTHOR SERIES



## **Indexing Service**

IJCSIS has been indexed by several world class databases, for more information, please access the following links:

Global Impact Factor

<http://globalimpactfactor.com/>

Google Scholar

<http://scholar.google.com/>

CrossRef

<http://www.crossref.org/>

Microsoft Academic Search

<http://academic.research.microsoft.com/>

IndexCopernicus

<http://journals.indexcopernicus.com/>

IET Inspec

<http://www.theiet.org/resources/inspec/>

EBSCO

<http://www.ebscohost.com/>

JournalSeek

<http://journalseek.net>

Ulrich

<http://ulrichsweb.serialssolutions.com/>

WordCat

<http://www.worldcat.org>

Academic Journals Database

<http://www.journaldatabase.org/>

Stanford University Libraries

<http://searchworks.stanford.edu/>

Harvard Library

<http://discovery.lib.harvard.edu/?itemid=|library/m/aleph|012618581>

UniSA Library

<http://www.library.unisa.edu.au/>

ProQuest

<http://www.proquest.co.uk>

Zeitschriftendatenbank (ZDB)

<http://dispatch.opac.d-nb.de/>

# 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 2021 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 Authors are invited to submit complete unpublished papers, which are not under review in any other conference or journal in the following, but not limited to, topic areas.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, IoT  
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 Editorial Board

It is our great pleasure to present the **June 2021 issue** (Volume 19 Number 6) of the **International Journal of Computer Science and Information Security (IJCSIS)**. High quality research, survey & review articles are proposed from experts in the field, promoting insight and understanding of the state of the art, and trends in computer science and technology. It especially provides a platform for high-caliber academics, practitioners and PhD/Doctoral graduates to publish completed work and latest research outcomes. According to Google Scholar, up to now papers published in IJCSIS have been cited over **19939 times** and this journal is experiencing steady and healthy growth. Google statistics shows that IJCSIS has established the first step to be an international and prestigious journal in the field of Computer Science and Information Security. There have been many improvements to the processing of papers; we have also witnessed a significant growth in interest through a higher number of submissions as well as through the breadth and quality of those submissions. IJCSIS is indexed in major academic/scientific databases and important repositories, such as: Google Scholar, Thomson Reuters, ArXiv, CiteSeerX, Cornell's University Library, Ei Compendex, ISI Scopus, DBLP, DOAJ, ProQuest, ResearchGate, LinkedIn, Academia.edu and EBSCO among others.

A great journal cannot be made great without a dedicated editorial team of editors and reviewers. On behalf of IJCSIS community and the sponsors, we congratulate the authors and thank the reviewers for their outstanding efforts to review and recommend high quality papers for publication. In particular, we would like to thank the international academia and researchers for continued support by citing papers published in IJCSIS. Without their sustained and unselfish commitments, IJCSIS would not have achieved its current premier status, making sure we deliver high-quality content to our readers in a timely fashion.

*"We support researchers to succeed by providing high visibility & impact value, prestige and excellence in research publication."* We would like to thank you, the authors and readers, the content providers and consumers, who have made this journal the best possible.

For further questions or other suggestions please do not hesitate to contact us at [ijcsiseditor@gmail.com](mailto:ijcsiseditor@gmail.com).

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

IJCSIS Vol. 19, No. 6, June 2021 Edition

**ISSN 1947-5500 © IJCSIS, USA.**

*Journal Indexed by (among others):*



**Open Access** This Journal is distributed under the terms of the Creative Commons Attribution 4.0 International License (<http://creativecommons.org/licenses/by/4.0/>), which permits unrestricted use, distribution, and reproduction in any medium, provided you give appropriate credit to the original author(s) and the source.





**Bibliographic Information**

ISSN: 1947-5500

Monthly publication (Regular Special Issues)  
Commenced Publication since May 2009

**Editorial / Paper Submissions:**

**IJCSIS Managing Editor**

[ijcsiseditor@gmail.com](mailto:ijcsiseditor@gmail.com)

**Pennsylvania, USA**

**Tel: +1 412 390 5159**

## IJCSIS EDITORIAL BOARD

IJCSIS Editorial Board	IJCSIS Guest Editors / Associate Editors
<b>Dr. Shimon K. Modi</b> <a href="#">[Profile]</a> Director of Research BSPA Labs, Purdue University, USA	<b>Dr Riktesh Srivastava</b> <a href="#">[Profile]</a> Associate Professor, Information Systems, Skyline University College, Sharjah, PO 1797, UAE
<b>Professor Ying Yang, PhD.</b> <a href="#">[Profile]</a> Computer Science Department, Yale University, USA	<b>Dr. Jianguo Ding</b> <a href="#">[Profile]</a> Norwegian University of Science and Technology (NTNU), Norway
<b>Professor Hamid Reza Naji, PhD.</b> <a href="#">[Profile]</a> Department of Computer Enigneering, Shahid Beheshti University, Tehran, Iran	<b>Dr. Naseer Alquraishi</b> <a href="#">[Profile]</a> University of Wasit, Iraq
<b>Professor Yong Li, PhD.</b> <a href="#">[Profile]</a> School of Electronic and Information Engineering, Beijing Jiaotong University, P. R. China	<b>Dr. Kai Cong</b> <a href="#">[Profile]</a> Intel Corporation, & Computer Science Department, Portland State University, USA
<b>Professor Mokhtar Beldjehem, PhD.</b> <a href="#">[Profile]</a> Sainte-Anne University, Halifax, NS, Canada	<b>Dr. Omar A. Alzubi</b> <a href="#">[Profile]</a> Al-Balqa Applied University (BAU), Jordan
<b>Professor Yousef Farhaoui, PhD.</b> Department of Computer Science, Moulay Ismail University, Morocco	<b>Dr. Jorge A. Ruiz-Vanoye</b> <a href="#">[Profile]</a> Universidad Autónoma del Estado de Morelos, Mexico
<b>Dr. Alex Pappachen James</b> <a href="#">[Profile]</a> Queensland Micro-nanotechnology center, Griffith University, Australia	<b>Prof. Ning Xu,</b> Wuhan University of Technology, China
<b>Professor Sanjay Jasola</b> <a href="#">[Profile]</a> Gautam Buddha University	<b>Dr . Bilal Alatas</b> <a href="#">[Profile]</a> Department of Software Engineering, Firat University, Turkey
<b>Dr. Siddhivinayak Kulkarni</b> <a href="#">[Profile]</a> University of Ballarat, Ballarat, Victoria, Australia	<b>Dr. Ioannis V. Koskosas,</b> University of Western Macedonia, Greece
<b>Dr. Reza Ebrahimi Atani</b> <a href="#">[Profile]</a> University of Guilan, Iran	<b>Dr Venu Kuthadi</b> <a href="#">[Profile]</a> University of Johannesburg, Johannesburg, RSA
<b>Dr. Dong Zhang</b> <a href="#">[Profile]</a> University of Central Florida, USA	<b>Dr. Zhihan Iv</b> <a href="#">[Profile]</a> Chinese Academy of Science, China
<b>Dr. Vahid Esmaeelzadeh</b> <a href="#">[Profile]</a> Iran University of Science and Technology	<b>Prof. Ghulam Qasim</b> <a href="#">[Profile]</a> University of Engineering and Technology, Peshawar, Pakistan
<b>Dr. Jiliang Zhang</b> <a href="#">[Profile]</a> Northeastern University, China	<b>Prof. Dr. Maqbool Uddin Shaikh</b> <a href="#">[Profile]</a> Preston University, Islamabad, Pakistan
<b>Dr. Jacek M. Czerniak</b> <a href="#">[Profile]</a> Casimir the Great University in Bydgoszcz, Poland	<b>Dr. Musa Peker</b> <a href="#">[Profile]</a> Faculty of Technology, Mugla Sitki Kocman University, Turkey
<b>Dr. Binh P. Nguyen</b> <a href="#">[Profile]</a> National University of Singapore	<b>Dr. Wencan Luo</b> <a href="#">[Profile]</a> University of Pittsburgh, US
<b>Professor Seifeidne Kadry</b> <a href="#">[Profile]</a> American University of the Middle East, Kuwait	<b>Dr. Ijaz Ali Shoukat</b> <a href="#">[Profile]</a> King Saud University, Saudi Arabia
<b>Dr. Riccardo Colella</b> <a href="#">[Profile]</a> University of Salento, Italy	<b>Dr. Yilun Shang</b> <a href="#">[Profile]</a> Tongji University, Shanghai, China
<b>Dr. Sedat Akleylek</b> <a href="#">[Profile]</a> Ondokuz Mayıs University, Turkey	<b>Dr. Sachin Kumar</b> <a href="#">[Profile]</a> Indian Institute of Technology (IIT) Roorkee

<b>Dr. Basit Shahzad</b> [ <a href="#">Profile</a> ] King Saud University, Riyadh - Saudi Arabia	<b>Dr. Mohd. Muntjir</b> [ <a href="#">Profile</a> ] Taif University Kingdom of Saudi Arabia
<b>Dr. Sherzod Turaev</b> [ <a href="#">Profile</a> ] International Islamic University Malaysia	<b>Dr. Bohui Wang</b> [ <a href="#">Profile</a> ] School of Aerospace Science and Technology, Xidian University, P. R. China
<b>Dr. Kelvin LO M. F.</b> [ <a href="#">Profile</a> ] The Hong Kong Polytechnic University, Hong Kong	<b>Dr. Man Fung LO</b> [ <a href="#">Profile</a> ] The Hong Kong Polytechnic University
<b>Dr. Nitish Pathak</b> [ <a href="#">Profile</a> ] Guru Gobind Singh Indraprastha University, New Delhi, India	<b>Dr. T. V. Surya Narayan</b> [ <a href="#">Profile</a> ] Chandigarh University, Chandigarh, India
<b>Dr. S. Sophia</b> [ <a href="#">Profile</a> ] Sri Krishna College of Engineering and Technology, Coimbatore, Tamilnadu, India	



# TABLE OF CONTENTS

## **1. PaperID 01062101: Understanding Cyber Safety Behavior Among Teenagers in Ghana (pp. 1-7)**

*Mathias Agbeko, Department of ICT Education, University of Education, Winneba, Winneba, Ghana*

**Full Text:** [PDF](#) [[Academia.edu](#) | [Scopus](#) | [Scribd](#) | [Archive](#) | [DOI](#) | [Google Scholar](#)]

## **2. PaperID 01062103: Challenges Cybersecurity Architects Are Facing in a Cloud Computing Environment (pp. 8-29)**

*Anton Allen, Texas A&M University, 400 Bizzell St, College Station, USA*

*Ethan Puchaty, Lockheed Martin, 1 Lockheed Blvd, Fort Worth, USA*

*Behbood Zoghi, Texas A&M University, 400 Bizzell St, College Station, USA*

**Full Text:** [PDF](#) [[Academia.edu](#) | [Scopus](#) | [Scribd](#) | [Archive](#) | [DOI](#) | [Google Scholar](#)]

## **3. PaperID 01062105: A Proposed Security Algorithm for Securing IoT Data (pp. 30-37)**

*Rana Wafeek Mansy, Department of Information Systems, Faculty of Computers and Artificial Intelligence, Helwan University, Cairo, Egypt.*

*Mohamed Helmy Megahed, Department of Communications, Arab Academy for Science and Technology and Maritime Transport (AASTMT), College of Computing & Information Technology, Cairo, Egypt.*

*Marwa Salah, Department of Information Systems, Faculty of Informatics and Computer Science, British University in Egypt, Cairo, Egypt. Department of Information Systems, Faculty of Computers and Artificial Intelligence, Helwan University, Cairo, Egypt.*

*Mahmoud M. El-khouly, Department of Information Systems, Faculty of Computers and Artificial Intelligence, Helwan University, Cairo, Egypt.*

**Full Text:** [PDF](#) [[Academia.edu](#) | [Scopus](#) | [Scribd](#) | [Archive](#) | [DOI](#) | [Google Scholar](#)]

## **4. PaperID 01062109: A New Approach Solving for Hybrid Constraint Satisfaction Problems (pp. 38-48)**

*Van Lam Ho (1), K. Robert Lai (2), Duong Hoang Huyen (1)*

*(1) Department of Information Technology, Quy Nhon University, Vietnam*

*(2) Department of Computer Science and Engineering, Yuanze University, Taiwan*

**Full Text:** [PDF](#) [[Academia.edu](#) | [Scopus](#) | [Scribd](#) | [Archive](#) | [DOI](#) | [Google Scholar](#)]

## **5. PaperID 01062111: Designing Service Level Agreements and Information Technology Service Level Management Process Standards based on the ISO 20000 and ITIL V3 2011: Case Study of PT XYZ (pp. 49-55)**

*Erlangga Al Farozi, Yudho Giri Sucahyo & Muhammad Kasfu Hammi,*

*Master of Information Technology Study Program, Faculty of Computer Science, University of Indonesia, Indonesia*

**Full Text:** [PDF](#) [[Academia.edu](#) | [Scopus](#) | [Scribd](#) | [Archive](#) | [DOI](#) | [Google Scholar](#)]

**6. PaperID 01062115: Adoption of Fuzzy Clustering Techniques to Determine the Genetic Characteristics of Some Dates Varieties (pp. 56-60)**

*Nima Abdullah AL-Fakhry & Ramadan Mahmood Ramo,  
College of Administration & Economic, Department of Management Information Systems, University of Mosul*

**Full Text:** PDF [[Academia.edu](#) | [Scopus](#) | [Scribd](#) | [Archive](#) | [DOI](#) | [Google Scholar](#)]

**7. PaperID 01062122: Suggested Approach Using Cloud Computing and DNA Test in Finding Missing Children in All Over The World (pp. 61-71)**

*Suhad Abu Shehab, Faculty of Information Technology  
Dr. Mostafa Alrawashdeh, Faculty of Law*

**Full Text:** PDF [[Academia.edu](#) | [Scopus](#) | [Scribd](#) | [Archive](#) | [DOI](#) | [Google Scholar](#)]

**8. PaperID 01062123: Standardized Security Design and Information System in Nigeria Educational Institution (pp. 72-88)**

*Eleberi Ebele Leticia, Department of Computer Science*

**Full Text:** PDF [[Academia.edu](#) | [Scopus](#) | [Scribd](#) | [Archive](#) | [DOI](#) | [Google Scholar](#)]

**9. PaperID 01062124: ICT Parks and Digital Literacy in Nigeria (pp. 89-108)**

*Eleberi Ebele Leticia, Department of Computer Science*

**Full Text:** PDF [[Academia.edu](#) | [Scopus](#) | [Scribd](#) | [Archive](#) | [DOI](#) | [Google Scholar](#)]

**10. PaperID 01062125: E-Security and Management Performance Among Small and Medium Scale Enterprises (SMEs) in Nigeria (pp. 109-129)**

*Eleberi Ebele Leticia, Department of Computer Science*

**Full Text:** PDF [[Academia.edu](#) | [Scopus](#) | [Scribd](#) | [Archive](#) | [DOI](#) | [Google Scholar](#)]

**11. PaperID 01062126: Energy Efficient Clustering Technique to Reduce Load in Cloud Computing (pp. 130-133)**

*Dr. Sumit Chaudhary, Associate Professor, Indrashil University, Rajpur, Kadi, India  
Neha Singh, Assistant Professor, Indrashil University, Rajpur, Kadi, India  
Ms. Jyoti Srivastava, Assistant Professor, Indrashil University, Rajpur, Kadi, India  
Mr. Bhavesh Jain, Assistant Professor, Indrashil University, Rajpur, Kadi, India*

**Full Text:** PDF [[Academia.edu](#) | [Scopus](#) | [Scribd](#) | [Archive](#) | [DOI](#) | [Google Scholar](#)]

# UNDERSTANDING CYBER SAFETY BEHAVIOR AMONG TEENAGERS IN GHANA

Mathias Agbeko

Department of ICT Education  
University of Education, Winneba  
Winneba, Ghana  
magbeko@uew.edu.gh

*Abstract – The development of mobile technology and the expansion of internet access has raised concerns about the cyber safety of teenagers in cyber space. The purpose of this study is to investigate the cyber safety practices, cyber security awareness and teenagers’ experiences with cyber-attacks in Ghana. This study adopted a descriptive survey research approach and targeted some public senior high schools in of Ghana. Questionnaire was the main instrument for data collection and it was used to collect data from 153 senior high school students who were conveniently sampled from eight (8) senior high schools in the Ashanti region of Ghana. The results showed that 74.5 percent of teenagers were aware of cybersecurity, 8.7 percent had been involved in cybercrime and their main motivation was either to make money and/or for fun. On the preventive measures against cyber-attacks, 42 percent said they changed their passwords whilst only 1.8 percent said they reported to the police. The cyber-attacks that teenagers often experience are malware attacks and phishing attacks. The study has revealed that these attacks are common among teenagers because they often open unknown email attachments and they fail to regularly update their antiviruses. It is therefore recommended that teenagers be more preventive than corrective in their approach toward cyber-attack. They need to periodically change their passwords and update their antiviruses. The security services should also be more proactive and apprehend perpetrators of cyber-attacks so that victims can have the confidence to report cyber cases to them. It is only in this way that the issue of online crime can be addressed effectively in Ghana.*

*Keywords – Cyber Safety; Internet; Security; Awareness; Cyber-Attack*

## I. INTRODUCTION

The expansion of internet access in Ghana is very laudable; considering the huge benefit it brings to individuals, institutions, businesses and the country. As of the third quarter of 2019, Ghana counted about 16.7 million unique mobile subscribers, 15.1 million smartphone devices and 10.7 million mobile internet users in the country [16]. In 2016, Ghana opened a multi-

million dollar 600-rack National Data Centre in Accra, the largest of its kind in West Africa [1]. This goes to confirm the huge investment the government is making to ensure that internet access is available to all of its citizens. In the educational sector, currently, thirteen public tertiary institutions in Ghana are benefiting from a free WiFi pilot project, with the aim that this initiative will soon be rolled out in the over seven hundred and twenty-two public senior high schools in Ghana. These initiatives, though positive, will come at a great cost if research in the cyber safety behavior of our teenagers in the senior high schools is understudied or non-existent.

Cyber safety is defined as the safe and responsible use of information and communication technologies [2] and [3], including protection against unsolicited marketing and advertising [7]. Cyber safety has been a major concern not only in Sub-Saharan Africa but also worldwide. Due to this, the Budapest convention on cybercrime was convinced that as a matter of priority, they need to pursue a common criminal policy aimed at the protection of society against cybercrime, inter alia, by adopting appropriate legislation and fostering international co-operation [5]. Although this convention remains the most significant instrument in this area, especially in protecting young ones against various forms of cybercrime, many nations are yet to take the initiative to adopt it.

As portrayed in a straightforward term, cybercrime is any unlawful action which is perpetrated utilizing any processing gadgets, similar to PC/cell phone [18]. There are various techniques by which digital wrongdoing is carried out, and which incorporates attacks on PC frameworks, cyber-harassing, email spam, phishing, and identity robbery. Cybercrime is the deadliest sort of wrongdoing. It can upset existing set-up within a second [24]. Additionally, cybercrime is characterized as offense that is carried out against individual or group of people with a criminal rationale to purposefully hurt the reputation of the person in question or cause physical or

mental mischief to the casualty directly or by implication, utilizing current media transmission organizations like web and cell phones [9]. Worldwide, teenagers are most susceptible to cyber-attack due to their avid use of the internet and their perceived lack of awareness of cyber security risks. A study conducted by [18] to explore teenager's familiarity with digital protection discovered that about half of the students were aware of digital wrongdoing. A comparable study by [20] discovered that students were tolerably mindful of digital violations and knew about the law against digital wrongdoing. On the other hand, an investigation led by [19] showed that a large number of secondary school students shared their private information online and did not know about the likely misuse of such information by cyber criminals.

The reason for increase in cybercrime owes to the fact that perpetrators gain easy access to mobile devices, the internet and network facilities [21]. Adopting a descriptive research design to survey 44,500 university undergraduate students in Nigeria, [17] found that students engage in online drug trafficking, cyber stalking, email hack, hacking of organizational accounts, identity theft, among others. The students in their various responses showed that they had been involved in one form of cybercrime or the other in their various institutions. [15] further explained that most of these students were deeply involved in cybercrime alongside their counterparts in the school. [6] disagreed vehemently with the finding of this study when he found out that undergraduates are fully occupied with academic and vocational activities that can make them associate with cyber theft.

On the issue of teenagers' experience with cyber - attack, a study by [11] conducted on a sample of more than 200 Slovenian Internet users revealed that 83% of respondents had experienced a computer virus infection. He also reported that just under one third of respondents' friends experienced computer hacking and online identity theft and that they reported knowing at least one person who was harmed by cybercrime. Thus, the forms of harassments the perpetrators of cyber bullying exhibit comes in different faces. The nature of harassment ranges from ignoring, disrespecting, threatening, calling names, spreading rumors, email bombing, picking on and ridiculing [22] to hiding names while sending SMS or when in a chat room, kicking someone out of a chat room, and violating the privacy of someone by a webcam [23].

On the preventive measure teenagers take to curb cyber-attacks, [13] mentioned the importance of cyber security training programs that can change the attitude and behavior of internet users, by decreasing the number

of risk affiliated with cyber security incidents. They also pointed out the need for appropriate security practices that will change the behavior of online users in their day-to-day practice. [11] reported that approximately one half of respondents have sufficient information to protect their devices misuse or personal data/theft. However, it turned out that 40% of them did not know or did not install any software protection on their Internet-connected devices (computer, phone, etc.). [25] also showed that internet users possess adequate cyber threat awareness but apply only minimal protective measures usually relatively common and simple ones.

[10] reported that respondents' behaviors towards curbing cyberattacks was ambivalent. On one hand, they argued that they know how to behave in the case of a cyberattack ( $M=3.10$ ,  $SD=1.19$ ). For example, they indicated that they would not provide information on the web ( $M=2.42$ ,  $SD=0.93$ ). In addition, they argued that their length of a standard password is 10 on the average, which was considered to them as safe. On the other hand, when asked to describe how they acted in order to protect their computer, they only indicated 4 measures on average out of 11 options. This indicated their uncertain posture towards cyber safety. Hence, [4] asserted that the primary tool for such prevention is undoubtedly education aimed at establishing greater awareness and knowledge regarding illegal internet content and cybercrime among children and teenagers, as well as parents and educators. Thus, Cyber violence is a relatively new phenomenon, with most of the reports emerging through publicity in the mass media. In the same vein, there should be a mandatory prevention-education on cybercrime and cyber safety for all incoming students [12].

A number of studies have been conducted to assess the causes and effects of cyber threats [8]. This is an indication of the increasing prominence of cyber-attacks among organizations and citizens all over the world. Despite the growing interest and impact of cyber-attacks on teenagers, there still remains a general lack of education on cyber security among the consuming Ghanaian public [14]. It is for this reason that the researcher decided to carry out this research to understand the cyber behavior of teenagers on the internet. Hence, these questions are formulated to form the basis of this study:

1. What is the level of awareness of cyber security among teenagers?
2. To what extent are teenagers involved in cybercrime?
3. How often do teenagers experience cyberattacks?

4. What preventive measures have teenagers put in place to prevent cyberattacks?

*A. Research Objectives*

The study seeks to achieve the following objectives:

1. To understand the cyber security awareness among teenagers.
2. To explore the extent to which teenagers are involved in cybercrime.
3. To find out how often teenagers experience cyberattacks.
4. To identify the preventive measures teenagers have put in place to prevent cyberattacks.

*B. Purpose of the study*

The study seeks to investigate the cyber safety practices, teenagers’ experiences with cyber-attacks, their cyber security awareness and preventive measures taken by teenagers in Ghana to curb cyber-attacks.

II. METHODOLOGY

This study adopted a descriptive survey design incorporating quantitative research approach with a researcher-made questionnaire as the instrument. The population of the study was all form two (2) students in eight senior high schools in Ashanti Region. The sampling technique used was convenience sampling since the researcher was supervising students on teaching practice in that region. In all, 153 students were selected from the eight schools. Questionnaire was administered by the researcher himself and was completed on the spot by all respondents. Thus, the return rate was 100%. Statistical Product and Service Solutions (SPSS) was used for the analysis.

III. RESULTS AND DISCUSSION

*A. Cybersecurity Awareness among Teenagers*

Fig. 1 represents students’ responses on the question on their awareness of cyber security. Out of the 153 respondents, 152 responded whereas only 1 respondent did not respond to the question. 114 students representing 74.5% said they are aware of cybersecurity, 27 students representing 17.6% said they are not aware of cybersecurity whereas 11 representing 7.2% responded that they are not sure. From the above, we can confidently conclude that most teenagers are very much aware of cybersecurity. This finding confirms the study made by [18] that about half of the students knew about digital wrongdoings.

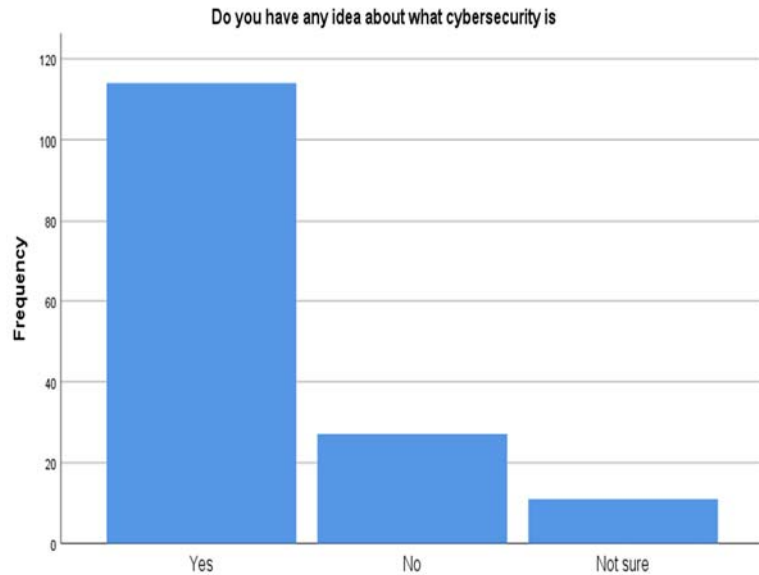


Figure 1. Awareness of Cyber Security

*B. Extent to which Teenagers are Involved in Cybercrime*

Students were further asked about the extent to which they are involved in cybercrime. The cross tabulation in Table I clearly shows that 13 students have been involved in cybercrime, 130 students have not been involved in cybercrime whereas 6 students stated they were not sure whether they had been involved or not. Thus, from the findings, majority (130) representing 87.2% of the respondents have not been involved in cybercrime. Thus, the findings are in line with the argument by [6] when he disagreed in his findings that students are fully occupied with academic and vocational activities which occupies them from engaging in cyber theft. However, [17] and [15] concluded from their findings that most students engage in various forms of cybercrimes.

TABLE I. TEENAGERS INVOLVEMENT IN CYBER CRIME

Age group	Have you been involved in any form of cybercrime before			Total
	Yes	No	Not sure	
10-20	6	44	3	53
16-20	7	84	3	94
21-25	0	2	0	2
Total	13	130	6	149

Furthermore, the students were asked to state their reasons for their involvement in cybercrime. The results from Table II showed that 5 of the teenagers said they were involved in cybercrime to make money and for fun whereas 1 teenager got involved out of ignorance. None of the students were involved in cybercrime due to pressure from friends nor to retaliate.

TABLE II. REASONS FOR INVOLVING IN CYBER CRIME

What was your motivation for getting involved	Frequency
To make money	5
For fun	5
Ignorance	1
Pressure from friends	0
To retaliate	0
Total	11

C. How Often Teenagers Experience Cyberattacks

From Table III, it can be seen that most of the respondents between the frequencies of 43 and 55 concluded that they have never experienced cyberattacks whereas another group which are between the frequency of 4 and 28 indicated that they experienced cyberattack once a while. From the responses, there is an indication that students generally do not experience cyberattacks and for those who do, they often get malware and phishing attacks. Thus, this finding does not confirm the studies by [23] when they found out that there is a higher rate of cyber bullying among public school students. However, the findings are in line with [11] who found that 83% of respondents had experienced a computer virus infection.

TABLE III. RATE OF CYBERATTACKS

Cyber attacks	N/A	Daily	Once a week	Once a month	Once in a while	Never
Malware attacks (viruses, worms, Trojan horses etc.)	5	8	6	3	28	43

Unauthorized access of confidential information like email and other school related documents	6	5	1	2	10	44
Stealing passwords to access accounts	7	5	1	3	25	50
Identity theft and impersonation	6	1	0	1	4	55
Phishing emails	5	6	0	2	13	50
Online fraud	4	7	1	4	13	54

D. Preventive Measures Against Cyberattacks

Fig. 2 is a chart to represent exactly the data in Table IV. From Table IV and Fig. 2, one can conclude that most students use strong passwords to prevent cyberattacks and this represent a frequency of 47 which is a valid percentage of 28%. Also, on the issue of malware protection, it was realized that only 12.4% regularly scan their computers for malwares and out of this, only 10.5% regularly updated their antiviruses. Unfortunately, only a minimal 4.6% of the respondents do not open unknown email attachment. This study confirms the study by [25] who found out that internet users possess adequate cyber threat awareness but apply only minimal protective measures usually relatively common and simple ones in cyber space. As opined by



[13], training of students at a younger age about cyber-attacks and involving them in discussions about cyber bullying will make them aware of cyber security and devise means and ways to stop such attacks and always remain safe and secured on the internet.

TABLE IV. PREVENTIVE MEASURES AGAINST CYBER ATTACKS

Preventive Measure	Frequency	Percentage
Use a mixture of lower- and upper-case alphabets, numbers and symbols for password	41	26.8
Regularly update antiviruses	16	10.5
Regularly update my operating system	12	7.8
Regularly scan computer for viruses and other forms of malware	19	12.4
Do not write/disclose password to anybody	12	7.8
Prevents others from looking over shoulder to view login password	7	4.6
Do not leave default password in use	5	3.3
Change password frequently	8	5.2
Do not open an unknown email attachment	7	4.6
Do not allow others to work in your computer account	5	3.3
Missing System	21	13.7
<b>Total</b>	<b>153</b>	<b>100.0</b>

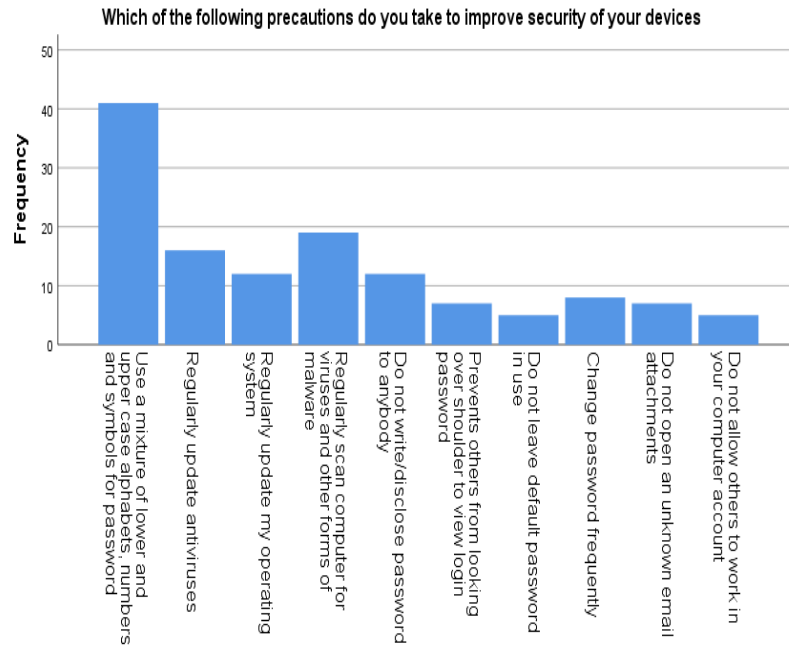


Figure 2. Preventive Measures Against Cyber Attacks

Furthermore, when the students were asked about the actions they take when they experience a cyber-attack and/or cyber bullying, 30.7 percent reported that they changed their password whereas 12.4 percent indicated they did not tell anyone about it and blocked their accounts. Just 1.3 percent reported to the police about cyber-attacks and/or cyber bullying. These results are presented in Table 5. Thus, in line with these findings, [13] opined that individuals facing cyberattacks should report the behavior to the appropriate institutions, and block their accounts. [10] also found that their length of a standard password is around 10 on average which is considered by them as safe.

TABLE V. ACTIONS TAKEN ON CYBERATTACK / CYBERBULLYING EXPERIENCE

Action taken	Frequency	Percent (%)
Report to police	2	1.3
Report to parent	6	3.9
Report to your teacher	5	3.3
Report to website administrator /telephone company	14	9.2
You didn't tell anyone	19	12.4

Changed password	47	30.7
Blocked your account	19	12.4
Missing System	41	26.8
Total	153	100.0

#### IV. CONCLUSION

It is clear from the study that cybersecurity awareness among teenagers in Ghana is high. A very few teenagers are involved in cyber-attacks for the purposes of making money and for fun. The cyber-attacks that teenagers often face are malware attacks and phishing attacks. The study has revealed that these attacks are common among teenagers because they often open unknown email attachments and they fail to regularly update their antiviruses. Again, it has been observed that teenagers change their passwords after they have experienced cyber-attacks. It is therefore recommended that teenagers be more preventive than corrective in their approach toward cyber-attack. They need to periodically change their passwords and update their antiviruses. Although cyber safety has not traditionally been part of the senior high school curriculum, the changing nature of society, in particular the increased use of ICT now justifies its inclusion. Rather than seeing cyber-attack as a reason to deny students access to ICT, the Ministry of Education should regard its increased use as an opportunity to impart safe and responsible practices to students so that they become ethical cybercitizens of the future. Also, the Government of Ghana in conjunction with the security services should develop a national cyber security framework that specifies cyber security requirement controls for individual network users. If approaches towards preventing cybercrime are to be truly effective, the security services should be more proactive and apprehend perpetrators of cyber-attacks so that victims can have the confidence to report cyber cases to them. It is only in this way that the issue of online crime can be addressed effectively.

#### REFERENCES

- [1] Ashiadey, B. Y. (2016). *National Data Centre to spur economic growth*. January 27. Available at: <http://thebftonline.com/business/ict/17079/national-data-centre-to-spureconomic-growth.html> [Accessed 10 February 2016]
- [2] Balfour, C. (2005). A journey of social change: Turning government digital strategy into cybersafe local school practices. In *International Conference on Cyber-Safety, Oxford University, Oxford, United Kingdom*. <http://www.oii.ox.ac.uk/cybersafety>.
- [3] Beach, R. (2010). Developing a cybersafety program for early childhood education. *High-tech tots: Childhood in a digital world*, 71.
- [4] Bele, J. L., Dimc, M., Rozman, D., & Jemec, A. S. (2014). *Raising Awareness of Cybercrime--The Use of Education as a Means of Prevention and Protection*. International Association for the Development of the Information Society.
- [5] Budapest Convention on Cybercrime. (2001). *Council of Europe*. <http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm>
- [6] Denga, A. (2011). *Youths and cyber theft*. Lagos: Ademola Publishers.
- [7] Frechette, J. (2005). *Cyber-democracy or cyber-hegemony? Exploring the political and economic structures of the Internet as an alternative source of information*.
- [8] Geheh, M., Usanov, A., Frinking, E., & Rademaker, M. (2015). *Assessing Cyber Security: A meta-analysis of threats, trends, and responses to cyberattacks*. The Hague Centre for Strategic Studies.
- [9] Halder, D. and Jaishankar, K. eds., 2011. *Cyber Crime and the Victimization of Women: Laws, Rights and Regulations: Laws, Rights and Regulations*. IGI Global.
- [10] Lesjak, D., Zwilling, M., & Klein, G. (2019). Cybercrime and cyber security awareness among students: a comparative study in Israel and Slovenia. *Issues in Information Systems*, 20(1), 80-87.
- [11] Lukanović L. (2017). *Računalniška kriminaliteta in varstvo osebnih podatkov: diplomatska naloga*.
- [12] Marcum, C. D., & Higgins, G. E. (2019). Cybercrime. In *Handbook on Crime and Deviance* (pp. 459-475). Springer, Cham.
- [13] McCrohan, K. F., Engel, K., & Harvey, J. W. (2010). Influence of awareness and training on cyber security. *Journal of internet Commerce*, 9(1), 23-41.
- [14] Ministry of Communications (2014). *Ghana National Cyber Security Policy & Strategy*. Accra.
- [15] Ngozi, S. (2016). Students' perception of cybercrime and its implications. *Journal of Social Development*, 4(2), 50-57.
- [16] Omondi G. (2020). *The state of mobile in Ghana's tech ecosystem*. Mobile for Development- GSMA.
- [17] Philips, C. A. (2018). Awareness and involvement in cybercrime among undergraduate students in Universities in Rivers State, Nigeria. *International Journal of Humanities and Social Science Invention*, 7(3), 39-43.
- [18] Rathod, P., & Potdar, A. B. (2019). Study of Awareness of Cyber-Security among Medical Students. *Indian Journal of Forensic Medicine & Toxicology*, 13(1), 196 – 198.
- [19] Rek, M., & Milanovski, B. K. (2017). Slovenija, Ljubljana: Fakulteta za medije [izdelava], 2016. *Slovenija, Ljubljana: Univerza v Ljubljani, Arhiv družboslovnih podatkov [distribucija]*, IDNo: MPSS16.
- [20] Saima B. (2018). *Cyber Crime Awareness amongst students of Government Law College, Trivandrum- A legal Survey*. Government Law College, Trivandrum. [Internet]. <https://acadpubl.eu/hub/2018-119-16/1/130.pdf>
- [21] Saul, B., & Heath, K. (2015). Cyber terrorism. In *Research Handbook on International Law and Cyberspace*. Edward Elgar Publishing.
- [22] Sourander, A., Klomek, A. B., Ikonen, M., Lindroos, J., Luntamo, T., Koskelainen, M. & Helenius, H. (2010). Psychosocial risk factors associated with cyberbullying among adolescents: A population-based study. *Archives of general psychiatry*, 67(7), 720-728.
- [23] Topçu, Ç., Erdur-Baker, Ö., & Çapa-Aydin, Y. (2008). Examination of cyberbullying experiences among Turkish students from different school types. *CyberPsychology & Behavior*, 11(6), 643-648.
- [24] Varghese, B., Wang, N., Barbhuiya, S., Kilpatrick, P., & Nikolopoulos, D. S. (2016, November). Challenges and

- opportunities in edge computing. In *2016 IEEE International Conference on Smart Cloud (SmartCloud)* (pp. 20-26). IEEE.
- [25] Zwillig, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., & Basim, H. N. (2020). Cyber security awareness, knowledge and behavior: a comparative study. *Journal of Computer Information Systems*, 1-16.

# Challenges Cybersecurity Architects Are Facing In A Cloud Computing Environment

Anton Allen

*Texas A&M University*

400 Bizzell St, College Station, USA

[lilant2012@tamu.edu](mailto:lilant2012@tamu.edu)

Ethan Puchaty

*Lockheed Martin*

1 Lockheed Blvd, Fort Worth, USA

Behbood Zoghi

*Texas A&M University*

400 Bizzell St, College Station, USA

[zoghi@tamu.edu](mailto:zoghi@tamu.edu)

**Abstract-** In the past decade, cloud computing has become an integral part of many companies' business strategies and IT architecture. Companies look to seek and adopt new business models, increase efficiency in handling massive amount of data, handle fluctuations in computing workloads for customers and stakeholders, and gain a competitive advantage in their industry. All these concepts have to be considered while also trying to deliver a product or service, and not disrupt existing operations for the company. This paper will address the multilevel challenges and threats in cloud computing and their potential solutions.

Cloud adoption has introduced the three types of cloud computing service models. The first is the Infrastructure as a Service (IaaS) model, which is defined as an instant computing infrastructure that is provisioned and managed over the internet. The second is the Platform as a Service (PaaS) model, in which companies essentially rent everything they need to build an application and rely on the cloud provider for development tools, infrastructure, and operating systems. The third is Software as a Service (SaaS) model, which is a software distribution model in which a cloud service provider will host applications for customers and makes them available over the internet.

Many companies have developed a new approach called hybrid cloud computing. The growth of the hybrid cloud model has allowed companies to use a mix of the three models with public and private clouds to create the best environment for their company's infrastructure. The top benefits of this approach include: Better security, Operating cost, improvements, and Speed and agility increase.

A hybrid cloud model can eliminate or greatly reduce trade-offs and offer the best solutions for the company. Implementation and management can still be challenging for a hybrid cloud model. Having different management tools for a private or public cloud, introduces a fragmented IT infrastructure that strongly lacks interoperability and visibly for the company.

**Keywords-component; cybersecurity; cloud computing; hybrid cloud**

## I. BACKGROUND

Cloud computing is a new name for an old concept that has been around for years and it is simply defined as the delivery of services or resources through the internet. These resources include tools and applications like data storage, servers, databases, networking, and software. It allows businesses to have the flexibility and efficiency to meet new and growing demands in any industry. Cloud computing provides the infrastructure, software, and platforms necessary for success in today's business landscape no matter where it is needed. As the presence of cloud computing becomes more widespread, the demand for professionals who can manage and configure these cloud networks properly is also becoming more inescapable.

Since 2009, companies have been shifting their data storage and computing needs to cloud-based services and away from agency-owned or in-house data centers. This shift was led by two primary goals: reduce the total investment into Information Technology (IT), which stands at about \$90 billion each year, and take advantage of what cloud adoption offers [1]. Which is efficiency, accessibility, collaboration, rapidity of innovation, reliability, and security. However,

this adoption also led to many challenges with shifting to cloud services. IT managers expressed concerns about security in certain cloud environments, the complexity of migrating existing legacy applications to the cloud, and the lack of skilled staff to manage the cloud environments. On the government side, planning for cloud adoption began with the 2010 publication “A 25-Point Implementation Plan to Reform Federal IT Management”. Then in 2017 the “Report to President on Federal IT Modernization”, the Office of Management and Budget (OMB) pledged to update the government’s legacy Federal Cloud Computing Strategy called “Cloud First”. This effort also led to the creation of The Federal Risk and Authorization Management Program (FedRAMP) which is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services [1].

As cloud adoption has become standard in most industries, cybersecurity architects have to configure and manage their companies cloud infrastructures while also mitigating the challenges that come with cloud environments. This research paper will discuss many topics but will focus on three main challenges: control, security and trade-offs, and risk. With these three focus areas, the scope of the project will discuss the challenge, mitigation, and the potential solutions for these challenges.

#### A. *Control*

In a cloud computing environment, the level of control a company has is based on the type of service and cloud deployment model you choose. With a public cloud, all hardware, software, and other supporting infrastructure is owned and managed by the cloud provider. Employees access these services and manage their accounts using a web browser. Although, public clouds can save companies from the expensive costs of having to purchase, manage, and maintain in-house hardware and application infrastructures. The cloud service provider is held responsible for all management and maintenance of the system. This severely reduces the control for a cybersecurity architect, since they have to rely on the cloud service providers for almost all aspects of the cloud infrastructure.

A private cloud provides the cloud computing resources to be used exclusively by a single business or organization. It can be physically located on-site at a company datacenter but most companies want to rely on a cloud service provider to host their private cloud, since the services and infrastructure are maintained on a private network. Private clouds deliver a higher level of security and privacy through both company firewalls and internal hosting, to ensure operations and sensitive data are not accessible to outside parties. This elevated level of control also has one key drawback that the company’s IT department is held responsible for the cost and accountability of managing the private cloud. This leads to private clouds requiring the same staffing, management, and maintenance expenses similar to traditional ownership of a data center. This also provides a company with high assurance since the private cloud is managed by their own in-house IT department.

Most cybersecurity architects will lean more towards a hybrid cloud which combines a public and private cloud, by allowing data and applications to be shared between them. When computing and processing demand fluctuates, hybrid cloud computing gives businesses the ability to seamlessly scale their on-site infrastructure up to the public cloud to handle any overflow, without giving third-party datacenters access to all of their data. Cybersecurity architects gain the flexibility and computing power of the public cloud for basic and non-sensitive computing tasks. While keeping business-critical applications and data on-site safely behind a company firewall. Companies will pay only for resources

they temporarily use instead of having to purchase, program, and maintain additional resources and equipment that could remain idle over long periods of time. The challenge with a hybrid cloud is with multiple infrastructure platforms come increased possibilities of incompatibility of tools and processes. Also, the combination of both clouds allows data to be moved across platforms and adds an increased risk of data exposure to the company. Companies will have to determine if existing tools will suffice or if teams need to acquire and learn new tools to ensure compatibility and security.

### *B. Security and Tradeoffs*


Security and tradeoffs can be discussed together based on the cloud service the company chooses to use for their cloud implementation. Most cloud computing services fall into three broad categories: Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). These are sometimes called the cloud computing "stack" because they build on top of one another. The most basic category of cloud computing services is Infrastructure as a service (IaaS). With IaaS the cloud service provider manages the infrastructure while the company purchases, installs, configures, and manages its software, operating systems, middleware, and applications. Platform as a service (PaaS) refers to cloud computing services that supply an on-demand environment for developing, testing, delivering, and managing software applications. PaaS is designed to make it easier for developers to quickly create web or mobile apps, without worrying about setting up or managing the underlying infrastructure of servers, storage, network, and databases needed for development. The company manages the applications and services they develop, and the cloud service provider typically manages everything else. Software as a service (SaaS) is a method for delivering software applications over the internet on-demand and typically on a subscription basis. With SaaS, cloud providers host and manage the software application and underlying infrastructure and handle any maintenance, like software upgrades and security patching. All of the underlying infrastructure, middleware, app software, and app data are located in the cloud service provider's data center. Authorized users connect to the application over the internet, usually with web a browser on their phone, tablet, or PC [2].

Each service model has its tradeoffs but when it comes to security, they all face similar security challenges. An Application Program Interface (API) is the key to successful cloud integration and interoperability, it allows the end-user to interact with a cloud provider's service. Many cloud providers have their own proprietary APIs unfortunately, not every API is entirely secure. Most cloud provider's APIs are initially developed in-house and external security assessments are not conducted and are later found to be insecure. This problem is compounded when the client company has built its application layer on top of these APIs. The security vulnerability will then exist in the customer's application. This could be an internal application, or even a public-facing application potentially exposing private data. Security with cloud data has an additional set of unique challenges since data is stored with the cloud service provider and accessed over the internet. This means visibility and control over that data are limited and also raises the question of how it can be properly secured. Cloud service providers treat cloud security as a shared responsibility model in which, the cloud service provider covers the security of the cloud itself and the customer covers the security of what they put in it [2].



Figure 1, provides a depiction of the shared responsibility model for cloud security:

Shared Responsibility Model for Security in the Cloud			
On-Premises (for reference)	IaaS (Infrastructure-as-a-service)	PaaS (Platform-as-a-service)	SaaS (Software-as-a-service)
User Access	User Access	User Access	User Access
Data	Data	Data	Data
Applications	Applications	Applications	Applications
Operating System	Operating System	Operating System	Operating System
Network Traffic	Network Traffic	Network Traffic	Network Traffic
Hypervisor	Hypervisor	Hypervisor	Hypervisor
Infrastructure	Infrastructure	Infrastructure	Infrastructure
Physical	Physical	Physical	Physical

 **Customer Responsibility**


 **Cloud Provider Responsibility**

Figure 1: Shared responsibility model for security in the Cloud.

### C. Risks

Something that is not widely discussed in the cloud computing environment is what risks are associated with cloud computing. Risk can be broken out into five key areas: data regulatory and security, technology, operational, vendor, and financial risks. Data security and regulatory risk can be associated with loss, leakage, or unavailability of data. This can cause business interruption, loss of revenue, loss of reputation, or regulatory non-compliance. The regulatory risk is associated with non-compliance with various national/geographic regulations, industry, or service-specific legal and regulatory requirements. The technology risk can be associated with constantly evolving technologies and lack of standardization in how they integrate or interoperate. These risks could lead to costly re-architecture efforts for adoption or integration with new technologies. Operational risk can be associated with the execution of IT services and tasks that the business relies upon. Cloud migration has also brought to the forefront a new approach called DevOps, where development and operations responsibilities are merging. This allows deployment times to be cut down to days rather than weeks or months. It can have an impact on day-to-day IT operations and development teams will need to be trained in cloud deployment and management. Vendor risk comes from leverage or association with vendors. Unforeseen vendor circumstances such as bankruptcy, lawsuits, SEC probe, or any other act of defamation for the vendor could significantly damage an organization’s reputation and goodwill. This risk would apply to private and public cloud computing scenarios due to the association with and reliance on a service provider. Lastly, financial risk can be associated with overspending and loss of revenue. Companies usually underestimate the initial cost to build and maintain a cloud environment and continue to carry the capital expenditure related to hardware and software. The financial risk is mainly related to the variable nature of costs, tied to running up the cost of using the cloud due

to poor planning and requirements from the business. Managing cloud costs needs a level of focus, skill, and tools that were not required in the past [3].

#### *D. Scope*

The scope of this project will provide a deliverable on mitigation, best practices, and potential solutions to the three main challenges described earlier in this report which is: control, security and trade-offs, and risk. This deliverable will also describe how cybersecurity architects can leverage FedRAMP and DISA requirements onto the potential cloud services providers to ensure regulatory compliance is adhered to. For the security aspect, the deliverable will address actions to take before adding a cloud service to the company workflows and enforcing an external cloud security risk assessment. This risk assessment involves identifying what the biggest risks are, what their impacts would be, and how the likelihood of each risk to occur.

## II. METHODOLOGY

The methodology design utilized a mixed method which is the nature of both quantitative and qualitative research. The qualitative research was based on fundamental four questions that the cyber expert was interviewed on:

1. What are the benefits of implementing Cloud Computing in your specific field/department?
2. What are the issues affecting the adoption of Cloud Computing by cyber architects?
3. How can these factors best be addressed to increase the rate of uptake and use of cloud computing?
4. What measures or procedures need to be in place to ensure the success of adoption and utilization of cloud computing?

In cloud computing quantitative research, it focused on how a company is assessing responses to a measure. One of the key benefits discussed that can be conducted is a cloud security assessment. The assessment provides an extensive report that includes the following:

- Identify cloud security risks
- A cloud security audit to document current controls and provide visibility into the strengths and weaknesses of the current systems
- Assess gaps in current capabilities that may weaken cloud security and recommend technology and services to address them
- Assess the security maturity by benchmarking current controls and practices against leading methods and standards
- Assess the effectiveness of current policies and their alignment with the company's business goals

#### *A. Participants*

As mentioned above on the four fundamental questions asked to participants that are currently in the cloud computing industry or have extensive experience in the field. The targeted number of participants were cybersecurity architects that have 5-10 years of experience in cloud computing infrastructure.

*B. Instruments*

In regards to instruments used; this is a very critical part of the methodology section. For this report, the instruments that were used are the four interview questions and a cloud security assessment, which include an extensive report base on the criteria used or agreed upon.

The following sections explain each metric in a cloud security assessment and how it can correlate to the quantitative data research [4]:

- **Policy** – This will include standard policies and procedures that should be implemented. The most common is called Security Technical Implementation Guide (STIG). Which is a cybersecurity methodology for standardizing security protocols within networks, servers, computers, and logical designs to enhance overall security. These guides, when implemented, enhance security for software, hardware, physical and logical architectures to further reduce vulnerabilities.
- **Control Result** – Provides which Risk Management Framework (RMF) controls that have passed or failed in the assessment. RMF will be explained in detail later in this section.
- **Services** – Provide the list of services/systems that were evaluated and included in the assessment
- **Evaluations** – Provide the criteria that are being scored or evaluated (i.e., password complexity)
- **Security Posture** – This is a breakout of all the evaluations assessed with the amount that has failed or passed the assessment
- **Failures to Criticality** – Breaks down all the findings from a ranking to Low, Medium, and High

### *C. Procedure & Data Analysis Plan*

In discussing the cloud security assessment as an instrument used to evaluate the quantitative data. The steps below are the procedures that would be followed to conduct the assessment, along with the deliverables that will be provided [5]:

- **Initial Document Review** of migration strategies, architecture diagrams, hardening documentation, access management policies and standards, SOPs/playbooks, and logging standards, conducted offsite in collaboration with client stakeholders
- **Onsite Workshops** to explore the cloud environment, the current security model in place, and potential security concepts and controls to implement in the future
- **Configuration Review** of the cloud platform to ensure security controls are implemented effectively, identify potential weaknesses, and confirm learnings from the onsite workshops to identify potential weaknesses that could be exploited by attackers.
- **Reporting** that details practical technical recommendations to harden the cloud environment, enhance visibility and detection and improve processes to reduce the risk of compromise.

