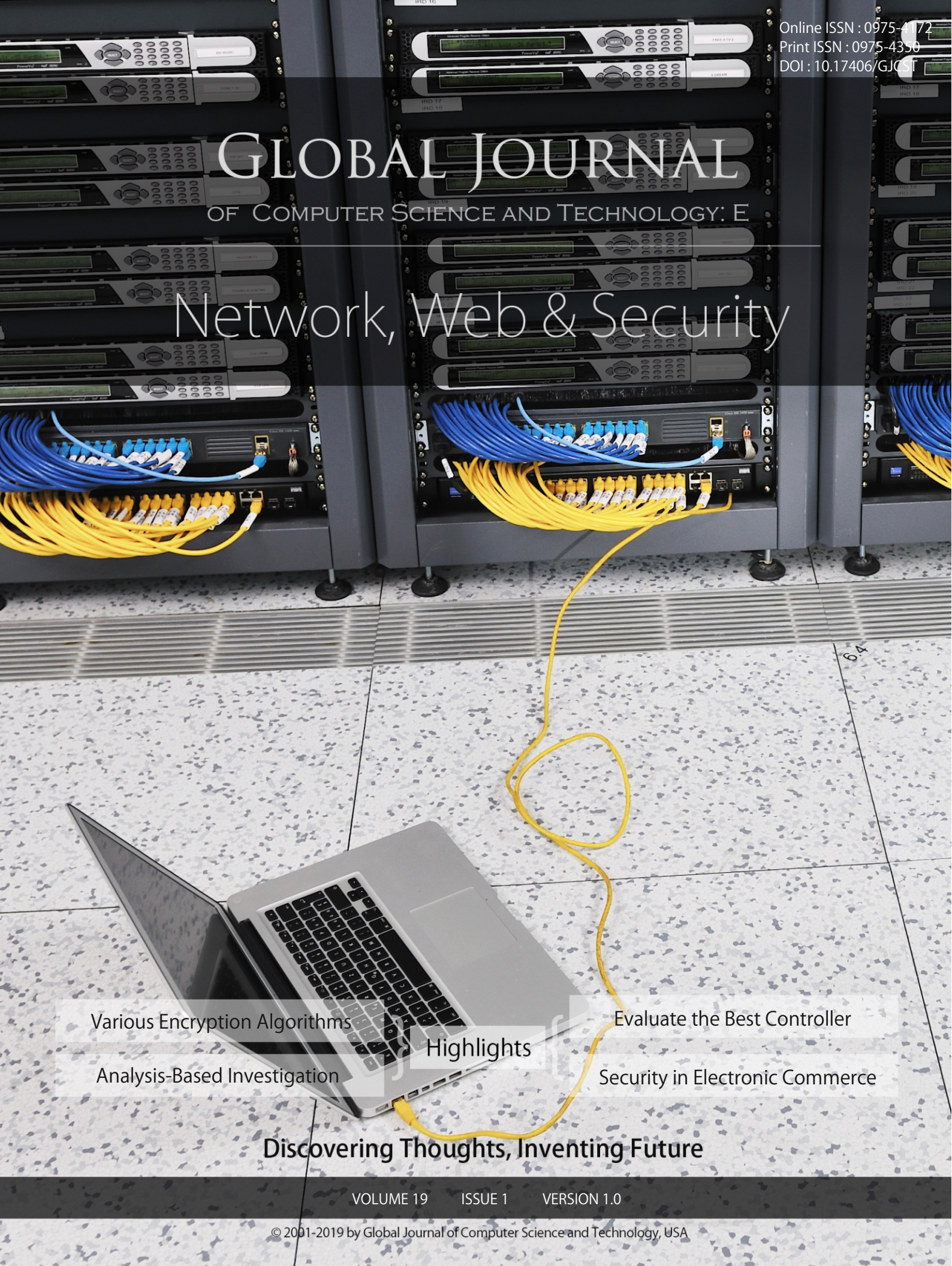
Online ISSN : 0975-4172
Print ISSN : 0975-4350
DOI : 10.17406/GJCST

Global Journal

of Computer Science and Technology: E

Network, Web & Security



Various Encryption Algorithms

Analysis-Based Investigation

Evaluate the Best Controller

Security in Electronic Commerce

Highlights

Discovering Thoughts, Inventing Future

VOLUME 19 ISSUE 1 VERSION 1.0

Global Journal of Computer Science and Technology: E
Network, Web & Security

Global Journal of Computer Science and Technology: E
Network, Web & Security

Volume 19 Issue 1 (Ver. 1.0)

Open Association of Research Society

Incorporation No.: 0423089
License No.: 42125/022010/1186
Registration No.: 430374
Import-Export Code: 1109007027
Employer Identification Number (EIN):
USA Tax ID: 98-0673427

Global Journals Inc.

*(A Delaware USA Incorporation with "Good Standing"; **Reg. Number: 0423089**)*

Sponsors: Open Association of Research Society
Open Scientific Standards

Publisher's Headquarters office

Global Journals® Headquarters
945th Concord Streets,
Framingham Massachusetts Pin: 01701,
United States of America
USA Toll Free: +001-888-839-7392
USA Toll Free Fax: +001-888-839-7392

Offset Typesetting

Global Journals Incorporated
2nd, Lansdowne, Lansdowne Rd., Croydon-Surrey,
Pin: CR9 2ER, United Kingdom

Packaging & Continental Dispatching

Global Journals Pvt Ltd
E-3130 Sudama Nagar, Near Gopur Square,
Indore, M.P., Pin:452009, India

Find a correspondence nodal officer near you

To find nodal officer of your country, please email us at *local@globaljournals.org*

eContacts

Press Inquiries: *press@globaljournals.org*
Investor Inquiries: *investors@globaljournals.org*
Technical Support: *technology@globaljournals.org*
Media & Releases: *media@globaljournals.org*

Pricing (Excluding Air Parcel Charges):

Yearly Subscription (Personal & Institutional)
250 USD (B/W) & 350 USD (Color)

Editorial Board

Global Journal of Computer Science and Technology

Dr. Abdurrahman Arslanyilmaz

Computer Science & Information Systems Department
Youngstown State University
Ph.D., Texas A&M University
University of Missouri, Columbia
Gazi University, Turkey
Web: cis.ysu.edu/~aarslanyilmaz/professional_web

Dr. Chutisant Kerdvibulvech

Dept. of Inf. & Commun. Technol.,
Rangsit University
Pathum Thani, Thailand
Chulalongkorn University Ph.D. Thailand
Keio University, Tokyo, Japan

Dr. Sukhvinder Singh Deora

Ph.D., (Network Security), MSc (Mathematics),

Masters in Computer Applications

Dr. Sotiris Kotsiantis

Ph.D. in Computer Science, University of Patras, Greece
Department of Mathematics, University of Patras, Greece

Dr. Ramadan Elaiess

Ph.D.,

Computer and Information Science

Dr. Manpreet Singh

Ph.D.,
(Computer Science)

Nicla Romano

Professor in Cellular and Developmental Biology;
Cytology and Histology; Morfogenesis and Comparative Anatomy

Dr. Muhammad Abid

M.Phil,
Ph.D Thesis submitted and waiting for defense

Dr. K. Venkata Subba Reddy

Ph.D in Computer Science and Engineering

Loc Nguyen

Postdoctoral degree in Computer Science

Faisal Mubuke

M.Sc (IT), Bachelor of Business Computing, Diploma in Finanicial services and Business Computing

Jiayi Liu

Physics, Machine Learning,
Big Data Systems

Dr. Yuanyang Zhang

Ph.D in Computer Science

Asim Gokhan Yetgin

Design, Modelling and Simulation of Electrical Machinery;
Finite Element Method, Energy Saving, Optimization

Anup Badhe

Bachelor of Engineering (Computer Science)

Dr. S. Nagaprasad

M.Sc, M. Tech, Ph.D

Contents of the Issue

Global Journal of Computer Science and Technology: E Network, Web & Security
Volume 19 Issue 1 Version 1.0 Year 2019
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Review of Various Encryption Algorithms

By Neyole Misiko Jacob
Jomo Kenyatta University of Agriculture and Technology

Abstract- Advancement in technology dictates that information security, user data integrity and security be paramount to protect user information and data from vulnerabilities from malicious intruders- third parties. Need is therefore a factor for information systems to secure user data and information. The concept data encryption ensures that user data is unreadable to third parties keeping their information more safe and secure while using the internet. A lot information on security has been provided by both the physical security and operating system security but neither of these methods have successfully and sufficiently provided a secure mechanism and support on storing and processing of user data and information. This paper reviews the various encryption algorithms that are employed to protect user information and data against various vulnerabilities.

Index terms: *encryption, algorithms, software's, behaviors.*

GJCST-E Classification: *I.1.m*

Strictly as per the compliance and regulations of:

Review of Various Encryption Algorithms

Neyole Misiko Jacob

Abstract- **Advancement in technology dictates that information security, user data integrity and security be paramount to protect user information and data from vulnerabilities from malicious intruders- third parties. Need is therefore a factor for information systems to secure user data and information. The concept data encryption ensures that user data is unreadable to third parties keeping their information more safe and secure while using the internet. A lot information on security has been provided by both the physical security and operating system security but neither of these methods have successfully and sufficiently provided a secure mechanism and support on storing and processing of user data and information. This paper reviews the various encryption algorithms that are employed to protect user information and data against various vulnerabilities.**

Index terms : encryption, algorithms, software's, behaviors.

I. Introduction

Advancement in technology dictates that information security, user data integrity and security have become paramount to protect user information and data from vulnerabilities due to technological advances especially the internet or access by third parties. With this there is dire need for information systems to secure user data and information like the use of anonymisation and encryption (Neubauer T, Heurix J, 2011).The concept encryption functions through scrambling of data to make it unreadable by the third party, this is enhanced in a number of ways such as the use of the key size and strength to create strong security of data (Bradford, 2016).

Much as information security has been provided by both the physical security and operating system security, neither of these methods have successfully and sufficiently provided a secure mechanism and support on storing and processing data (Priti V. Bhagat, Kaustubh S. Satpute, Vikas R. Palekar, 2013). This paper reviews the various encryption algorithms that are employed to protect user information and data against various vulnerabilities.

II. Encryption Algorithms

Encryption and cryptography algorithm can be defined as an approach that make data, information or network more secure (Rajdeep Bhanot and Rahul Hans, 2015). As a science, cryptography encamps the use of encryption algorithms to secure data within computer systems. The high reliance of the internet for communication purpose requires that data and information be encrypted to limit intruders from accessing to read messages. The process of information encryption also called cipher text enables users of systems to transfer information and data much securely. There are many encryption algorithms that are used widely. Those available and used in data and information security can broadly be categorized into Symmetric also called private and Asymmetric also called public keys encryption (Prerna Mahajan and Abhishek Sachdeva, 2013).

III. Software Behaviors

By definition encryption is the technology of converting plain text information into cipher text, the cipher text can then be securely communicated over any unsecure network. This process of encryption is usually achieved using encryption algorithm (Rajdeep Bhanot and Rahul Hans, 2015). Users benefit from encryption as it makes their data and information be more confidential, have integrity, be non-repudiation, be authentic and have access Control. There are various encryption algorithms in use currently, whose key size and strength generally being the differences between them (Bradford, 2016).

Bradford further categorizes them as:- Data Encryption Standard (DES), the Triple DES a symmetric algorithm, the RSA a public key encryption algorithm, the Blowfish algorithm, the Twofish algorithm and the Advanced Encryption Standard (AES). Hossain et.al 2016 classified the algorithms as symmetric-key algorithms in which the same key used for both encryption and decryption of data, asymmetric-key algorithms in which a public key is used by a sender to encrypts data and a private key used by receiver for decryption and hashing. (Md. Alam Hossain, Md. Biddut Hossain, Md. Shafin Uddin, Shariar Md. Imtiaz, 2016).

The Triple DES a symmetric algorithm makes use of three individual keys with 56 bits, was designed to replace the Data Encryption Standard (DES) algorithm which was much vulnerable to hackers, the RSA a public key encryption algorithm utilized by modern computers to encrypt and decrypt messages. The Blowfish algorithm which is a symmetry cipher used to split and encrypt messages individually whose advantages are its speed and the overall operation effectiveness.

The Twofish algorithm, keys used in this algorithm vary up to 256 bits in length and use

Author: Jomo Kenyatta University of Agriculture and Technology.
e-mail: Jneyole434@gmail.com

symmetric technique for only one key. It is regarded as one of the fastest algorithm and is ideal for use in both hardware and software systems. The Advanced Encryption Standard (AES) which is the algorithm trusted as the standard by many numerous organizations. It is extremely efficient and largely impervious to attacks except for brute force.

A study conducted by Rejani R and Deepu.V. Krishnan on the test of algorithms concluded that between AES, DES, 3DES, RC2, Blowfish, and RC6, Blowfish was the best encryption algorithm between different symmetric and asymmetric encryption algorithms (Rejani. R, 2015). The study further advanced that DES algorithm was no longer secure especially with the advancement in the computer processing power whereas the AES encryption algorithm is faster and flexible hence widely applied in many security applications.

A research on encryption Algorithms AES, DES and RSA for Security by Prerna and Sachdeva (2013) indicated that DES algorithm is used to provide a standardized method to protecting sensitive commercial and unclassified data. The Advanced Encryption Standard (AES) algorithm is appropriate for both hardware and software implementation and is of greater speed, while the Rivest-Shamir-Adleman (RSA) which is widely used Public-Key algorithm is used to encrypt data to provide security so that only the concerned user can access it.

In comparison therefore AES has a block size of 128 bits, DES 64 bits while RSA has a minimum of 512 bits. In terms of encryption and decryption, the AES algorithm is faster while DES is moderate and RSA algorithm is much slower. AES is excellently secured while DES is not enough secured and RSA is the least secure algorithm. All the algorithms are inherently vulnerable to brute forced attacks- a trial and error means employed by various application programs to decode or decrypt encrypted data for instance passwords or Data usually on the internet (Rouse, 2006).

A long this DES is prone to linear and differential cryptanalysis attacks which involves cracking codes to decode privacies through violation of authentication schemes by breaking cryptographic protocols (Heward, 2014), while RSA is vulnerable to oracle attacks that exploit the availability of weaknesses in system. On the other hand the asymmetric algorithm includes: - RSA, DSA, Diffie-Hellman, El-Gamal and Pailier. The hashing which includes the MD5, MD6, the SHA and SHA256 (Md. Alam Hossain, Md. Biddut Hossain, Md. Shafin Uddin, Shariar Md. Imtiaz, 2016).

The RSA Rivest-Shamir-Adleman an asymmetric encryption and decryption algorithm uses a public and private key. The public key which is described to everyone is used for encrypting messages. The messages encrypted with the public key are usually decrypted through the private key. RSA performs generation, encryption and decryption of algorithm keys (Priyanka Arora, Arun Singh and Himanshu Tyagi, 2014). The DIFFIE-HELLMAN key has a specific approach of exchanging cryptographic keys that enable two parties having no understanding of each other to equally make a shared-secret key over an insecure communications path. The keys are then encrypt the posterior communications using a symmetric key cipher.

The PAILLIER algorithm has homomorphic properties that facilitate it to perform normal addition operations on several encrypted values to achieving the encrypted sum, they are then decrypted later with no knowledge of the sum value (Priyanka Arora, Arun Singh and Himanshu Tyagi, 2014). The motivation behind the hash functions is the management of data security, integrity and consistency (Neyole, 2015). The Message Digest5 for instance takes random data information of text and binary as input and generate a fixed size hash value as the output.

The input data can be of any length and size, but the output hashed value is always fixed (Neyole, 2015). For MD5 the input message is allocated to groups of 512-bits then the message is then packed by making its length divisible by 512 (Priyanka Arora, Arun Singh and Himanshu Tyagi, 2014). The MD5 is mostly used in the database design to encrypt passwords. It's faster to use but suffers with the challenges of easy decryption using web based applications such as HashKiller. The SHA- Secure Hashing Algorithm on the other hand is a hashing algorithm that is structured differently and are named SHA-0, SHA-1, SHA-2, and SHA-3. SHA-0 whose original version was the 160-bit hash function (Neyole, 2015) this algorithms are more secure and stable especially in the design of database systems.

IV. Conclusions

Does increased security provide 100% assurance to technology consumers? With the Internet as a major essential communication between billions of people and also a tool for commerce, social interaction, and the exchange of an increasing amount of personal information, security has become a matter of grave concern. There are a number approaches to data and information security where many applications to securing commerce and payments are employed to manage private communications and user data and information. But in all this, encryption which makes use of encryption algorithms makes communication more secure to user data and information.

With the many encryption algorithms schemes in existence each out to improve on security of system, data, information and communication channels managers have enhanced them on data and information to facilitate users with more system integrity and confidentiality while working with them. The main

concerns of these schemes is to optimize technology use. The Hash functions for instance, are well established to ensure data integrity where any change made to the contents of a message will result in the receiver calculating a different hash value than the one placed in the transmission by the sender. This then ensures user with a high degree of confidence (Kessler, 2017).

As the number of attacks and their sophistications increase, attacks on encryptions such as brute-force requires that systems be equipped with the various algorithms to support each other to the management of the systems. On performance analysis, the best algorithms both symmetric and asymmetric should possess the following aspects:- the set of keys and the enciphering algorithm should be free from complexity, the implementation of the process should be as simple as possible, errors in ciphering should not propagate and cause corruption of further information in the message and the size of the enciphered text should be no larger than the text of the original message among other measures (Pfleeger, Charles P. and Shari Lawrence, 2006).

References Références Referencias

1. Bradford, C. (2016, July 31st). *Storagecraft Recovery Zone*. Retrieved from 5 Common Encryption Algorithms and the Unbreakables of the Future: http://www.storagecraft.com/blog/5-common-encryption-algorithms/
2. Heward, G. (2014, January 26th). *Cryptanalysis and Attacks*. Retrieved from Experts-Exchange: https://www.experts-exchange.com/articles/12460/Cryptanalysis-and-Attacks.html
3. Md. Alam Hossain, Md. Biddut Hossain, Md. Shafin Uddin, Shariar Md. Imtiaz. (2016). Performance Analysis of Different Cryptography Algorithms. *International Journal of Advanced Research in Computer Science and Software Engineering*, pp. 659-666.
4. Kessler, G. C. (2017). *An Overview of Cryptography*. Australia: McGraw-Hill.
5. Neubauer T, Heurix J. (2011). A Methodology for the Pseudonymization of Medical data. *International Journal of Medical Information*, pp. 190-204.
6. Neyole, J. M. (2015). Vulnerability of data security using MD5 function in php database design. *International Journal of Science and Engineering*, pp. 11-16.
7. Prerna Mahajan and Abhishek Sachdeva. (2013). A Study of Encryption Algorithms AES, DES and RSA for Security. *Global Journal of Computer Science and Technology Network, Web & Security*, pp 1-9.
8. Priti V. Bhagat, Kaustubh S. Satpute, Vikas R. Palekar. (January 2013). Reverse Encryption Algorithm: A Technique for Encryption & Decryption. *International Journal of Latest Trends in Engineering and Technology (IJLTET)*, pp.90-96.
9. Priyanka Arora, Arun Singh and Himanshu Tyagi. (2014). Evaluation and Comparison of Security Issues on Cloud Computing Environment. *World of Computer Science and Information Technology Journal*, pp. 179-183.
10. Pfleeger, Charles P. and Shari Lawrence. (2006). Making Good Encryption Algorithms. In C. P. Pfleeger, Security in Computing 4th Edition (pp. pp. 176- 181). Upper Saddle River, NJ 07458 USA: Pearson Education, Inc.
11. Rajdeep Bhanot and Rahul Hans. (2015). A Review and Comparative Analysis of Various Encryption Algorithms. *International Journal of Security and Its Applications*, pp. 289-306.
12. Rejani. R, a. D. (2015). Study of Symmetric key Cryptography Algorithms. *International Journal of Computer Techniques*, pp. 45-51.
13. Rouse, M. (2006, July). *Brute force cracking*. Retrieved from TechTarget network of technology: http://searchsecurity.techtarget.com/definition/brute-force-cracking.

This page is intentionally left blank

Global Journal of Computer Science and Technology: E Network, Web & Security
Volume 19 Issue 1 Version 1.0 Year 2019
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Factor Analysis-Based Investigation into Financial Crime Related Issues in Nigeria

By Gabriel Babatunde Iwasokun
Federal University of Technology

Abstract- This paper proposes sixteen indices that were considered very important for the analysis of financial crime related issues in Nigeria. The indices were listed in the questionnaire that was administered on the FCT and thirty out of thirty-six states that span the six geo-political zones of Nigeria to obtain relevant data. Copies of the questionnaire were administered during meetings with stakeholders of banks, insurance companies, educational institutions and other relevant government and private owned establishments. The data obtained were subjected to factor analysis by principal component using SPSS. The analysis identified policies and regulations, responses and management, capacity building and awareness and litigation as the major issues to be addressed if financial crimes are to be checked. The percentage of the contributory effect of these issues and the degree of relevance of their associated indices were determined and found to be less than 100, indicating that the indices of some extraneous issues were not considered in the research instrument. Such issues include but not limited to economic status and cultural and societal impacts. Moreover, a coefficient score matrix was generated and used to estimate and rank the contribution of each respondent to the extracted issues.

Keywords: *PCA, financial crimes, Nigeria, causal factors, extracted factors.*

GJCST-E Classification: *I.1.2*

Strictly as per the compliance and regulations of:

Factor Analysis-Based Investigation into Financial Crime Related Issues in Nigeria

Gabriel Babatunde Iwasokun

Abstract- This paper proposes sixteen indices that were considered very important for the analysis of financial crime related issues in Nigeria. The indices were listed in the questionnaire that was administered on the FCT and thirty out of thirty-six states that span the six geo-political zones of Nigeria to obtain relevant data. Copies of the questionnaire were administered during meetings with stakeholders of banks, insurance companies, educational institutions and other relevant government and private owned establishments. The data obtained were subjected to factor analysis by principal component using SPSS. The analysis identified policies and regulations, responses and management, capacity building and awareness and litigation as the major issues to be addressed if financial crimes are to be checked. The percentage of the contributory effect of these issues and the degree of relevance of their associated indices were determined and found to be less than 100, indicating that the indices of some extraneous issues were not considered in the research instrument. Such issues include but not limited to economic status and cultural and societal impacts. Moreover, a coefficient score matrix was generated and used to estimate and rank the contribution of each respondent to the extracted issues.

