Journal of Data Acquisition and Processing
ISSN: 1004-9037
https://sjcjycl.cn/
DOI: 10.5281/zenodo.777530

FRAMEWORK & TECHNIQUES TO IMPROVE CYBER SECURITY IN NIGERIA

Lawan Bulama
Ph.D. Research Scholar, Department of Computer Science and Engineering,
Vivekananda Global University, Jaipur Rajasthan, India
Email: lawanblm@gmail.com

Manish Shrivastava
Professor, Department of Computer Science and Engineering, Vivekananda Global University, Jaipur, Rajasthan, India,
Email: shrvastava@vgu.ac.in

Abstract
The development of Information & Communication Technology has transformed the world into a global village through the use of the internet and other communication tools to connect people from different geographical locations. However, this development has also caused losses of billions of dollars to the world, and especially Nigeria, due to various forms of cybercrimes, which include Email Spam, Online Charity, Phishing/Spamming, and the spread of computer viruses. The consequences of this necessitate the need for the development of frameworks and techniques to improve cyber security.
A framework is a guideline and process through which the government and private sector can mitigate cyber criminals' activities in the country. On the other hand, techniques deal with applications and software to combat cybercrime and protect the cyber environment. In an attempt to do so, this paper employs a mixed method of data collection, presentation, and analysis, which entails primary and secondary source data collection.
The objective of this paper is to examine the framework and techniques to improve cyber security in Nigeria. The paper's recommendations include the adoption of effective use of techniques such as Digital Right Management (DRM), IP address tracker, Cryptography, Interactive Voice Response, the establishment of Cyber Security Police Stations, and the introduction of Cyber Education ethics to primary and secondary schools and related tools to mitigate cybercrime in the country.
In conclusion, the recommendations provided in this paper would be useful in developing effective strategies for improving Cyber Security in Nigeria. The government and private agencies should take the necessary steps to implement these recommendations to protect the country's cyber environment and prevent the loss of billions of dollars due to cybercrime.
Keywords: Framework, Techniques, Cyber-Security, Improve, Nigeria

Introduction

Background of the study
A conceptual review of Cyber Security would be an excellent way to deepen our understanding of the topic. It would also be useful to gather data on the current state of Cyber Security in Nigeria, the types of cyber-attacks that are most prevalent, and their impact on the country's

economy. Such data would provide a solid foundation for creating effective Frameworks and Techniques for addressing the challenges posed by cybercrime in Nigeria.

In developing the Frameworks and Techniques, it is important to consider the unique challenges and characteristics of the Nigerian environment. This would include an understanding of the cultural, social, and economic factors that contribute to the prevalence of cybercrime in the country.

In conclusion, the issue of Cyber Security in Nigeria is a critical concern that requires urgent attention. The collaboration of various companies and organizations, as well as the development of Frameworks and Techniques, is crucial to achieving a safe, secure, and resilient Cyberspace in Nigeria. It is also important to note that addressing the challenges of cybercrime in Nigeria has the potential to create job opportunities and improve the country's economy.

Objectives of the study

The main aim of the research is to find out the role of Framework & Techniques to improve Cyber Security in Nigeria. Other specific objectives of the research as follows:

1. To examine the framework and Techniques for improving Cyber Security in Nigeria

2. To explore the efforts of Nigeria Computer Emergency Response Team (ngCERT) in mitigate Cyber Crime in Nigeria

3. To access the significance of framework & techniques for mitigate Cyber Crime.

Method of Investigation /Research Method

The research title, Framework & Techniques to Improve Cyber Security in Nigeria, applies mixed methods of data collection, presentation, and analysis. Consequently, primary and secondary sources of data collection will be used in conducting this research. In terms of primary sources, Questioners and interviews will be used to obtain first-hand information from respondents in order to obtain reliable and verified information that is empirical in nature. On the other hand, the secondary source of data collection will constitute document and content analysis from relevant text books, journals, publications, Ph.D. theses, newsletters, magazines, bulletins, and newspapers, as well as world-wide websites, otherwise known as internet sources, employed in this research.

Literature Review

Internet of Thing (IOT):

Cyber Crime

Radanliev (2019). Contrarily, the term "Internet of Things" refers to actual, tangible objects that are equipped with sensors, computer power, software, and other devices that can communicate with other hardware. With this technique, moving data between locations is rather simple.

The term "Internet of Things" (IOT) often refers to network cyber-physical items that may connect and share data in a variety of limited situations, such as technologies that regularly significantly increase safety risk and cause considerable ethical concerns.

However, Longe (2019) contends that email fraud and phishing are the most repulsive cybercrime phenomena. The victims' investment information and plans are stolen by these scams, which solicit and present fake financial documents. In addition to the aforementioned,

they occasionally utilize women to commit crimes and fool investors into believing that their deceased husbands were members of parliament. that she requires someone to look after her finances and other assets.

According to Vidya, P.M. (2014), "cybercrime" is the act of committing a crime and erasing data from a database while using a computer or internet network as a method of communication. The U.S. Department of Justice, however, broadens the definition of cybercrime to include any criminal action that uses a computer to steal personal information without authority's consent.

The nation's precarious political and socioeconomic system will be destroyed by cybercrime, according to Adewole (2011). Attempts by the country to rank among the top twenty economies in the world by 2020 would undoubtedly fail or be a mirage as a result of this. For countries to reduce the activity of cybercriminals, cyber ethics and regulatory agencies are necessary.

Biometric

Bulama, L. (2022), highlights the potential benefits of incorporating biometric data as a component of ICT, emphasizing the ability to identify and verify millions of individuals through the use of both physiological and behavioral biometric data. Specifically, the implementation of biometric technology in Nigeria has the potential to significantly reduce the country's high levels of cybercrime and other criminal activities, providing a powerful tool for law enforcement and security agencies to combat these threats and safeguard citizens' personal and financial information.

Cyber Crime Victims

According to Cable News Paper ( ) the Nigeria ranked 16th in FBI global cyber-crime victims report ranked 16th among the countries' musts affected by internet in the world 2020. In addition to above, the FBIS Internet Crime Complaint Centre (ICCC) said it received 791,790 complaints related to internet crime increase more than 300, 000 complaints from 2019.