Below are the deliverables that would be provided after the assessment:

- A snapshot of the current cloud environment, detailing existing architecture and security controls
- Security for specific cloud services aligned with the current configurations and operational processes
- Practical recommendations for enhancing visibility and detection
- Prioritized and detailed recommendations for further hardening the cloud infrastructure

There will be key focus areas that will be evaluated during each assessment as shown in Figure 2 [5]:

Governance, Risk and Compliance	Security Architecture and Networking	Identity and Access Management
<ul style="list-style-type: none"> <li>• Cloud governance and services</li> <li>• Cloud policies and standards</li> <li>• Threat risk assessments</li> <li>• Vulnerability management</li> <li>• Regulatory compliance requirements</li> </ul>	<ul style="list-style-type: none"> <li>• Cloud architecture and security controls</li> <li>• Network segmentation and on-premise integration</li> <li>• Remote system connectivity and management</li> <li>• Disaster recovery</li> <li>• Containers, configurations and security controls</li> </ul>	<ul style="list-style-type: none"> <li>• Cloud authentication infrastructure, including on-premise connectivity (e.g., ADFS)</li> <li>• Identity management</li> <li>• Privilege access management</li> <li>• Role-based access controls</li> </ul>
Secrets and Data Protection	DevOps	Threat Detection and Response
<ul style="list-style-type: none"> <li>• Data protection and loss prevention</li> <li>• Database security</li> <li>• Certificates and keys management</li> <li>• Encryption</li> </ul>	<ul style="list-style-type: none"> <li>• Pipeline configurations</li> <li>• System and application deployment</li> <li>• Secure software development life cycle</li> <li>• Code repository security controls</li> </ul>	<ul style="list-style-type: none"> <li>• System, database, and application logging</li> <li>• Security logging and centralization</li> <li>• Endpoint and network security controls</li> <li>• Cloud incident response processes</li> </ul>

Figure 2: Core Focus Areas for Evaluation During the Assessment.

#### D. Risk Management Process

The Risk Management Framework (RMF) is a set of information security policies and standards the federal government developed by The National Institute of Standards and Technology (NIST). There are three NIST special publications that cover the RMF process and cloud computing control guidance [6]:

- **NIST SP 800-37** “Guide for Applying the Risk Management Framework to Federal Information Systems”
  - Describes the formal RMF certification and accreditation process
- **NIST SP 800-53**, “Security and Privacy Controls for Federal Information Systems and Organizations”
  - Describes a structured process for integrating information security and risk management activities into system development from start to finish.
- **NIST SP 800-210**, “General Access Control Guidance for Cloud Systems”
  - Describes cloud access control characteristics and a set of general access control guidance for cloud service models

The RMF process applies a risk-based approach that considers effectiveness, efficiency, and restrictions due to regulations, directives, executive orders, and policies. The RMF process has identified the following activities, which can be applied to both new and legacy systems and are broken down into six steps [6]:

1. **Categorize** – Classify and label the information processed, stored, and shared, and the systems that are used; this is done based on an impact analysis
2. **Select** – Review the categorization and select baseline security controls; revise and add to the security control baseline as necessary, based on organization assessment of risk and local conditions
3. **Implement** – Implement the security controls and integrate with legacy systems; document how the controls are arrayed within the system and their effects on the environment
4. **Assess** – Evaluate the security controls to determine whether or not they are implemented correctly, and their quality and effectiveness

5. **Authorize** – top management tests and approves the secured system based on the accepted risk appetite to operations and assets (i.e., how much risk the organization is willing to tolerate). Management also considers the system’s operational impact on individuals and other organizations. It will identify how much risk is still present, and either authorize it or decide on changes needed.
6. **Monitor** – Set up an ongoing monitoring and assessment schedule for security controls to measure effectiveness. Document system or operation adjustments, and include impact analyses of changes made, Report findings to information security officials

As the RMF process is meant to be a continuous cycle, the evaluator can then start again from step one, all the way through to step six to account for changes in the cloud computing environment. In Figure 3, it depicts the RMF process in a continuous life cycle and the applicable SP guidelines to adhere to [6]:



Figure 3: The RMF Process.

During the RMF process, a Plan of Actions and Milestones (POA&M) is developed that describes specific measures to be taken to correct deficiencies found during the cloud security assessment. The POA&M identifies the following [7]:

- The tasks needed to correct the deficiency
- The resources required to make the plan work
- Milestones in completing the tasks
- Scheduled completion dates for the milestones
- The categorization impact level of the system



- The specific deficiencies that have been found
- What potential impact the deficiency can have on the risk exposure of the organization or the ability to perform its mission
- The proposed approach to risk mitigation
- Any rationale for accepting some risk level caused by specific deficiencies

POA&M's are key to both the authorization and the continuous monitoring process. An assessment of security controls triggers the need for a POA&M, and the POA&M deficiency item must be kept open and tracked until the deficiency has been mitigated. Continuous Monitoring uses the POA&M items as one of the criteria to select candidates for monitoring [7].

### III. ANALYSIS

In any project to determine the best outcome regardless of what industry a company is in, some form of analysis has to be conducted. As mentioned in the previous section of this report, data were collected with a mix of qualitative and quantitative research. In this section, the report will review and provide the answers to the four fundamental questions in cybersecurity and also provide the results from the 2020 Amazon Web Services (AWS) cloud security assessment report.

#### A. Interviews

##### 1) *What Are the Benefits?*

The first question on the survey the cybersecurity professionals answered was “What are the benefits of implementing Cloud Computing into your specific field/department? The answers to this question were all very common with the use of cloud computing in any industry today was cost-cutting. Reduced IT costs are one of the key motivators for any company to adopt cloud computing and this was a common answer among the group. The reason for this is because with cloud computing the company is utilizing the computing power and resources of a cloud service provider. This allows the company to require the employee or customer access to the application program interface (API) through an internet connection. Many companies that are not currently using a cloud computing infrastructure have to budget for system upgrades and computing resources for their employees and in some instances for the customer. Another aspect that reduces cost ties to a reduction in required IT staff. Most companies have numerous IT staff to help with maintenance and computer support, with cloud computing this can be shifted to the Cloud Service Provider (CSP). Which allows the company to have a small dedicated IT staff for the company.

The second benefit was scalability. Which is defined as the ability to increase or decrease IT resources as needed to meet changing demand. Scalability is one of the top key benefits a company would consider to move their infrastructure to the cloud. Everyone in the world has seen the benefits of this firsthand due to the Covid-19 pandemic, which resulted in 75% of the workforce having to work from home. Companies had to quickly scale up their computing resources to adapt to the surge in demand from employees working from home. Companies that had already adopted cloud computing were quickly able to see the benefits.

The third benefit was business continuity. Which is an organization's ability to ensure operations and core business functions, are not severely impacted by a disaster or unplanned incident that takes critical systems offline. This also includes company data been backed up and protected. Many large-scale companies can afford to have large data centers in various locations, in the event of a natural disaster to one data center. Smaller companies don't have the resources to do this and adopting a cloud computing environment, would allow them to back up company data and ensure it is protected in the event of a natural disaster.

The last benefit was collaboration efficiency, which enables employees to work simultaneously on documents that live "in the cloud". This allows authorized users to access files from anywhere with an internet connection. This concept has been standard practice in corporations and education, Google Drive is one of the most used collaboration tools. This program allows multiple users to update and edit documents in real-time with multiple users.

## 2) *Issues Affecting the Adoption of Cloud Computing*

The first issue was risk, and this can be further broken down into three parts:

1. **Policy & Organizational** – Once a company chooses a CSP they are locked into that service provider and also risk the loss of governance for the cloud infrastructure once the service is established.
2. **Legal** – This risk lies with how the CSP protects the client or companies data and who is at fault in the event of a data breach.
3. **Availability** – When you are dependent on another cloud provider, you could encounter unexpected downtime.

The next issue was security and privacy. These two topics are the main issues that companies face day-to-day even beyond just in the cloud computing environment. AWS is a very popular cloud service and has multiple safeguards in place to secure your data. The concern is how are they ensuring your data are protected? In many cases, CSPs provide a potential client a few overviews on how they protect your data but the customer doesn't have control if they feel it's more or less secure than an in-house setup. There are tiers of service a company can pay for to increase the level of protection, the increase in protection the higher the cost. The other caveat to data protection is compliance, most CSPs have internal metrics for cloud computing compliance. A few CSPs do provide FedRAMP compliance certifications but are not mandated or required by the government, unless the company is doing business with a government entity or a defense contractor. Companies also have to factor in the service level agreement that is agreed upon by both parties. CSPs provide an SLA for all customers, the risk is this agreement is very hard to customized based on the company or service required.

The last issue was data confidentiality, this is a major concern for government and commercial organizations. Since cloud service is based on being stored on various data centers all over the country or sometimes the world. The client takes the risk and has a lack of control of the physical infrastructure where the data are stored. An in-house infrastructure can provide an extra layer of physical protection from data centers. CSPs normally provide a local security company and minimum safeguards in most centers. This allows off-premises staff access to data from the CSPs customers.

### 3) *How Can the Issues Be Addressed and What Procedures Need to be in Place*

The last two questions were designed to be answered together to allow the questionees to provide their answer and a solution on how it can be done. The first answer was cost savings. This is something that IT departments and upper management will want to cover in great detail. In cloud computing, most services have a pay-as-you-go model. In this approach, companies can scale up or down based on the expected usage for the company. During lower peaked times a company will pay less money for the cloud services and can anticipate an increase in spending when more computing resources are needed. Before a company considers moving its network to the cloud, the IT department should build action plans to meet the organizational objectives for the company in a cloud computing environment. From a security standpoint, CSPs have the full-time job to carefully monitor security on their cloud networks as well as their clients. Companies can employ a small, dedicated staff just to monitor the companies cloud environment and this will also make it easier to meet government or company compliance requirements. The company also needs to work with the CSP to encrypt data during transit and at rest for all data stored on the cloud provider's network.

In regard to the risk, one major topic was to implement cloud and on-site backups of company data. In the event the CSPs service is disrupted or not in service, the client still has access to their data on their company networks. This will allow the company to develop contingency plans in the event of a cloud service outage. During the planning phase for cloud adoption ensure the company can choose a CSP that allows modification to the SLA. That should include the following:

- Clauses and procedures for terminating service
- Data protection techniques or services that have to be implemented
- Able to choose physical locations where data will be stored
- Procedures in place for only cleared staff can access data offsite

## IV. RETURN ON INVESTMENT

Organizations are switching to the cloud at a faster rate than ever. Companies will need to incorporate a sound migration plan for any enterprise taking on cloud migration. Along with this plan, the company will want to perform due diligence to understand the costs and returns associated with the migration. Executives will want hard figures to justify the investment to themselves and management. Many organizations that choose the cloud migration path tend to use a return on investment (ROI) assessment. To determine if cloud migration will save the company money, help them achieve their organizational goals, and how long it will take them to recoup that investment [8].

### A. *The Cloud ROI Formula*

The ROI formula of return over costs appears relatively simple, it can be surprisingly complicated when applied to cloud migration. Comparing on-premise vs cloud ROI calculations can be complicated and may not return enough numerical data the company would need to make decisions. As mentioned earlier in this report, cloud models range from Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). In the cloud, if the service is less customized and more dependent on the cloud service provider, it will reduce the initial capital investment and increases the operational investment over time based on subscription fees.

Figure 4, summarizes the three cloud models and how they range in scope:

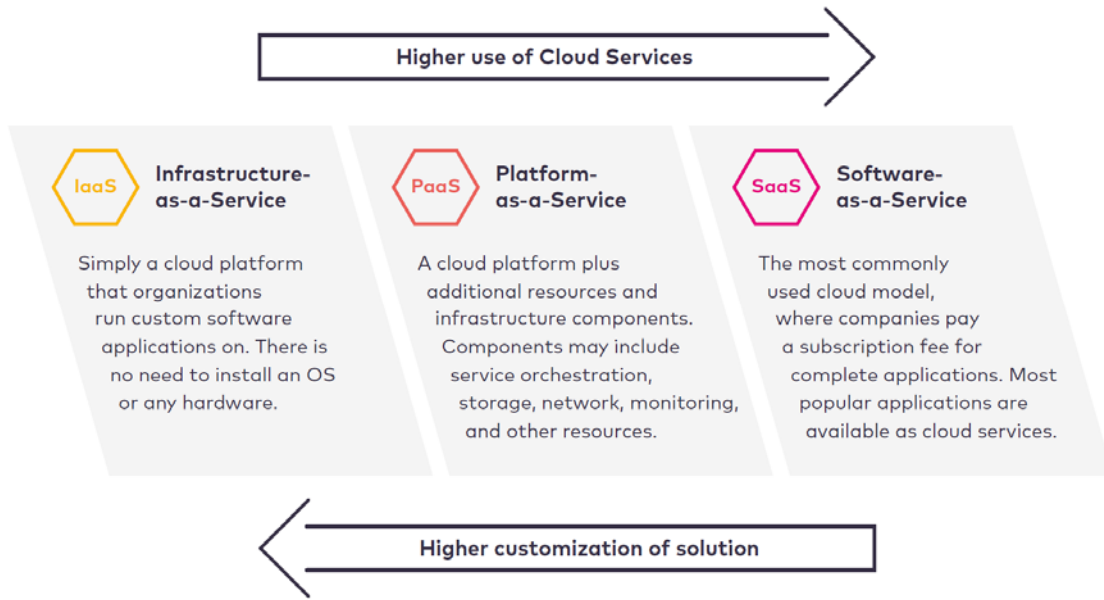


Figure 4: Cloud Model Service Ranges.

A particular company cloud migration can mix many of these cloud models on an application-by-application basis. Some applications may need a very custom Infrastructure-as-a-Service (IaaS) approach versus others that may only require a Platform-as-a-Service (PaaS) configuration. It may be decided that there is a need to keep some applications on-premises and move others to the cloud, creating a hybrid solution.

### B. Cloud Value

Cloud Value can be broken out into five categories: Agility, Productivity, Quality, Reduced Costs, and Employee Retention. Any improvements in these will have a lasting impact on any organization [8].

#### 1) Agility

Refers to the ability to rapidly adapt and provide cost efficiency in response to changes in the business environment. Cloud computing allows companies to decrease the time it takes to provision and de-provision IT infrastructure. This speeds the delivery of IT projects that are critical to revenue growth or cost reduction, this can be calculated into a numerical value based on the IT project.

#### 2) Productivity

The cloud provides a more productive environment for collaborative working. The flexible infrastructure that can be accessed translates into businesses enhancing their productivity among their employees and customers. Organizations can increase or scale down their operations to support their business goals such as attracting and retaining new customers or speeding up the time-to-market for the latest services.

#### 3) Quality

The cloud can improve service and product quality through customization and enhanced user experience. The cloud provides the opportunity to automate deployments and rollbacks. The company can ship and test features faster as

many times as they want in a business day. This feature is especially important since it creates an environment for continuous improvement, improving the product and the client's experience overall.

#### *4) Reduced Costs*

Cloud computing can optimize ownership use by reducing the application total cost of ownership. This is established through reducing licensing costs, open-source adoption, and Service-Oriented Architecture (SOA) reuse adoption. The cloud also optimizes the cost associated with delivering a specified IT service capacity by aligning IT costs with IT usage, this can be effectively managed with pay-as-you-go savings. Thanks to economies of scale, cloud providers can facilitate better up-to-date resources for less money than most on-premise infrastructures.

#### *5) Employee Retention*

Cloud implementation provides the opportunity for the IT team to go through a full cultural transformation. This transformation puts cooperation, communication, and empowerment at the core of a company's values. The new culture provides the ideal scenario for team members to shift their focus from process-oriented and support tasks to research and development, and it breaks the communication barriers between many company silos. A successful movement to the cloud culture makes for happy employees that are engaged in the work they want to do, and can greatly increase employee retention.

All these categories roll up to provide any company a great deal of value. But, as mentioned, much of this value is intangible and difficult for management to translate into numeric terms. These five categories are part of the reason a company is willing to invest the move to the cloud.

### *C. Estimating Cost in the Cloud*

Moving to the cloud means moving away from all the hardware-related, software-related, and personnel costs of managing rooms of servers and data centers towards a pay-as-you-go model with ongoing subscription fees.

Figure 5, illustrates some of the initial and ongoing costs related to a cloud transition [8]:

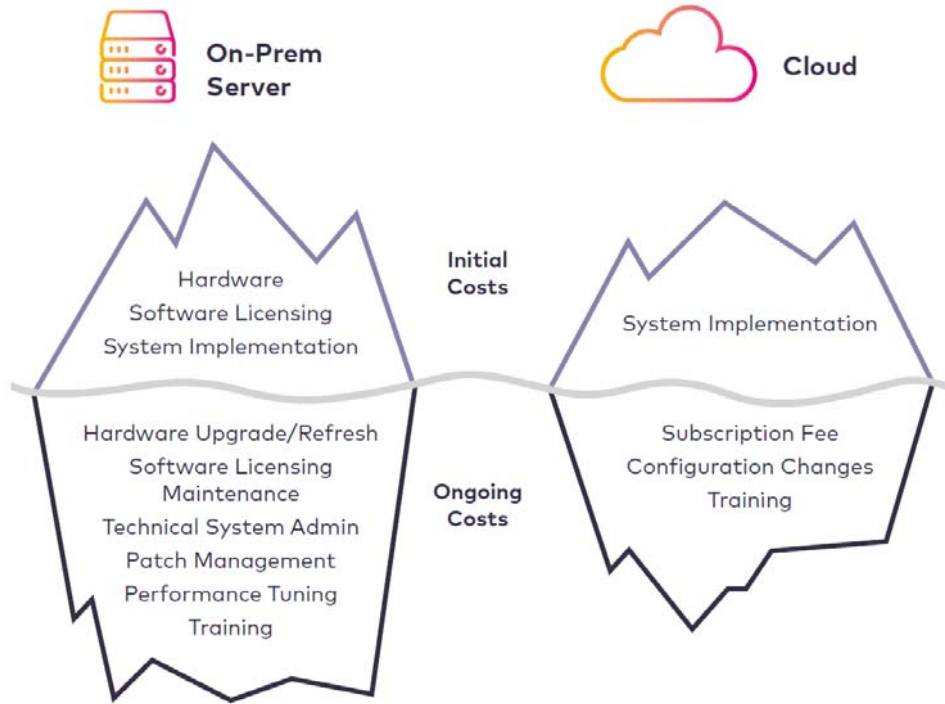


Figure 5: Initial and On-Going Cloud Costs.

The bulk of ongoing costs for the cloud involve subscription fees, configuration changes, and training or new hiring. To assess cloud migrations many companies, use the concept of Total Cost of Ownership (TCO) for comparing cloud solutions to their current state. TCO intends to uncover both the direct and indirect costs of owning and procuring certain assets or products. It includes a few key components:

- Acquisition/Physical Hardware Costs
- Operations Costs
- Personnel Costs

The steps for calculating TCO costs for an application are listed below:

- Audit current IT infrastructure costs
- Calculate the estimated cloud infrastructure costs
- Estimate cloud migration costs
  - Data Migration
  - Integration and Testing
  - Consulting Fees
- Approximate additional post-migration costs

Within the TCO calculations, companies often overlook and identify the hidden costs. Figure 6 identifies hidden costs as related to software development. Rows represent resource categories and columns represent IT life-cycle stages [8]:

	Acquisition	Maintenance	Upgrade/Retire
Software	Obvious Cost	Obvious Cost	Hidden Cost
Hardware	Obvious Cost	Obvious Cost	Hidden Cost
Personnel/HR	Hidden Cost	Hidden Cost	Hidden Cost
Facilities	Hidden Cost	Hidden Cost	Hidden Cost

Figure 6: Cloud Computing Hidden Cost.

*D. Investing IT Resources in the Cloud*

To truly understand the ROI for cloud adoption, we have to understand how value is created from investing in IT. Figure 7, shows a comparison of demand for traditional IT resources versus cloud-based resources [4]:

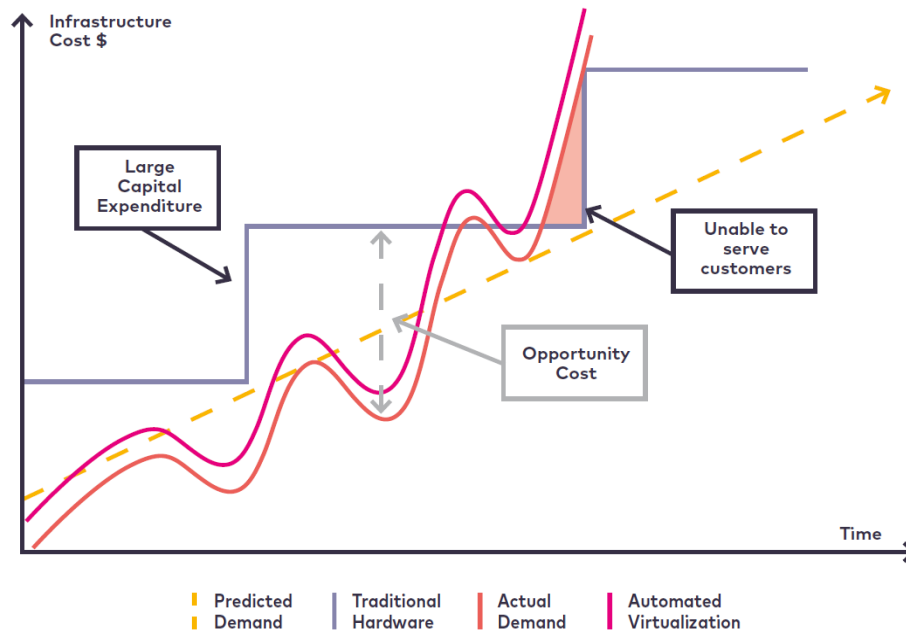


Figure 7: Traditional IT Resources vs. Cloud-Based.

Traditional on-premise infrastructure requires provisioning resources for the companies estimated demand. In most cases, this translates into underutilized resources and large capital expenditures (represented as the blue stair-stepping line graph above). Cloud services (represented by the yellow line) grow as an on-demand model that provides the necessary resources at the right time, aligning with the companies demand and minimizing downtime. It is important to note that the ROI of cloud services is directly related to how cloud-native those services are. The deeper the infusion into cloud services, the bigger the return. In traditional systems, incorporating new technology, adding a new product, or implementing a new feature is often a lengthy process.

Figure 8, illustrates how the timeline for these kinds of deployments can be greatly reduced in the cloud:

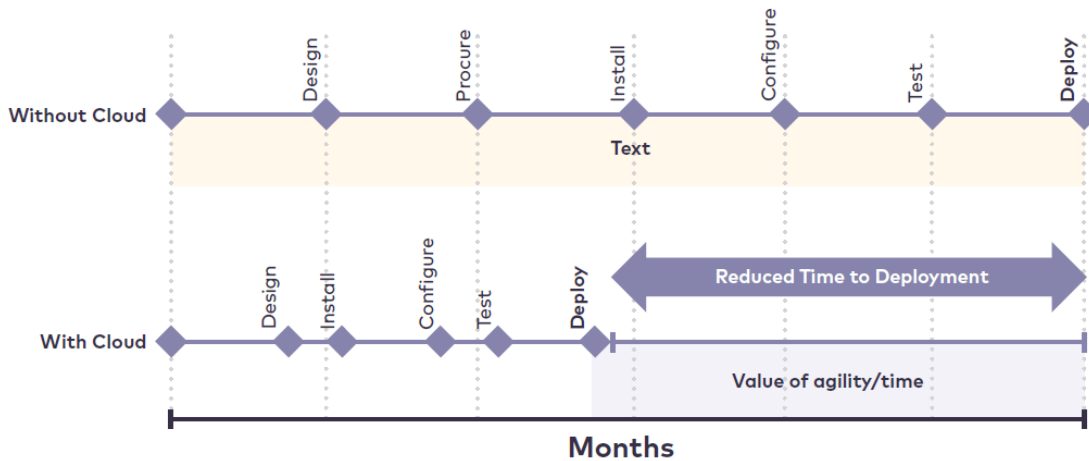


Figure 8: Cloud Deployment Time Comparison.

With a cloud infrastructure, it can allow quick access to a broad set of resources. The company can set up fast installation and configuration of their software, do all the necessary testing, take the new product or feature to market, or in the worst-case scenario. Fail fast and only pay for the time utilized for those resources. The increased speed provides the perfect scenario for developing new sources of revenue at a faster rate and potential innovation from quick access to experimentation. Cloud computing allows companies to focus their attention on doing things that help grow revenue, increase customer engagement, and open new product channels. That is the true compound return on investment of cloud computing technology [8].

## V. RECOMMENDATIONS AND CONCLUSIONS

The final section of this report with a combination of the data gathered and analysis conducted. Provides a company’s cloud security architect recommendations to help prevent some of the issues addressed in this report.

### A. DevSecOps Adoption for Cloud Security

DevSecOps is defined as integrating security practices within the development process that involves creating a 'Security as Code' culture with ongoing flexible collaboration between release engineers and security teams. This allows breaking the norm of having security as a separate process. DevSecOps allows for security integration across all stages of software development while addressing security concerns during the System Development Life Cycle (SDLC) and not just at the end. The DevSecOps approach for cloud security requires some detailed planning and a cultural change with the company’s IT department. The planning stages require security teams to [9]:

- Collaborate with development teams as they move code to the cloud and close monitoring of quality in the production cycle.
- Work with the quality analysis and development teams in deciding qualifier and parameter aspects required for code approval



There is a six-step continuous process to successfully implement DevSecOps into the cloud is shown in Figure 9 [9]:



Figure 9: Veritis Six-Step DevSecOps Implementation Process.

- **Code Analysis** – During a software’s lifecycle, continuous improvements to the code will be required. Agile development teams utilize this in today’s environments, but traditional security models are unable to meet the rapid delivery cycles. Agile methodologies help companies deliver updates at a faster rate while also conducting code analysis as part of quality assurance.
- **Automated Testing** - Automation is one of the key principles DevSecOps automated testing simplifies the testing process with a minimum set of tools and scripts. Since this is automated, it can perform the same task every time and completely avoid human error. Doing this at every stage of the process chain saves time and gives a final quality output.
- **Change Management** – Collaboration with the developers in key processes like security makes an effective change management process. Making them aware of related tools and providing expertise in addressing critical issues ensures timely remediation and attention to potential threats and vulnerabilities.
- **Compliance Monitoring** - Compliance continues to be major for any company especially when it comes to cloud adoption. Having the required regulations established is equally important during new code creation or modifying the existing code. Providing evidence and sharing the results with the team keep you prepared for audits and reports. Ensuring the team has the right compliance process in place reduces the stress at the time of formal audit and keeping up the transparency for the company.

- **Threat Investigation** – Ensuring the company has regular monitoring of cloud security, minus the tools and procedures in place. Continuous discovery, threat investigation, regular security scans, and code reviews are key to the identification of any possible vulnerabilities.
- **Personnel Training** – Training personnel internally is also important for any company. This can be provided by introducing certification courses and hands-on training on specific topics or interests. When the team is more knowledgeable this will inadvertently allow the company to be more successful.

### *B. FedRAMP Compliance*

The US government adopted a “cloud-first” initiative to ease agency data frustrations and compliance it established the Federal Risk and Authorization Management Program (FedRAMP). Many companies assume that FedRAMP applies only to those companies seeking to work with federal agencies, FedRAMP compliance can benefit the private sector as well. Cloud computing services are utilized for managing, analyzing, and storing data and these services remain a primary target for malicious hackers. Ensuring your CSP is FedRAMP compliant can ensure the likely hood of not being vulnerable to a malicious attacker on the companies cloud network. There are three key problems FedRAMP solves [10]:

- Focuses specifically on security elements unique to CSPs
- Security controls go beyond the NIST baseline requirements
- Requires a third-party assessment organization to certify the security controls

Companies that apply the FedRAMP framework to their evaluation of cloud services and products can achieve the following benefits:

- Significant cost and time savings compared to carrying out independent assessments, many of which can often be redundant
- Uniform evaluation and authorization of cloud information security controls
- Enhanced insights into cloud security controls
- Confidence in the validity of assessments and the reduction of cloud security concerns
- A faster cloud adoption roadmap

In Figure 10, is the approval and authorization process for an organization to become FedRAMP complaint [10]:

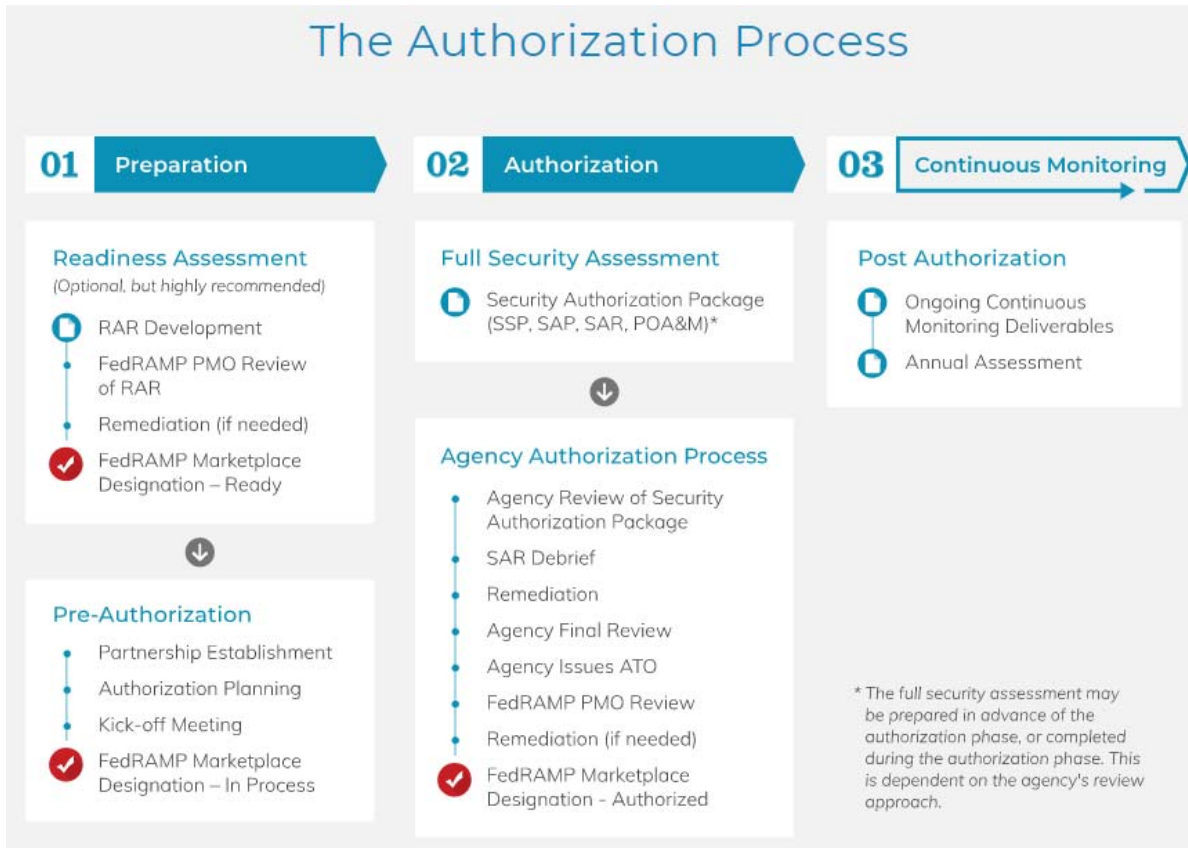


Figure 10: FedRAMP Authorization Process.

### C. Customized Service Level Agreements

When a company considers moving to the cloud the foundation of the agreement between the CSP and the client is the Service Level Agreement (SLA). An SLA outlines what the provider and customer are responsible for in regard to using the service. The contract allows the company to know upfront what specifically the cloud provider implements and manages. It also gives the client knowledge of what they will contribute to continue using the service [11]. It is recommended to include the following before signing an SLA with a CSP:

- **Availability** – The SLA should cover and include the CSPs promised availability and some might break down this depending on a specific time frame (i.e., 99.9% during business hours). The terms should also include the policy and procedures for unexpected downtime, which includes alerting users while providing status updates on service repairs and maintenance.
- **Data Ownership** – The SLA should specifically outline its data ownership policies so that everything is transparent and clear, and this should also include that all ownership rights of data belong to the client.
- **Cloud Hardware and Software** – The CSP should outline the hardware that the cloud services rely on including servers, data centers, and other applicable devices. Depending on the organization, include geographical limitations of where the company’s data can be stored (i.e., only on US servers)

- **Disaster Recovery and Backup** – In the event of a disaster, the CSP should have plans and procedures in place to prevent the loss of the client’s data. The SLA should have a section that describes the disaster recovery and backup solutions in detail. Depending on the client the SLA can also include the CSP to provide automatic backups and snapshots of the company’s data.
- **Customer Responsibilities** – Ensure the SLA outlines responsibilities that both the CSP and client agree on. The SLA has to include what the company and the CSP are liable for in regard to data loss or cyber-related incidents.

#### *D. Implement a Small In-House Cloud Department*

It is recommended for any company moving to a cloud infrastructure to assign individuals or a small department with the sole responsibility of the companies cloud management. This would include the following duties and more:

- Responsible for cloud budgets and forecast reporting to management
- Responsible for working directly with the CSP for issues, maintenance, or service
- Responsible for continued FedRAMP compliance and audits
- Responsible for 24/7 security monitoring of the companies cloud networks

#### *E. Conclusion*

In conclusion, this report has discussed the challenges cybersecurity architects face in a cloud computing environment. It provided qualitative and quantitative data that consisted of one-on-one interviews and a comprehensive survey among 427 cybersecurity professionals. It also included the unique take on ROI and the recommendations to some of the challenges faced. Although this report didn’t cover every challenge in the cloud computing realm, it does address some of the major ones that are affecting cloud computing infrastructures around the world.

#### REFERENCES

- [1] EveryCRSReport.com, "Cloud computing: background, status of adoption by federal agencies, and congressional action," 2020, March, 25. [Online]. Available: <https://www.everycrsreport.com/reports/R46119.html>
- [2] "What is cloud computing? A beginner's guide: Microsoft Azure," What Is Cloud Computing? A Beginner's Guide | Microsoft Azure. [Online]. Available: <https://azure.microsoft.com/en-us/overview/what-is-cloud-computing/>
- [3] S. Gadia, "How to manage five key cloud computing risks," KPMG, 2018. [Online]. Available: <https://assets.kpmg/content/dam/kpmg/ca/pdf/2018/03/cloud-computing-risks-canada.pdf>
- [4] "Cloud security assessment: Qualys, Inc.," Qualys, 2019. [Online]. Available: <https://www.qualys.com/apps/cloud-security-assessment/>
- [5] F. E. Mandiant, "Cloud architecture and security assessment." FireEye, Inc., Milpitas, CA, 2019.
- [6] L. Irwin, "An introduction to the NIST risk management framework," IT Governance USA Blog, 2020, July, 7. [Online]. Available: <https://www.itgovernanceusa.com/blog/an-introduction-to-the-nist-risk-management-framework>
- [7] O. Frank, "Plan of action and milestones," HackingTheUniverse, 2008, December, 16. [Online]. Available: <http://www.hackingtheuniverse.com/infosec/nist-computer-security/security-plans/poams>
- [8] C. R. Hernandez, "Evaluating the ROI of cloud migration." Amdocs Global Services, December, 2020.
- [9] "DevSecOps solution to cloud security challenge," Veritis Group Inc, 2020, October, 8. [Online]. Available: <https://www.veritis.com/blog/devsecops-solution-to-cloud-security-challenge/>
- [10] K. Walsh, "Checklist for FedRAMP requirements," Reciprocity, 2020, August, 29. [Online]. Available: <https://reciprocitylabs.com/checklist-for-fedramp-requirements/>
- [11] D. Hein, "5 Things to look for in a cloud service level agreement," Best Enterprise Cloud Strategy Tools, Vendors, Managed Service Providers, MSP and Solutions, 2019, April, 9. [Online]. Available: <https://solutionsreview.com/cloud-platforms/5-things-to-look-for-in-a-cloud-service-level-agreement/>

# A Proposed Security Algorithm for Securing IoT Data

**Rana Wafeek Mansy**

Department of Information Systems, Faculty of Computers and Artificial Intelligence, Helwan University, Cairo, Egypt.

[rana.manse@fci.helwan.edu.eg](mailto:rana.manse@fci.helwan.edu.eg)

**Mohamed Helmy Megahed**

Department of Communications, Arab Academy for Science and Technology and Maritime Transport (AASTMT), College of Computing & Information Technology, Cairo, Egypt.

[De.mohameed.helmy@gmail.com](mailto:De.mohameed.helmy@gmail.com)

**Marwa Salah**

Department of Information Systems, Faculty of Informatics and Computer Science, British University in Egypt, Cairo, Egypt.

Department of Information Systems, Faculty of Computers and Artificial Intelligence, Helwan University, Cairo, Egypt.

[marwa.salah@bue.edu.eg](mailto:marwa.salah@bue.edu.eg)

**Mahmoud M. El-khouly**

Department of Information Systems, Faculty of Computers and Artificial Intelligence, Helwan University, Cairo, Egypt.

[elkhouly@fci.helwan.edu.eg](mailto:elkhouly@fci.helwan.edu.eg)

**Abstract**—Recently, the Internet-of-Things (IoT) provides new challenges to security and privacy. Security of IoT systems is considered a milestone. It is used in many appliances such as healthcare, e-voting, and industrial applications. Cryptography and steganography are applied to prevent attackers from reading secret data, where steganography is found to be best suited for applications that prevent attackers from knowing someone is sending secret data. Sending encrypted messages over the IoT channels reveals the existence of a sensitive data. When sensitive data is sent, the attackers can apply Denial-of-Service (DoS) attack. By using steganography on the same IoT channel, it will protect this data from DoS attack. This paper aims to propose a new steganography algorithm. This algorithm consists of four main steps: compression, encryption, splitting and hiding. After the first two steps, we split the data into 3 bytes and then hide these 3 bytes by choosing words with a number of characters same as the 3 bytes and then hide them using an automated dictionary that is shared between sender and receiver. The proposed algorithm is tested for different security attacks which it passed effectively. In addition, we had conducted a comparative study to briefly survey the new features which are added to the algorithm compared to other algorithms. The proposed algorithm was built in an IoT application. It took 10ms for coding and 13ms for decoding at the cloud, message size is 265 bits. Then, the experiment was used to evaluate the performance of the proposed algorithm.

**Keywords** — *Steganography, Cryptography, IoT, AES, IoT application.*

## I. INTRODUCTION

IoT is a collection of a set of several interconnected services, objects, people and devices that are able to communicate, exchange information and data to fulfill a common goal in several applications and areas. IoT has many fields of implementation such as the agriculture, transportation, production, health and distribution of energy [1].

Data protection and privacy is one of the main IoT challenges [2]. The lack of safety measures would lead to decreased adoption by users and is thus one of the motivating

forces for the success of the IoT. IoT technologies provide many benefits in the smart cities, smart transportation, smart homes and infrastructure etc... [3,4]. However, the successful development and use of IoT-based services requires security and privacy. IoT security has always remained a critical point of concern, since the very dawn of IoT, there by positioning the in security of IoT among the top security threats in 2019 [5]. Thus such security concerns need to be dealt with priority to exploit IoT benefits for global development worldwide.

Cryptography is another word for encryption [6]. Encryption is the process of encoding that hackers cannot read, but may obtain authorizations. Advanced Encryption Standard (AES) is one algorithm that is used in this work [7] and a new proposed steganography algorithm is the core. AES is a symmetric encryption algorithm where both sides use the same key. [8]. AES has a static message block size of 128 bits of text (cipher or plain), and key length 128, 192, or 256 bits. The messages are divided into 128-bit blocks if longer messages are sent. On the other hand, Rivets Shamir Adelman (RSA) is an integral public algorithm used extensively in the corporate and personal communication industries [9]. The benefit of RSA is to provide authentication with customizable key size from 1024 bits to 2048 bits.

The main research is in hiding data through steganography, which means embedding messages within other for the aim of hiding data. It is the art and science of using the digital communication object in such a way that it conceals the existence of secret information [10]. The advantage of steganography is that it can be used without the transmission being detected to transmit classified messages. The generic stenographic embedding and decoding method is clearly described in Figure 1. In this example, a secret message is being embedded inside a cover to produce the stego object [11, 12, 13].

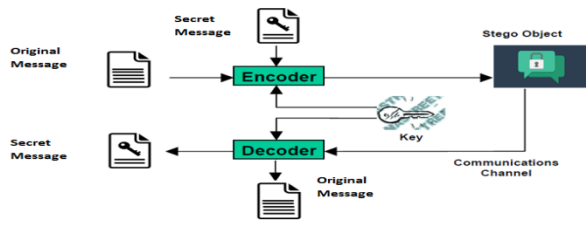


Figure 1 : Generic Process of Encoding and Decoding for Steganography [11]

The first step in embedding and hiding information is the transmission of both the cover message and the secret message into the encoder. One or many protocols are used inside the encoder to embed the secret information in the cover message. The aim of the steganography is not only to prevent others from learning the secret data, but also to eliminate assumption of having concealed information. The message is a secret text which is sent and camouflaged within the carrier to make it more difficult to detect. Second step is the decoding process for the extraction of secret data from a stego object; the stego object is fed into the system. The public or private key to decrypt the original key used within the process of encoding is required to decode the secret information. The secret information embedded within the stego object can be extracted and displayed after the decoding process is completed. Communication mediums/carriers are usually digital files or data, i.e. image, video, text and audio [14, 15, 16]. Various digital mediums use their different features to embed secret data. This paper aims to improve the security in application layer in IoT model (as shown in section 2) based on a new steganography algorithm to get a highly secured IoT application model.

The rest of the paper is organized as follows: Section 2 presents background; section 3 presents the literature review. In section 4, the proposed algorithm is presented, while in Section 5, the performance and security analysis is explained. In section 6, a comparison with others works is demonstrated, and finally, in section 7, we conclude the paper.

## II. BACKGROUND

### A. IoT Architecture

In IoT systems, the functions and the devices are defined in multiple layers. The numbers of IoT layers are varied according to several opinions. However, according to many researchers [17, 18, 19], The IoT consists mainly of three layers called perception, network and application layers. Each IoT layer has associated security issues. IoT's basic architectural has three layer structures for the devices and technologies; the covering of each layer is shown in figure 2.

- Perception Layer

Perception layer, also known as recognition / sensor layer, obtains the environmental attribute by sensor uses. Also it consists of several sensors such as RFID, infra-red, ZigBee and QR code for collecting surrounding data such as humidity, temperature, power, etc. The function of IoT's devices

cooperation in local and short range networks can also be used in this layer [18].

- Network Layer

The purpose of this layer allows data transmission and routing over the Internet to several IoT hub and devices. In this layer, gateways, switches, Internet and routing devices are used to provide various network services by using some modern technology such as 4G, Wi-Fi, ZigBee, and 3G [19].

- Application Layer

This layer gives the end user the services to fulfill his/her needs. The data availability, confidentiality and authenticity are secured by this layer. In this layer, the main function of IoT is to ensure connectivity between machine, people, and things are achieved [18]. Smart Home, smart cities, smart transport, healthcare and utility services are typical IoT applications.

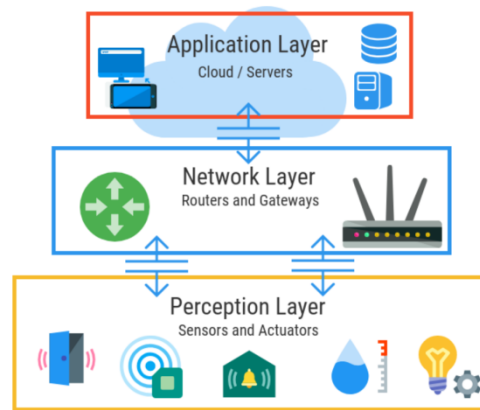


Figure 2 : The three layers of IoT Architecture [17]

Referring to Section 2, this research focuses on the application layer because it's considered as a top layer of conventional IoT architecture. This layer provides the customized based services according to user relevant needs [18]. This layer's main responsibility is to connect the major gap between the users and applications securely.

### B. Security Challenges in IoT Application Layer

The IoT application may be compromised or shut down abruptly as a result of security issues. The malicious attack may be a reason of a virus in the application code which can cause the application to break down. Sometimes applications are unable to provide authenticated services which they are designed to accomplish or even provide inaccurate services. Some main threats for this layer are given as follows:-

- Malevolent code attacks

This kind of attack may be a malicious "worm" that can attack Internet-enabled devices such as home routers security cameras [20]. Moreover, it could get control over steering wheel of autonomous car which results in a serious accident or destroy Wi-Fi of a car.



- Software defenselessness

This type of attack Software vulnerabilities may be increased by non-standard codes written by programmers, the malicious users use this method to obtain their immoral desires

- Phishing attacks

The confidential information can be obtained by attacker via infected email or website by spoofing the participant's verification identity

- Spyware, Worms, and Virus

Attacker may infect the device with malicious software, to steal information, corrupt or denial of service data.

### III. LITRATURE REVIEW

In recent years, several researchers have investigated the issue in IoT security vulnerabilities and their solutions. In this section, some of the most relevant researches will be discussed.

Abd El-Latif, A. et.al. [21], described the quantum steganography algorithm with a consideration of the involvement of the quantum computer, hashing and exclusive OR operation (XOR) operations to secure data in fog cloud IoT Technology. It is because in current data communications, in particular both Cloud technologies and IoT technology, the protection of sensitive data is more important. As a result, the choice of protection schemes for these systems therefore needs more time and effort. Their protocol doesn't use quantum states and networking, but only to transmit confidential data and to validate them. To guarantee that their algorithm is protected, hash functions are implemented. Their results showed that the efficiency and protection were reliable, after subjecting their quantum steganography algorithm to the most well-known attacks.

Shah, A., et.al. [22] Implemented lightweight cryptography algorithms. Lightweight cryptography algorithms are the mostly utilized as a part of IoT innovation for more model security with lower memory and power consumption.

Yi, et.al. [23] Acted on protection standard above 80 bits of the rainbow, and the physical analysis was used for the cryptography of Multivariate Quadratic equations (MQ). The outcome of this work reveals that the hidden keys to the rainbow signature could be successfully hacked, thus securing multi-variant signatures on medical systems is significant.

Jan, M.A., et.al. [24] Presented IoT systems mutual authentication. The framework uses the lightweight features of Constrained Application Protocol (CoAP) as an application layer protocol for client-server communication. The AES cypher provides the secure communication channel. Both the Server and the Client challenge each other for mutual authentication by encrypting a 256 bit payload, and then exchanging check-loads. The authentication is achieved during the encounter of request-response without the use of a further layer Datagram Transport Layer Security (DTLS), which improves the cost of communication and computation.

Kothmayr, T et.al. [25] Proposed a two-way IoT authentication protocol. The authentication is handled using the DTLS protocol by exchanging certificates based on RSA.

Qi, M. et.al. [26] Proposed key management and an authentication scheme based on symmetric cryptography and Elliptic curve. The proposed model has resilience to stolen verifier, replay, password guessing, DoS and impersonation attacks in addition to mutual authentication between the user and the Network Control Center (NCC).

Taha, M. S et.al. [27] In order to ensure sensitive message protection during transmission, a combination of a solid steganography and encryption technology was proposed. This approach suggested that the use of the key encryption technique AES-128 be extended before encoding the hidden message in a QR code. Then, the encrypted message in Unicode Transformation Format (UTF-8) format is transformed to a base 64 format to ensure that it is compliant with further processing. Then, another level of security is added to the process by scrambling the encoded image. Finally, the distorted QR code is hidden in an acceptable carrier that is safely transmitted to provide hidden information. The process used was the least significant bit method to obtain digital image steganography.

Demonstration of a comparison between the researches is explained in table1. The comparison consists of two key features that fulfill their patterns to validate the goals of their IoT protection approaches.

TABLE1. COMPARISON WITH OTHER WORKS

	Used Tools	Security algorithms
Abd El-Latif, A. et.al. [21]	The hash function, (XOR), gray code,	steganography in fog cloud IoT
Shah, A., et.al. [22]	-----	cryptography
Yi, et.al. [23]	Sakura-G, Xilinx ISE software, FPGA board	ECC, RSA Cryptography
Jan, M.A, et.al. [24]	-----	CoAP, AES, DTLS protocol
Kothmayr, T et.al. [25]	-----	AES, DTLS protocol
Qi, M. et.al. [26]	-----	key management, Cryptography
Taha, M. S et.al. [27]	QR code	steganography and encryption technology AES-128

In this work, another security solution is proposed using steganography, which is based on some dictionary structure. The next section shows the details of the proposed algorithm.

### IV. PROPOSED ALGROTHIM

This section describes the hiding algorithm for securing an application layer in IoT environments. The new proposed steganography algorithm which is composed of four steps: (1) compression. (2) Encryption using AES encryption algorithm. (3) Splitting encrypted text into three bits, (4) Hiding the information by choosing word with number of characters according to the 3 bits where an automated dictionary is required between the sender and the receiver.

#### A. Hiding Algorithm for Encoding

The proposed algorithm implements the new steganography algorithm. The hiding process takes the secret text message (SM) and generates a cipher paragraph message. While the



embedded message is extracted during the extraction process. The embedding hiding algorithm can be described by the given pseudocode:

<b>Algorithm 1</b> Embedding hiding Algorithm	
<b>Inputs:</b> secret plain message (SM).	
<b>Output:</b> cipher_new paragraph composed of ordinary paragraph and secret message	
Begin	
Step 1	1. Convert SM to ASCII Code as ASCII-Msg.
	2. Compress ASCII-Msg by using Lempel-Ziv.
Step 2	3. Encrypt compressed ASCII-Msg by using AES-256 as EncMsg.
	4. Convert EncMsg to binary as BinMsg.
	5. Divide BinMsg to 8 bit.
Step 3	6. Loop
	6.1. SHR 1= Shift right the BinMsg 5 bits and convert result to decimal
	6.2. SHR 2 = Shift right BinMsg 2 bits followed by a logical AND operation with binary value of the number seven and convert result to decimal
	6.3. AND 3 = Logical AND operation BinMsg with binary value of the number three and convert result to decimal
	7. End loop
	8. Generate dictionary key array (KD) = adding (SHR 1, SHR 2, AND 3).
	9. Loop
	9.1. If the word length < the element of KD, hide KD element in word by adding several dots at the word's end equals the difference between the word's length and the KD element .
	9.2. If the word length > the element of KD, hide KD element in word by inserting dash after a number of characters equal to the KD element
	9.3. If the word length = the element of KD, hide KD element in word by adding a comma at the end of the word
Step 4	10. End loop
	11. Add semi colons to the end of some unused words in paragraph.
	12. Return cipher_new paragraph composed of ordinary paragraph and secret message.

**Experimental 1 for Embedding hiding Algorithm:**

1. Secret Message: hello world
2. Convert secret message to ASCII code :
  - 2.1 ASCII code of letter (h) is (104)
  - 2.2 ASCII code of letter (e) is (101)
  - 2.3 ASCII code of letter (l) is (108)

And so on until we get the following ASCII code:  
104 101 108 108 111 032 119 111 114 108 100

**3. Encrypt using AES & compressed ASCII-Secret Message:**

Using Lempel-Ziv compression algorithm and AES encryption algorithm method on the ASCII code resulted from previous step gives us the following compressed encrypted message:

61,246,55,40,96,6,120,203,165,37,121,37,186,86,82,131

**4. Convert result to cipher byte array of (8 bit binary) numbers :**

Converting number each of the previous numbers in the compressed encrypted message result in the following (8 bit binary) array:

- a. 61 in (8 bit binary) is 00111101
- b. 246 in (8 bit binary) is 11110110 And soon  
00111101 11110110 00110111 00101000 01100000  
00000110 01111000 11001011 10100101 00100101  
01111001 00100101 10111010 01010110 01010010  
10000011.

**5. For each binary number (8 bit) in the cipher byte array, the three following operations are apply :**

- 5.1 Shift right five bits plus one.
- 5.2 Shift right two bits followed by a logical AND operation with binary value of the number seven plus one
- 5.3 Logical AND operation with binary value of the number three plus one.

TABLE 2:  
CIPHER BYTE ARRAY ENCRYPTION OPERATION

binary number (8 bit)	SHR 1	SHR 2	AND 3
00111101	00000001	00000111	00000001
Result	1+1 = 2	7 + 1 = 8	1+1 = 2

**6. Generate dictionary key array (KD) = adding (SHR 1,SHR 2,AND 3) :**

By adding the results of outputs of previous operations (explained in table 2) from the previous step in an array the resulting array is the dictionary key array which is the shared paragraph between sender and receiver  
2,8,2,8,6,3,2,6,4,2,3,1,4,1,1,1,2,3,4,7,1,7,3,4,6,2,2,2,2,  
2,4,7,2,2,2,2,6,7,3,3,6,3,3,5,3,5,1,4.

