Investigating the impact of Cyberspace threats on electronic device users in Nigerian tertiary institutions (a Case study of IJBCOE, Sagbama)

Samson, Isobo D[*], Vincent, Tamaramiebi D [**], Apere, Tonubari [**]

[*] Department of Mathematics, Isaac Jasper Boro College of Education, Sagbama, Bayelsa, Nigeria.
[**] Department of Computer Science, Isaac Jasper Boro College of Education, Sagbama, Bayelsa, Nigeria.
[**] Department of Computer Science, Isaac Jasper Boro College of Education, Sagbama, Bayelsa, Nigeria.

DOI: 10.29322/IJSRP.13.06.2023.p13819
http://dx.doi.org/10.29322/IJSRP.13.06.2023.p13819

Paper Received Date: 11th April 2023
Paper Acceptance Date: 24th May 2023
Paper Publication Date: 6th June 2023

Abstract- The impact of cyberspace threats in the Isaac Jasper Boro College of education (IJBCOE), Sagbama, on electronic device users was investigated using both online and offline survey forms to obtain direct data from both staff and students. Analysis of the data with the percentage method revealed over 75% of the college population have experienced negative impact of cyberspace threat with fear, anxiety and embarrassment as the most prevalent impacts.

Index Terms- Impact, Cyberspace, threats, Electronic Device, Tertiary Institution.

I. Introduction

The 21st century is an era of technological advancement associated with electronic devices and internet collaboration to perform our daily tasks and interactions at school, work and home. The internet enables users to process, store, retrieve, and transfer various kinds of activities of data and information across global platforms ranging from personal data, education, sensitive business, health, science and engineering research, entertainment, military, entertainment, etc. Global usage and dependence on technology and the internet grow exponentially yearly which also demands a greater level of security and awareness for its users. Therefore, internet and electronic device users have a great responsibility to protect the integrity of data and information under their possession from unwanted access, theft, modification during processing, storage, and transmission. Hence, cyber-security is a shared responsibility that requires collective awareness and vigilance from all members of the internet community to defend and guard against online unauthorized attacks.

Cyber-security is the protection of computers and computer systems against unauthorized attacks or intrusion. Cyber-security threats evolve as rapidly as the internet evolves and expands and its associated risks are becoming increasingly global. [7] noted that cyber security is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance, and technologies that can be used to protect cyberspace and users' assets. Users' assets include connected computing devices, personnel, infrastructure, web applications, services, telecommunications systems, and the totality of transmitted and/or stored information in cyberspace [18].

According to Gary, [8], Staying protected against cyber security threats requires all users to be aware of the threats and improve their security practices daily. Users need to identify effective techniques to recognize cyber threats, risks, and vulnerabilities that exist and their impact on the internet community. This implies users should understand the five (5) W's (who, what, when, where, and why) in cyber risk analysis [13]. According to this report, cyberspace users need to know, **who** is sharing the cyberspace with them, **what** program they are using online, **when** can a cyberspace attack occur, **where** can a cyberspace attack be carried out and **why** cyberspace threats exist in the cyberspace.

There is no tertiary institution that is globally free from cyber risk but managements of these institutions can take efficient steps to minimize the chances of cybercrime occurrence by ensuring proper implementations of cyber security objectives (Confidentiality, Integrity, and Availability). Confidentiality can be defined as the protection of data and information from unauthorized attack, access, or disclosure. Ensuring that only authorized users gain legitimate access to data and information provided by the institution. Integrity simply refers to the protection of data and information from unauthorized modification and destruction. Integrity ensures that data and information remain complete, uncorrupted, and accurate. Availability ensures that data and information are made timely and reliably accessible or available to the users and protects it from unauthorized disruption but is available for efficient use by the employees of that institution.

In today's world, every tertiary institution around the globe has integrated electronic data processing into their daily activities and the processed data and information are shared with staff and students of that institution and with other institutions around the world. Educational institutions are facing risks of losing valuable intellectual property and their research data such as patents awarded to the professors and students, and also the personal data and information about the students, staff and the institution daily. Protecting the integrity, availability, and confidentiality of the tertiary institution information processed electronically is a complex task considering the high cyber-attacks rates. Because of the higher frequency of hacking attacks on institutions of higher education, the need for cyber awareness has increased.