Table 1: of cyber crimes and their estimate daily activity

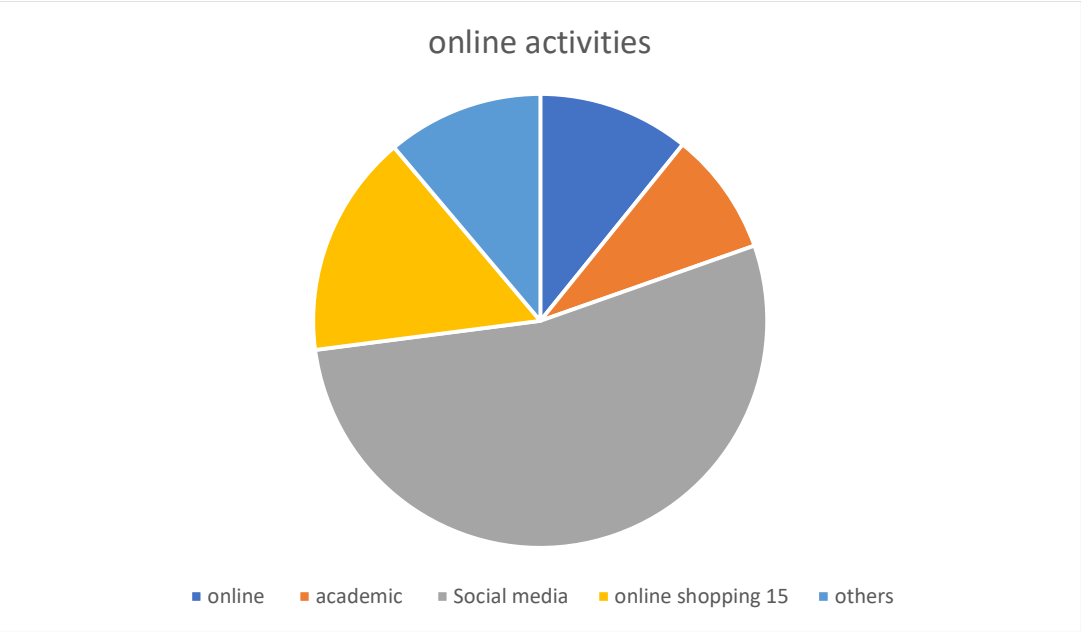
Ransomware	400
Phishing	33,000
New malicious software /malware	300,000
Record lost to hacking daily	780,000
Malicious	80.billion

Source: Kabanda, G. 2018 Compile by author

Regulation and law enforcement

Shail, ( ) argued that the United States of America (USA) the regulation and law enforcement of Cyber Crime is similar to the EU. In the mid 1980s the two important statutes were passed by US Congress to combat computer related crime in which federal interests involve the counterfeit access devices and computer fraud and Abuse Act(18USC & 1030-1984) as well as electronic communication privacy Act (18USC 88 2500-2711-1986) the cyber fraud and making international false representation online, identity theft which happens in the form of unauthorize used of another person's social security number, drivers licence ,work Id or credit

card online is also federal cybercrime. In recent times there was a radical upward departure from sentencing guideline in conviction for identity theft.



Source : by Author

When the activities that were usually done online were examined, it was found that 10.2% of people spent more time playing online games, 8.3% of people read online news and other articles, and 50.3% of people browsed through various social networking sites including Facebook, Instagram, Whatsapp, and others. 15% of people shop online. 10.5 percent of users were active in academic research, while the rest were doing other online activities including watching videos and listening to music. The conclusions and subsequent responses were disclosed.

Motiwala. A. (2017), by the law enforcement agencies most provide the intensive training for law enforcement and military official so they have a good computer knowledge to identify cyber crime activities and how to how to collect the relevant evidence and data from computers and service providers in properly evaluate them in a timely manner. While Nigeria are currently provides limited training in this area.

Cyber Security

As agued by Akintoye, (2022), the cyber security refers to attendant of practices and activities fashioned out with a view to ensuring the protection of personal and organization data information and network from possible threat whether internally or externally. Moreover, cybercrime is a criminal's activities by using computer and internet to steal the personal information of targeted victim through different ways.

According to Zwilling, M. and et'al (2022), importance of good cyber hygiene practices and how to recognize and report phishing attempts. This helps to reduce the risk of successful cyber-attacks on the organization. In addition, regular cybersecurity awareness training can also help in creating a security-conscious culture within the organization, where employees are

actively engaged in protecting the organization's valuable assets, including sensitive data and intellectual property. Overall, it is critical that organizations and individuals take cybersecurity seriously and implement preventive measures such as strong passwords, two-factor authentication, and regular security awareness training to reduce the risk of cyber-attacks. The authors suggest that cybersecurity is a shared responsibility, and everyone has a role to play in keeping the digital world safe and secure. Thus, the government should make cybersecurity awareness training mandatory in all schools, colleges, and universities to ensure that the next generation is well-equipped to deal with the growing cyber threats prioritize preventative and proactive techniques.

The authors suggest that cybersecurity is a shared responsibility, and everyone has a role to play in ensuring the digital world remains safe and secure. Consequently, it is recommended that the government should make cybersecurity awareness training mandatory in all schools, colleges, and universities to equip the next generation with the necessary skills to handle the increasing number of cyber threats and prioritize preventative and proactive techniques. Overall, by emphasizing the importance of good cyber hygiene practices and implementing regular cybersecurity awareness training, organizations and individuals can reduce their vulnerability to cyber threats and contribute to creating a safer digital environment.

Internet fraud

According to Igwe, K.N. & Ibgwan, A. (2014), the Nigerian government is actively working towards fostering a digital economy and advancing e-governance in the nation. This is evidenced by the various initiatives and programs undertaken by numerous government ministries, departments, and agencies (MDAs), such as the National Communication Commission (NCC) and the National Information Technology Agency (NITDA), among others.

Despite these efforts, the success of these agencies in developing Nigeria's e-government is contingent upon their ability to establish a supportive framework and procedures to improve cyber security. Without such measures in place, the agencies' attempts to connect the nation's information and communication technology will be in vain, as information theft by cybercriminals is a global problem that poses a significant threat to the security and integrity of data systems.

To this end, the Nigerian government has recognized the importance of cybersecurity and has taken steps to improve it. For instance, the government has established more than 400 rural information technology centers (RITCs) in various communities across the country in order to implement the National Information Technology Policy of 2001. These RITCs have helped to extend the reach of digital services and infrastructure to remote and underserved areas, and have also helped to create jobs and stimulate economic growth in these communities.