**7. Hiding the numbers of dictionary key array (KD) in words from the shared paragraph.**

I wa-nt to watch... th-e match today... then i..... will sta-rt to make my ho-mework but... before i will make, a. cup of. tea t-o make me refresh and ready to study my lessons I... want t-o w-atc h the m-atc h today th-en i wil-l start to make my.. homewor-k but before i w-ill make... a cup, of tea. to make me refresh and ready to study my lesson-s I wa-nt to, watch th-e match to-day then i. will start to make, my..... homework but before i. wi-ll make a. cup of, tea to make me refresh and ready to study my.... lessons I..... wan-t to wat-ch the match. today th-en i will start to. make. my homework but bef-ore i.... will m-ake a cup. of tea to make me refresh and ready to study; my lessons; I; want to; watch the; match today; then i will start; to; make my homework but; before; i will; make a; cup of tea to make me refresh and ready to; study my; lessons; I want; to watch; the match; today then i will; start; to make my homework; but; before i; will make; a cup of tea to make me refresh

and ready; to study; my; lessons I; want to; watch the; match today then i; will; start to make my; homework; but before; i will; make a cup of tea to make me refresh and; ready to; study; my lessons; I want; to watch; the match today then; i; will start to make; my; homework but; before i; will make a cup of tea to make me refresh; and ready; to; study my; lessons I; want to; watch the match today; then; i will start to; make; my homework; but before; i will make a cup of tea to make me; refresh and; ready; to study; my lessons;

**B. Hiding Algorithm for decoding**

Decryption of stego paragraph converts encrypted data to the familiar user format; it is the reverse of encryption process. Throughout the encryption method, the same key (KD) used by the sender must be used over the cipher-text. As shown in following pseudo code, the decryption process is expressed:

<b>Algorithm 2</b> Decryption Algorithm	
<b>Inputs:</b> cipher new paragraph composed of ordinary paragraph and secret message.	
<b>Output:</b> secret plain message (SM).	
Begin	
Step 4	1. Scan the cipher_paragraph word by word using dictionary
	2. Loop
	2.1. If word contains dots, extract the element of KD by counting word character and dots.
	2.2. If word contains dash, extract the element of KD by counting word character after dash.
	2.3. if word contain comma, Extract the element of KD by counting word character
	3. End loop
	4. Append dictionary key array ( KD )
Step 3	5. Convert KD from decimal to binary as BinMsg
	6. Loop
	6.1. SHL 1= Shift left the BinMsg 5 bits.
	6.2. SHL 2 = Shift left BinMsg twice bits.
	6.3. SAME 3 = take BinMsg as it is.
	7. End loop
Step 2	8. Decrypt BinMsg by using AES-256 as DecMsg
Step 1	9. Decompress DecMsg by using Lempel-Ziv as ASCII-Msg
	10. Convert ASCII-Msg by using ASCII Code
	11. Return secret_plain message (SM).
	12. End

**Experimental 2 for Decryption Algorithm:**

**1. Extract the hidden numbers from the shared paragraph where there is one of following three cases:**

- 1.1 If the word length is exactly equal to the number required to be hidden in it, the word will be ended by a comma.
- 1.2 If the word length is less than the number required to be hidden in it, the word will have several dots at its end equals the difference between its length and the hidden number.

1.3 If the word length is more than the number required to be hidden in it, the word will contain a dash after a number of characters equal to the number required to be hidden in the word.

I wa-nt to watch... th-e match today... then i..... will sta-rt to make my ho-mework but... before i will make, a. cup of. tea t-o make me refresh and ready to study my lessons I... want t-o w-atc h the m-atc h today th-en i wil-l start to make my.. homework-k but before i w-ill make... a cup, of tea. to make me refresh and ready to study my lesson-s I wa-nt to, watch th-e match to-day then i. will start to make, my..... homework but before i. wi-ll make a. cup of, tea to make me refresh and ready to study my.... lessons I..... wan-t to wat-ch the match. today th-e-n i will start to. make. my homework but bef-ore i.... will m-ake a cup. of tea to make me refresh and ready to study; my lessons; I; want to; watch the; match today; then i will start; to; make my homework but; .....etc.

**Hidden numbers** = 2,8,2,8,6,3,2,6,4,2,3,1,4,1,1,1,2,3,4,7,1,7,3,4,6,2,2,2,2,4,7,2,2,2,2,6,7,3,3,6,3,3,5,3,5,1,4.

**2. KD = hidden numbers – 1**

By subtracting one from each number of extracted hidden numbers the result is the following key dictionary array:

**Result** = 1,7,1,7,5,2,1,5,3,1,2,0,3,0,0,1,2,3,6,0,6,2,3,1,1,1,1,1,3,6,1,1,1,1,5,6,2,2,5,2,2,4,2,4,0,3.

**3. Convert KD from decimal to binary :**

Convert each of the number in the key dictionary array to its 8-bit binary value to get the following binary array:

- a. 1 in 8-bit binary is (00000001)
- b. 7 in 8-bit binary is (00001111) and so on

00000001	00001111	00000001	00001111	00001010
00000010	00000001	00001010	00000011	00000001
00000010	00000000	00000011	00000000	00000000
00000000	00000001	00000010	00000011	00001110
00000000	00001110	00000010	00000011	00000001
00000001	00000001	00000001	00000001	00000011
00001110	00000001	00000001	00000001	00000001
00001010	00001110	00000010	00000010	00001010
00000010	00000010	00001000	00000010	00001000
00000000	00000011			

**4. For each binary number (8 bit) in the cipher byte array, the three following operations are apply :**

- 4.1 The first (8 bit binary value) is shifted left five bits.
- 4.2 The second (8 bit binary value) is shifted left twice bits
- 4.3 The third (8 bit binary value) take it as it is.

TABLE 3:  
CIPHER BYTE ARRAY DECRYPTION OPERATION

	SHL 1	SHL 2	SAME 3
binary number (8 bit)	00000001	00001111	00000001
Result	00100000	00011100	00000001
OR (SH1+SH2+SMAE3)	00111101		

❖ **The result is cipher byte array of (8 bit binary) numbers :**

00111101 11110110 00110111 00101000 01100000  
00000110 01111000 11001011 10100101 00100101  
01111001 00100101 10111010 01010110 01010010  
10000011.

**5. Convert cipher byte array to decimal :**

By converting each number of the cipher byte array to its decimal value:

- a. 00111101 decimal value is 61
- b. 11110110 decimal value is 246

And so on and collect them in an array to get the following decimal array:

61,246,55,40,96,6,120,203,165,37,121,37,186,86,82,  
131

**6. Decrypt decimal array using AES & decompress to get ASCII code:**

For each value in the resulting decimal array from previous step its decompressed using Lempel-Ziv method and decrypted using AES method the result is the ASCII code of the secret message  
104 101 108 108 111 032 119 111 114 108 100

**7. Convert the ASCII code to secret message:**

Converting each element of the ASCII code array to its corresponding character the result is required secret message as shown below

**Secret Message:** hello world

**V. PERFORMANCE AND SECURITY ANALYSIS**

In the following section we will be discussing performance and security analysis of the proposed algorithm.

*A. Performance Analysis*

The performance analysis is measured according to the followings:

1. Embedded Capacity (EC)

The limitation of the input of steganography process is the output from AES-256 which is 128 bits block length. Therefore, the total size of message plus secret message is 0.5 Kbyte which compressed by 25% to be 125 bytes then encrypted to be 1024 bits then using steganography, each three bits need a word to carry its content.

2. Compression

Lossless compression Lempel-Ziv (LZ) [28,29] technique is used as original data can be recovered exactly from the compressed data after a compress/expand cycle, applied for the purpose of reducing required storage space and for reducing the transmission time associated with transfer data from point to point. The proposed algorithm used Lempel-Ziv Lossless compression algorithm that compress the secret

message from 0.5 Kbyte by 25% to be 125 bytes.

3. Time delay

The proposed algorithm time delay to use all the algorithms at sender side is 10 m/s.

The proposed algorithm time delay at the receiver server is 13 m/s.

*B. Security Analysis*

In this paper, the stego message was embedded in the original cover message. The proposed algorithm has been validated using numerous longitudinal messages and concealed in a shared paragraph. Analyzing the hidden message before and after transmission to the intended receiver reveals that the original cover file has less distortion after secret text is covered.

**VI. COMPARISON AND DISCUSSION**

Researchers have worked on numerous methods and algorithms in different types of steganography. Researchers have highlighted crucial points for the evaluation of their proposed methods.

Abd El-Latif, A. et.al. [21] Depending on XOR grey code with hash function tools that have been developed based on the IoT Fog Cloud model. Authors also suggested a new IoT protection policy for the industry and created a new protected Fog Cloud IoT Quantum Steganography Algorithm.

Yi, et.al. [23] Based on Sakura-G field-programmable gate array (FPGA) board and Xilinx Integrated Synthesis Environment (Xilinx ISE) software tools for a security of MQ cryptographic algorithm. This algorithm has been described using (RSA) and Elliptic-curve cryptography (ECC) algorithms. The relevance applies to the presentation of a Rainbow physical analysis with a level of protection equal to and greater than 80 bits.

Comparing the new proposed algorithm to existing secure data; there are several points of comparison. There is the technical dimension which compares technologies used in each algorithm that includes:

1. Compression reduces the data to 25% of its original size, which is a vital point in transferring data over network on contrary to other two algorithms which do not compress data before securing.
2. Steganography on the other hand is not commonly used in securing data over network which is considered the main added value in the new proposed algorithm and it gives a new layer of hiding sent data where there is no relation between the secret message and the steganography output.

## VII. CONCLUSION

This paper proposes a new algorithm of steganography for secure data in the application layer of the IoT. Through comparison with previous works, the new secure steganography algorithm based on Lempel-Ziv compression, AES cryptography and new steganography algorithm. Performance analysis of the proposed algorithm shows its efficiency while security analysis shows that the attacker is unable to know data in secret message mean while the algorithm is resistant to attacks through encryption and steganography.

## REFERENCES

- [1] G. O. & P. E. Ofori-Dwumfuo, "The design of an electronic voting system," *Research Journal of Information Technology*, vol. 3, pp. 91-98, 2011.
- [2] G. K. V. A. A. & A. K. Misra, "Internet of things (iot)-a technological analysis and survey on vision, concepts, challenges, innovation directions, technologies, and applications (an upcoming or future generation computer communication system technology)," *American Journal of Electrical and Electronic Engineering*, vol. 4, pp. 23-32, 2016.
- [3] I. Y. Sajjad Hussain Shah, "A survey: Internet of Things (IoT) technologies, applications and challenges," *4th IEEE International Conference on Smart Energy Grid Engineering*, pp. 381-385, 2016.
- [4] T. W. J. B. & P. M. Xu, "Security of IoT systems: Design challenges and opportunities," *IEEE/ACM International Conference on Computer-Aided Design (ICCAD)*, pp. 417-423, 2014.
- [5] D. & K. M. Johnson, "IoT: Application Protocols and Security," *International Journal of Computer Network & Information Security*, vol. 4, pp. 1-8, 2019.
- [6] S. F. V. M. & P. L. Mare, "Secret data communication system using Steganography, AES and RSA," *IEEE 17th International Symposium for Design and Technology in Electronic Packaging (SIITME)*, pp. 339-344, 2011.
- [7] A. K. P. C. & T. A. Mandal, "Performance evaluation of cryptographic algorithms: DES and AES," *IEEE Students' Conference on Electrica*, pp. 1-5, 2012.
- [8] D. L. L. & M. V. Hjelme, *A Multidisciplinary Introduction to Information Security, Quantum Cryptography*, 2011.
- [9] R. L. S. A. & A. L. Rivest, "A method for obtaining digital signatures and public-key cryptosystems," *Communications of the ACM*, vol. 1, pp. 96-99, 1983.
- [10] M. T. L. Q. H. J. M. H. D. & Z. J. Ahvanooy, "AITSteg: An innovative text steganography technique for hidden transmission of text message via social media," *IEEE Access*, vol. 6, pp. 65981-65995, 2018.
- [11] S. & D. A. Singh, "Improved hash based approach for secure color image steganography using canny edge detection method," *International Journal of Computer Science and Network Security (IJCSNS)*, vol. 15, pp. 92-98, 2015.
- [12] S. A. I. V. & T. P. L. Patibum, "Text steganography using daily emotions monitoring," *International Journal of Education and Management Engineering*, vol. 3, pp. 1-14, 2017.
- [13] S. K. D. A. & Y. D. K. Mahato, "A modified approach to data hiding in Microsoft Word documents by change-tracking technique," *Journal of King Saud University-Computer and Information Sciences* 32, vol. 2, pp. 216-224., 2020.
- [14] Y. Y. T. & X. G. Liu, "Text steganography in chat based on emoticons and interjections," *Journal of Computational and Theoretical Nanoscience*, vol. 12(9), pp. 2091-2094., 2015.
- [15] A. & D. V. Dhamija, "A novel cryptographic and steganographic approach for secure cloud data migration," *International Conference on Green Computing and Internet of Things (ICGCIoT)*, pp. 346-351, 2015.
- [16] M. M. K. A. S. & M. M. G. Sadek, "Video steganography: a comprehensive review," *Multimedia tools and applications*, vol. 74(17), pp. 7063-7094, 2015.
- [17] R. N. M. Omerah Yousuf, "A survey on the Internet of Things security: State-of-art, architecture, issues and countermeasures," *Information & Computer Security*, vol. 27, no. 2, 2019.
- [18] L. I. A. M. G. & N. M. Atzori, "The social internet of things (siot)-when social networks meet the internet of things: Concept, architecture and network characterization," *Computer networks*, vol. 56, no. 16, pp. 3594-3608, 2012.
- [19] M. B. F. C. M. & N. A. Leo, "A federated architecture approach for Internet of Things security," *In 2014 Euro Med Telco Conference (EMTC)*, pp. 1-5, 2014.
- [20] S. A. V. T. & S. H. Kumar, "Security in internet of things: Challenges, solutions and future directions," *In 2016 49th Hawaii International Conference on System Sciences (HICSS)*, pp. 5772-5781, 2016.
- [21] A. A. A.-E.-A. B. H. M. S. E. S. & G. A. Abd El-Latif, "Secure quantum steganography protocol for fog cloud Internet of Things," *IEEE access*, vol. 6, pp. 10332-10340, 2018.
- [22] A. & E. M. Shah, "A survey of lightweight cryptographic algorithms for iot-based applications," *In Smart Innovations in Communication and Computational Sciences Springer*, pp. 283-293, 2019.
- [23] H. Y. & Z. Nie, "On the security of MQ cryptographic systems for constructing secure Internet of medical things," *Personal and Ubiquitous Computing*, vol. 22, pp. 1075-1081, 2018.
- [24] F. K. M. A. M. U. Mian Ahmad Jana, "payload-based mutual authentication scheme for Internet of Things.," *Future Generation Computer Systems*, 92, , vol. 92, pp. 1028-1039, 2019.
- [25] C. S. ., M. Thomas Kothmay, "DTLS based security and two-way authentication for the Internet of Things," *Ad Hoc Networks*, vol. 11, no. 8, pp. 2710-2723, 2013.
- [26] J. C. Y. C. Mingping Qi, "A secure authentication with key agreement scheme using ECC for satellite communication systems," *International Journal of Satellite Communications and Networking*, vol. 37, no. 3, pp. 234-244, 2019.
- [27] M. S. M. R. S. a. I. Mustafa Sabah Taha, "Combination of steganography and cryptography: A short survey.," *In IOP conference series: materials science and engineering*, vol. 518, p. 052003, 2019.
- [28] P. E. A. Fouzia I Khandwani, "A Survey of Lossless Image Compression Techniques," *International Journal of Electrical Electronics & Computer Science Engineering*, vol. 5, no. 1, pp. 39-42, 2018.
- [29] J. A. ., D. C. Tanvi Patel, "Survey of Text Compression Algorithms," *International Journal of Engineering Research & Technology (IJERT)*, vol. 4, no. 3, pp. 974-977, 2015.

## BIOGRAPHY



**Rana Wafeek Moustafa Mansy** is a Teacher Assistant at Canadian International College in Cairo. She Received her Bachelor Degree from Faculty of Business Information Systems - Helwan University in 2014. She Studied Business Information Technology diploma in faculty of computer science - Helwan University in 2015. She finished Pre-Master in information Systems in faculty of computer science - Helwan University in 2017. She is working on her Master thesis in Internet of Things (IOT).

Email: [rana.manse@ci.helwan.edu.eg](mailto:rana.manse@ci.helwan.edu.eg)



**Marwa Salah Farhan** holds a Ph.D. in Information Systems. She is an associate professor, information systems department, Faculty of Informatics and Computer science, British university in Egypt, Egypt. Her research interests focus on Big data and data analytics, Advanced Database Management and software engineering.

Email: [marwa.salah@bue.edu.eg](mailto:marwa.salah@bue.edu.eg)



**Mohamed Helmy Megahed** received his B.Sc. in July 1997 from Egyptian Military Technical College, Communications Department. Dr. Megahed received his master's in May 2003 from Egyptian Military Technical College in the field of security and cryptography.

Dr. Megahed received his PhD from university of Ottawa in 2014. He invented the unpredictability concept in cryptography to design computationally secure cipher systems and unconditionally secure

cipher systems. He was a doctor in Communications Department in the Egyptian Military Technical College then he worked at Canadian International College (CIC) in Cairo. Currently, he is working part time at Arab Academy for Science and Technology and Maritime Transport AASTMT. His works is focusing on security of communication systems and networks such as 5G network, cryptography, cyber security, block chain, networks, IoT and embedded systems.

Dr. Megahed recent works was IEEE paper providing the architecture of Authenticated Encryption One Time Pad Algorithm. Also, Dr. Megahed designed Customized Elliptic Curve Cryptography resistant to Quantum Computer. Moreover, Dr. Megahed designed cooperative network for Vehicle to Vehicle communications V2V and cooperative network for swarm of drones.

E-mail: [De.mohameed.helmy@gmail.com](mailto:De.mohameed.helmy@gmail.com)



**Mahmoud M. EL-KHOULY** is associated professor at Helwan University, Egypt. He received his BSc degree from Helwan University in (1983), his first Master Degree from the same University, Egypt (1994), his second Master Degree from Cairo University in computer sciences Egypt (1995), and his Doctorate of Philosophy from Saitama University in computer sciences, Japan (2000). He held different academic positions: Lecturer at Temple University Japan (TUJ) (2001), culture attaché' at Egyptian embassy in London/UK (2005-2008), head of management information system project, Helwan University, Egypt (2009), and vice dean for education and students affairs, faculty of Computers & Information, Helwan university, Egypt (2012-2013). Dr. El-Khouly has participated with more than 70 research papers in conferences and journals. He is acting now as a head of Information Technology Department, Faculty of Computer and Information, Helwan University, Egypt. His research interests are Software Agent, e-learning, Information Retrieval, and Network security, Cloud computing.

URL: <http://www.elkhouly.net>

E-mail: [elkhouly@ci.helwan.edu.eg](mailto:elkhouly@ci.helwan.edu.eg)



# A NEW APPROACH SOLVING FOR HYBRID CONSTRAINT SATISFACTION PROBLEMS

Van Lam Ho<sup>1</sup>, K.Robert Lai<sup>2</sup>, Duong Hoang Huyen<sup>1</sup>

<sup>1</sup>Department of Information Technology, Quy Nhon University, Vietnam  
[hovanlam@qnu.edu.vn](mailto:hovanlam@qnu.edu.vn), [duonghoanghuyen1@qnu.edu.vn](mailto:duonghoanghuyen1@qnu.edu.vn)

<sup>2</sup>Department of Computer Science and Engineering, Yuanze University, Taiwan  
[krlai@cs.yzu.edu.tw](mailto:krlai@cs.yzu.edu.tw)

## ABSTRACT

*In this paper we introduce a new approximate method to solve the Hybrid constraint satisfaction problems (HCSPs), named Hybrid Landmark-based Approximate Inference. HCSPs cannot be deal with computing algebraic systems, since there is not any particular algorithm for common hybrid constraint systems. In addition, splitting and searching techniques for global consistency may incur a huge cost and remain highly complex. Our proposed approach improves the performance and sound results for HCSPs. The main idea of this approach is to generate candidates of landmarks to be utilized during the pruning process to facilitate a quiescent condition of variables in hybrid constraint. The method has been shown to reach not only a local consistency but also a global consistency for complex HCSPs. Besides, it holders complicated problems with a low cost and captures the solutions for various types of hybrid constraints.*

## KEYWORDS

*Approximate reasoning, hybrid constraint satisfaction problems, consistency solutions, global consistency.*

## 1. INTRODUCTION

A Hybrid constraint satisfaction problem (HCSP) is a set of objects, each with an associated domain of possible continuous or discrete values, and set of constraints on these objects [2], [5], [7]. We can transform a real world problem to a HCSP and various frameworks for hybrid constraint systems have been proposed for different purposes in engineering and science such as modeling systems have discrete and continuous changes over time [10], [11], embedded controllers for automobiles [10], simulation industrial mixer system [5]. The real-world application problems are represented by hybrid constraint satisfaction problems such as in [1], [2], [5], [7].

There also are limitations in former algorithms solving for HCSPs such as the time-running increases when we try to find more accurate solutions [2] or focus only on solving local consistency problems for specific types of constraint [5] while the real-world systems are extremely complex systems. The previous methods have not represented clearly the techniques to solve for global consistency solutions of HCSP in possible period running time. Some algorithms have been introduced to solve for HCSPs: Esther Gelle and Boi Faltings [5] solved HCSPs by integrating numeric variables with discrete ones in a single search process. In the algorithm, continuous constraint satisfaction problems are solved using interval methods which create a tree of intervals through bisection, and then intervals are pruned using interval analysis. On the other hand, discrete constraint satisfaction problems are solved by enumerating combinations of variable values. The method only solves for several types of hybrid constraints and returns local consistency solution. Daiske Ishii [2] proposed an interval method for solving of HCSP. The algorithm coordinated interval-based solving of nonlinear ODEs (ordinary differential equations) and a constraint programming technique for reducing interval enclosures of solutions. The method guarantees the existence and uniqueness of a solution in a domain and helps to find the earliest solution reliably. However, the method does not point out global consistency solution and the time for process.

In this paper, we present new algorithms hybrid approximate approach, namely hybrid landmark-based approximate inference to solve for HCSPs. The method uses landmark-based values in constraint propagations to find out not only local consistency but also global consistency solutions of hybrid constraint systems. One approximate mathematical tool is employed to find landmarks propagation for local consistency, and then partitions are found based on the landmarks for global consistency. The key ideas of the method are point and partition landmarks in local and global constraint propagations. The point and partition landmarks which are infeasible will be deleted from the domain of variables and save only feasible values in each iteration of the finding solution process. By generating candidates of landmarks to be utilized during process to facilitate a

quiescent condition, the proposed approach improves the running time and obtains sound results with a low complexity.

The rest of this paper is organized as follows: Section 2 represents some definitions about HCSP. Section 3 gives a framework and properties of our algorithm to find local consistency for hybrid constraint systems. Section 4 discusses how global consistencies for HCSPs get using Hybrid-LAI. The complexity of our algorithm is proved in Section 5. In Section 6 will represent some experimental results after using our method for HCSPs and followed by conclusion in Section 7.

## 2. PRELIMINARIES

Hybrid Constraint Satisfaction Problem is a network of hybrid constraints which expresses relations among objects by hybrid constraints. HCSP is a decision problem to determine whether there exists a tuple value of all objects which satisfies all hybrid constraints of network. Real world applications of constraint satisfaction problems involve objects with either discrete or continuous domains in the system.

**Definition 1** A discrete constraint  $\Gamma(X_1, X_2, \dots, X_k)$  defines constraint relations among discrete variables  $X_1, \dots, X_k$  in  $\Gamma$  that a set of allowed value tuples  $(x_{1,j}, \dots, x_{k,j})$  such that  $(x_{1,j}, \dots, x_{k,j}) \in D_1, \dots, D_k$ , where  $x_{i,j}$  is a value of variable  $X_i$ ,  $X_1, \dots, X_k$  is set of discrete variables have value domains in set of discrete values  $D_1, \dots, D_k$ .

This means that domains of variables in constraint system are discrete and finite values. A tuple onto the variables  $X_1, \dots, X_k$  will be written  $t[X_1, \dots, X_k]$  in which the value of  $X_i$  is designated by  $t[X_i]$ .

In a continuous constraint satisfaction problem, the variable domains are defined over the real numbers or intervals with format  $[\alpha, \beta]$ , where  $\alpha, \beta$  are real numbers,  $\alpha \leq \beta$ . A continuous constraint is any relation over the real domain or interval domain. In this paper we use interval domain to represent for continuous domain in the constraints.

**Definition 2** A continuous constraint  $\Phi(X_1, \dots, X_m)$  is a relation  $E \triangleright 0$ , where  $\triangleright \in \{=, \leq, \geq, >, <\}$  and  $E$  is an expression built from constraints, variables, and unary or binary operations  $\{+, -, *, /, \exp, \text{sqrt}, \dots\}$  over the real numbers or intervals,  $X_1, \dots, X_m$  is set of continuous variables have value domains in set of continuous values  $D_1, \dots, D_m$  and the variables  $X_i, i=1, \dots, m$  have constraint relations in  $\Phi$ .

**Definition 3** A hybrid constraint  $\Omega(X_1, \dots, X_n)$  is a relation defined over the discrete and the continuous variables in set of variables  $X_1, \dots, X_n$  of constraint  $\Omega$  with the each object  $X_i, i=1, \dots, n$  in constraint  $\Omega$  will have discrete domain or continuous domain.

For example the hybrid constraint in Industrial mixer system [5]:

$$\left\{ \begin{array}{l} V = \text{hemispherical} \\ V.\text{volume} = \frac{1}{12} * \pi * V.\text{diameter}^3 + \\ \frac{1}{14} * \pi * V.\text{diameter}^2 * (V.\text{height} - \frac{1}{2} * V.\text{diameter}) \\ V = \text{cylindrical} \\ V.\text{volume} = \frac{1}{14} * \pi * V.\text{diameter}^2 * V.\text{height} \end{array} \right.$$

$$V = \{\text{cylindrical}; \text{elliptical}; \text{hemispherical}\}$$

$$V.\text{volume} = [0.01, 1000]$$

$$V.\text{diameter} = [0.01, 1000]$$

$$V.\text{height} = [0, 1000]$$

**Definition 4** A hybrid constraint satisfaction problem (HCSP) is a triple  $(D, X, C)$ , where  $D$  is a set of discrete or continuous domains  $D_1, \dots, D_n$ ,  $X$  is a sequence of variables  $X_1, \dots, X_n$  and  $C$  is a set of  $m$  constraints in which can contain discrete constraints  $\Gamma$ , continuous constraints  $\Phi$  or hybrid constraints  $\Omega$ . A domain may be discrete domain or an interval and constraints are given as equalities or inequalities or conditional constraints or mixer constraints. The solution of a hybrid constraint network is:

$\Pi_{D,X,C} = \left\{ (x_1, x_2, \dots, x_n) \in X_1 \times X_2 \times \dots \times X_n : \bigwedge_{j=1}^m C_j(x_1, x_2, \dots, x_n) \right\}$  Here, the solution of a hybrid constraint network is a set of  $n$ -tuples, each tuple giving, for the  $n$  objects in  $X$ , a valuation which is acceptable to all the constraints in  $C$ . A hybrid constraint network is satisfiable if the network solution is not the empty set  $\Pi_{D,X,C} \neq \emptyset$ .

To solve for hybrid constraints in HCSPs, we need algorithms which combine good performance, obtainable correct results methods for continuous CSPs and discrete CSPs.

### 3. LOCAL CONSISTENCY PROBLEM

Local consistency is an important property in HCSP. In [3] considered propagate-algorithm computing local consistency (2-consistency), or in [5] integrated the local consistency methods for discrete and continuous constraints into a fix-point algorithm and it is achieved by specifying refine operators for each constraint type. In this section, we represent an algorithm which can solve local consistent for HCSP. The algorithm called HybridLocalLAI is built based on landmark.

The idea use Landmark-based Approximate Inference (LAI) method to solve for hybrid constraint satisfaction problems is proposed in this research. By the approach, we use approximate methods in mathematics to find landmarks for local consistent propagation and landmark partitions for global consistent propagation of HCSPs. The landmarks of each variable are obtained from constraint propagation helped the method solves not only local consistency but also global consistency solutions for HCSPs. The key of method is landmarks in domains of variables. Landmark is defined as follow:

**Definition 5** (Landmarks) For a feasible domain of variable  $X$ , there exists interval  $I_A$  and  $I_B$ . Suppose  $I_B$  would be involved continuous solution, and  $I_A$  enclose with  $I_B$ . Any points  $p$  are in the interval  $I_B$ , which are fallen within interval space  $p \in [B^L, \dots, B^U]$ . If the following conditions are hold, the boundaries of interval  $I_B$  are called Landmarks  $\{LM_n, LM_{n+1}\}$ :  $S$  is a solution of variable  $X$ ,  $S \notin I_A \setminus I_B$ , where  $I_A \setminus I_B = \{x | (x \in I_A) \wedge (x \notin I_B)\}$ .  $I_B = \{LM_n, LM_{n+1}\}$ , then  $\{LM_n, LM_{n+1}\}$  are called landmarks.

In our method, the landmarks are found by using approximate mathematical tool, Newton's method, is integrated into the filtering algorithm for finding set of tolerating landmarks. During the refinement process, landmarks are local maximum, minimum and intersection points of constraints which are treated as finding solutions for  $\frac{\partial f(X_1, \dots, X_n)}{\partial X_i} = 0$  with  $f(X_1, \dots, X_n)$  are functions represent to constraints and  $X_1, \dots, X_n$  are objects in

constraint system. Through a landmark deduction procedure, we obtain a set of values in every variable domain for each constraint. These significant landmark points can be defined as:

**Definition 6** Given a variable  $X$ ,  $D$  is domain of  $X$  ( $D = [L^B, U^B]$ ), the landmark point of  $X$  is a point  $p_i$  such that  $L^B \leq p_i \leq U^B$ , set of points  $p_j : L^B \leq p_j \leq U^B, \forall_j$  called set of landmark points of  $X$ , if  $p_i, p_j (i \neq j)$  are landmark points of  $X$  then  $(p_i < p_j) \vee (p_i > p_j)$ .

Each value in domain of discrete variables is treated as landmark-point in the landmark deduction procedure. We proposal an algorithm called HybridLocalLAI to solve local consistency and obtain set of landmark points in HCSP.



---

```

HybridLocalLAI( $C, X, D$ )
1. for each hybrid constrain
    $C_i$  ( $may$  be  $\Gamma, \Phi$  or  $\Omega$ ) in  $C$  do
2.   for each variable  $X_i$  in  $C_i$  do
3.      $SL_i \leftarrow \phi$ 
4.     if  $(0 \in D_{X_i}) \&\& (X_i \in \Phi)$  then
5.        $SL_i \leftarrow SL_i \cup \{0\}$ 
6.     endif
7.     if  $X_i \in \Phi$  then
8.       while
          $(|x_{i,j+1} - x_{i,j}| > \varepsilon) \&\& (x_{i,j} \text{ located within } D_{X_i})$ 
       do
9.          $x_{i,j+1} = x_{i,j} - C_i / d(X_i)$ 
10.      endwhile
11.     if  $(x_{i,j} \text{ satisfy with } C_i) \&\& (x_{i,j} \notin SL_i)$  then
12.        $SL_i \leftarrow SL_i \cup x_{i,j}$ 
13.     endif
14.   else
15.     if  $(x_{i,j} \text{ satisfy with } C_i) \&\& (x_{i,j} \notin SL_i)$  then
16.        $SL_i \leftarrow SL_i \cup x_{i,j}$ 
17.     endif
18.   endif
19. endfor
20. endfor
21. for each variable  $X_i \in X$  do
22.   return  $D_{X_i}, SL_i$ 
23. endfor
24. end

```

---

Fig.1 Hybrid algorithm for local consistency HCSP.

Local propagation algorithm has computed a concise representation of potential solutions for a given hybrid constraint system and return sets of landmark-based of all variables in HCSP. The algorithm has reduced domains of variables by removing values which are infeasible with the constraints from domains. Therefore, reduced domains are represented by labels. Local propagation algorithm has used Newton's method as the approximate tool for the processing find landmark-based values of continuous variables. Filtering process will drop out landmark-based which are infeasible from domains and remained of domains will satisfy with the constraints in HCSP so output of the algorithm will obtain local consistency solutions.

We describe for the algorithm by a synthetic example about hybrid constraint system which has two hybrid constraints:

$$\begin{cases} \Omega_1 : bx^2 - y + 26(a-d) + 1 \leq 0 \\ \Omega_2 : -ax^2 + c - (y-6)^2 + 15b + 10 \leq 0 \end{cases} \quad (1)$$

In this hybrid system, there are two continuous variables  $x, y$  with initial interval domain  $x = [-5, 5]$ ,  $y = [4, 9]$  and four discrete variables  $a, b, c, d$  with discrete initial domains  $a = \{-15, 3, 70, -8, 19, 100\}$ ,  $b = \{1, -6, 3, -9, 15, 10\}$ ,  $c = \{-1, 800, -7, 1200, 9, 100\}$ ,  $d = \{5, -20, 9, -160, 21, -42\}$ . We have the graph to

represent the hybrid constraint network (1) in Fig. 2. The finding solution process, we obtain landmark points of variables:  $x = [-2.82, -2.13, -0.75, 0.75, 2.13, 2.82]$ ,  $y = [7.79, 9.00]$ ,  $a = \{-15; 3; -8; 19\}$ ,  $b = \{1; -6; 3; -9\}$ ,  $c = \{-1; -7; 9; 100\}$ ,  $d = \{5; 9; 21\}$  and from the landmark-based values of variables in HCSP, the HybridLocalLAI algorithm returns local consistency solution with narrower domains  $x = [-2.82, 2.82]$ ,  $y = [7.79, 9.00]$ ,  $a = \{-15; 3; -8; 19\}$ ,  $b = \{1; -6; 3; -9\}$ ,  $c = \{-1; -7; 9; 100\}$ ,  $d = \{5; 9; 21\}$ . However, the results are local consistency and intermediate results that are used for the method finding global consistency.

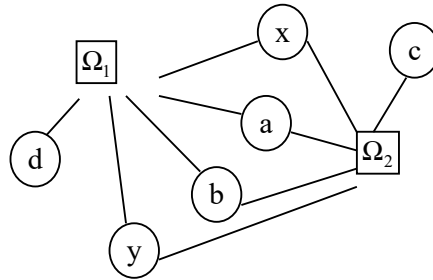


Fig. 2 Graph represents hybrid constraint system (1)

#### 4. GLOBAL CONSISTENCY PROBLEMS

The goal of global consistent of HCSP is to find interval solutions and values of continuous and discrete variables that satisfy all constraints in HCSP. The key idea of the method is to generalize local consistency criterion to a higher level where the set of all hybrid constraints is treated as a single global constraint. To compute the complete solution space of HCSPs, the propagation of all constraints can be represented by a set of landmarks of the feasible space. The set of landmarks are deduced in each domain of each variable of HCSP in during propagation finding local consistent and global consistent. The general framework of the proposed approach is an advanced reasoning algorithm, a consistent checking process that enforce on the local solution with new narrow domains and landmarks points. To isolate the continuous variables' domain by interval partitions in which including landmarks of local solution and consistent checking points as landmarks were yielded from local consistent propagation. Then each landmarks of domain will be checked and refined for global consistency by HybridGlobalLAI. Base on Newton's method, HybridLocalLAI and HybridGlobalLAI find the approximate solution on feasible landmark partitions in efficiency and quickly, it enforced a consistent checking process which is just considered for excluding the inconsistent space.

**Definition 7** Given is a hybrid constraint network  $(D, X, C)$ , where  $D$  is a set of discrete and continuous domains  $D_1, \dots, D_n$ ,  $X$  is a sequence of variables  $X_1, \dots, X_n$  and  $C$  is a set of  $m$  constraints in which can contain discrete constraints  $\Gamma$ , continuous constraints  $\Phi$  and hybrid constraints  $\Omega$ . The network is said to be globally consistent if

$$(\forall x_{i,0} \in C_i(X_i)) (\exists (x_{1,0}, \dots, x_{i,0}, \dots, x_{n,0}) \in C_1 \times \dots \times C_i \times \dots \times C_n) \left[ ((\forall C(x_{1,0}, \dots, x_{n,0})) \in C) (C(x_{1,0}, \dots, x_{n,0}) \text{ is satisfiable}) \right]$$

For any constraint  $C_j$  after using local filtering we get new domain for each variable, in which the domain is viewed as unions of sub-domains divided by consistent points. The sub-domains are used as interval landmarks and landmark points in propagation global consistency. With each landmark of domain will be checked and refined for global search by filtering function of HybridGlobalLAI. In refined iteration, if landmark is not consistent then it will be discarded from domain so the running time of global propagation will be reduced. The global consistency propagation performs as below: With hybrid constraint system  $(D, X, C)$ , the local consistent and landmark-based values of variables will be obtained by HybridLocalLAI algorithm, from the landmark-based values we will have partitions for global consistency process, after that we will assign in turn variables with in turn values in domain of variable  $S_1 = \{X_1 = x_{1,1}, X_2 = x_{2,1}, \dots, X_n = x_{n,1}\}, \dots, S_m = \{X_1 = x_{1,k}, X_2 = x_{2,l}, \dots, X_n = x_{n,m}\}$ .

When we get all tuple  $S_i$  and then the tuples  $S_i$  will be checked with all hybrid constraints in HCSP. The tuple  $S_i$  which satisfies with all constraints will be added into global consistency solution space of the HCSP. The process finding global conThe HybridGlobalLAI can be produced the global solution by the operator  $\Psi^C = \Psi\left(\{p_{1,1}, \dots, p_{2,n}\}, \{p_{j,1}, \dots, p_{k,n}\}\right)$ . Eventually, operator  $\Psi$  is newly applied to  $D$  such that:  $\Psi(D) = \Psi\left(\{p_1, p_1^{h_1}\}, \{p_1^{h_1}, p_2\}, \{p_2, p_2^{h_2}\}, \{p_2^{h_2}, p_j\}, \{p_j, p_j^{h_j}\}, \{p_j^{h_j}, p_k\}\right)$  we obtained consistency solution will be stopped after all the tuples have been checked.

$$\Psi^C = \left\{ p_{1,1}, p_{1,2}, \dots, p_{1,m-1}, p_{1,m}^{h_1}, \{p_{1,1}, p_{1,2}, \dots, p_{2,n-1}, p_{2,n}\}, \right. \\ \left. \{p_{2,1}, \hat{p}_{2,2}, \dots, \hat{p}_{2,m-1}, \hat{p}_{2,m}^{h_2}\}, \{\hat{p}_{2,1}, \hat{p}_{2,2}, \dots, \hat{p}_{j,n-1}, p_{j,n}\}, \right. \\ \left. \dots, \{p_{j,1}, p_{j,2}, \dots, p_{j,m-1}, p_{j,m}^{h_j}\}, \{p_{j,1}, p_{j,2}, \dots, p_{k,n-1}, p_{k,n}\} \right\}$$

where  $p_x$  are assumptive remained which error  $\delta < \epsilon$ , and  $\hat{p}_x$  are assumptive removed points which error  $\delta > \epsilon$  such that:  $\Psi^C = \Psi\left(\{p_{1,1}, \dots, p_{1,m}^{h_1}\}, \{p_{1,1}^{h_1}, \dots, p_{2,2}\}, \{p_{2,1}\}, \{p_{j,n}\}, \{p_{j,1}, \dots, p_{j,m}^{h_j}\}, \{p_{j,1}^{h_j}, \dots, p_{k,n}\}\right)$

Since  $p_{1,m}^{h_1} = p_{1,1}^{h_1}$ ,  $p_{2,n} = p_{2,1}$ ,  $p_{j,n} = p_{j,1}$ , and  $p_{j,m}^{h_j} = p_{j,1}^{h_j}$  which are contiguous to the domain, thus we union these isolated solution  $\{p_{1,1}, \dots, p_{1,m}^{h_1}\}, \{p_{1,1}^{h_1}, \dots, p_{2,2}\}, \{p_{2,1}\}$  and  $\{p_{j,n}\}, \{p_{j,1}, \dots, p_{j,m}^{h_j}\}, \{p_{j,1}^{h_j}, \dots, p_{k,n}\}$ , such that the global solution is obtained by

$$\Psi^C = \Psi\left(\{p_{1,1}, \dots, p_{2,n}\}, \{p_{j,1}, \dots, p_{k,n}\}\right).$$

Return hybrid constraint system (1) example, we see that with approach landmark-based values, we can obtain not only local consistency but also global consistency for the constraint system. If we do not use landmark-based for process finding solution then we will obtain relaxed solution for  $x = [-2.82, 2.82]$  and  $y = [4, 9]$  for constraint system (1). However, among from  $-0.75^+$  to  $0.75^-$  is not satisfied the constraint for a reason of rigorous consistency and so the values of  $x, y$  are not global consistent for constraint system (1). The global solution space can be found by landmark-based values which are used for process finding global consistent solution. The key of method is landmarks in domains of variables which are remained to parts of refined domain by considering all constraints. There are so many points deduced during inference process, however, these points are meaningful and useful for finding solution in whole solving system. The final global consistent solution results are found with values of variables  $x = [-2.82, -0.75] \cup [0.75, 2.82]$  and  $y = [7.79, 9.00]$  which are shown in fig 4. We use HybridGlobalLAI for the constraint system (1) and obtain the results in Table 1.

Table 1 The results of HybridGlobalLAI used for HCSP (1)

Var	Initial Domain	HybridGlobalLAI
$x$	$[-5, 5]$	$[-2.82, -0.75], [0.75, 2.82]$
$y$	$[4, 9]$	$[7.79, 9.00]$
$a$	$\{-15; 3; 70; -8; 19; 100\}$	$\{-15; 3; -8; 19\}$
$b$	$\{1; -6; 3; -9; 15; 10\}$	$\{1; -6; 3; -9\}$
$c$	$\{-1; 800; -7; 1200; 9; 100\}$	$\{-1; -7; 9; 100\}$
$d$	$\{5; -20; 9; -160; 21; -42\}$	$\{5; 9; 21\}$

**HybridGlobalLAI**( $D, X, C$ )

1.  $Q \leftarrow C_1, \dots, C_m$
2.  $T \leftarrow \phi$
3. HybridPropagationLAI( $D, X, C$ )
4. **for** each variable  $X_i \in X$  **do**
  1. **if**  $X_i \in$  continuous variables **then**
  2.  $P_i \leftarrow$  {landmark points in  $SL_i$  divide domain into interval partitions}
  3. **else**
  4.  $P_i \leftarrow SL_i$
  5. **endif**
  6. **endfor**
5. **for** each variable  $X_i \in X$  **do**
  6. **for** each value  $x_{i,j}$  in  $P_i$  **do**
  7.  $S_k \leftarrow \{X_1 = x_{1,j}, \dots, X_n = x_{n,j}\}$
  8. **endfor**
  9.  $T \leftarrow T \cup \{S_k\}$
  10. **endfor**
11. **while** ( $Q \neq \phi$ ) **do**
  12.  $C \leftarrow pop(Q)$
  13. **for** each  $S_i \in S$  **do**
    14. **if**  $S_i$  unsatisfy  $C$  **then**
    15.  $T \leftarrow T \setminus \{S_i\}$
    16.  $Q \leftarrow C_1, \dots, C_m$
    17. **endif**
  18. **endfor**
  19. Delete  $C$  from  $Q$
  20. **endwhile**
  21. **if**  $T = \phi$  **then**
  22. *return* no global consistency
  23. **else**
  24. *return*  $T$
  25. **endif**
  26. **end**

Fig. 3 Hybrid algorithm solve for global consistency

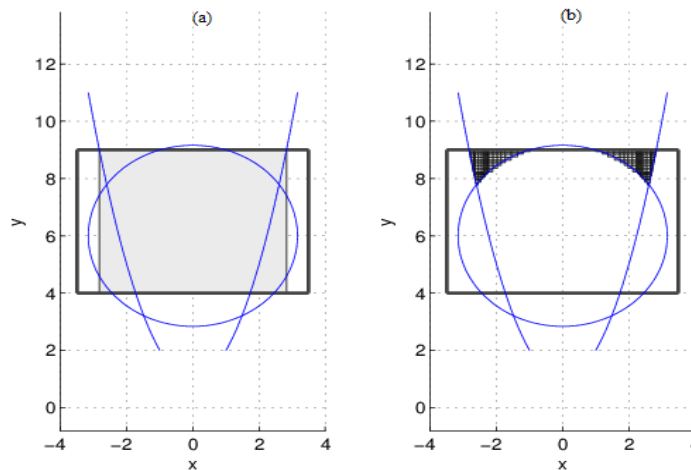


Fig. 4 Local consistency (a) and global consistency (b).

### 5. COMPLEXITY OF HYBRIDGLOBALLAI ALGORITHM

Complexity of our algorithm is estimated by the complexity of process for finding landmark-based values in local consistency propagation and complexity of process finding global consistency solutions. Sets of landmark-based values of variables are obtained by Newton's method and then the landmark-based values do not satisfy with constraints in HCSP will be deleted from domain to get local consistency. Therefore, the time complexity of process finding landmark-based values in local consistency propagation in the worst case is  $O(m * n * \lg(\epsilon) * F(\epsilon))$ , where  $n$  is number of variable,  $m$  is number of hybrid constraint in HCSP,  $F(\epsilon)$  is cost of calculating  $F(\Omega) / F'(\Omega)$  with  $\epsilon$ -digit precision. On other words, the complexity of our method for local consistency is  $O(n)$ . Without taking advantage of landmark-based in constraint propagation, a search procedure would have to consider  $k^n$  assignments for  $n$  variables with  $k$  is number of values in domain and the complexity of search procedure for global consistency in the worst case is  $O(m * n * k^n)$ . However, with landmark-based the running time of process finding global consistency will be reduced because we never have to consider all values in domain. The complexity of our algorithm in the worst case will be

$$O(m * n * \lg(\epsilon) * F(\epsilon) + m * d^n) = O(d^n) \tag{2}$$

where  $d$  is the largest number in number of landmark-based of all variables. From expression (2), we see that the complexity of HybridGlobalLAI algorithm in the worst case is  $O(d^n)$  and lower than the complexity of search procedure without using landmark-based for global consistency of HCSP  $O(k^{n+1})$ . We have  $d$  is the number of landmark-base and  $k$  is number of partitions in domains, by the algorithm then  $d < k$ , and  $m, n, d, k \geq 1$ , therefore, we have that  $O(d^n) < O(k^{n+1})$ . This means that our algorithm is better than search procedures without using landmark-based.

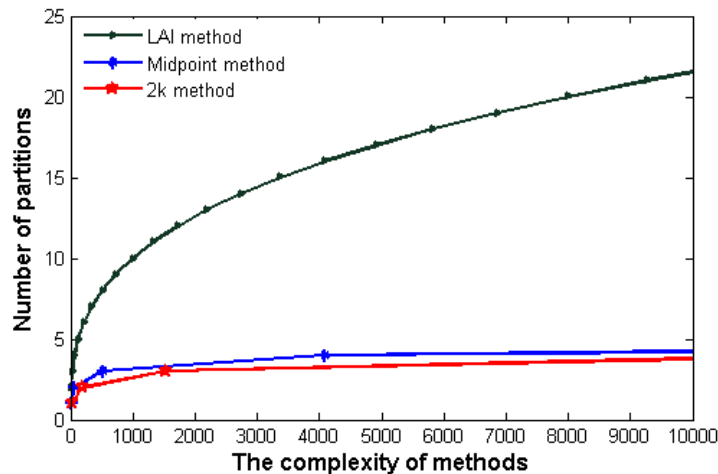


Fig. 5 Represent the complexity of other methods

In the Fig. 5, we have three demonstrations about the complexity of three methods: Landmark-based Approximate Inference which we propose to solve HCSP, Midpoint method which was used in [5] and 2K method used in [4] to solve global consistency solutions. We see that when the number of partitions of other methods increases then the complexity of the methods also increase. However, the increase of LAI method is slower than other methods, indications that LAI method solving for global consistent solution of CSP is better than Midpoint method and 2K method.

### 6. EXPERIMENTATION

Solving for Hybrid constraint systems based on numerical often get wrong results even for simple models such as the bouncing particle [2], we contend that landmark techniques guarantee the existence of a solution provide a

reliable framework for the problems by HybridLocalLAI and HybridGlobalLAI methods. There are several methods which have been proposed to solve for hybrid systems but they have problems with difficulties in numerical computation [6], [8], [10]. The methods output floating-point numbers that seem not to be completely incorrect, but there are some errors. More recently, some methods [2], [4] are proposed to solve HCSP which have different properties from the before methods. However, they also have some restrictions in performance such as only solving for specific type of constraints or only return local consistent of HCSPs. Our method with the landmark techniques has been used for some real work systems and we obtained the results which are not only local consistent but also global consistent. We use the hybrid system in [5] which will be tested by our method and we will show the results for testing the real application system: Industrial Mixer systems [5]. The problem system will be represented by hybrid constraint systems and has been described in [5] consists of configuring mixers used in industry. This system is very complex and described by discrete and continuous objects in constraints. The system can be presented as a hybrid constraint satisfaction problem, in which the relations of components or properties of components are constraints and variables in constraints are the components or properties. In Table 2 shows variables and the domain of variables in the system and the results local, global consistency solutions after we use HybridLocalLAI and HybridGlobalLAI algorithms for the hybrid constraint system. Moreover, the results were compared with Gelle's local consistency method [5]. From the comparison, we show that our method obtains not only local consistency results with interval values narrower than Gelle's method but also global consistency solution for the system.

## 7. CONCLUSIONS

We have introduced an efficient refinement algorithm which allows us to tackle constraint system without losing any solution for HCSPs. HybridGlobalLAI approach performs a global refinement on a constraint system, the principles presented here could be extended to other problems. The approach could play a role of global constraint for handling all equation constraints in many real-world applications where there exist numerous hybrid constraints.

We have compared our approach with corresponding refinement methods, the experiments show that the quality is comparable or even better in some cases; the strength is the low complexity and the ability to balance the workload. The methods have the following important aspects:

- i. Easy to implement: Based on the landmark technique, we can easily obtain the landmark points of continuous variables and discrete variables in HCSP and new narrower domains of variables from HybridLocalLAI procedure. The information will be used in HybridGlobalLAI to obtain global consistent for HCSP.
- ii. Efficiency improvement: The proposed approach tackles complicated problems with a low cost. The algorithm balances the work load and minimizes the number of operation with a low complexity.
- iii. Higher consistency level: The proposed approach can reach not only a local consistency, but also a global consistency for HCSP.
- iv. New efficiency approach to solve for HCSP: Local and global consistency are supported by refine landmark-based operators which are designed for hybrid constraint satisfaction problems. The propagation help to avoid searching all domains of variables, backtracking in order to obtain the complete solutions even the domains contain separate intervals in solution of continuous variables.

With the results of HybridGlobalLAI approach for real-world applications of HCSP, and on standard benchmark from the hybrid constraints. The algorithm has faster running time and returns correct results than other approaches, thus HybridGlobalLAI is more useful when the hybrid constraint system is very complicated with many continuous and discrete domains of the variables. Although the experimental results were obtained in a particular, we believe that HybridGlobalLAI approach can scale up to more complex and realistic problems, real-world applications.

Table 2. Representation local consistency solutions obtained from our method comparison with Gelle’s method.

Variables	Initial Domains	Consistency Gelle’s method	Local consistency our method	Global consistency our method
MT	{blending, entrainment, dispersion}	{blending, entrainment, dispersion}	{dispersion}	{dispersion}
MT.heattransfer	{true, false}	{false}	{false}	{false}
MT.slurrypressure	{low, high}	{low, high}	{low, high}	{high}
MT.slurryviscosity	{low, high}	{low, high}	{low, high}	{low}
MT.slurrydensity	[1, 2000]	[1, 2000]	[1, 2000]	[2, 2000]
M	{reactor, storagetank, mixer}	{storagetank, mixer}	{storagetank, mixer}	{mixer}
E.power	[0, 5000]	[0.2, 5000]	[0.2, 5000]	[0.827, 4999.722]
El.bottomArea	[0.01, 1000]	[0.01, 1000]	[0.01, 1000]	[0.01, 1000]
El.sradius	[0.01, 1000]	[0.01, 1000]	[0.803, 1.00]	[0.804, 1.000]
I.diameter	[0.1, 1000]	[0.4573, 6.9883]	[0.457, 0.658]	[0.529, 0.658]
I.entry	{top, side, center}	{top, side, center}	{top }	{top}
I.position	[0, 5]	[0, 5]	[5.00, 5.00]	[5.00, 5.00]
I.power	[0, 5000]	[0.1, 2500]	[0.2, 2500]	[0.413, 2499.86]
I.ratio	[0, 1]	[0, 1]	[0.329, 0.329]	[0.329, 0.329]
I.rps	[1, 100]	[1, 29.24]	[1, 1.265]	[1.000, 1.266]
V.diameter	[0.01, 1000]	[0.4817, 21.2344]	[1.607, 2.00]	[1.607, 2.00]
V.height	[0,1000]	[0.2408, 42.4688]	[3.215, 4.00]	[3.21, 4.00]
V.volume	[0.01, 1000]	[0.01, 150]	[4.22, 12.56]	[1.754, 2.00]
V	{cylindrical, elliptical, hemispherical}	{cylindrical, elliptical, hemispherical}	{cylindrical, hemispherical}	{ hemispherical}

## REFERENCES

- [1] Chia-Yu Hsua, Bo-Ruei Kao, Van Lam Ho, Lin Li, K. Robert Lai, “An agent-based fuzzy constraint-directed negotiation model for solving supply chain planning and scheduling problems”, *Applied Soft Computing* 48, 703–715, 2016.
- [2] Daisuke Ishii, Kazunori Ueda, Hiroshi Hosobe, Alexandre Goldsztejn, “Interval-based Solving of Hybrid Constraint Systems”, *In Grant-in-aid for Young Scientists, supported by JSPS*, 2010.
- [3] Davis, E, “Constraint Propagation with Interval Labels”, *Artificial Intelligence* 32, pp 281-331, 1987.
- [4] D. Sam-Haround and B. Faltings, “Consistency Techniques for Continuous Constraints”, *Constraints*, 1, 85-118, 1996.
- [5] Esther Gelle, Boi Faltings, “Solving Mixed and Conditional Constraint Satisfaction Problems”, *Constraints* 8, pp 107-141, 2003.
- [6] Hyvönen, E, “Constraint Reasoning Based on Interval Arithmetic: The Tolerance Propagation Approach”, *Artificial Intelligence* 58, pp 71-112, 1992.
- [7] Jean-Paul Watson, J. Christopher Beck, “A Hybrid Constraint Programming/Local Search Approach to The Job-Shop Scheduling Problem”, *CPAIOR 2008, LNCS 5015*, pp.263-277, 2008.
- [8] Larroudé, V., et al., “Constraint Based Approach for The Steady-state Simulation of Complex Systems: Application to Ship Control”, *Engineering Applications of Artificial Intelligence*, 26(1): p. 499-514, 2013.
- [9] Pedomallu, C.S., Kumar, A., Csendes. T. and Prosfai, J., “An Interval Partitioning Algorithm for Constraint Satisfaction Problems”, *Int. J Modelling, Identification and Control*, Vol. 14, Nos. 1/2, pp. 133-140, 2011.
- [10] Pratik J. Parikh and Sara S. Y. Lam, “A Hybrid Strategy to Solve the Forward Kinematics Problem in Parallel Manipulators”, *IEEE Transactions on Robotics*, Vol. 21, No. 1, February 2005.
- [11] J. Lunze and F. Lamnabhi-Lagarrigue, “Handbook of Hybrid Systems Control: Theory, Tools, Applications”, *Cambridge University Press*, 2009.
- [12] Van Lam Ho, K. Robert Lai, “A Fast Filtering Algorithm for Continuous Constraint Satisfaction Problems”, *RIVF 2019 IEEE Xplore*, 2019.