Keywords: PCA, financial crimes, Nigeria, causal factors, extracted factors.

I. Introduction

Financial crime is a non-violent but intentional crime committed for illicit monetary or other unlawful gain from individuals, corporations, government bodies and financial institution (IMF, 2001; Ladan, 2005). It constitutes a very serious threat that manifests itself in virtually all aspects of national life. It is widely spread and involves Internet-based cheque issuance, cash deposit, wire transfer and Automated Teller Machine (ATM) withdrawals performed by institutions, government and individuals on a daily basis. Notable financial crimes include theft, scams, embezzlement, identity theft, money laundering, bribery, smuggling, forgery, counterfeiting and tax evasion (Ibrahim *et al.,* 2015). Financial crimes are characterized by deceit, concealment or violation of trust and can be committed with every form of dynamism, subtleness and camouflage (Agus *et al*., 2010a). Considerably, financial crime may lead to colossal loss of money as well as undermining the integrity of financial institutions and markets. It may also subvert national growth and development (Spencher and Pickett, 2002; McDowell and Novis, 2001; Okoye and Gbegi, 2013; Ejiofor *et al*., 2007). Financial crimes may lessen the ability of a country to attract foreign investment and subvert the growth and development of local manufacturing industries (IMF, 2001; Spencher and Pickett, 2002; Yusu, 2009). Financial crime may manifest inform of corruption, fraud and theft. Corruption is any illegal act such as kickbacks, embezzlement and extortion and another misuse of entrusted funds and power for private gain or improper and unlawful enrichment (Gottschalk, 2010; Ksenia, 2008).

Fraud is a despicable act with the aim of achieving a personal gain or creating a loss for another through concealment of an illegal act and it is a significant and growing threat to several organizations (Golden *et al.,* 2006*;* Edelherz, 1977). Most prominent financial frauds are the conversion of public money into personal use, granting of unauthorized loans or overdraft, fraudulent transfer or withdrawals, misrepresentation of quality and quantity during procurement and pyramid trading schemes. Others are posting of fictitious credits, cheque counterfeiting or forging, payroll padding (ghost workers), contract over billings and over-invoicing among others (Okeyi and Gbegi, 2013). Theft of cash, intellect, art or identity is said to take place if it is carried out unlawfully and out of all proportions. Several strategies and measures for combating financial crimes include the use of technology and establishment of agencies and commissions. Technological tools offer a more holistic view of data and highlight potential areas of risk to organizations thereby reducing the incidence of fraud (Deloitte, 2014). Big data and text mining, machine learning and forensic accounting are some of the existing technologies for combating financial crimes (Adegbeie and Fakile, 2012; Shai and Shai, 2014; Agus *et al*., 2010b; Raghavendra *et al*., 2011; Kitten, 2016). Impact of criminal personality, opportunity structures, corporate identity, values on crime, and business ethics had been identified as causes of financial crimes (Bussman, 2003). These causes could be attributed to bio-genetic factors which include genetic mutation and heredity (Horton, 1939), psychological factors comprising of personality disorders and sociological factors that include learning environment (Sutherland, 1939).

Author: Department of Software Engineering, Federal University of Technology, Akure, Nigeria. e-mail: gbiwasokun@futa.edu.ng

The fundamental techniques for combating financial crime still require a good understanding of its causes and dynamics as all technical and scientific proof have yielded unsatisfactory results (Ayoola *eat al.,* 2015). Existing techniques for presenting the understanding of the causes and dynamics of financial crimes include some baseline and dimension-reduction tools such as *Missing Values Ratio (MVR), Low Variance Filter (LVF) and High Correlation Filter (HCF). Others are Random Forests Ensemble Trees (RFET), Backward Feature Elimination (BFE), Forward Feature Construction (FFC), Principal Component Analysis (PCA) (Silipo, 2015)* and Factor Analysis (FA). Factor analysis is a method for investigating whether some variables of interest N_1, N_2, . . ., N_m, are linearly related to a smaller number of unobservable factors F_1, F_2, . . ., F_k. It is used to identify dimensions underlying response (outcome) for a set of variables such that the observed values for the variables are determined as manifest variables. Some standardized variables are generally used with the correlation matrix modelled such that its dimensions correspond to the factors. Several of manifest variables can be used but more appropriate if they have more than a few distinct values and an approximate bell-shaped distribution. Factor analysis based on principal components uses weights and scores to produce factor loadings and scores. These attributes informed its choice for the analysis of the financial security-related issues in Nigeria. The main objective of the study is to take a holistic view of the conceptualization of the main issues that relate to financial crime and provides data that serve the basis for the determination of their impact in Nigeria. Also, the study also provides data that is relevant for drawing conclusion based on a comparison between results from current and some related works.

II. Related Works

An exploration of the statistical methods for fighting financial crime by financial institutions is carried out in (Agus *et al*., 2010a). Issues on the growing losses of revenue by governments, financial institution and individuals to the various forms of financial crime as well as the review of some statistical techniques for investigative studies of financial crimes were also discussed. The research formulated the necessary steps for account opening, described some visualization, description, analysis and computational tools for data on high volume transactions as well as a machine learning algorithm for detecting financial crime. An investigative study on the impact of economic and financial crime on the Nigerian economy is presented in (Yusus, 2009). A review of the conceptual legal framework as well as the nature, scope and effects of economic and financial crimes under the Nigerian law, was presented. The authors concluded that ICT infrastructure is the main tool that financial criminals rely on in carrying out their unlawful acts.

The authors in (Okoye and Gbegi, 2013) evaluated the effect of fraud and related financial crime on the Nigerian economy. The research placed a premium on how the Internet, electronic money transfer (wire transfer) and other related platforms contributed to the current spate of financial crime. Regression-based analysis on available financial crime data revealed that financial crimes portend dwindling Gross Domestic Product (GDP) and shrinking economy. In (Iwasokun *et al*., 2012), an investigation on the effect of financial crime on the society was presented. A platform for determining the correlation between crimes was also presented based on PCA-based analysis of financial crime data from a Criminal Investigation Department. The authors in [3] examined the effect of financial crime and corruption on manufacturing firms and organizations. The Two Way-ANOVA-based analysis of financial crime data obtained from primary and secondary sources revealed significant and negative implications of financial crime on the manufacturing firms as manifested through drained revenue, operational instability and low level of interest from foreign and domestic investors.

III. Research Methodology

The research methodology is conceptualized in Figure 1 showing data survey, factor analysis by principal components and results phases.

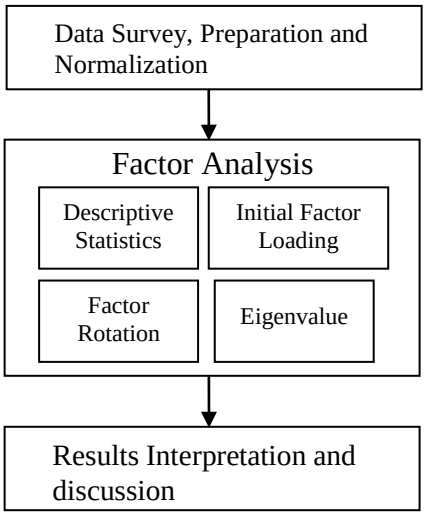


Figure 1: Conceptualization of the Factor Analysis-based model

a) Data Survey, preparation and Normalization

Data survey involved a survey of public and private agencies such as banks, insurance company, educational institutions that are involved in different forms of financial activities both offline and online. The selection was based on stratified sampling and respondents were randomly chosen with equal probability. Data preparation involved determination of all relevant variables for inclusion in the analysis, determination of the number of observations sufficient to provide reliable estimations of the correlations between the indices, estimation of valid measure of associations among selected variables and the arrangement of the surveyed observations as a set of data vectors $y_1, y_2, \ldots, y_d$ with each denoting a grouped observation of V variables. Data normalization is used to transform the surveyed data to a formatted form. Data with ratings were restructured to a notionally common scale before averaging.

b) PCA-Based Factor Analysis

The variables for PCA-based factor analysis of the inducement factors of financial crime are related to one another for the j^{th} respondents, and it is represented as follows (Iwasokun *et al*., 2012; Gulumbe *et al*., 2012):

$$\text{var}(Z_j) = \lambda_j \quad (1)$$

$$\alpha_{j1}{}^2 + \alpha_{j2}{}^2 + \cdots + \alpha_{jk}{}^2 = 1 \quad (2)$$

Z_j represents the j^{th} respondent (the principal component of j^{th} data), α_{jk} represents the assessment of the j^{th} indices by the k^{th} respondent (the elements of the j^{th} eigenvector λ_j for the correlation matrix).

The principal components analysis of the survey involved descriptive statistic, correlation matrix, Bartlett's and Kaiser-Mayer Olkin (KMO) tests, component extraction and other statistics of relevance. Descriptive statistics ensured standardization of the measurements used in the normalized data and covered the assigning of the data set variables to zero means, unit variances and standard deviation. The sample correlation coefficient is calculated as follows:

$$r_{x,y} = \frac{s_{x,y}}{s_x s_y} \quad (3)$$

$s_{x,y}$ is the variance between two columns in the data matrix, s_x *and* s_y are the standard deviations of columns x and y respectively. For multivariate analysis, the correlation matrix is analogous to the covariance matrix with correlations in place of covariances. Barlett's test of sphericity β is used to confirm the adequacy of a sample population by testing the null hypothesis that the variables in the population correlation matrix are uncorrelated. The observed significance level of .0000 is used to reject this hypothesis. The test is based on the formula (Donal, 1993):

$$\beta = -\left[n - 1 - \frac{2p+5}{6}\right] ln|R| \quad (4)$$

$|R|$ is the determinant of the correlation matrix, n is the number of observation and p is the number of variables. The KMO test γ for the hypothesis that the variables are uncorrelated in the population is based on the formula:

$$\gamma = \frac{\sum_i \sum_{i \neq j} r_{ij}^2}{\sum_i \sum_{i \neq j} r_{ij}^2 + \sum_i \sum_{i \neq j} a_{ij}{}^2} \quad (5)$$

r_{ij} is the correlation coefficient in the correlation matrix; a_{ij} is the partial correlation coefficient and i,j represent the rows and column sizes respectively. A near-zero partial correlation, A guarantees effective factorization and it is obtained from the correlation matrix R as follows:

$$A = -\frac{1}{R \times \sqrt{v_{ii} \times v_{jj}}} \quad (6)$$

The Communality of the squared component loadings for component *i* is computed as follows:

$$c_i = {\alpha_{i1}}^2 + {\alpha_{i2}}^2 + \cdots + {\alpha_{ip}}^2 = \sum_{i=1}^{p} {\alpha_{ip}}^2 \quad (7)$$

p is the number of variables, α_{ip} is the value in A for row *i*, column *p*. The communalities narrate how well the model performs for each variable while the total communality gives an overall assessment.

The eigenvalues of R is calculated as follows:

$$|R - \lambda I_p| = 0 \quad (8)$$

I_p is a $p \times p$ identity matrix with eigenvalues $\widehat{\lambda_1} \geq \widehat{\lambda_2} \geq \cdots \geq \widehat{\lambda_p}$ and the eigenvector V is calculated as follows:

$$V = DR^{-1} \quad (9)$$

D is the *p* x *p* diagonal matrix of eigenvalues of R.

From p variables, the principal components (un-rotated factors) are extracted based on the criterion presented as follows (Kaiser, 1960):

$$\bar{\lambda} = \frac{1}{p}\sum_{j=1}^{p} \quad (10)$$

The criterion only extracted a principal component with an eigenvalue greater than $\bar{\lambda}$. The un-rotated factors are subjected to orthogonal transformation using varimax, equimax, quartimax and promax and the best result was taken. Orthogonal transformation is used to obtain meaningful representation of variables and component mapping along the principal axis. Rotation by varimax is based on the assumption that the interpretability of a factor can be measured by the variance of the squares of its factor loadings. Quartimax rotation involves the minimization of the number of factors needed to explain each variable while equamax rotation is a compromise that attempts to simplify both components and variables. Promax is an oblique rotation that allows factors to be correlated and because it is often more easily calculated than any direct oblimin rotation, it is more useful for large datasets.

The determination of component scores is based on a linear equation of the weighted standard scores of each respondent on the variables as follows:

$$M_{b,c} = \sum_{m=1}^{f} d_{a,c} W_{b,a}, b = 1, 2, \ldots, x; \quad m = 1, 2, \ldots, f \quad (11)$$

$M_{b,c}$ represents the contribution of bth respondent to cth component, $d_{a,c}$ is the component score coefficient of ath variable for cth component, *f* is the number of the extracted components, $W_{b,a}$ represents the standard score of bth respondent for ath variable and x is the respondents' population. $W_{b,a}$ is estimated as follows:

$$W_{b,a} = X + \frac{S_b - T_b}{u_b} \quad (12)$$

X represents the allowable minimum score, which in this case is 1, S_b represents the raw score for bth index, T_b and u_b represent the mean and standard deviation respectively, of the raw scores of bth index by the sampled respondents.

IV. Results and Interpretation

The result from the analysis is interpreted to determine the correlation and relationship between indices. The Questionnaire shown in Appendix 1 was designed using the indices for the analysis of financial security-related issues. Each of these indices was offered loosed linguistic description and range of values as shown in Table 1.

Table 1: Matrix of Weight Attached to Linguistic Value

Linguistic Representation	Excellent	Very Good	Good	Average	Poor
Range of Values	4.01-5.0	3.01-4.0	2.01-3.0	1.01-2.0	0.0-1.0

The first part of the Questionnaire provided vital information about each respondent while the second part presented five columns for the respondent to rank each of the sixteen indices based on the scale presented in Table 1. The Questionnaire was administered to Thirty States in the six geo-political zones and the Federal Capital Territory (FCT) in Nigeria and the summary of the survey is presented in Table 2.

Table 2: Summary of the survey

Serial No.	State	No. of LG Surveyed	Total Questionnaire Administered	Total Questionnaire Returned	Total Questionnaire not Returned
1	Abia	5	300	263	37
2	Adamawa	6	425	415	10
3	Akwa-Ibom	8	524	522	2
4	Anambra	5	275	254	21
5	Bauchi	7	589	487	102
6	Benue	7	652	623	29
7	Delta	10	524	451	73
8	Cross River	11	687	671	16
9	Ebonyi	6	165	128	37
10	Edo	8	785	687	98
11	Ekiti	7	570	457	113
12	Enugu	8	622	528	94
13	Imo	7	522	420	102
14	Jigawa	3	420	259	161
15	Kaduna	3	186	181	5
16	Kano	11	894	856	38
17	Kebbi	3	202	202	0
18	Kogi	6	414	401	13
19	Kwara	4	551	510	41
20	Lagos	20	1026	896	130
21	Nasarawa	6	239	239	0
22	Ogun	7	658	452	206
23	Niger	8	659	659	0
24	Ondo	18	1524	1325	199
25	Osun	8	354	258	96
26	Oyo	12	742	468	274
27	Plateau	6	231	197	34
28	Rivers	6	402	401	1
29	Sokoto	3	189	175	14
30	Taraba	5	580	574	6
31	FCT	3	627	587	40
Total		158	11289	9500	1789

A total of Sixteen Thousand Five Hundred and Thirty-Eight (16538) copies of the Questionnaire were administered through direct and online contacts. In the direct contact, the researcher visited the surveyed states or engaged the services of third parties while indirect contact involved hosting the Questionnaire on Google forms for online assessment. In both cases, Fourteen Thousand Five Hundred and Forty-Six (14546) respondents returned duly completed Questionnaires. Where necessary, the responses were verified and validated through follow-up meetings and personal interviews with the respondents

All the 14546 responses were subjected to factor analysis by principal components using SPSS. The analysis of the respondents' knowledge of financial crime, times fallen victim of financial crime and the distribution of crimes are presented in Tables 3, 4 and 5 respectively.

Table 3: Knowledge of Financial Crime

Values	Frequency	Percent	% Cumulative
Poor	988	6.8	6.8
Average	3102	21.3	28.1
Good	4803	33.0	61.5
Very Good	3863	26.3	87.7
Excellent	1790	12.3	100.0
Total	14546	100.0	

Table 4: Distribution Range of Occurrences

Range	Frequency	Percent	Valid Percent	Cumulative Percent
0	11655	80.1		
1-5	1372	9.4	47.4	47.4
6-10	447	3.1	15.4	62.8
11-15	164	1.1	5.7	68.5
16-20	357	2.5	12.4	80.9
> 20	551	3.3	19.1	100.0
Total	14546	100.0		

Table 5: Classes of Financial Crime Victims Distribution

Classes of Financial Crime	Number of Occurrences	%
Advance fee fraud	1177	12.72
Forgery (Fake Cheque)	834	9.02
Money Theft Through ATM	850	9.18
Kickbacks and Extortion	730	7.89
Embezzlement	775	8.37
Corruption and Bribery	1014	10.95
Fraud	865	9.34
Money Laundering	536	5.8
Identity theft	462	4.99
Counterfeit Money	700	7.57
Financial Grooming	640	6.92
Insider Trading	372	4.03
Phishing	297	3.22
Total	9252	100

Table 6: Descriptive Statistics of Variables

Variables	N	Mean	Std. Deviation
National Policy on Financial operations and Security	1341	3.47	1.245
Legislative, Regulatory and Institutional Framework on Financial operations	1350	3.25	1.172
Legislative, Regulatory and Institutional Framework on Financial Security	1347	3.27	1.184
Implementation of Conventional Security in Financial Institution	1338	3.21	1.177
Implementation of Financial Security Policy	1340	3.13	1.219
Financial Crime Case Assessment	1338	3.15	1.210
Prosecution of Financial Criminals	1344	3.05	1.223
Proficiency of litigators on Financial Crime Cases	1323	3.13	1.223
Public Awareness on Financial Security	1344	3.17	1.196
IT Literacy of Conventional Security Personnel	1346	3.13	1.150
Availability of IT Security Facility at Financial Centres	1259	3.05	1.213
Capacity Building/ IT Staff Development	1268	3.04	1.197
Rapid Response to Financial Emergency by Security Agencies	1346	3.11	1.270
Development and Usability of Financial Crime Database System	1355	3.07	1.267
Collaboration Between Financial Agencies	1341	3.09	1.221
Availability of Independent/Private Financial Security organization	1343	3.03	1.235

The descriptive statistics shown in Table 6 presents the means and standard deviation of the rating of the indices for the analysis of the financial crime related issues by the respondents. The mean and standard deviation of the rating on 'National Policy on Financial operations and Security' are 3.47(69.0%) and 1.245 respectively while the mean and standard deviation of the rating on 'Legislative, Regulatory and Institutional Framework on Financial operations' are 3.25(65.0%) and 1.172 respectively. These values reveal that on the average, the respondents agreed that the 'National Policy on Financial Operations and Security' and 'Legislative, Regulatory and Institutional Framework on Financial Operations' are strong financial crime related issues. The interpretation is based on the matrix of weight attached to the linguistic values presented in Table 1. Similarly, standard deviations represent the statistical measure of dispersion from the mean for the response values for 'National Policy on Financial Operations and Security' and for 'Legislative, Regulatory and Institutional Framework on Financial Operations' respectively. The communalities of the indices for financial crime related issues are presented in Table 7 showing that communalities of the 'National Policy on Financial operations and Security' and 'Legislative, Regulatory and Institutional Framework on Financial operations' are 0.719 and 0.731 respectively. These imply that 71.9% of the variance in 'National Policy on Financial operations and Security' can be explained by the extracted factors while the remaining 28.1% is attributed to extraneous factors. Similarly, 73.1% of the variance in 'Legislative, Regulatory and Institutional Framework on Financial operations' can be explained by the extracted factors while the remaining 26.9% is credited to extraneous factors.

Table 7: Communalities of Variables

Variables	Initial	Extraction
National Policy on Financial operations and Security	1.000	0.719
Legislature's, Regulatory and Institutional Framework on Financial operations	1.000	0.731
Legislature's, Regulatory and Institutional Framework on Financial Security	1.000	0.718
Implementation of Conventional Security in Financial Institution	1.000	0.648
Implementation of Financial Security Policy	1.000	0.664
Public Awareness on Financial Crime/Security	1.000	0.698
Development and Usability of Financial Crime Database System	1.000	0.795
IT Literacy of Conventional Security Personnel	1.000	0.69
Capacity Building/ IT Staff Development	1.000	0.761
Collaboration Between Financial Agencies	1.000	0.756
Availability of Independent/Private Financial Security organization	1.000	0.68
Availability of IT Security Facility at Financial Centres	1.000	0.791
Proficiency of litigators on Financial Crime Cases	1.000	0.788
Financial Crime Case Assessment	1.000	0.623
Rapid Response to Financial Emergency by Security Agencies	1.000	0.621
Prosecution of Financial Criminals	1.000	0.681

Table 8: Correlation Matrix of Variables

Variables	NpFos	AsFrO	AsFrS	CsAss	FsAss	FCCcAs	ProFC	LigPr	PubAr	ItLit	FCSEc	CapSt	RapRe	FCDbs	Collb	InOrg
NpFos	1.000	.711	.656	.573	.542	.558	.473	.441	.421	.432	.383	.376	.451	.458	.470	.420
AsFrO	.711	1.000	.710	.594	.556	.570	.500	.460	.449	.493	.439	.441	.515	.493	.489	.445
AsFrS	.656	.710	1.000	.604	.565	.572	.522	.523	.466	.476	.466	.446	.484	.488	.478	.421
CsAss	.573	.594	.604	1.000	.632	.585	.496	.472	.464	.464	.462	.431	.500	.497	.518	.451
FsAss	.542	.556	.565	.632	1.000	.635	.442	.419	.431	.485	.448	.483	.489	.453	.489	.468
FCCcAs	.558	.570	.572	.585	.635	1.000	.565	.481	.455	.456	.471	.438	.471	.463	.481	.476
ProFC	.473	.500	.522	.496	.442	.565	1.000	.631	.502	.488	.457	.416	.512	.498	.491	.471
LigPr	.441	.460	.523	.472	.419	.481	.631	1.000	.605	.519	.440	.453	.481	.517	.499	.455
PubAr	.421	.449	.466	.464	.431	.455	.502	.605	1.000	.593	.482	.460	.458	.489	.474	.454
ItLit	.432	.493	.476	.464	.485	.456	.488	.519	.593	1.000	.612	.558	.515	.498	.506	.471
FCSEc	.383	.439	.466	.462	.448	.471	.457	.440	.482	.612	1.000	.668	.531	.451	.475	.522
CapSt	.376	.441	.446	.431	.483	.438	.416	.453	.460	.558	.668	1.000	.525	.471	.501	.492
RapRe	.451	.515	.484	.500	.489	.471	.512	.481	.458	.515	.531	.525	1.000	.643	.540	.527
FCDbs	.458	.493	.488	.497	.453	.463	.498	.517	.489	.498	.451	.471	.643	1.000	.696	.590
Collb	.470	.489	.478	.518	.489	.481	.491	.499	.474	.506	.475	.501	.540	.696	1.000	.626
InOrg	.420	.445	.421	.451	.468	.476	.471	.455	.454	.471	.522	.492	.527	.590	.626	1.000

The analysis of the correlation matrix presented in Table 8 shows that the highest correlation of 0.711 exists between 'National Policy on Financial Operations and Security' and 'Legislative, Regulatory and Institutional Framework on Financial Operations'. The next highest correlation of 0.710 exists between 'Legislative, Regulatory and Institutional Framework on Financial Security' and 'Legislative, Regulatory and Institutional Framework on Financial Operations'. The implication of the former is that 'National Policy on Financial Operations and Security' is most likely to share the same factor with 'Legislative, Regulatory and Institutional Framework on Financial Operations'. Similarly, in the later, 'Legislative, Regulatory and Institutional Framework on Financial Security' and 'Legislative, Regulatory and Institutional Framework on Financial operations' will likely share the same factor.