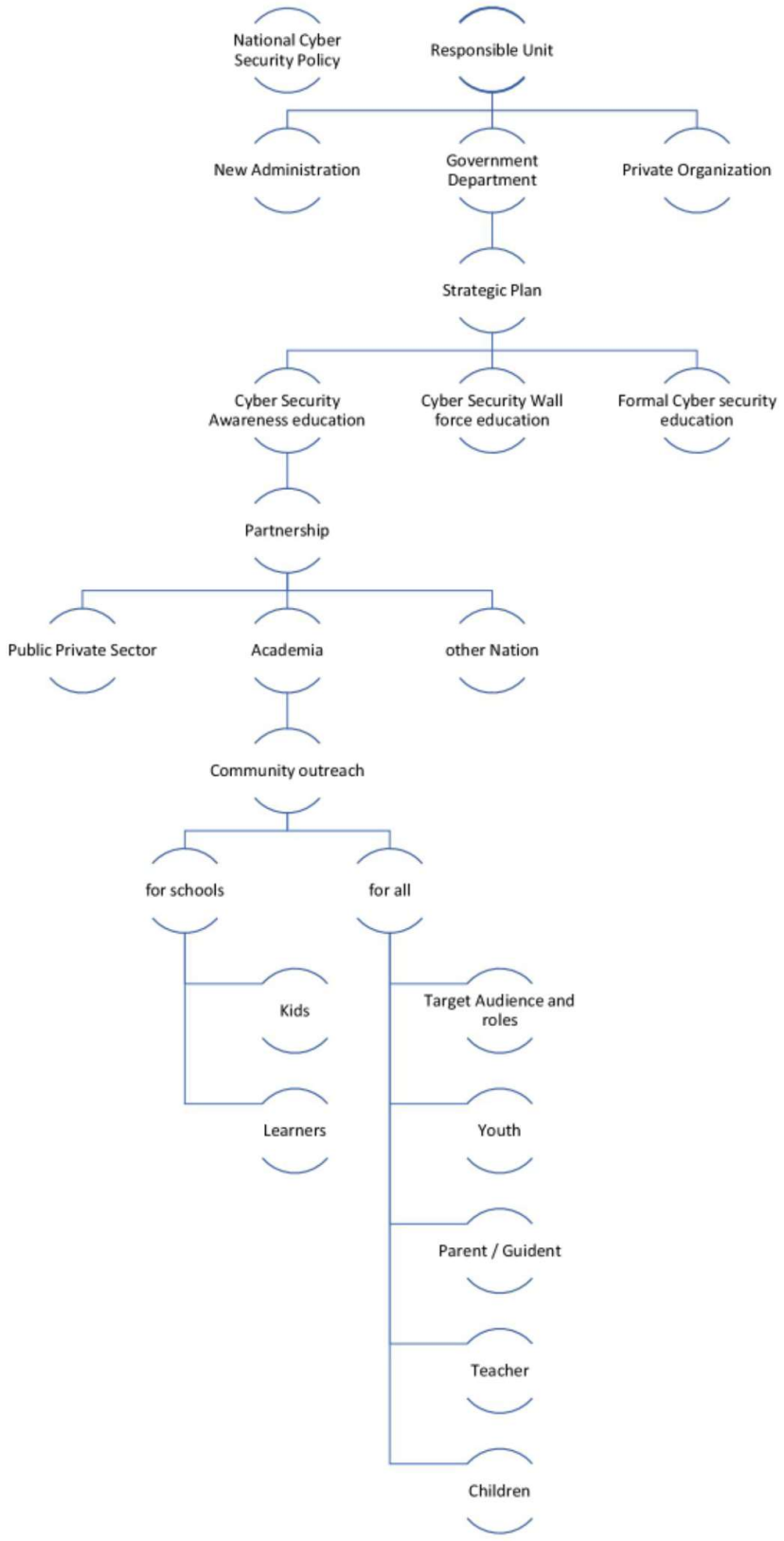
In conclusion, while the Nigerian government is making strides towards developing a digital economy and advancing e-governance, it is crucial that cybersecurity measures are put in place to safeguard against cyber threats. By establishing supportive frameworks and procedures, and by continuing to invest in initiatives such as the RITCs, Nigeria can build a strong and secure digital infrastructure that will enable its citizens to fully participate in the digital economy and reap its benefits.

However, Akintoye, (2022), further stressed that the electronic fraud tracker (Nigeria electronic fraud forum) the total value of cyber induce electronic fraud was in excess of NGN 6.1 billion as 2019. The issues need to be addressed by the government to reduce cybercrime in the country.