# Designing Service Level Agreements and Information Technology Service Level Management Process Standards based on the ISO 20000 and ITIL V3 2011: Case Study of PT XYZ

<sup>1</sup>Erlangga Al Farozi, <sup>2</sup>Yudho Giri Sucahyo and <sup>3</sup>Muhammad Kasfu Hammi

<sup>1</sup>Master of Information Technology Study Program, Faculty of Computer Science, University of Indonesia, Indonesia

<sup>2</sup>Master of Information Technology Study Program, Faculty of Computer Science, University of Indonesia, Indonesia

<sup>3</sup>Master of Information Technology Study Program, Faculty of Computer Science, University of Indonesia, Indonesia

*E-mail:* <sup>1</sup>[erlangga.al.farozi@gmail.com](mailto:erlangga.al.farozi@gmail.com), <sup>2</sup>[yudhogs@gmail.com](mailto:yudhogs@gmail.com), <sup>3</sup>[kasfu.hammi@gmail.com](mailto:kasfu.hammi@gmail.com)

**Abstract**—The development of technology today is very fast and has changed companies' perspective and strategic plans. The knowledge of information technology has begun to reach the strategic level, but there are still many companies that have not been able to map the development of information technology from its strategic level. PT XYZ is a customer relationship management-based company that provides several services to meet its business needs. Some of these services have problems regarding their service capabilities. Many businesspeople question whether the IT division is able to provide everything needed by the business and whether the IT division in accordance with the agreement, with this problem a service level agreement document will be made that is in line with the business requirements expected by the board of directors of PT XYZ. However, some of these problems have measures that have never been defined before, so they cannot produce something that can be measured and assessed. This study seeks to develop service level agreements that are in accordance with formal standards that are not yet available at PT XYZ using the ISO 20000 standard and the 2011 ITIL V3 framework and develop measures that can be measured and assessed. This service level agreement will contain 19 parts, each of which will be customized based on the characteristics of the service and the company

**Keywords:** *Service Level Agreement; Service Level Management; ISO 20000; ITIL V3 2011*

## I. INTRODUCTION

The development of technology today is very fast and has changed companies' perspective and strategic plans. The knowledge of information technology has begun to reach the strategic level, but there are still many companies that have not been able to map the development of information

technology from its strategic level. PT XYZ is a customer relationship management-based company.

PT XYZ has a vision to become a major CRM company that helps clients achieve their business goals in the continuously changing consumer space by providing data-driven, actionable, and accountable solutions. Problems that arise in PT XYZ focus on service capabilities provided by the IT division are not yet optimal.

Their services problems start from the unclear planning stage of IT development services to the many problems that arise in IT services that has gone live, causing clients' trust to decrease. Based on the initial analysis with the IT Head, the problems to be discussed are problems coming from the organization and management domain, namely the absence of a formal management process and the absence of a service level agreement.

From the problems that arise on the surface, the research question to be solved in this study is what are the contents of the service level agreement that suits the needs of PT XYZ? How are IT service level management standards implemented so that they can meet the needs of PT XYZ? The aim of this research is to make PT XYZ's IT service level agreement in accordance with the results of the implementation of ISO 20000 and ITIL V3 2011 and to make PT XYZ IT service level management standards using ITIL V3 2011 based on the results of using ISO 20000.

## II. LITERATURE REVIEW

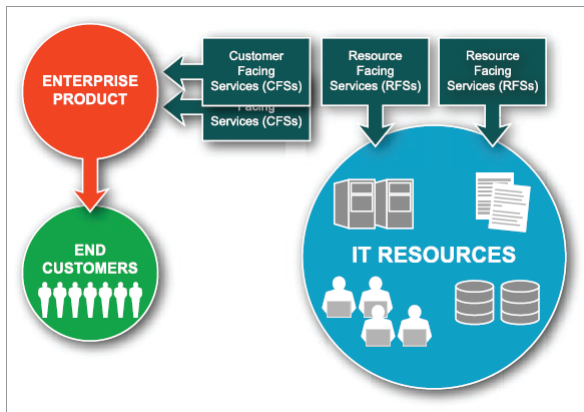
Measuring the quality of IT services is more difficult than measuring the quality of goods. This is because IT services are intangible and unclear (indistinct obstruct). Quality of service is a measure of how a service can provide what customers expect. Service information data is a de facto standard in defining services. Defining IT services is the first step in the process of Service Portfolio Management (SPM), Business Service Management (BSM), Service Level

Management (SLM) and Information Technology Service Management (ITSM). [1]

Service information data defines two types of services, namely services used by customers or Customer Facing Services (CFS) and services that support services used by customers but not visible to customers or Resource Facing Services (RFS). RFS is used to build CFS. Some steps to determine services that are included in CFS, RFS and resources are as follows: [2]

1. Select company products and identify the services that support them.
2. Make a list of IT services that support the product.
3. Mark the CFS or RFS.
4. Map the CFS and RFS.
5. Identify Resources that support RFS.

Figure 1 describes the relationship between CFS, RFS, and resources with the products or services that the company has:



**Figure 1. The Relationship between CFS, RFS, and Resources.**

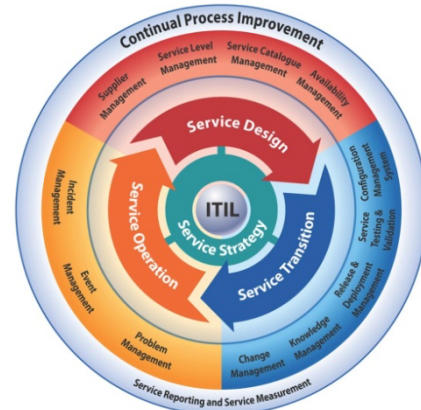
Information Technology Service Management is a set of organizational specific capabilities to deliver value to customers and businesses in the form of IT services. The aim of Information Technology Service Management is to provide the quality and level of service needed by businesses and to continually improve the quality of services provided to customers so that they can reduce costs effectively (Rudd, 2007). One of the main capabilities needed in the service management process is the ability to measure all service quality, effectiveness, and efficiency of the process. [3]

This research will focus on one of the ISO 20000 processes, namely the Service Delivery Process in which there is a Service Level Management (SLM) sub-process. This management aims to establish, agree, record, and manage service levels.

ITIL is a best practice related to Information Technology Service Management. The 2011 ITIL V3 life cycle is based on the service management concept that is tied to service and value. The service life cycle consists of five stages, the initial stage in the service life cycle starts with the initial definition and analysis of the business demand on service strategy and

service design, after that, migrating into an active environment in service transition (Service Transition), up to the active process and improvement in service operations and continuity of service improvement (Continual Service Improvement). [4]

Each stage has a direct impact on service performance. In essence, services are expected to provide structure, stability, and strength for service management capabilities with durable principles, methods, and equipment's. The IT service life cycle according to ITIL V3 2011 is as follows [4]:



**Figure 2. IT Service Life Cycle according to ITIL V3 2011**

Service Level Management in ITIL V3 2011 is conducting negotiation, approval, and documentation activities to ensure the existence of IT service targets with business representatives and then oversee and produce reports on the ability of service providers to provide a level of service in accordance with the agreement. The objectives of the SLM process are as follows [5]:

1. To ensure that the agreed level of IT services for all IT services activities and future IT services are given and agreed targets are achieved.
2. To ensure that all operational services and service performance are measured consistently, professionally throughout the organization, and that the produced services and reports meet the business and customer needs.
3. To establish, document, approve, monitor, measure, report and review the level of available IT services.
4. To provide and improve communication links between business and customers.
5. To ensure that the targets are specific and measurable to be developed on all IT services.
6. To ensure that IT and customers have clear and unambiguous expectations regarding the communicated level of service.
7. To ensure proactive measures to increase the level of service provided have been implemented at any cost structure.

The parts that must be included in the SLA document are service descriptions, service scope, service time, service availability, service reliability, customer support, contactable personnel and escalation, service performance, batch

turnaround times, functions, change management, service continuity, security, printing, responsibility, charging, reporting services and evaluation processes, terms, and amendments sheet. [5]

Amongst the challenges IT faces is determining metrics that must be measured in a part that has been previously defined. Metrics will aim to help calculation in a section so that it can know how much value is obtained in that section, and how it performs. A high value or low will provide a broad view for management so the management can make decisions for the future. According to Randy A. Steinberg, IT metrics have several categories, namely operational, key performance indicators, tolerance, critical success factors, dashboards, and reports. These metrics have the following relationships [6]:

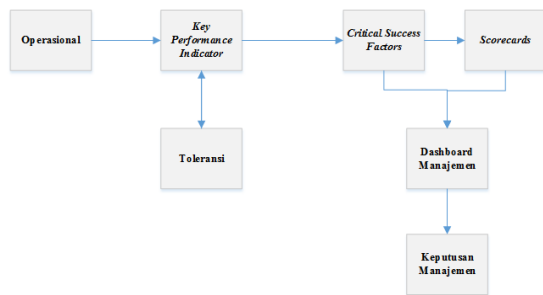


Figure 3. Relationships between metrics

Some of the previous research that took the same theme with this research were as follows:

Tabel 1. Differences between this Research with some Previous Research

Differences	Previous Research			Al Farozi (2013)
	Hammi (2009)	Akmal (2011)	Utama (2013)	
Standard	ISO 20000	ISO 20000, ISO 27001	-	ISO 20000
Framework	ITIL V2	COBIT 4.1	ITIL V3 2011	ITIL V3 2011
Research Object	Educational Institution	PT Bhandha Ghara Reksa	Pusat Grosir Cililitan	PT XYZ
Final Result	Service Management Implementati on Plan	Policy	Service Management Mechanism	Service Level Agreement

Information technology service management has two theories, one ISO 20000 standard and one ITIL V3 2011 framework. In ISO 20000 it has a cycle called PDCA, which is the Deming cycle. In the PDCA Cycle in ISO 20000 there is a Service Level Management process. The Service Level Management process has information technology service management standards regarding Service Level Management. The ITIL V3 2011 framework has a Service Design section in which there is a Service Level Management process.

The ITIL V3 Service Level Management 2011 has sections on service level agreements that can be used for the making of service level agreements. In each part of the service level agreement, there are quantifiable metrics. Each metric has a target and tolerance that has been agreed upon. These metrics have calculations that can be used for the making of service level agreements. The current condition of the company supports the arrangement of service level agreements so that it can be said that the company currently has a service level agreement. The above theoretical framework can be described as follows:

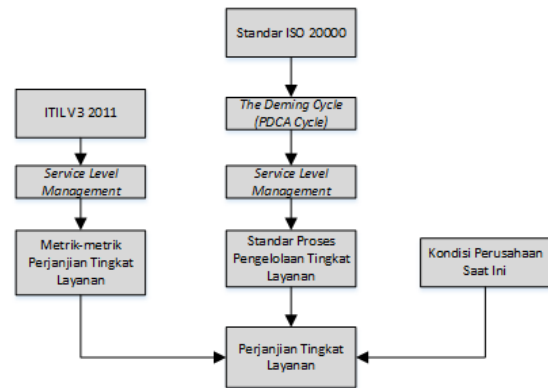


Figure 4. Theoretical Framework

### III. RESEARCH METHODS

The stages in this study and their information can be described as follows:

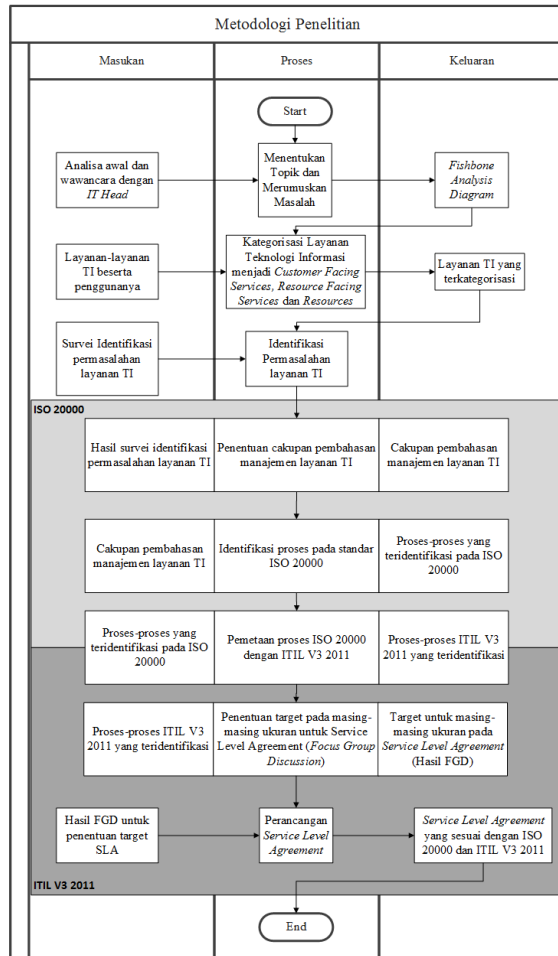


Figure 5. Research Methods

From the picture and explanation of the research methodology, the lighter colored box indicates the use of ISO 20000 in this study, while the darker colored box indicates the use of ITIL V3 2011. The ISO 20000 will be used in several processes, including the following:

1. Method for determining the scope of discussion of IT service management.
2. Processes identification that is in accordance with the problems of IT services at PT XYZ.
3. As a standard that must be used entirely, because PT XYZ does not have a business strategy document.
4. As a basis for mapping Service Level Management processes at ISO 20000 to ITIL V3 2011.

The use of ITIL V3 2011 in this study is as follows:

1. As a result of mapping from ISO 20000, the same process is also called Service Level Management.
2. As a guideline for determining the metrics that will be used in the service level agreement.
3. As a guideline or guide for creating or designing service level agreements.

#### IV. ANALYSIS AND DISCUSSION

The discussion of this research starts with listing the IT services, including Customer Facing Services (CFS) and Resource Facing Services (RFS). The stage for determining these IT services is by selecting company products and identifying services that support them. The product in question is product that is sold to customers or product used by internal users of the company. The next step is to list IT services that support the product.

The meaning of IT services at this stage is people, products, and processes. IT services are not software or hardware that is used, but rather the functionality of these services. IT services at PT XYZ are divided into 35 services which fall into 10 service categories. Service categories are divided based on the type of service, and sub-categories are divided by modules or details of services in the category. All services contained in PT XYZ are provided and managed by the IT division itself.

The next step is to mark Customer Facing Services (CFS) or Resources Facing Services (RFS). IT services in companies falls in the CFS category if customers or service users directly use the service. While IT services are categorized as RFS, if the customer or service user does not directly use the service and is not aware of the service. After identifying services that are included either in CFS and RFS, these services will be mapped with their service categories so that relationships between services in one service category can be seen. Some of the identified and mapped services are as follows:

Table 2. IT Service Identification and Mapping Results

No	IT Services Category	Layanan TI	CFS	RFS	Resources
1	Application Service	ABC Loyalty Program Application Service	X		
2		Timesheet Application Service	X		
3		ABC Database Backup Service			X
4		Timesheet Backup Database Service			X
5		ABC Database Service		X	
6		Timesheet Database Service		X	
7		ABC Application Report Service	X		

Next will be mapped each IT service that has been identified with users who use the service. Users are categorized by divisions at PT XYZ. The selected divisions are divisions that use IT services significantly, some divisions such as Creative and Analytic use tools that are not provided or managed by the IT division. The selected divisions are the

Account Executive division, Human Resource, Finance, Call Center, and IT division. The RACI graph (Responsible, Accountable, Consulted, Informed) is used for mapping IT services and their users. The followings are the mapping results with RACI charts:

**Table 3. List of IT Service Users**

No	IT Service Category	TI Service	IT Service User Division				
			ACC	FIN	HRD	CC	IT
1	Applicatin Service	ABC Loyalty Program Application Service	R			R	R
2		Timesheet Application Service	R	R	I	R	R
3		ABC Database Backup Service					R
4		Timesheet Backup Database Service					R
5		ABC Database Service					R
6		Timesheet Database Service					R
7		ABC Application Report Service	R			I	R

Survey of IT service problems is tailored to the services used by users, so users can know in detail what the problem is with each service. Surveys are carried out using two variables, namely impacts and tendency, where impact is the failure of a service that affects the ongoing business process. The impact here is defined as a failure that has happened for one year, while tendency is described as the frequency of service failure for one year.

Each variable is divided into three categories: High (H), Medium (M), and Low (L). High for impact is given a value of 3, meaning the failure that has ever occurred resulting in the service being down, the application cannot be accessed, or the loss of important data. Medium for impact is given a value of 2, meaning the failure that has ever occurred is significant enough, but does not disturb the availability of existing services. Low for impact is given a value of 1 in the sense that the failure occurs does not have a significant impact on service. As for the tendency of High is given a value of 3 in the sense that the frequency of events is more than 10 times a year (> 10). Medium for tendencies is given a value of 2, which means the frequency of events is between 3 and 10 times a year (3-10). Low for tendencies is given a value of 1, which means the frequency of occurrence is less than 3 times a year (<3). The following are the results of the survey on IT service problems:

**Table 4. Survey Results on IT Service Problems**

No	IT Service	Average		Result	
		D	K	D	K
1	ABC Loyalty Program Application Service	3.00	2.33	H	M
2	Timesheet Application Service	1.00	1.20	L	L
3	ABC Database Backup Service	1.00	1.00	L	L
4	Timesheet Backup Database Service	1.00	1.00	L	L
5	ABC Database Service	3.00	1.00	H	L
6	Timesheet Database Service	1.00	1.00	L	L
7	ABC Application Report Service	2.33	2.00	M	M

Of the 35 identified services, only two service level agreements were chosen to be made, this is because the tendency level is worth 2 or Medium and the service is that is directly used by users (Customer Facing Services). The reason for choosing CFS category services is because the level agreement that will be made is a service level agreement, if RFS is chosen, the level agreement made is an operational level agreement that is more internal and only used within the IT division.

Service level agreements are important because a service level agreement will ensure that the IT services provided are well-provided and measurable with the targets to be achieved. So if an IT service fails or is down, this is merely not a big problem to the management part. Failed services will be measured on how long the service is down and how long it takes to complete the service so that the service is active again based on the agreement to determine the target for each of the prioritized IT service. Services that will be a priority for determining targets are services that have high impact and tendency value based on the results of IT service problem surveys, namely the ABC Loyalty Program application service and Email services.

To determine the service level agreement target for ABC Loyalty Program and Email service application services, a Focus Group Discussion (FGD) is conducted that addresses technical issues related to service time, service availability, service reliability, customer support, and service performance. The specified target has been discussed and will be reported to the board of directors to be an evaluation material that will be applied to PT XYZ in the form of a service level agreement document. Service time is defined in the number of days in one week and one year. Service time must also include maintenance time and total maintenance days in one year. From the results of the discussion, the service time section consists of four metrics, namely the service time itself where

customers can expect services to be available, the total days of service available, the total time to do maintenance, and the total day of maintenance.

The metrics to be measured for the service availability section that has been agreed upon and in accordance with the definition of ITIL V3 2011 are total time between failures; which means the total of time between failures, total time to repair; which is the total time to improve service, down time; which is the number of down hours within one year, the downs number; meaning the down frequencies for one year, the average down time that occurred for one year, and the percentage of service availability.

The metrics on the reliability of services that have been agreed upon and in accordance with ITIL V3 2011 are, mean time between failures, which is the average time between failures that occur within one year, number of transactions on services, time of transactions on services, constants e, results from calculating one divided with MTBF, and service reliability percentage. Calculation of service reliability is adjusted to the circumstances of the company and in accordance with Curtis M. White's theory.

Metrics on customer support for a service that has been agreed upon and in accordance with the definition of ITIL V3 2011 are response times; which is the time needed by the service to respond to requests, time of resolution; which is the time needed from the detection stage to the service has been repaired, the total demand entry, total calls that were not picked-up, total telephone extensions that were always available for services, and percentage of customer support performance.

The metrics on service performance that has been agreed upon and in accordance with the definition of ITIL V3 2011 are total active users, response time needed by services, total users accessing services simultaneously, total transactions in one day, and service performance percentages. The measures defined above function to assess whether the part mentioned is in accordance with the target or not, so that further decisions can be taken to determine the next step. Not all parts defined by ITIL V3 2011 can be targeted, because there are several parts that cannot be measured or already exist based on the current condition of the company.

Based on the ISO 20000 process, it can be adjusted to the Plan-Do-Check-Act method in the service level management (SLM) process. These methods can be used to standardize service level management processes in accordance with ISO 20000. The methods that are in accordance with the FGD results are as follows:

1. *Plan*
  - a) All services provided, including the target level of service and the appropriate load characteristics, must be agreed upon by various parties and there is a record of the agreement. The person responsible for this process is the IT Operation Manager.
2. *Do*
  - a) Each service provided must be determined, agreed upon and documented in one or more

service level agreement agreements (SLAs). The person responsible for this process is the IT Operation Manager.

- b) Service level agreement (SLA), together with service agreement support, supplier contracts, and appropriate procedures, must be agreed upon by all relevant parties and there is a record of the agreement. The person in charge of this process is the IT Project Manager.

3. *Check*

- a) Service level agreements (SLAs) must be under the control of the change management process. The person in charge of this process is the IT Project Manager.
- b) Service level agreements (SLAs) must be maintained by related parties by periodically reviewing those service level agreements. Maintenance of this service level agreement is made to ensure that the service level agreements are always up to date and remain valid from time to time. The person responsible for this process is the IT Operation Manager.

4. *Act*

- a) Service levels must be monitored and reported based on the targets set, by displaying information both current information and current information trends. Corrective actions identified during this process must be recorded and used as input on planning to improve services. The person responsible for this process is the IT Operation Manager.

V. CONCLUSIONS

The conclusions in this study are as follows:

1. The problem that occurs in PT XYZ lies in the absence of service level agreements and the absence of a formal IT service management process.
2. The result of IT service categorization at PT XYZ is they have 35 IT services which are divided into three types of services, namely Customer Facing Services, Resources Facing Services and Resources.
3. IT services are divided into several users who use these services. Five divisions were identified, which plays a significant role in IT services, namely the Account division, the Human Resource division, the Finance division, the Call Center division, and the IT division itself.
4. Survey of problems in IT services is divided into 2 variables, namely Impact; which is defined as the failure of a service that influences ongoing business processes, and Trend; defined as the frequency of service failures.
5. Based on the survey results of IT service problems, there were seven services that have a high value impact (value of 3). Of these seven, two services were selected based on the level of trends that have

occurred. These two services are ABC Loyalty Program services and email services.

6. Problem solving was done using the ISO 20000 standard considering that ISO 20000 has a Service Level Management process and the 2011 ITIL V3 framework to find out what should be done to create a service level agreement.
  7. The result of ISO 20000 and ITIL V3 2011 mapping is one to one. The ISO 20000 process is Service Level Management and the ITIL V3 2011 process is Service Level Management.
  8. The results of discussions with several colleagues at PT XYZ who have roles and responsibilities for service level agreements are targets set for the two selected services.
  9. The metrics determination on service level agreements at PT XYZ is only based on the operational metrics and tolerance theory by Randy A. Steinberg. More studies are expected, focusing more on the overall metric to achieve metrics for management decisions
- [2] Enterprise Management Associates, 5 Steps to Defining IT Services, A Hands-on Workbook, p. 13, 2008.
  - [3] IT Service Management Forum, An Introductory Overview of ITIL V3, UK: The UK Chapter of the itSMF, 2007.
  - [4] V. Haren, ITIL V3 2011 A Pocket Guide, US: Office Government Commerce, 2011.
  - [5] Office Government Commerce, ITIL Service Design, UK, 2007.
  - [6] R. A. Steinberg, ITSM Metric That Matters, US: Migration Technologies Inc., 2012.

## VI. REFERENCES

- [1] C. Rudd, Introducing ITSM and ITIL: A Guide to IT



# Adoption of fuzzy clustering techniques to determine the genetic characteristics of some dates varieties (proposed model)

Nima Abdullah AL-Fakhry  
nama\_alfakhry@uomosul.edu.iq

Ramadan Mahmood Ramo  
ramadan\_mahmood@uomosul.edu.iq

College of Administration & Economic  
Department of management Information Systems  
University of Mosul

## Abstract

Data mining analyzing amount of data to find relations among them and summarized for getting patterns like, graphical models, statistical models. and etc. These patterns are understandable and useful to their users by employing a range of automated extraction of knowledge from hideaways

This Research is a step to illustrate the concept of clustering technique in both theoretical and practical aspects. The theoretical side of the research dealt with the concept of data complexity and types, as well as an explanation of the algorithm (Fcm). The practical side applied the application of the nearest neighboring algorithm to determine the extent of convergence between some date varieties from the adoption of Fructose and and Glucose in Dates . The research concluded that the Fcm algorithm are easy and fast to clarify the genotypes of date species. We use Matlab R2013a to implement the practical side.

**Keyword:** Data mining, Clustering, Fuzzy clustering, Fuzzy C-Mean, Dates

## I Introduction

The science of data mining aims to build graphical models, These models are algorithms or procedures...etc. The purpose of these models is to connect the inputs to obtain new knowledge based on the common characteristics between them, and thus benefit them in interpreting the results and making appropriate decisions. The Fcm algorithm is the best in classifying data fuzziness, The importance of research in the theoretical aspect is a modest contribution to the understanding of clustering concepts and Fuzzy clustering , And an explanation of the algorithm and the stages of Fcm. Different approaches to the problem of cluster analysis exist, such as: The modified fuzzy C-Mean method for clustering of microarray data[9]. A simple and fast method to determine the parameters for fuzzy C-Mean cluster analysis, Comparison of K-Means and Fuzzy c-Means Algorithm Performance for Automated Determination of the Arterial Input Function, An Improved Fuzzy C-Means Algorithm for the implementation of demand side management measure [11][17]

On the practical side we applied FCM algorithm to determine the extent of convergence between some date varieties from the adoption of Fructose and Glucose in Dates because they belong to more than one category at a time .We use Matlab R2013a to implement the practical side.

## II Clustering :

Is a technique of data mining, the process of fragmentation of the original data into groups and collect

data with similar characteristics and put them in clusters depending on the measurement of distance between them, The purpose of this compilation is to construct descriptive models to facilitate the study of these models and to produce important and useful results for decision-makers.

The process of splitting the data into group depends on their sharing of similar properties. therfor the cluster is a group of similar data between them and are not similar to members belonging to other cluster[18].

To implement the clustering, pre-processing data should be performed as follows[16]:

Choose the cluster algorithm: Choose the appropriate algorithm that results from defining a good cluster chart for the data set.

- Evaluation of results: The results of the cluster algorithm are validated by appropriate techniques and standards, and cluster algorithms define previously unknown clusters, regardless of method, so the final fragmentation of the data requires certain types of assessment.
- Interpretation of results: Experience in the field of application needs to integrate cluster results with other proven and analyzed experiences in order to draw appropriate conclusions. Fig(1) illustrates the pre-Processing of data.
- method, so the final fragmentation of the data requires certain types of assessment.

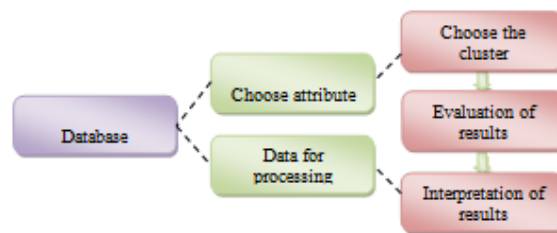


Figure (1): illustrates the pre-Processing of data

## III Types of clustering

The cluster is classified according to the criterion or criterion that defines the similarity between the elements of the data entered into the algorithm, as well as the theoretical and fundamental concepts on which the cluster analysis technique is based, for example, the fuzzy theory and statistics.

Clustering algorithms have evolved based on related topics such as data mining, automated learning, pattern recognition...etc, and these algorithms have been classified into the following categories[2][12][13] :



1. Hierarchical Clustering
2. Partitioned Clustering.
3. Clustering High Dimensional Data.
4. Clustering With Genetic Attributes.

Some researchers have classified clustering algorithms according to the method given in the definition of clusters to the following categories[3]:

1. Hierarchical Clustering.
2. Partitional Clustering.
3. Density-Based Clustering.
4. Grid-Based Clustering.

Each of the above varieties has sub-types and different algorithms to find clusters, so cluster algorithms can be classified according to the type of variables in the data as follows[7]:

- Statistical Clustering: This type is based on the concepts of statistical analysis, and is used to measure the similarity of the fragmentation of models that are specified by numerical data.
- Conceptual Clustering: Used to clustered the Metadata, where models are modeled according to the concepts that carry rather than their values.
- Fuzzy Clustering: Specified techniques for cluster data, assuming that models can be grouped into more than one cluster, use The actual data uncertain (unreliable).
- Crisp Clustering: This type assumes a non-nested segmentation, meaning that the data point either belongs to the cluster or does not belong.
- Kohonen Net Clustering: Clustering in this type depends on the concepts of the neural network, and the cluster consists of external nodes.

#### IV Fuzzy Clustering

clustering is the process of data collection to explore their structures and commonalities, The fuzzy clustering technique allows objects to belong to several categories at the same time.

With different degrees of membership. In many cases, the data sets in the fuzzy clustered are more natural than the fixed aggregates, so that the organisms located on the boundary of the classes of classes are not necessarily bound to belong to one of the categories, But a membership rank of between 0 and 1 is assigned to each object to indicate its partial membership[5][6][10].

When trying to find graphic structures or models of data aggregates that are intertwined with each other and their complexity, one must consider the following[4]:

1. Data representation to convert data group cases into vectors of properties.
2. Use similarity measures. To approach the group of data sets.
- 3 - Hierarchical cluster algorithms are the basis for the structure of cluster algorithms, which divide the structure of data into smaller parts up to one single part. Stratified fuzzy cluster algorithms seek to create structures for data in which an

object is more than one class at a time and one of the most commonly used fuzzy clustering algorithms:

- ❖ Fuzzy Knn
- ❖ Weighted Knn
- ❖ Hcm

#### V Fcm algorithm

It is an iterative algorithm that divides data into groups based on the concept of Fuzzy membership. Instead of assigning each element to a single group, each element will have a different membership value for each group, so that the elements in the middle of the group have more membership value than those on the edges of the group, This algorithm attempts to identify the groups within the data by obtaining the smallest value of the sequence, which is useful when the required number of clusters is predetermined[15]; Thus, the algorithm attempts to place each point of data in a cluster. The probability (membership grade) of membership of a data point is calculated. Because absolute membership is not calculated, the algorithm is very fast because the number of duplicates required to achieve the specified aggregation match the required accuracy[1]

#### VI Implement the system

The Fuzzy cluster means that clusters belong to more than one species at a time, Thus, the idea of research has been developed by constructing a proposed model to find the distance between the two most important characteristics of dates, which are the ratios of fructose and glucose, the purpose of which is to estimate the number of clusters that will be based on the implementation of the algorithm Fcm [8].

#### VII specimen the study

In this research, 44 varieties of dates were selected, In this study, 44 varieties of date varieties were selected, which are produced in most Arab countries for the implementation of the model. They have properties such as fructose, glucose, sucrose,, etc. The fructose levels have been adopted because they are monounsaturated, easy to absorb, And does not need to absorb insulin from the pancreas to support the cluster, and determine the genetic characteristics of some dates varieties and table (1), which shows the dates of the research sample.

Table (1) : DATES VARIETIES WITH FRUCTOSE & GLUCOSE

#	Dates type	Glucose Rate	Fructose Rate
1	Sukkari	14.51	12.85
2	Sulaj	25.9	34.8
3	Shebebi	27.8	18.3
4	Meneifi	32.7	20.5
5	Shaishee	15.53	30.9
6	Safawi	37.5	20.6
7	Assela	32.18	25.3
8	Seqae	30.52	25.3
9	Ajwa	32.07	15.3
10	Anbara	32.7	20.5
11	Shaqra	29.67	21.07
12	Qatarah	32.3	30.9
13	Mabroom	32.07	20.08
14	Mjdool	27.5	34.33
15	Hulwah	31.3	28.6
16	Maktoumi	31.8	30.4
17	Barhi	29.23	20.5
18	Barni Madina	32.7	21.2
19	Romia	32.8	32
20	Abo al-kashab	30.8	30.2
21	Teeba	37.9	32.8
22	Khadyry	33.3	31.8
23	Khalas	32.15	18.3
24	Jamara	28.58	15.56
25	Um Kbare	31.45	32.8
26	Thawee	26.7	27.4
27	Rabeaa	30.09	28.7
28	Tabaeb	31.7	19.6
29	Rashadia	29.23	26.4
30	Ruthana	26.5	30.2
31	Sabala	30.35	25.5
32	Maktoumi	33	37.13
33	Molokia	35.81	15.08
34	Um kashab	35.3	34.5
35	Nabtat Ali	19.17	18
36	Sukkari Ahmer	14.96	11.36
37	Sukkari Asfer	21.7	19.8
38	Majnonna	40.4	36.5
39	Beraim	27.3	27
40	Nabtat Seif	22.27	21.2
41	Sanaf Kaber	31.4	29.4
42	Labane Hamra	33.7	22.3
43	Luna	41.2	36.5
44	Um Hamam	46.09	37.2

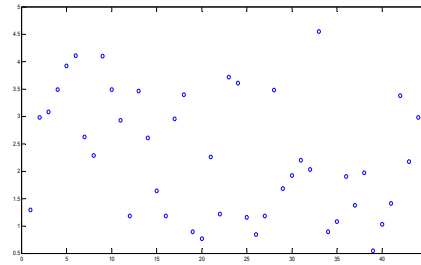


FIGURE (2) : DISTANCE BETWEEN FRUCTOSE & GLUCOSE RATIO OF DATE FRUITS

After obtaining the distance between the fructose and glucose ratios of the selected date, we arranged the results obtained from the ascending Knn algorithm, To determine the number of clusters to be adopted in the implementation sample of the Fcm algorithm, as shown in table (2) and Fig(3)

TABLE (2): THE ASCENDING SORTING OF DISTANCE & DETERMINATION THE CLUSTERS

Ascending Sorting	Dates type	distance	Dates type	#
20.73	Molokia	1.66	Sukkari	1.
16.90	Safawi	8.90	Sulaj	2.
16.77	Ajwa	9.50	Shebebi	3.
15.37	Shaishee	12.20	Meneifi	4.
13.85	Khalas	15.37	Shaishee	5.
13.02	Jamara	16.90	Safawi	6.
12.20	Meneifi	6.88	Assela	7.
12.20	Anbara	5.22	Seqae	8.
12.10	Tabaeb	16.77	Ajwa	9.
11.99	Mabroom	12.20	Anbara	10.
11.50	Barni Almadina	8.60	Shaqra	11.
11.40	Labane Hamraa	1.40	Qatarah	12.
9.50	Shebebi	11.99	Mabroom	13.
8.90	Sulaj	6.83	Medjool(majdool)	14.
8.89	UmAlhamam	2.70	Hulwa	15.
8.73	Barhi	1.40	Maktoumi	16.
8.60	Shaqra	8.73	Barhi	17.
6.88	Assela	11.50	Barni Almadina	18.
6.83	Medjool(majdool)	0.80	Romia	19.
5.22	Seqae	0.60	Abo Al kashab	20.
5.10	Teeba	5.10	Teeba	21.
4.85	Sabala	1.50	Khadyry	22.
4.70	Luna	13.85	Khalas	23.
4.13	Maktoumi	13.02	Jamara	24.
3.90	Majnonna	1.35	Um kbar	25.
3.70	Ruthana	0.70	Thawee	26.
3.60	Sukkari Ahmer	1.39	Rabeaa	27.
2.83	Rashadia	12.10	Tabaeb	28.
2.70	Hulwa	2.83	Rashadia	29.
2.00	Khabeer Variety	3.70	Ruthana	30.
1.90	SukkariAsfer	4.85	Sabala	31.
1.66	Sukkari	4.13	Maktoumi	32.
1.50	Khadyry	20.73	Molokia	33.
1.40	Maktoumi	0.80	Um kashab	34.
1.40	Qatarah	1.17	Nabtat Ali	35.
1.39	Rabeaa	3.60	Sukkari Ahmer	36.
1.35	Um Khar	1.90	Sukkari Asfer	37.
1.17	Nabtat Ali	3.90	Majnonna	38.
1.07	Nabtat Seif	0.30	Beraim	39.
0.80	Romia	1.07	Nabtat Seif	40.
0.80	Um Khashab	2.00	Khabeer Variety	41.
0.70	Thawee	11.40	Labane Hamraa	42.
0.60	Abo Al kashab	4.70	Luna	43.
0.30	Beraim	8.89	Um alhamam	44.

VIII Implement The distance between the Fructose

We will compute the distance between the fructose and glucose ratios according to equation (1) and Fig(2) Represents the result of executing the algorithm

$$d(i,j) = \sqrt{|x_i - x_j|^2} \quad (1)$$

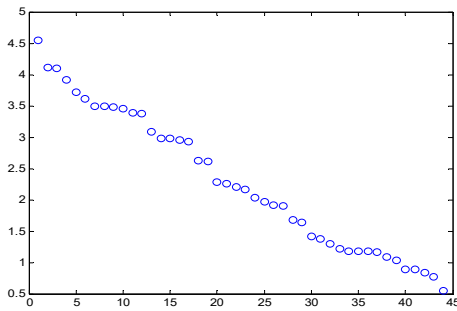


FIGURE (3) : DETERMINE THE NO. OF CLUSTER AFTER ARRANGE

**IX Implement Fcm algorithm[14][15]**

After arranging the distance between the two properties ascending, we divided the data into 6 clusters to begin implementing the Fcm algorithm, The basis of its work is to divide the set of points  $N=\{1,2,3,\dots X_m\}$  to a number of clusters, So that each point belongs to all clusters with different degrees of belonging. Each of these points has a special n (representing the number n dimension space). The idea of the algorithm is to minimize the target function in each frequency as shown in relation (2)

$$u_{ik} = \frac{1}{\sum_{j=1}^c \left( \frac{|x_k - c_i|}{|x_k - c_j|} \right)^{2/(m-1)}} \quad (2)$$

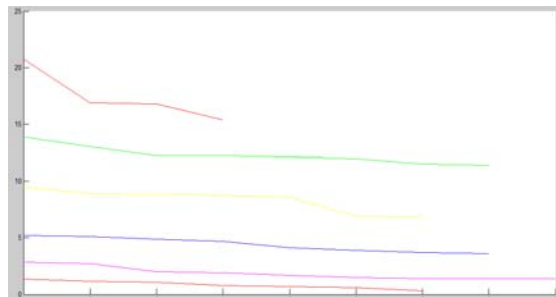
Where :

i:1,2,.....c.

ci : represent the center of cluster (i).

The degree of xj element membership can be determined by the cluster centered on Ci from the equation(3).

$$J(U, c_1, c_2, \dots, c_c) = \sum_{i=1}^c J_i = \sum_{i=1}^c \sum_{k=1}^n (u_{ik}^m)(d_{ik})^2 \quad (3)$$



FIGURE(4): DATES VARIETIES AFTER IMPLEMENTATION OF FCM ALGORITHM

**IX Interpretation of results**

Note from Figure (4) :

1. the fcm algorithm was wonderful in explain relations between different types of dates and is easy to implement and does not take a time.
2. symbols because the goal of the algorithm is to reduce the target function.
3. The class of kingship, is very different from the rest of the varieties and there is no common property between him and the varieties in the same cluster or with varieties

in other clusters, while the convergence of both Safawi and Ajwa with varieties of clusters 2 and 4.

4. The items in the fifth & sixth clusters shared in the qualities with the varieties in the clusters other than the Priem category, that is, it is possible to grow in most countries of the Arab countries.
5. The fifth cluster diverged most of the varieties, i.e. they do not share with the other clusters in genetic traits, that is, they can not be planted in areas other than Saudi
6. Most of the items in the third cluster whose genetic characteristics are similar to those of other clusters.

**X Conclusion:**

The observed results from the fcm algorithm showed that the algorithm was clear in determining the relationship between date types through the characteristics adopted in the research, and this algorithm is quick and easy in the application

**Reference**

- 1-Almazroie, Mishal,Vadivelloo, Mogana, Abdullah, Rosni, "GPU-Based Fuzzy C-Means Clustering Algorithm for Image Segmentation", arXiv: 1601.00072v3.[cs.DC], PP.1-2., 2016, Malaysia.
- 2- Deokkar, SidMeans Clustering, P.,Pulau Pinang, Madharth, "Weighted K-nearest Neighbor", CS 8751, Institut Fur Statistik, 2004, Germany. <http://www.csee.umbc.edu/>.
- 3- Dunham, Margaret H., "Data Mining, Introductory and Advanced Topics-Part II", Prentice Hall, Companion slides website, 2012: <http://lyle.smu.edu/~mhd/dmbook/part2.ppt>
- 4- Francesco, Masulli, " Fuzzy Clustering", Dip. Informatica, Bioingegneria, Robotica e Ingegneria dei Sistemi University of Genova - Via Dodecaneso 35, 16146 , 2015,Genoa – ITALY.
- 5-<http://homes.di.unimi.it/valenti/SlideCorsiBioinformatica05/Fuzzy-Clustering-lecture->
- 6- Gomathi, c & Velusamy, K, , " SOLVING FUZZY CLUSTERING PROBLEM USING HYBRIDIZATION OF FUZZY C-MEANS AND FUZZY BEE COLONY OPTIMIZATION", International Journal of Computer Engineering and Applications, Volume XII, Issue IV, 2018
- 7- HALKIDI, MARIA & BATISTAKIS, YANNIS & VAZIRGIANNIS, MICHALIS, "On Clustering Validation Techniques". Journal of Intelligent Information Systems, Vol. 17, Kluwer Academic Publishers, PP. 108-111, 2001, Netherlands
- 8-Hans Peter, Schubert, Erich; Zimek, . "The (black) art of runtime evaluation: Are we comparing algorithms or implementations". Knowledge and Information Systems, P. 52,2016.
9. J. P. Stitt & R. L. Tutwiler & A. S. Lewis, "Synthetic Aperture Sonar Image Segmentation using the Fuzzy C-Means Clustering Algorithm", Autonomous Control and Intelligent Systems Division The Pennsylvania State Applied Research Laboratory PO BOX 30, State College, PA, 16804 USA ,2001.
- 10- Klawonn, Frank and Hoppner , Frank, "What is Fuzzy About Fuzzy Clustering? Understanding and Improving the Concept of the Fuzzifier", Department of Computer

Science, University of Applied Sciences Braunschweig /  
Wolfenbuettel ,PP. 1-4, 2003, Germany.

- 11.L'aszl'o G. Ny'ul, "Fuzzy Techniques for Image Segmentation", Department of Image Processing and Computer Graphics University of Szeged,2008
- 12- Pande ,S. R., Sambare ,Ms. S. S., Thakre,V. M., " Data Clustering Using Data Mining Techniques", International Journal of Advanced Research in Computer and Communication Engineering Vol. 1, Issue 8, PP.494-495, 2012, India, web site: [www.ijarce.com](http://www.ijarce.com).
- 13- Rajagopal, Sankar , "Customer data clustering using data mining technique ", International Journal of Database Management Systems ( IJDMS ) Vol.3, No.4, PP. 2-3, 2011, India.
- 14-Song ,Jian-Hua & Cong, Wang & Li, Jin , A Fuzzy C-means clustering algorithm for image segmentation using nonlinear weighted local information" ,journal of information hiding and multimedia signal processing, Ubiquitous International Volume 8, No. 3, 2017,China.
- 15- YANG, Jun & KE ,Yun-sheng, WANG , Mao-zheng , "An adaptive clustering segmentation algorithm based on FCM",Turkish Journal of Electrical Engineering & Computer Sciences, 25: 4533 – 4544, 2017,Turkey
- 16-Yang ,Shih-Feng & Rayz ,Julia Taylor ," An Event Detection Approach Based On Twitter Hashtags", arXiv: 1804.11243v1.[cs.SI], P. 8, 2018, Purdue University, USA.
- 17- Yao, Yaqiang & Chen, Huanhuan, " Multiple Kernel k-Means Clustering by Selecting Representative Kernels", arXiv: 1811.00264v1.[cs.LG],2018, China.
- 18- Yousif, Manahel Abd AL\_Kareem , " Using one of the methods of clustering and Fuzzy logic to classify tissues images", Journal of Tikrit University, Journal of Tikrit University of Pure Sciences , University of Tikrit, P. 296, 2011, Iraq

# Suggested Approach Using Cloud Computing And DNA Test in Finding Missing Children In All Over The World

Suhad Abu Shehab  
A Scientific Research  
suhad\_cis@hotmail.com  
Facility Of Information Technology

Dr. Mostafa Alrawashdeh  
(Lawyer, Author and Cyber Crimes Expert)  
mostafaalrawashdeh1155@gmail.com  
Facility Of Law

**Abstract** - Wars, natural disasters, conflicts in some areas, abandoned and kidnapped children .. etc. all these juveniles cause a big human's problem all over the world (unknown and foundlings Childs). Parents and relatives to those unknown children try everything to find their children, it became an impossible mission in some situations like wars, natural disasters .. etc, because of the huge numbers of unknown children they be founded by other people, rescue teams, and any other way especially when child moves from country to another country or parents are forced to leave their countries. To solve this huge human's problem, countries must use law and technology of database and comparisons algorithms between the DNA of the child and DNA of their parents or relatives.

**Key Words:** Cloud computing, Unknown Children, DNA test , Data Mining, Algorithms, child's rights, law.

## I. INTRODUCTION

War, Natural disasters and other juveniles caused a lot of families to lose children's during these situations, they try as possible as they can to find their children's, but they arrive to an end road without finding their child , his or her child become a missing child. "A missing child or unknown child is a child whose whereabouts are not known to the parents, legal guardian or any other person or institution legally entrusted with the custody of the child, whatever may be the circumstances or causes of disappearance, and shall be considered missing and in need of care and protection until located or his safety and well-being established" [1]. In the other hand these juveniles caused to find a lot of very young children without knowing anything about their parents , their names or anything about them, that makes finding their parents during this mess an impossible mission. The same thing about foundling's child, "Foundling' is an historic term applied to children, usually babies, that have been abandoned by parents and discovered and cared for by others" [2]. In this case we cannot know anything about the child or about his or her parents. It becomes so hard in the future to know anything about his or her root. In this paper we will call foundling, missing and unknown children the (Unknown Children).

The solution for this painful problem is a combination of all human's knowledge from different felids with each other (Information technology, biology and law). In this paper we come up with a suggested solution for this problem by suggestion of establishing a huge DNA cloud database for all children without knowing their parents or anything about them in all countries all over the word, then uploading this data for international shared Cloud (Cloud computing). Every parent tries to find their

missing child's by making a DNA test then the results are uploaded and compared with the data in the cloud that has all the DNA test for unknown children to find match in it. The result of the match process is his or her missing child by the international law.

## II. USING DNA TEST TO FIND BIOLOGICAL PARENTS AND RELATIVE'S BACKGROUND

As shown in figure (1) Google search for "DNA in finding parents", a lot of websites concern about finding parents by comparing DNA test results, such as "Connecting with Your Biological Family" through DNA Test, in this web site they focus on Adoptees and others with unknown parentage they use DNA testing to find and connect with their biological families or to learn more about where their ancestors came from. In the beginning, they take a DNA Test and review of DNA matches, using some companies database to provide a DNA match list. In the next step of this process is reviewing the DNA matches. The final step is reaching Out but in this step they tell the person who tries to find his or her parents to take care of

- “1. Your DNA match may not know how to help you determine your birth parents or immediate family.
- 2. Your birth and subsequent adoption may have been kept a secret from other members of the birth parents' families.
- 3. Your birth family may not wish to make a connection” [11].

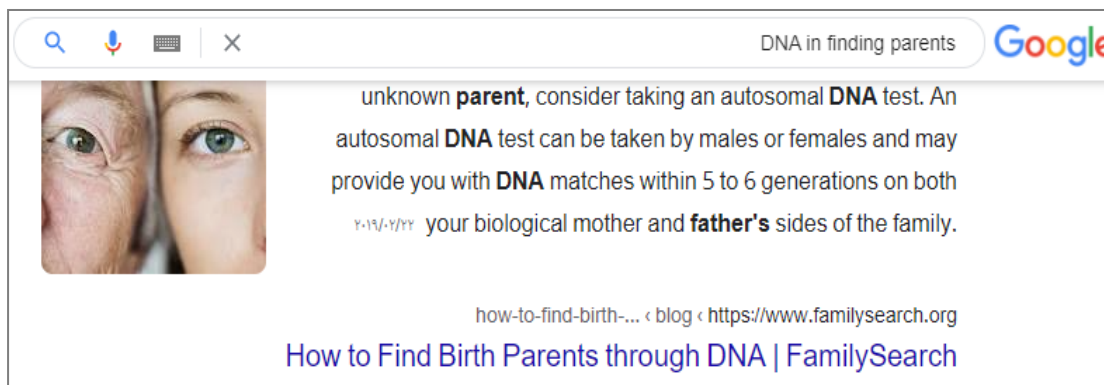


Figure (1) Google search for "DNA in finding parents" [9]

As shown in figure (2) Google search for "DNA in finding relatives", a lot of websites concern about finding relatives by comparing DNA test results, such as "MyTrueAncestry - Compare your DNA test results , Genealogy search - Free Ancestry Database and Finding Biological Family - Ancestry Support .. etc". All these websites concern to find matches by comparing the DNA results to find relatives. these websites are free and they are just for people in the UK , they are an online access to family history records. All their teams are volunteers to create high-quality transcriptions of public records from governmental sources, parish churches, and other trusted institutions. They have an *Open Data* and *Open Source* to make and keep public records accessible to all. The databases which are created freely, are available for people to search in order to support their family history research [12].



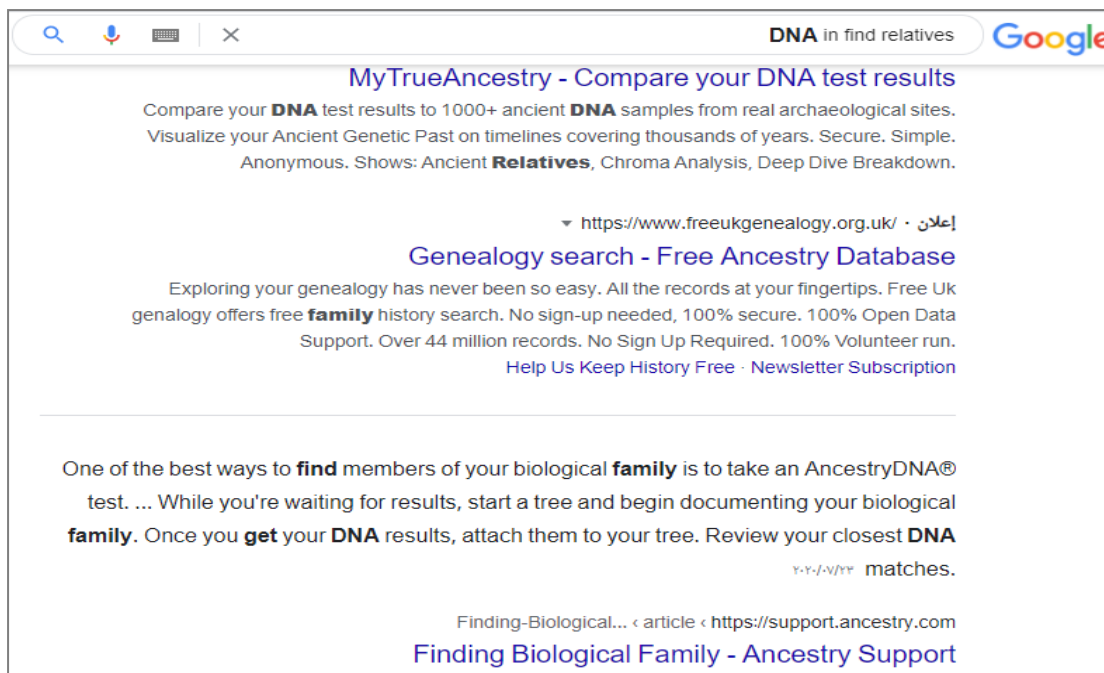


Figure (2) Google searches for " DNA in finding relatives" [10]

In figure (3) Google search for " Unknown children in cloud computing" as seen there is no papers or websites about establishing a database or cloud for all unknown children in the world.