The Least correlation of 0.376 exists between 'Capacity Building/ IT Staff Development' and 'National Policy on Financial Operations and Security'. This means that 'Capacity Building/ IT Staff Development' and 'National Policy on Financial Operations and Security' are not likely to share the same factor. The Barlett's test of sphericity produces a $\chi^2$of 7493.525 with a significance level of 0.000 which indicates that the sample population is adequate while the Kaiser-Mayer Olkin (KMO) test produced a measure of 0.950, which further confirmed the adequacy of the sample population.

The result of Kaiser Criterion based initial component extractions is presented in Table 9. The orthogonal transformation of the initial component extractions by varimax, promax, equamax and quartimax were carried out and the result obtained from the rotation by varimax, which is presented in Table 10, appeared most realistic and meaningful for interpretation among all others. Table 10 reveals four factors with their corresponding loadings.

Table 9: Extracted Initial Component Matrix

Variables	Component			
	1	2	3	4
Legislative, Regulatory and Institutional Framework on Financial Security	0.762			
Legislature's, Regulatory and Institutional Framework on Financial operations	0.761			
Implementation of Conventional Security in Financial Institution	0.750			
Collaboration Between Financial Agencies	0.748			
Development and Usability of Financial Crime Database System	0.746		-0.421	
Financial Crime Case Assessment	0.744			
Rapid Response to Financial Emergency by Security Agencies	0.740			
Implementation of Financial Security Policy	0.732			
IT Literacy of Conventional Security Personnel	0.732			
Prosecution of Financial Criminals	0.724			
National Policy on Financial operations and Security	0.717	-0.450		
Proficiency of litigators on Financial Crime Cases	0.717			-0.469
Availability of IT Security Facility at Financial Centres	0.708			
Availability of Independent/Private Financial Security organization	0.708			
Public Awareness on Financial Crime/Security	0.699			
Capacity Building/ IT Staff Development	0.695			

Principal Component 1(Policies and Regulations) loads on National Policy on Financial Operations and Security, Legislature's, Regulatory and Institutional Framework on Financial Operations, Legislature's, Regulatory and Institutional Framework on Financial Security, Implementation of Financial Security Policy, Implementation of Conventional Security in Financial Institutions and Financial Crime Case Assessment. Principal Component 2 (Responses and Management) loads on Collaboration between Financial Agencies, Development and Usability of Financial Crime Database System, Availability of Independent/Private Financial Security organization and Rapid Response to Financial Emergency by Security Agencies.

Similarly, Principal Component 3 (Capacity Building) loads on Capacity Building/ IT Staff Development, Availability of IT Security Facility at Financial Centres and IT Literacy of Conventional Security Personnel. Principal Component 4 (Awareness and Litigation) loads on Proficiency of litigators on Financial Crime Cases, Public Awareness on Financial Crime and Security and Prosecution of Financial Criminals.

The result highlighted government-approved policies and regulation as the most critical issues on financial crimes. This view was corroborated by the authors in (Galina, 2014; Sofia de Oliveira *et al*., 2016) who mentioned that the state of national financial security depends solely on governance efficiency as well as policies and regulations. Other financial crimes related issues highlighted are response and management strategies, capacity building and public awareness and litigation measures. These also agreed with the opinions presented in (Galina, 2014; Sofia de Oliveira *et al*., 2016; Usman *et al*., 2012; Durmus, 2007). The Component Score which is a linear combination of the original variables to the extracted factors is presented in Table 11.

Table 10: Rotated Component matrix

Variables	Component			
	1	2	3	4
National Policy on Financial operations and Security	0.788			
Legislature's, Regulatory and Institutional Framework on Financial operations	0.773			
Legislature's, Regulatory and Institutional Framework on Financial Security	0.744			
Implementation of Conventional Security in Financial Institution	0.688			
Implementation of Financial Security Policy	0.685			
Financial Crime Case Assessment	0.66			
Development and Usability of Financial Crime Database System		0.784		
Collaboration Between Financial Agencies		0.754		
Availability of Independent/Private Financial Security organization		0.701		
Rapid Response to Financial Emergency by Security Agencies		0.582		
Availability of IT Security Facility at Financial Centres			0.792	
Capacity Building/ IT Staff Development			0.77	
IT Literacy of Conventional Security Personnel			0.614	0.441
Proficiency of litigators on Financial Crime Cases				0.783
Public Awareness on Financial Crime and Security				0.691
Prosecution of Financial Criminals				0.658

Table 11: Component Score Coefficient Matrix

Variables	Component			
	1	2	3	4
National Policy on Financial operations and Security	0.346	-0.063	-0.162	-0.06
Legislative, Regulatory and Institutional Framework on Financial operations	0.316	-0.08	-0.077	-0.072
Legislature's, Regulatory and Institutional Framework on Financial Security	0.288	-0.148	-0.066	0.033
Implementation of Conventional Security in Financial Institution	0.252	-0.018	-0.032	-0.099
Implementation of Financial Security Policy	0.270	-0.051	0.124	-0.246
Public Awareness on Financial Crime/Security	-0.135	-0.159	0.061	0.493
Development and Usability of Financial Crime Database System	-0.113	0.522	-0.209	-0.022
IT Literacy of Conventional Security Personnel	-0.096	-0.166	0.35	0.167
Capacity Building/ IT Staff Development	-0.081	-0.066	0.547	-0.171
Collaboration Between Financial Agencies	-0.083	0.486	-0.138	-0.092
Availability of Independent/Private Financial Security organization	-0.108	0.433	-0.001	-0.146
Availability of IT Security Facility at Financial Centres	-0.083	-0.13	0.567	-0.112
Proficiency of litigators on Financial Crime Cases	-0.125	-0.073	-0.156	0.602
Financial Crime Case Assessment	0.228	-0.083	-0.012	-0.015
Rapid Response to Financial Emergency by Security Agencies	-0.052	0.283	0.039	-0.087
Prosecution of Financial Criminals	-0.031	-0.03	-0.185	0.454

Table 12: Standard scores by Ten Respondents

Respond-nets	NpFos	AsFrO	AsFrS	CsAss	FsAss	FCcAs	ProFC	LigPr	PubAr	ItLit	FCSEc	CapSt	RapRe	FCDbs	CollB	InOrg
Res1	5	3	4	2	5	3	2	5	3	4	1	3	3	4	5	5
Res2	5	4	5	5	5	5	4	2	3	1	1	1	3	5	3	1
Res3	4	4	4	4	5	4	4	5	4	4	4	4	5	4	4	4
Res4	5	5	5	4	5	5	5	5	4	3	3	1	5	5	4	3
Res5	5	4	3	5	1	2	5	4	3	4	1	1	5	4	3	2
Res6	5	2	4	1	3	5	5	5	2	4	5	4	5	3	5	4
Res7	4	3	3	3	4	3	2	3	4	4	3	4	3	2	3	2
Res8	4	4	4	3	3	2	2	2	3	2	1	1	1	1	2	2
Res9	5	4	5	4	5	4	4	3	5	4	3	5	4	3	3	5
Res10	1	1	1	1	1	1	1	1	2	3	4	3	2	4	2	3

Given that the standard scores by the b^{th} respondent in the sixteen variables under consideration are $W_{b,1}$, $W_{b,2}$, $W_{b,3}$ . . ., $W_{b,16,}$ the financial crimes related issues based on the view of each respondent, in the areas of policies and regulations, responses and management, capacity building and awareness and litigation denoted by M_1 $M_{2,}$ $M_{3,}$ and M_4 are modeled as follows:

$$M_1 = 0.346W_{b,1} + 0.316W_{b,2} + \cdots - 0.031W_{b,16} \quad (9)$$

$$M_2 = -0.063W_{b,1} - 0.800W_{b,2} + \cdots - 0.30W_{b,16} \quad (10)$$

$$M_3 = -0.162W_{b,1} - 0.077W_{b,2} + \cdots - 0.185W_{b,16} \quad (11)$$

$$M_4 = -0.060W_{b,1} - 0.072W_{b,2} + \cdots + 0.454W_{b,16} \quad (12)$$

The standard scores by ten randomly selected respondents for each of the sixteen variables under consideration are presented in Table 12. Table 13 shows the calculated percentage contributions of each of the ten sampled respondents to each of the four factors. It is revealed that sampled respondent described with identity Res2 has the highest contribution of 5.76 (17.47%) to issue 1 while sampled respondent Res6 has the highest contribution of 3.89 (21.85%) to issue 2. Similarly, sampled respondent described with identity Res7 has the highest contribution of 3.29 (19.35%) to issue 3 and sampled respondent Res6 has the highest contribution of 4.50 (19.93%) to issue 4.

Table 13: Aggregate factor scores with percentage contributions for a subset of respondents

Respondents	Factor 1		Factor 2		Factor 3		Factor 4	
	Score	% Contribution	Score	% Contribution	Score	% Contribution	Score	% Contribution
Res1	3.76	11.36	0.80	4.51	2.31	13.56	2.68	11.85
Res2	5.79	17.47	0.02	0.10	0.65	3.84	1.62	7.19
Res3	3.22	9.73	2.34	13.15	2.92	17.14	3.03	13.42
Res4	4.62	13.96	1.83	10.28	1.08	6.32	3.51	15.54
Res5	3.47	10.48	2.55	14.33	-0.30	-1.77	2.77	12.28
Res6	1.17	3.52	3.89	21.85	1.57	9.20	4.50	19.93
Res7	2.66	8.04	1.74	9.77	3.29	19.35	0.78	3.47
Res8	4.02	12.12	0.45	2.53	0.93	5.47	0.21	0.93
Res9	3.91	11.80	1.67	9.41	3.05	17.91	2.49	11.01
Res10	0.50	1.51	2.50	14.08	1.53	8.98	0.99	4.38
Total	33.12	100.00	17.78	100.00	17.03	100.00	22.58	100.00

The eigenvalues and percentage variance for each of the four issues is shown in Table 14. It is revealed that the four extracted issues contributed 71.02% to financial crime related issues in Nigeria. Component 1 described as 'Policies and Regulations' contributes 53.37% out of 71.02%. This implies that government policies and regulations are very germane issues of financial security and must not be taken with levity. Components 2, 3 and 4 contribute 7.43%, 5.13% and 5.10% respectively. These imply that government must also focus on raising the awareness of its people to the need for safe and secure financial system as well as ensuring strong litigation measures against financial related crimes. It is also important that adequate attention be given to building strong capacity for all relevant groups and agencies as well as putting in place facilities for timely response and management of threats to safe financial system. The remaining 28.98% is considered as the expected influences of some extraneous components that are important but their related indices were not considered.

Table 14: Eigenvalue of factors

Component	Extraction Sums of Squared Loadings		
	Total	% of Variance	Cumulative %
1	8.539	53.367	53.367
2	1.188	7.426	60.793
3	.821	5.131	65.925
4	.815	5.095	71.020

V. Conclusion

Nigerian economy has suffered greatly in recent years dues to the rising cases of financial crimes in several agencies of public and private sectors. Financial criminals have used the Internet to commit all manners of frauds, embezzlement, tax invasion, money laundering and other despicable financial acts. Nigeria's international image has also suffered due to the involvement of some of her citizens in cases of financial crimes at local and international levels. In view of these, factor analysis by principal components has been used for the analysis of financial crimes related issues in Nigeria. Four issues were extracted with their respective related indices. The initial component matrix generated was subjected to orthogonal transformation to ensure reasonable factorization. The obtained factor score coefficient matrix provided the basis for the determination of the degree of reasonability of the assessment of every respondent.

The obtained eigenvalue of each issue gave its percentage impact on the current spate of financial crimes in Nigeria. The percentage contribution was less than 100, which is a pointer to some significant extraneous (latent) factors whose indices were not considered in the research instrument. The results of the factor analysis placed a high premium on government policies and regulations, responses and management, capacity building as well as awareness and litigation as the major issues for safe and secure financial system in Nigeria. These corroborated the positions held by the authors in [30-33] who opined that good governance should be provided at all levels for economic and social security, promoting selflessness and patriotism. The authors also agreed on the need for adequate counter-measure and litigation systems as necessary strategies for curbing the menace of financial crime. Findings from the research also established that systemic ways of ensuring that citizens adopt technical know-how for national development rather than committing crimes should be introduced and enforced by the Nigerian government.

References Références Referencias

1. Adegbie F., Fakile, A. (2012). Economic and Financial Crime in Nigeria: Forensic Accounting. British Journal of Arts and Scocial Sciences, 6.
2. Agus S., Sheela, N., Ming, Y., Aijun, Z., Daniel, K., Fernando, C. D. (2010). Statistical Methods for Fighting Financial Crimes. . American Statistical Association.
3. Agus, S., Nair, S., Yuan, M., Zhang, A., Kern, D., Cala-Diaz, F. (2010a). Statistical Methods For Fighting Financial Crimes. Technometrics, 5-19.
4. Ayoola F. J., Adeyemi M. A., Jabaru, S. O. (2015). On the Estimation of Crime Rate in the Southwest of Nigeria:Principal Component Analysis Approach. Global Journal of Science Frontier Research: F Mathematics and Decision Sciences.
5. Bussman K. (2003). Causes of Economic Crime and the Impact of Values:Business Ethics As a Crime Preventive Measure.
6. Deloitte J. (2014). Risk Angles: Five questions on financial crime. Deloitte Touche Tohmatsu Limited.
7. Donald J. A. (1993). Stopping Rules in Principal Component Analysis: Acomparison of Heuristical and Statistical Approaches. Ecology 74(8), 2204-2214.
8. Durmuş Y. (2007): Financial Security and Stability. İstanbul.
9. Edelherz E. (1977). White – collar and Professional Crime: The Challenge for the 1980s. American Behavioural Scientist, 109 – 128.
10. Ejiofor, O. C., Oni, S., Nwajei, R. I. (2007). Economic Crimes and National Security: A Perspective of The Nigerian Military. International Journal of Social Sciences and Humanities Reviews, 7, 190-202.
11. Galina P. (2014). Issues of Country Financial Security Governance, Forum Scientiae Oeconomia, 2.
12. Golden, T., Skalak, S., and Clayton, M. (2006). A Guide to Forensic Accounting Investigation. New York: Wiley.
13. Gottschalk, P. (2010). Categories of Financial Crim. Journal of Financial Crime.
14. Gulumbe S. U., Dikko, H., Bello, Y. (2012). Analysis of Crime Data using Principal Component Analysis: A Case Study of Katsina State. CBN Journal of Applied Statistics.
15. Horton E. H. (1939). The American Criminal Cambridge, MA: Harvard University Press.
16. Ibrahim, J., Adeyemi, M., Odunayo, K. (2015). Implication of Financial Crimes and Corruption on Manufacturing Firms in Osun State, Nigeria. European Journal of Business and Management.
17. International Monetary Fund (IMF) (2006). Financial System Abuse, Financial Crime and Money Laundering- Background Paper.
18. Iwasokun G. B., Alese B. K., Thompson A. B. Aranuwa O. F. (2012). Statistical Evaluation of the Impact of ICT on Nigerian Universities', International Journal of Educational Development with ICT', 8(1): 104-120.
19. Kaiser H. F. (1960). The Application of Electronic Computers to Factor Analysis. Education and Psychologic Measurement, 141-151.
20. Kitten T. (2016). News:BankInfo Security. Retrieved from BankInfo Security, Available: http://www.bankinfosecurity.com/big-datas-tie-to-fraud-prevention-a-6251
21. Ksenia, G. (2008). Can corruption and economic crime be controlled in developing countries and if so, is it cost-effective. Journal of Financial Crime, 223-233.
22. Ladan, M.(2005). Crime Prevention and Control and Human Rights in Nigeria.
23. McDowell, J., Novis, G. (2001). The consequences of Money Laundering and Financial Crime. An Electronic Journal of the U.S. Department of State.
24. Okoye, E., Gbegi, D. (2013). An Evaluation of the Effect of Fraud and Related Financial Crimes on the Nigerian Economy. Kuwait Chapter of Arabian Journal of Business and Management Review.
25. Raghavendra K., Konugurthi, P. K., Agarwal, A., Raghavendra, R. C., Rajkumar, B. (2011). The Anatomy of Big Data Computing.
26. Shai S. S., Shai B. D. (2014). Algorithm, Understanding Machine Learning: from Theory to. Cambridge Univerisity Press.
27. Silipo R. (2015). Seven Techniques for Data Dimensionality Reduction, Available: https://www.kdnuggets.com/2015/05/7-methods-data-dimensionality-red
28. Sofia de Oliveira, I., Keatinge, T., Stickings, A. (2016). Building Trust and Taking Risks in the Global Effort to Tackle Financial Crime. RUSI Occasional Paper.
29. Spencer P., and Pickett, J. (2002). Financial Crime, Investigation and Control. John Wiley and Sons, Inc.
30. Sutherland, E. (1939). The White-collar Criminal. American Sociological Reviews, 1-12.
31. Usman, U., Yakubu, M., Bello, A.Z. (2012). Encouraging Public-Private Partnerships to Fight Financial Crime An Investigation on the Rate of Crime in Sokoto State Using Principla Componenet Analysis. Nigerian Journal of Basic and Applied Science, 152-160.
32. Yusuf, I. (2009). The Devastating Impact of Money Laundering and other Economic and Financial Crimes on the Economy of Developing Countries: Nigeria as a Case Study. Curtin International Business Conference.

Appendix 1

Questionnaire on Analysis of Financial Crime Related Issues in the Scenery of Nigeria

The purpose of this Questionnaire is to conduct investigative analysis of financial crimes related issues in Nigerian with a view to developing a pro-active solution. Confidentiality of personal information is guaranteed. We would therefore appreciate your sincere contributions to the research by giving a very accurate and honest response to this Questionnaire.

Section A: Profile of Respondents

1. *AGE* (Please Tick as appropriate)

5-10		11-18		19-44		45 and above	

2. *SEX* (Please Tick as appropriate)

Male		Female	

3. *Highest Academic Qualification* (Please Tick as appropriate)

Primary Schl. Cert.	
O. Level	
A. Level	
B. Sc./B. Tech.	
M. Sc./M. Tech.	
PhD/D. Sc./D. Tech	
Others	

4. Occupation

5. Organization

6. *LOCATION* (local Government and State)

7. *Computer Literacy Level* (Pls. Tick (√) as appropriate)

Excellent	
Very Good	
Good	
Average	
Poor	

8. *Understanding of the Internet* (Pls. Tick (√) as appropriate)

Excellent	
Very Good	
Good	
Average	
Poor	

9. *Understanding of Financial/Computer Crime* (Pls. Tick (√) as appropriate)

Excellent	
Very Good	
Good	
Average	
Poor	

10. *Have You Been a Victim of Computer Crime* (Please Tick (√) as appropriate)

Yes	
No	

IF YES:

11. TICK (√) AS APPROPRIATE, THE INCIDENCES

Advance fee fraud ("Yahoo Yahoo")	
Forgery (Fake Office Documents, Certificates, etc.)	
ATM (Money Theft Through ATM)	
Piracy (Pirated Software, Video/Audio CDs, etc.).	
Phreaking (Making Fraudulent free calls)	
Spamming (Unsolicited emails)	
Embezzlement (Executive Theft, Salami Shaving. etc.).	
Computer Virus and/or Denial of Service	
Pornography/Financial Grooming	
Others(Specify):	

12. TICK (√) AS MANY AS POSSIBLE MODE OF OCCURRENCES

1-5	
6-10	
11-15	
16-20	
Above 20	

13. Financial Crime Gender Incidence

Index	Very High	High	Medium	Low
Male				
Female				

14. Financial Criminals' Age Range

Index	*Very High*	*High*	*Medium*	*Low*
2-11				
12-17				
18-25				
26-45				
Above 45				

Section B: Assessment of Financial Security Related Issues

Pls. Tick/Write as appropriate depending on the level/Intensity of Indices using the scale of Excellent, Very Good, Good Average or Poor.