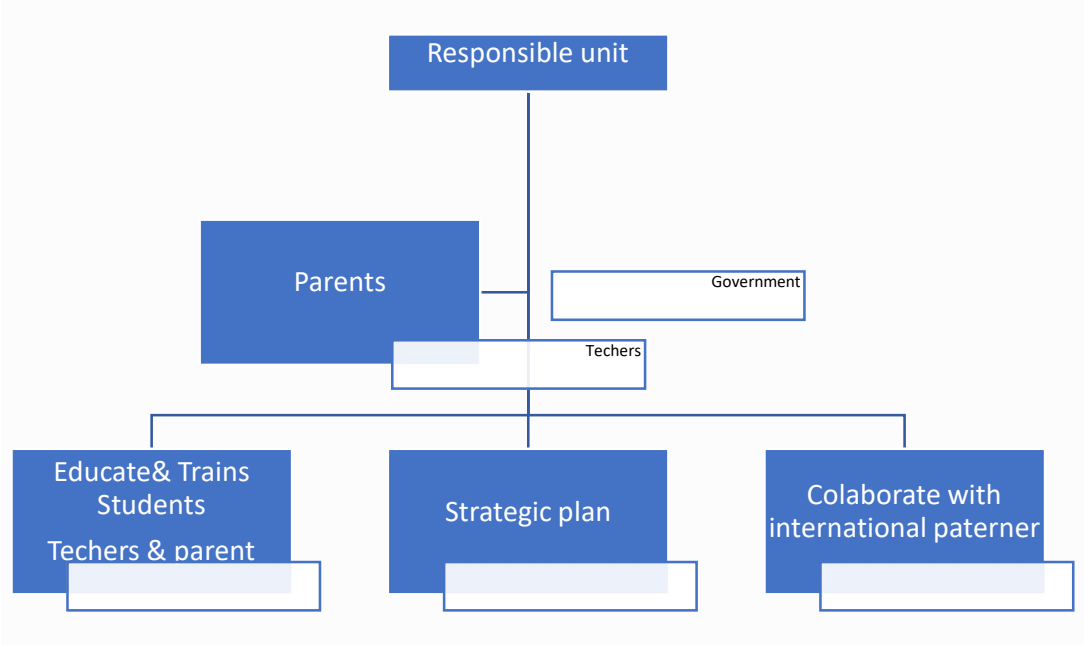
Multipurpose framework

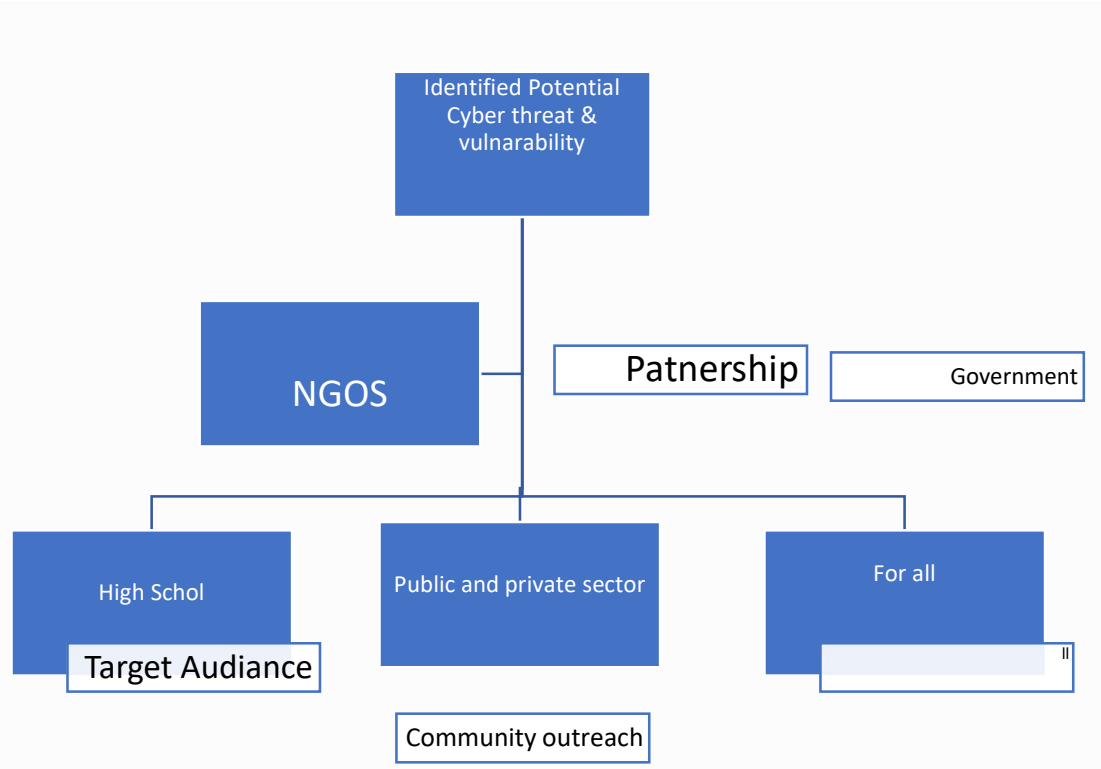
Conforming with Karthick, et'al ( ) multipurpose framework (OS) is programming that permit cell phone tablet PCS, and different gadget to run application along with projects there are several types of mobile operating system available in market the commonly used mobile operating systems are Android working framework is open source and source code discharge by Google under Apache Permit Licence based on Linux – Kernel designed for Smartphone and tablets. An Android (Mobile Technology) is one of the most popular operating systems for smart phones at the last quarter of 2016 the total number of application available in Google play store was 2.6 million and a total number of Android operating system based Smartphone(Mobile Technology) sold was 2.1 billion the market share of android in the first quarter of 2016 was 84.1% whereas iOS windows ,blackberry, and other hold 14.8%, 0.7%, 0.2% and respectively there it is clear that android has widest market when compared to others mobile operating systems.

Furthermore, Said by Katsontonis it is important to stay up-to-date with the latest security trends and technologies, which can include implementing next-generation firewalls, intrusion detection and prevention systems, and security information and event management solutions, as well as regularly conducting penetration testing and vulnerability assessments to identify weaknesses in the security posture of organizations and take steps to address them. It is also crucial to have a dedicated security team to monitor network traffic and respond to incidents in a timely manner, along with contingency plans in place in the event of a cyber-attack or data breach, including regularly backing up critical data and having procedures in place to restore systems and services quickly and efficiently. Overall, a strong and effective cybersecurity strategy requires a combination of technology, policies, and procedures, as well as employee education and training, to comprehensively approach security and better protect organizations from cyber threats, ensuring the continuity of their operations.



Framework on curbing cyber security





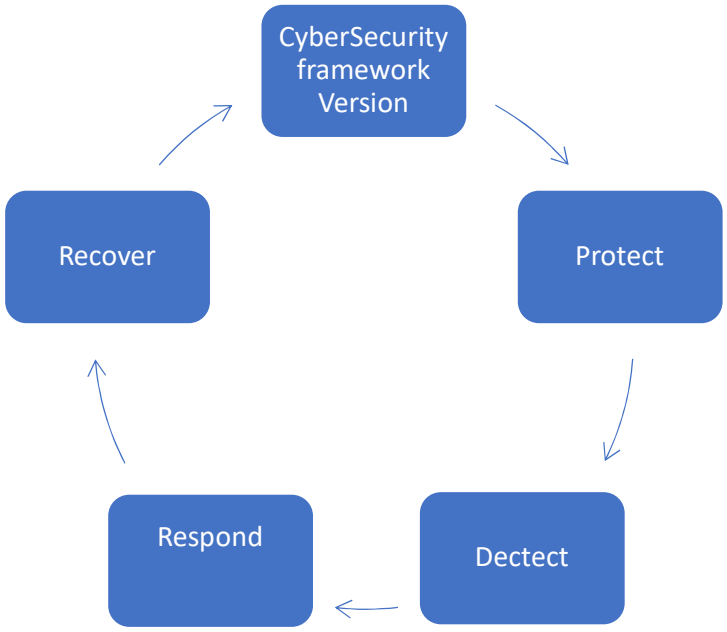
Framework for Primary school students on cyber security

Said by Almuhammadi, S, NIST has introduced an integrated framework to organizations with critical infrastructure in order to improve cybersecurity. It is recommended to use this framework on top of complement within the organization.

According to Eric, A, the Obama administration also took several actions relating to the issues of cyber attacks in cybersecurity. They focused on modernizing federal ICT and established a

commission to improve security in Africa, especially in Nigeria because of the high prevalence of cybercrime in the country.

The NIST Cybersecurity Framework consists of five sub-components or activities, which are Identify, Protect, Detect, Respond, and Recover, as shown in Figure 1: Framework on Cybersecurity.



Source: Macafee(2018)

According to Kabanda, G. (2018), the lack of framework to provide direction, focus guidance and standardise way of addressing cyber security framework in how prevent response and reduce the cyber crime. However, if the is proper framework and some techniques it significantly reduces said cyber crime in the country. In addition to above, the according to world Economic Forum cybercrime costs the $U.S 575 billion annually which constitute 0.5% of the world Gross Domestic Product. The damage caused by cyber-crime is also expected to reach U S 86 trillion by 2021 (KPMG) 2018.