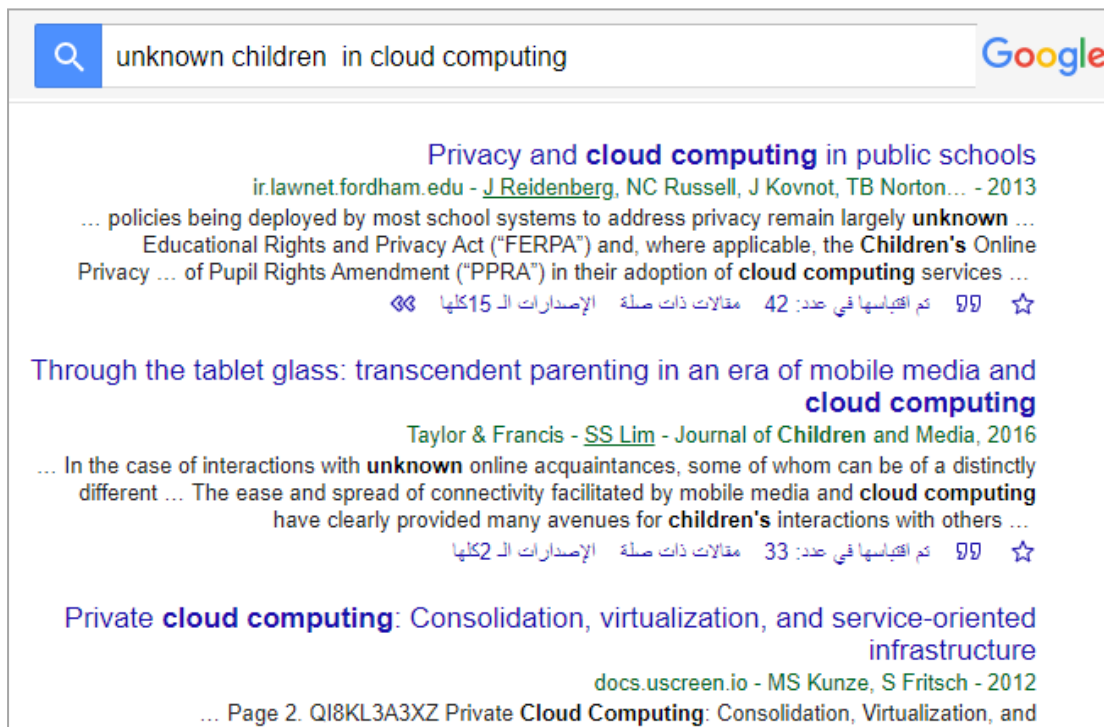


Figure (3) Google search for " Unknown children in cloud computing"[14]

These websites concern about adults trying to find their biological parents or relatives. Some of these websites charge money for their service and some of those are free of charge. The person who tries to find his or her parent must enter his or her DNA test to find the match from other DNA results

uploaded from other adults. These websites are working in some countries only. In this paper the most concern issue is establishing a formal shared global cloud database for all unknown children's without parents or relatives, using the power of technology and algorithms to find their biological parents or relatives in all over the world. In this suggested approach the most important thing is children's reunion to their parents.

### III. UNKNOWN CHILDREN PROBLEM AND CLOUD COMPUTING

#### *A. The Problem*

Family and children's rights "The International Convention on the Rights of the Child gives all children the right to a family. The right to a family allows children to be connected to their history, and it offers a protective perimeter against violation of their rights. Children separated from their families become easy victims of violence, exploitation, trafficking, discrimination and all other types of abuse"[19]. The most painful of the human's problem when parents lose their child because of wars, natural disaster .. etc, his or her child is alone in this hard world, they may face danger in his or her own live, they have no future, living in non human conditions in some cases (in some refugee camp) and a lot of dangers we cannot think about it. The child grows up without knowing anything about himself or herself ( name, family, roots ... etc). This is the most painful issue in this modern world because of a lot of wars and disasters which happened in the last two decades. They cause a millions of unknown children who do not know anything about their families. At the same time, there are wounded parents or relatives trying to find their missing child using any way they can.

#### *B. Suggested solution Using DNA test results and Cloud Computing and the Law to solve this problem:*

In this suggested approach the solution to solve this human's painful problem is that every country in the world must involve in this solution, which is responsible for their duties in helping the parents and child's to find each other. Each country must make a DNA test for every unknown child whom are found without their parents. The DNA test is reliable because each person's genetic fingerprint is unique. The DNA test is taken by the law to proof the paternity for the child.

The only method that can help in this situation is DNA test. Each person's genetic fingerprint is unique, so we can depend on this kind of test. A biological child has the same DNA with his biological father and his or her biological mother. A DNA paternity test compares a DNA sample from an alleged father or mother and a DNA sample from a child to determine if this child is biological son for them. [3]

Part of the Paternity law refers to law underlying legal relationship between a father and his or her biological children (Proofed by DNA test) and deals with the rights and obligations of parent (father) and child to each other. Child's paternity may be relevant in relation to issues rights to a putative father's title, as well as the biological father's rights to child custody [4].

Cloud computing is on-demand availability of computer system especially data storage (cloud storage) The term is generally used to describe data centers available to many users over the Internet



(over all the world). Large clouds, often have functions distributed over multiple locations from central servers.[5]

A cloud database is a database service built and accessed through a cloud platform[13]. cloud database acts like traditional database with the added flexibility of cloud computing. Users can use it by install the software to establish a cloud infrastructure to implement the database. The key features of cloud computing is a database service built and accessed through a cloud platform ,users can host databases without the need to have a hardware equipment, support relational databases like MySQL and NoSQL databases. Accessed through a web interface or vendor-provided API. [13]

The most important features of cloud computing are *Easy of access* Users can access cloud databases from virtually anywhere, using a vendor’s API or web interface. *Scalability* organizations only pay for what they use. *Disaster recovery* in the event of a natural disaster, equipment failure or power outage, data is kept secure through backups on remote servers [13].

Cloud Computing is the best solution to establish an international cloud database for creating a DNA test result for all these unknown children without parents or legal garden, because any user in the world can access and use this database if this user have the privilege to access and use it.

### C. DNA test and match algorithm

DNA is an inherited concept of inheritance from a common ancestor. Humans have 22 pairs of chromosomes in which one chromosome is inherited from the father and one from the mother, each child inherits an equal amount of DNA (50%) from the mother and the father , child inherits one copy of each chromosome from each parent. The child’s chromosomes is a mixture of each parent’s two chromosome copies. The biological process responsible for the transmission of chromosomes from parents to child in this way is what is called meiosis. The random assortment of these chromosome fragments during meiosis is called recombination. The end result is that each child’s DNA is a random mixture of DNA from his or her two parents. Comparing the chromosomes of the siblings, lining them up, observing that some regions of the chromosomes have the same color (Figure (4)) in each sibling. This indicates that they have almost identical sequences of DNA at those locations on their chromosome. These locations on the chromosome are called “identical-by-descent” (IBD) because they were inherited from a common ancestor (in this case, the common ancestor is the mother or the father)[15].

Figure (4) shows that DNA is an identical-by-descent between distant cousins (C, D, E). Chromosomes of the common ancestors (A) and their children (B) are shown. The blue and red circles indicate chromosome segments that are IBD between the indicated chromosomes.

DNA is essential in finding parents and relatives, it is about several genetic analyses to help individual find, preserve, and share their family history using Identity-by-descent" (IBD) detecting “matches” from DNA by identify long chromosome segments shared by pairs of individuals.

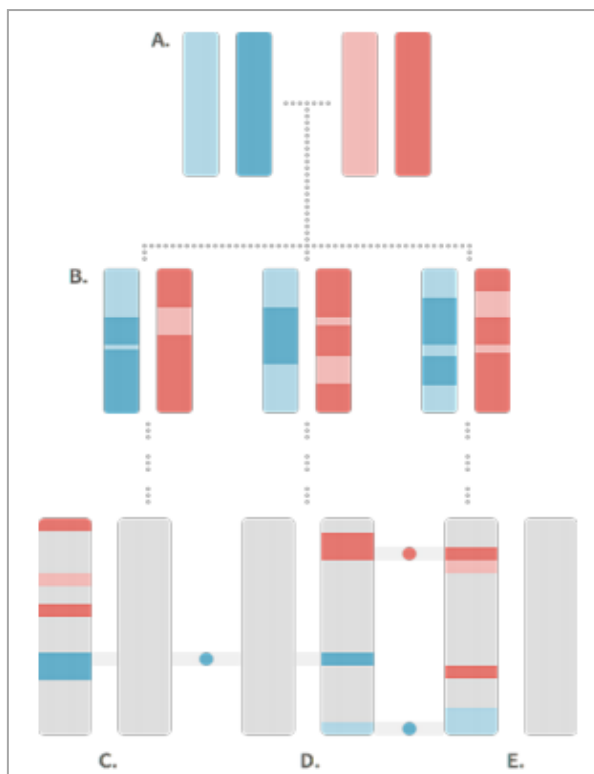


Figure (4) The process of recombination of DNA [15].

In the figure (4), all inherited some DNA from the common ancestors, only a few short segments of the chromosomes are actually identical in the same places on the chromosome of different cousins. In this example, one segment of DNA is shared by cousins C and D, and two segments are shared by cousins D and E. When IBD segments are identified, this information is used to estimate how people are related to one another by drawing connections between relatives through their DNA [15].

To improve the process of finding parents and relatives, they increased precision in identifying shared segments. The relationship between DNA matches is about how much shared DNA between people. In figure (5) determined each level of relationship based on how many centimorgans matches share [16].

As seen in figure (5), when individual knows the number of centimorgans you share with a match, it can help in understanding your relationship to them. For example, in case of 3rd cousin you will share about range (90 - 180) centimorgans [16].

For the comparison the unit for segments of DNA is the centimorgan (cM), humans full genome is about 6500 cM. The longest length of a match is the greater chances that is match [17].

Approximate Amount of Shared DNA (in centimorgans [cM])	Predicted Relationship
3,475 cM	parent, child, or identical twin
2,400–2,800 cM	immediate family: full sibling
1,450–2,050 cM	close family: grandparent, aunt, uncle, half-sibling
680–1,150 cM	1st cousin, great-grandparent
200–620 cM	2nd cousin
90–180 cM	3rd cousin
20–85 cM	4th cousin
6–20 cM	distant cousin: 5th to 8th cousins

Figure (5) Relationship based on how many centimorgans matches share [16].

*D. An example of algorithm Used to find a match in DNA test*

(Multiple Bloom Filters (MBFs)): Method of storing chromosome data and searching patterns in the data, described the method of using MBFs or an array of BFs to store chromosome data in the compressed format. Subsequently, describing the procedure to search patterns in the DNA sequences that are stored in MBFs [18].

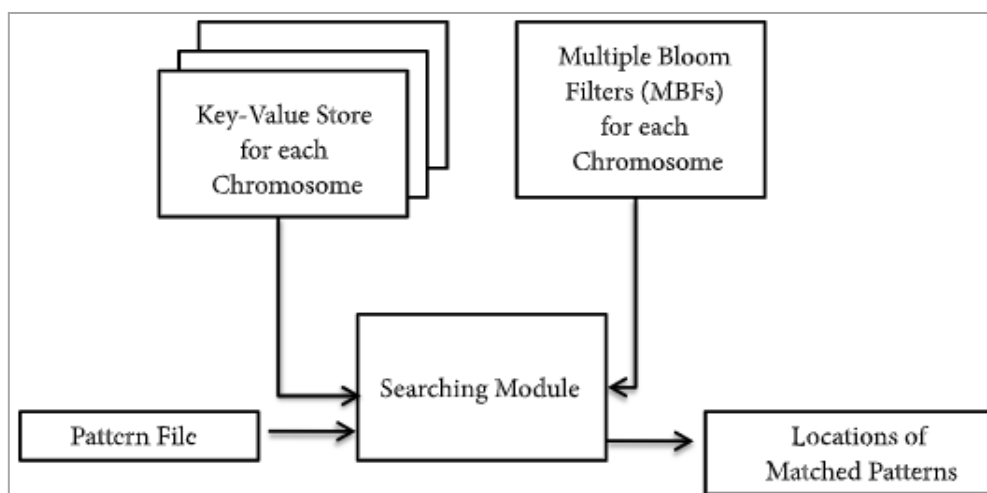


Figure (6) Multiple Bloom Filters (MBFs) [18].

This phase comprises of three important steps as seen in figure (6) the Multiple Bloom Filters (MBFs) phases: (1) Formation of k-mers of the given chromosome. (2) Storing locations of each unique k-mer in the Key-Value (KV) store on disk. (3) Storing location data for each unique k-mer of chromosome in a separate BF [18].

In the beginning of this process determined the length ( $k$ ) of DNA words, DNA is a sequence of characters called word, example (A,C,G,T) of length  $k$ . Increasing  $k$ -mer size increases number of unique  $k$ -mers and gets reduced in the sequence as length of the DNA words is increased. In this case,  $k$ -mer size is a critical parameter and has a different impact on the size of KV store and MBF. a Key-Value (KV) storage is required to store all the locations of each unique  $k$ -mer in the given chromosome. Value is the sequence of locations where specific  $k$ -mer is located in the chromosome, The next step is the construction of Multiple Bloom Filters (MBFs) for each single chromosome. Bloom filter (BF), a probabilistic data structure, is used to store all the location data of each unique  $k$ -mer in a separated BF. As a result existed a BF for each distinctive  $k$ -mer present in the chromosome. This consequently leads to the formation of MBFs, the size of the BF plays a significant role in achieving compression to determine the accurate size of the BF a pattern is a sequence of DNA characters (A,C,G,T) that is to be searched in a DNA sequence or chromosome. Before the pattern matching process starts, a pattern is decomposed into  $k$ -mers of size  $k$ . DNA word or  $k$ -mer size is set to 4 when KV store is built. The 4 is selected as the final value of  $k$  and a pattern is decomposed into  $(N-k+1)$   $k$ -mers where  $N$  is the length of the pattern sequence. After that one  $k$ -mer is part of the pattern is selected such that it has the least number of occurrences in the chromosome (target string to be searched) among all other  $k$ -mers that are part of a pattern. The next step is to select the  $k$ -mer from the pattern with the least number of occurrences in the sequence. In case, there is a tie between two or more  $k$ -mers then the one that comes first in the sorted list of  $k$ -mers is selected. KV store is an integral part which stores all the locations of each unique  $k$ -mer present in the chromosome. [18]

#### *E. Data mining techniques to manage Cloud Computing*

When we establish a database in a cloud for all DNA test results of unknown children, Data Mining algorithms are used to organize the data in cloud computing to find hidden pattern between the data, it may find relatives children (cousin children) in the cloud. Data Mining is a technique used to extract a new knowledge from existing data and emerged as a significant technology for gaining knowledge from vast quantities of data. Data mining is used to find hidden patterns "relations" between data in huge datasets, it is one of the business intelligence techniques because it can extract valuable knowledge from huge databases and find hidden relations between data [8]. The Data mining techniques is: **Classification Trees** classify a categorical variable which is dependent and based on the measurements, it divides the data nodes into small subgroup [6]. **Logistic Regression** Statistical technique that; expands the conception to work with classification Provides a method that is used to predict the probability of the occurrence of the independent variables as a function. **Neural Networks;** a software algorithm that is a set of comparable architecture of brains, network elements, weight is assigned to each unit. Different varieties of data are inputted to the input node, used a technique of trial and error, various algorithms are used to adjust the weights until it meets a certain halting criterion. **Clustering Techniques;** a technique that is used to partition a set of data into meaningful subclasses which is known as cluster. The nearest neighbour technique used finds out the gap between data. After finding that gap, it assigns the particular record to the class which is the closest neighbour in the whole data set. **Association Rule Mining;** observes that association rule mining technique involves the use of

machine learning models to analyse data for patterns in a database. Identifying the frequent and associations which are called association rules. **Machine Learning**; software can be included and learned from the data and the main focus is on making predictions.[7]

These algorithms will help in finding a match in this cloud or hidden pattern in the results of DNA test to find the relatives of the unknown child's or reunion brothers and sisters in unknown children. We can use any other algorithms or tools to find the match between unknown children and the family who tries to find his or her missing child.

#### IV .CLOUD COMPUTING IN PROOFING PATERNITY OF UNKNOWN CHILDREN USING DNA TEST RESULTS

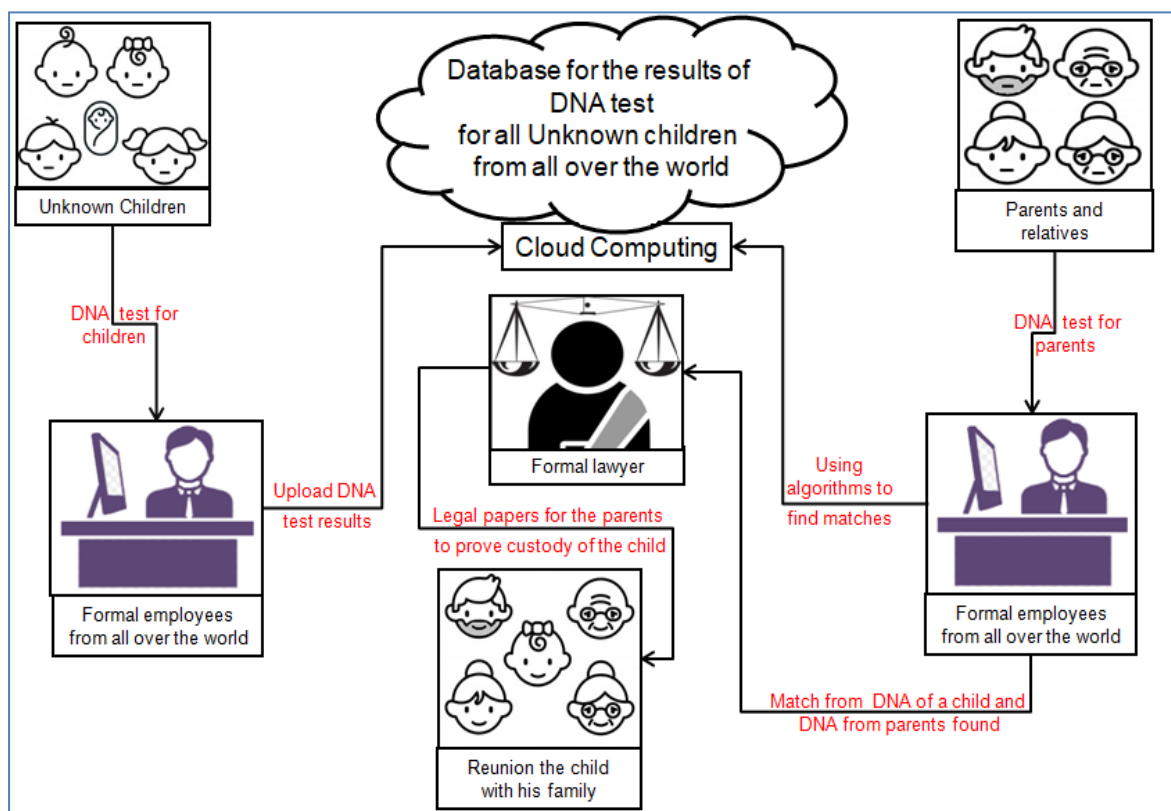


Figure (7) Cloud Computing in Proofing paternity of unknown Children use DNA test results

In figure (7) Cloud Computing in Proofing paternity of unknown Children use DNA test results, it shows the steps of the process of parents finding their missing child. For example, during a war a family lost his or her child, The family is forced to move to another country, the child's is found by rescue team. The formal employee makes a DNA test to the unknown child, then uploads the result to an unknown children database cloud.

The parents start searching of their baby, they make a DNA test and give the result to the formal employee in their country they live in. The employee use algorithm to find a match from the international unknown children database cloud. The match is found, the employee sends the result of

finding a match and the parents to the formal lawyer to communicate between countries and to make all the papers to proof the paternity of their own child. The formal lawyer makes all the procedures for the reunion process by the international law. The parent's reunion with their missing child is completed.

#### CONCLUSION

A million of unknown children in the worlds and a million of families all over the world are missing their children. If we apply this suggested approach in this paper; a thousand or millions of unknown children will reunion with their families, then one of Child's Rights will be achieved. All countries in the world must involve in the process of establishing a cloud computing database containing all unknown children DNA tests, and establishing a formal process containing all fields of (Information technology, biology and law) to make the process of reunion the child and the family possible. These children are a part of future. We must take care of them, to have a bright future of humanity.

## REFERENCES

- [1] Juvenile Justice , "Care and Protection of Children". Act, Article 92 (G.S.R. 898) , 2016.
- [2] <https://foundlingmuseum.org.uk/about/our-history/what-is-a-foundling/>, [Last Accessed May, 2021].
- [3] <https://dnacenter.com/blog/everything-you-need-to-know-about-a-dna-paternity-test/>, [Last Accessed May, 2021].
- [4] Richards, Edward P. "The Presumption of Legitimacy". Law and the Physician. The Law, Science & Public Health Law Site, 2017.
- [5] "An Introduction to Dew Computing: Definition, Concept and Implications - IEEE Journals & Magazine". doi:10.1109/ACCESS.2017.2775042. S2CID 3324933, 2017.
- [6] J.Nageswara Rao, M.Ramesh, "A Review on Data Mining & Big Data, Machine Learning Techniques" , International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878, Volume-7 Issue-6S2, pp 914-916, 2019.
- [7] RItu Ratra , Preeti Gulia "Big Data Tools and Techniques: A Roadmap for Predictive Analytics", International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-9 Issue-2, 2019.
- [8] Alaa H Al-Hamami, Suhad Abu Shehab " An Approach for Preserving Privacy and Knowledge In Data Mining Applications", Vol. 4, No. 1 SSN 2079-8407 Journal of Emerging Trends in Computing and Information Sciences , CIS Journal, 2013.
- [9] <https://www.google.com/search?q=DNA+in+finding+parents&ei=>, [Last Accessed June, 2021].
- [10] <https://www.google.com/search?q=dna+in+find+relatives&source=hp&ei=> ,[Last Accessed June, 2021].
- [11] <https://www.familysearch.org/blog/en/how-to-find-birth-parents-through-dna/> ,[Last Accessed June, 2021].
- [12] <https://www.freeukgenealogy.org.uk/> ,[Last Accessed June, 2021].
- [13] <https://www.ibm.com/cloud/learn/what-is-cloud-database> ,[Last Accessed June, 2021].
- [14] [https://scholar.google.com/scholar?hl=ar&as\\_sdt=0%2C5&as\\_vis=1&q=unknown+children++in+cloud+computing&btnG=](https://scholar.google.com/scholar?hl=ar&as_sdt=0%2C5&as_vis=1&q=unknown+children++in+cloud+computing&btnG=) ,[Last Accessed June, 2021].
- [15] <https://www.ancestry.com/dna/resource/whitePaper/AncestryDNA-Matching-White-Paper.pdf> ,[Last Accessed June, 2021].
- [16] <https://www.ancestry.com/corporate/blog/the-science-behind-a-more-precise-dna-matching-algorithm/> ,[Last Accessed June, 2021].
- [17] [https://en.wikipedia.org/wiki/Genealogical\\_DNA\\_test](https://en.wikipedia.org/wiki/Genealogical_DNA_test) ,[Last Accessed June, 2021].
- [18] Raihan Ur Rasool and others ' Pattern Matching for DNA Sequencing Data Using Multiple Bloom Filters' , *BioMed Research International*, Volume 2019 |Article ID 7074387, 2019.
- [19] <https://www.humanium.org/en/family-and-childrensrights/> ,[Last Accessed June, 2021].

# STANDARDIZED SECURITY DESIGN AND INFORMATION SYSTEM IN NIGERIA EDUCATIONAL INSTITUTION.

Eleberi Ebele Leticia

Department of Computer Science

[Ebyfav2001@yahoo.com](mailto:Ebyfav2001@yahoo.com)

## *Abstract*

*This paper investigates standardized security design and information system in Nigeria educational institution. The paper disaggregated standardised security design to inter office communication, firewall, virus protection programmes and encryption as explanatory variables while information system remains the dependent variable. Data were generated via Primary source through the use of a structured questionnaire and analysed through multiple regression analysis (ordinary least square). The study found that to inter office communication, firewall and encryption has significant effect on information system while virus protection programmes was found to be statistically insignificant. In essence, it was observed that there is need for every organization to have an information security management system that can adequately provide reasonable assurance and support for IT application and business processes.*

**Keywords:** *Standardized Security Design, Information system, Education Institution.*

## **1.1 Introduction**

Nigeria's founding fathers fought valiantly and successfully to liberate the country from British rule on October 1, 1960. There were expectations that the country would be much stronger under self-rule and would adopt policies to ensure the growth and personal development of people in all fields, which would translate to national development. However, when the topic of Nigeria's educational system is brought up today, the first thoughts that come to mind are a decrease in standards, a degradation in the information system, deterioration of services, and examination malpractices.

Before anything else, there should be a focus on mass marketing syndrome and the like. Education is one of the most visible and visible sectors in Nigeria, commanding

attention and consuming much of the country's scarce resources, and like a home sickness, many Nigerians yearn for, strive for, and try to gain access to more and more of it. Nigerian government at all levels must be active for the sake of national growth. Globally, technology is having an effect.

The internet has had a huge impact on the world's educational institutions. A knowledge infrastructure in terms of protocols and processes is one of the alternatives (Author's Observations. 2020). The Internet is a computing philosophy that seeks to link our daily life objects (computing devices or things) by using the Internet as a networking medium. It also aims to provide information processing capability that will enable things to sense, incorporate, and present data when responding



to all facets of the physical environment (Atzori, Iera, & Morabito, 2010).

The Internet infrastructure is built on a layered architecture style, and it uses this perspective to abstract and simplify object integration, as well as to offer smart services solutions to applications (Jing, Vasilakos, Wan, Lu, & Qiu, 2014). There is something that no educational system can do without. Both parties should have access to school-related information through the internet, but information must be held secret using a reasonable standard security architecture.

Standard security architecture is a high-level system layers, application layer that are composed of internet applications and middleware system, which is an organization that simplifies the creation of applications through interoperability necessity of heterogeneous devices and external and internal hacking. Information System provides prompt and accurate output of data & information for policy decision. Hua and Herstein (2003)

Nigeria's educational institutions have created a modern education management information system infrastructure built on web-based networks that is ready for adoption in a growing number of states in order to increase information quality for stakeholders. An

education management information system is a system used to capture, integrate, process, retain, and disseminate an interconnected collection of appropriate, accurate, unambiguous, and timely data and information to education executives, policy makers, planners, and managers at all levels in order for them to fulfil their roles in order to meet an organization's goals and objectives (Wako, 2003).

Both workers of the organisations, whether academics or non-academics, have information. The majority of this information is available in a variety of formats, and these types of information have different values within an entity. With a wide variety of information institutions facing internet security challenges, it is critical to enforce uniform security systems (design), which Brykczynski and Small (2003) believe the security design methodology will assist in implementing. Maintaining and improving the interconnected collection of rules, controls, and procedures that guarantee the integrity of an organization's information properties must be done in a way that is suitable for the organization's strategic goals.

## 1.2 Statement of the problem

Because of the ever-increasing number of users connected to the internet, the internet is becoming extremely congested; security has become increasingly critical. " The number of computers connecting to the internet continues to grow exponentially, from about 497 million

in 2015 to more than 637 million in 2018. (Parenty, 2019).

Nigeria's educational establishments are not immune to this. As many advantages as online platforms have, new advancements can pose new risks to information technology systems. Organizational security frameworks currently include: inter-office communication systems, firewalls, malware detection services, encryption, and so on, while future systems will need new Extensible Mark-up Language (XML) standard formats such as XML Encryption, XML Digital Signature, and XML Key Management Systems to structure security data.

While XML solves several issues, it has also raised security concerns that must be addressed. The primary goal of traditional security framework design is to enforce effective measures to remove or mitigate the effect that multiple security-related risks and weaknesses can have on an enterprise. Through doing so, Information Security Management would allow the company to enforce attractive qualitative characteristics of its services (such as service compatibility, data protection and integrity).

According to Pattinson (2007), "an information management system architecture focuses on designing information security within an organisation, a topic that is of growing interest to many organisations as they contend with the problems faced by the information society." These issues include emerging information protection and privacy

laws, written rules, cyber security, and environmental (fire, storm, earthquake, tornado) or human risks (Viruses, spam, privacy, hacking, and industrial espionage).

The National Institute of Standards and Technology has proposed sets of more detailed principles for protecting information technology infrastructure (NIST). The Principles were derived from the Organization for Economic Cooperation and Development's (OECD) Guidelines for the Security of Information Systems. These standards serve as a foundation for organisations to develop and assess their IT security systems. A substantial amount of effort has also been used in the assessment of defense options.

Much exposure has not been paid to this in Nigerian educational institutions for proper considerations. Universities, polytechnics, and colleges in Nigeria should be aware of this. Nigeria's educational system must look beyond analogue and accept digital with an appropriate information security system. On this basis, the paper aimed to assess the uniform defense design and information structure of Nigeria's educational system.

### 1.3 Objectives of the study

The core focus of this paper is to investigate on standardized security design and information system in Nigeria educational institution. Specifically, the paper set to achieve the underlisted specific objectives;

1. ascertain the effect of inter-office communication on information system in Nigeria education institution.

2. evaluate the effect of firewalls on information system in Nigeria education institution.
3. determine the effect of virus protection programmes on information system in Nigeria education institution.
4. investigate the effect of encryption on information system in Nigeria education institution.

#### 1.4 Research Questions

The research paper is guided by the underlisted research questions;

1. what effect has inter-office communication on information system in Nigeria education institution?
2. To what extent has firewalls affected information system in Nigeria education institution?
3. What is the effect of virus protection on information system in Nigeria education institution?
4. What effect has encryption on information system in Nigeria education institution?

#### 1.5 Research Hypotheses

The following research questions were subjected to empirical testing;

1. **H<sub>0</sub>**: there is no significant relationship between inter-office communication and information system in Nigeria education institution.

2. **H<sub>0</sub>**: there is no significant relationship firewalls and information system in Nigeria education institution.
3. **H<sub>0</sub>**: there is no significant relationship virus protection and information system in Nigeria education institution.
4. **H<sub>0</sub>**: there is no significant relationship encryption and information system in Nigeria education institution.

#### 1.6 Scope of the study

The content scope of this paper is to investigate on standardized security design and information system in Nigeria educational institution. Standardized security design was disaggregated into inter-office communication, firewalls, virus protection and encryption as explanatory variables while information system as proxy for dependent variable.

#### 2.1 Literature review

##### 2.1.1 Information system

Information consists of data being processed and made meaningful to the users while system consists of set of components used to operate together to make possible conversion of data into information for use by any decision maker within or outside an organization (Davis & Olson, 1985; McLeod, 1995). Information system is also known as computer based information system. In general, the term information system refers to a system of people, data records and activities that process the data and information in an organization

which includes the organization manual and automated process.

Educational institution should have in information system security officers. These set of individuals perform the following roles to ensure the safety of information within the organization via internet or off-lines. Information system security officers must request persons responsible for information systems to establish a method to maintain security throughout the information system's lifecycle. Information system security officers must define security requirements for information systems. Requirements for systems which provide online application and notification services between employees, organizations, and the government must be formulated based on the "Guidelines on Risk Assessment and DigitalSignature/Authentication Fore-Governments'. Integrated Payment and Personal InformationSystem (IPPIS). Information system security officers must define measures for hardware procurement (including leasing), software development, information security function configuration, information security threats, and information system components in order to meet the security requirements of information systems. Information system security officers must examine the necessity of monitoring the information system for information security violation or threats, and formulate the necessary measures if it is deemed necessary.

There are various types of information systems, for example: transaction processing

systems, office system, decision support system, knowledge management systems, data management systems, and office information systems. Critical to most management are management technologies, which are typically designed to enable humans to perform tasks for which the human brain is not well suited, such as: handling large amounts of information, performing complex calculations, and controlling many simultaneous processes (Kock et al., 2002).

Today's information systems are complex collections of technology (i.e., hardware, software, and firmware), processes, and people, working together to provide organizations With the capability to process, store, and transmit information in a timely manner to support various missions and business functions. Information needs to be available, accurate and up-to-date to enable an organization make good business decisions. While various information security system frameworks have been implemented and adopted by organizations, the focus has been more on the use of technology as a means of securing information systems. However, information security needs to become an organisation-wide and strategic issue, taking it out of the information technology (IT) domain and aligning it with the corporate governance approach.

### **2.1.2 Conceptualization of standardized security design**

In general, security is "the quality or state of being secure to be free from danger. Information security design can be defined as a collection of policies concerned with Information Technology (IT) related risks or Information Security Management (ISM). Information Security design is a documented system that provides security for information and data in an organization. Every organization is faced with the task of providing a comprehensive plan for information security. Caralli & Wilson (2004) opined that modern organizations have a huge challenge on their hands as they must secure the organization in the face of increasing complexity, uncertainty, and interconnection brought about by an unprecedented reliance on technology vis-à-vis legislative policies on security". Carlson (2008) characterizes information security design as "coordinated activities to direct and control the preservation of confidentiality, integrity, and availability of information". He notes the concept of information security design thus: "information security designs an example of applying the management system conceptual model to the discipline of Information Security"

The framework within which an organization strives to meet its needs for information security is codified as security policy. A security policy is a concise statement, by those responsible for a system (e.g., senior management), of information values, protection responsibilities, and organizational commitment. One can implement that policy by taking specific

actions guided by management control principles and utilizing specific security standards, procedures, and mechanisms. Conversely, the selection of standards, procedures, and mechanisms should be guided by policy to be most effective.

To be useful, a security policy must not only state the security need (e.g., for confidentiality—that data shall be disclosed only to authorized individuals), but also address the range of circumstances under which that need must be met and the associated operating standards. Without this second part, a security policy is so general as to be useless (although the second part may be realized through procedures and standards set to implement the policy). In any particular circumstance, some threats are more probable than others, and a prudent policy setter must assess the threats, assign a level of concern to each, and state a policy in terms of which threats are to be resisted. For example, until recently most policies for security did not require that security needs be met in the face of a virus attack, because that form of attack was uncommon and not widely understood. As viruses have escalated from a hypothetical to a commonplace threat, it has become necessary to rethink such policies in regard to methods of distribution and acquisition of software. Implicit in this process is management's choice of a level of residual risk that it will live with, a level that varies among organizations.

The various steps involved in building an information system are:

**Step 1: Risk Assessment:** An organization-accepted security risk assessment should be done. The goal is to identify assets, threats, vulnerabilities and controls to mitigate risks. Some risks will be accepted and management approval should be attained on this.

**Step 2: Top-down approach:** Security is a management issue and not just an information technology issue. Hence it is critical that top management plays an important role in building an information security management system like educational information management system (EIMS). Education Management Information System is playing an important role in planning, decision making and monitoring of the schools but there are considerable limitations and challenges across EMIS cells in terms of the use of IT technologies in education management and decision making. Management should encourage a culture within the enterprise to follow security principles.

**Step 3: Functional roles:** Once the management's approval is attained, functional roles will have to be identified. Depending on the type and size of the enterprise, the roles can vary in type and number. A chief information security officer should be identified who solely owns the information security management system. Other functional roles could include Data stewards, Security awareness trainers etc.

**Step 4: Write the policy:** The security policy is a document that states the

organization's information security strategy at a high level. The language in the policy is derived from the risk assessment. In order to make the policy acceptable to all stakeholders, the manner in which the policy is expressed should be at a high level and align nicely with the organization's business priorities and goals.

**Step 5: Write the standards:** Standards are definite requirements that an organization should put forth for everybody to follow. The standards should support the security policy and be measurable. It is good practice to document what the penalties are when standards are not met.

**Step 6: Write the guidelines and procedures:** Guidelines are recommended ideas for an organization. It should be noted that the effectiveness of an organization's security management will not be measured by the guidelines present. Procedures are step by step description on how to meet the standards or guidelines so that the policy is supported. Procedures are usually targeted at the system level people who actually implement the control.

### 2.1.3 Frameworks for standardized security design

There are many standardized security design for information security management suitable for educational institution in Nigeria. There are:

**Inter-office communications system:** Inter-office Communications system electronically link all educational stakeholders irrespective of the level and office for sharing of files, reports,

important email messages, across the internet for fast operations of the organization. And an officer should be appointed to handle the affairs and security matters.

**Secondly, the BS7799 standard** that was released in 1999 by Li. et al. (2003). They presented this standard as a suitable model for information security. The BS7799 is based on a standard archived by best practices in the information security management area. Organizations have been using their own developed framework earlier. They have concluded that BS7799 together with organization-specific requirement is the most effective way of providing information security.

**Firewalls:** A firewall is a network security device that monitors incoming and outgoing network traffic and decides whether to allow or block specific traffic based on a defined set of security rules. Firewalls have been a first line of defense in network security for over 25 years. A firewall can be hardware, software, or both. A firewall basically allows a company to set up its own set of online rules for its users. Also, it allows a company to prevent its employees from visiting websites that are not trustworthy and can cause serious damage. Therefore, in this internet-driven era, if you don't have a firewall installed, then the chances are really high that your business might fall into the playground of hackers. Eg Bitdefender Box (Bitdefender Box is a firewall hardware that protects all kinds of smart devices. Once set up, the device blocks malware, prevents passwords from getting stolen, prevents

identity theft and hacker attacks for all internet-connected devices); CUJO AI Smart Internet Security (CUJO AI is a company that utilizes machine learning, data science and AI to provide

network operators with a multi-solution AI-driven software platform); The FortiGate Next Generation firewall by Fortinet is a high-performance network security device that prevents intruders from entering your network; Protectli is another firewall provider that has some of the best firewall devices in the industry.

**Virus protection programs:** these are internet virus that protects the information system from external access.

**Encryption:** Encryption is the process of encoding a message or information in such a way that only authorized parties can access it and those who are not authorized cannot. Encryption does not itself prevent interference but denies the intelligible content to a would-be interceptor. Encryption is a way of scrambling data so that only authorized parties can understand the information. In technical terms, it is the process of converting plaintext to ciphertext. In simpler terms, encryption takes readable data and alters it so that it appears random. Encryption requires the use of an encryption

**key:** a set of mathematical values that both the sender and the recipient of an

encrypted message know. The two main kinds of encryption are symmetric encryption and asymmetric encryption. Asymmetric encryption is also known as public

key encryption. In symmetric encryption, there is only one key, and all communicating parties use the same key for encryption and decryption. In asymmetric, or public key, encryption.

**Extensible mark-up language (XML):** Extensible Mark-up Language is a mark-up language that defines a set of rules for encoding documents in a format that is both human-readable and machine-readable. Eg XML encryption, XML digital signature and XML key management system.

#### 2.1.4 Security Design Objectives

Protect the company and its assets,

Manage Risks by identifying assets, discovering threats and estimating the risk,

Provide direction for security activities by framing of information security policies, procedures, standards, guidelines and baselines,

Information classification

Security organization and

Security education.

#### 2.1.5 Security Management Responsibilities

Determining objectives, scope and policies,

Evaluate business objectives, security risks, user productivity, and functionality requirements.

Define steps to ensure that all the above are accounted for and properly addressed.

#### 2.1.6 Major challenges of information security system

**Database Security:** The risk of data security is very high in each educational management information system cell as every individual computer is maintaining its own individual database. Analysis shows that the data is not secure from the virus and can change or alter attack; unauthorized personnel have access to data very easily the data because there is no secure password in 50% of the districts educational management information system Cells computers.

**Lack of Information Sharing:** Information and data is not completely shared among all the districts. Provincial educational management information system cell distributes annual statistical reports to all districts as a major source of information sharing. Districts do not have direct links with each other for valuable information sharing. If a district wants information about the other district, the request is forwarded to the Provincial educational management information system office where it is either fulfilled or denied if did not found in the central database.

**Non-Availability of adequate Information:** Annual Statistical Report developed and disseminated to all the districts consists of limited information/data, based on the perceived demands of the users/stakeholders results non availability and inadequacy of data/



information for planning and decision making at all level.

**Delay/Slow Data Dissemination Processed:**

Data is disseminated to all the districts inform of hard copy Annual Statistical Reports via physical medium, this process takes alot of time in distribution of reports to all the districts. Though report gets also available on the educational management information system intranet but due to unavailability of internet the districts have no access to it.

**Delays in Planning and Decision Making at District Level:**

At National level, educational management information system is playing significant role in generating targets for policy framework and decisionmaking but at decentralized level educational management information system is not as good as at National level due to lack of capacity constraints and delay in transmission of desired data.

**Internet Adoptability and Accessibility:**

The use of internet as a method of communication has not been widely adopted in most District educational management information system cells. Majority of the Districts educational management information system cells have internet availability and accessibility.

**2.1.7 Condition necessary for standardized security design in Nigerian educational sector**

**Confidentiality:** Confidentiality is a requirement whose purpose is to keep sensitive information from being disclosed to unauthorized recipients. The secrets might be

important for reasons of national security (nuclear weapons data), law enforcement (the identities of undercover drug agents), competitive advantage (manufacturing costs or bidding plans), or personal privacy (credit histories). **Integrity:** Integrity is a requirement meant to ensure that information and programs are changed only in a specified and authorized manner. It may be important to keep data consistent or to allow data to be changed only in an approved manner.

**Availability:** Availability is a requirement intended to ensure that systems work promptly and service is not denied to authorize users. From an operational standpoint, this requirement refers to adequate response time and/or guaranteed bandwidth. From a security standpoint, it represents the ability to protect against and recover from a damaging event.

**2.2 Theoretical framework**

Thecla, Chinelo (2020), investigated on management of information security in public universities in Nigeria. They discovered that education information stores immense amount of information which they rely on for effective and hitch free running of their operation.

HuseinAdul-Hamed (2014), examined what matters most for education management system; the study x-rays for policy areas; specifically, enabling environment, system soundness, data quality and utilization of decision making. The study employed situation analysis he found out that management information system is set to use

information generated to improve operational efficiency and educational quality.

Amannah&Ahiakwo(2013) examined Systematic Approach to the Improving Standard of Nigeria Educational System. *The paper examines the root cause of the falling standard of the Nigeria educational system and the rightful solution to these problems. Education is the bedrock of development, but unfortunately, education in Nigeria is bisected with myriads of problems. These include: poor actualise the policies of 14 civilian Presidents and military Heads of States. Many of these policies were laudable. This study also employed situation analysis.*

Al-Awadi and Renaud (2016) opine that information is an asset, and having specific, relevant and correct information can make a massive difference to an organization's efficiency. In view of these reasons, these assets being of utmost importance need to be securely stored and managed. Managing accounts can be laborious, to make this easier, it can be automated. Information security has been established as a core support for mission of organizations and so, would require a comprehensive and integrated approach that will involve both management and staff of organizations.

Due to the fact that there is a great premium attached to the information asset of these organizations, they are vulnerable to the risk of threats from unauthorized persons and entity. Risk in the context of information

security is the outcome the business faces when a threat exploits a vulnerability to successfully attack a target that is being defended

Okpanem (2013) asserts that the only true security system is one that is powered off, cast in a block of concrete and sealed in a lead-lined room with armed guards- and even then there are still doubts. Bearing this in mind therefore, it behooves on the institutions to devise means of managing information security most appropriately. Threats are continually evolving such as spam mails, identity thefts, phishing, data leakage and many more. The primary role of an information security manager is to identify, manage and mitigate security risks on behalf of the organization. In addition to the manager's technical competences, it is also important that the role is carried out within set principles and regulations in order to be able to understand what is, and how it is, allowable by law to carry out this function. Campbell opines that most information security managers in executing their roles, build a process framework known as information security management system (ISMS) that integrates corporate policy with legislation and compliance requirements, linking in external process, procedures and records.

### 3.1 RESEARCH METHODS

This study made use of an interview survey method in gathering data. The interview method involves questioning and discussing issues with insurance practitioners with respect to standardized security design and information system in Nigeria educational institution. This technique has been seen to be very useful in gathering such data which would likely not be accessible using techniques such as observation or questionnaire [Blaxter, Hughes, Tight, 2006]. The interview is scheduled and structured; and advantageous because of its ability to generally produce fewer incomplete questionnaires, achieve higher completion rates than self-administered questionnaires, and more effective for complicated issues (Babbie , 2005 and Osuala, 2005). The views of respective respondents were coded to improve the completion of the interview scheduled which was drawn using a Likert-type scale measurement of ‘Strongly Agree’, ‘Partially Agree’, ‘Not Agree’.

The research adopted a survey design and that which was exploratory in nature. The involvement of survey design was because of its ability to predict behaviour and help in gathering the same information about all the cases in a sample [Aldridge, Levine, 2005]. This study employed a judgmental sampling technique because it helped select the unit(s) to be observed on the basis of the researchers’ knowledge or judgement of the population, its element and purpose of the study. In a bid to gather relevant information for the study, a

predetermined interview schedule was designed to few selected education institutions in Owerri Imo State, which informed the selection of the surveyed institution. This study thus chooses 3 institution in Imo state; e.g Imo State University, Federal Polytechnic Nekede and AlvanIkoku College of Education the respondents were per institutions.

The questionnaire raised was coded to generate parameters that will fit into multiple regression analysis via ordinary least square method of estimation.

### 3.2 Model specification

$$Y_i = \beta_0 + \beta_1 X_{1i} + \beta_2 X_{2i} + \beta_3 X_{3i} + \beta_4 X_{4i} + \mu$$

$Y=1$ , if the respondents uses information system in their institution and 0 if otherwise.

$X_1$ = inter-office

$X_2$ = firewalls

$X_3$ = virus protection programmes

$X_4$ = encryption

$\mu$  = Error term.

The main instrument to be used in sourcing the required data is structured questionnaire. The questionnaire is designed and administered to the purposely selected respondents from respondent.

### 3.3 Decision Rule

At 5% level of significance using t-statistics for the hypotheses tests, the decision to accept or reject the null hypothesis will be based on the following rules:

**Accept null hypothesis ( $H_0$ ) and reject alternative (HA) if:** P-value > 0.05 which would indicate a case no significant effect, impact or relationship. **OR**

**Reject null hypothesis ( $H_0$ ) and accept alternative (HA) if:** P-value < 0.05 which would indicate a case significant effect, impact or relationship.

#### 4.1 Data Analysis and Interpretation

The questionnaire generated were coded to fit in to regression analysis, so as to determine the effect of standardized security design on information system in Nigeria educational institution

**Table 4.1 Model Summary**

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.867 <sup>a</sup>	.771	.003	.326

R<sup>2</sup> also known as coefficient of determination was obtained as 77.1% which implies that the generated data from field survey strongly determine standardized security design on information system in Nigeria educational institution to the tune of 77.1%

**Table 4.2 Coefficients<sup>a</sup>**

Model	Unstandardized Coefficients		Standardized Coefficients	T	Sig.	95.0% Confidence Interval for B	
	B	Std. Error	Beta			Lower Bound	Upper Bound
(Constant)	.874	.224		3.894	.000	.423	1.325
1 IOC	.115	.006	.259	19.166	.000	.017	.247
VPP	.012	.009	.028	1.333	.845	.106	.130
ENT	.039	.004	.127	-9.750	.000	.127	.049
FW	.058	.007	.128	8.256	.000	.077	.194

**H<sub>0</sub>:** there is no significant relationship between inter-office communication and information system in Nigeria education institution.

Table 4.2 shows that the intercept ( $\beta_0$ ) of the models is positive at .874. These indicate that when the independent variables in the model is zero, the dependent variables (Standardize security design) will be positive to the tune of 0.874. The table also reveals that  $\beta_1$  (the coefficient of inter-office communication) is

positive at .115, these indicate that the first independent variable (inter-office communication) has positive effect on dependent variables (Standardize security design). However, the table also reveals  $\beta_2$  (the coefficient of the second independent variables) is positive at .058. The implication is the second independent variable (firewalls) also exerts a positive effect on information system in Nigeria education institution.

The coefficient of virus protection and Encryption was obtained as .012 and 0.039

which are positively signed and directly related to information system in Nigeria education institution.

The table also reveals that changes in the independent variables account for about 77.1% changes in information system in Nigeria education institution.

#### 4.2 Test for Significance and Decisions on the Hypotheses of the Study

The t-statistics results from the regression analysis as shown in appendix 2 are summarized in the following table 4.2.

**H1:** there is no significant relationship between inter-office communication and information system in Nigeria education institution.

The above table 4.2 revealed inter-office communication p-value as 0.000 (i.e.  $p < 0.05$ ); indicating a significant effect exists between the independent variable (inter-office communication) and information system in Nigeria education institution. The study thus holds the null hypothesis to be false and affirm that the inter-office communications significantly affects information system in Nigeria education institution.

**H2:** there is no significant relationship between firewalls and information system in Nigeria education institution.

Table 4.2 further reveals that the p-value in respect of firewall is .000 ( $P > 0.05$ ) which also shows a significant effect of the dependent variable (information system in Nigeria education institution). The null hypothesis is rejected and the alternative accepted. We thus affirm that firewall has

significant effect on information system in Nigeria education institution.

**H3:** there is no significant relationship virus protection and information system in Nigeria education institution.

The estimated slope for virus protection revealed p-value of .845 ( $P > 0.05$ ) showing an insignificant relationship with information system in Nigeria education institution. The null hypothesis is accepted and the alternative rejected. We thus affirm that virus protection has significant effect on information system in Nigeria education institution.

**H4:** there is no significant relationship encryption and information system in Nigeria education institution.

The estimated parameter for encryption revealed p-value of .000 ( $P < 0.05$ ); indicating a significant effect exists between the independent variable (encryption) and information system in Nigeria education institution. The study thus holds the null hypothesis to be false and affirm that the encryption significantly affects information system in Nigeria education institution.

#### 4.3 Discussion of Findings

From the results analysis carried out in this chapter as summarized in tables 4.2; the following findings are made:

The finding from the analysis in relation to the first objective and hypothesis indicated that the inter-office communication shows positive significant effect on information system in Nigeria education institution.

The findings from the analysis in respect of the second objective of this study show that firewalls have a significant effect information system in Nigeria education institution.

The study also revealed that virus protection has an insignificant effect with information system in Nigeria education institution which

led to the rejection of the alternative hypothesis.

The parameter with respect to objective four show that encryption significant affect information system in Nigeria education institution

### 5.1 Conclusion

In conclusion, information system which is also known as computer-based information system, is important in Nigerian educational systems at all levels because of its transaction process systems, knowledge management systems and information technologies designed to enable individual persons to perform task for which the human brain is not well suited. In addition, the organization of a data system with national coverage is very complex. Studies have shown that there is need for every educational institution in Nigeria to accommodate the use of an information security management system in its operation. The currently existing frameworks for this system have centered much on the use of technology as a means of securing information systems. There is need for information security to become widespread so much so that strategic issues be expunged from the IT domain and aligned with corporate governance approach.

### 5.2 Recommendation

The following recommendations were proffered as follows;

1. In view of the observed inadequacies in the present policy document there is the need to revise the document. Such revision should be undertaken to involve stakeholders in the area of education so that they can ensure that the policy cover issues related to learning about ICT and learning through ICT.
2. Furthermore, the objectives in sectorial application areas should address education specifically in order

to broaden the market driven objectives. The integration of ICT into every aspect of teaching and learning should also be the key focus.

3. Although the issue of infrastructure is implicit in the present policy it should be reviewed in such a way that access policy is addressed in concrete terms, since this is important in ICT integration.
4. Given the importance of ICT integration in education, the national policy on IT should address the issue of institutions professional development. This should incorporate issues relating to teacher training institutions and ICT, pre-service teacher education, in-service teacher education, and standards for teacher competence and certification in ICT.
5. Also, research, evaluation, and assessment are critical for ICT usage in education. In this context, the national policy should identify a frame of reference in order to gauge success of ICT application in education, such a frame of reference will encourage refinement of school practices relating to ICT integration.