Index	Excellent	Very Good	Good	Average	Poor
National Policy on Financial operations and Security					
Legislative, Regulatory and Institutional Framework on Financial operations					
Legislative, Regulatory and Institutional Framework on Financial Security					
Implementation of Conventional Security in Financial Institution					
Implementation of Financial Security Policy					
Financial Crime Case Assessment					
Prosecution of Financial Criminals					
Proficiency of litigators on Financial Crime Cases					
Public Awareness on Financial Security					
IT Literacy of Conventional Security Personnel					
Availability of IT Security Facility at Financial Centers					
Capacity Building/ IT Staff Development					
Rapid Response to Financial Emergency by Security Agencies					
Development and Usability of Financial Crime Database System					
Collaboration Between Financial Agencies					
Availability of Independent/Private Financial Security organization					

This page is intentionally left blank

Global Journal of Computer Science and Technology: E Network, Web & Security
Volume 19 Issue 1 Version 1.0 Year 2019
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

SDN-Based Approach to Evaluate the Best Controller: Internal Controller NOX and External Controllers POX, ONOS, RYU

By Mohammad Nowsin Amin Sheikh, Monishanker Halder, Sk. Shalauddin Kabir, Md. Wasim Miah & Sawrnali Khatun

Jessore University of Science and Technology

Abstract- Software Defined Networking (SDN) is a rising technique to deal with replace patrimony network (coupled hardware and software program) control and administration by separating the control plane (software program) from the information plane (hardware). It gives adaptability to the engineers by influencing the focal control to plane straightforwardly programmable. Some new difficulties, for example, single purpose of disappointment, may be experienced because of the original control plane. SDN concentrated on flexibility where the security of the system was not essentially considered. It promises to give a potential method to present Quality of Service (QoS) ideas in the present correspondence networks. SDN automatically changes the behavior and functionality of system devices utilizing a single state program. Its immediate OpenFlow is planned by these properties. The affirmation of Quality of Service (QoS) thoughts winds up possible in a versatile and dynamic path with SDN. It gives a couple of favorable circumstances including, organization and framework versatility, improved exercises and tip-top performances.

Keywords: *SDN, QoS, NOX, POX, ONOS, CPU, TCP, OS, BSD, WAN, ODL, FIB, IP, MAC, API, IT, IOT, IOE.*

GJCST-E Classification: *B.4.2*

Strictly as per the compliance and regulations of:

SDN-Based Approach to Evaluate the Best Controller: Internal Controller NOX and External Controllers POX, ONOS, RYU

Mohammad Nowsin Amin Sheikh [α], Monishanker Halder [σ], Sk. Shalauddin Kabir [ρ], Md. Wasim Miah [ω] & Sawrnali Khatun [¥]

Abstract- Software Defined Networking (SDN) is a rising technique to deal with replace patrimony network (coupled hardware and software program) control and administration by separating the control plane (software program) from the information plane (hardware). It gives adaptability to the engineers by influencing the focal control to plane straightforwardly programmable. Some new difficulties, for example, single purpose of disappointment, may be experienced because of the original control plane. SDN concentrated on flexibility where the security of the system was not essentially considered. It promises to give a potential method to present Quality of Service (QoS) ideas in the present correspondence networks. SDN automatically changes the behavior and functionality of system devices utilizing a single state program. Its immediate OpenFlow is planned by these properties. The affirmation of Quality of Service (QoS) thoughts winds up possible in a versatile and dynamic path with SDN. It gives a couple of favorable circumstances including, organization and framework versatility, improved exercises and tip-top performances. This research work will concentrate on the Quality of Service (QoS) like delay, response time, throughput, and other execution assessing parameters of our proposed arrange design using internal controller, e.g., Network Operating System (NOX) and external controller, e.g., Pythonic Network Operating System (POX), Open Network Operating System (ONOS) and RYU. Regardless of the way that thoughts of QoS, they did not comprehend the correspondence systems with high utilization, diverse quality and acknowledgment costs. It will focus on the outside controller and inner controller execution in the proposed architecture. These perceptions of switch diversity may give SDN application engineer's bits of knowledge while acknowledging QoS ideas in an SDN-based system.

Keywords: SDN, QoS, NOX, POX, ONOS, CPU, TCP, OS, BSD, WAN, ODL, FIB, IP, MAC, API, IT, IOT, IOE.

Author α: Assistant Professor in the department of Computer Science and Engineering in Jessore University of Science and Technology, Bangladesh. e-mail: nowsin.jstu@gmail.com

Author σ: Lecturer in the department of Computer Science and Engineering in Jessore University of Science and Technology, Bangladesh. e-mail: monicsejust@gmail.com

Author ρ: M.Sc. degree in the department of Computer Science and Engineering in Jessore University of Science and Technology, Bangladesh. e-mail: riponcse32@gmail.com

Author ωY¥: B.Sc. degree in the department of Computer Science and Engineering in Jessore University of Science and Technology, Bangladesh. e-mails: wasimcse767@gmail.com, sawrnalikhatun@gmail.com

I. Introduction

Software Defined Networking (SDN) is the current worldview of the systems administration which is taken under consideration by stakeholders with a huge concern. The idea works towards significantly decreasing system organization and administration costs. SDN's innovation is a novel method to manage conveyed figuring that encouraged to arrange administration and empowers system setup automatically, keeping in mind the end goal to enhance monitoring and network performance [1]. It is intended to address the way that the static engineering of the conventional network is decentralized and complex while current systems require greater adaptability and simple investigating. SDN recommends incorporating system insight in one system segment by disassociating the sending procedure of network parcels (Data Plane) from the routing procedure (Control plane). The control plane comprises of at least one controller which is the cerebrum of SDN and the entire insight consolidates there. In any case, the knowledge centralization has its particular downsides with regards to security, [2] versatility and elasticity [3] of SDN. Software Defined Networking [4], [5] is a network system that offers a plan to change the impediments of current system frameworks. In the first place, it breaks the vertical coordination by isolating the system's control logic (the control plane) from the hidden switches and routers that forward the activity (the information plane). Second, with the detachment of the control and information planes, arrange switches end up straightforward sending gadgets and the controlling rationale is executed in a sensibly brought together controller (or system working framework), disentangling strategy implementation and network reconfiguration and advancement [6]. It encompasses different sorts of network headway proposed to make more versatile and spry to help the capacity structure and virtual server of the line server ranches. We will without a lot of an understand SDN against standard framework by a prime portrayal; acknowledged inside the groups that we have to pass on a bundle in the standard; it must change its course thing times for finding the ideal way. It is a proficient structure to use better Quality of Service (QoS) which

exhibits to a framework's profitability to achieve most vital transmission limit and oversee other framework execution parts like inactivity, error rate and run time [7]. An SDN controller is an application in SDN that supervises stream control to engage smart frameworks administration. SDN controllers rely upon convention, for instance, OpenFlow, that empower servers to encourage changes where to send Packets.

Network Operating Systems (NOX) is the first OpenFlow controller. It fills in as a system control stage that gives an abnormal state automatic interface for administration and the advancement of system control applications. Its framework reflects the change and sorting out into a product issue. NOX is a bit of the software-defined networking (SDN) biological system. In particular, it's a stage for building system control applications. The main SDN innovation to get acknowledgment is OpenFlow, and NOX is the first creation at Nicira Networks next to each other with OpenFlow — NOX was the primary OpenFlow controller. Nicira gave NOX to the examination group in 2008, and from that point forward, it has been the reason for some and different research extends in the early investigation of the SDN space. Its applications are different kinds of activities on an abnormal state of nonattendance of unfaltering quality in organizing execute fragment, not at all like bring down back of estimation game-plan [8][9] applications. The system working structure does not manage itself; It outfits a programming interface with top state objects, (for instance, plate accumulating volume, CPU preparing power, memory control, etc.) of framework resources, which engages sort out application undertakings to manage secure and down to earth complex assignments on a combination of network [9]. The NOX, in any case, fails in giving the required capacities to QoS-guaranteed Software Defined Networking (SDN) [10] convenience provisioning on transporter review supplier Internet, for example, QoS-cautious virtual network inserting, end-to-end arrange QoS appraisal, and joint efforts among control components for others space network.

Pythonic Network Operating System (POX) [11] is an open source advancement stage for Python-based software-defined networking (SDN) control applications, for example, OpenFlow SDN controllers. The controller gives an effective method to actualize the OpenFlow convention which is the accepted correspondence convention between the controllers and the switches. Utilizing POX controller can run distinctive applications like center point, switch, firewall, and load balancer. TCP dump bundles catch the instruments to see the bundles streaming between POX controller and OpenFlow devices. It uses as a part of SDN network systems since it has a Python dialect interface for research [12]. OpenFlow, when all says in done has pulled in considerable enthusiasm from industry [13] [14]. POX formally requires Python 2.7 (however quite a bit of it will work fine with Python 2.6) and should keep running under Linux, Mac OS, and Windows. (What's more, pretty much anyplace else - we've run it on Android telephones, under FreeBSD, Haiku, and somewhere else).

Open Network Operating System (ONOS) [15] is the main open source SDN controller for building next-generation SDN/NFV solutions. It gives the control plane to a software-defined network (SDN), overseeing network segments, for example, switches and connections, and running programming projects or modules to give correspondence administrations to end has and neighboring systems. ONOS stages do flaunt being intended to help, like different controllers, different application classifications, for example, control, setup and the executive's applications. Among the applications that are distributed by ON.Lab, some of them are Segment Routing, multi-layer SDN control, topology watcher, way calculation and SDN-IP peering applications.[16][17] ONOS strengthen different types of southbound protocols like OpenFlow, NetConf, and so on., for correspondence with an assortment of net gadgets. ONOS, like different controllers (ex: ODL), utilizes the idea of suppliers — one each for each southbound convention – which conceals convention unpredictability from different segments of the controller stage. These suppliers give all the essential 'depictions' of system components profoundly layer. [18]

RYU Controller is an open; Software Defined Networking (SDN) Controller intended to expand the deftness of the system by making it simple to oversee and adjust how traffic is taken carefully. By and large, the SDN Controller is the brains of the SDN condition, imparting data down to the switches and switches with southbound APIs, and up to the applications and business rationale with northbound APIs. It gives programming segments, with all around characterized application program interfaces (APIs) that make it simple for designers to make new system the executives and control applications. This segmented approach encourages associations to redo arrangements to meet their particular needs; engineers can rapidly and effortlessly adjust existing segments or execute their very own to guarantee the fundamental system can meet the changing requests of their applications. RYU bolsters different conventions for overseeing system gadgets, for example, OpenFlow, NetConf, OF-Config, and so forth. [19]

II. Related Work

Past work on giving QoS ensures utilizing Open-Flow can be divided into three classifications. To start with, studies about conveying dynamic QoS in an SDN domain [20][21][22]. Second, ponders on switch assorted variety [23] [24] [25] [26].Third, look into on

arranging execution coming about because of QoS with OpenFlow-empowered switches [27], [28].

A portion of the work done in the region of SDN-based, on request provisioning of system assets is concentrated towards computerized, strategy based system provisioning [29] [30], while other focuses towards movement designing crosswise over Wide Area Networks (WANs) [31][32]. Dynamic distribution of system assets additionally requires inside the server farms, and numerous Investigations address this test. For instance, an OpenFlow-based calculation for designation of transfer speed assets between virtual machines in server farms is exhibited in [33], while in [34] the creators depict a stage for incorporated provisioning of a process, stockpiling and system assets in server farms.

Lately, different specialists have been done to break down SDN controllers like NOX, ODL, ONOS, and RYU and so on. Other research paper had found out the beginning consequences of benchmarking through Open-Daylight SDN external Controller with Floodlight controller. The Researcher had assessed throughput, inaction and response time of Open Daylight SDN Controller and Floodlight under various conditions [35]. A related undertaking of particular note is Maestro [36] (made in parallel to NOX), which also charge as a "framework working system." Through NOX controller 4D structures are to control sending (e.g., FIBs in switches), and in this way their frameworks consolidate to arrange an establishment (e.g., joins, switches/switches). The Rational [37] and Ethane [38] wanders give more broad class of convenience by including a namespace for customers and center points in their framework view and observing the ties between these names and the low-level IP addresses and MAC.

Scientists were Used POX Controller for measuring the Network Programmability [39]. POX is used to examine the Performance parameters including inactivity and throughput, service quality, versatility, delay, response time and security. The exploration of execution and adaptability finish with Clench. Security and service quality test has alter with probe.

III. Description of the Proposed Architecture

To measure the Quality of Service (QoS) like throughput, response time, delay and other execution evaluating parameters, we made SDN based cloud architecture. In our created engineering, there are nine routers connected with three cloud interfaces. These various routers connect with eight hosts which have an IP address. For measuring QoS shows from hosts to switches, SDN controllers use as existing controllers and external controllers.

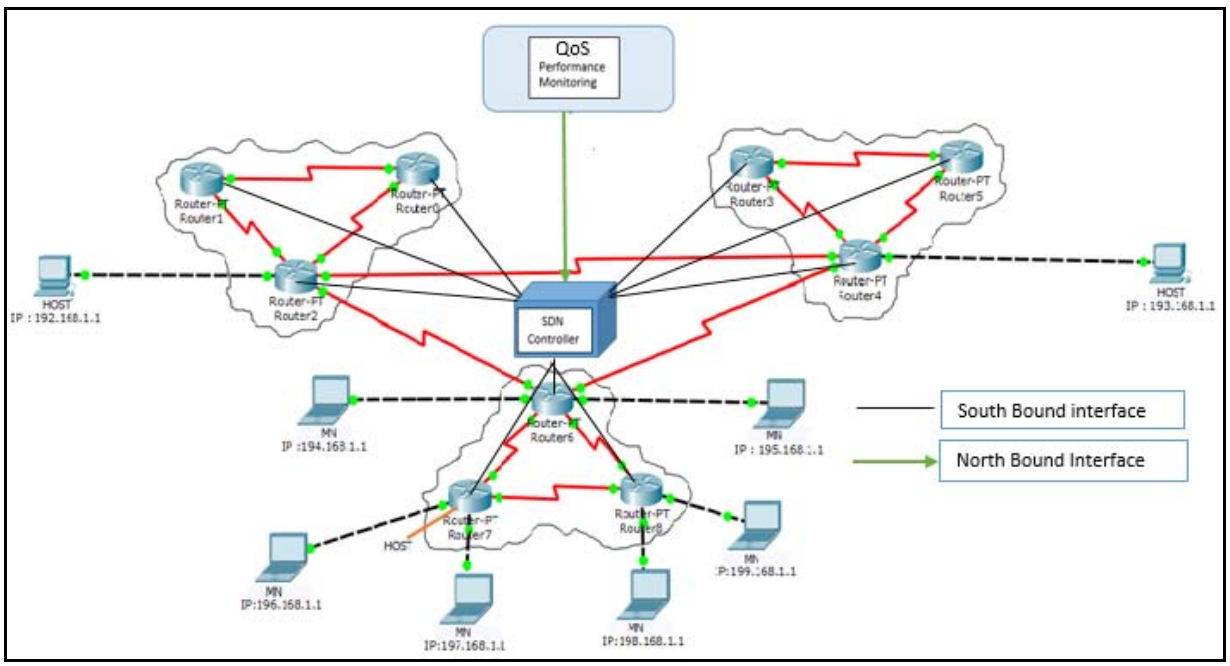


Fig. 1: Proposed_SDN_architecture and its real-time loop

a) Architectural description based on NOX controller

Network operating system (NOX) empowers administration applications to develop as brought together projects over high state reflections of system assets as an inverse to the dispersed calculations over low-level locations [40, 41]. The essential parts of a NOX-based system: an arrangement of switches and at least one organize appended servers. The NOX programming (and the administration applications that keep running on NOX) keep running on these servers. IT

includes a few distinctive controller forms (commonly one on each system appended server), and a system sees (this keep in a database running on one of the servers). The arrange see contains the consequences of NOX's system perceptions; applications utilize this state to settle on administration choices. For NOX to control organized the activity, it must control arrange switches; for this reason, we use the switches that help the OpenFlow switch reflection [42].

b) Architectural description based on POX controller

POX, which creates in python, is a tip-top, open source OpenFlow controller. An SDN controller developer develops POX in light of Haiku, a trial OpenFlow controller from Stanford University. Huge Switch Networks backs POX as an association that essentially offers answers for business data centers. It offers different features and consultations for controlling an OpenFlow organize. For perfect utilization of benefits, POX relies upon multi-threading and can manage a couple of million new streams for each second. The Westbound python allows the change of custom modules in python and quick interfacing with the middle controller. The modules are stacked by methods for an alternate structure when the POX controller starts. You would along these lines have the capacity to utilize the full handiness of the controller and OpenFlow API and speedily respond to events on the framework, for instance, the ascent of new packages or new streams. The Open Flow datapath despite QoS modules shapes the QoS Flow datapath. This datapath is a consumption space utilize where lines mastermind in the portion space. The QoS module develops a station with the bit through Netlink to relate for both service and bit map. Like this, the POX can instantiated to connect with activity adornment and enqueuing of streams in our proposed engineering.

c) Architectural description based on ONOS controller

ONOS was intended to address the issues of administrators wishing to construct bearer level arrangements that use the financial aspects of white box vendor silicon equipment while offering the adaptability to make and send new unique system administrations with disentangled automatic interfaces. It underpins both setup and constant control of the system, disposing of the need to run directing and exchanging control conventions inside the system texture. By moving knowledge into the ONOS cloud controller, advancement empowers, and end-clients can undoubtedly make new system applications without the need to adjust the data-plane frameworks. In ONOS, in contrast to different controllers, disseminated engineering support is one of the plan standards and not an idea in retrospect bolster. It is additionally like five to six of the dispersed models portrayed above in the Distributed SDN Controller Architecture segment. That is, ONOS can be sent as the gathering of controller-servers that facilitate with one another to accomplish strength, adaptation to non-critical failure, and better load the executives.

d) Architectural description based on RYU controller

RYU controller is single-strung substances which execute different functionalities in RYU. Events are messages between them. It sends offbeat occasions to one another. Other than that, there are some RYU-inner occasion sources which are not RYU applications. One of the instances of such occasion sources is Open-stream controller. While an occasion can as of now contain self-assertive python protests, it's debilitated to pass complex items (e.g. unpick capable terms) between RYU. Each RYU controller has a get line for occasions. It has a string for occasion preparing. The RYU controller continues depleting the get line by lining a datapath and calling the proper occasion handler for the occasion's type. Since the occasion handlers bring with regards to the occasion preparing string, it ought to be cautious when blocking. While an occasion handler hinders, no further occasions for the RYU application will process. There are sorts of handlers which are utilized to actualize synchronous between application calls between RYU controller.

IV. Comparison Between the Internal and External Controllers on our Proposed Architecture

a) NOX controller

i. *Response Time of NOX* controller

Figure 2 shows the graph of the calculation of Response Time with NOX of Table 1.

Table 1: Calculation of Response Time with NOX controller

Number of Operations	Response Time (NOX) ms
4	0.028
8	0.029
12	0.030
16	0.029
20	0.031
24	0.032
28	0.033
32	0.032
36	0.033
40	0.031
44	0.034
48	0.033
52	0.034
56	0.034
60	0.035
64	0.034

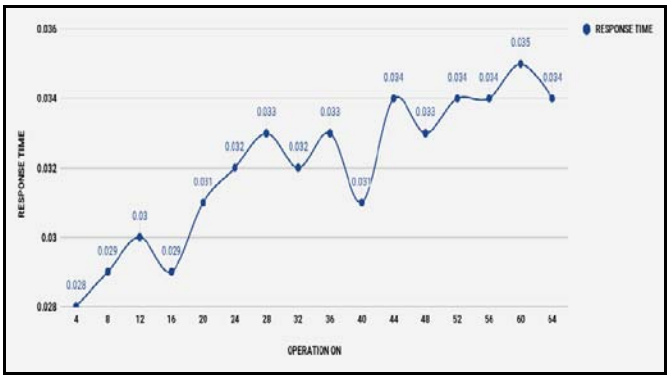


Fig. 2: Response Time of NOX controller

ii. *Throughput of NOX* controller

Figure 3 shows the graph of the calculation of Throughput with NOX of Table 2.

Table 2: Calculation of Throughput with NOX controller

Number of Operations	Throughput (NOX) ms
4	0.138
8	0.156
12	0.234
16	0.274
20	0.279
24	0.274
28	0.231
32	0.234
36	0.275
40	0.274
44	0.187
48	0.234
52	0.244
56	0.217
60	0.217
64	0.187

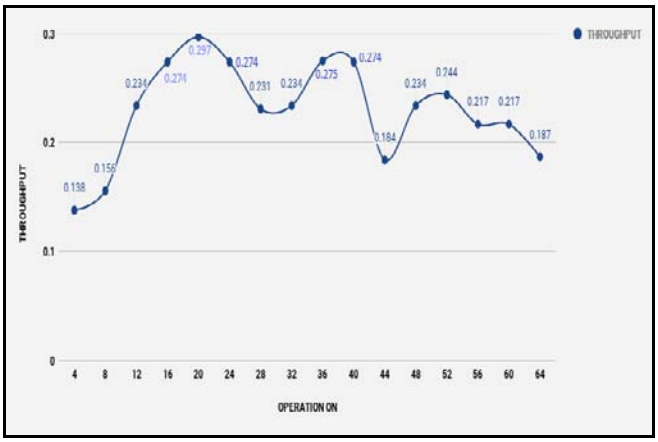


Figure 3: Throughput of NOX controller

b) Pythonic Network Operating System (POX) controller

i. *Response Time of POX controller*

Figure 4 represents the graph for the calculation of Response Time with POX of Table 3.

Table 3: Calculation of Response Time with POX controller

Number of Operations	Response Time (POX) ms
4	0.045
8	0.041
12	0.037
16	0.039
20	0.039
24	0.040
28	0.039
32	0.038
36	0.037
40	0.036
44	0.036
48	0.041
52	0.040
56	0.044
60	0.043
64	0.042

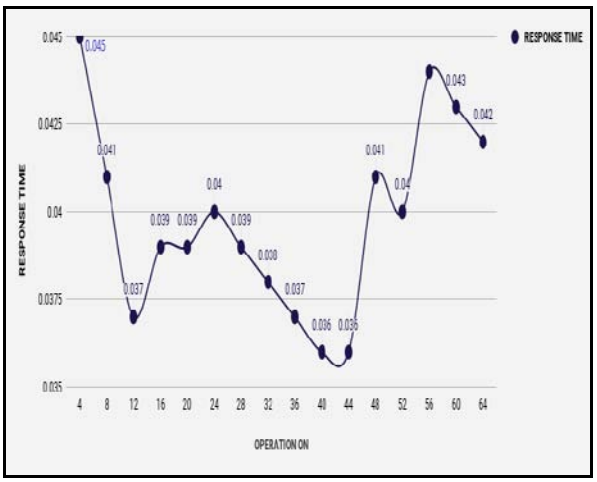


Figure 4: Response Time of POX controller

ii. *Throughput of POX controller*

Figure 5 shows the graph of the calculation of Throughput with POX of Table 4.