Losses to Cyber Crime

In 2017, Kshetri reported that the African economy suffered a significant loss of $3.5 billion due to cybercrimes, with Nigeria and Kenya bearing the brunt of the losses, estimated at $649 million and $210 million, respectively, whereas South Africa lost $157 million annually to cyber-crimes, according to the South African Banking Risk Information Centre (SABRIC). Moreover, cyber-attacks originating from African economies have impacted the global landscape. For example, in 2010, a staggering 80% of personal computers (PCs) used in Africa were infected with viruses and malware, which cybercriminals exploited to launch cyber-attacks against targets worldwide**.**

As pointed out by Raghava et al. (2014), cybercriminals have developed advanced techniques not only to steal finance and financial information, but also to conduct business espionage and access important business information. Records have revealed that banks globally lose an average of $114 billion US dollars each year due to cybercrimes.

In view of the above, the cost of combating cybercrimes is sometimes double the amount lost to such crimes, which amounts to an average of $274 billion US dollars in the banking sector. Moreover, it has been estimated that $4 billion is spent on recovering $3.6 billion US dollars from a given crime in order to prevent such crimes from happening in the future.

Sule et al. (2021) reported that Nigeria has lost an average of 127 billion Naira (equivalent to about $328,842,878 million US Dollars) to cybercrime in recent years. The report also highlighted the fact that Nigeria has gained a reputation as the global headquarters of cybercrime due to the high frequency of daily incidents linked to the country. This has been a major concern for the Nigerian government and stakeholders in the technology industry, as cybercrime not only causes financial losses but also damages the country's reputation and hinders its economic development.

Awhefeada (2020), on the other hand is of the opinion that, Central Bank of Nigeria should promulgate laws governing the online transactions as the country loses one hundred and twenty seven (N127 billion)naira to cybercrime which negatively affected the Gross Domestic Product (GDP). This is a serious challenge of Cyber Crime which is usually being conducted through the use of different devices to conduct criminal's activities.

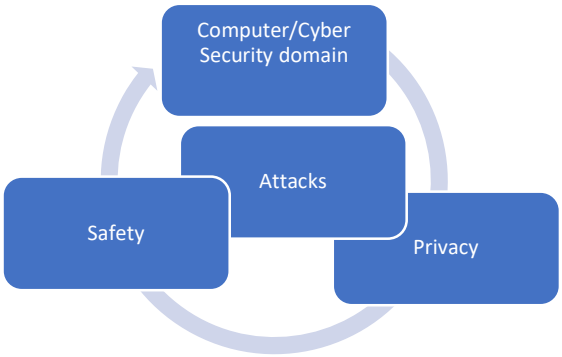
Furthermore, it was argued by Dauda et'al (2020), The quotation by the National Security Adviser to President Mohammadu Buhari Says Nigeria losses N127 Billion annually to Cybercrime that is how devastating the effect of Cyber Crime to Nigeria. Hence, fighting and defeating it remains the only way forward. It is embarrassing when foreign Countries catch Nigerians who commit Cybercrime, till date Nigeria suffers from the sigma of 419 put on the nation in the 90's according to the president of integrated Cyber Security Solution in Nigeria 2015 Nigeria lost $400 Billion this show that crime activities in Nigeria is worsen the economy and reputation of the country.

Growth of Technology

According to Fedis, C. et al. (2013), the rise in the usage of smart phones and mobile devices such as iPhone, Blackberry, Nokia, and Android phones, etc., has exacerbated the mobile security challenges in Nigeria, rapidly contributing to the spread of worms, viruses, trojans, logic bombs, and other malicious files, among other tools in committing cybercrimes. However, Fedis said millions of users and subscribers use mobile platforms, but there is no holistic framework to protect mobile users from cyber-crime. A framework for improving cyber security.

However, to tackle mobile cyber security challenges in Nigeria, there are some factors to consider, like cyber security domains. classified the computer and cyber security domain into the three following categories: Safety Attacks Privacy

Moreover, safety deals with both the physical well-being and security of mobile platform users (subscribers) and mobile equipment. Attacks deal with all types of security vulnerabilities and breaches that affect the smooth operation of mobile platforms and services. Privacy deals with the concerns over the preservation and protection of confidentiality and integrity of mobile data information from unauthorised users or hackers.



Computer and Cyber Security domain.

Joshi, et'al ( ) argued that the growth of technology has led to the growth of the Smartphone industry today almost every person irrespective of the age or group has their own Smartphone this also lead to increase in cyber thefts and crimes related to smart phones and data stored on mobile devices and more than 1 billion Android devices (Mobile) are at risk of being hacked because they are no longer protected by security updates while Apple ensures that its iPhone cannot be hacked because it has strong interfaces in place. Android users continued to remain fearful of getting the devices hacked through their leakage of their data. The researcher has further tested a huge range of smart phones and result shocking reveals that popular model like Samsung Galaxy S3 and Sony Xperia Z2 are particular at risk to hackers.

However, the threat of cybercrime is breaking into homes and offices without smashing doors or windows; instead, they utilise computer systems and internet facilities to steal the victims' personal information. The government's incapacity to sufficiently safeguard its information system is the cause of all these ongoing issues.

Digital Rights Administration

Ebersohn (2003), states that the objective of the Digital Rights Management (DRM) technology is to control access to and use of digital content during the course of the content's lifetime by defining viewing, copying, and the system's prevention of online privacy of digital contents like: The construction of a data baseband content identification is the first phase of the audio fingerprint technology, which focuses on information that may identify music based on its contents.

Cyber Forensic

According to Goni, (nd) digital forensic is a sciences that described the techniques of forensics investigation of crime that take place in a computer network or computer system has been used as weapon for cyber attack or conduct a criminals activities.

Zukarnain, Z.A. et'al (2022), The study was carried out through an interactive workshop designed for elementary school children, aged between 8 and 12 years old. During the workshop, children were introduced to basic cybersecurity concepts and were taught how to safeguard their personal information, avoid online scams, and protect their digital devices.

Furthermore, the workshop included interactive sessions that allowed children to explore the potential cybersecurity risks by engaging in problem-based learning activities.
The study found that the workshop was effective in enhancing children's cybersecurity knowledge and awareness. The children were able to identify potential risks and take appropriate measures to mitigate them. Moreover, the children demonstrated an increased understanding of the importance of responsible online behaviour and the need to protect themselves and others while online.
Overall, the study suggests that awareness training programs can play a vital role in educating children about safe online practices. It is essential to continue developing such programs to provide children with the necessary knowledge and skills to stay safe online. Moreover, it is equally important to encourage active involvement from parents and educators to guide children and reinforce good cybersecurity practices. By working together, we can create a safer and more secure online environment for our children.