A. Some Reasons Why Cyber Crimes Are Committed

[11] listed several reasons that catalyze the increase of cybercrime around the globe. Here below are some visible reasons:

1. Fun: The non-professionals commit cybercrime because of their desire to test the newest tools they have come in contact with for fun.
2. Recognition: technology world is engulfed with pride. This implies that if someone succeeds in hacking highly secured networks like defense sites/networks he/she takes pride and a success record on such achievement.
3. Cyber Espionage: government is sometimes involved in cybercrime by trespassing or keeping an eye over another country/network/person without its concert for economic, social, and politically motivated reasons.
4. Revenge: some are involved in cybercrime just for them to take revenge against a country/organization/caste/religion/person by bringing physical or economic loss or harming its reputation. This can also be placed under cyber terrorism.
5. Money: this cybercrime is most common because its primary motivation is to make quick and easy money.
6. Anonymity: it is easier to commit cybercrime and get away with it than commit any form of crime in the real world. Anonymity most times provide motivation for people to commit cybercrime in cyberspace and remain anonymous in the real world.

B. Problem Statement

Data and information value is driven by five critical characteristics (availability, accuracy, authenticity, confidentiality, and integrity). This implies that any modification made to this characteristic changes the value level of that information. Some of these characteristics have more effect level on information's value than others depending on the circumstances. However electronic devices and internet users share common grounds concerning securing the data and information value but tautness can arise when the need to secure the information from threats conflicts with the end users' desire or need for unlimited access to the information. Users become frustrated once they experience a delay in the data computation process, storage, and transmission of data and information.

Many developed countries understand cyber security as a matter of global interest and importance and have strategically defined policies, strategies, methods, and approaches to identify analyze and defend against cyberspace-related crimes. These cyber-related crimes range from cyberbullying, home automation, digital media, cyber terrorism, malicious hacking, insider threat (employee), fraud and theft, malicious code, identity theft, etc. However, many developing countries have failed to outline a unified approach and mechanism for combating cyberspace-related crime in their respective countries. Hence no proper government agencies whose sole setup purpose is to protect internet users and organizations/institutions from cyberspace criminals and bring them to proper justice. This gives leverage to cyberspace criminals to continually abuse/harass electronic devices and internet users and organizations/institutions in such countries.

Staff and students of tertiary institutions use the Internet for their daily activities. These activities include: online banking, virtual healthcare, communication, entertainment, education research, sport, etc. continuous connection to the internet and use of electronic devices cause an increased risk of cyber-attack. Every tertiary institution is faced with several cyberspace threats against its critical infrastructure, economic and social development. Therefore, tertiary institutions in Nigeria must provide means of protecting their information value at every level within their institutions

To address and expose cyber security threats in Nigerian tertiary institutions, there is a need for proper cyber security and cyberspace-related awareness program geared toward educating staff and students of tertiary institutions on current cybercriminal activities treading the globe. This survey study intends to create cyber security awareness among staff and students of tertiary institutions in Nigeria using Isaac Jasper Boro College of Education (IJBCOE), Sagbama, as a case study.

II. Literature Review

Globally cyberspace is evolving geometrically every day with new emerging technologies, techniques, and methodologies as a result of the human desire to simplify nature. Cyber-threats are also moving accordingly with the current trend of global cyberspace development by modernizing its approaches toward better cyberattacks. Cyber threats are one of the serious national security challenges facing various sectors of the national economy and development daily. Developing countries like Nigeria are one pure example where cyber attackers explore and prevail in their criminal activities without the proper mechanism to defend and enlighten their citizenry from cybercrimes. The educational sector is one of the common sectors which has a surface significant portion of this national security in Nigeria. Every tertiary institution in Nigeria is daily exposed to cyberspace threats and the challenge of securing its digital information value on both staff and students. This is as a result of the lack of awareness among staff and students about the several criminal acts that can be done with computers and electronic gadgets. There are several criminal activities performed under the high disguise of various degrees committed against computers, electronic devices and internet users that exist within Nigerian tertiary institutions.

Education invokes the hidden innovative capabilities of individuals in society. It has created dynamic opportunities for improvements in the social, political, economic and moral behavior of individuals in nations [5]. Every nation seeks to invest in its educational sector to stimulate national development [17]. According to [4], as the internet continues to penetrate more aspects of human activities in this modern era so are humans vulnerable to cyber victimization. [3] defined cybercrime as a criminal activity performed using electronic devices (computers, smart & mobile phones, etc.), communication networks (internet) and data with the main aim of exploring and extorting valuables from victims once a weakness is noticed. The Nigerian educational sector is not excluded from cyberspace threat attacks. The education sector has faced many terrible challenges from cyberattacks [16].