## References

- Al-Awadi, M & Renaud, K. (2016). Success factors in information security implementation in organizations. <http://www.semanticscholar.org/6aff/eddfdfdiadcf737184ffd887602007afod.pdf>
- Amannah, P.I.&Ahiakwo, M.J (2013) Systematic Approach to the Improving Standard of Nigeria Educational System An International *Multidisciplinary Journal, Ethiopia Vol. 7 (4), Serial No. 31, September, 2013:252-264* .ISSN 1994-9057 (Print
- Atzori, L., A. Iera, & G. Morabito, (2010). The internet of things: A survey, in *computernetworks*,54(15), 2787-2805.
- Blaxter L, Hughes C, Tight M. How to Research. 3<sup>rd</sup> Ed. Berkshire: Open University Press; 2006.
- Babbie E. (2005) *The Basics of Social Research*. 3<sup>rd</sup> Ed. Canada: Thomson Learning Inc.
- Bryczynski, B. & Small B. (2003). Securing your organization's information assets. Retrieved from 10.1.1.177.8675
- Caralli, R. A. & Wilson, W. R. (2004). The challenges of security management. Retrieved from ESM
- Campbell, T. (2016). *Practical information security measurement*. Appress. Australia.  
White Paper v1.0 Final-2.doc
- Carlson, T. (2008). *Understanding information security management systems*. New York: Auerbach Publications
- Davis.. G.B. & M.H. Olson., (1985). *Management information system: Conceptual, foundations, structure and development*. 2nd ed. New York.: McGraw-Hill.
- Hua, H. and J. Herstein, (2003). *Education management information system (EMIS): Integrated data and information systems and their implications in educational management*, in Annual Conference of Comparative and International Education Society. New Orleans, LA USA.
- HuseinAdul-Hamed (2014), *What Matters Most for Education Management Information Systems: A Framework Paper*. SABER working paper series No.7
- Jing. Q., A. Vasilakos, J. Wan, J. Lu, and D. Qiu, (2014). *Security of the internet of things: Perspectives and challenges*, "in wireless networks, Springer, 20(8), 2481-2501.
- Kock N, Gray P, Hoving R, Klein H, Myres M, Rockart(2002). *Information systems research relevance Revisited: Subtle accomplishment, unfulfilled promise, or serialhypocrisy?* Communications of the Association for Information Systems, 8(23), 330-346.
- Li et. al, (2003). BS7799: A suitable model for information security management.
- McLeod, R., (1995). *Management information systems: A study of computer-based information systems* 6th ed. New Delhi.: Prentice Hall of India. Parenty, T. (2019). *Digital Defense*. Boston, Massachusetts: Harvard Business School Press.

- Okpanem (2013V., (2017). An Introduction to Information Security. NIST Special Publication 800-12 Revision 1, <https://doi.org/10.6028/NIST.SP.800-12r1>.
- Pattinson,. F. (2007). Certifying information security managementsystems.Retrieved from<http://www.atsec.com/download/s/pdf/CertifyingISMS.pdf>(2003).Americas Conference on Information Systems.Pattinson,M.R.
- Ricky S. Anedo, m., (2003). Non-formal education management information system, P.M.O.II, Editor, Bureau of Non-formal Education-Department of Education, Culture andScience (BNFE-DECS): Philippines.
- Siponen. M. T. (2000). A conceptual foundation for organizational information securityawareness.Information Management & Computer Security, 8 (1), 31-41.
- Tejay. G. 2005). Making sense of information systems security standards, Americasconference on Information Systems.
- Thecla, A.E Chinelo, C.A (2020), Management of Information Security in Public Universities in Nigeria; *Enugu State University of Science and Technology, Nigeria University of Hull, UK*
- Wako, T.N., (2003). Education management information systems (EMIS): A guide for youngmanagers, ed. NESIS/UNESCO. 2003, Harare, Zimbabwe.



# ICT PARKS AND DIGITAL LITERACY IN NIGERIA

**Eleberi Ebele Leticia**

**Department of Computer Science**

[Ebyfav2001@yahoo.com](mailto:Ebyfav2001@yahoo.com)

*Abstract*

*This paper investigates on ICT parks and digital literacy in Nigeria. The paper disaggregated information communication technology into Wifi, Mobile phone and social media as explanatory variables while digital literacy remains the dependent variable. Data were generated via Primary source through the use of a structured questionnaire and analysed through analysis of variance. The study found that WiFi, Mobile phone and social media has significant effect on digital literacy, it was observed that government should enhance the range of coverage of WiFi, since WiFi security protocols prevent unauthorized access or damage to computers using wireless networks*

**Keywords** Information Communication Technology, WiFi, Digital literacy,

## **1.1 Introduction**

The importance of ICT in our present world cannot be overemphasized and Education being the backbone of any nation is not left out at all level, this implies that education that is innovative and resource-based produces graduates who will lead the nation forward. To achieve this, there must be a move from conventional methods of teaching, learning, and research to current methods, which requires the use of ICT as a new technology that presents potential for enhanced personnel development. College lecturers are the foundational personnel of educational institutions, and they make significant contributions to the achievement of institutional goals. With the rise of ICT, college instructors now have a plethora of possibilities for teaching and learning.

Any form of learning that recognizes ICT is a crucial is as a method of educating college undergraduate students for the knowledge economy in the twenty-first century, since learners are now exposed to varied technologies and are now referred to be "digital natives" (Kumari & D'Souza, 2016). It is no secret that ICT has taken over modern life, and there is general acceptance of the necessity to employ ICT in higher education institutions as we enter the era of globalization, when the free flow of information via satellite and the internet holds sway in global knowledge distribution.

The use of technology in teaching and learning is quickly becoming one of the most significant and highly debated problems in modern educational policy (Thierer, 2000). Most education professionals agreed that, when utilized appropriately, ICT has significant promise for improving teaching and learning as well as influencing job possibilities. Kolawale (2008)

describes ICT as "technology that assist us in recording, storing, processing, retrieving, transferring, and disseminating recorded information."

This means that the user and the data are interacting. As a result, information and communication technology is a broad phrase that encompasses any communication device used for teaching and learning. This type of gadget could be

Computer system, communication device, telecommunication, phone, satellites, telex, facsimile, internet, email, fax, video text and document delivery, electronic copiers, radio, television, and so on. According to Olakule (2014), these networks connect schools, families, businesses, students, and hospitals, facilitating teaching and learning.

Previous academics characterized digital literacy as a collection of complex and linked subdisciplines that include skill, knowledge, ethics, and creative outputs in the digital network environment (Calvani, Cartelli, Fini& Ranieri, 2008; Covello, 2010). Thus, digital literacy entails more than merely incorporating technology into the classroom; it entails using technology to comprehend and create modern communication, to situate oneself in the digital realm, and to manage knowledge and experience in the information age for the benefit of students. As a result, the purpose of this research tends to investigate the ICT parks on digital literacy in Nigeria.

## **1.2 Statement of problems**

ICT has been a transformational instrument in the educational sector, transforming classroom instruction to virtual learning in developed countries as a result of the ICT and digital literacy abilities carried by university and college of education teachers. However, in developing nations such as Nigeria, the application of ICT to the teaching and learning process is still in its infancy, with college of education lecturers having little or no digital literacy capability (Ebele, Ejedafiru, & Oghenetega, 2013). This is having a negative impact on the entire educational growth of university students, as university education is the pinnacle of educational levels in developing a literate individual, who would then change society into a literate society. As a result, the purpose of this research is to investigate on the effective use of ICT parkson digital literacy in Nigeria.

## **1.3 Objective of the study**

The main objective of this paper is to investigate on ICT parks and digital literacy in Nigeria; the study will specifically achieve the following;

1. ascertain the importance of Wi-fi on digital literacy in Nigeria
2. determine the effect of mobile phone on digital literacy in Nigeria
3. examine the effect of social media on digital literacy in Nigeria

#### **1.4 Research questions**

This paper is guided by the following research questions;

1. what is the importance of Wi-Fi on digital literacy in Nigeria?
2. what effect has mobile phone on digital literacy in Nigeria?
3. to what extent has social media affected digital literacy in Nigeria?

#### **1.5 Research Hypotheses**

**H<sub>01</sub>:** Wi-Fi has no significant effect on digital literacy in Nigeria.

**H<sub>02</sub>:** Mobile phone has no significant effect on digital literacy in Nigeria.

**H<sub>03</sub>:** Social media has no significant effect on digital literacy in Nigeria.

#### **1.6 Scope of the study**

The content scope of this study is to investigate on ICT parks and digital literacy: the Nigeria experience. The research adopts Imo state as the study area where questionnaires constructed will be distributed to customers of banks and telecommunication on their literate usage level of Wifi, mobile phone and social media.

## **2.0 Review of related literature**

### **2.1 concept of social media**

According to Jimmie (2014) Social media is the term often used to refer to new forms of media that involve interactive participation. Often the development of media is divided into two different ages, the broadcast age and the interactive age. In the broadcast age, media were almost exclusively centralized where one entity such as a radio or television station,

newspaper company, or a movie production studio distributed messages to many people. Feedback to media outlets was often indirect, delayed, and impersonal. Mediated communication between individuals typically happened on a much smaller level, usually via personal letters, telephone calls, or sometimes on a slightly larger scale through means such as photocopied family newsletters. With the rise of digital and mobile technologies, interaction on a large scale became easier for individuals than ever before; and as such, a new media age was born where interactivity was placed at the center of new media functions. One individual could now speak to many, and instant feedback was a possibility. Where citizens and consumers used to have limited and somewhat muted voices, now they could share their opinions with many. The low cost and accessibility of new technology also allowed more options for media consumption than ever before – and so instead of only a few news outlets, individuals now have the ability to seek information from several sources and to dialogue with others via message forums about the information posted. At the core of this ongoing revolution is social media. The characteristics, common forms, and common functions of social media are explored here.

All social media involve some sort of digital platform, whether that be mobile or stationary. Not everything that is digital, however, is necessarily social media. Two common characteristics help to define social media. First, social media allow some form of participation. Social media are never completely passive, even if sometimes social networking sites such as Facebook may allow passive viewing of what others are posting. Usually, at bare minimum, a profile must be created that allows for the beginning of the potential for interaction. That quality in and of itself sets social media apart from traditional media where personal profiles are not the norm. Second, and in line with their participatory nature, social media involve interaction. This interaction can be with established friends, family, or acquaintances or with new people who share common interests or even a common acquaintance circle. Although many social media were or are initially treated or referred to as novel, as they continue to be integrated into personal and professional lives they become less noticed and more expected Jimmie (2014).

Forms As this overview of common forms of social media demonstrates, some are used primarily for recreation or personal connections, others for work or professional reasons, but most allow leeway for both.

Email. Probably the most common form of social media used in everyday life, email (short for electronic mail) involves users logging into an account in order to send and receive messages to other users. Anyone who sends or receives an email must have an account. Many options for free email accounts are available via the World Wide Web, but many times internet service providers will also offer free email accounts with service packages or employers will offer email addresses to their employees. Most workplaces have strict rules about how email accounts can be used, although many organizations report that they have no specific email training. Those who work for public organizations (including politicians, professors at state universities, and administrators and assistants for government offices) are often subject to open records laws that will allow interested people or organizations to request any emails sent or received to a government funded email account or an email account used to conduct government business.

**Texters.** Similar to email, a texter is a two-way communication channel that allows individuals to quickly send a message to another person or a group of people. Although media portrayals often make it look as if texting is a particularly youthful behavior, people of all ages have adapted to texting. Still, younger individuals tend to text more often and usually do so at a faster speed. As texting technology has improved, it is easier to text photos or to copy and paste links into texters in order to share them with others. Texters often make use of emoticons, the use of keyboard characters to make pictures such as a smiley face (e.g., :-P), a practice that is also common with email. Texters are derived from chatters, or computer programs that make use of the internet to allow people to quickly talk back and forth via text characters. Although the use of texting is often highly convenient and allows many benefits, particular attention has been paid to two texting behaviors that has led to problems: texting while driving and sexting. It is estimated that texting while driving makes a car crash almost 23% more likely. Sexting is mostly harmful when adolescent children share pictures that are later redistributed to others by the receiver. In some cases, those forwarding pictures of people under the age of 18 have been charged with child pornography. Politicians have faced scrutiny for sharing sexual messages with others, including interns. Despite these problematic

potentials, many adults report that sexting is a satisfying alternative to sexual interaction when they are away from their partners.

**Blogs.** The word blog is derived from the word weblog. A blog is a webpage where an individual or group can share information or ideas with a large group of people via the internet. It is not uncommon for a person to start a blog and then never update it again. Some of the most successful blogs are updated on a regular basis so the followers of the blog can know when to expect new entries. Blogs cover a wide range of topics, including political issues of all kinds. A common feature to blogs is a feedback forum where, after reading an entry, people can interact with both the blog author and others who have commented. Many traditional media outlets have adopted blog-like features online in order to entice readers to continue sticking with their news or entertainment offerings. For example, many newspaper stories end with the opportunity for readers to share their thoughts or comments about a current issue. These news stories— especially when about hot or particularly partisan political issues—can lead to serious debates. Because of the contentious nature many blogs and news outlets find, it is not uncommon for a user to be required to register in order to participate.

**Connection sites.** Online dating is another form of social media. Users approach online dating sites—some that require paid membership and others that are free of charge—and create a profile that tells who they are and what they seek in a relationship. Some may be skeptical about how honest some are about the information displayed in an online profile, but research shows that people are generally honest. The stigma placed upon online dating sites has continued to diminish as more people continue to use them in order to meet dating partners. In addition to dating, others may use connection sites to find friends or activity partners. For example, the connection site Meet Up allows users to find activist groups, book clubs, or hobby circles. Users enter a profile, and then they can even send messages to meet up group leaders in order to learn more about the activity or see if they would make a good fit for the group.

**Social networking sites.** Facebook and other social networking sites are almost ubiquitous features in contemporary culture. Even those who choose not to create an online profile and participate will often hear from others information gained from such social platforms. A key distinguishing feature that makes a social networking site is the fellow list of users that one connects with, usually based upon friendship, family, work relationships, or even weak tie relationships. Initially social networking sites were great ways to meet new people, and although that is still a possibility many social networking sites now discourage people from adding connections they do not know. The public nature of information posted to social networking sites often allow a space for social or political viewpoints to be displayed, although research suggests much of this political activity reinforces pre-existing beliefs – especially because people tend to be online friends with those that are most like them.

### **2.1.2 The concept of Wifi**

WiFi stands for Wireless Fidelity. This term was coined by a branding company, and it only caught on in its abbreviated form. It describes a technology for radio wireless local area networking of devices based on the IEEE 802.11 standards, which are maintained by the Institute of Electrical and Electronics Engineers (IEEE) LAN/MAN Standards Committee (IEEE 802).

The first version of the IEEE 802.11 standards was released in 1997, but their origin dates to 1985 and the release of the ISM band for unlicensed use by the U.S. Federal Communications Commission. Today, multiple revisions of the IEEE 802.11 standards are in use, which is possible thanks to the backward compatibility of IEEE 802.11 hardware.

Similar to the traditional transistor radio, WiFi networks transmit information over the air using radio waves, which are a type of electromagnetic radiation with wavelengths in the electromagnetic spectrum longer than infrared light.

WiFi radio waves typically have the frequency of either 2.4 gigahertz or 5.8 gigahertz. These two WiFi frequency bands are then subdivided into multiple channels, with each channel possibly being shared by many different networks.

When you download a file over a WiFi network, a device known as a wireless router first receives the data from the internet via your broadband internet connection and then converts it into radio waves. The wireless router then emits the radio waves to the surrounding area, and the wireless device that has initiated the download request captures them and decodes them.

Because WiFi depends on radio waves, WiFi networks can be disrupted by interference caused by other WiFi networks or various electronic appliances, including microwave ovens, cordless telephones, refrigerators, televisions, transistor radios, or Bluetooth devices.

To ensure optimal WiFi performance, network administrators often rely on WiFi analyzers such as NetSpot to visualize, manage, and troubleshoot WiFi connections. NetSpot can generate a comprehensive visual map of WiFi networks, highlight areas of signal weakness, and reveal potential causes of interference. In the current era of omnipresent WiFi networks, a tool like NetSpot is indispensable even when setting up a basic WiFi home network.

### **Most Important WiFi Terminology**

Now that we've explained what WiFi stands for and provided you with a widely accepted WiFi definition, it's time to take a closer look at some of the most important WiFi terminology. As you can probably imagine, we can only scratch the surface of the IEEE 802.11 standard here, but knowing the terms described below should be enough to help you make wise purchasing decisions when buying a new WiFi router or selecting a new internet provider.

### **Wi-Fi Radio Spectrum**

#### **802.11 Networking Standards**



## **WiFi Security Protocols**

### **Wi-Fi Radio Spectrum**

As we've already mentioned, WiFi is transmitted at the 2.4 GHz and 5 GHz frequencies. In North America, the 2.4 GHz band is divided into 11 channels, with channels 1, 6, and 11 being non-overlapping. The 5 GHz band is divided into a much larger number of channels, with each country applying its own regulations to the allowable channels.

The biggest difference between the two frequency bands is the fact that the 5 GHz signal is only about half the range of the 2.4 GHz signal. What's worse, it has more trouble penetrating walls and solid objects. On the other hand, the 5 GHz band is far less crowded than the 2.4 GHz band, which is a huge advantage in heavily populated urban areas where WiFi networks are virtually everywhere.

### **802.11 Networking Standards**

Most modern WiFi routers support the 802.11ac networking standard, which has a multi-station throughput of at least 1 gigabit per second and single-link throughput of at least 500 megabits per second (500 Mbit/s).

Many older WiFi routers only support the 802.11n networking standard, which has a maximum net data rate of 600 Mbit/s, and some even only support the 802.11g networking standard, which has a maximum net data rate of just 54 Mbit/s.

Since 802.11 networking standards are backward compatible, there's no reason not to purchase a router that supports the latest 802.11n networking standard, which is 802.11ac.

## **WiFi Security Protocols**

WiFi security protocols prevent unauthorized access or damage to computers using wireless networks. The most basic wireless security is Wired Equivalent Privacy (WEP). It was ratified in 1997 and declared deprecated in 2004 because of its security limitations.

WEP was superseded by Wi-Fi Protected Access (WPA) and Wi-Fi Protected Access II (WPA2), which became available in 2003 and 2004 respectively. Soon, WPA2 will be superseded by WPA3, which uses even stronger encryption and mitigates security issues posed by weak passwords.

### **2.1.3 The concept of mobile phone**

Mobile phone data, like GPS data, is passively collected. However, mobile phone datasets have distinct characteristics compared to GPS datasets. Mobile phone data contains location information at much coarser temporal resolution than GPS data. As reviewed by Chen, Ma, Susilo, Liu, and Wang (2016), there are two types of mobile phone data: call detail record (CDR) data and sightings data. These two data types differ in temporal resolution, spatial resolution, and user interactions. Sightings data has higher temporal and spatial resolutions but is not based on user interactions as the case for CDR data. Due to its relatively low temporal and spatial resolutions, the most intuitive application of mobile phone data is to infer trip rates and OD pairs in studying mobility patterns. However, recent advances have demonstrated inferred travel times (Toole et al., 2015) and modes (Wang, He, & Leung, 2018).

Mobile phones have played an important role in people's lives. They have not only been used as a communication device but also served as a sensing device to collect information from its users (Lane et al., 2010). Mainly types of user information: (1) mobile phone usage, and (2)

spatiotemporal traces. In this subsection, we discuss the mobile phone technologies that enable the generation of spatiotemporal traces of users. There are mainly four location systems that can record mobile phone users' spatiotemporal traces: (1) cellular-network-based positioning system (Demissie et al., 2013), (2) GPS positioning system (Wolf et al., 2004), (3) Wi-Fi positioning system (Danalet et al., 2016), and (4) Bluetooth positioning system (Delafontaine et al., 2012). In this chapter, we limit our scope to cellular-network-based positioning system, which generates the most widely applied type of mobile phone data in travel behavior research (Wang et al., 2017).

Mobile phones are able to communicate with each other and connect to the mobile internet, based on cellular networks composed of transceivers that cover their respective land areas. With the movement of a mobile phone, it searches and connects to the nearest transceiver. This process is known as mobile phone positioning (Chen et al., 2016). Positioning data about such connections between users and transceivers are recorded mostly for cellular network operators' own purposes (e.g., billing), which are often not related to transportation, whilst as a by-product, they have been utilized by urban decision makers and researchers to estimate and understand mobility patterns (Wang and Chen, 2018). Because such data are in terms of spatiotemporal traces, researchers named them as mobile phone traces (Jiang et al., 2013a).

Mobile phone traces can be categorized into event-driven traces and network-driven traces (Pinelli et al., 2015). Call detail records and records of internet connections belong to the former one since the production of these data is triggered by user events, including usage of calls, SMS, and internet (Pinelli et al., 2015). Network-driven data are generated regardless whether people are using phones, but either in a periodic way or when a phone moves between two areas. Due to the nature of event-driven traces, their sampling is usually infrequent and could be biased to specific locations, e.g., home locations, and times, e.g.,

during the evenings; on the other hand, the sampling rate of network-driven traces is relatively higher and stable over time (Calabrese et al., 2014).

Spatial inaccuracy has always been an issue if mobile phone traces are used to estimate locations and represent individual mobility (Ahas et al., 2007). There are mainly two causes: (1) the difference between the actual location of a user and the location of the transceiver that the user is connecting to, and (2) the possibility of a user switching the connection between towers due to signal jumps even if the user is not moving (Alexander et al., 2015; Wang and Chen, 2018). To solve the first problem, the simplest way is to regard the transceiver's location or its Voronoi cell as a proxy for the user's location (Montjoye and Smoreda, 2014). Some telecom providers can estimate locations with a higher accuracy based on triangulation with several factors including the number of surrounding cells and received signal strength. The accuracy can reach about 100–500 m in urban areas and 400–10,000 m in rural areas, reported in a Chinese study (Wang et al., 2017b). Qi et al. (2016) named the second problem as the oscillation problem, to which Wang and Chen (2018) have presented an in-depth review on the solutions, including heuristic rules, spatiotemporal clustering, etc. Those algorithms can be used to pre-process mobile phone traces before conducting activity-travel behaviour analysis.

### **3.0 Methodology**

Survey research was adopted for this study. The total population for this study comprised of 50 bank customers and 70 telecommunication users across the three major networks in Nigeria. The data collected for this study was analysed using simple percentage frequency counts and analysis of variance. The composition of the sample size is presented in the table below.

The area of coverage of the research is Imo state capturing bank customers and telecommunication users within the state were generated questionnaires distributed accordingly. The population for the study captures the under listed departments

S/N	Population of the study
Bank Customers	85
Telecom Customers	97
Total	182

**Source: Field Survey, 2021**

From the population of the study, the sample size is determined using Taro Yamen formula below;

$$n = \frac{N}{1 + N(e)^2}$$

Where n = sample size

N = population size

1 = constant figure

e = marginal error of 0.05 or 5%

$$\begin{aligned}
 n &= \frac{182}{1 + 182(0.05)^2} \\
 &= \frac{182}{1 + 182(0.0025)} \\
 &= \frac{182}{1.456} \\
 &= 125
 \end{aligned}$$

### 3.1 Description of Analytical tool

In the tool’s analysis of the research, information will first be edited in order to ascertain their completeness and consistency, the data are then classified and tabulated which later will be followed by the analysis and interpretation of data.

However, only relevant and important questions were considered and analyzed. The analysis of variance statistical techniques will be used for a meaningful, reliable and easy inference.

According to Egbulonu and Nwachukwu (2000) to test the hypothesis regarding equality of population means, we will use the sum of squares of the three types of variance namely;

1. Total Sum of Square (TSS)
2. Treatment Sum of Square (TRSS)
3. Error Sum of Square (ESS)

Where  $TSS = TRSS + ESS$

**Decision rule**

We then look at the f-table for the critical value of the test, with r-1 and n-r degrees of freedom in the table, r-1 is for the numerator and n-e for the denominator degrees of freedom. The f-distribution.

The null hypothesis is rejected and the alternative accepted is our calculated F value is greater than value found from the table. Otherwise, the null hypothesis is accepted.

The ANOVA calculation performed above

Source of variation	SS	DF	MS	F-Value
Between samples (treatment)	TRSS	r-1	$\frac{TRSS}{r-1}$	$\frac{TRMS}{EMS}$
Within samples (error)	ESS	n-r	$\frac{ESS}{n-1}$	
Total	TSS	n-1		

**4.1 Data analysis and interpretation of result**

**Presentation of data: on the effect of Wifi in digital literacy in Nigeria**

	Frequency	Percent	Valid Percent	Cumulative Percent
SA	39	31.2	31.2	31.2
A	40	32.0	32.0	63.2
Valid DA	24	19.2	19.2	82.4
SDA	22	17.6	17.6	100.0
Total	125	100.0	100.0	

**Source: SPSS result output, 2021**

The above table shows that 39 representing 31.2% of the respondent are he view that have sufficient knowledge on the usage of wifi, 40 representing 32.2 support the view while 24, 22 of the respondent representing 19.2 and 17.6 respectively are of the opinion that they do not have sufficient knowledge of the use of Wifi.

**Descriptive Statistics**

	N	Minimum	Maximum	Mean	Std. Deviation
WHAT IS THE EFFECT OF WIFI IN DIGITAL LITERACY IN NIGERIA	125	1.00	4.00	2.2320	1.07865
Valid N (listwise)	125				

**Source: SPSS result output, 2021**

The mean value and its corresponding standard deviation for the above responds was obtained as 2.2320 and 1.07865 respectively. The mean value cut across the average agreement level of the respondent, indicating that majority of the respondent have sufficient knowledge of the use of Wifi.

**Presentation of data: on the effect of MOBILE PHONE on DIGITAL LITERACY**

	Frequency	Percent	Valid Percent	Cumulative Percent
SA	51	40.8	40.8	40.8
A	23	18.4	18.4	59.2
Valid DA	26	20.8	20.8	80.0
SDA	25	20.0	20.0	100.0
Total	125	100.0	100.0	

**Source: SPSS result output, 2021**

The table reveals that 51 representing 40.8% of the respondent strongly agree that ICT parks (mobile phone) influence digital literacy in Nigeria, 23 representing 18.4 support the view while 26, 25 of the respondent representing 20.8% and 20% respectively disagree and strongly disagree on the opinion that ICT parks (mobile phone) influence digital literacy in Nigeria.

**Descriptive Statistics**

	N	Minimum	Maximum	Mean	Std. Deviation
WHAT EFFECT HAS MOBILE PHONE AND DIGITAL LITERACY	125	1.00	4.00	2.2000	1.17775
Valid N (listwise)	125				

**Source: SPSS result output, 2021**

The mean value and its corresponding standard deviation for the above responds was obtained as 2.2000 and 1.17775 respectively. The mean value cut across the average agreement level of the respondent, indicating that majority of the respondent agree that ICT parks (mobile phone) influence digital literacy in Nigeria.

**Presentation of data: on the EXTENT OF SOCIAL MEDIA ON DIGITAL LITERACY**

	Frequency	Percent	Valid Percent	Cumulative Percent
SA	43	34.4	34.4	34.4
A	43	34.4	34.4	68.8
Valid DA	8	6.4	6.4	75.2
SDA	31	24.8	24.8	100.0
Total	125	100.0	100.0	

**Source: SPSS result output, 2021**

The table reveals that 43 representing 34.4% of the respondent strongly agree that social media affect digital literacy in Nigeria, 43 representing 34.4 support the view while 8, 31 of the respondent representing 6.4% and 24.8% respectively disagree and strongly disagreed that social media influence digital literacy in Nigeria.



**Descriptive Statistics**

	N	Minimum	Maximum	Mean	Std. Deviation
TO WHAT EXTENT HAS SOCIAL MEDIA AFFECTED DIGITAL LITERACY	125	1.00	4.00	2.2160	1.16801
Valid N (listwise)	125				

**Source: SPSS result output, 2021**

The mean value and its corresponding standard deviation for the above responds was obtained as 2.2160 and 1.16801 respectively. The mean value cut across the average agreement level of the respondent, indicating that majority of the respondent agrees that ICT parks (social media)influence digital literacy in Nigeria.

**Test of hypotheses at 5% level of significance**

Presentation of analysis of variance result for hypothesis one.

	Sum of Squares	Df	Mean Square	F	Sig.
Between Groups	20.671	4	5.168	5.017	.001
Within Groups	123.601	120	1.030		
Total	144.272	124			

**Source: SPSS result output, 2021**

**Hypothesis one**

**H<sub>01</sub>:** Wi-Fi has no significant effect on digital literacy in Nigeria.

From the above result, the estimated f-calculated and its corresponding P-value was obtained as 5.017 and 0.001 respectively. We therefore reject the null hypothesis that WiFi has no significant effect on digital literacy in Nigeria and accept the alternative inferring that the knowledge of respondent of WiFi has significant influence on digital literacy in Nigeria

**Presentation of analysis of variance result for hypothesis two.**

	Sum of Squares	Df	Mean Square	F	Sig.
Between Groups	10.902	4	2.725	2.030	.044
Within Groups	161.098	120	1.342		
Total	172.000	124			

**Source: SPSS result output, 2021**

**Hypothesis two**

**H<sub>02</sub>:** Mobile phone has no significant effect on digital literacy in Nigeria.

From the above result, the estimated f-calculated and its corresponding P-value was obtained as 2.030 and 0.044 respectively. We therefore reject the null hypothesis that mobile phone has no significant effect on digital literacy in Nigeria and accept the alternative inferring that the knowledge of respondent of mobile phone has significant influence on digital literacy in Nigeria.

**Presentation of analysis of variance result for hypothesis three.**

	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	27.570	4	6.892	5.841	.000
Within Groups	141.598	120	1.180		
Total	169.168	124			

**Source: SPSS result output, 2021**

**Hypothesis three**

**H<sub>03</sub>:** Social media has no significant effect on digital literacy in Nigeria.

From the above result, the estimated f-calculated and its corresponding P-value was obtained as 5.841 and 0.000 respectively. We therefore reject the null hypothesis that social media has no significant effect on digital literacy in Nigeria and accept the alternative inferring that the knowledge of respondent of social media has significant influence on digital literacy in Nigeria.

**Discussion of findings**

Having empirically investigated on ICT parks and digital literacy in Nigeria, the study came up with the following findings;

The study revealed, the estimated f-calculated and its corresponding P-value was obtained as 5.017 and 0.001 respectively which is less than 5% level of significance. The study therefore concludes that the knowledge of respondent of WiFi has significant influence on digital literacy in Nigeria.

The study show in the second hypothesis, an estimated f-calculated and its corresponding P-value of 2.030 and 0.044 respectively. This implies we reject the null hypothesis that mobile

phone has no significant effect on digital literacy in Nigeria and accept the alternative inferring that the knowledge of respondent of mobile phone has significant influence on digital literacy in Nigeria.

The third hypothesis revealed an estimated  $f$ -calculated and its corresponding  $P$ -value of 5.841 and 0.000 respectively which is less than 5% critical level. We therefore reject the null hypothesis that social media has no significant effect on digital literacy in Nigeria and accept the alternative inferring that the knowledge of respondent of social media has significant influence on digital literacy in Nigeria.

The descriptive statistics indicates that a significant percentage of the respondent are of the opinion that the knowledge of the use of WiFi, mobile phone and social media influences digital literacy in Nigeria.

## **Conclusion**

It is imperative that the knowledge of information technology parks has significant impact on digital literacy in Nigeria ICT space as evidence in our study. Developing Nations of the world are gearing towards linking all economic activity to ICT based economy. Like in the case of Nigeria, the ministry of information was changed to ministry of science and digital economy. This implies that all economic and political activities are tied around information communication technological space.

## **Recommendations**

The following recommendations were proffered based on the study

There is need for government to enhance range of coverage of WiFi, since WiFi security protocols prevent unauthorized access or damage to computers using wireless networks.

There is need for mobile phone industry to sensitize their buyer on the various networks assessable on their phone based on the range of coverage.

There is need for constant ICT training on the usage of social media and its economic and social importance in every society.

## Reference

- Ademola F. O, Effurun S. B, Ejiro G. B, Benjamin K. N, Angela C. N (2018); ICT and Digital Literacy Skills: a Mechanism for Efficient Teaching in Nigerian Colleges of Education; *Information Impact: Journal of information and knowledge management* 2018, Vol. 9 (3) Pg. 57-71 ISSN: 2141 – 4297 (print) ISSN: 2360 – 994X (e-version)
- Ebele, C, U., Ejedafiru, E.F., & Oghenetega, U.L.(2013). Information /ICT literacy levels and skills among librarians in Madonna University Library, Okija. *Journal of Humanities and Social Science (IOSR-JHSS)*, 15(3), 70-75.
- Calvani, A., Cartelli, A., Fini, A., & Ranieri, M. (2008). Models and instruments for assessing digital competence at school. *Journal of E-Learning and Knowledge Society*, 4(3): 183-193.
- Olakule N (2007). (2014). *Effectiveness of multimedia approach in teaching of Arts at secondary stage*. EDUTRACKS, 13(8): 17-19.
- Kolawale C (2008). Integration of ICT in education in a secondary school in Kenya: A case study. *Literacy Information and Computer Education Journal (LICEJ)*, 6(2): 1904-1909.
- Thierer, S (2000). *Computer technology as an interactive teaching system: A new trend in education*. EDUTRACKS, 12(5): 15- 18.
- Jimmie M. (2014): Definition and Classes of Social; Media University of Nevada, Reno 102 Publications 738 Citations
- <https://www.netspotapp.com/what-is-wifi.html>

# E-security and management performance among small and medium scale enterprises (SMEs) in Nigeria.

Eleberi Ebele Leticia  
Department of Computer Science  
[Ebyfav2001@yahoo.com](mailto:Ebyfav2001@yahoo.com)

## Abstract

*This paper investigates issues on E-security and management performance among small and medium scale enterprises (SMEs) in Nigeria. Proxy of E-security was disaggregated into Web payment system, electronic fund transfer and mobile payment system and regressed on Small and medium enterprises performance from 2005-2019. Multiple regression ordinary least square method was employed to analysed data generated. This study found WPS, EFT and MPS has positive and direct effect on SMEP but only EFT revealed statistical significance at 5% critical level. The study also revealed all parameter estimate jointly impact on the performance of Small and Medium Enterprises performance in Nigeria.*

**Keywords:** *E-security, E-commerce, Web Payment System, Electronic Fund Transfer, Mobile Payment System*

## 1. Introduction

E- security is a data's piece security system and is particularly connected to the segment that influences e-business that incorporates PC security, information security and other more extensive domains of the data security. Today, privacy and security are a noteworthy sympathy toward electronic advances business offers security worries with other innovation in the field. Advancement in instalment framework empowers transaction to be carryout easily crosswise over outskirt and plastic cards are one of the essential methods for picking up to record regardless of where the client is living. In Africa, illustration, the connection of outskirts and the Euro' presentation have prompted a generous increment in cross outskirt transaction and related fraud.

E-commerce, that we all know of today has been existing for the past of ten years. Be that as it may, its antecedents, for example, material requirement planning (MRP), enterprise resource

planning. (ERP), electronic data interchange (EDI), have been existing for over forty years and as yet living. Electronic information interchanged is the electronic communication of business of business transaction, for example, confirmation and involves between organizations although interactive access may be part of it, electronic data interchange (EDI) implies computer to computer transaction into vendors database and ordering system. The details data of the Material requirement planning (MRP) and Enterprise resource planning (ERP) is covered.

### 1.1 Statement of the problem

E-security entails measures put forward to combat electronic commerce threat and other online or electronic malicious factors that negatively affect organizational performance online. Electronic or Information security is used to protect against unavoidable security forces ensure the continuity of business, and reduce destruction. Businesses recognize security as a critical issue even many lacks the knowledge

behind electronic security techniques, if the organization is not knowledgeable enough on the security protocols then it is not able to part on its employee's education about how its intellectual property can be guarded. Therefore for them to gain from their security management practices they must have the necessary insight into problems at hand and security management controls within the scope that they can effectively accommodate (PACIS, 2013). Fu-guo and Yujie (2010) opined that e-commerce security threats are not focused on as single aspect of electronic (e) commerce but spins around different aspects of e-commerce transactions. These transactions could include electronic payment processes, buying process, receiving process, registration and online storage. The authors argued that e-security issues are considered as both systems engineering and social issues which demands general participation of members of the society. The threats fighting against e-security has been classified differently by different authors like DiYanni (2012) classified them as malicious code attacks which include: viruses, worms, Trojan horses, logic bombs, denial of service attack i.e.-distributed denial of service, SYN Flooding and Phishing. Rahman and Lackey (2013) classified e-security threats as web server threats, database threats, reconnaissance, social engineering, port scanning, vulnerability scanning, e-commerce server attacks, physical attacks, malware, and denial of service which SMEs must put into consideration. Since E-security centres on data integrity, data confidentiality, data authenticity and data reliability, this study captures specifically variable with element of E-security that facilitate the performance of SMEs in Nigeria such as ; web payment system, mobile payment system and electronic fund transfers.

## 1.2 Objective of the study

The objective of this study is to investigate issues on E-security and management performance among small and medium scale enterprises (SMEs) in Nigeria. The Specific objective of the study are to;

1. determine the effect of web payment system on the performance SMEs in Nigeria
2. evaluate the effect of electronic fund transfer on the performance of SMEs in Nigeria
3. Ascertain the effect of mobile payment system on the performance of SMEs in Nigeria

## 1.3 Research questions

This research paper is guided by the underlisted questions;

1. what effect has web payment E-security on performance of SMEs in Nigeria.
2. what is the of Electronic fund transfer E-security on performance of SMEs in Nigeria
3. to what extent has mobile payment system e-security affected the performance of SMEs in Nigeria

## 1.4 Research hypotheses

**H<sub>0</sub>:** there is no significant relationship between web payment system and performance of SMEs in Nigeria

**H<sub>0</sub>:** there is no significant relationship between Electronic fund transfer and performance of SMEs in Nigeria

**H<sub>0</sub>:** there is no significant relationship between mobile payment system and performance of SMEs in Nigeria

## 1.5 Scope of the study

The content scope of this paper is to ascertain the effect e-security and management of the performance of SMEs in Nigeria. E-security

system was disaggregated into web payment system, electronic fund transfer and mobile payment system as published in CBN statistical bulletin various years regressed against SME performance in Nigeria.

## 2.0 Review of related literature

### 2.1 Conceptual E-security

Electronic security entails measures put forward to combat electronic commerce threats, Determines and other online or electronic malicious factors that negatively affect organizations Performance online. Electronic or Information security is used to protect against unavoidable Security forces, ensure the continuity of business, and reduce destruction. Businesses recognize Security as a critical issue even many lacks the knowledge behind electronic security techniques, if the organization is not knowledgeable enough on the security protocols then it is not able to impart on its employee's education about how its intellectual property can be guarded. Therefore, for firms to gain from their security management practices they must have the necessary insights into problems at hand and security management controls within the scope that they can effectively accommodate (PACIS, 2013). Fu-guo and Yujie (2010) opined that e-commerce security threats are not focused on as single aspect of electronic (e) commerce but spins around different aspects of e-commerce transactions. These transactions could include electronic payment processes, buying process, receiving process, registration and online storage. The authors argued that e-security issues are considered as both systems engineering and social issues which demands general participation of members of the society. The threats fighting against e-security has been classified differently by different authors like DiYanni (2012) classified them as malicious code attacks which include: viruses, worms, Trojan horses, logic bombs, denial of service attack i.e.-distributed denial of service, SYN Flooding and Phishing. Rahman and Lackey (2013) classified e-security

threats as web server threats, database threats, reconnaissance, social engineering. port scanning, vulnerability scanning, e-commerce server attacks, physical attacks, malware, and denial of service which SMEs must put into consideration.

#### 2.1.1 Management Performance

Management performance is the measure of the extent an organization achieve its stated goals and objectives. Richard et al (2009) opined that performance in an organizational settings consist of three specific aspect of firm outcomes, that is financial performance, return on assets, return on investment are involve in that organizational performance. Secondly, product market

performance where sales, market share are involved and lastly shareholder return where total shareholder return, economic value added are involved. Kotane (2015) noted that management performance can be measured using both financial and non-financial dimensions. Managements performance measurement could be done via financial and non-financial performance indicators of the organizations such time, cost, quality, customer Satisfaction, stakeholders such as employees, investors, and suppliers are all critical measurement aspects (Kaplan, 1983). Performance can be measured using certain parameters like unit cost of production. Product specifications, delivery performance, product development, product innovation, and customer support and services Chairoel, Widarto, &Pujani, 2015). Didier (2002) opined that performance consists in "achieving the goals that were given to you in convergence of enterprise orientations"

The author stated that performance is not a mere finding of an outcome, but rather a function of a comparison between the outcome and the set objectives. In other words, management performance is the measurement of what management previous set as target and what they eventually got as a result. Rolstadas (1998) considers that the performance of an

organizational system is a complex relationship consisting of seven performance criteria that must be adhered to and they include factors such as: effectiveness, efficiency, quality, productivity, and quality of work, innovation and profitability. The author noted that performance of organizations or individual form revolves around the criteria enlisted above.

### **2.1.2 Factors Influencing SMEs ICT Adoption in Nigeria**

The use of information communication technology (ICT) has been widely embraced by various regions including developing and developed countries. Thus, various studies have delved into Similar studies and found different factors such Adebayo, Balogun and Kareem, (2013) indicated that cost, funds, infrastructure, skills and training, management support and government support attitude are the major elements or factors that influencing information communication technology (ICT) establishment adoption in Nigeria by SMEs. Further, Sajuyigbe and Alabi, (2012) also confirm that infrastructural, cost of acquisition, lack of finance, skills, management and government support are the main challenges of ICT adoption by SMES in Nigeria. Pinsonneault and Kraenmer (1993) outlined the factors into internal and external barriers that impede adoption of ICT by SMEs in developing countries. The internal barriers include; owner manager characteristics, cost and return on investment, and external barriers include; infrastructure, social, cultural, political, legal and regulatory. Factors such as owner/manager characteristics, the role of top management, firm characteristics, costs and return on investment, lack of adequate telecommunication infrastructures such as poor internet connectivity, lack of fixed telephone lines for end-users, dial-up access and the underdeveloped state of the Internet Service Providers (ISPs) have been identified by Kapurubandara and Lawson (2006) as problems that hinder SMEs' adoption of ICT in a developing country. While Chau (1995) proposed

that the owner's lack of knowledge of ICT technology and perceived benefits is a major barrier to the adoption of ICT. The lack of knowledge on how to use the technology and the low computer literacy are other contributing factors for not adopting ICT (Knol and Stroeken2001).

### **2.1.3 E-security Guidelines for SMEs in Nigeria**

Despite the setbacks preventing SMEs from adopting and utilizing electronic business transactions, various elements could be considered to enhance e-security in order to achieve enhanced performance. The following are guides on how organizations can handle security issues as provided by Obodoeze et al (2012):

1. Provide end-to-end data encryption using strong cryptographic cipher engines (AES 128 bit) to enhance data confidentiality.
2. Create strong user authentication to improved confidentiality and integrity.
3. Establish Message Authentication Codes (MAC) to enhance data authentication and protection of data from unauthorized users.
4. Perform vulnerability and compliance system scan on all interconnected stakeholders on their network on a regular basis at a minimal fee to the stakeholders.

Further, Park, Robles, Hong, and Kim (2008) identified electronic security standards for SMEs which includes established standard and pragmatic approach. The established standards entails security frameworks developed by organizations to remain at a service quality and security while the pragmatic approach accommodates smaller companies than the standard security frameworks. In addition, Pipkin(2000) proposed a data security process model that consist of five facets: (1) inspection, (2) protection. (3) detection, (4) reaction, and (5)



reflection.

## 2.2 Theoretical Review

### Davis' (1989) Technology Acceptance Model (TAM)

Davis Technology Acceptance Model (Davis, 1989) predicts information technology acceptance and usage. In this model the user's behavioral intention to use a technology is affected by their perceived usefulness and perceived ease of use of the technology.

This model was originally developed for studying technology at work. Later it has been used as such or modified to study user acceptance of consumer services such as Internet services or e-commerce (Kaasinen, 2005). The Technology Acceptance Model constitutes a solid framework for identifying issues that may affect user acceptance of technical solutions. As Davis and Venkatesh (2004) have proved, the model can be enhanced from the original purpose of studying user acceptance of existing products to study planned product concepts, e.g. in the form of mock-ups. This indicates that Technology Acceptance Model could also be used in connection with technology development projects and processes to assess the usefulness of proposed solutions. Applied in this way, the model also supports the human-centered design approach.

Technology acceptance model (TAM) is currently the most effective tool for describing information systems adoption. It was developed by Davis (1989) to explain and predict computer-usage security behaviour. It has its theoretical root in Theory of Reasoned Action (TRA) (Fishbein et al., 1975). TRA depicts that beliefs influence attitudes, which lead to intentions, and finally to behaviours. The Theory of Reasoned Action (TRA) introduced two independent determinants, attitude towards behaviour and subjective norm.

Attitude toward behaviour refers to the degree that an individual has a positive or negative reaction towards a specific behaviour. Normative beliefs consider the probability that important persons or groups approve or disapprove of performing a specific behaviour.

According to the TRA, individuals' attitudes towards behaviours are determined by their most important beliefs and the consequences of performing specific behaviours. As Fishbein et al. (1975) demonstrated through their theory, behaviour is best predicted by intentions, and intentions are jointly determined by the person's attitude and subjective norm concerning the behaviour. TAM's proposition posits two constructs: Perceived usefulness (PU) which is defined as "the prospective user's subjective probability that using a specific application system will increase his or her job performance" and perceived ease of use (PEOU), which refers to the degree to which the prospective user expects the target system to be free of effort (Davis et al, 1989).

Both perceived usefulness and perceived ease of use have been used in examining users' acceptance of information systems. Perceived usefulness has been proven consistently as significant in attitude formation (Jiang et al., 2008; Klopping, 2004). TAM has also been employed to predict consumers' adoption of Web technology (Pavlou, 2003; Tan et al., 2014; Klopping). Lee et al. (2001) extended TAM with perceived risk (PR) and found that the TAM predicted individual purchasing behaviour online and that perceived risk affects perceived usefulness. Chen et al. (2002) also found TAM effective in evaluating online shopping at "virtual" on-line store. Building on these empirically validated views, the TAM is suitable for determining e-commerce but may not fully determine the users' intention to adopt the technology. Therefore, the study proposes an

extended TAM, with integration of task-technology fit model, trust, and perceived risk to better predict consumers' adoption of e-commerce. The original TAM was also modified by dropping perceived ease of use – perceived usefulness the path based on previous e-commerce adoption studies which argued that Web tools are exceptionally easy to use (Klopping et al., 2004). Also, to simplify TAM, the attitude construct was dropped and focused on the relationship between perceived usefulness and perceived ease of use on intention to use.

Trust is a belief that one can rely upon a promise made by another (Pavlou, 2003). Klopping and McKinney (2004) defines trust in electronic commerce as the subjective probability with which consumers believe that an online transaction with a web retailer will occur in a manner consistent with their expectations. Scholars have identified lack of trust as one of the main reasons for consumers' cynicism towards electronic commerce. In the context of e-commerce, trust beliefs include the online consumers' beliefs and expectancies about trust-related characteristics of the online seller (McKnight and Chervany, 2012). The online consumers desire the online sellers to be willing and able to act in the consumers' interests, to be honest in transactions (not divulging personal information to other vendors), and to be capable of delivering the ordered goods as agreed. According to Mahmood and Bagchi (2004), the trust factor has significant positive contributions to consumers' online shopping behaviour. Jiang et al (2008) argued that consumer trust is a critical enabler of successful online retailing and knowledge is one important factor influencing the level of trust. The work of Maskus (2013) and May (2017), among others presented integrated trust model with the technology acceptance model for business-to-consumer (B2C) e-commerce.

### 2.3 Empirical Review

Okeke, Oboreh&Ezeaghaego (2016) examined the effects of e-commerce on the growth of small scale enterprises in Anambra State. The study adopted judgmental sampling technique. A sample size of 282 respondents was chosen through purposive sampling. The data used were generated from the selected small scale enterprises in Nnewi, Onitsha and Awka. The data generated were analyzed using percentage analysis while the hypotheses formulated were tested using Z-test statistics. The study found that business-to-customer (B2C) exerts significant effect on the performance of small scale enterprises. It also revealed that E-commerce adoption has significant effect on growth of small scale enterprises. It was recommended that small scale enterprises yet to adopt e-commerce technology should do so to remain competitive in their industries.

Oluwafemi, Christopher, Joel & Adeyinka (2016), researched on e-commerce in Nigeria: a survey of security awareness of customers and factors that influence acceptance. The study aimed at accessing the security awareness of customers of e-commerce sites in Nigeria, and identifying factors that influence acceptance of these platforms. Data were collected via the use of questionnaire and was analyzed using T-test. Results show that most customers are aware that their information are stored by the e-commerce sites, and are concerned about the security of their data on these sites and the possibility of their information to be transferred to third party without their knowledge or permission. Yet only few of them make effort to always check the security and privacy policies of the sites before making purchases. Also, only few users are conversant with security technologies for securing e-commerce platforms. The proposed

factors were found to be important or likely to influence transacting on e-commerce sites.

Akanbi & Akintunde (2018), studied E-commerce adoption and small medium scale Enterprises performance in Nigeria. The study aimed at examining the impact e-commerce adoption has on SMEs Operators performance. The study employed the use of a quantitative research approach. Based on the quantitative approach imbibed in the study, questionnaire was used to capture data that examined the objectives of the research. The questionnaire was distributed both manually and electronically to total sample of over 250 SMEs. Data collected were analysed using descriptive analysis. The study showed that e-commerce has potentials to improve the performance of SMEs operators and bring about expansion in business outlook if factors limiting the adoption of e-commerce like security issues, under developed infrastructures, poor delivery logistics and poor courier systems, infrastructure facilities, incompatibility of business with e-commerce etc., were eliminated. The study recommended improved infrastructural facilities and better strategies that will improve consumers and business technological knowledge and ensure favourable environment for ecommerce adoption.

Rita & John (2015) carried out a study on Determinant factors of e-commerce adoption by SMEs in developing country: evidence from Indonesia. The aim of this study is to investigate those factors that influence SMEs in developing countries in adopting ecommerce. A descriptive survey method using an on-line questionnaire was employed. Eleven variables were proposed as the factors that influence SMEs in adopting of e-commerce. These were organized into four groups, namely: technological factors, organizational factors, environmental factors and individual factors. A sample of 292 respondents was drawn from a population of 3,267 SMEs, a

response rate of 8.9%. To investigate the relationship between the variables, multiple regression analysis is used. The result shows that the individual factors play a significant role in adopting of e-commerce technology by SMEs in Indonesia. It was also found that perceived benefits, technology readiness, owners innovativeness, owners IT ability and owners IT experience are the determinant factors that influence Indonesian SMEs in their adopting e-commerce.

Kareem, Owomoyela, & Oyebamiji (2014), conducted a research on electronic commerce and business performance: an empirical investigation of business organizations in Nigeria. This research paper examined the impact of e-commerce on business performance with particular reference to the selected supermarkets in Ibadan metropolis. The study sample was made up of 8 Supermarkets. Structured questionnaire designed by the researchers were used to collect data from each operator and 5 staff respectively, totalling 48 respondents. Data analysis was conducted with simple regression analysis. The result showed that e-commerce adoption has significant impact on service operations, cost operation reductions and profit levels. It was concluded that adoption of e-commerce by Nigerian supermarkets will reduce transaction cost, improve service operations, expand business base, better understand the needs of foreign customers, and increase profit levels. The study recommended that the operators and staff of supermarkets should embark on more effective Information Technology (IT) training in order to further enhance their performance. It also recommends management of supermarkets should procure quality IT gadgets that will enhance efficiency and customers retention.

Kabuba (2014), carried out a study on e-commerce and performance of online businesses in Kenya. The aim of the study was to establish the performance of existing online businesses as well establish the relationship between e-commerce models and performance. The study targeted 30 online companies based in Nairobi County and a cross sectional survey design was adopted. Descriptive statistics was employed. The regression analysis model was then used for data analysis. The study findings revealed that some of the challenges affecting online businesses but to a moderate extent are: potential customers reluctance to shop online due to desire to touch/interact with the product prior to making a purchase, lack of personal contact with customers which might be beneficial to business, e-commerce software incompatibility with existing infrastructure, customer distrust regarding privacy of personal data and finally, customers general lack of trust for online businesses. It was recommended that the government needs to invest in the enactment of laws and regulatory infrastructure that supports online purchasing. Most importantly Kenyan consumers have to be more willingly to purchase products and services online.

Mutia, Ahmad, Aziz & Mohamad (2014), examined the relationship between e-commerce adoption and organization performance of hotel industry in Malaysia. This study uses a cross-sectional research design. Data was analysed using a statistical Package for Social Science (SPSS) Version 11. The study also found that there is a correlation between organization performance with E-commerce business network, and E-commerce competency. The research also employed stepwise regression analysis to look at dominant factor in predicting organizational performance. The research contributed to both academic research and management practice as it provide comprehensive impact of how e-

commerce adoption influence organizational performance at least in the case of Tourism industry in a small developing economy like Malaysia.

### **3.0 Methodology**

#### **3.1 Research Design**

The researcher adopt quasi experimental design to analyse data generated for E-security and management performance among small and medium scale enterprises (SMEs) in Nigeria. This choice of design will be employed since it involves the manipulation of independent variable without a random assignment of participants to conditions or order of conditions.

#### **3.2 Sources of Data**

This study employed secondary source as the sole source of data collection. The data sourced from the Central Bank of Nigeria (CBN) online published bulletin reports various years. The data collected (and analyzed) enabled the realization of the research objectives, answering of the research questions and forming opinion of the assertions of the study's hypotheses. The quantitative data collected covered the various proxies for the dependent and independent variables of the study namely SMEs performance (SMEP), Web payment System (WPS), Electronic Fund Transfer (EFT) and mobile payment system (MPS), for the period of 13 years covering 2005 – 2017.