In addition to the above, Hackers make use of the weaknesses and loop holes in operating system to destroy data and steal important information from victim's computer. Its normally dove through the use of a backdoor programme install in machine. A lot of hackers also try to gain access to resource through use of password hacking software

Funding to Cyber Security

According to Cyre University costs and funding for Research & Development (R&D) and education in this era early 2015, the Secretary of Defense released the DOD'S strategy where it was emphasized that the scale of the cyber threat require urgent action towards building capabilities for cyber defense and cyber operation.
Moreover, Premium Times (2022), reported that, the Nigeria Communication Commission (NCC) has informed of new high-risk, critical and short messaging service-based malware used for tangle Bot thereby infecting Mobile devises. This attitude targeted Mobile users in Nigeria to hack their data and vital information to steal their money or bank details as well as other data that is highly confidential.

Fake News on social media

According to the Hindu Times (2020), India registered 50,355 instances of fake news on social media in 2020, which have been connected to cybercrimes conducted by cybercriminals. This illustrates how widespread cybercrimes are and how urgently they need to be tackled and curbed to the bare minimum.

Cyber Infrastructure

Moreover, President Obama has allocated $5.5 billion for DOD's cyber infrastructure operation and maintenance program. A total of $ 14 billion has been designated for cyber security in the 2016 budget by the president, which is an increase of 10% from the 2015 NSFS () estimated funding for SATC. The mainstream programme for cyber security at NSF is $ 124.25 million. Almomoni, I. et al. (2021), Hence the higher education institutions and universities should

learn lessons from previous hacking scenarios in the HEI service and be always ready to depend on agents for all possible attacks that might target this. This shows that there is a need to protect the cyberspace.

Internet

Notwithstanding, Odoom (2012) opined that cyber threats are a big issue in Africa (inclusive of Nigeria), where cybercrimes are on the rise due to the fact that many computers and mobile phones are not protected. This allows hackers to access the information of many mobile users and make them victims of cybercrime.

Internet

As argued by Charis (2016), the internet is a global network that unites millions of computers located in different countries and opens broad opportunities to obtain and exchange information, but it is now used for criminal purposes due to economic factors. Nigeria is a third world country, and with so many economic challenges such as poverty, corruption, and unemployment among others, there is a need to improve job opportunities in the country.

According to Frank (2013), web site cloning is one of the recent trends in cybercrime, with the emergence of fake copycat web sites that take advantage of customers who are unfamiliar with the internet or who do not know the exact web address of a legitimate company that they wish to visit.

Cyber Attack

According to Cyre University Pittsburgh, a recent cyber-attack occurred on Sony, breaching the company's information and stealing personal data. Because of their vulnerability, individuals, organizations, and nations become targets for cybercriminals who cause harm on the internet. More so, hackers breached Hollywood celebrities' I-Cloud accounts, which caused the loss of $148 million US dollars in 2014 alone. This portrays social embarrassment and downsizing the economy of the nation, and it also destroys job opportunities among the teeming youth.

Data Presentation and Analysis

The research noted that there are lots of losses incurred by the government of Nigeria as a result of cybercrime, which can be seen in the following table. This necessitated the need to have a strong framework along with techniques for improving cyber security in Nigeria.

Table 1: Details of loss due to Cyber Crime, Year and factors responsible

S/N	Year of Reporting	Lose due to Cyber Crime	Factors Responsible	Source/Reference
1	2019	NGN 127 Billion Naira	Inability to secure information system	Mat et'al

2	2021	$ 328,842,878 million	Cyber Crime	Sule et'al
3	2020	NGN 127 Billion	Cyber Crime	Awhefeada et'al
4	2014	$114 Billion	Cyber Crimes at Banks	Raghavan et'al

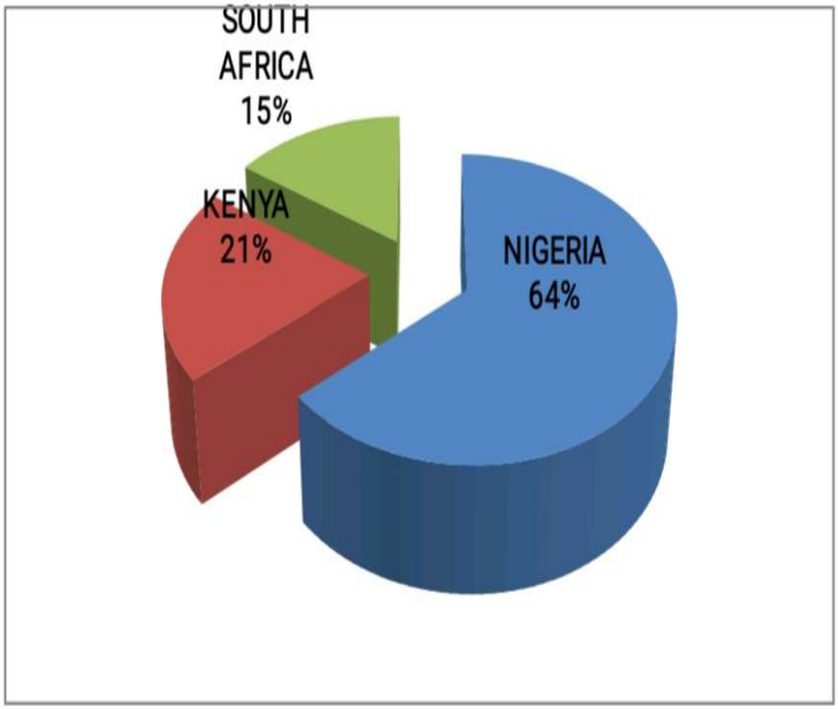
Source: Mat et'al, (2019) Sule et'al, (2021) Awhefeada et'al, (2020) Raghavan et'al (2014) and compiled by Author, 2022

Table 2: Details of Cyber Crimes in some African Countries

S/N	Country	Amount loss in US Dollar	Factors Responsible for the loss
1	Nigeria	$649 USD	Cyber Crimes
2	Kenya	$210 USD	Cyber Crimes
3	South Africa	$157 USD	Cyber Crimes

Source: Kshetri (2017) and compiled by the Author 2022

Figure 1: Showing Countries with Percentage of loss due to Cyber Crime



Source: Kshetri (2017) and compiled by the Author 2022

Based on the above Table &Figure it is clear that the problem of Cyber Crimes and its effect on the Countries is increasing.