Cybercrime is committed by both old and young around the world. However, in Nigeria, the young recently seems to be the worst offenders. This young age range falls under [4] reported that Nigerian students are seriously involved in cybercrime in their quest for money rather than quality tertiary education. Several youths also involve in cybercrimes intending to become the best hackers, or for profit making since modern hacking tools have become available and affordable to any interested person. In Nigeria, one can easily associate the high rate of cybercrime to be caused by urbanization, corruption, unemployment and poverty [9].

[15] research showed the negative impacts of cybercrime activities done by students on school campuses which affect social equality, merit, and competence in the education sector. [1] also mentioned that these criminal acts in Nigeria's education sector have drained the quality of the education system, influence social and moral advancement, and impeded the sustainable development of the country.

[4] mentioned hacking, unauthorized and illegal access to bank accounts, identity theft, phishing, spoofing, unauthorized reading of emails, desktop counterfeiting, document forgery, pornography, cyber harassment, fraudulent conversion of property, chat room conspiracy, sending computer viruses, plagiarism, phreaking, and downloading unauthorized data as most common cybercrimes committed by students in Nigeria tertiary institutions [4].

[10] added cyber-laundering, prohibited/illegal content sharing, cyberbullying, ATM fraud, cyber extortion, crypto-jacking, cyber espionage, software piracy, phishing and cyberstalking to the list of cybercrimes commited by youths in tertiary institutions. Their research adopted Ex-post facto design method to determine the involvement of tertiary institution students in cybercrime in Imo state. They noted the importance of taking precautionary measures for students while using the internet to avoid being a victim of cybercrime. They also raised the need for federal, state and education communities to adequately orient Nigerian undergraduate students about cybercrime, cybersecurity, and punishment under the criminal act. The rate at which Nigerian students are involved in these various forms of cybercrime calls for urgent concern [14]. [4] research showed that cybercrime offenders are not farfetched. They are our friends, neighbors, relatives and colleagues who can be curbed under appropriate circumstances with the right orientation, education, communication and empowerment. The research called on the government to institute effective risk management, enhance the capacity to carry out a forensic investigation to tackle cybercrime and collaborate with corporate entities and citizens to checkmate cybercrime.

[12] conducted structured survey research on the implications of technological advancement concerning the internet on educational development (effect of cybercrime on education) using the chi-square test method to analyze the collected data. He recommended that cyber-related crime sensitization campaigns in schools are key to protecting information values and adopting good security protocols and rigid regulations. [6] research study adopted a questionnaire fact-finding approach to analyze the common prevailing cyber-related crimes within Nigerian tertiary institutions using Usmanu Danfodiyo University as a case study. The study recommended government intervention in providing basic amenities and individuals taking responsibility to ensure adequate security of their computer systems as measures of preventing cybercrime. In all of the works considered, we found out that non considered the impact of these cybercrimes on the victims. Thus, this article is to expose some of the impacts of cyber-threats on electronic device users in the mentioned institution.

However, every tertiary institution comprises of academic staff, non-academic staff and students. Both the academic and non-academic staff can be offenders and victims of cybercrime like the students. These staffs are actively involved in the daily administration and running of every section or part of the institution using diverse modern electronic devices and the internet. It is important to note that several successful cybercrime activities in tertiary institution environments can be attributed to a lack of awareness, inability to identify cyberattacks, and lack of prevention skills of most academic and non-academic staff. Our data revealed that many people within the Nigerian tertiary institution community have heard about cybercrime and cyber security but only a few have considered ways of protecting their electronic devices and themselves while using the internet. This may be so because Nigerian tertiary institutions have not given critical thought to the importance of staff and students protecting themselves and their electronic devices against cyberspace threats and attacks as a means of securing themselves from cybercrimes. If a staff or student is adequately oriented, educated or enlightened about cybercrimes and cybersecurity it will help him/her to identify attacks and apply the right protective measures on his/her devices and the institution's information value under his/her care and promptly report such attacks to the institution management. Hence this research is to investigate the impact of cyberspace threats on electronic device users (academic, and non-academic staff and students) in Nigerian tertiary institutions.