Table 4: Calculation of Throughput with POX controller

Number of Operations	Throughput (POX) ms
4	0.660
8	0.751
12	0.692
16	0.745
20	0.649
24	0.673
28	0.604
32	0.589
36	0.554
40	0.533

44	0.510
48	0.502
52	0.476
56	0.462
60	0.442
64	0.420

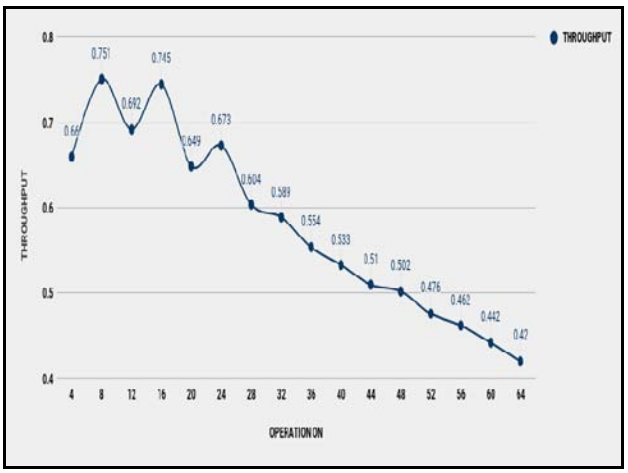


Figure 5: Throughput of POX controller

c) *Open Network Operating System (ONOS) controller*

i. *Response Time of ONOS controller*

Figure 6 shows the graph of the calculation of Response Time with ONOS of Table 5.

Table 5: Calculation of Response Time with ONOS controller

Number of Operations	Response Time (ONOS) ms
4	0.070
8	0.063
12	0.060
16	0.058
20	0.057
24	0.056
28	0.055
32	0.054
36	0.053
40	0.052
44	0.050
48	0.049
52	0.049
56	0.047
60	0.047
64	0.048

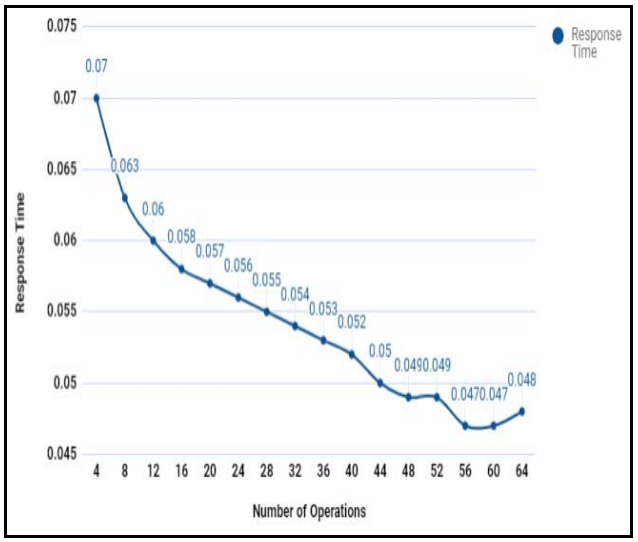


Figure 6: Response Time of ONOS controller

ii. *Throughput of ONOS controller*

Figure 7 shows the graph of the calculation of Throughput with ONOS of Table 6.

Table 6: Calculation of Throughput with ONOS controller

Number of Operations	Throughput (ONOS) ms
4	0.634
8	0.449
12	0.351
16	0.303
20	0.228
24	0.180
28	0.161
32	0.122
36	0.121
40	0.118
44	0.117
48	0.129
52	0.116
56	0.123
60	0.119
64	0.127

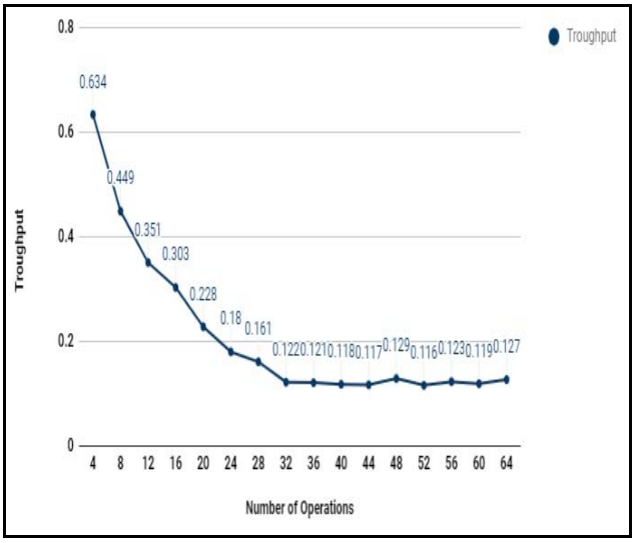


Figure 7: Throughput of ONOS controller

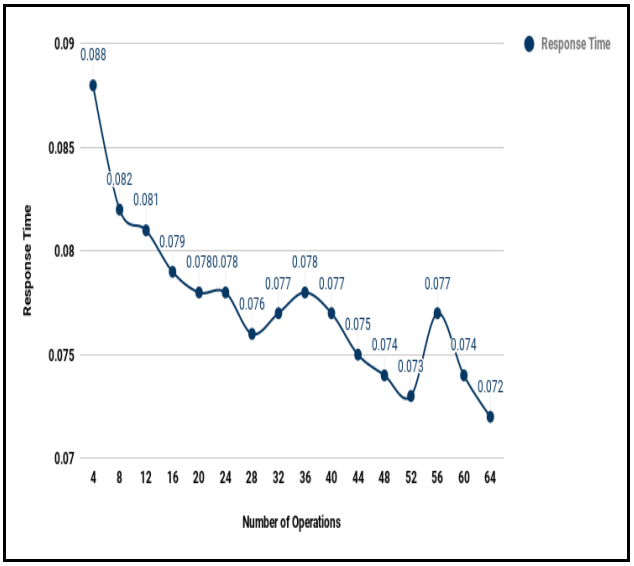


Figure 8: Response Time of RYU controller

d) RYU controller

i. *Response Time of RYU controller*

Figure 8 shows the graph of the calculation of Response Time with RYU of Table 7.

Table 7: Calculation of Response Time with RYU controller

Number of Operations	Response Time (RYU) ms
4	0.088
8	0.082
12	0.081
16	0.079
20	0.078
24	0.078
28	0.076
32	0.077
36	0.078
40	0.077
44	0.075
48	0.074
52	0.073
56	0.077
60	0.074
64	0.072

ii. *Throughput of RYU controller*

Figure 9 shows the graph of the calculation of Throughput with RYU of Table 8.

Table 8: Calculation of Throughput with RYU controller

Number of Operations	Throughput (RYU) ms
4	1.177
8	0.652
12	0.442
16	0.460
20	0.251
24	0.435
28	0.251
32	0.215
36	0.435
40	0.188
44	0.262
48	0.271
52	0.195
56	0.276
60	0.269
64	0.178

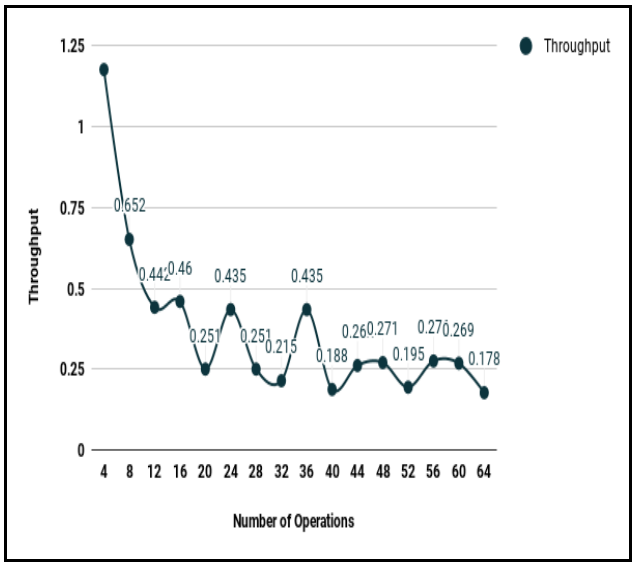


Figure 9: Throughput of RYU controller

V. Performance Analysis Equation

We executed 64 operations in our Proposed_SDN_architecture. In the comparison of response time and throughput among internal controller Network operating system (NOX) and external controllers Pythonic Network Operating System (POX), Open Network Operating System (ONOS) and RYU.

The performance of response time and throughput in our Proposed_SDN_architecture can be calculated against internal and external controllers by the following equation:

Let, Performance (P) = M/N

Where N = Sum of the response time or the throughput of internal controller NOX.

M = Sum of the response time or the throughput of external controllers POX, ONOS, and RYU.

VI. Performance Analysis Among Internal Controller Nox And External Controllers Pox, Onos, Ryu

a) Comparison of Response Time

i. *Response Time between NOX and POX, NOX and ONOS, NOX and RYU controllers*

The performance of response time in our Proposed_SDN_architecture can be calculated against internal controller NOX and external controllers POX, ONOS and RYU by the following equation:

NOX and POX:

Let, Performance (P) = M/N

Where N = sum of the response time of internal controller NOX

M = sum of the response time of external controller POX

Here, M = 0.637

N = 0.512

So, P = (0.637/0.512) times

= 1.244 times

NOX and ONOS:

Let, Performance (P) = M/N

Where N = sum of the response time of internal controller NOX

M = sum of the response time of external controller ONOS

Here, M = 0.868

N = 0.512

So, P = (0.868/0.512) times

= 1.695 times

NOX and RYU:

Let, Performance (P) = M/N

Where N = sum of the response time of internal controller NOX

M = sum of the response time of external controller RYU

Here, M = 1.239

N = 0.512

So, P = (1.239/0.512) times

= 2.420 times

ii. *Throughput between NOX and POX, NOX and ONOS, NOX and RYU controllers*

The performance of throughput in our Proposed_SDN_architecture can be calculated against internal controller NOX and external controllers POX, ONOS and RYU by the following equation:

NOX and POX:

Let, Performance (P) = M/N

Where N = sum of the throughput of internal controller NOX

M = sum of the throughput of external controller POX

Here, M = 9.262

N = 3.655

So, P = (9.262/3.655) times

= 2.534 times

NOX and ONOS:

Let, Performance (P) = M/N

Where N = sum of the throughput of internal controller NOX

M= sum of the throughput of external controller ONOS

Here, M = 3.798

N = 3.655

So, P = (3.798/3.655) times

= 1.039 times

NOX and RYU:

Let, Performance (P) = M/N

Where N = sum of the throughput of internal controller NOX

M = sum of the throughput of external controller RYU

Here, M = 5.957
N = 3.655
So, P = (5.957/3.655) times
= 1.630 times

VII. Performance Analysis between External Controllers Pox, Onos, RYU

a) Comparison of Response Time

i. *Response Time between POX and ONOS, POX and RYU, ONOS and RYU controllers*

The performance of response time in our Proposed_SDN_architecture can be calculated against external controllers POX, ONOS, and RYU by the following equation:

POX and ONOS:

Let, Performance (P) = M/N

Where N = sum of the response time of external controller POX

M = sum of the response time of external controller ONOS

Here, M = 0.868
N = 0.637
So, P = (0.868/0.637) times
= 1.363 times

POX and RYU:

Let, Performance (P) = M/N

Where N = sum of the response time of external controller POX

M = sum of the response time of external controller RYU

Here, M = 1.239
N = 0.637
So, P = (1.239/0.637) times
= 1.945 times

ONOS and RYU:

Let, Performance (P) = M/N

Where N = sum of the response time of external controller ONOS

M = sum of the response time of external controller RYU

Here, M = 1.239
N = 0.868
So, P = (0.651/0.528) times
= 1.427 times

ii. *Throughput between POX and ONOS, POX and RYU, ONOS and RYU controllers*

The performance of throughput in our Proposed_SDN_architecture can be calculated against external controllers POX, ONOS and RYU by the following equation:

POX and ONOS:

Let, Performance (P) = M/N

Where N = sum of the throughput of external controller ONOS

M = sum of the throughput of external controller POX

Here, M = 9.262
N = 3.798
So, P = (9.262/3.798) times
= 2.439 times

POX and RYU:

Let, Performance (P) = M/N

Where N = sum of the throughput of external controller RYU

M = sum of the throughput of external controller POX

Here, M = 9.262
N = 5.957
So, P = (9.262/5.957) times
= 1.555 times

ONOS and RYU:

Let, Performance (P) = M/N

Where N = sum of the throughput of external controller ONOS

M = sum of the throughput of external controller RYU

Here, M = 5.957
N = 3.798
So, P = (5.957/3.798) times
= 1.568 times

VIII. Result Discussion

In our Proposed_SDN_architecture, we executed 64 operations, and we find the better QoS from the architecture through internal and external SDN controller. After measuring performance, we find that internal SDN controller is better than external SDN controller. As a result of comparison between internal controller NOX and external controllers POX, ONOS and RYU, the following results find-

- The response time of internal controller NOX is **1.244x** higher than the response time of external controller POX.
- The response time of internal controller NOX is **1.695x** higher than the response time of external controller ONOS.
- The response time of internal controller NOX is **2.420x** higher than the response time of external controller RYU.
- So, internal SDN controller **NOX** is better in the performance of response time than other controllers.

- The throughput of internal controller NOX is **2.534x** better than the throughput of external controller POX.
- The throughput of internal controller NOX is **1.039x** better than the throughput of external controller ONOS.
- The throughput of internal controller NOX is **1.630x** better than the throughput of external controller RYU.
- So, internal SDN controller **NOX** is better in the performance of throughput than other controllers.

As a result of comparison between external controllers POX, ONOS, and RYU, the following results find-

- The response time of external controller POX is **1.363x** higher than the response time of external controller ONOS.
- The response time of external controller POX is **1.945x** higher than the response time of external controller RYU.
- The response time of external controller ONOS is **1.427x** higher than the response time of external controller RYU.
- So, external SDN controller **POX** is better in the performance of response time than other external controllers.
- The throughput of external controller ONOS is **2.439x** better than the throughput of external controller POX.
- The throughput of external controller RYU is **1.555x** better than the throughput of external controller POX.
- The throughput of external controller ONOS is **1.568x** better than the throughput of external controller RYU.
- So, external SDN controller **ONOS** is better in the performance of throughput than other external controllers.

IX. Conclusion And Future Work

Software-defined networking (SDN) is a design implying to be dynamic, reasonable, cost-effective, and versatile, trying to be appropriate for the high-data transmission, dynamic nature of the present applications. It enables associations to quicken application sending and conveyance, drastically lessening IT costs through strategy empowered work process automation. SDN technology develops cloud models by giving mechanized, on-request application conveyance and versatility at scale. With SDN the item that harps on these controllers settles on the sum decisions and sends this information down to each physical gadget. The central goal of this work is empowering included regard benefits in sort out system. SDN uses to find the security services in different framework structures. It favors a fundamental and flexible insistence of existing dynamic Quality of Service (QoS) parts in the present correspondence arrange. In the examination of the response time of the proposed architecture, internal controller NOX is superior to external controller POX, ONOS, and RYU. On account of throughput, internal controller NOX is additionally better. Among external controllers, POX is better in the performance of response time, and ONOS is better in the performance of throughput than other external controllers. Using SDN, we will work with Number of Bandwidth Isolation, Queues Impact, QoE Evaluation, and Switch Capacity. We will likewise chip away at stack adjust, security frameworks, remote system, Secure Mobility, Cloud Networking, etc. We will work at IOE or IOT like city automation, industry, home, country etc. through the best Quality of Service (QoS) by adducting our proposed SDN architecture with different controllers.

References Références Referencias

1. Benzekki Kamal et al.Software defined networking (SDN): a survey., Security and Communication Networks 9, no. 18 (2016): 5803-5833.
2. Benzekki Kamal et al.Devolving IEEE 802.1 X authentication capability to data plane in software-defined networking (SDN) architecture. Security and Communication Networks 9.17 (2016): 4369-4377.
3. Benzekki Kamal et al Software-defined networking (SDN): a survey., Security and Communication Networks 9, no. 18 (2016): 5803-5833.
4. N. Mckeown, "How SDN will Shape Networking," October 2011. [Online]. Available: http://www.youtube.com/watch?v=c9-K5O qYgA
5. S. Schenker, "The Future of Networking, and the Past of Protocols," October 2011. [Online]. Available: http://www.youtube.com/watch?v=YHeyuD89n1Y
6. H. Kim and N. Feamster, "Improving network management with software defined networking," Communications Magazine, IEEE, vol. 51, no. 2, pp. 114–119, 2013.
7. "Control of Multiple Packet Schedulers for Improving QoS on OpenFlow/SDN Networking - IEEE Xplore Document." 12 December 2013.
8. ArsalanTavakoli et al, "Applying NOX to the Datacenter," in Proc. Of SIGCOMM Hotnet 2009.
9. Natasha Gude et al., "NOX: Towards an Operating System for Networks," editorial note submitted to CCR.
10. DimitriStaessens et al., "Software Defined Networking: Meeting Carrier Grade Requirements," in Proc. of IEEE Workshop on Local & Metropolitan Area Networks (LANMAN), 2011.
11. Fernandez, Marcial. "Evaluating OpenFlow controller paradigms." In ICN 2013, The Twelfth

International Conference on Networks, pp. 151-157. 2013.
12. Rodrigues Prete, L. et al, "Simulation in an SDN network scenario using the POX Controller," 2014 IEEE COLCOM Conference, pp.1-6, 4-6 June 2014.
13. Levy, S., "Going with the Flow: Google's Secret Switch to the Next Wave of Networking", Wired, April 17, 2012.
14. Neagle, C. "HP takes giant first step into OpenFlow: HP is announcing its first effort to support OpenFlow standard on its Ethernet switches". Network World, February 2012.
15. ON.Lab white paper "Introducing ONOS — A SDN Network Operating System for Service Providers", 2014.
16. Pankaj Berde, Matteo Gerola, Jonathan Hart, Yuta Higuchi, Masayoshi Kobayashi, Toshio Koide, Bob Lantz, Brian O'Connor, Pavlin Radoslavov, William Snow, and Guru Parulkar. 2014. ONOS: Towards an Open, Distributed SDN OS. In "Proceedings of the Third Workshop on Hot Topics in Software Defined Networking" (HotSDN '14). ACM, New York, NY, USA, 1-6
17. Prajakta Joshi, "Introducing ONOS," Webinar, 2014 http://www.opennetsummit.org/ons-inspire-webinars-onlab-onos-nov11.php
18. ON.Lab white paper, "Driving SDN Adoption in Service Provider Networks", 2014.
19. Mohammad Nowsin Amin Sheikh, Monishanker Halder, SK. Shalauddin Kabir, Rathindra Nath Mohalder "Performance Evaluation on Software Defined Networking through External Controller Floodlight and Internal Controller NOX" International Journal of Scientific and Engineering Research (IJSER) - (ISSN 2229-5518), IJSER Volume 9, Issue 7, July 2018.
20. P. Georgopoulos, Y. Elkhatib, M. Broadbent et al., "Towards networkwide QoE fairness using OpenFlow-assisted adaptive video streaming," in Proc. of the 2013 ACM SIGCOMM Workshop on Future Human- Centric Multimedia Networking (FhMN 2013), Hong Kong, China, 2013, pp. 15–20.
21. T. Zinner, M. Jarschel, A. Blenk et al., "Dynamic application-aware resource management using software-defined networking: implementation prospects and challenges," in Proc. of the 2014 IEEE Network Operations and Management Symposium (NOMS '14), Krakow, Poland, 2014, pp. 1–6.
22. A. Lazaris, D. Tahara, X. Huang et al., "Tango: simplifying SDN control with automatic switch property inference, abstraction, and optimization," in Proc. of the 10th ACM International on Conference on emerging Networking Experiments and Technologies (CoNEXT), Sydney, Australia, 2014, pp. 199–212.
23. M. Kuzniar, P. Peresini, and D. Kostic, "What you need to know about SDN control and data planes," EPFL, Lausanne, Switzerland, Tech. Rep. EPFL-REPORT-199497, 2014.
24. V. Mann, A. Vishnoi, A. Iyer et al., "VMPatrol: dynamic and automated QoS for virtual machine migrations," in Proc. of the 8th International Conference on Network and Service Management (CNSM), Las Vegas, USA, 2012, pp. 174–178.
25. Z. Bozakov and A. Rizk, "Taming SDN controllers in heterogeneous hardware environments," in Proc. of Second European Workshop on Software Defined Networks (EWSDN), Berlin, Germany, 2013, pp. 50 – 55.
26. M. Kuzniar, P. Peresini, and D. Kostic, "What you need to know about sdn flow tables," in Passive and Active Measurement, ser. Lecture Notes in Computer Science, J. Mirkovic and Y. Liu, Eds. Springer International Publishing, 2015, vol. 8995, pp. 347–359.
27. Md. Alam Hossain, Mohammad Nowsin Amin Sheikh, Monishanker Halder, Sujan Biswas & Md. Ariful Islam Arman, "Quality of Service in Software Defined Networking", Global Journal of Computer Science and Technology: ENetwork, Web & Security, Volume 18, Issue 3, Version 1.0, Year 2018, Online ISSN: 0975-4172& Print ISSN: 0975-4350.
28. A. Nguyen-Ngoc, S. Lange, S. Gebert et al., "Investigating isolation between virtual networks in case of congestion for a Pronto 3290 switch," in Proc. of the Workshop on Software-Defined Networking and Network Function Virtualization for Flexible Network Management (SDNFlex 2015), Cottbus, Germany, 2015.
29. Bari, M.F., Chowdhury, S.R., Ahmed R., Boutaba, R.: PolicyCop: an autonomic QoS policy enforcement framework for software defined networks. In: IEEE SDN for Future Networks and Services, Trento, Italy, pp. 1–7, November 2013.
30. Hong, C.Y., et al.: Achieving high utilization with software-driven WAN. In: Proceedings of the ACM SIGCOMM, Hong Kong, China, pp. 15–26 (2013).
31. Egilmez, H.E., Dane, S.T., Bagci, K.T., Tekalp, A. M.: OpenQoS: an openflow controller design for multimedia delivery with end-to-end Quality of Service over Software-Defined Networks. In: Proceedings of the Signal and Information Processing Association Annual Summit and Conference, Hollywood, California, US, pp. 1–8, December 2012.
32. Guo, J., Fangming, L., Haowen, T., Yingnan, L., Hai, J., John, L.: Falloc: fair networkbandwidth allocation in IaaS datacenters via a bargaining game approach. In: Proceedings ofthe ICNP, Gotingen, Germany, pp. 1–10, October 2013.