Conclusion

The research in its findings discovered that there is a lack of training and awareness for citizens about cyber threats and related activities on how to protect people's information, which resulted in hacking and the theft of important information. More so, the study noticed that Enterprise Application Software (EAS) is used in some public places. The research equally explored the fact that digital investigation technology as a component of EN cases is very relevant in curbing cybercrime. Notwithstanding, the research noted that an air gap system is lacking in Nigeria to secure the flow of information between two contending networks. Much more importantly, the findings of the research revealed that the software detection techniques usually reduce the chance of hacking to commit cybercrime. When a particular website is attacked by a virus, it will malfunction and give room or access to penetrate it and steal relevant data or information that can be used to commit cybercrime.

Recommendations

Based on the aforementioned findings, the research proffers the following recommendations:

1. That is, there should be awareness and training of the citizens on cyber threats and their consequences on people's information and data, which would reduce the hacking and stealing of relevant dossiers for committing cybercrime in Nigeria at the expense of both the government and citizens.
2. That there are should Enterprise Application Software (EAS) is computer software used to stratify the needs of an organization's users, which include businesses, schools, governments, and charities. It is therefore recommended that it be adopted in Nigeria.
3. EN Case is the global standard in Digital Investigation Technology (DIT) for forensically sound data collection by using a repeatable and defensible method to curb cybercrime in Nigeria. There is an air gap system for securing data flow between two networks that will be favourable and applicable in Nigeria.
4. Antivirus detection of malicious software by its signature and behaviour should be adopted with possible modifications in Nigeria.
5. Establishment of a cyber security police station and training the officers about cyber security Cyber ethics education and its content should be properly articulated and integrated into computer education or social studies subjects in primary and secondary schools in the country.
6. Cyber Security Framework and techniques.

References

1. Adewole, K., et al. (2011), an inquiry into the awareness level of cyber security policy and measures in Nigeria. *International Journal of Science and Advanced Technology*, Vol. 1, No. 7, Pp. 91–96.
2. Akintoye, R. et al. (2022), "Cyber Security and Financial Innovation of Selected Deposit Banks in Nigeria." Universal Journal of Accounting and Finance, Vol. 10, No. 3, pp. 643-652.

3. Awhefeada, et al(2020),Appraising the Law Governing the Control of Cyber Crime in Nigeria," *Journal of Law and Criminal Justice, Volume 8, 2020, Number 1, pp. 30-49.*
4. Bulama, L. and Shirivastata, M. (2022), The Role of Information & Communication Technology Towards Protection of Lives and Property in Northern Nigeria: A Focus on Maiduguri Borno State in *Vidyabharti International Interdisciplinary Research Journal, Volume 14 Number 1, March 2022. Pp. 1 – 9.*
5. Cable News Paper Nigeria Ranked 16th in FBI Global Cyber Crime: Victims Report

6. Chais, O, (2016) Crime, Cyber Crime and Nigeria business environment. *National Journal of Advance Research .Vol.2 Issue, 2.pp 28-38*
6. Dauda, A. et'al (2020) Challenges and way out of Cyber Security Issues in Nigeria.
7. Ebersohn, G. Catching Hacking in data Business. *The quarterly Law Review for people in Business* Volume, 12. 2003 part 1.
8. Frank, I. And Odumayo, E. Approach to Cyber Security issues in Nigeria: Challenges and Solution *International Journal of Cognitive Research in Science, Engineering and Education (IJCRSEE)* Volume 1, Number 1, 2013.
9. Goni, I, & Mohammed, M. Machine Learning Approach to Mobile Forensics Framework for Cyber Crime Detection in Nigeria. Unpublished paper

10. Joshi, E. Cyber Crime 1 billion Android Devices at Risk of Hacking. Reported law street journal.
11. Karthicks S. Et'al Android Security issues and Solution. International Conference on Innovative Mechanism for Industry Application unpublished paper.
12. Kortjan, N, and Solms, V. (2014), A conceptual framework for Cyber –Security Awareness and Education in South Africa. *Research Article SACJ No*, 52. Pp 29-41.

13. Kshetri, N. Cyber Crime and Cyber Security in Africa. *Journal of Global Information Technology Management* Volume,22. 2017 Issue 2 pp. 77 81.

14. Longe, O, et'al (2009), Criminal uses of Information & Communication Technologies in Sub- Saharan African: Trends Concerns and Perspective. *Journal of Information Technology Impact* Vol.9 No.3, pp- 155 172.

15. Mat, B., Pero, S. Wahid, and Sule, B, CyberSecurity and Digital Economy in Malaysia: Trusted, Law for Customer and Enterprise Protection, Intrnational Journal of Innovative Technology and Exploring Engineering 2019

16. Odoom, Q. Fighting Cyber Crime in Africa. *Journal of Computer Science and Engineering Volume 2 Number 6, 2012 Pp 98 - 100*

17. Okutan, A et'al (2019), A Framework for Cyber Crime Investigation. *Proscenia Computer Science* Vol.1 No. 158, pp 287-294.

18. Primer Times. New SMS-based android Malware, TangleBot Unleashed by Criminals NCC. 2022. Press Statement: Available @ https://www.premiumtimesng.com/promoted/508545-news-sms-based-android-malware-tanglebot-unleashed-by-cybercriminals-ncc.html

19. Radanliev, P. et'al (2019), Cyber Security Framework for Internet –of Thing Industry Vol.4, pp- 1-7 unpublished paper.

20. Shell, S. The United States of America The Regulation and Law Enforcement Of Cyber Crime.

23.The Hindu Times. Available @ https:www.thehindu.com/news /national/india-reported-118-rise –in cyber-crime-in -2020-578-incidents- of fake-news –on social –media-data/article36480525 *Villanova Journal of Science Technology and Management volume*, 2. 2020. Number 1. Pp 33-47.

24.Vidya P.M.(2014), Cyber Security -Trend and Challenges. International Journal of Computer Science and Mobile computing.Vol.3, Issue.2 pp-586-590.

25.Motiwala ,A (2017),Cyber Security in Ghana : Evaluating Readiness for the Future. Annaar International Peacekeeping Training Centre Brief (1) pp-1-4.

26.Almomoni, A.A. & Maglara .L.(2021), Cyber Security Martunity Assesment Framework for higher Education Institution in Saudi Arabia. Peer Computer Science 7:703 https://doi:org/10.7717 peerd -cs 703.