A. *Cyber Threats*

[19] identified over twenty criminal activities done with the aid of computer and electronic technology. Some of them include bank accounts, identity theft, phishing, spoofing, desktop counterfeiting, document forgery, pornography, cyber harassment, fraudulent conversion of property, chat room conspiracy, sending computer viruses & worms, plagiarism, phreaking, downloading unauthorized, cyber-laundering, prohibited/illegal content sharing, cyberbullying, ATM fraud, cyber extortion, crypto-jacking, cyber espionage, software piracy, system Hacking, Cyber Terrorism, and cyberstalking, Direct-access attacks, Computer Vandalism, cyber bullying and social media account hacking.

B. Malicious Software (malware)

Malware is a software designed to gain unauthorized access or install unhealthy software to a computer without the user's consent. The third-party computer is the main beneficiary by launching indirect attacks on the host computer. Malware is written to perform various degree of attacks to capture sensitive data from the host computer and send to its remote servers. It can distract and annoy the host computer user. According to [11], the most popular malware types present on the internet are Adware, Spyware, Browser hijacking software, Scareware, Virus, Worms and Trojan horse.

III. Methodology

This research adopted online and offline questionnaire survey methods. A sample size of 150 respondents drawn from staff and students of IJBCOE was obtained and analysed. A Google survey form (questionnaire) was produced and sent to the social network (What's App) groups of staff and students within the college community and the printed hard copy of the form was also distributed to randomly selected staff and students at the college to cover for those who may not have access to the group questionnaire online. Statistical analysis of the data was done and presented as charts. A high percentage, say above 60 percent, of occurrence of a particular event affirms its possible occurrence and a low percentage reported a rare occurrence. The percentage method was used since all our data was finite with variables independent.

IV. Results and Discussion

From the survey data collected and analyzed 80% of the IJBCOE college community has knowledge about cyberspace security and cyberspace related crimes. 54% of the college community was found to have experienced at least one form of cyberspace related crime. The survey showed that adware, phishing, digital media piracy, document forging and counterfeiting, browser hijacking, device hacking, social media account hacking, virus, worms, and identity theft are the most prevalent cybercrimes committed within the college. Scareware, spoofing, repudiation, and spyware are non-prevalent cybercrimes at the college. The survey also showed that 91% of the college community has experienced social media account hacking. The percentage distribution of the prevalent online abuses experienced in the college community is as presented in chart-1 below. The result showed that harassment is the most common online abuse followed by threats while, violence and minor sexual harassment are the least experienced. It further revealed that a very minute number of persons have not experienced any form of the cyberspace abuses in question.

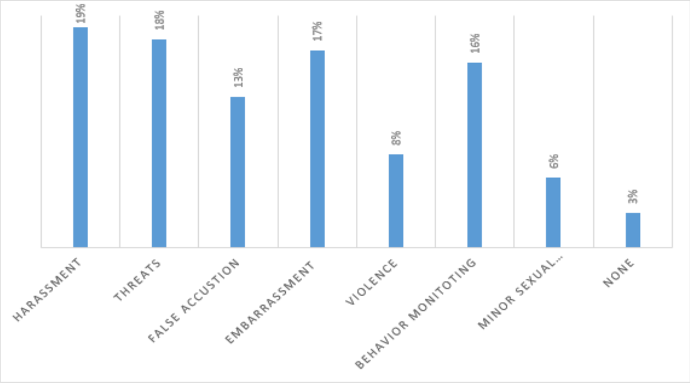

Chart-1: Prevalent online abuses experienced by staff and students at IJBCOE Sagbama.

Victims of cyberspace threats go through different situations both on themselves and their devices. Some negative impact of viruses and worms on victims' electronic devices in the college community are shown graphically in chart-2. The most common effects are corruption of files (denial of access to file) and file deletion while the least is that of uncontrollable sounds and music from system. These experiences could cost academic, non-academic staff and students loss of productive time, loss of valuable information and resources at the college.