33. Benson, T., Akella, A., Shaikh, A., Sahu, S.: CloudNaaS: a cloud networking platform for enterprise applications. In: Proceedings of the 2nd ACM Symposium on Cloud Computing, Cascais, Portugal (2011)
34. Jain, S., et al.: B4: Experience with a globally-deployed software defined WAN. ACMSIGCOMM Comput. Commun. Rev. 43(4), 3–14 (2013).
35. Z. K. Khattak, M. Awais and A. Iqbal, "Performance evaluation of OpenDaylight SDN controller," 2014 20th IEEE International Conference on Parallel and Distributed Systems (ICPADS), Hsinchu, Taiwan, 2014, pp. 671-676.
36. Z. Cai, F. Dinu, J. Zheng, A. L. Cox, and T. S. E. Ng. Maestro: A Clean-Slate System for Orchestrating Network Control Components. Under submission, 2008.
37. M. Casado, T. Garfinkel, M. Freedman, A. Akella, D. Boneh, N. McKeown, and S. Shenker. SANE: A Protection Architecture for Enterprise Networks. In Usenix Security Symposium, 2006.
38. M. Casado, M. J. Freedman, J. Pettit, J. Luo, N. McKeown, and S. Shenker. Ethane: Taking control of the enterprise. In SIGCOMM '07, 2007.
39. Shalimov, Alexander, Dmitry Zuikov, Daria Zimarina, Vasily Pashkov, and Ruslan Smeliansky. "Advanced study of SDN/OpenFlow controllers." In Proceedings of the 9th Central & Eastern European Software Engineering Conference in Russia, p. 1. ACM, 2013.
40. M. Betts, S. Fratini, N. Davis, R. Dolin and others, "SDN Architecture". Open Networking Foundation ONF SDN ARCH, Issue 1, June, 2014.
41. M. Joselli et al., "An Architeture with Automatic Load Balancing for Real-Time Simulation and Visualization Systems," Journal of Computational Interdisciplinary Sciences, vol. 1, no. 3, pp. 207–224, 2010.
42. N. McKeown, T. Anderson, H. Balakrishnan, G. Parulkar, L. Peterson, J. Rexford, S. Shenker, and J. Turner. Openflow: enabling innovation in campusnetworks. SIGCOMM Comput. Commun. Rev., 38(2):69–74, 2008.

Global Journal of Computer Science and Technology: E Network, Web & Security
Volume 19 Issue 1 Version 1.0 Year 2019
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

A Systematic Review of Security in Electronic Commerce- Threats and Frameworks

By N. Kuruwitaarachchi, P.K.W. Abeygunawardena, L.Rupasingha & S.W.I.Udara

Abstract- There is a remarkable scope for more streamlined living through an increase of e-platforms especially e-commerce, but this coincides with an increase in security concerns since the global market place is virtual and anonymous. Therefore, users have to trust the online providers blindly. To overcome this physiological barrier, the e-platforms should ensure utmost security. If not the e-commerce, industry is unable to perform in the market effectively. Thereby arises the need to carry out a systematic review of security issues in the e-commerce industry and to discover how different frameworks address these problems. This paper aims to identify the main security problems faced by both customers and vendors in E-commerce applications and general security management frameworks based on the key security areas are also presented.

Keywords: authentication; availability; B2C; E-commerce; frameworks; Integrity; non-repudiation; privacy; security; threats.

GJCST-E Classification: K.4.4

Strictly as per the compliance and regulations of:

A Systematic Review of Security in Electronic Commerce- Threats and Frameworks

N. Kuruwitaarachchi [α], P.K.W. Abeygunawardena [σ], L.Rupasingha [ρ], S.W.I.Udara [ω]

Abstract- **There is a remarkable scope for more streamlined living through an increase of e-platforms especially e-commerce, but this coincides with an increase in security concerns since the global market place is virtual and anonymous. Therefore, users have to trust the online providers blindly. To overcome this physiological barrier, the e-platforms should ensure utmost security. If not the e-commerce, industry is unable to perform in the market effectively. Thereby arises the need to carry out a systematic review of security issues in the e-commerce industry and to discover how different frameworks address these problems. This paper aims to identify the main security problems faced by both customers and vendors in E-commerce applications and general security management frameworks based on the key security areas are also presented.**

Keywords: authentication; availability; B2C; E-commerce; frameworks; integrity; non-repudiation; privacy; security; threats.

I. Introduction

In general E-commerce is referred as buying and selling products via electronic channels, primarily the Internet, the global market place. Thus, this is characterized by virtuality and anonymity and is considered an important development worldwide in the field of business, that changed the economies and commercial methods worldwide[1]. With the advantages including the high interaction, convenience, transparency and individualization, the internet makes online shopping increasingly popular among consumers[2]. The increasing profit, business continuity, reduced operational cost, improved storage management, customer service, and improved competitiveness makes e-commerce advantageous to businesses[3]. However, the use of such ubiquitous technology is not assuming apex of its success owing to the menace of security issues that have become a matter of great concern to the customers as well as to the online providers[4][5][6]. When the security is preserved properly, the essence of success in e-commerce can be inhaled, but if this is not successful, a considerable number of users will eventually refuse to use the platform due to lack of trust[4].The online vendors compete pull more and more customers to inflate their business and customers, on the other hand, are trying to ensure security before use of the online platform that their trust issue may not be at stake[4]. Thus to improve and to continue the e-commerce business the vendor organizations should be more specific on the security strategy. In this paper the aim is to explore the perception of security in business to consumer (B2C) e-commerce platforms from both customer and organizational point of view. This paper gives an overview of the dimensions of security, different security threats on e-commerce and the available frameworks to provide the necessary levels of security.

Author α σ ρ ω: Department of Information Systems Engineering Sri Lanka Institute of Technology Malabe, Sri Lanka.
e-mails: nuwan.ku@sliit.lk, pradeep.a@sliit.lk, lakmal.r@sliit.lk, isuriudara03@gmail.com

II. Literature Review

E-commerce connects customers and vendors over the internet as they conduct business interactions. Even though this can be incredibly convenient and productive, when utilized successfully there is a risk of security. Recent studies concluded that the primary factor hampering the success and further growth of e-commerce is the lack of security[2]. As the trend of online transactions continues to grow, there is an increase in the number and type of attacks against the safety[7]. E-commerce security has become more essential accelerate off the great developments achieved with growth in all fields of information technology. With the changing culture of the people on the concept of e-commerce and increased commercial transactions has emerged the greatest need for e-commerce security. E-commerce security is the protection of e-commerce assets from unauthorized access, use, alteration, or destruction[8]. The disadvantages comes in two different ways in E-commerce. One is the customer's risk of loss in financial information and service providers in monitory losses and bad publicity through that[8]. Thus, the state of being free from danger is, to be safe and to go about the business with minimal interruption. Hence, the importance of a secure platform cannot be overstated. The existence of a system's weakness may be exploited by an attack could cause the platform to enter an unsafe state [9].The three significant points of vulnerability in a transaction are the customer end, server side, and the communication channel. Thus, security is one of the principals and continuing concerns that restrict customers and vendor organizations engaging with e-commerce. E-commerce security is a part of the information security framework, which is explicitly applied to the components that affect e-commerce

interactions, which includes computer security, i.e., security from intrusion, viruses, worms, etc. Network security, i.e., to protect communication and all participants. Therefore, security is the combined technique of achieving robustness and fault tolerance by preventing known and distinct threats and quickly detecting and handling new threats.

a) Dimensions of Security

This research identified five main dimensions of security that needs to be preserved to bring about the desired security for e-commerce platforms.

i. *Privacy*

Privacy[4][5]is considered as a fundamental right of any consumer. It is the ability to control the terms under which different information is find and utilize.That is the control over the secondary use of information [8]. From the e-commerce point of view, information or data privacy and online privacy [1] is the privacy of personal information, financial information and usually considered how those information is stored on a information storage and used. Any act of copying or reading by an unauthorized party result in the loss of privacy.

ii. *Authentication*

Authentication [7] is the process of determining whether someone or something is in fact who or what it claims itself to be. Authentication technology provides access control for systems by checking to see if a user's credentials match the credentials in a database of authorized users or a data authentication server. In e-commerce, information and communication security is essential to ensure that the data, transactions, and documents are genuine and to validate that both parties involved are who they claim they are. This factor also guarantees that the particular user is the only one who is allowed to log in to the internet banking account.

iii. *Integrity*

Integrity can be defined as the dependability and trustworthiness of information. More specifically, it is the accuracy, consistency, and reliability of the information content, processes and systems. This means assuring that the data being accessed or read has neither been tampered with nor been altered or damaged, since the time of the last authorized access. Ine-commerce, integrity is particularly important for critical safety and financial information used for activities such as electronic fund transfers and financial accounting [7].

iv. *Non-Repudiation*

Non-repudiation means one's intention to fulfill their obligations to a contract [7]. It also means that one party of a transaction cannot deny having received a transaction nor can the other party deny having sent a transaction. So, this is a legal concept that is widely used in information security and refers to a service, which provides proof of the origin of data. Regarding e-commerce, it is to not reject a sale or a purchase.

v. *Availability*

Availability is the purpose of any information system to make information available whenever it is needed[7]. In this study it means that the computing systems used to store and process the information, the security controls and the communication channels used to access it must be functioning appropriately. E-commerce platforms are high availability systems aiming to remain available at all times, preventing all possible service disruptions. Therefore, prevention against data delays or removal and providing an uninterrupted service is focused.

III. E-Commerce Security Issues

The literature paved the way to identify four main security problems the e-commerce industry face based on three criteria; the e-platform, the owner, and it's users.

a) Transactional Security in E-Commerce

Transactional security in e-commerce refers to a secure non-fraudulent transfer of monetary value from the payer to the payee via electronic means, which links the exchanged data to some economic real world value. Securing the information available in the payment card is the major concern from a client perspective. Therefore, the transparency of the transaction should be maintained; financial information should not be stored after the transaction is completed and the information should not be revealed or sold to third parties[7]. Thereby if the online payment system is simple, hazardless, convenient and tightly secured, users will not feel hesitated in using the e-commerce platform. Thus, the three major players that need to be considered in an online transaction are the online seller, e-commerce page, and payer's perception[10]. Hence, the exchange nature requires confidentiality and the success of the operation hinges on the data transmission security. From the electronic business perspective, in order to survive the customer and vendor relationship should be built upon trust. There should not be any unease throughout the decision-making process and even beyond. Thereby, vendors, banks, and customers will collaborate with the electronic commerce platform without their inner fears.

b) Privacy in E-Commerce

In online transactions, clients are required to disclose a large number of private information to the vendor, which is associated with a high risk of confidential and cooperate sensitive information leakage. Clients have two kinds of privacy concerns[8]. First, they are concerned about the reuse of their data for unrelated purposes without their consent such as sharing with third parties. Second, consumers are

concerned over unauthorized access to personal data because of security breaches. Privacy is required to be looked into through social, organizational, technical and economical perspectives, as it is a legitimate right of the client[4]. It is evident that end users are very much concerned over unauthorized access to personal data and also about the reuse of their data by others without their permission[10]. Therefore, when deciding to provide private information, clients rely on their perceptions of trustworthiness irrespective of whether the vendor is a click only or motor business. Thus, consumer concern with the privacy of information is having an immense impact on the business to consumer e-commerce, and that for electronic commerce to reach its full potential. Ensuring control over secondary use of information will lead to an assurance of privacy in clients mind.

c) System Security in E-Commerce

System security arises mainly from the vendor's end and this discuss about the server, the availability and the database security. For an e-commerce platform to serve its purpose, the information must be available 24*7. This means that the systems used to store and process the information, the security controls used, and the communication channels used to access it must be functioning correctly. Availability attacks can create a delay, causing data to be held or otherwise made unavailable for a period. The attackers flood the network with useless traffic, make the system extremely slow to serve the customers, and in the extreme case, cause the system to crash down. E-commerce platforms store client personal data and retrieve product information from databases linked to the web-server. Database attackers change system resources or gain access to system information without authorization by either sharing logins or passwords or using an unattended terminal and alter, modify or disclose product information, consumer information and even valuable and private information that could irreparably damage the business[7].

d) Cyber Crime in E-Commerce

Cybercrime in e-commerce[8][5][11] is mainly computer as a target crime with the motive of intentionally causing financial loss, data breach or risking reputation directly or indirectly. Identity theft, fraud, virus attacks, spam, Trojan horses, worms, phishing and page jacking, can be considered popular crimes. Hackers break into e-commerce web servers to yield archives of transactional and personal information when a consumer makes an online purchase. Fraudulent practices steal, modify or use another person's personal information under pretense and thereby affect confidentiality and trust. Unusual unsolicited e-mail bombing aims a computer or network and send thousands of email messages. Viruses self-replicate and infect targeted computers triggered by an event[7]. Worms spread using direct internet connections, and Trojan Horses are disguised as legitimate software that trick users into running the program[7]. These attacks hinder the platform availability to consumers. Stealing content and placing it on another site with the hope of increasing site's search engine rankings, rerouting traffic from a vendor's e-commerce site and directing visitors to a different website with potential malicious material affects the e-commerce platforms risk of reputation and financial loss.

IV. Comparison of Frameworks

This section provides a review of four different security frameworks and summarizes the main contributions for each e-commerce security problem domain. The differentiating characteristics of each security framework is emphasized so that both clients and providers can distinguish which framework(s) suits their requirements for a successful, secure platform.

a) CISCO Security Framework

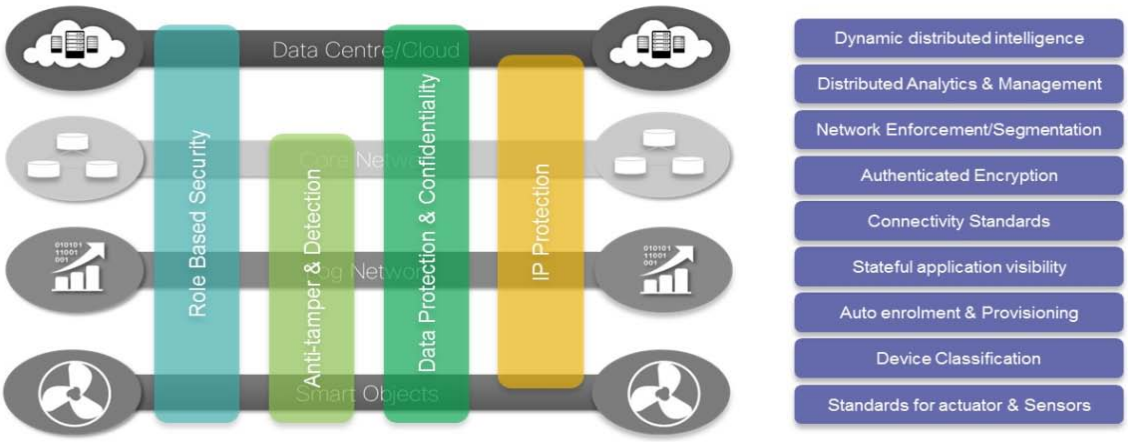


Figure 1: Cisco proposed model[12]

Figure 1 shows the Cisco proposed security framework, which can be the foundation for the execution of security. The authors have developed such a framework to be used in protocol and product development, in addition to, policy enforcement in operational environments that is suitable for both application and infrastructure. This framework review will mainly help to protect from physical attacks, such as DAR (data at rest protection) and Intrusion detection/prevention system (IDS/IPS)[13]. The above discussed e-commerce security concerns addressed in following frameworks.

Table I: CISCO framework support for the security threats

Security Threat	Concerns	Framework Support
Transactional Security	Information should not be revealed or sold to third parties	Anti-tamper and detection Role based access
	The exchange nature requires confidentiality	Data protection and security Role based access
	Success of the operation hinges on the data transmission security	Data protection and security Anti-tamper and detection
Privacy	Risk of confidential and cooperate sensitive information leakage	Data protection and security Anti-tamper and detection
	Reuse of their personal data for unrelated purposes without their consent	Anti-tamper and detection Role based access
	Unauthorized access to personal data because of security breaches	Data protection and security Role based access
System Security	Database threats	Data protection and security Role based access
Cyber Crime	Identity theft	Data protection and security
	Fraud	Data protection and security
	Virus attacks	Threat detection

b) Floodgate Security Framework

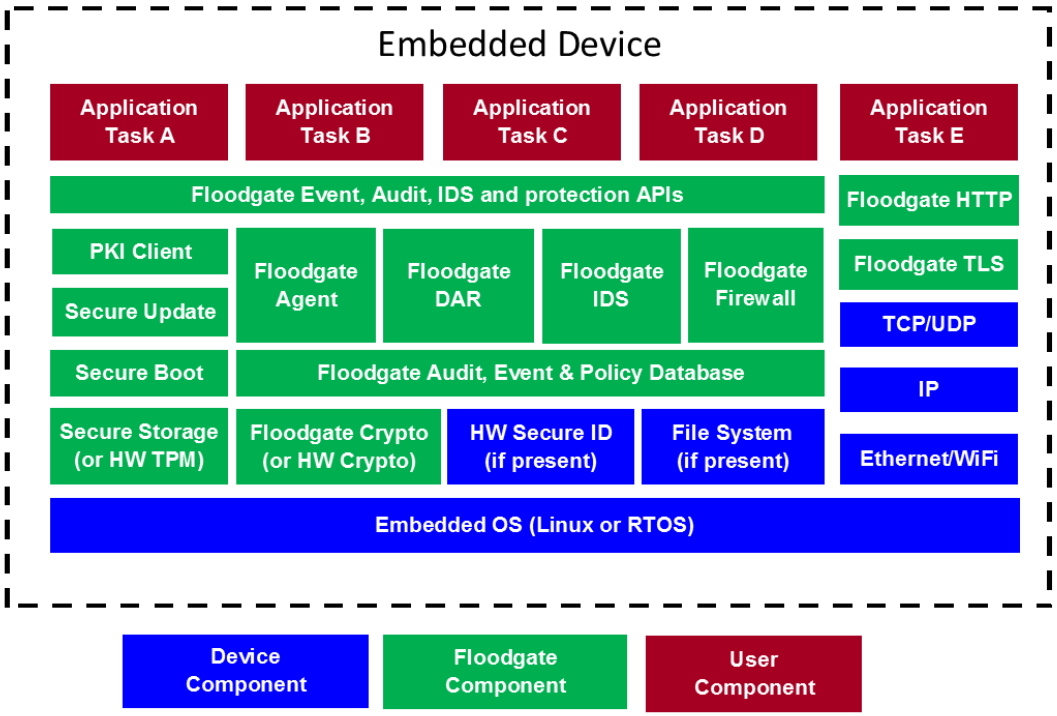


Figure 2: Floodgate Security framework[14]

Floodgate security framework mainly helps to securing against today's cyber threats. This helps to build secure, authenticated, trusted devices. Thus, this fits best for the infrastructure level security[13].

Table II: Floodgate framework support for the security threats

Security Threat	Concerns	Framework Support
Transactional Security	Information should not be revealed or sold to third parties	PKI Client
	The exchange nature requires confidentiality	PKI Client IDS module
	Success of the operation hinges on the data transmission security	PKI Client IDS module
Privacy	Reuse of their personal data for unrelated purposes without their consent	PKI Client IDS module
	Unauthorized access to personal data because of security breaches	PKI Client IDS module
System Security	Availability attacks	Firewall module
	Database threats	PKI Client IDS module
Cyber Crime	Identity theft	IDS module
	Fraud	IDS module
	Virus attacks	PKI Client IDS module
	Trojan horse	PKI Client IDS module
	Worms	Firewall module

c) Constrained Application Protocol Framework (CoAP)

This framework consists of various modules to handle security and trust issues. The CoAP works at application layers first and this framework best suit for the application security[13].

Table III: CoAP framework support for the security threats

Security Threat	Concerns	Framework Support
Transactional Security	Success of the operation hinges on the data transmission security	Packet protection
System Security	Availability attacks	Availability
Cyber Crime	Identity theft	Packet protection
	Virus attack	Duplicate detection
	Spam	Duplicate detection

d) Object Security Architecture Framework

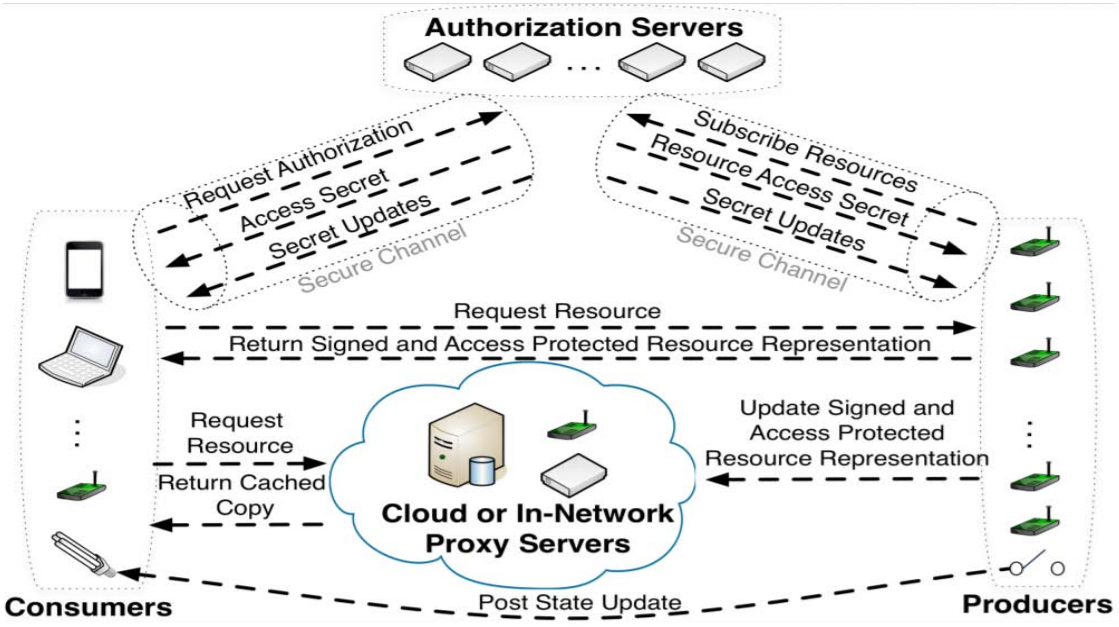


Figure 3: OSCAR Security Framework[15]

OSCAR security framework explores a novel approach to the problem of end-to-end security. This framework is based on the concept of object security that introduces security within the application payload[13]. This addresses confidentiality, authenticity, and privacy through capability-based access control.