#### **3.3 Method of Data Analysis**

Ordinary Least Square (OLS) Analysis was employed in the analysis of data with the aid of E-view statistical package Version 9.0. The choice of this technique for this study is based on the uniqueness and time frame of the data collected and it give room for expressing the relationship in a mathematical form. That is, it

provides an estimated equation which expresses the functional relationship between the dependent and independent; such that one variable can be predicted given the value of the other variable. Individual significance test using t-statistics (prob) was utilized in the hypothesis test. The researcher thus adjudged this technique as being suitable for the analysis of this study. However, the t-statistics was adopted in testing each of the hypotheses of this study.

### 3.3.1 Model Specification

To capture the proxies for the variables in the three specific objectives of the study, the models bellow was developed:

$$SMEP = F(WPS, MPS, EFT) \dots\dots\dots (1)$$

The above equation can be rewritten into multiple regression models as follows:

$$SMEP = \beta_0 + \beta_1 WPS + \beta_2 EFT + \beta_3 MPS + \epsilon_t \dots\dots\dots (2)$$

Where: SMEP = Small and Medium Enterprises Performance.

EFT = Electronic Fund Transfer

WPS = Web Payment System

MPS = Mobile

MPS= Mobile payment system

Where:  $\beta_0$  is the intercept of the multiple regression line

$\beta_1, \beta_2, \& \beta_3$  are the coefficient of the explanatory

YEAR	LOGsmep	LOGwps	LOGeft	LOGmps
2005	0.40567	1.659441	3.894241	0.09691
2006	-0.00636	1.658584	4.01508	0.276462
2007	-0.06926	1.892762	3.992902	0.404834
2008	-0.76133	1.940765	4.018405	0.346353
2009	-0.77138	1.925054	4.078755	0.103804
2010	-0.86505	1.398808	4.055259	0.822822
2011	-0.78947	1.775319	4.080594	1.278296
2012	-0.87687	1.499238	4.135452	1.498439
2013	-0.87615	1.675011	4.155558	2.15472
2014	-0.91391	1.869488	4.164846	2.539662
2015	-1.02028	1.961807	4.116843	2.64577
2016	-0.49485	2.121758	4.163901	2.879037
2017	-0.58503	2.266224	4.174538	3.042181
2018	-0.5376	2.607027	4.042613	3.262617
2019	-0.38722	2.679546	4.113586	3.640635

(independent) variables

$\epsilon$  is the stochastic variable or error term

## 4.0 Data Presentation, Analysis And Interpretations

### 4.1 Data Presentation

Data collected for this study include data on aggregate Small and Medium Enterprises Performance (SMEP), Web Payment System (WPS), Electronic Fund Transfer (EFT) and Mobile Payment System (MPS). The data are presented on table 4.1 below:

**Table 4.1: Data on, SMEP, WPS, EFT, MPS for the period covering 2005 – 2019.**

YEAR	SMEP	WPS	EFT	MPS
2005	2.54	45.65	7838.64	1.25
2006	0.99	45.56	10353.33	1.89
2007	0.85	78.12	9837.89	2.54
2008	0.17	87.25	10432.91	2.22
2009	0.17	84.15	11988.23	1.27
2010	0.14	25.05	11356.89	6.65
2011	0.16	59.61	12039.09	18.98
2012	0.13	31.57	13,660.03	31.51

2013	0.13	47.32	14,307.32	142.80
2014	0.12	74.04	14,616.58	346.47
2015	0.10	91.58	13,087.09	442.35
2016	0.32	132.36	14,584.80	756.90
2017	0.26	184.60	14,946.46	1,102.00
2018	0.29	404.60	11,030.96	1,830.70
2019	0.41	478.13	12,989.32	4,371.55

**Source: CBN statistical bulletin various edition.**

**Table 4.1: Data on, SMEP, WPS, EFT, MPS for the period covering 2005 – 2019.**

*Ms Excel computation from table 4.1 above*

The above data are in different bases; therefore, to bring the data in the same base, we calculate the logarithm for the data on each of the variables.

**4.2 Data Analysis**

Data analysis in this section is of two parts; the pre-test (diagnostic test) and model estimation as presented in the previous section. The paper employs the use of ordinary least square method of data analysis as the suitable tool in determining the effect E-security on SMEs performance in Nigeria.

**4.2.1 Test for stationarity (Unit root test)**

Having subjected PAT, ROA, ATM, POS, MPS to stationarity test Using Augmented Dickey-

Fuller test statistics, the following results were obtained.

**Table 4.2.1: Augmented Dickey Fuller Stationarity Test Result**

Variables	Critical value@ 5%	P-value
SMEP	-2.098896	0
WPS	-2.098896	0
ETF	-3.098896	0
MPS	-3.098896	0

**Source:** *Extracts from Appendix 1*

Table 4.2.1 shows that the time series data collected for the four (4) variables are all stationary at level. With this, we conclude that the time series data used in the analysis of this paper are all stationary and are therefore adjudged valid for the analysis using OLS estimate since all variables are stationary at level; findings of the analysis are thus reliable for policy decisions.

**4.2.2 Result of Heteroskedasticity Test**

F-statistic	0.526247	Prob. F(3,11)	0
Obs*R-squared	1.882631	Prob. Chi-Square(3)	0
Scaled explained SS	0.344145	Prob. Chi-Square(3)	0

**Source:** E-view result output 2021.

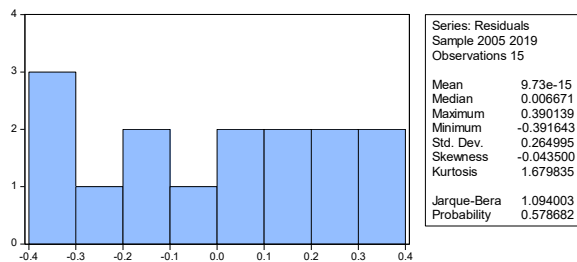
The test above reveals the presence of homoscedasticity since the observed R-square

probability value of 0.5971 is greater the critical value of 0.05. Indicating that the variance of the parameters is consistent overtime.

Log likelihood	-0.845958	Hannan-Quinn criter.	0.644116
F-statistic	4.844393	Durbin-Watson stat	1.733670
Prob(F-statistic)	0.021892		

**Source:** E-view version 9.0 statistical Result, 2021

### 4.2.3 Normality Test



The above result reveals p-value of jargua-bera statistic as 0.578682 indicating that the variables are normally distributed since the probability value is greater than 5%.

**Table 4.2.4 Ordinary least square estimated result**

Dependent Variable: LOGSMEP  
Method: Least Squares  
Date: 05/08/21 Time: 17:03  
Sample: 2005 2019  
Included observations: 15

Variable	Coefficient	Std. Error	t-Statistic	Prob.
C	17.28076	6.895058	2.506253	0.0292
LOGWPS	0.133132	0.352754	0.377408	0.7131
LOGEFT	4.461725	1.642601	2.716256	0.0201
LOGMPS	0.058296	0.136994	0.425538	0.6787

R-squared	0.569188	Mean dependent var	0.569939
Adjusted R-squared	0.451694	S.D. dependent var	0.403732
S.E. of regression	0.298955	Akaike info criterion	0.646128
Sum squared resid	0.983112	Schwarz criterion	0.834941

The result on the above table reveals that the coefficient of LOGWPS is positive with the value of 0.133132; the coefficient of LOGEFT is positive at 4.461725 while the coefficient of LOGMPS is positive with the value of 0.058296. it was evident from the result that all the parameter estimates are positive related to the performance of small and medium enterprises. The value of the intercept (C) is 17.28076, indicating that the collective effect of the independent variables on ROA is positive.

### 4.3 Test of Hypotheses

To ascertain the significance of these results, the t-statistics results of each of the independent variables were considered as follows;

#### Test of Hypothesis 1

**H<sub>0</sub>:** there is no significant relationship between web payment system and performance of SMEs in Nigeria

In testing this first hypothesis of the study, the regression result on table 4.3 reveal the p-value (t-stat probability) of the first independent variable web payment system (WPS) as 0.7131; which is greater than the significant level of 0.05 (5%) i.e.  $P > 0.05$ . This result indicates an insignificant effect exists WPS and SMEP. Therefore, we accept the null hypothesis which states that there is no significant relationship between web payment system and performance of SMEs in Nigeria and consequently reject the associating alternative hypothesis that a significant relationship exists between web payment system and performance of SMEs in Nigeria

## Test of Hypothesis 2

**H<sub>0</sub>:** there is no significant relationship between Electronic fund transfer and performance of SMEs in Nigeria

From the result of regression analysis on table 4.3, the p-value (t-stat probability) of electronic fund transfer was obtained as (EFT) 0.0201; which is less than the significant level of 0.05 (5%) i.e.  $P < 0.05$ . This result indicates that a significant effect exists. Therefore, we reject the null hypothesis which states that 0.0201 and consequently accept the alternative hypothesis that a significant relationship exist between ETF and SMEP.

## Test of Hypothesis 3

**H<sub>0</sub>:** there is no significant relationship between mobile payment system and performance of SMEs in Nigeria

In testing the third hypothesis of the study, we adopt the test of significance result from the regression analysis on table 4.3. From the result, the p-value (t-stat probability) of the third independent variable mobile payment system is 0.6787; which is greater than significant level of 0.05 (5%) i.e.  $P > 0.05$ . This result shows an insignificant effect of the independent variable on the dependent variable. Therefore, we accept the null hypothesis which states that mobile payment system has no significant effect on performance of SMEP and consequently reject the alternative hypothesis that state otherwise.

## 4.4 Discussion of Findings

The findings from the analysis and test statistics are discussed in line with the empirical review this study. Discussion of the findings is as follows:

1. In respect of the first objective and the first hypothesis of this study, we find that web payment system has insignificant positive effect on small and medium enterprises performance in Nigeria. This implies that e-security as proxy by web payment being an electronic instrument of e-commerce has no significant effect on SMEP in Nigeria. This result is not in agreement with Kareem, Owomoyela, & Oyebamiji (2014) with who hold that e-security significantly affect the SMEP.
2. The second findings of this study reveal electronic fund transfer to be statistically significant with SMEP. This disagrees with Oluwafemi, Christopher, Joel & Adeyinka (2016) who researched on e-commerce in Nigeria but support the findings of Kareem, Owomoyela, & Oyebamiji (2014).
3. The study also revealed mobile payment system has positive but insignificantly related to small and medium enterprises in Nigeria. This finding disagrees with the work of Kareem, Owomoyela, & Oyebamiji (2014) who are of the opinion that e-security adoption has significant impact on service operations, cost operation reductions and profit levels. They concluded that adoption of e-security by SMEs will reduce transaction cost, improve service operations, expand business base, better understand the needs of foreign customers, and increase profit levels.



**REFERENCES**

- Akanbi, B. E. & Akintunde, T. S. (2018). E-commerce Adoption And Small Medium Scale Enterprises Performance In Nigeria. *European Journal of Management and Marketing Studies*, 3(1), 10-24.
- Anil, K. (2012). Introduction to e-commerce. MM-409/1B419. <http://www.ddegjust.ac.in/studyaterial/mcom/mc-201.pdf>.
- Chen, Q. & Zhang, N. (2015). Does E-Commerce Provide a Sustained Competitive Advantage? An Investigation of Survival and Sustainability in Growth-Oriented Enterprises, *Journal of Open Access Sustainability*, 7, 1411-1428.
- Cudjoe, D. (2014). Electronic Commerce: State-of-the-Art. *American Journal of Intelligent Systems*, 4(4), pp. 135-141.
- Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly*, 319-40.
- Davis, F. D., Bagozzi, R. P. & Warshaw, P. R. (1989). User Acceptance of Computer Technology: A Comparison of Two. *Management Science*, 35(8), 982-1001.
- Fishbein, M. & Ajzen, I. (1975). *Belief, attitude, intention, and behavior: an introduction to theory and research*. Reading, MA: Addison-Wesley.
- Kabuba, P. K. (2014). E-Commerce And Performance Of Online Businesses In Kenya. Unpublished M.Sc. Thesis. University of Nairobi, Kenya.
- Kareem, T. S., Owomoyela, S. K., & Oyebamiji, F. F. (2014). Electronic Commerce and Business Performance: An Empirical Investigation of Business Organizations in Nigeria. *International Journal of Academic Research in Business and Social Sciences*, 4(8), 215-221.
- Lawal, A. S. (2010). Electronic commerce in Nigeria banking industry (a case study of guaranty trust bank Nigeria plc.). Department of business administration, faculty of business and social science. University of Ilorin, Ilorin.
- Len, M. (2015). 10 Customer Retention Strategies to Implement Today. Retrieved July, 10 2019 from <https://www.groovehq.com/support/customer-retention-strategies>
- Ma, Q. & Liu, L. (2017). *The Technology Acceptance Model: A Meta-Analysis of Empirical Findings*. Hershey: Idea Group Publishing.
- MacGregor, R. (2011). Perception of Barriers to e-Commerce adoption in SMEs in a Developed and Developing Country: a Comparison between Australia and Indonesia. *Journal of Electronic Commerce in Organizations*, 8(1), 61-82..
- Mutia, A. H. S., Ahmad, M. M. W., Aziz, B. M. A. & Mohamad, S. M. (2014). The Relationship between E-Commerce Adoption and Organization Performance. *International Journal of Business and Management*, 9(1), 56-62.
- Nasir, M. A. (2009). Legal Issues Involved in E-Commerce. *Communication of the ACM: Ubiquity*, 3(37).
- OECD (2004). *ICT, E-Business & SMEs, Organisation for Economic Co-Operation and Development*, Retrieved 04 October 2010, from <http://www.oecd.org/dataoecd/32/28/34228733.pdf>.
- Okeke, M. N., Oboreh, J. C., & Ezeaghaego, C. C. (2016). Effect Of E-commerce And The Growth Of Small Scale Enterprises In Selected Enterprises In Anambra State. *Singaporean Journal Of Business Economics, And Management Studies*, 5(2), 82- 92.
- Oluwafemi, O., Christopher, I. O., Joel, N. U., & Adeyinka, A. F. (2016). E-Commerce in

Nigeria: A Survey of Security Awareness of Customers and Factors that Influence Acceptance. Research gate journal. <https://www.researchgate.net/publication/311589556>

<http://www.rogerclarke.com/EC/ECDefns.html>.

Onugu, B. A. N. (2005). Small And Medium Enterprises (SMEs) In Nigeria: Problems And Prospects. Unpublished Ph.D. Thesis. St. Clements University.

Raheem, A. R., Vishnu, P., & Ahmed, A. M. (2014). Impact Of Product Packaging On Consumer's Buying Behavior. European Journal of Scientific Research, 122(2), 125-134.

Rita, R. & John, D. (2015). World Conference on Technology, Innovation and Entrepreneurship: Determinant Factors of Ecommerce Adoption by SMEs in Developing Country: Evidence from Indonesia. Procedia - Social and Behavioral Sciences, 195,142 – 150.

Roger, C. (1999). Electronic Commerce Definition.

### Appendix

Data set for Small and Medium enterprises, Web Payment System Electronic Fund Transfer and Mobile Payment System

YEAR	LOGsmep	LOGwps	LOGeft	LOGmps
2005	0.40567	1.659441	3.894241	0.09691
2006	-0.00636	1.658584	4.01508	0.276462
2007	-0.06926	1.892762	3.992902	0.404834
2008	-0.76133	1.940765	4.018405	0.346353
2009	-0.77138	1.925054	4.078755	0.103804
2010	-0.86505	1.398808	4.055259	0.822822
2011	-0.78947	1.775319	4.080594	1.278296
2012	-0.87687	1.499238	4.135452	1.498439
2013	-0.87615	1.675011	4.155558	2.15472
2014	-0.91391	1.869488	4.164846	2.539662
2015	-1.02028	1.961807	4.116843	2.64577
2016	-0.49485	2.121758	4.163901	2.879037
2017	-0.58503	2.266224	4.174538	3.042181
2018	-0.5376	2.607027	4.042613	3.262617
2019	-0.38722	2.679546	4.113586	3.640635

Source: CBN Statistical bulletin various years

**UNIT ROOT TEST**

Null Hypothesis: LOGEFT has a unit root  
Exogenous: Constant  
Lag Length: 0 (Automatic - based on SIC, maxlag=3)

	t-Statistic	Prob.*
Augmented Dickey-Fuller test statistic	-2.999900	0.0193
Test critical values: 1% level	-4.004425	
5% level	-2.098896	
10% level	-2.690439	

\*MacKinnon (1996) one-sided p-values.  
Warning: Probabilities and critical values calculated for 20 observations  
and may not be accurate for a sample size of 14

Augmented Dickey-Fuller Test Equation  
Dependent Variable: D(LOGEFT)  
Method: Least Squares  
Date: 05/08/21 Time: 17:05  
Sample (adjusted): 2006 2019  
Included observations: 14 after adjustments

Variable	Coefficient	Std. Error	t-Statistic	Prob.
LOGEFT(-1)	-0.489452	0.163156	-2.999900	0.0111
C	2.011546	0.665437	3.022895	0.0106
R-squared	0.428555	Mean dependent var		0.015668
Adjusted R-squared	0.380935	S.D. dependent var		0.060585
S.E. of regression	0.047669	Akaike info criterion		-3.117522
Sum squared resid	0.027268	Schwarz criterion		-3.026228
Log likelihood	23.82265	Hannan-Quinn criter.		-3.125972
F-statistic	8.999403	Durbin-Watson stat		2.305977
Prob(F-statistic)	0.011069			

Null Hypothesis: LOGMPS has a unit root  
Exogenous: Constant  
Lag Length: 0 (Automatic - based on SIC, maxlag=3)

	t-Statistic	Prob.*
Augmented Dickey-Fuller test statistic	-4.300899	0.0289
Test critical values: 1% level	-4.004425	
5% level	-3.098896	
10% level	-2.690439	

\*MacKinnon (1996) one-sided p-values.  
Warning: Probabilities and critical values calculated for 20 observations  
and may not be accurate for a sample size of 14

Augmented Dickey-Fuller Test Equation  
Dependent Variable: D(LOGMPS)  
Method: Least Squares

Date: 05/08/21 Time: 17:06

Sample (adjusted): 2006 2019

Included observations: 14 after adjustments

Variable	Coefficient	Std. Error	t-Statistic	Prob.
LOGMPS(-1)	0.018468	0.061375	0.300899	0.7686
C	0.224958	0.117391	1.916304	0.0794
R-squared	0.007489	Mean dependent var		0.253123
Adjusted R-squared	-0.075221	S.D. dependent var		0.255635
S.E. of regression	0.265075	Akaike info criterion		0.313956
Sum squared resid	0.843177	Schwarz criterion		0.405250
Log likelihood	-0.197689	Hannan-Quinn criter.		0.305505
F-statistic	0.090540	Durbin-Watson stat		1.824139
Prob(F-statistic)	0.768641			

Null Hypothesis: LOGSMEP has a unit root  
Exogenous: Constant  
Lag Length: 0 (Automatic - based on SIC, maxlag=3)

	t-Statistic	Prob.*
Augmented Dickey-Fuller test statistic	-3.059408	0.0335
Test critical values:		
1% level	-4.004425	
5% level	-2.098896	
10% level	-2.690439	

\*MacKinnon (1996) one-sided p-values.  
Warning: Probabilities and critical values calculated for 20 observations  
and may not be accurate for a sample size of 14

Augmented Dickey-Fuller Test Equation  
Dependent Variable: D(LOGSMEP)

Method: Least Squares  
Date: 05/08/21 Time: 17:07  
Sample (adjusted): 2006 2019  
Included observations: 14 after adjustments

Variable	Coefficient	Std. Error	t-Statistic	Prob.
LOGSMEP(-1)	-0.430912	0.140848	-3.059408	0.0099
C	-0.307852	0.099627	-3.090055	0.0094
R-squared	0.438202	Mean dependent var		-0.056635
Adjusted R-squared	0.391385	S.D. dependent var		0.270587
S.E. of regression	0.211095	Akaike info criterion		-0.141455
Sum squared resid	0.534732	Schwarz criterion		-0.050161
Log likelihood	2.990185	Hannan-Quinn criter.		-0.149906
F-statistic	9.359975	Durbin-Watson stat		2.206350
Prob(F-statistic)	0.009910			

Null Hypothesis: LOGWPS has a unit root  
Exogenous: Constant  
Lag Length: 0 (Automatic - based on SIC, maxlag=3)

	t-Statistic	Prob.*
Augmented Dickey-Fuller test statistic	-5.356727	0.0042
Test critical values:		
1% level	-4.004425	
5% level	-3.098896	
10% level	-2.690439	

\*MacKinnon (1996) one-sided p-values.  
Warning: Probabilities and critical values calculated for 20 observations  
and may not be accurate for a sample size of 14

Augmented Dickey-Fuller Test Equation  
Dependent Variable: D(LOGWPS)  
Method: Least Squares  
Date: 05/08/21 Time: 17:08

Sample (adjusted): 2006 2019  
Included observations: 14 after adjustments

Variable	Coefficient	Std. Error	t-Statistic	Prob.
LOGWPS(-1)	-0.077121	0.216190	-0.356727	0.0275
C	0.217473	0.410596	0.529653	0.0060
R-squared	0.010493	Mean dependent var		0.072865
Adjusted R-squared	-0.071966	S.D. dependent var		0.235842
S.E. of regression	0.244181	Akaike info criterion		0.149749
Sum squared resid	0.715492	Schwarz criterion		0.241043
Log likelihood	0.951759	Hannan-Quinn criter.		0.141298
F-statistic	0.127254	Durbin-Watson stat		2.491090
Prob(F-statistic)	0.727490			

**ORDINARY LEAST SQUARE ESTIMATE**

Dependent Variable: LOGSMEP

Method: Least Squares

Date: 05/08/21 Time: 17:03

Sample: 2005 2019

Included observations: 15

Variable	Coefficient	Std. Error	t-Statistic	Prob.
C	17.28076	6.895058	2.506253	0.0292
LOGWPS	0.133132	0.352754	0.377408	0.7131
LOGEFT	4.461725	1.642601	2.716256	0.0201
LOGMPS	0.058296	0.136994	0.425538	0.6787
R-squared	0.569188	Mean dependent var		-0.569939
Adjusted R-squared	0.451694	S.D. dependent var		0.403732
S.E. of regression	0.298955	Akaike info criterion		0.646128
Sum squared resid	0.983112	Schwarz criterion		0.834941
Log likelihood	-0.845958	Hannan-Quinn criter.		0.644116
F-statistic	4.844393	Durbin-Watson stat		1.733670
Prob(F-statistic)	0.021892			

**DESCRIPTIVE STATISTICS**

	LOGSMEP	LOGEFT	LOGMPS	LOGWPS
Mean	-0.569939	4.080172	1.666169	1.928722
Median	-0.761335	4.080594	1.498439	1.892762
Maximum	0.405670	4.174538	3.640635	2.679546
Minimum	-1.020281	3.894241	0.096910	1.398808
Std. Dev.	0.403732	0.078630	1.277007	0.366422
Skewness	1.121863	-0.753402	0.090471	0.741745
Kurtosis	3.331273	3.028225	1.463375	2.852947
Jarque-Bera	3.215033	1.419535	1.496223	1.388978
Probability	0.200385	0.491758	0.473259	0.499330
Sum	-8.549083	61.20257	24.99254	28.93083
Sum Sq. Dev.	2.281997	0.086557	22.83045	1.879714
Observations	15	15	15	15

**Heteroskedasticity Test**

Heteroskedasticity Test: Breusch-Pagan-Godfrey

F-statistic	0.526247	Prob. F(3,11)	0.6733
Obs*R-squared	1.882631	Prob. Chi-Square(3)	0.5971
Scaled explained SS	0.344145	Prob. Chi-Square(3)	0.9515

Test Equation:

Dependent Variable: RESID^2

Method: Least Squares

Date: 05/08/21 Time: 17:25

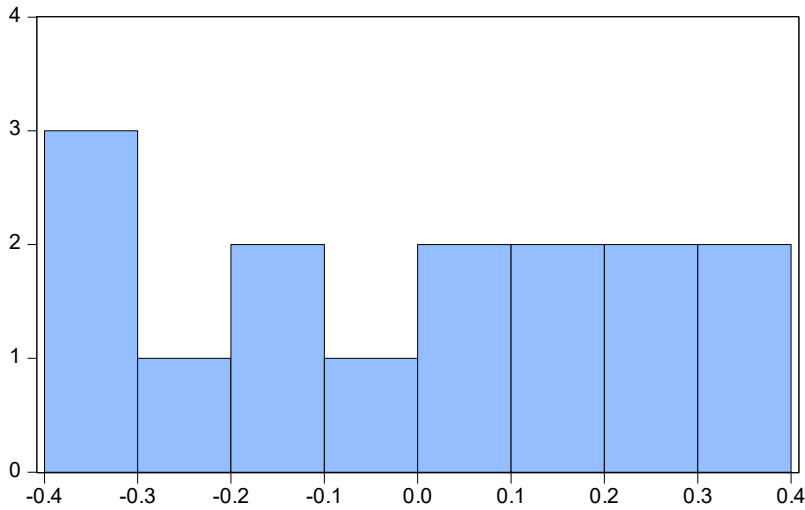
Sample: 2005 2019

Included observations: 15

Variable	Coefficient	Std. Error	t-Statistic	Prob.
C	1.203957	1.361047	0.884581	0.3953
LOGWPS	0.015471	0.069632	0.222187	0.8282
LOGEFT	-0.288087	0.324241	-0.888499	0.3933
LOGMPS	0.004315	0.027042	0.159580	0.8761
R-squared	0.125509	Mean dependent var		0.065541
Adjusted R-squared	-0.112989	S.D. dependent var		0.055936
S.E. of regression	0.059012	Akaike info criterion		-2.598973
Sum squared resid	0.038307	Schwarz criterion		-2.410160
Log likelihood	23.49230	Hannan-Quinn criter.		-2.600984
F-statistic	0.526247	Durbin-Watson stat		2.211243
Prob(F-statistic)	0.673270			



**NORMALITY TEST**



Series: Residuals	
Sample 2005 2019	
Observations 15	
Mean	9.73e-15
Median	0.006671
Maximum	0.390139
Minimum	-0.391643
Std. Dev.	0.264995
Skewness	-0.043500
Kurtosis	1.679835
Jarque-Bera	1.094003
Probability	0.578682

**MULTICOLLINEARITY TEST**

Variance Inflation Factors  
Date: 05/08/21 Time: 17:26  
Sample: 2005 2019  
Included observations: 15

Variable	Coefficient Variance	Uncentered VIF	Centered VIF
C	47.54183	7979.155	NA
LOGWPS	0.124435	80.30682	2.617125
LOGLEFT	2.698139	7541.414	2.613114
LOGMPS	0.018767	13.53833	4.794096

# ENERGY EFFICIENT CLUSTERING TECHNIQUE TO REDUCE LOAD IN CLOUD COMPUTING

Dr. Sumit Chaudhary, Associate Professor, Indrashil University,  
Rajpur, Kadi, India

[drsumitchaudhary@gmail.com](mailto:drsumitchaudhary@gmail.com)

Neha Singh, Assistant Professor, Indrashil University, Rajpur,  
Kadi, India

[singh.neha773@gmail.com](mailto:singh.neha773@gmail.com)

Ms. Jyoti Srivastava, Assistant Professor, Indrashil University,  
Rajpur, Kadi, India

[Jyotisrivastava688@gmail.com](mailto:Jyotisrivastava688@gmail.com)

Mr. Bhavesh Jain, Assistant Professor, Indrashil University,  
Rajpur, Kadi, India

[bmjain007@gmail.com](mailto:bmjain007@gmail.com)

**Abstract:** For provisioning of various computing resources in recent days cloud computing data centers are becoming popular. Now reducing of energy consumption is the main issues at different data centers. In the field of Cloud Computing Clustering technique is the best technique to reduce the load at data centers and finally energy consumption will be reduced. In this paper, energy efficiency with reducing load is the main issue and to reduce the load at different data centers different energy efficiency and load balancing techniques implemented.

**Keywords:** Load Balancing, Clustering, Energy Consumption, Cloud Computing

**Introduction:** Cloud Computing is network of computers connected to each other with internet and shared resources. Recourses can be any type of resources like Hardware, Application, Services, Server, Processing Power, Memory, Operating System, Network etc...

A cloud word shows the internet and computing is a process of utilizing computer technology to complete our task. The two important concepts in the “cloud” are:

1. Abstraction [14]: From users and developers the information of system implementation is abstracted in cloud computing. On unknown addresses data is saved, on unspecified physical system applications run and also system administration is provided to others. Therefore, on unspecified physical system all the applications run, on unknown address data is saved, system administration is outsourced to others and finally it is accessed by users.
2. Virtualization [10]: By pooling and resource sharing Cloud computing virtualizes systems. Systems and storage can be provisioned as needed from a centralized infrastructure, costs are assessed on a metered basis, multi-tenancy is enabled, and resources are scalable with agility. By creating virtual version of any device or any resource and dividing framework in executable environment virtualization can be achieved. Electricity can be an example of virtualization, where it is coming from substation and distributed to different location and same time. Cloud Computing is on demand computing services initially offered by commercial provides such as Amazon, Google and Microsoft.

This model aim is to provide resources as services which can be used or accessed from anywhere and anytime.

As per NIST “Cloud Computing [12] is a model for having omnipresent, suitable, whenever required network access to shared pool with so many computing assets which are

configurable like (Network, Server, Storage, Application and Services) which can be fast equipped and then can be released with least control efforts or providers communication”.

## Explain Layer Architecture of cloud computing: -

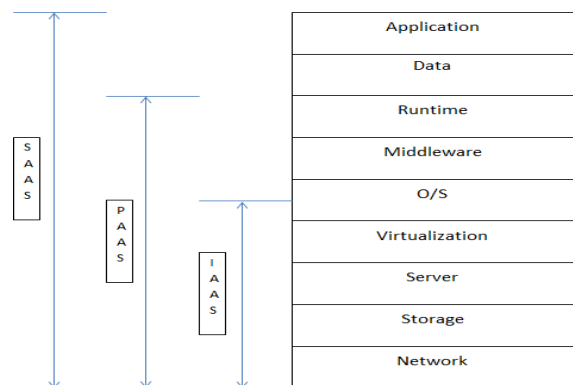
According to level of abstraction of the capability and provided service model Cloud computing services are divided into three classes, namely:

1. Infrastructure as a Service (IaaS)
2. Platform as a Service (PaaS)
3. Software as a Service (SaaS)

Services of higher level can be composed from underlying in abstraction level.

### ● Infrastructure as a Service:

- Infrastructure as a Service (IaaS) [1,2,4,12,13] is popular for providing on demand virtual resources.
- Several options of operating system and software stack with customization is available for on demand provisioning of servers. Such services are observed as the bottom layer of cloud computing.
- IaaS mainly offers Amazon Web Services which in the case of its EC2service which means it is offering VMs with the help of a software stack that can be customized similar to how an ordinary physical server can be customized.
- Various privileges for performing activity to the server like starting and stopping, installing software packages and customizing it, virtual disks are given to users.



**Figure 1: Layered Architecture of Cloud Service Model**

**Platform as a Service:**

- Platform as a Service (PaaS) [1,2,4,12,13] means higher level of abstraction which help cloud easily programmable.
- An environment where developers create and deploy applications and also don't need to know about the processors and memory will be using is offered by a cloud platform offers.
- Specialized services like data access, authentication and payments are offered as building blocks to new applications.
- It offers environment for developing and hosting web applications which can be written in specific language like python or Java. Google App Engine, an example of Platform as a Service.

**Software as a Service:**

- With the help of Web portals end users can use services provided by this layer. Applications reside on the top of the cloud stack. From locally installed computer programs now consumers are shifting to online services.
- As a service in web can be used to access traditional desktop applications such as word processing and spreadsheet. This model of delivering applications, known as Software as a Service (SaaS) [1,2,4,12,13].

**Problem Statement:** In cloud data centers Methods and standards are needed to benchmark the energy efficiency of cloud services at IaaS, PaaS and SaaS [1,2,4,12,13] levels. The use of software defined infrastructures and the associated protocols, tools, and models allow new levels of flexibility in clouds and new multi-objective optimization models are needed to trade-off between performance levels, energy efficiency [5,7,9], and cost. New intelligent deployment and runtime optimization approaches are needed to take into account the energy consumed considering the user demand patterns. Some Applications are only used during day-time, others during the weekend and algorithms need to be developed to predict the behavior of the different applications deployed in the cloud. Virtual infrastructure can be re-deployed at runtime in cloud infrastructures to minimize the Number of physical machines being used and to switch off unused machines to reduce both Costs and energy consumed.

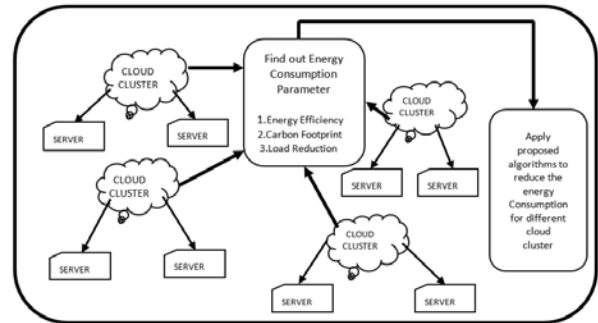
Many research papers already published for save energy and for reduce load [2,3,4,6] in cloud. When system in ideal state then we can save energy and also save energy when system in working state. Lots of user working at that time then load is producing so that system works slow down. That's way we can reduce load in cloud computing data centers.

Lots of algorithms available for save energy and for reduce load [2,3,4,6] in cloud. but they can save very less energy we can try to save more energy and try to reduce load in cloud computing using only algorithm.

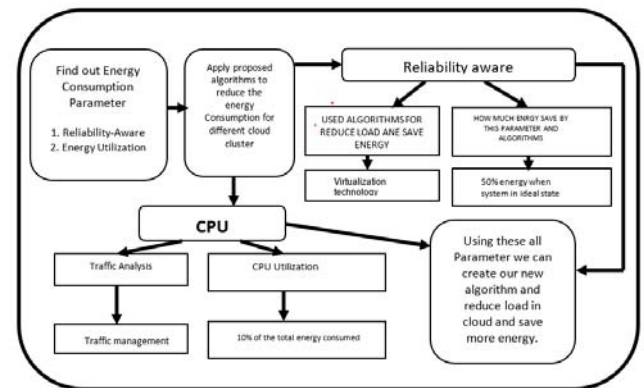
**Existing and proposed work:** Different research paper

available for reduce energy efficient [5,7,9]. It reduces load over network and efficient the energy in terms of saving using different algorithms and different technique and also uses different tools. But they can 10% to 15% energy save only.

I can try to save more energy in my project and try to reduce load [2,3,4,6] also using different algorithms and different technique.



**Figure 2: Flow of Control**



**Figure 3: Proposed Architecture**

Using above parameter, we will implement our new algorithm and make cloud energy more efficient and also reduce load in cloud computing.

**Proposed Algorithm:**

In past research work, many research papers available for reducing load and energy efficiency. Most of the algorithm reduces load and in terms of energy it is efficient using different algorithms and different technique using different tools. But they can save 10% to 15% energy only.

The proposed algorithm can save more energy in cloud datacenter and reduce load using different algorithms and different technique.

Here one algorithm has implemented for load reduction, carbon footprint reduction and save more energy in cloud computing.



- Cloud)(I-SMAC), 2018 2nd International Conference on (pp. 213-219). IEEE.
15. Ahmad, B., Maroof, Z., McClean, S., Charles, D., & Parr, G. (2019). Economic impact of energy saving techniques in cloud server. *Cluster Computing*, 1-11.

## IJCSIS REVIEWERS' LIST

Assist Prof (Dr.) M. Emre Celebi, Louisiana State University in Shreveport, USA  
Dr. Lam Hong Lee, Universiti Tunku Abdul Rahman, Malaysia  
Dr. Shimon K. Modi, Director of Research BSPA Labs, Purdue University, USA  
Dr. Jianguo Ding, Norwegian University of Science and Technology (NTNU), Norway  
Assoc. Prof. N. Jaisankar, VIT University, Vellore, Tamilnadu, India  
Dr. Amogh Kavimandan, The Mathworks Inc., USA  
Dr. Ramasamy Mariappan, Vinayaka Missions University, India  
Dr. Yong Li, School of Electronic and Information Engineering, Beijing Jiaotong University, P.R. China  
Assist. Prof. Sugam Sharma, NIET, India / Iowa State University, USA  
Dr. Jorge A. Ruiz-Vanoye, Universidad Autónoma del Estado de Morelos, Mexico  
Dr. Neeraj Kumar, SMVD University, Katra (J&K), India  
Dr Genge Bela, "Petru Maior" University of Targu Mures, Romania  
Dr. Junjie Peng, Shanghai University, P. R. China  
Dr. Ilhem LENGILIZ, HANA Group - CRISTAL Laboratory, Tunisia  
Prof. Dr. Durgesh Kumar Mishra, Acropolis Institute of Technology and Research, Indore, MP, India  
Dr. Jorge L. Hernández-Ardieta, University Carlos III of Madrid, Spain  
Prof. Dr.C.Suresh Gnana Dhas, Anna University, India  
Dr Li Fang, Nanyang Technological University, Singapore  
Prof. Pijush Biswas, RCC Institute of Information Technology, India  
Dr. Siddhivinayak Kulkarni, University of Ballarat, Ballarat, Victoria, Australia  
Dr. A. Arul Lawrence, Royal College of Engineering & Technology, India  
Dr. Wongyos Keardsri, Chulalongkorn University, Bangkok, Thailand  
Dr. Somesh Kumar Dewangan, CSVTU Bhilai (C.G.)/ Dimat Raipur, India  
Dr. Hayder N. Jasem, University Putra Malaysia, Malaysia  
Dr. A.V.Senthil Kumar, C. M. S. College of Science and Commerce, India  
Dr. R. S. Karthik, C. M. S. College of Science and Commerce, India  
Dr. P. Vasant, University Technology Petronas, Malaysia  
Dr. Wong Kok Seng, Soongsil University, Seoul, South Korea  
Dr. Praveen Ranjan Srivastava, BITS PILANI, India  
Dr. Kong Sang Kelvin, Leong, The Hong Kong Polytechnic University, Hong Kong  
Dr. Mohd Nazri Ismail, Universiti Kuala Lumpur, Malaysia  
Dr. Rami J. Matarneh, Al-isra Private University, Amman, Jordan  
Dr Ojesanmi Olusegun Ayodeji, Ajayi Crowther University, Oyo, Nigeria  
Dr. Riktsh Srivastava, Skyline University, UAE  
Dr. Oras F. Baker, UCSI University - Kuala Lumpur, Malaysia  
Dr. Ahmed S. Ghiduk, Faculty of Science, Beni-Suef University, Egypt  
and Department of Computer science, Taif University, Saudi Arabia  
Dr. Tirthankar Gayen, IIT Kharagpur, India  
Dr. Huei-Ru Tseng, National Chiao Tung University, Taiwan  
Prof. Ning Xu, Wuhan University of Technology, China  
Dr Mohammed Salem Binwahlan, Hadhramout University of Science and Technology, Yemen  
& Universiti Teknologi Malaysia, Malaysia.  
Dr. Aruna Ranganath, Bhoj Reddy Engineering College for Women, India  
Dr. Hafeezullah Amin, Institute of Information Technology, KUST, Kohat, Pakistan

Prof. Syed S. Rizvi, University of Bridgeport, USA  
Dr. Shahbaz Pervez Chattha, University of Engineering and Technology Taxila, Pakistan  
Dr. Shishir Kumar, Jaypee University of Information Technology, Wakanaghat (HP), India  
Dr. Shahid Mumtaz, Portugal Telecommunication, Instituto de Telecomunicações (IT) , Aveiro, Portugal  
Dr. Rajesh K Shukla, Corporate Institute of Science & Technology Bhopal M P  
Dr. Poonam Garg, Institute of Management Technology, India  
Dr. S. Mehta, Inha University, Korea  
Dr. Dilip Kumar S.M, Bangalore University, Bangalore  
Prof. Malik Sikander Hayat Khiyal, Fatima Jinnah Women University, Rawalpindi, Pakistan  
Dr. Virendra Gomase , Department of Bioinformatics, Padmashree Dr. D.Y. Patil University  
Dr. Irraivan Elamvazuthi, University Technology PETRONAS, Malaysia  
Dr. Saqib Saeed, University of Siegen, Germany  
Dr. Pavan Kumar Gorakavi, IPMA-USA [YC]  
Dr. Ahmed Nabih Zaki Rashed, Menoufia University, Egypt  
Prof. Shishir K. Shandilya, Rukmani Devi Institute of Science & Technology, India  
Dr. J. Komala Lakshmi, SNR Sons College, Computer Science, India  
Dr. Muhammad Sohail, KUST, Pakistan  
Dr. Manjaiah D.H, Mangalore University, India  
Dr. S Santhosh Baboo, D.G.Vaishnav College, Chennai, India  
Prof. Dr. Mokhtar Beldjehem, Sainte-Anne University, Halifax, NS, Canada  
Dr. Deepak Laxmi Narasimha, University of Malaya, Malaysia  
Prof. Dr. Arunkumar Thangavelu, Vellore Institute Of Technology, India  
Dr. M. Azath, Anna University, India  
Dr. Md. Rabiul Islam, Rajshahi University of Engineering & Technology (RUET), Bangladesh  
Dr. Aos Alaa Zaidan Ansaef, Multimedia University, Malaysia  
Dr Suresh Jain, Devi Ahilya University, Indore (MP) India,  
Dr. Mohammed M. Kadhum, Universiti Utara Malaysia  
Dr. Hanumanthappa. J. University of Mysore, India  
Dr. Syed Ishtiaque Ahmed, Bangladesh University of Engineering and Technology (BUET)  
Dr Akinola Solomon Olalekan, University of Ibadan, Ibadan, Nigeria  
Dr. Santosh K. Pandey, The Institute of Chartered Accountants of India  
Dr. P. Vasant, Power Control Optimization, Malaysia  
Dr. Petr Ivankov, Automatika - S, Russian Federation  
Dr. Utkarsh Seetha, Data Infosys Limited, India  
Mrs. Priti Maheshwary, Maulana Azad National Institute of Technology, Bhopal  
Dr. (Mrs) Padmavathi Ganapathi, Avinashilingam University for Women, Coimbatore  
Assist. Prof. A. Neela madheswari, Anna university, India  
Prof. Ganesan Ramachandra Rao, PSG College of Arts and Science, India  
Mr. Kamanashis Biswas, Daffodil International University, Bangladesh  
Dr. Atul Gonsai, Saurashtra University, Gujarat, India  
Mr. Angkoon Phinyomark, Prince of Songkla University, Thailand  
Mrs. G. Nalini Priya, Anna University, Chennai  
Dr. P. Subashini, Avinashilingam University for Women, India  
Assoc. Prof. Vijay Kumar Chakka, Dhirubhai Ambani IICT, Gandhinagar ,Gujarat  
Mr Jitendra Agrawal, : Rajiv Gandhi Proudlyogiki Vishwavidyalaya, Bhopal  
Mr. Vishal Goyal, Department of Computer Science, Punjabi University, India  
Dr. R. Baskaran, Department of Computer Science and Engineering, Anna University, Chennai

Assist. Prof. Kanwalvir Singh Dhindsa, B.B.S.B.Engg.College, Fatehgarh Sahib (Punjab), India  
Dr. Jamal Ahmad Dargham, School of Engineering and Information Technology, Universiti Malaysia Sabah  
Mr. Nitin Bhatia, DAV College, India  
Dr. Dhavachelvan Ponnurangam, Pondicherry Central University, India  
Dr. Mohd Faizal Abdollah, University of Technical Malaysia, Malaysia  
Assist. Prof. Sonal Chawla, Panjab University, India  
Dr. Abdul Wahid, AKG Engg. College, Ghaziabad, India  
Mr. Arash Habibi Lashkari, University of Malaya (UM), Malaysia  
Mr. Md. Rajibul Islam, Ibnu Sina Institute, University Technology Malaysia  
Professor Dr. Sabu M. Thampi, .B.S Institute of Technology for Women, Kerala University, India  
Mr. Noor Muhammed Nayeem, Université Lumière Lyon 2, 69007 Lyon, France  
Dr. Himanshu Aggarwal, Department of Computer Engineering, Punjabi University, India  
Prof R. Naidoo, Dept of Mathematics/Center for Advanced Computer Modelling, Durban University of Technology,  
Durban, South Africa  
Prof. Mydhili K Nair, Visweswaraiah Technological University, Bangalore, India  
M. Prabu, Adhiyamaan College of Engineering/Anna University, India  
Mr. Swakkhar Shatabda, United International University, Bangladesh  
Dr. Abdur Rashid Khan, ICIT, Gomal University, Dera Ismail Khan, Pakistan  
Mr. H. Abdul Shabeer, I-Nautix Technologies, Chennai, India  
Dr. M. Aramudhan, Perunthalaivar Kamarajar Institute of Engineering and Technology, India  
Dr. M. P. Thapliyal, Department of Computer Science, HNB Garhwal University (Central University), India  
Dr. Shahaboddin Shamshirband, Islamic Azad University, Iran  
Mr. Zeashan Hameed Khan, Université de Grenoble, France  
Prof. Anil K Ahlawat, Ajay Kumar Garg Engineering College, Ghaziabad, UP Technical University, Lucknow  
Mr. Longe Olumide Babatope, University Of Ibadan, Nigeria  
Associate Prof. Raman Maini, University College of Engineering, Punjabi University, India  
Dr. Maslin Masrom, University Technology Malaysia, Malaysia  
Sudipta Chattopadhyay, Jadavpur University, Kolkata, India  
Dr. Dang Tuan NGUYEN, University of Information Technology, Vietnam National University - Ho Chi Minh City  
Dr. Mary Lourde R., BITS-PILANI Dubai , UAE  
Dr. Abdul Aziz, University of Central Punjab, Pakistan  
Mr. Karan Singh, Gautam Budtha University, India  
Mr. Avinash Pokhriyal, Uttar Pradesh Technical University, Lucknow, India  
Associate Prof Dr Zuraini Ismail, University Technology Malaysia, Malaysia  
Assistant Prof. Yasser M. Alginahi, Taibah University, Madinah Munawwarah, KSA  
Mr. Dakshina Ranjan Kisku, West Bengal University of Technology, India  
Mr. Raman Kumar, Dr B R Ambedkar National Institute of Technology, Jalandhar, Punjab, India  
Associate Prof. Samir B. Patel, Institute of Technology, Nirma University, India  
Dr. M.Munir Ahamed Rabbani, B. S. Abdur Rahman University, India  
Asst. Prof. Koushik Majumder, West Bengal University of Technology, India  
Dr. Alex Pappachen James, Queensland Micro-nanotechnology center, Griffith University, Australia  
Assistant Prof. S. Hariharan, B.S. Abdur Rahman University, India  
Asst Prof. Jasmine. K. S, R.V.College of Engineering, India  
Mr Naushad Ali Mamode Khan, Ministry of Education and Human Resources, Mauritius  
Prof. Mahesh Goyani, G H Patel Collge of Engg. & Tech, V.V.N, Anand, Gujarat, India  
Dr. Mana Mohammed, University of Tlemcen, Algeria  
Prof. Jatinder Singh, Universal Institution of Engg. & Tech. CHD, India



Mrs. M. Anandhavalli Gauthaman, Sikkim Manipal Institute of Technology, Majitar, East Sikkim  
Dr. Bin Guo, Institute Telecom SudParis, France  
Mrs. Maleika Mehr Nigar Mohamed Heenaye-Mamode Khan, University of Mauritius  
Prof. Pijush Biswas, RCC Institute of Information Technology, India  
Mr. V. Bala Dhandayuthapani, Mekelle University, Ethiopia  
Dr. Irfan Syamsuddin, State Polytechnic of Ujung Pandang, Indonesia  
Mr. Kavi Kumar Khedo, University of Mauritius, Mauritius  
Mr. Ravi Chandiran, Zagro Singapore Pte Ltd. Singapore  
Mr. Milindkumar V. Sarode, Jawaharlal Darda Institute of Engineering and Technology, India  
Dr. Shamimul Qamar, KSJ Institute of Engineering & Technology, India  
Dr. C. Arun, Anna University, India  
Assist. Prof. M.N.Birje, Basaveshwar Engineering College, India  
Prof. Hamid Reza Naji, Department of Computer Enigneering, Shahid Beheshti University, Tehran, Iran  
Assist. Prof. Debasis Giri, Department of Computer Science and Engineering, Haldia Institute of Technology  
Subhabrata Barman, Haldia Institute of Technology, West Bengal  
Mr. M. I. Lali, COMSATS Institute of Information Technology, Islamabad, Pakistan  
Dr. Feroz Khan, Central Institute of Medicinal and Aromatic Plants, Lucknow, India  
Mr. R. Nagendran, Institute of Technology, Coimbatore, Tamilnadu, India  
Mr. Amnach Khawne, King Mongkut's Institute of Technology Ladkrabang, Ladkrabang, Bangkok, Thailand  
Dr. P. Chakrabarti, Sir Padampat Singhania University, Udaipur, India  
Mr. Nafiz Imtiaz Bin Hamid, Islamic University of Technology (IUT), Bangladesh.  
Shahab-A. Shamshirband, Islamic Azad University, Chalous, Iran  
Prof. B. Priestly Shan, Anna Univeristy, Tamilnadu, India  
Venkatramreddy Velma, Dept. of Bioinformatics, University of Mississippi Medical Center, Jackson MS USA  
Akshi Kumar, Dept. of Computer Engineering, Delhi Technological University, India  
Dr. Umesh Kumar Singh, Vikram University, Ujjain, India  
Mr. Serguei A. Mokhov, Concordia University, Canada  
Mr. Lai Khin Wee, Universiti Teknologi Malaysia, Malaysia  
Dr. Awadhesh Kumar Sharma, Madan Mohan Malviya Engineering College, India  
Mr. Syed R. Rizvi, Analytical Services & Materials, Inc., USA  
Dr. S. Karthik, SNS College of Technology, India  
Mr. Syed Qasim Bukhari, CIMET (Universidad de Granada), Spain  
Mr. A.D.Potgantwar, Pune University, India  
Dr. Himanshu Aggarwal, Punjabi University, India  
Mr. Rajesh Ramachandran, Naipunya Institute of Management and Information Technology, India  
Dr. K.L. Shunmuganathan, R.M.K Engg College , Kavaraipettai ,Chennai  
Dr. Prasant Kumar Pattnaik, KIST, India.  
Dr. Ch. Aswani Kumar, VIT University, India  
Mr. Ijaz Ali Shoukat, King Saud University, Riyadh KSA  
Mr. Arun Kumar, Sir Padam Pat Singhania University, Udaipur, Rajasthan  
Mr. Muhammad Imran Khan, Universiti Teknologi PETRONAS, Malaysia  
Dr. Natarajan Meghanathan, Jackson State University, Jackson, MS, USA  
Mr. Mohd Zaki Bin Mas'ud, Universiti Teknikal Malaysia Melaka (UTeM), Malaysia  
Prof. Dr. R. Geetharamani, Dept. of Computer Science and Eng., Rajalakshmi Engineering College, India  
Dr. Smita Rajpal, Institute of Technology and Management, Gurgaon, India  
Dr. S. Abdul Khader Jilani, University of Tabuk, Tabuk, Saudi Arabia  
Mr. Syed Jamal Haider Zaidi, Bahria University, Pakistan

Dr. N. Devarajan, Government College of Technology, Coimbatore, Tamilnadu, INDIA  
Mr. R. Jagadeesh Kannan, RMK Engineering College, India  
Mr. Deo Prakash, Shri Mata Vaishno Devi University, India  
Mr. Mohammad Abu Naser, Dept. of EEE, IUT, Gazipur, Bangladesh  
Assist. Prof. Prasun Ghosal, Bengal Engineering and Science University, India  
Mr. Md. Golam Kaosar, School of Engineering and Science, Victoria University, Melbourne City, Australia  
Mr. R. Mahammad Shafi, Madanapalle Institute of Technology & Science, India  
Dr. F. Sagayaraj Francis, Pondicherry Engineering College, India  
Dr. Ajay Goel, HIET, Kaithal, India  
Mr. Nayak Sunil Kashibarao, Bahirji Smarak Mahavidyalaya, India  
Mr. Suhas J Manangi, Microsoft India  
Dr. Kalyankar N. V., Yeshwant Mahavidyalaya, Nanded, India  
Dr. K.D. Verma, S.V. College of Post graduate studies & Research, India  
Dr. Amjad Rehman, University Technology Malaysia, Malaysia  
Mr. Rachit Garg, L K College, Jalandhar, Punjab  
Mr. J. William, M.A.M college of Engineering, Trichy, Tamilnadu, India  
Prof. Jue-Sam Chou, Nanhua University, College of Science and Technology, Taiwan  
Dr. Thorat S.B., Institute of Technology and Management, India  
Mr. Ajay Prasad, Sir Padampat Singhanian University, Udaipur, India  
Dr. Kamaljit I. Lakhtaria, Atmiya Institute of Technology & Science, India  
Mr. Syed Rafiul Hussain, Ahsanullah University of Science and Technology, Bangladesh  
Mrs Fazeela Tunnisa, Najran University, Kingdom of Saudi Arabia  
Mrs Kavita Taneja, Maharishi Markandeshwar University, Haryana, India  
Mr. Maniyar Shiraz Ahmed, Najran University, Najran, KSA  
Mr. Anand Kumar, AMC Engineering College, Bangalore  
Dr. Rakesh Chandra Gangwar, Beant College of Engg. & Tech., Gurdaspur (Punjab) India  
Dr. V V Rama Prasad, Sree Vidyanikethan Engineering College, India  
Assist. Prof. Neetesh Kumar Gupta, Technocrats Institute of Technology, Bhopal (M.P.), India  
Mr. Ashish Seth, Uttar Pradesh Technical University, Lucknow, UP India  
Dr. V V S S S Balam, Sreenidhi Institute of Science and Technology, India  
Mr Rahul Bhatia, Lingaya's Institute of Management and Technology, India  
Prof. Niranjana Reddy, P, KITS, Warangal, India  
Prof. Rakesh. Lingappa, Vijetha Institute of Technology, Bangalore, India  
Dr. Mohammed Ali Hussain, Nimra College of Engineering & Technology, Vijayawada, A.P., India  
Dr. A. Srinivasan, MNM Jain Engineering College, Rajiv Gandhi Salai, Thorapakkam, Chennai  
Mr. Rakesh Kumar, M.M. University, Mullana, Ambala, India  
Dr. Lena Khaled, Zarqa Private University, Aman, Jordan  
Ms. Supriya Kapoor, Patni/Lingaya's Institute of Management and Tech., India  
Dr. Tossapon Boongoen, Aberystwyth University, UK  
Dr. Bilal Alatas, Firat University, Turkey  
Assist. Prof. Jyoti Praaksh Singh, Academy of Technology, India  
Dr. Ritu Soni, GNG College, India  
Dr. Mahendra Kumar, Sagar Institute of Research & Technology, Bhopal, India.  
Dr. Binod Kumar, Lakshmi Narayan College of Tech. (LNCT) Bhopal India  
Dr. Muzhir Shaban Al-Ani, Amman Arab University Amman – Jordan  
Dr. T.C. Manjunath, ATRIA Institute of Tech, India  
Mr. Muhammad Zakarya, COMSATS Institute of Information Technology (CIIT), Pakistan