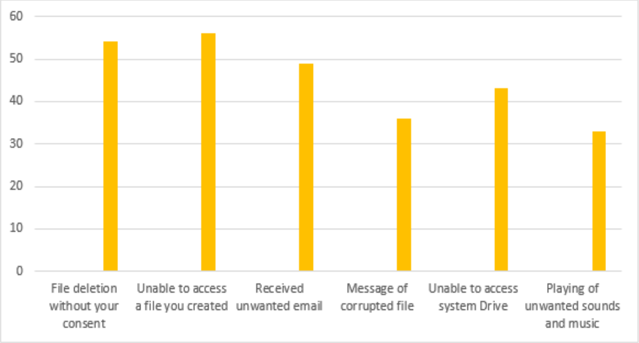

Chart-2: Virus and worms impact on electronic devices at IJBCOE Sagbama

The study also revealed that the identified prevalent cybercrimes in the college community have great impacts on the academic and non-academic staff and student's finances, education, health, relationships, and others as shown in chart-3 below. Impact on victim’s finances has the highest figure of 27% while impact on health has the lowest rating of 8%.

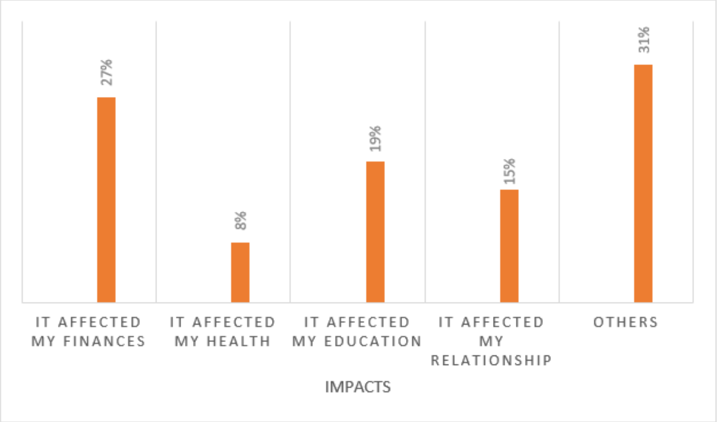

Chart-3: Cybercrime Impact on the Life of Electronic Devices and Internet Users at IJBCOE.

The study revealed that these impacts shown in chart 1-3 created negative psychological impacts on electronic devices and internet users. Victims of cybercrime within the IJBCOE college community have to deal with depression, anxiety, fear, loss of self-esteem, guilt, anger and embarrassment. Chart-4 shows the psychological behavioral impact on electronic device and internet users who were victims of cybercrimes at the college in one way or the other.

http://dx.doi.org/10.29322/IJSRP.13.06.2023.p13819

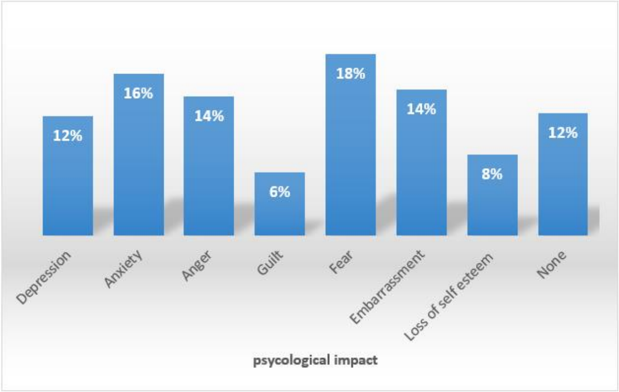

Chart-4: Cybercrime psychological impact on electronic device and Internet users at IJBCOE.

V. CONCLUSION

The rate of cybercrime at tertiary institutions in Nigeria is growing speedily. Staff and students must protect themselves and their information value at his/her position. It is the responsibility of the management to adequately provide a platform for the institution community (staff and students) to be properly educated or enlightened on cyber security and cyber-related crimes. The best way to fight against cybercrime in Nigerian tertiary institutions is through regular awareness and enlightenment campaigns (such as cyber security workshops, orientation programs, staff training, etc.). We recommend Nigerian tertiary institutions should ensure periodic cyber security and cyber-related crime awareness and enlightenment platform for staff and students. Nigerian tertiary institutions should create a department to handle cyber security issues, cyber risk management, cybercrime reporting, victim counseling and offender prosecution. Nigerian tertiary institutions should consider basic computer studies in their curriculum design as a general study course which should include cyber security and cybercrime as part of the course content.

ACKNOWLEDGEMENT

This search was sponsored by Tertiary Education Trust Fund (TETFUND) Abuja, Nigeria.