Table IV: OSCAR framework support for the security threats

Security Threat	Concerns	Framework Support
Transactional Security	Information should not be revealed or sold to third parties	Authentication
	The exchange nature requires confidentiality	Confidentiality Authentication
	Success of the operation hinges on the data transmission security	Authentication
Privacy	Risk of confidential and cooperate sensitive information leakage	Confidentiality
	Reuse of their personal data for unrelated purposes without their consent	Confidentiality Authentication
	Unauthorized access to personal data because of security breaches	Confidentiality Authentication
System Security	Availability attacks	Availability
	Database threats	Authentication
Cyber Crime	Identity theft	Confidentiality Authentication
	Fraud	Confidentiality Authentication Integrity
	Virus attacks	Duplicate detection
	Spam	Duplicate detection
	Worms	Duplicate detection

V. Conclusion

Security in e-commerce is becoming more topical as the shift from traditional shopping and transactions move away from brick and mortar to click only business. E-commerce is rapidly growing in the global marketplace, and still, it comes with a risk that the transactions are compromised, which ultimately leads to a damaged reputation and financial loss. Therefore, the security of e-commerce transactions holds the criticality of the ongoing success as well as the growth of e-commerce. E-commerce security has five main dimensions- privacy, authentication, integrity, non-repudiation, and availability. The main security issues faced by both consumers and providers are transactional security, privacy, system security, and cyber crime. This research found insights that, a single framework capable of addressing these needs as a whole is not present yet and a unique security framework solely addressing e-commerce related security issues is not proposed so far. This research sheds light on the need of a distinct security framework to overcome the dark side of e-commerce.

References Références Referencias

1. Haya Alshehri, Farid Meziane, "The Influence of Advanced and Secure E-Commerce Environments on Customers Behaviour: The Case of Saudis in the UK," in 12th International Conference for Internet Technology and Secured Transactions, 2017.
2. Cong Cao, Jun Yan, Mengxiang Li, "The Effects of Consumer Perceived Different Service of Trusted Third Party on Trust Intention: An Empirical Study in Australia," in 14th IEEE International Conference on e-Business Engineering, 2017.
3. Puspa Indahati Sandhyaduhita, "Supporting and Inhibiting Factors of E-Commerce Adoption: Exploring the Sellers Side in Indonesia," in International Conference on Advanced Computer Science and Information Systems, 2016.
4. Sheshadri Chatterjee, "Security and Privacy Issues in E-Commerce: A Proposed Guidelines to Mitigate the Risk," in IEEE International Advance Computing Conference, 2015.
5. Revathi C, Shanthi K, Saranya A.R, "A Study on E-Commerce Security Issues," International Journal of Innovative Research in Computer and Communication Engineering, vol. 3, no. 12, December 2015.
6. Abdul Gaffar Khan, "Electronic Commerce: A Study on Benefits and Challeges in an Emerging Economy," Global Journal of Management and Business Research: B Economics and Commerce, vol. 16, no. 1, 2016
7. Dr. Mohammed Ali Hussain, "A Study of Information Security in E- Commerce Application," International Journal of Computer Engineering Science, vol. 3, no. 3, 2013.

8. Ms. Palak Gupta, Dr. Akshat Dubey, "E-Commerce-Study of Privacy, Trust and, Security from Consumer's Perspective" International Journal of Computer Science and Mobile Computing, vol. 5, no. 6, pp. 224-232, June 2016.
9. Xia Wang, Ke Zhang, Qingtian Wu, "A Design of Security Assessment System for E-commerce Website," in 8th International Symposium on Computational Intelligence and Design, 2015.
10. Ghada El Haddad, Esma Aimeur, Hicham Hage, "Understanding Trust, Privacy and Financial Fears in Online Payment," in 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications, 2018.
11. "Trends in e-commerce & digital fraud: Mitigating the risks," EKN, 2017.
12. "Securing the Internet of Things: A Proposed Framework", [Online]. Available: https://www.cisco.com/c/en/us/about/security-center/secure-iot-proposed-framework.html
13. Mohammad Irshad, "A Systematic Review of Information Security Frameworks in the Internet of Things," in IEEE 18th International Conference on High Performance Computing and Communications, 2016.
14. "Floodgate Security Framework", [Online]. Available: https://www.iconlabs.com/prod/product-family/floodgate-security-framework
15. "OSCAR: Object Security Architecture for the Internet of Things", [Online]. Available:https://drakkar.imag.fr/IMG/pdf/oscar-vucinic.pdf

Global Journals Guidelines Handbook 2019

www.GlobalJournals.org

FELLOW OF ASSOCIATION OF RESEARCH SOCIETY IN COMPUTING (FARSC)

Global Journals Incorporate (USA) is accredited by Open Association of Research Society (OARS), U.S.A and in turn, awards "FARSC" title to individuals. The 'FARSC' title is accorded to a selected professional after the approval of the Editor-in-Chief/Editorial Board Members/Dean.

- The "FARSC" is a dignified title which is accorded to a person's name viz. Dr. John E. Hall, Ph.D., FARSC or William Walldroff, M.S., FARSC.

FARSC accrediting is an honor. It authenticates your research activities. After recognition as FARSC, you can add 'FARSC' title with your name as you use this recognition as additional suffix to your status. This will definitely enhance and add more value and repute to your name. You may use it on your professional Counseling Materials such as CV, Resume, and Visiting Card etc.

The following benefits can be availed by you only for next three years from the date of certification:

FARSC designated members are entitled to avail a 40% discount while publishing their research papers (of a single author) with Global Journals Incorporation (USA), if the same is accepted by Editorial Board/Peer Reviewers. If you are a main author or co-author in case of multiple authors, you will be entitled to avail discount of 10%.

Once FARSC title is accorded, the Fellow is authorized to organize a symposium/seminar/conference on behalf of Global Journal Incorporation (USA).The Fellow can also participate in conference/seminar/symposium organized by another institution as representative of Global Journal. In both the cases, it is mandatory for him to discuss with us and obtain our consent.

You may join as member of the Editorial Board of Global Journals Incorporation (USA) after successful completion of three years as Fellow and as Peer Reviewer. In addition, it is also desirable that you should organize seminar/symposium/conference at least once.

We shall provide you intimation regarding launching of e-version of journal of your stream time to time. This may be utilized in your library for the enrichment of knowledge of your students as well as it can also be helpful for the concerned faculty members.

The FARSS can go through standards of OARS. You can also play vital role if you have any suggestions so that proper amendment can take place to improve the same for the benefit of entire research community.

As FARSS, you will be given a renowned, secure and free professional email address with 100 GB of space e.g. johnhall@globaljournals.org. This will include Webmail, Spam Assassin, Email Forwarders,Auto-Responders, Email Delivery Route tracing, etc.

The FARSS will be eligible for a free application of standardization of their researches. Standardization of research will be subject to acceptability within stipulated norms as the next step after publishing in a journal. We shall depute a team of specialized research professionals who will render their services for elevating your researches to next higher level, which is worldwide open standardization.

The FARSS member can apply for grading and certification of standards of their educational and Institutional Degrees to Open Association of Research, Society U.S.A.
Once you are designated as FARSS, you may send us a scanned copy of all of your credentials. OARS will verify, grade and certify them. This will be based on your academic records, quality of research papers published by you, and some more criteria. After certification of all your credentials by OARS, they will be published on your Fellow Profile link on website https://associationofresearch.org which will be helpful to upgrade the dignity.

The FARSS members can avail the benefits of free research podcasting in Global Research Radio with their research documents. After publishing the work, (including published elsewhere worldwide with proper authorization) you can upload your research paper with your recorded voice or you can utilize chargeable services of our professional RJs to record your paper in their voice on request.

The FARSS member also entitled to get the benefits of free research podcasting of their research documents through video clips. We can also streamline your conference videos and display your slides/ online slides and online research video clips at reasonable charges, on request.

The FARSS is eligible to earn from sales proceeds of his/her researches/reference/review Books or literature, while publishing with Global Journals. The FARSS can decide whether he/she would like to publish his/her research in a closed manner. In this case, whenever readers purchase that individual research paper for reading, maximum 60% of its profit earned as royalty by Global Journals, will be credited to his/her bank account. The entire entitled amount will be credited to his/her bank account exceeding limit of minimum fixed balance. There is no minimum time limit for collection. The FARSS member can decide its price and we can help in making the right decision.

The FARSS member is eligible to join as a paid peer reviewer at Global Journals Incorporation (USA) and can get remuneration of 15% of author fees, taken from the author of a respective paper. After reviewing 5 or more papers you can request to transfer the amount to your bank account.

MEMBER OF ASSOCIATION OF RESEARCH SOCIETY IN SCIENCE (MARSS)

The ' MARSS ' title is accorded to a selected professional after the approval of the Editor-in-Chief / Editorial Board Members/Dean.

The “MARSS” is a dignified ornament which is accorded to a person’s name viz. Dr. John E. Hall, Ph.D., MARSS or William Walldroff, M.S., MARSS.

MARSS accrediting is an honor. It authenticates your research activities. After becoming MARSS, you can add 'MARSS' title with your name as you use this recognition as additional suffix to your status. This will definitely enhance and add more value and repute to your name. You may use it on your professional Counseling Materials such as CV, Resume, Visiting Card and Name Plate etc.

The following benefitscan be availed by you only for next three years from the date of certification.

MARSS designated members are entitled to avail a 25% discount while publishing their research papers (of a single author) in Global Journals Inc., if the same is accepted by our Editorial Board and Peer Reviewers. If you are a main author or co-author of a group of authors, you will get discount of 10%.

As MARSS, you will be given a renowned, secure and free professional email address with 30 GB of space e.g. johnhall@globaljournals.org. This will include Webmail, Spam Assassin, Email Forwarders,Auto-Responders, Email Delivery Route tracing, etc.

We shall provide you intimation regarding launching of e-version of journal of your stream time to time. This may be utilized in your library for the enrichment of knowledge of your students as well as it can also be helpful for the concerned faculty members.

The MARSC member can apply for approval, grading and certification of standards of their educational and Institutional Degrees to Open Association of Research, Society U.S.A.

Once you are designated as MARSC, you may send us a scanned copy of all of your credentials. OARS will verify, grade and certify them. This will be based on your academic records, quality of research papers published by you, and some more criteria.

It is mandatory to read all terms and conditions carefully.

Auxiliary Memberships

Institutional Fellow of Open Association of Research Society (USA)-OARS (USA)

Global Journals Incorporation (USA) is accredited by Open Association of Research Society, U.S.A (OARS) and in turn, affiliates research institutions as "Institutional Fellow of Open Association of Research Society" (IFOARS).

The "FARSC" is a dignified title which is accorded to a person's name viz. Dr. John E. Hall, Ph.D., FARSC or William Walldroff, M.S., FARSC.

The IFOARS institution is entitled to form a Board comprised of one Chairperson and three to five board members preferably from different streams. The Board will be recognized as "Institutional Board of Open Association of Research Society"-(IBOARS).

The Institute will be entitled to following benefits:

The IBOARS can initially review research papers of their institute and recommend them to publish with respective journal of Global Journals. It can also review the papers of other institutions after obtaining our consent. The second review will be done by peer reviewer of Global Journals Incorporation (USA) The Board is at liberty to appoint a peer reviewer with the approval of chairperson after consulting us.

The author fees of such paper may be waived off up to 40%.

The Global Journals Incorporation (USA) at its discretion can also refer double blind peer reviewed paper at their end to the board for the verification and to get recommendation for final stage of acceptance of publication.

The IBOARS can organize symposium/seminar/conference in their country on behalf of Global Journals Incorporation (USA)-OARS (USA). The terms and conditions can be discussed separately.

The Board can also play vital role by exploring and giving valuable suggestions regarding the Standards of "Open Association of Research Society, U.S.A (OARS)" so that proper amendment can take place for the benefit of entire research community. We shall provide details of particular standard only on receipt of request from the Board.

The board members can also join us as Individual Fellow with 40% discount on total fees applicable to Individual Fellow. They will be entitled to avail all the benefits as declared. Please visit Individual Fellow-sub menu of GlobalJournals.org to have more relevant details.

We shall provide you intimation regarding launching of e-version of journal of your stream time to time. This may be utilized in your library for the enrichment of knowledge of your students as well as it can also be helpful for the concerned faculty members.

After nomination of your institution as "Institutional Fellow" and constantly functioning successfully for one year, we can consider giving recognition to your institute to function as Regional/Zonal office on our behalf.
The board can also take up the additional allied activities for betterment after our consultation.

The following entitlements are applicable to individual Fellows:

Open Association of Research Society, U.S.A (OARS) By-laws states that an individual Fellow may use the designations as applicable, or the corresponding initials. The Credentials of individual Fellow and Associate designations signify that the individual has gained knowledge of the fundamental concepts. One is magnanimous and proficient in an expertise course covering the professional code of conduct, and follows recognized standards of practice.

Open Association of Research Society (US)/ Global Journals Incorporation (USA), as described in Corporate Statements, are educational, research publishing and professional membership organizations. Achieving our individual Fellow or Associate status is based mainly on meeting stated educational research requirements.

Disbursement of 40% Royalty earned through Global Journals : Researcher = 50%, Peer Reviewer = 37.50%, Institution = 12.50% E.g. Out of 40%, the 20% benefit should be passed on to researcher, 15 % benefit towards remuneration should be given to a reviewer and remaining 5% is to be retained by the institution.

We shall provide print version of 12 issues of any three journals [as per your requirement] out of our 38 journals worth $ 2376 USD.

Other:

The individual Fellow and Associate designations accredited by Open Association of Research Society (US) credentials signify guarantees following achievements:

- The professional accredited with Fellow honor, is entitled to various benefits viz. name, fame, honor, regular flow of income, secured bright future, social status etc.

- In addition to above, if one is single author, then entitled to 40% discount on publishing research paper and can get 10%discount if one is co-author or main author among group of authors.
- The Fellow can organize symposium/seminar/conference on behalf of Global Journals Incorporation (USA) and he/she can also attend the same organized by other institutes on behalf of Global Journals.
- The Fellow can become member of Editorial Board Member after completing 3yrs.
- The Fellow can earn 60% of sales proceeds from the sale of reference/review books/literature/publishing of research paper.
- Fellow can also join as paid peer reviewer and earn 15% remuneration of author charges and can also get an opportunity to join as member of the Editorial Board of Global Journals Incorporation (USA)
- • This individual has learned the basic methods of applying those concepts and techniques to common challenging situations. This individual has further demonstrated an in–depth understanding of the application of suitable techniques to a particular area of research practice.

Note :

"

- In future, if the board feels the necessity to change any board member, the same can be done with the consent of the chairperson along with anyone board member without our approval.
- In case, the chairperson needs to be replaced then consent of 2/3rd board members are required and they are also required to jointly pass the resolution copy of which should be sent to us. In such case, it will be compulsory to obtain our approval before replacement.
- In case of "Difference of Opinion [if any]" among the Board members, our decision will be final and binding to everyone.

"

Preferred Author Guidelines

We accept the manuscript submissions in any standard (generic) format.

We typeset manuscripts using advanced typesetting tools like Adobe In Design, CorelDraw, TeXnicCenter, and TeXStudio. We usually recommend authors submit their research using any standard format they are comfortable with, and let Global Journals do the rest.

Alternatively, you can download our basic template from https://globaljournals.org/Template.zip

Authors should submit their complete paper/article, including text illustrations, graphics, conclusions, artwork, and tables. Authors who are not able to submit manuscript using the form above can email the manuscript department at submit@globaljournals.org or get in touch with chiefeditor@globaljournals.org if they wish to send the abstract before submission.

Before and during Submission

Authors must ensure the information provided during the submission of a paper is authentic. Please go through the following checklist before submitting:

1. Authors must go through the complete author guideline and understand and *agree to Global Journals' ethics and code of conduct,* along with author responsibilities.
2. Authors must accept the privacy policy, terms, and conditions of Global Journals.
3. Ensure corresponding author's email address and postal address are accurate and reachable.
4. Manuscript to be submitted must include keywords, an abstract, a paper title, co-author(s') names and details (email address, name, phone number, and institution), figures and illustrations in vector format including appropriate captions, tables, including titles and footnotes, a conclusion, results, acknowledgments and references.
5. Authors should submit paper in a ZIP archive if any supplementary files are required along with the paper.
6. Proper permissions must be acquired for the use of any copyrighted material.
7. Manuscript submitted *must not have been submitted or published elsewhere* and all authors must be aware of the submission.

Declaration of Conflicts of Interest

It is required for authors to declare all financial, institutional, and personal relationships with other individuals and organizations that could influence (bias) their research.

Policy on Plagiarism

Plagiarism is not acceptable in Global Journals submissions at all.

Plagiarized content will not be considered for publication. We reserve the right to inform authors' institutions about plagiarism detected either before or after publication. If plagiarism is identified, we will follow COPE guidelines:

Authors are solely responsible for all the plagiarism that is found. The author must not fabricate, falsify or plagiarize existing research data. The following, if copied, will be considered plagiarism:

- Words (language)
- Ideas
- Findings
- Writings
- Diagrams
- Graphs
- Illustrations
- Lectures

- Printed material
- Graphic representations
- Computer programs
- Electronic material
- Any other original work

Authorship Policies

Global Journals follows the definition of authorship set up by the Open Association of Research Society, USA. According to its guidelines, authorship criteria must be based on:

1. Substantial contributions to the conception and acquisition of data, analysis, and interpretation of findings.
2. Drafting the paper and revising it critically regarding important academic content.
3. Final approval of the version of the paper to be published.

Changes in Authorship

The corresponding author should mention the name and complete details of all co-authors during submission and in manuscript. We support addition, rearrangement, manipulation, and deletions in authors list till the early view publication of the journal. We expect that corresponding author will notify all co-authors of submission. We follow COPE guidelines for changes in authorship.

Copyright

During submission of the manuscript, the author is confirming an exclusive license agreement with Global Journals which gives Global Journals the authority to reproduce, reuse, and republish authors' research. We also believe in flexible copyright terms where copyright may remain with authors/employers/institutions as well. Contact your editor after acceptance to choose your copyright policy. You may follow this form for copyright transfers.

Appealing Decisions

Unless specified in the notification, the Editorial Board's decision on publication of the paper is final and cannot be appealed before making the major change in the manuscript.

Acknowledgments

Contributors to the research other than authors credited should be mentioned in Acknowledgments. The source of funding for the research can be included. Suppliers of resources may be mentioned along with their addresses.

Declaration of funding sources

Global Journals is in partnership with various universities, laboratories, and other institutions worldwide in the research domain. Authors are requested to disclose their source of funding during every stage of their research, such as making analysis, performing laboratory operations, computing data, and using institutional resources, from writing an article to its submission. This will also help authors to get reimbursements by requesting an open access publication letter from Global Journals and submitting to the respective funding source.

Preparing your Manuscript

Authors can submit papers and articles in an acceptable file format: MS Word (doc, docx), LaTeX (.tex, .zip or .rar including all of your files), Adobe PDF (.pdf), rich text format (.rtf), simple text document (.txt), Open Document Text (.odt), and Apple Pages (.pages). Our professional layout editors will format the entire paper according to our official guidelines. This is one of the highlights of publishing with Global Journals—authors should not be concerned about the formatting of their paper. Global Journals accepts articles and manuscripts in every major language, be it Spanish, Chinese, Japanese, Portuguese, Russian, French, German, Dutch, Italian, Greek, or any other national language, but the title, subtitle, and abstract should be in English. This will facilitate indexing and the pre-peer review process.

The following is the official style and template developed for publication of a research paper. Authors are not required to follow this style during the submission of the paper. It is just for reference purposes.

Manuscript Style Instruction (Optional)

- Microsoft Word Document Setting Instructions.
- Font type of all text should be Swis721 Lt BT.
- Page size: 8.27" x 11'", left margin: 0.65, right margin: 0.65, bottom margin: 0.75.
- Paper title should be in one column of font size 24.
- Author name in font size of 11 in one column.
- Abstract: font size 9 with the word "Abstract" in bold italics.
- Main text: font size 10 with two justified columns.
- Two columns with equal column width of 3.38 and spacing of 0.2.
- First character must be three lines drop-capped.
- The paragraph before spacing of 1 pt and after of 0 pt.
- Line spacing of 1 pt.
- Large images must be in one column.
- The names of first main headings (Heading 1) must be in Roman font, capital letters, and font size of 10.
- The names of second main headings (Heading 2) must not include numbers and must be in italics with a font size of 10.

Structure and Format of Manuscript

The recommended size of an original research paper is under 15,000 words and review papers under 7,000 words. Research articles should be less than 10,000 words. Research papers are usually longer than review papers. Review papers are reports of significant research (typically less than 7,000 words, including tables, figures, and references)

A research paper must include:

a) A title which should be relevant to the theme of the paper.
b) A summary, known as an abstract (less than 150 words), containing the major results and conclusions.
c) Up to 10 keywords that precisely identify the paper's subject, purpose, and focus.
d) An introduction, giving fundamental background objectives.
e) Resources and techniques with sufficient complete experimental details (wherever possible by reference) to permit repetition, sources of information must be given, and numerical methods must be specified by reference.
f) Results which should be presented concisely by well-designed tables and figures.
g) Suitable statistical data should also be given.
h) All data must have been gathered with attention to numerical detail in the planning stage.

Design has been recognized to be essential to experiments for a considerable time, and the editor has decided that any paper that appears not to have adequate numerical treatments of the data will be returned unrefereed.

i) Discussion should cover implications and consequences and not just recapitulate the results; conclusions should also be summarized.
j) There should be brief acknowledgments.
k) There ought to be references in the conventional format. Global Journals recommends APA format.

Authors should carefully consider the preparation of papers to ensure that they communicate effectively. Papers are much more likely to be accepted if they are carefully designed and laid out, contain few or no errors, are summarizing, and follow instructions. They will also be published with much fewer delays than those that require much technical and editorial correction.

The Editorial Board reserves the right to make literary corrections and suggestions to improve brevity.

Format Structure

It is necessary that authors take care in submitting a manuscript that is written in simple language and adheres to published guidelines.