27.Kabanda,G. (2018), Cyber Security Culture Framework and its Impact on Zimbabwean organization . Asian Journal of management Engineering & Computer Sciences (AJMECS) Vol, 3 No, 4, pp-17 34.

28.Igwe , K .N. & Ibegwan , A.(2014), Imperation of Cyber Ethics Education to Cyber Crimes prevention and cyber security in Nigeria Vol, 2 Issue- 2 pp-102-115 .

29.Omodunbi,B. A e'tal (2020), Cyber Security Treats in the Era of Covid-19 Pandemic : A Case Study of Nigeria System .International Journal Advanced Research in Engineering and Technology (IJARET) Vol,11. Issue ,9. Pp-387 -396

30. Tutorialsmate,com /2022/01/advantages -of internet html https//www.

31.Fedilis, C & et'al (2013), A Holistic Mobile Security Framework for Nigeria .International Journal of Innovative Technology and Exploring Engineering (IJITEE) Vol ,1 Issues -3 pp- 1-7.

32.Dawson, R. e'tal (2015), The urgent need for an Enforced Awareness Programme to create internet Security Awareness in Nigeria .

33.Adamu, A et'al (2021), Cyber Security Awareness of university Students in Nigeria : Analysis Approach .Turkish Journal of Computer and mathematics Education Vol,12. No 12 pp- 3739-3752.
34. Fera,M.et'al (2021), Security by design for big data frameworks over cloud computing . Non publication article
35.Patricia ,A (2019), Cyber Security Education in Nigeria :A Pree -requisite for the long learner in 21st century .The colloquium- A multidisplinery Thematic Policy Journal . Vol,7 No,1 pp-18-21
36.F.E Ekuro(2022),preliminary Review of Cyber Security Coordinator in Nigeria . Nigeria Journal of Technology (NIJOTECH) Vol,42. No,3 pp- 521-526
37.Mphatheni, R.M & Moluleke,W. (2022), Cyber Security as a Response to combating cyber crime :Demystifying the Prevailing threat and offering recommendation to the Africa region .International Journal of Research in Business and social Science Vol, 11.No, 4. Pp-384-396
38.F.E Ikuero & w.zeng (2022),Improving Cyber Security Incidents Reporting in Nigeria : Micro and small Enterprises Perspectives .Nigeria Journal of Technology (NIJOTECH) Vol, 41. No,3.
39.Dash, B.C.et'al (2022), Prevention of Phishing Attacks using al Based Cyber Security Awareness Training. International Journal of Smart Sensor and Adhoc Network. Vol,3. Issues, 3. Pp-50 -75.
40.Zukarain, Z.A. et'al (2022), Impact of training on cyber security awareness goading journal of science and Technology. Vol,3 No,1. Pp-115-120.
41.Alam,G. & Hijji,M.(2022), Cyber Security Awareness and Training (CAT) Framework for Remote working employees: sonsors.https://doiorg/
42.Katsontonis, M.N. et'al(2023), Cyber range design framework for cyber security education and training .International Journal of Information.
43.Ghelani,D. (2022), Cyber Security ,Cyber Threats Implication and future perspective : A Review. American Journal of science , Engineering and Technology .Vol, 3. No, 6. Pp-12-19.
44.Knight,R.& et'al(2020), A framework for effective corporate communication after cyber security incidents. Computer & security journal pp-2-34.
45.Vladimir, S.P. Freize,F. (2019), A Contingency plan framework for cyber attacks. Journal of information systems Engineering & management.Vol,4.No2.
46.Dsouza, J. et'al(2019), Security in cyber Physical System . In amity International Conference on artificial Intelligence (AICAI) pp-840-844
47Al Shamsi,A.A. (2019), Effectiveness of cyber security Awareness Program for young Children: A cast study UAE. International Journal of Information Technology and language studies.
48.Azam et'al(2020), Assessing and Reviewing of Cyber Security Threats, Attacks Mitigation in IOT Environment. Journal of Theoretical and Applied Information Technology Vol, 100, No, 6. Pp-2958-3011.
49..Alam,G. & Hijji,M. (2022), Cyber Security Awareness and Training (CAT) Framework for remote Working Employees .Sensors. https//doiiorg.
50.Ghelani,D. (2022), Cyber Security Threats and Implication and future Perspective: A Review American Journal of Science and Engineering and Technology Vol, 3.No,6. Pp-12-19.

51.Knighgt, R. & et'al(2020), A framework for effective Corporate Communication after Cyber Security Incidents. Computer & Security Journal pp-2-34.
52.Yadav,T. & Mallari, R. A. Technical Aspects of Cyber Kill Chain
53.Atoum, I. et'al(2014), A holistic Cyber Security Implementation Framework .Information management & Computer Security.
54.Bournemouth,LTD, et'al the development of International E- learning Materials and Implementation Techniques for Cyber Security Behaviour charge Non published
55..Ofori, A. Y. & Brimicombe, A. (2017),Cyber Security intelligence & OSONT: Developing mitigation Techniques Against Cyber Crime Threats on Social Media A Systematic Review. International Journal of Cyber Security and Digital Forensics(IJCSDF) Vol, 7.No,1. Pp-87-98.
56.Tianfield, H.(2016), Cyber Security Situation Awareness .International Conference on Internet of Things and IEEE Green Computing.
57..Almaih, M. A. & Nafea,R.(2021), Cyber Security Threats in Cloud: Literature Review. International Conference on Information Technology (ICIT), pp-779-786.
58.Gautan,R.K. (2015), Importance of Cyber Security. International Journal of Computer Application Vol, 111.No,7.pp-14-17
59. Abass,N.N. et'al(2019), Investigating the applications of artificial Intelligence in Cyber Security.Scientometric.
57.El kenawy, S.T. et'al(2019), an Intergrated Framework to ensure Information Security. International Journal of Computer Application pp-1-3.
58.Arab, M.S.(2019), Role of Artificial Interlligence in Cyber Security .International Journal of Innovative Technology and Exploring Engineering (IJITEE) Vol,9. Issue, 1.pp-4628-4630
59.Nazir,S. et'al(2017), Assesing and augmenting SCADA Cyber Security : Survey of Techniques Computer & Security Vol,70. Pp-436-454.
60.Mynard,S(2018), Toward a Framework for Strategic Security Content in Information Security Governance. Pacific Asia Journal of the Association for Information Systems Vol, 10. Issue, 4.
61.Labuschagne, W. et'al(), Design of Cyber Security Awareness Game Utilizing a Social Media Framework.
62.Singh, H.L. (2019), A Review of Attack Graph and Attack Tree Visual Systax in Cyber Security Elsevier Computer Science.Vol.00. pp-1-46.