REFERENCES

[1] Abraham, N. M. (2011). Functional education, militancy and youth restiveness in Nigerias Niger Delta: *The place of multi-national oil corporations (MNOCs). African Journal of Political Science and International Relations, 5(10), 442-447.*

[2] Afrozulla K. Z, Vaishnavi R. T., & Arjun, (2018). Cyber Crime Awareness among Msw Students, School Of Social Work, Mangaluru. *Journal of Forensic Sciences & Criminal Investigation Volume-9 Issue2 DOI:10.19080/JFSCI.2018.09.555757*

[3] Aghatise, E J. (2006). Cybercrime definition. Computer research centre. https://www.researchgate.net/publication/265350281

[4] Akpan, E. E., & Friday, E. P. (2021). The effect of cybercrime on the educational system of Nigeria. *Gaspro International journal of eminent scholars, vol.7, no.2, Germany.*

[5] Chimombo, J. P. (2015). Issues in basic education in developing countries: An exploration of policy options for improved delivery. *Journal of international cooperation in education, 8(1), 129-152.*

[6] Daniel D. W., Mairiga B. R., Abdullahi B. A., Ebenezer A. A., Danjumma B., (2020). Combatting cybercrimes in the education sector. *International Journal of Engineering Applied Sciences and Technology, Vol. 5, Issue 4, ISSN No. 2455-2143, Pages 108-117. http://www.ijeast.com*

[7] Douwe Korff, (2019). Cyber security definitions - A selection. *Associate of the oxford martin school of the university of oxford's global cyber security capacity center.* Douwe@korff.co.uk

[8] Gary Locke, (2011). Cyber security, innovation, and the internet economy. *The department of commerce internet policy task force.*

[9] Hassan A., Lass F. & Makinde J. (2012). Cybercrime in Nigeria: causes, Effects and the way out. *ARPN Journal of science and technology, 2(7), 626-631*

[10] Iwuji F. I., & Amah K. O., (2021). The Implications and Remedies of Student Involvement in Cyber-Crime: Empirical Survey of the Students of Tertiary Institutions in Imo State. *Gaspro international journal of eminent scholars, vol.7, no.1, Germany*

[11] Jeetendra Pande, (2017). Introduction to Cyber Security. *Uttarakhand Open University, http://uou.ac.in*

[12] Azuka Josephine O., (2018). Cyber crime and its implications for educational development in Nigeria. *International Journal of Multidisciplinary Research and Development Online ISSN: 2349-4182, Print ISSN: 2349-5979*

[13] Homeland Security (2016-2021) National Cyber Security Strategy, progress report. https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national_cyber_security_strategy_2016.pdf 13/5/2023 9:56pm

[14] Ngozi, S. (2016). Students' perception of cybercrime and its implications. *Journal of Social Development, 4(2), 50-57*

[15] Nwaokugha, D. O. & Ezeugwu, M. C. (2017). Corruption in the education industry in Nigeria, Implications for national development. *European Journal of Training and Development Studies*, 4(1), 1-17.

[16] Ololube, N. P. (2016). Education fund misappropriation and mismanagement and the provision of quality higher education in Nigeria. *International Journal of Scientific Research in Education, 9(4), 333-349.*

[17] Ozturk, Ilhan (2008), The Role of Education in Economic Development: A Theoretical Perspective. *http://dx.doi.org/10.2139/ssrn.1137541*

[18] Rossouw von S., & Johan van N., (2012). From information security to cyber security. *School of ICT, Nelson Mandela Metropolitan University, Port Elizabeth 6031, South Africa*

[19] Sumitra K. & Chandrasekhar R. (2017). Information Security Lecture Notes. *Department of Computer Science and Engineering & Information Technology, Veer Surendra Sai University of Technology Burla, Odisha.*

AUTHORS

1. Samson Isobo D., B.Sc., M.Sc. Pure & Applied Mathematics,
Isaac Jasper Boro College of Education, Sagbama.
isosamdigi@ijbcoe.edu.ng
2. Vincent Tamaramiebi D., B.Sc., M.Sc. Computer Science,
Isaac Jasper Boro College of Education, Sagbama.
vincotams@gmail.com
3. Apere, Tonubari, B.Sc. PGDE,. Computer Science, Isaac
Jasper Boro College of Education, Sagbama.
akekuetonubari@yahoo.com

http://dx.doi.org/10.29322/IJSRP.13.06.2023.p13819