Assist. Prof. Harmunish Taneja, M. M. University, India  
Dr. Chitra Dhawale , SICSR, Model Colony, Pune, India  
Mrs Sankari Muthukaruppan, Nehru Institute of Engineering and Technology, Anna University, India  
Mr. Aaqif Afzaal Abbasi, National University Of Sciences And Technology, Islamabad  
Prof. Ashutosh Kumar Dubey, Trinity Institute of Technology and Research Bhopal, India  
Mr. G. Appasami, Dr. Pauls Engineering College, India  
Mr. M Yasin, National University of Science and Tech, karachi (NUST), Pakistan  
Mr. Yaser Miaji, University Utara Malaysia, Malaysia  
Mr. Shah Ahsanul Haque, International Islamic University Chittagong (IIUC), Bangladesh  
Prof. (Dr) Syed Abdul Sattar, Royal Institute of Technology & Science, India  
Dr. S. Sasikumar, Roever Engineering College  
Assist. Prof. Monit Kapoor, Maharishi Markandeshwar University, India  
Mr. Nwaocha Vivian O, National Open University of Nigeria  
Dr. M. S. Vijaya, GR Govindarajulu School of Applied Computer Technology, India  
Assist. Prof. Chakresh Kumar, Manav Rachna International University, India  
Mr. Kunal Chadha , R&D Software Engineer, Gemalto, Singapore  
Mr. Mueen Uddin, Universiti Teknologi Malaysia, UTM , Malaysia  
Dr. Dhuha Basheer abdullah, Mosul university, Iraq  
Mr. S. Audithan, Annamalai University, India  
Prof. Vijay K Chaudhari, Technocrats Institute of Technology , India  
Associate Prof. Mohd Ilyas Khan, Technocrats Institute of Technology , India  
Dr. Vu Thanh Nguyen, University of Information Technology, HoChiMinh City, VietNam  
Assist. Prof. Anand Sharma, MITS, Lakshmanagarh, Sikar, Rajasthan, India  
Prof. T V Narayana Rao, HITAM Engineering college, Hyderabad  
Mr. Deepak Gour, Sir Padampat Singhania University, India  
Assist. Prof. Amutharaj Joyson, Kalasalingam University, India  
Mr. Ali Balador, Islamic Azad University, Iran  
Mr. Mohit Jain, Maharaja Surajmal Institute of Technology, India  
Mr. Dilip Kumar Sharma, GLA Institute of Technology & Management, India  
Dr. Debojyoti Mitra, Sir padampat Singhania University, India  
Dr. Ali Dehghantanha, Asia-Pacific University College of Technology and Innovation, Malaysia  
Mr. Zhao Zhang, City University of Hong Kong, China  
Prof. S.P. Setty, A.U. College of Engineering, India  
Prof. Patel Rakeshkumar Kantilal, Sankalchand Patel College of Engineering, India  
Mr. Biswajit Bhowmik, Bengal College of Engineering & Technology, India  
Mr. Manoj Gupta, Apex Institute of Engineering & Technology, India  
Assist. Prof. Ajay Sharma, Raj Kumar Goel Institute Of Technology, India  
Assist. Prof. Ramveer Singh, Raj Kumar Goel Institute of Technology, India  
Dr. Hanan Elazhary, Electronics Research Institute, Egypt  
Dr. Hosam I. Faiq, USM, Malaysia  
Prof. Dipti D. Patil, MAEER's MIT College of Engg. & Tech, Pune, India  
Assist. Prof. Devendra Chack, BCT Kumaon engineering College Dwarahat Almora, India  
Prof. Manpreet Singh, M. M. Engg. College, M. M. University, India  
Assist. Prof. M. Sadiq ali Khan, University of Karachi, Pakistan  
Mr. Prasad S. Halgaonkar, MIT - College of Engineering, Pune, India  
Dr. Imran Ghani, Universiti Teknologi Malaysia, Malaysia  
Prof. Varun Kumar Kakar, Kumaon Engineering College, Dwarahat, India

Assist. Prof. Nisheeth Joshi, Apaji Institute, Banasthali University, Rajasthan, India  
Associate Prof. Kunwar S. Vaisla, VCT Kumaon Engineering College, India  
Prof Anupam Choudhary, Bhilai School Of Engg.,Bhilai (C.G.),India  
Mr. Divya Prakash Shrivastava, Al Jabal Al garbi University, Zawya, Libya  
Associate Prof. Dr. V. Radha, Avinashilingam Deemed university for women, Coimbatore.  
Dr. Kasarapu Ramani, JNT University, Anantapur, India  
Dr. Anuraag Awasthi, Jayoti Vidyapeeth Womens University, India  
Dr. C G Ravichandran, R V S College of Engineering and Technology, India  
Dr. Mohamed A. Deriche, King Fahd University of Petroleum and Minerals, Saudi Arabia  
Mr. Abbas Karimi, Universiti Putra Malaysia, Malaysia  
Mr. Amit Kumar, Jaypee University of Engg. and Tech., India  
Dr. Nikolai Stoianov, Defense Institute, Bulgaria  
Assist. Prof. S. Ranichandra, KSR College of Arts and Science, Tiruchencode  
Mr. T.K.P. Rajagopal, Diamond Horse International Pvt Ltd, India  
Dr. Md. Ekramul Hamid, Rajshahi University, Bangladesh  
Mr. Hemanta Kumar Kalita , TATA Consultancy Services (TCS), India  
Dr. Messaouda Azzouzi, Ziane Achour University of Djelfa, Algeria  
Prof. (Dr.) Juan Jose Martinez Castillo, "Gran Mariscal de Ayacucho" University and Acantelys research Group, Venezuela  
Dr. Jatinderkumar R. Saini, Narmada College of Computer Application, India  
Dr. Babak Bashari Rad, University Technology of Malaysia, Malaysia  
Dr. Nighat Mir, Effat University, Saudi Arabia  
Prof. (Dr.) G.M.Nasira, Sasurie College of Engineering, India  
Mr. Varun Mittal, Gemalto Pte Ltd, Singapore  
Assist. Prof. Mrs P. Banumathi, Kathir College Of Engineering, Coimbatore  
Assist. Prof. Quan Yuan, University of Wisconsin-Stevens Point, US  
Dr. Pranam Paul, Narula Institute of Technology, Agarpara, West Bengal, India  
Assist. Prof. J. Ramkumar, V.L.B Janakiammal college of Arts & Science, India  
Mr. P. Sivakumar, Anna university, Chennai, India  
Mr. Md. Humayun Kabir Biswas, King Khalid University, Kingdom of Saudi Arabia  
Mr. Mayank Singh, J.P. Institute of Engg & Technology, Meerut, India  
HJ. Kamaruzaman Jusoff, Universiti Putra Malaysia  
Mr. Nikhil Patrick Lobo, CADES, India  
Dr. Amit Wason, Rayat-Bahra Institute of Engineering & Boi-Technology, India  
Dr. Rajesh Shrivastava, Govt. Benazir Science & Commerce College, Bhopal, India  
Assist. Prof. Vishal Bharti, DCE, Gurgaon  
Mrs. Sunita Bansal, Birla Institute of Technology & Science, India  
Dr. R. Sudhakar, Dr.Mahalingam college of Engineering and Technology, India  
Dr. Amit Kumar Garg, Shri Mata Vaishno Devi University, Katra(J&K), India  
Assist. Prof. Raj Gaurang Tiwari, AZAD Institute of Engineering and Technology, India  
Mr. Hamed Taherdoost, Tehran, Iran  
Mr. Amin Daneshmand Malayeri, YRC, IAU, Malayer Branch, Iran  
Mr. Shantanu Pal, University of Calcutta, India  
Dr. Terry H. Walcott, E-Promag Consultancy Group, United Kingdom  
Dr. Ezekiel U OKIKE, University of Ibadan, Nigeria  
Mr. P. Mahalingam, Caledonian College of Engineering, Oman  
Dr. Mahmoud M. A. Abd Ellatif, Mansoura University, Egypt

Prof. Kunwar S. Vaisla, BCT Kumaon Engineering College, India  
Prof. Mahesh H. Panchal, Kalol Institute of Technology & Research Centre, India  
Mr. Muhammad Asad, Technical University of Munich, Germany  
Mr. AliReza Shams Shafigh, Azad Islamic university, Iran  
Prof. S. V. Nagaraj, RMK Engineering College, India  
Mr. Ashikali M Hasan, Senior Researcher, CelNet security, India  
Dr. Adnan Shahid Khan, University Technology Malaysia, Malaysia  
Mr. Prakash Gajanan Burade, Nagpur University/ITM college of engg, Nagpur, India  
Dr. Jagdish B.Helonde, Nagpur University/ITM college of engg, Nagpur, India  
Professor, Doctor BOUHORMA Mohammed, Univertsity Abdelmalek Essaadi, Morocco  
Mr. K. Thirumalaivasan, Pondicherry Engg. College, India  
Mr. Umbarkar Anantkumar Janardan, Walchand College of Engineering, India  
Mr. Ashish Chaurasia, Gyan Ganga Institute of Technology & Sciences, India  
Mr. Sunil Taneja, Kurukshetra University, India  
Mr. Fauzi Adi Rafrastara, Dian Nuswantoro University, Indonesia  
Dr. Yaduvir Singh, Thapar University, India  
Dr. Ioannis V. Koskosas, University of Western Macedonia, Greece  
Dr. Vasantha Kalyani David, Avinashilingam University for women, Coimbatore  
Dr. Ahmed Mansour Manasrah, Universiti Sains Malaysia, Malaysia  
Miss. Nazanin Sadat Kazazi, University Technology Malaysia, Malaysia  
Mr. Saeed Rasouli Heikalabad, Islamic Azad University - Tabriz Branch, Iran  
Assoc. Prof. Dharendra Mishra, SVKM's NMIMS University, India  
Prof. Shapoor Zarei, UAE Inventors Association, UAE  
Prof. B.Raja Sarath Kumar, Lenora College of Engineering, India  
Dr. Bashir Alam, Jamia millia Islamia, Delhi, India  
Prof. Anant J Umbarkar, Walchand College of Engg., India  
Assist. Prof. B. Bharathi, Sathyabama University, India  
Dr. Fokrul Alom Mazarbhuiya, King Khalid University, Saudi Arabia  
Prof. T.S.Jeyali Laseeth, Anna University of Technology, Tirunelveli, India  
Dr. M. Balraju, Jawahar Lal Nehru Technological University Hyderabad, India  
Dr. Vijayalakshmi M. N., R.V.College of Engineering, Bangalore  
Prof. Walid Moudani, Lebanese University, Lebanon  
Dr. Saurabh Pal, VBS Purvanchal University, Jaunpur, India  
Associate Prof. Suneet Chaudhary, Dehradun Institute of Technology, India  
Associate Prof. Dr. Manuj Darbari, BBD University, India  
Ms. Prema Selvaraj, K.S.R College of Arts and Science, India  
Assist. Prof. Ms.S.Sasikala, KSR College of Arts & Science, India  
Mr. Sukhvinder Singh Deora, NC Institute of Computer Sciences, India  
Dr. Abhay Bansal, Amity School of Engineering & Technology, India  
Ms. Sumita Mishra, Amity School of Engineering and Technology, India  
Professor S. Viswanadha Raju, JNT University Hyderabad, India  
Mr. Asghar Shahrzad Khashandarag, Islamic Azad University Tabriz Branch, India  
Mr. Manoj Sharma, Panipat Institute of Engg. & Technology, India  
Mr. Shakeel Ahmed, King Faisal University, Saudi Arabia  
Dr. Mohamed Ali Mahjoub, Institute of Engineer of Monastir, Tunisia  
Mr. Adri Jovin J.J., SriGuru Institute of Technology, India  
Dr. Sukumar Senthilkumar, Universiti Sains Malaysia, Malaysia

Mr. Rakesh Bharati, Dehradun Institute of Technology Dehradun, India  
Mr. Shervan Fekri Ershad, Shiraz International University, Iran  
Mr. Md. Safiqul Islam, Daffodil International University, Bangladesh  
Mr. Mahmudul Hasan, Daffodil International University, Bangladesh  
Prof. Mandakini Tayade, UIT, RGTU, Bhopal, India  
Ms. Sarla More, UIT, RGTU, Bhopal, India  
Mr. Tushar Hrishikesh Jaware, R.C. Patel Institute of Technology, Shirpur, India  
Ms. C. Divya, Dr G R Damodaran College of Science, Coimbatore, India  
Mr. Fahimuddin Shaik, Annamacharya Institute of Technology & Sciences, India  
Dr. M. N. Giri Prasad, JNTUCE, Pulivendula, A.P., India  
Assist. Prof. Chintan M Bhatt, Charotar University of Science And Technology, India  
Prof. Sahista Machchhar, Marwadi Education Foundation's Group of institutions, India  
Assist. Prof. Navnish Goel, S. D. College Of Engineering & Technology, India  
Mr. Khaja Kamaluddin, Sirt University, Sirt, Libya  
Mr. Mohammad Zaidul Karim, Daffodil International, Bangladesh  
Mr. M. Vijayakumar, KSR College of Engineering, Tiruchengode, India  
Mr. S. A. Ahsan Rajon, Khulna University, Bangladesh  
Dr. Muhammad Mohsin Nazir, LCW University Lahore, Pakistan  
Mr. Mohammad Asadul Hoque, University of Alabama, USA  
Mr. P.V.Sarathchand, Indur Institute of Engineering and Technology, India  
Mr. Durgesh Samadhiya, Chung Hua University, Taiwan  
Dr Venu Kuthadi, University of Johannesburg, Johannesburg, RSA  
Dr. (Er) Jasvir Singh, Guru Nanak Dev University, Amritsar, Punjab, India  
Mr. Jasmin Cosic, Min. of the Interior of Una-sana canton, B&H, Bosnia and Herzegovina  
Dr S. Rajalakshmi, Botho College, South Africa  
Dr. Mohamed Sarrab, De Montfort University, UK  
Mr. Basappa B. Kodada, Canara Engineering College, India  
Assist. Prof. K. Ramana, Annamacharya Institute of Technology and Sciences, India  
Dr. Ashu Gupta, Apeejay Institute of Management, Jalandhar, India  
Assist. Prof. Shaik Rasool, Shadan College of Engineering & Technology, India  
Assist. Prof. K. Suresh, Annamacharya Institute of Tech & Sci. Rajampet, AP, India  
Dr . G. Singaravel, K.S.R. College of Engineering, India  
Dr B. G. Geetha, K.S.R. College of Engineering, India  
Assist. Prof. Kavita Choudhary, ITM University, Gurgaon  
Dr. Mehrdad Jalali, Azad University, Mashhad, Iran  
Megha Goel, Shamli Institute of Engineering and Technology, Shamli, India  
Mr. Chi-Hua Chen, Institute of Information Management, National Chiao-Tung University, Taiwan (R.O.C.)  
Assoc. Prof. A. Rajendran, RVS College of Engineering and Technology, India  
Assist. Prof. S. Jaganathan, RVS College of Engineering and Technology, India  
Assoc. Prof. (Dr.) A S N Chakravarthy, JNTUK University College of Engineering Vizianagaram (State University)  
Assist. Prof. Deepshikha Patel, Technocrat Institute of Technology, India  
Assist. Prof. Maram Balajee, GMRIT, India  
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 Sonar, 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 Rafiqhi, 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  
Assist. Prof. Shekhar. R, Dr.SM College of Engineering, India  
Prof. P. Senthilkumar, Vivekanandha Institue of Engineering and Technology for Woman, India  
Mr. M. Kamarajan, PSNA College of Engineering & Technology, India  
Dr. Angajala Srinivasa Rao, Jawaharlal Nehru Technical University, India  
Assist. Prof. C. Venkatesh, A.I.T.S, Rajampet, India  
Mr. Afshin Rezakhani Roozbahani, Ayatollah Boroujerdi University, Iran  
Mr. Laxmi chand, SCTL, Noida, India  
Dr. Dr. Abdul Hannan, Vivekanand College, Aurangabad  
Prof. Mahesh Panchal, KITRC, Gujarat  
Dr. A. Subramani, K.S.R. College of Engineering, Tiruchengode

Assist. Prof. Prakash M, Rajalakshmi Engineering College, Chennai, India  
Assist. Prof. Akhilesh K Sharma, Sir Padampat Singhanian University, India  
Ms. Varsha Sahni, Guru Nanak Dev Engineering College, Ludhiana, India  
Associate Prof. Trilochan Rout, NM Institute of Engineering and Technology, India  
Mr. Srikanta Kumar Mohapatra, NMIET, Orissa, India  
Mr. Waqas Haider Bangyal, Iqra University Islamabad, Pakistan  
Dr. S. Vijayaragavan, Christ College of Engineering and Technology, Pondicherry, India  
Prof. Elboukhari Mohamed, University Mohammed First, Oujda, Morocco  
Dr. Muhammad Asif Khan, King Faisal University, Saudi Arabia  
Dr. Nagy Ramadan Darwish Omran, Cairo University, Egypt.  
Assistant Prof. Anand Nayyar, KCL Institute of Management and Technology, India  
Mr. G. Premsankar, Ericsson, India  
Assist. Prof. T. Hemalatha, VELS University, India  
Prof. Tejaswini Apte, University of Pune, India  
Dr. Edmund Ng Giap Weng, Universiti Malaysia Sarawak, Malaysia  
Mr. Mahdi Nouri, Iran University of Science and Technology, Iran  
Associate Prof. S. Asif Hussain, Annamacharya Institute of technology & Sciences, India  
Mrs. Kavita Pabreja, Maharaja Surajmal Institute (an affiliate of GGSIP University), India  
Mr. Vorugunti Chandra Sekhar, DA-IICT, India  
Mr. Muhammad Najmi Ahmad Zabidi, Universiti Teknologi Malaysia, Malaysia  
Dr. Aderemi A. Atayero, Covenant University, Nigeria  
Assist. Prof. Osama Sohaib, Balochistan University of Information Technology, Pakistan  
Assist. Prof. K. Suresh, Annamacharya Institute of Technology and Sciences, India  
Mr. Hassen Mohammed Abdullaah Alsafi, International Islamic University Malaysia (IIUM) Malaysia  
Mr. Robail Yasrab, Virtual University of Pakistan, Pakistan  
Mr. R. Balu, Bharathiar University, Coimbatore, India  
Prof. Anand Nayyar, KCL Institute of Management and Technology, Jalandhar  
Assoc. Prof. Vivek S Deshpande, MIT College of Engineering, India  
Prof. K. Saravanan, Anna university Coimbatore, India  
Dr. Ravendra Singh, MJP Rohilkhand University, Bareilly, India  
Mr. V. Mathivanan, IBRA College of Technology, Sultanate of OMAN  
Assoc. Prof. S. Asif Hussain, AITS, India  
Assist. Prof. C. Venkatesh, AITS, India  
Mr. Sami Ulhaq, SZABIST Islamabad, Pakistan  
Dr. B. Justus Rabi, Institute of Science & Technology, India  
Mr. Anuj Kumar Yadav, Dehradun Institute of technology, India  
Mr. Alejandro Mosquera, University of Alicante, Spain  
Assist. Prof. Arjun Singh, Sir Padampat Singhanian University (SPSU), Udaipur, India  
Dr. Smriti Agrawal, JB Institute of Engineering and Technology, Hyderabad  
Assist. Prof. Swathi Sambangi, Visakha Institute of Engineering and Technology, India  
Ms. Prabhjot Kaur, Guru Gobind Singh Indraprastha University, India  
Mrs. Samaher AL-Hothali, Yanbu University College, Saudi Arabia  
Prof. Rajneeshkaur Bedi, MIT College of Engineering, Pune, India  
Mr. Hassen Mohammed Abdullaah Alsafi, International Islamic University Malaysia (IIUM)  
Dr. Wei Zhang, Amazon.com, Seattle, WA, USA  
Mr. B. Santhosh Kumar, C S I College of Engineering, Tamil Nadu  
Dr. K. Reji Kumar, N S S College, Pandalam, India



Assoc. Prof. K. Seshadri Sastry, EILM University, India  
Mr. Kai Pan, UNC Charlotte, USA  
Mr. Ruikar Sachin, SGGSIET, India  
Prof. (Dr.) Vinodani Katiyar, Sri Ramswaroop Memorial University, India  
Assoc. Prof., M. Giri, Sreenivasa Institute of Technology and Management Studies, India  
Assoc. Prof. Labib Francis Gergis, Misr Academy for Engineering and Technology (MET), Egypt  
Assist. Prof. Amanpreet Kaur, ITM University, India  
Assist. Prof. Anand Singh Rajawat, Shri Vaishnav Institute of Technology & Science, Indore  
Mrs. Hadeel Saleh Haj Aliwi, Universiti Sains Malaysia (USM), Malaysia  
Dr. Abhay Bansal, Amity University, India  
Dr. Mohammad A. Mezher, Fahad Bin Sultan University, KSA  
Assist. Prof. Nidhi Arora, M.C.A. Institute, India  
Prof. Dr. P. Suresh, Karpagam College of Engineering, Coimbatore, India  
Dr. Kannan Balasubramanian, Mepco Schlenk Engineering College, India  
Dr. S. Sankara Gomathi, Panimalar Engineering college, India  
Prof. Anil kumar Suthar, Gujarat Technological University, L.C. Institute of Technology, India  
Assist. Prof. R. Hubert Rajan, NOORUL ISLAM UNIVERSITY, India  
Assist. Prof. Dr. Jyoti Mahajan, College of Engineering & Technology  
Assist. Prof. Homam Reda El-Taj, College of Network Engineering, Saudi Arabia & Malaysia  
Mr. Bijan Paul, Shahjalal University of Science & Technology, Bangladesh  
Assoc. Prof. Dr. Ch V Phani Krishna, KL University, India  
Dr. Vishal Bhatnagar, Ambedkar Institute of Advanced Communication Technologies & Research, India  
Dr. Lamir LAOUAMER, Al Qassim University, Dept. Info. Systems & European University of Brittany, Dept. Computer Science, UBO, Brest, France  
Prof. Ashish Babanrao Sasankar, G.H.Raisoni Institute Of Information Technology, India  
Prof. Pawan Kumar Goel, Shamli Institute of Engineering and Technology, India  
Mr. Ram Kumar Singh, S.V Subharti University, India  
Assistant Prof. Sunish Kumar O S, Amalijothei College of Engineering, India  
Dr Sanjay Bhargava, Banasthali University, India  
Mr. Pankaj S. Kulkarni, AVEW's Shatabdi Institute of Technology, India  
Mr. Roohollah Etemadi, Islamic Azad University, Iran  
Mr. Oloruntoyin Sefiu Taiwo, Emmanuel Alayande College Of Education, Nigeria  
Mr. Sumit Goyal, National Dairy Research Institute, India  
Mr Jaswinder Singh Dilawari, Geeta Engineering College, India  
Prof. Raghuraj Singh, Harcourt Butler Technological Institute, Kanpur  
Dr. S.K. Mahendran, Anna University, Chennai, India  
Dr. Amit Wason, Hindustan Institute of Technology & Management, Punjab  
Dr. Ashu Gupta, Apeejay Institute of Management, India  
Assist. Prof. D. Asir Antony Gnana Singh, M.I.E.T Engineering College, India  
Mrs Mina Farmanbar, Eastern Mediterranean University, Famagusta, North Cyprus  
Mr. Maram Balajee, GMR Institute of Technology, India  
Mr. Moiz S. Ansari, Isra University, Hyderabad, Pakistan  
Mr. Adebayo, Olawale Surajudeen, Federal University of Technology Minna, Nigeria  
Mr. Jasvir Singh, University College Of Engg., India  
Mr. Vivek Tiwari, MANIT, Bhopal, India  
Assoc. Prof. R. Navaneethakrishnan, Bharathiyar College of Engineering and Technology, India  
Mr. Somdip Dey, St. Xavier's College, Kolkata, India

Mr. Souleymane Balla-Arabé, Xi'an University of Electronic Science and Technology, China  
Mr. Mahabub Alam, Rajshahi University of Engineering and Technology, Bangladesh  
Mr. Sathyapraksh P., S.K.P Engineering College, India  
Dr. N. Karthikeyan, SNS College of Engineering, Anna University, India  
Dr. Binod Kumar, JSPM's, Jayawant Technical Campus, Pune, India  
Assoc. Prof. Dinesh Goyal, Suresh Gyan Vihar University, India  
Mr. Md. Abdul Ahad, K L University, India  
Mr. Vikas Bajpai, The LNM IIT, India  
Dr. Manish Kumar Anand, Salesforce (R & D Analytics), San Francisco, USA  
Assist. Prof. Dheeraj Murari, Kumaon Engineering College, India  
Assoc. Prof. Dr. A. Muthukumaravel, VELS University, Chennai  
Mr. A. Siles Balasingh, St. Joseph University in Tanzania, Tanzania  
Mr. Ravindra Daga Badgujar, R C Patel Institute of Technology, India  
Dr. Preeti Khanna, SVKM's NMIMS, School of Business Management, India  
Mr. Kumar Dayanand, Cambridge Institute of Technology, India  
Dr. Syed Asif Ali, SMI University Karachi, Pakistan  
Prof. Pallvi Pandit, Himachal Pradesh University, India  
Mr. Ricardo Verschueren, University of Gloucestershire, UK  
Assist. Prof. Mamta Juneja, University Institute of Engineering and Technology, Panjab University, India  
Assoc. Prof. P. Surendra Varma, NRI Institute of Technology, JNTU Kakinada, India  
Assist. Prof. Gaurav Shrivastava, RGPV / SVITS Indore, India  
Dr. S. Sumathi, Anna University, India  
Assist. Prof. Ankita M. Kapadia, Charotar University of Science and Technology, India  
Mr. Deepak Kumar, Indian Institute of Technology (BHU), India  
Dr. Dr. Rajan Gupta, GGSIP University, New Delhi, India  
Assist. Prof. M. Anand Kumar, Karpagam University, Coimbatore, India  
Mr. Mr Arshad Mansoor, Pakistan Aeronautical Complex  
Mr. Kapil Kumar Gupta, Ansal Institute of Technology and Management, India  
Dr. Neeraj Tomer, SINE International Institute of Technology, Jaipur, India  
Assist. Prof. Trunal J. Patel, C.G.Patel Institute of Technology, Uka Tarsadia University, Bardoli, Surat  
Mr. Sivakumar, Codework solutions, India  
Mr. Mohammad Sadegh Mirzaei, PGNR Company, Iran  
Dr. Gerard G. Dumancas, Oklahoma Medical Research Foundation, USA  
Mr. Varadala Sridhar, Varadhman College Engineering College, Affiliated To JNTU, Hyderabad  
Assist. Prof. Manoj Dhawan, SVITS, Indore  
Assoc. Prof. Chitreshh Banerjee, Suresh Gyan Vihar University, Jaipur, India  
Dr. S. Santhi, SCSVMV University, India  
Mr. Davood Mohammadi Souran, Ministry of Energy of Iran, Iran  
Mr. Shamim Ahmed, Bangladesh University of Business and Technology, Bangladesh  
Mr. Sandeep Reddivari, Mississippi State University, USA  
Assoc. Prof. Ousmane Thiare, Gaston Berger University, Senegal  
Dr. Hazra Imran, Athabasca University, Canada  
Dr. Setu Kumar Chaturvedi, Technocrats Institute of Technology, Bhopal, India  
Mr. Mohd Dilshad Ansari, Jaypee University of Information Technology, India  
Ms. Jaspreet Kaur, Distance Education LPU, India  
Dr. D. Nagarajan, Salalah College of Technology, Sultanate of Oman  
Dr. K.V.N.R.Sai Krishna, S.V.R.M. College, India

Mr. Himanshu Pareek, Center for Development of Advanced Computing (CDAC), India  
Mr. Khaldi Amine, Badji Mokhtar University, Algeria  
Mr. Mohammad Sadegh Mirzaei, Scientific Applied University, Iran  
Assist. Prof. Khyati Chaudhary, Ram-eesh Institute of Engg. & Technology, India  
Mr. Sanjay Agal, Pacific College of Engineering Udaipur, India  
Mr. Abdul Mateen Ansari, King Khalid University, Saudi Arabia  
Dr. H.S. Behera, Veer Surendra Sai University of Technology (VSSUT), India  
Dr. Shrikant Tiwari, Shri Shankaracharya Group of Institutions (SSGI), India  
Prof. Ganesh B. Regulwar, Shri Shankarprasad Agnihotri College of Engg, India  
Prof. Pinnamaneni Bhanu Prasad, Matrix vision GmbH, Germany  
Dr. Shrikant Tiwari, Shri Shankaracharya Technical Campus (SSTC), India  
Dr. Siddesh G.K., : Dayananada Sagar College of Engineering, Bangalore, India  
Dr. Nadir Bouchama, CERIST Research Center, Algeria  
Dr. R. Sathishkumar, Sri Venkateswara College of Engineering, India  
Assistant Prof (Dr.) Mohamed Moussaoui, Abdelmalek Essaadi University, Morocco  
Dr. S. Malathi, Panimalar Engineering College, Chennai, India  
Dr. V. Subedha, Panimalar Institute of Technology, Chennai, India  
Dr. Prashant Panse, Swami Vivekanand College of Engineering, Indore, India  
Dr. Hamza Aldabbas, Al-Balqa'a Applied University, Jordan  
Dr. G. Rasitha Banu, Vel's University, Chennai  
Dr. V. D. Ambeth Kumar, Panimalar Engineering College, Chennai  
Prof. Anuranjan Misra, Bhagwant Institute of Technology, Ghaziabad, India  
Ms. U. Sinthuja, PSG college of arts &science, India  
Dr. Ehsan Saradar Torshizi, Urmia University, Iran  
Dr. Shamneesh Sharma, APG Shimla University, Shimla (H.P.), India  
Assistant Prof. A. S. Syed Navaz, Muthayammal College of Arts & Science, India  
Assistant Prof. Ranjit Panigrahi, Sikkim Manipal Institute of Technology, Majitar, Sikkim  
Dr. Khaled Eskaf, Arab Academy for Science ,Technology & Maritime Transportation, Egypt  
Dr. Nishant Gupta, University of Jammu, India  
Assistant Prof. Nagarajan Sankaran, Annamalai University, Chidambaram, Tamilnadu, India  
Assistant Prof. Tribikram Pradhan, Manipal Institute of Technology, India  
Dr. Nasser Lotfi, Eastern Mediterranean University, Northern Cyprus  
Dr. R. Manavalan, K S Rangasamy college of Arts and Science, Tamilnadu, India  
Assistant Prof. P. Krishna Sankar, K S Rangasamy college of Arts and Science, Tamilnadu, India  
Dr. Rahul Malik, Cisco Systems, USA  
Dr. S. C. Lingareddy, ALPHA College of Engineering, India  
Assistant Prof. Mohammed Shuaib, Interat University, Lucknow, India  
Dr. Sachin Yele, Sanghvi Institute of Management & Science, India  
Dr. T. Thambidurai, Sun Univercell, Singapore  
Prof. Anandkumar Telang, BKIT, India  
Assistant Prof. R. Poorvadevi, SCSVMV University, India  
Dr Uttam Mande, Gitam University, India  
Dr. Poornima Girish Naik, Shahu Institute of Business Education and Research (SIBER), India  
Prof. Md. Abu Kausar, Jaipur National University, Jaipur, India  
Dr. Mohammed Zuber, AISECT University, India  
Prof. Kalum Priyanath Udagepola, King Abdulaziz University, Saudi Arabia  
Dr. K. R. Ananth, Velalar College of Engineering and Technology, India

Assistant Prof. Sanjay Sharma, Roorkee Engineering & Management Institute Shamli (U.P), India  
Assistant Prof. Panem Charan Arur, Priyadarshini Institute of Technology, India  
Dr. Ashwak Mahmood muhsen alabaichi, Karbala University / College of Science, Iraq  
Dr. Urmila Shrawankar, G H Raison College of Engineering, Nagpur (MS), India  
Dr. Krishan Kumar Paliwal, Panipat Institute of Engineering & Technology, India  
Dr. Mukesh Negi, Tech Mahindra, India  
Dr. Anuj Kumar Singh, Amity University Gurgaon, India  
Dr. Babar Shah, Gyeongsang National University, South Korea  
Assistant Prof. Jayprakash Upadhyay, SRI-TECH Jabalpur, India  
Assistant Prof. Varadala Sridhar, Vidya Jyothi Institute of Technology, India  
Assistant Prof. Parameshachari B D, KSIT, Bangalore, India  
Assistant Prof. Ankit Garg, Amity University, Haryana, India  
Assistant Prof. Rajashe Karappa, SDMCET, Karnataka, India  
Assistant Prof. Varun Jasuja, GNIT, India  
Assistant Prof. Sonal Honale, Abha Gaikwad Patil College of Engineering Nagpur, India  
Dr. Pooja Choudhary, CT Group of Institutions, NIT Jalandhar, India  
Dr. Faouzi Hidoussi, UHL Batna, Algeria  
Dr. Naseer Ali Hussein, Wasit University, Iraq  
Assistant Prof. Vinod Kumar Shukla, Amity University, Dubai  
Dr. Ahmed Farouk Metwaly, K L University  
Mr. Mohammed Noaman Murad, Cihan University, Iraq  
Dr. Suxing Liu, Arkansas State University, USA  
Dr. M. Gomathi, Velalar College of Engineering and Technology, India  
Assistant Prof. Sumardiono, College PGRI Blitar, Indonesia  
Dr. Latika Kharb, Jagan Institute of Management Studies (JIMS), Delhi, India  
Associate Prof. S. Raja, Pauls College of Engineering and Technology, Tamilnadu, India  
Assistant Prof. Seyed Reza Pakize, Shahid Sani High School, Iran  
Dr. Thiyagu Nagaraj, University-INO, India  
Assistant Prof. Noreen Sarai, Harare Institute of Technology, Zimbabwe  
Assistant Prof. Gajanand Sharma, Suresh Gyan Vihar University Jaipur, Rajasthan, India  
Assistant Prof. Mapari Vikas Prakash, Siddhant COE, Sudumbare, Pune, India  
Dr. Devesh Katiyar, Shri Ramswaroop Memorial University, India  
Dr. Shenshen Liang, University of California, Santa Cruz, US  
Assistant Prof. Mohammad Abu Omar, Limkokwing University of Creative Technology- Malaysia  
Mr. Snehasis Banerjee, Tata Consultancy Services, India  
Assistant Prof. Kibona Lusekelo, Ruaha Catholic University (RUCU), Tanzania  
Assistant Prof. Adib Kabir Chowdhury, University College Technology Sarawak, Malaysia  
Dr. Ying Yang, Computer Science Department, Yale University, USA  
Dr. Vinay Shukla, Institute Of Technology & Management, India  
Dr. Liviu Octavian Maftciu-Scai, West University of Timisoara, Romania  
Assistant Prof. Rana Khudhair Abbas Ahmed, Al-Rafidain University College, Iraq  
Assistant Prof. Nitin A. Naik, S.R.T.M. University, India  
Dr. Timothy Powers, University of Hertfordshire, UK  
Dr. S. Prasath, Bharathiar University, Erode, India  
Dr. Ritu Shrivastava, SIRTIS Bhopal, India  
Prof. Rohit Shrivastava, Mittal Institute of Technology, Bhopal, India  
Dr. Gianina Mihai, Dunarea de Jos" University of Galati, Romania

Assistant Prof. Ms. T. Kalai Selvi, Erode Sengunthar Engineering College, India  
Assistant Prof. Ms. C. Kavitha, Erode Sengunthar Engineering College, India  
Assistant Prof. K. Sinivasamoorthi, Erode Sengunthar Engineering College, India  
Assistant Prof. Mallikarjun C Sarsamba Bheemna Khandre Institute Technology, Bhalki, India  
Assistant Prof. Vishwanath Chikaraddi, Veermata Jijabai technological Institute (Central Technological Institute), India  
Assistant Prof. Dr. Ikvinderpal Singh, Trai Shatabdi GGS Khalsa College, India  
Assistant Prof. Mohammed Noaman Murad, Cihan University, Iraq  
Professor Yousef Farhaoui, Moulay Ismail University, Errachidia, Morocco  
Dr. Parul Verma, Amity University, India  
Professor Yousef Farhaoui, Moulay Ismail University, Errachidia, Morocco  
Assistant Prof. Madhavi Dhingra, Amity University, Madhya Pradesh, India  
Assistant Prof.. G. Selvavinayagam, SNS College of Technology, Coimbatore, India  
Assistant Prof. Madhavi Dhingra, Amity University, MP, India  
Professor Kartheesan Log, Anna University, Chennai  
Professor Vasudeva Acharya, Shri Madhwa vadiraja Institute of Technology, India  
Dr. Asif Iqbal Hajamydeen, Management & Science University, Malaysia  
Assistant Prof., Mahendra Singh Meena, Amity University Haryana  
Assistant Professor Manjeet Kaur, Amity University Haryana  
Dr. Mohamed Abd El-Basset Matwalli, Zagazig University, Egypt  
Dr. Ramani Kannan, Universiti Teknologi PETRONAS, Malaysia  
Assistant Prof. S. Jagadeesan Subramaniam, Anna University, India  
Assistant Prof. Dharmendra Choudhary, Tripura University, India  
Assistant Prof. Deepika Vodnala, SR Engineering College, India  
Dr. Kai Cong, Intel Corporation & Computer Science Department, Portland State University, USA  
Dr. Kailas R Patil, Vishwakarma Institute of Information Technology (VIIT), India  
Dr. Omar A. Alzubi, Faculty of IT / Al-Balqa Applied University, Jordan  
Assistant Prof. Kareemullah Shaik, Nimra Institute of Science and Technology, India  
Assistant Prof. Chirag Modi, NIT Goa  
Dr. R. Ramkumar, Nandha Arts And Science College, India  
Dr. Priyadarshini Vydhialingam, Harathiar University, India  
Dr. P. S. Jagadeesh Kumar, DBIT, Bangalore, Karnataka  
Dr. Vikas Thada, AMITY University, Pachgaon  
Dr. T. A. Ashok Kumar, Institute of Management, Christ University, Bangalore  
Dr. Shaheera Rashwan, Informatics Research Institute  
Dr. S. Preetha Gunasekar, Bharathiyar University, India  
Asst Professor Sameer Dev Sharma, Uttaranchal University, Dehradun  
Dr. Zhihan Iv, Chinese Academy of Science, China  
Dr. Ikvinderpal Singh, Trai Shatabdi GGS Khalsa College, Amritsar  
Dr. Umar Ruhi, University of Ottawa, Canada  
Dr. Jasmin Cosic, University of Bihac, Bosnia and Herzegovina  
Dr. Homam Reda El-Taj, University of Tabuk, Kingdom of Saudi Arabia  
Dr. Mostafa Ghobaei Arani, Islamic Azad University, Iran  
Dr. Ayyasamy Ayyanar, Annamalai University, India  
Dr. Selvakumar Manickam, Universiti Sains Malaysia, Malaysia  
Dr. Murali Krishna Namana, GITAM University, India  
Dr. Smriti Agrawal, Chaitanya Bharathi Institute of Technology, Hyderabad, India  
Professor Vimalathithan Rathinasabapathy, Karpagam College Of Engineering, India

Dr. Sushil Chandra Dimri, Graphic Era University, India  
Dr. Dinh-Sinh Mai, Le Quy Don Technical University, Vietnam  
Dr. S. Rama Sree, Aditya Engg. College, India  
Dr. Ehab T. Alnfwawy, Sadat Academy, Egypt  
Dr. Patrick D. Cerna, Haramaya University, Ethiopia  
Dr. Vishal Jain, Bharati Vidyapeeth's Institute of Computer Applications and Management (BVICAM), India  
Associate Prof. Dr. Jiliang Zhang, North Eastern University, China  
Dr. Sharefa Murad, Middle East University, Jordan  
Dr. Ajeet Singh Poonia, Govt. College of Engineering & technology, Rajasthan, India  
Dr. Vahid Esmaeaelzadeh, University of Science and Technology, Iran  
Dr. Jacek M. Czerniak, Casimir the Great University in Bydgoszcz, Institute of Technology, Poland  
Associate Prof. Anisur Rehman Nasir, Jamia Millia Islamia University  
Assistant Prof. Imran Ahmad, COMSATS Institute of Information Technology, Pakistan  
Professor Ghulam Qasim, Preston University, Islamabad, Pakistan  
Dr. Parameshachari B D, GSSS Institute of Engineering and Technology for Women  
Dr. Wencan Luo, University of Pittsburgh, US  
Dr. Musa PEKER, Faculty of Technology, Mugla Sitki Kocman University, Turkey  
Dr. Gunasekaran Shanmugam, Anna University, India  
Dr. Binh P. Nguyen, National University of Singapore, Singapore  
Dr. Rajkumar Jain, Indian Institute of Technology Indore, India  
Dr. Imtiaz Ali Halepoto, QUEST Nawabshah, Pakistan  
Dr. Shaligram Prajapat, Devi Ahilya University Indore India  
Dr. Sunita Singhal, Birla Institute of Technology and Science, Pilani, India  
Dr. Ijaz Ali Shoukat, King Saud University, Saudi Arabia  
Dr. Anuj Gupta, IKG Punjab Technical University, India  
Dr. Sonali Saini, IES-IPS Academy, India  
Dr. Krishan Kumar, MotiLal Nehru National Institute of Technology, Allahabad, India  
Dr. Z. Faizal Khan, College of Engineering, Shaqra University, Kingdom of Saudi Arabia  
Prof. M. Padmavathamma, S.V. University Tirupati, India  
Prof. A. Velayudham, Cape Institute of Technology, India  
Prof. Seifeidne Kadry, American University of the Middle East  
Dr. J. Durga Prasad Rao, Pt. Ravishankar Shukla University, Raipur  
Assistant Prof. Najam Hasan, Dhofar University  
Dr. G. Suseendran, Vels University, Pallavaram, Chennai  
Prof. Ankit Faldu, Gujarat Technological University- Atmiya Institute of Technology and Science  
Dr. Ali Habiboghli, Islamic Azad University  
Dr. Deepak Dembla, JECRC University, Jaipur, India  
Dr. Pankaj Rajan, Walmart Labs, USA  
Assistant Prof. Radoslava Kraveva, South-West University "Neofit Rilski", Bulgaria  
Assistant Prof. Medhavi Shriwas, Shri vaishnav institute of Technology, India  
Associate Prof. Sedat Akleylek, Ondokuz Mayıs University, Turkey  
Dr. U.V. Arivazhagu, Kingston Engineering College Affiliated To Anna University, India  
Dr. Touseef Ali, University of Engineering and Technology, Taxila, Pakistan  
Assistant Prof. Naren Jeeva, SASTRA University, India  
Dr. Riccardo Colella, University of Salento, Italy  
Dr. Enache Maria Cristina, University of Galati, Romania  
Dr. Senthil P, Kurinji College of Arts & Science, India

Dr. Hasan Ashrafi-rizi, Isfahan University of Medical Sciences, Isfahan, Iran  
Dr. Mazhar Malik, Institute of Southern Punjab, Pakistan  
Dr. Yajie Miao, Carnegie Mellon University, USA  
Dr. Kamran Shaukat, University of the Punjab, Pakistan  
Dr. Sasikaladevi N., SASTRA University, India  
Dr. Ali Asghar Rahmani Hosseinabadi, Islamic Azad University Ayatollah Amoli Branch, Amol, Iran  
Dr. Velin Kralev, South-West University "Neofit Rilski", Blagoevgrad, Bulgaria  
Dr. Marius Iulian Mihailescu, LUMINA - The University of South-East Europe  
Dr. Sriramula Nagaprasad, S.R.R.Govt.Arts & Science College, Karimnagar, India  
Prof (Dr.) Namrata Dhanda, Dr. APJ Abdul Kalam Technical University, Lucknow, India  
Dr. Javed Ahmed Mahar, Shah Abdul Latif University, Khairpur Mir's, Pakistan  
Dr. B. Narendra Kumar Rao, Sree Vidyanikethan Engineering College, India  
Dr. Shahzad Anwar, University of Engineering & Technology Peshawar, Pakistan  
Dr. Basit Shahzad, King Saud University, Riyadh - Saudi Arabia  
Dr. Nilamadhab Mishra, Chang Gung University  
Dr. Sachin Kumar, Indian Institute of Technology Roorkee  
Dr. Santosh Nanda, Biju-Pattnaik University of Technology  
Dr. Sherzod Turaev, International Islamic University Malaysia  
Dr. Yilun Shang, Tongji University, Department of Mathematics, Shanghai, China  
Dr. Nuzhat Shaikh, Modern Education society's College of Engineering, Pune, India  
Dr. Parul Verma, Amity University, Lucknow campus, India  
Dr. Rachid Alaoui, Agadir Ibn Zohr University, Agadir, Morocco  
Dr. Dharmendra Patel, Charotar University of Science and Technology, India  
Dr. Dong Zhang, University of Central Florida, USA  
Dr. Kennedy Chinedu Okafor, Federal University of Technology Owerri, Nigeria  
Prof. C Ram Kumar, Dr NGP Institute of Technology, India  
Dr. Sandeep Gupta, GGS IP University, New Delhi, India  
Dr. Shahanawaj Ahamad, University of Ha'il, Ha'il City, Ministry of Higher Education, Kingdom of Saudi Arabia  
Dr. Najeed Ahmed Khan, NED University of Engineering & Technology, India  
Dr. Sajid Ullah Khan, Universiti Malaysia Sarawak, Malaysia  
Dr. Muhammad Asif, National Textile University Faisalabad, Pakistan  
Dr. Yu BI, University of Central Florida, Orlando, FL, USA  
Dr. Brijendra Kumar Joshi, Research Center, Military College of Telecommunication Engineering, India  
Prof. Dr. Nak Eun Cho, Pukyong National University, Korea  
Prof. Wasim Ul-Haq, Faculty of Science, Majmaah University, Saudi Arabia  
Dr. Mohsan Raza, G.C University Faisalabad, Pakistan  
Dr. Syed Zakar Hussain Bukhari, National Science and Technology Azad Jamu Kashmir, Pakistan  
Dr. Ruksar Fatima, KBN College of Engineering, Gulbarga, Karnataka, India  
Associate Professor S. Karpagavalli, Department of Computer Science, PSGR Krishnammal College for Women  
Coimbatore, Tamilnadu, India  
Dr. Bushra Mohamed Elamin Elhaim, Prince Sattam bin Abdulaziz University, Saudi Arabia  
Dr. Shamik Tiwari, Department of CSE, CET, Mody University, Lakshmangarh  
Dr. Rohit Raja, Faculty of Engineering and Technology, Shri Shankaracharya Group of Institutions, India  
Prof. Dr. Aqeel-ur-Rehman, Department of Computing, HIET, FEST, Hamdard University, Pakistan  
Dr. Nageswara Rao Moparthi, Velagapudi Ramakrishna Siddhartha Engineering College, India  
Dr. Mohd Muqem, Department of Computer Application, Integral University, Lucknow, India  
Dr. Zeeshan Bhatti, Institute of Information and Communication Technology, University of Sindh, Jamshoro, Pakistan

Dr. Emrah Irmak, Biomedical Engineering Department, Karabuk University, Turkey

Dr. Fouad Abdulameer salman, School of Informatics and Applied Mathematics, Universiti Malaysia Terengganu

Dr. N. Prasath, Department of Computer Science and Engineering, KPR Institute of Engineering and Technology, Arasur, Coimbatore

Dr. Hasan Ashrafi-rizi, Health Information Technology Research Center, Isfahan University of Medical Sciences, Hezar Jerib Avenue, Isfahan, Iran

Dr. N. Sasikaladevi, School of Computing, SASTRA University, Thirumalisamudram, Tamilnadu, India.

Dr. Anchit Bijalwan, Arba Minch University, Ethiopia

Dr. K. Sathishkumar, BlueCrest University College, Accra North, Ghana, West Africa

Dr. Dr. Parameshachari B D, GSSS Institute of Engineering and Technology for Women, Affiliated to Visvesvaraya Technological University, Belagavi

Dr. C. Shoba Bindu, Dept. of CSE, JNTUA College of Engineering, India

Dr. M. Inbavalli, ER. Perumal Manimekalai College of Engineering, Hosur, Tamilnadu, India

Dr. Vidya Sagar Ponnamp, Dept. of IT, Velagapudi Ramakrishna Siddhartha Engineering College, India

Dr. Kelvin LO M. F., The Hong Kong Polytechnic University, Hong Kong

Prof. Karimella Vikram, G.H. Rasoni College of Engineering & Management, Pune, India

Dr. Shajilin Loret J.B., VV College of Engineering, India

Dr. P. Sujatha, Department of Computer Science at Vels University, Chennai

Dr. Vaibhav Sundriyal, Old Dominion University Research Foundation, USA

Dr. Md Masud Rana, Khulna University of Engineering and Technology, Bangladesh

Dr. Gurcharan Singh, Khalsa College Amritsar, Guru Nanak Dev University, Amritsar, India

Dr. Richard Otieno Omollo, Department of Computer Science and Software Engineering, Jaramogi Oginga Odinga University of Science and Technology, Kenya

Prof. (Dr) Amit Verma, Computer Science & Engineering, Chandigarh Engineering College, Landran, Mohali, India

Dr. Vidya Sagar Ponnamp, Velagapudi Ramakrishna Siddhartha Engineering College, India

Dr. Bohui Wang, School of Aerospace Science and Technology, Xidian University, P.R. China

Dr. M. Anjan Kumar, Department of Computer Science, Satavahana University, Karimnagar

Dr. Hanumanthappa J., DoS in CS, Uni of Mysuru, Karnataka, India

Dr. Pouya Derakhshan-Barjoei, Dept. of Telecommunication and Engineering, Islamic Azad University, Iran

Dr. Tanweer Alam, Islamic University of Madinah, Dept. of Computer Science, College of Computer and Information System, Al Madinah, Saudi Arabia

Dr. Kumar Keshamoni, Dept. of ECE, Vaagdevi Engineering College, Warangal, Telangana, India

Dr. G. Rajkumar, N.M.S.S.Vellaichamy Nadar College, Madurai, Tamilnadu, India

Dr. P. Mayil Vel Kumar, Karpagam Institute of Technology, Coimbatore, India

Dr. M. Yaswanth Bhanu Murthy, Vasireddy Venkatadri Institute of Technology, Guntur, A.P., India

Asst. Prof. Dr. Mehmet Barış TABAKCIOĞLU, Bursa Technical University, Turkey

Dr. Mohd. Muntjir, College of Computers and Information Technology, Taif University, Kingdom of Saudi Arabia

Dr. Sanjay Agal, Aravali Institute of Technical Studies, Udaipur, India

Dr. Shanshan Tuo, xAd Inc., US

Dr. Subhadra Shaw, AKS University, Satna, India

Dr. Piyush Anand, Noida International University, Greater Noida, India

Dr. Brijendra Kumar Joshi, Research Center Military College of Telecommunication Engineering, India

Dr. V. Sreerama Murthy, GMRIT, Rajam, AP, India

Dr. S. Nagarajan, Annamalai University, India

Prof. Pramod Bhausaheb Deshmukh, D. Y. Patil College of Engineering, Akurdi, Pune, India



# CALL FOR PAPERS

## International Journal of Computer Science and Information Security

**IJCSIS 2021-2022**

**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, Embedded 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](mailto: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> .



**© IJCSIS PUBLICATION 2021**

**ISSN 1947 5500**

**<http://sites.google.com/site/ijcsis/>**