All manuscripts submitted to Global Journals should include:

Title

The title page must carry an informative title that reflects the content, a running title (less than 45 characters together with spaces), names of the authors and co-authors, and the place(s) where the work was carried out.

Author details

The full postal address of any related author(s) must be specified.

Abstract

The abstract is the foundation of the research paper. It should be clear and concise and must contain the objective of the paper and inferences drawn. It is advised to not include big mathematical equations or complicated jargon.

Many researchers searching for information online will use search engines such as Google, Yahoo or others. By optimizing your paper for search engines, you will amplify the chance of someone finding it. In turn, this will make it more likely to be viewed and cited in further works. Global Journals has compiled these guidelines to facilitate you to maximize the web-friendliness of the most public part of your paper.

Keywords

A major lynchpin of research work for the writing of research papers is the keyword search, which one will employ to find both library and internet resources. Up to eleven keywords or very brief phrases have to be given to help data retrieval, mining, and indexing.

One must be persistent and creative in using keywords. An effective keyword search requires a strategy: planning of a list of possible keywords and phrases to try.

Choice of the main keywords is the first tool of writing a research paper. Research paper writing is an art. Keyword search should be as strategic as possible.

One should start brainstorming lists of potential keywords before even beginning searching. Think about the most important concepts related to research work. Ask, “What words would a source have to include to be truly valuable in a research paper?” Then consider synonyms for the important words.

It may take the discovery of only one important paper to steer in the right keyword direction because, in most databases, the keywords under which a research paper is abstracted are listed with the paper.

Numerical Methods

Numerical methods used should be transparent and, where appropriate, supported by references.

Abbreviations

Authors must list all the abbreviations used in the paper at the end of the paper or in a separate table before using them.

Formulas and equations

Authors are advised to submit any mathematical equation using either MathJax, KaTeX, or LaTeX, or in a very high-quality image.

Tables, Figures, and Figure Legends

Tables: Tables should be cautiously designed, uncrowned, and include only essential data. Each must have an Arabic number, e.g., Table 4, a self-explanatory caption, and be on a separate sheet. Authors must submit tables in an editable format and not as images. References to these tables (if any) must be mentioned accurately.

Figures

Figures are supposed to be submitted as separate files. Always include a citation in the text for each figure using Arabic numbers, e.g., Fig. 4. Artwork must be submitted online in vector electronic form or by emailing it.

Preparation of Eletronic Figures for Publication

Although low-quality images are sufficient for review purposes, print publication requires high-quality images to prevent the final product being blurred or fuzzy. Submit (possibly by e-mail) EPS (line art) or TIFF (halftone/ photographs) files only. MS PowerPoint and Word Graphics are unsuitable for printed pictures. Avoid using pixel-oriented software. Scans (TIFF only) should have a resolution of at least 350 dpi (halftone) or 700 to 1100 dpi (line drawings). Please give the data for figures in black and white or submit a Color Work Agreement form. EPS files must be saved with fonts embedded (and with a TIFF preview, if possible).

For scanned images, the scanning resolution at final image size ought to be as follows to ensure good reproduction: line art: >650 dpi; halftones (including gel photographs): >350 dpi; figures containing both halftone and line images: >650 dpi.

Color charges: Authors are advised to pay the full cost for the reproduction of their color artwork. Hence, please note that if there is color artwork in your manuscript when it is accepted for publication, we would require you to complete and return a Color Work Agreement form before your paper can be published. Also, you can email your editor to remove the color fee after acceptance of the paper.

Tips for writing a good quality Computer Science Research Paper

Techniques for writing a good quality computer science research paper:

1. Choosing the topic: In most cases, the topic is selected by the interests of the author, but it can also be suggested by the guides. You can have several topics, and then judge which you are most comfortable with. This may be done by asking several questions of yourself, like "Will I be able to carry out a search in this area? Will I find all necessary resources to accomplish the search? Will I be able to find all information in this field area?" If the answer to this type of question is "yes," then you ought to choose that topic. In most cases, you may have to conduct surveys and visit several places. Also, you might have to do a lot of work to find all the rises and falls of the various data on that subject. Sometimes, detailed information plays a vital role, instead of short information. Evaluators are human: The first thing to remember is that evaluators are also human beings. They are not only meant for rejecting a paper. They are here to evaluate your paper. So present your best aspect.

2. Think like evaluators: If you are in confusion or getting demotivated because your paper may not be accepted by the evaluators, then think, and try to evaluate your paper like an evaluator. Try to understand what an evaluator wants in your research paper, and you will automatically have your answer. Make blueprints of paper: The outline is the plan or framework that will help you to arrange your thoughts. It will make your paper logical. But remember that all points of your outline must be related to the topic you have chosen.

3. Ask your guides: If you are having any difficulty with your research, then do not hesitate to share your difficulty with your guide (if you have one). They will surely help you out and resolve your doubts. If you can't clarify what exactly you require for your work, then ask your supervisor to help you with an alternative. He or she might also provide you with a list of essential readings.

4. Use of computer is recommended: As you are doing research in the field of computer science then this point is quite obvious. Use right software: Always use good quality software packages. If you are not capable of judging good software, then you can lose the quality of your paper unknowingly. There are various programs available to help you which you can get through the internet.

5. Use the internet for help: An excellent start for your paper is using Google. It is a wondrous search engine, where you can have your doubts resolved. You may also read some answers for the frequent question of how to write your research paper or find a model research paper. You can download books from the internet. If you have all the required books, place importance on reading, selecting, and analyzing the specified information. Then sketch out your research paper. Use big pictures: You may use encyclopedias like Wikipedia to get pictures with the best resolution. At Global Journals, you should strictly follow here.

6. Bookmarks are useful: When you read any book or magazine, you generally use bookmarks, right? It is a good habit which helps to not lose your continuity. You should always use bookmarks while searching on the internet also, which will make your search easier.

7. Revise what you wrote: When you write anything, always read it, summarize it, and then finalize it.

8. Make every effort: Make every effort to mention what you are going to write in your paper. That means always have a good start. Try to mention everything in the introduction—what is the need for a particular research paper. Polish your work with good writing skills and always give an evaluator what he wants. Make backups: When you are going to do any important thing like making a research paper, you should always have backup copies of it either on your computer or on paper. This protects you from losing any portion of your important data.

9. Produce good diagrams of your own: Always try to include good charts or diagrams in your paper to improve quality. Using several unnecessary diagrams will degrade the quality of your paper by creating a hodgepodge. So always try to include diagrams which were made by you to improve the readability of your paper. Use of direct quotes: When you do research relevant to literature, history, or current affairs, then use of quotes becomes essential, but if the study is relevant to science, use of quotes is not preferable.

10.Use proper verb tense: Use proper verb tenses in your paper. Use past tense to present those events that have happened. Use present tense to indicate events that are going on. Use future tense to indicate events that will happen in the future. Use of wrong tenses will confuse the evaluator. Avoid sentences that are incomplete.

11. Pick a good study spot: Always try to pick a spot for your research which is quiet. Not every spot is good for studying.

12. Know what you know: Always try to know what you know by making objectives, otherwise you will be confused and unable to achieve your target.

13. Use good grammar: Always use good grammar and words that will have a positive impact on the evaluator; use of good vocabulary does not mean using tough words which the evaluator has to find in a dictionary. Do not fragment sentences. Eliminate one-word sentences. Do not ever use a big word when a smaller one would suffice.

Verbs have to be in agreement with their subjects. In a research paper, do not start sentences with conjunctions or finish them with prepositions. When writing formally, it is advisable to never split an infinitive because someone will (wrongly) complain. Avoid clichés like a disease. Always shun irritating alliteration. Use language which is simple and straightforward. Put together a neat summary.

14. Arrangement of information: Each section of the main body should start with an opening sentence, and there should be a changeover at the end of the section. Give only valid and powerful arguments for your topic. You may also maintain your arguments with records.

15. Never start at the last minute: Always allow enough time for research work. Leaving everything to the last minute will degrade your paper and spoil your work.

16. Multitasking in research is not good: Doing several things at the same time is a bad habit in the case of research activity. Research is an area where everything has a particular time slot. Divide your research work into parts, and do a particular part in a particular time slot.

17. Never copy others' work: Never copy others' work and give it your name because if the evaluator has seen it anywhere, you will be in trouble. Take proper rest and food: No matter how many hours you spend on your research activity, if you are not taking care of your health, then all your efforts will have been in vain. For quality research, take proper rest and food.

18. Go to seminars: Attend seminars if the topic is relevant to your research area. Utilize all your resources.

19. Refresh your mind after intervals: Try to give your mind a rest by listening to soft music or sleeping in intervals. This will also improve your memory. Acquire colleagues: Always try to acquire colleagues. No matter how sharp you are, if you acquire colleagues, they can give you ideas which will be helpful to your research.

20. Think technically: Always think technically. If anything happens, search for its reasons, benefits, and demerits. Think and then print: When you go to print your paper, check that tables are not split, headings are not detached from their descriptions, and page sequence is maintained.

21. Adding unnecessary information: Do not add unnecessary information like "I have used MS Excel to draw graphs." Irrelevant and inappropriate material is superfluous. Foreign terminology and phrases are not apropos. One should never take a broad view. Analogy is like feathers on a snake. Use words properly, regardless of how others use them. Remove quotations. Puns are for kids, not grunt readers. Never oversimplify: When adding material to your research paper, never go for oversimplification; this will definitely irritate the evaluator. Be specific. Never use rhythmic redundancies. Contractions shouldn't be used in a research paper. Comparisons are as terrible as clichés. Give up ampersands, abbreviations, and so on. Remove commas that are not necessary. Parenthetical words should be between brackets or commas. Understatement is always the best way to put forward earth-shaking thoughts. Give a detailed literary review.

22. Report concluded results: Use concluded results. From raw data, filter the results, and then conclude your studies based on measurements and observations taken. An appropriate number of decimal places should be used. Parenthetical remarks are prohibited here. Proofread carefully at the final stage. At the end, give an outline to your arguments. Spot perspectives of further study of the subject. Justify your conclusion at the bottom sufficiently, which will probably include examples.

23. Upon conclusion: Once you have concluded your research, the next most important step is to present your findings. Presentation is extremely important as it is the definite medium though which your research is going to be in print for the rest of the crowd. Care should be taken to categorize your thoughts well and present them in a logical and neat manner. A good quality research paper format is essential because it serves to highlight your research paper and bring to light all necessary aspects of your research.

Informal Guidelines of Research Paper Writing

Key points to remember:

- Submit all work in its final form.
- Write your paper in the form which is presented in the guidelines using the template.
- Please note the criteria peer reviewers will use for grading the final paper.

Final points:

One purpose of organizing a research paper is to let people interpret your efforts selectively. The journal requires the following sections, submitted in the order listed, with each section starting on a new page:

The introduction: This will be compiled from reference matter and reflect the design processes or outline of basis that directed you to make a study. As you carry out the process of study, the method and process section will be constructed like that. The results segment will show related statistics in nearly sequential order and direct reviewers to similar intellectual paths throughout the data that you gathered to carry out your study.

The discussion section:

This will provide understanding of the data and projections as to the implications of the results. The use of good quality references throughout the paper will give the effort trustworthiness by representing an alertness to prior workings.

Writing a research paper is not an easy job, no matter how trouble-free the actual research or concept. Practice, excellent preparation, and controlled record-keeping are the only means to make straightforward progression.

General style:

Specific editorial column necessities for compliance of a manuscript will always take over from directions in these general guidelines.

To make a paper clear: Adhere to recommended page limits.

Mistakes to avoid:

- Insertion of a title at the foot of a page with subsequent text on the next page.
- Separating a table, chart, or figure—confine each to a single page.
- Submitting a manuscript with pages out of sequence.
- In every section of your document, use standard writing style, including articles ("a" and "the").
- Keep paying attention to the topic of the paper.
- Use paragraphs to split each significant point (excluding the abstract).
- Align the primary line of each section.
- Present your points in sound order.
- Use present tense to report well-accepted matters.
- Use past tense to describe specific results.
- Do not use familiar wording; don't address the reviewer directly. Don't use slang or superlatives.
- Avoid use of extra pictures—include only those figures essential to presenting results.

Title page:

Choose a revealing title. It should be short and include the name(s) and address(es) of all authors. It should not have acronyms or abbreviations or exceed two printed lines.

Abstract: This summary should be two hundred words or less. It should clearly and briefly explain the key findings reported in the manuscript and must have precise statistics. It should not have acronyms or abbreviations. It should be logical in itself. Do not cite references at this point.

An abstract is a brief, distinct paragraph summary of finished work or work in development. In a minute or less, a reviewer can be taught the foundation behind the study, common approaches to the problem, relevant results, and significant conclusions or new questions.

Write your summary when your paper is completed because how can you write the summary of anything which is not yet written? Wealth of terminology is very essential in abstract. Use comprehensive sentences, and do not sacrifice readability for brevity; you can maintain it succinctly by phrasing sentences so that they provide more than a lone rationale. The author can at this moment go straight to shortening the outcome. Sum up the study with the subsequent elements in any summary. Try to limit the initial two items to no more than one line each.

Reason for writing the article—theory, overall issue, purpose.

- Fundamental goal.
- To-the-point depiction of the research.
- Consequences, including definite statistics—if the consequences are quantitative in nature, account for this; results of any numerical analysis should be reported. Significant conclusions or questions that emerge from the research.

Approach:

- Single section and succinct.
- An outline of the job done is always written in past tense.
- Concentrate on shortening results—limit background information to a verdict or two.
- Exact spelling, clarity of sentences and phrases, and appropriate reporting of quantities (proper units, important statistics) are just as significant in an abstract as they are anywhere else.

Introduction:

The introduction should "introduce" the manuscript. The reviewer should be presented with sufficient background information to be capable of comprehending and calculating the purpose of your study without having to refer to other works. The basis for the study should be offered. Give the most important references, but avoid making a comprehensive appraisal of the topic. Describe the problem visibly. If the problem is not acknowledged in a logical, reasonable way, the reviewer will give no attention to your results. Speak in common terms about techniques used to explain the problem, if needed, but do not present any particulars about the protocols here.

The following approach can create a valuable beginning:

- Explain the value (significance) of the study.
- Defend the model—why did you employ this particular system or method? What is its compensation? Remark upon its appropriateness from an abstract point of view as well as pointing out sensible reasons for using it.
- Present a justification. State your particular theory(-ies) or aim(s), and describe the logic that led you to choose them.
- Briefly explain the study's tentative purpose and how it meets the declared objectives.

Approach:

Use past tense except for when referring to recognized facts. After all, the manuscript will be submitted after the entire job is done. Sort out your thoughts; manufacture one key point for every section. If you make the four points listed above, you will need at least four paragraphs. Present surrounding information only when it is necessary to support a situation. The reviewer does not desire to read everything you know about a topic. Shape the theory specifically—do not take a broad view.

As always, give awareness to spelling, simplicity, and correctness of sentences and phrases.

Procedures (methods and materials):

This part is supposed to be the easiest to carve if you have good skills. A soundly written procedures segment allows a capable scientist to replicate your results. Present precise information about your supplies. The suppliers and clarity of reagents can be helpful bits of information. Present methods in sequential order, but linked methodologies can be grouped as a segment. Be concise when relating the protocols. Attempt to give the least amount of information that would permit another capable scientist to replicate your outcome, but be cautious that vital information is integrated. The use of subheadings is suggested and ought to be synchronized with the results section.

When a technique is used that has been well-described in another section, mention the specific item describing the way, but draw the basic principle while stating the situation. The purpose is to show all particular resources and broad procedures so that another person may use some or all of the methods in one more study or referee the scientific value of your work. It is not to be a step-by-step report of the whole thing you did, nor is a methods section a set of orders.

Materials:

Materials may be reported in part of a section or else they may be recognized along with your measures.

Methods:

- Report the method and not the particulars of each process that engaged the same methodology.
- Describe the method entirely.
- To be succinct, present methods under headings dedicated to specific dealings or groups of measures.
- Simplify—detail how procedures were completed, not how they were performed on a particular day.
- If well-known procedures were used, account for the procedure by name, possibly with a reference, and that's all.

Approach:

It is embarrassing to use vigorous voice when documenting methods without using first person, which would focus the reviewer's interest on the researcher rather than the job. As a result, when writing up the methods, most authors use third person passive voice.

Use standard style in this and every other part of the paper—avoid familiar lists, and use full sentences.

What to keep away from:

- Resources and methods are not a set of information.
- Skip all descriptive information and surroundings—save it for the argument.
- Leave out information that is immaterial to a third party.

Results:

The principle of a results segment is to present and demonstrate your conclusion. Create this part as entirely objective details of the outcome, and save all understanding for the discussion.

The page length of this segment is set by the sum and types of data to be reported. Use statistics and tables, if suitable, to present consequences most efficiently.

You must clearly differentiate material which would usually be incorporated in a study editorial from any unprocessed data or additional appendix matter that would not be available. In fact, such matters should not be submitted at all except if requested by the instructor.

Content:

- Sum up your conclusions in text and demonstrate them, if suitable, with figures and tables.
- In the manuscript, explain each of your consequences, and point the reader to remarks that are most appropriate.
- Present a background, such as by describing the question that was addressed by creation of an exacting study.
- Explain results of control experiments and give remarks that are not accessible in a prescribed figure or table, if appropriate.
- Examine your data, then prepare the analyzed (transformed) data in the form of a figure (graph), table, or manuscript.

What to stay away from:

- Do not discuss or infer your outcome, report surrounding information, or try to explain anything.
- Do not include raw data or intermediate calculations in a research manuscript.
- Do not present similar data more than once.
- A manuscript should complement any figures or tables, not duplicate information.
- Never confuse figures with tables—there is a difference.

Approach:

As always, use past tense when you submit your results, and put the whole thing in a reasonable order.

Put figures and tables, appropriately numbered, in order at the end of the report.

If you desire, you may place your figures and tables properly within the text of your results section.

Figures and tables:

If you put figures and tables at the end of some details, make certain that they are visibly distinguished from any attached appendix materials, such as raw facts. Whatever the position, each table must be titled, numbered one after the other, and include a heading. All figures and tables must be divided from the text.

Discussion:

The discussion is expected to be the trickiest segment to write. A lot of papers submitted to the journal are discarded based on problems with the discussion. There is no rule for how long an argument should be.

Position your understanding of the outcome visibly to lead the reviewer through your conclusions, and then finish the paper with a summing up of the implications of the study. The purpose here is to offer an understanding of your results and support all of your conclusions, using facts from your research and generally accepted information, if suitable. The implication of results should be fully described.

Infer your data in the conversation in suitable depth. This means that when you clarify an observable fact, you must explain mechanisms that may account for the observation. If your results vary from your prospect, make clear why that may have happened. If your results agree, then explain the theory that the proof supported. It is never suitable to just state that the data approved the prospect, and let it drop at that. Make a decision as to whether each premise is supported or discarded or if you cannot make a conclusion with assurance. Do not just dismiss a study or part of a study as "uncertain."

Research papers are not acknowledged if the work is imperfect. Draw what conclusions you can based upon the results that you have, and take care of the study as a finished work.

- You may propose future guidelines, such as how an experiment might be personalized to accomplish a new idea.
- Give details of all of your remarks as much as possible, focusing on mechanisms.
- Make a decision as to whether the tentative design sufficiently addressed the theory and whether or not it was correctly restricted. Try to present substitute explanations if they are sensible alternatives.
- One piece of research will not counter an overall question, so maintain the large picture in mind. Where do you go next? The best studies unlock new avenues of study. What questions remain?
- Recommendations for detailed papers will offer supplementary suggestions.

Approach:

When you refer to information, differentiate data generated by your own studies from other available information. Present work done by specific persons (including you) in past tense.

Describe generally acknowledged facts and main beliefs in present tense.

The Administration Rules

Administration Rules to Be Strictly Followed before Submitting Your Research Paper to Global Journals Inc.

Please read the following rules and regulations carefully before submitting your research paper to Global Journals Inc. to avoid rejection.

Segment draft and final research paper: You have to strictly follow the template of a research paper, failing which your paper may get rejected. You are expected to write each part of the paper wholly on your own. The peer reviewers need to identify your own perspective of the concepts in your own terms. Please do not extract straight from any other source, and do not rephrase someone else's analysis. Do not allow anyone else to proofread your manuscript.

Written material: You may discuss this with your guides and key sources. Do not copy anyone else's paper, even if this is only imitation, otherwise it will be rejected on the grounds of plagiarism, which is illegal. Various methods to avoid plagiarism are strictly applied by us to every paper, and, if found guilty, you may be blacklisted, which could affect your career adversely. To guard yourself and others from possible illegal use, please do not permit anyone to use or even read your paper and file.

Criterion for Grading a Research Paper (Compilation) by Global Journals Inc. (US)

Please note that following table is only a Grading of "Paper Compilation" and not on "Performed/Stated Research" whose grading solely depends on Individual Assigned Peer Reviewer and Editorial Board Member. These can be available only on request and after decision of Paper. This report will be the property of Global Journals Inc. (US).

Topics	Grades		
	A-B	**C-D**	**E-F**
Abstract	Clear and concise with appropriate content, Correct format. 200 words or below	Unclear summary and no specific data, Incorrect form Above 200 words	No specific data with ambiguous information Above 250 words
Introduction	Containing all background details with clear goal and appropriate details, flow specification, no grammar and spelling mistake, well organized sentence and paragraph, reference cited	Unclear and confusing data, appropriate format, grammar and spelling errors with unorganized matter	Out of place depth and content, hazy format
Methods and Procedures	Clear and to the point with well arranged paragraph, precision and accuracy of facts and figures, well organized subheads	Difficult to comprehend with embarrassed text, too much explanation but completed	Incorrect and unorganized structure with hazy meaning
Result	Well organized, Clear and specific, Correct units with precision, correct data, well structuring of paragraph, no grammar and spelling mistake	Complete and embarrassed text, difficult to comprehend	Irregular format with wrong facts and figures
Discussion	Well organized, meaningful specification, sound conclusion, logical and concise explanation, highly structured paragraph reference cited	Wordy, unclear conclusion, spurious	Conclusion is not cited, unorganized, difficult to comprehend
References	Complete and correct format, well organized	Beside the point, Incomplete	Wrong format and structuring

INDEX

save our planet

Global Journal of Computer Science and Technology

Visit us on the Web at www.GlobalJournals.org | www.ComputerResearch.org
or email us at helpdesk@globaljournals.org

ISSN 9754350