RESEARCH ARTICLE

DOI: 10.34256/ajir20114

ASIAN JOURNAL OF INTERDISCIPLINARY RESEARCH

Cybercrimes: Threats, Challenges, Awareness, and Solutions in Sierra Leone

Ibrahim Abdulai Sawaneh [a,b] *

[a] Department of Management Science and Engineering, Wuhan University of Technology, Wuhan, PR. China

[b] Department of Computer Science at the Ernest Bai Koroma University of Science and Technology, Magburaka, Sierra Leone,

*Corresponding author email: ciddiisawaneh@hotmail.com

DOI: https://doi.org/10.34256/ajir20114

Received: 24-01-2020
Accepted: 09-03-2020

Abstract: The internet hosts all online activities either for public or private usage. It is a powerful online podium where people socialize, make new friends, conduct academic research, perform online business transactions, share sensitive data, communication over the internet, surveillance purpose by security agencies, monitor climatic condition, used in e-healthcare system, online banking, online pay, e-commerce, defense system, and host of others critical infrastructures are the new order of the day. This has attracted online criminals to diverse numerous malicious techniques to invade people's privacy and also exploit those data. A new game has resulted in these online malicious activities are known as "cybercrime or internet crime" which is a rewarding business as of today. Therefore, it has become difficult to protect those online activities as cybercrimes are growing daily, which suggests that effective and appropriate countermeasures are needed to combat those threats and make online activities more secure. The research paper presents the various types of cybercrime activities, countermeasures, and suggestions for online users.

Keywords: Cybercrime, Cyber-Law, Cybercriminals, Cyberspace, Hacking.

1. Introduction

Today's humans largely depend on technology to perform their numerous duties ranging from household chores to office tasks via the internet. This is proven as we largely see in government and private institutions using internet-related technologies as the backbones of those institutions; such as airports, railway stations, aerospace industries, manufacturing industries, healthcare sectors, nuclear power plants, defense industries, educational sectors, e-commerce industries, online financial institutions, surveillance systems, immigration departments, and several other vital infrastructures. Furthermore, the increase in social media applications used for communications and other purposes are other benefits of the globally interconnected communities. Citing Newton's Laws of Motion, *"For every action, there is an equal and*

opposite reaction". This implies that every technology has both merits and demerits. The internet also provides both good and bad as there are good people and bad people who use cyberspace. Cyberspace uses electronics and electromagnetic spectrum for storing, modifying, and exchanging data through a network of networks connected to several physical infrastructures. Cybercrimes have increased drastically despite the preventive measures adopted by governments, individuals, and private organizations in the last five years. This is attributed to the fact that as technologies improve, so do the people using them to break new grounds on how to misuse them. Cybercrime is associated with the doing of a malicious act to commit online fraud which is against the cyber ethics for which the culprit is liable to be punished upon a verdict depending on the geographical location (Hemraj Saini et al, 2012). It is also an online criminal activity that targets computing systems, database systems and other online platforms with malicious intention; such as manipulating sensitive data, stealing of important data stored on a computer or online, and gain competitive advantage over their opponents for financial gain or sabotaging their opponents' computing systems and data.

Cybercrime is a lucrative business that is growing fast since 2010. The online criminals extort valuable data that worth millions of U.S dollars with greater anonymity that has no geographical boundaries either virtual or physical that negatively affects internet users globally. Cybercrime can comprise of any act to commit financial frauds and non-financial crimes including online bullying, designing programs that inflict viruses on computer systems, and/or disclosing sensitive financial records of others on the internet (Richard Donegan, 2012; Harpreet Singh Dalla, Ms. Greeta, 2013).

Cybercrime needs to be addressed as the world has embraced technological innovations in all sectors of human activities. Most nations today virtually relied on the internet to do almost everything and this poses great challenges to data privacy and data protection. Several governmental agencies including the Office of the National Security (ONS), Ministry of Information and Communications, the Cybercrime Unit of the Criminal Investigation Department (CID) of the Sierra Leone Police Force, the Military Force, the Mobile Network Operators (MNO) and other private sectors in Sierra Leone. These agencies are working together to establish strong laws on cybercrime within Sierra Leone. A reporting mechanism of cybercrimes and cyber abuse should be reported to the appropriate authority and defaulters should be penalized according to the laws governing cybercrime and information security in Sierra Leone. The paper discusses the types of cybercrimes, its preventive measures, and other related topics.

The rise in cybercrime globally in the last two decades has caused a series of problems costing billions of U.S dollars. It is being viewed as a lucrative business where the cybercriminals target their victims anonymously using malicious online software that hides their online activities (Vineet Kandpal and ** R. K. Singh, 2013). Furthermore, with the introduction of "Bitcoins" as a form of online payment method, has empowered cybercriminals to further exploit online users. Moreover, the rapid innovations in technology and sciences pose great challenges to security and data privacy, though it also exhibits positive outcomes, such as making life comfortable. Therefore, the research is conducted to provide the basic techniques that will prevent online users from being targeted by cybercriminals, and possibly minimize such cyber-attacks.

2. Research methodology

The research uses a descriptive methodology and employs secondary data only. The secondary data consists of related

journal articles, internet, and textbooks on cybercrime and cybersecurity.

3. Various Forms of Cybercrimes

Cyber-Stalking

Cyberstalking involves harassing online users via an electronic communication platform to commit a crime, and examples include; email, instant messaging (IM), social media group messaging apps, and/or messages posted onto a website. The attacker uses malicious software to hide his/her online identity without being exposed to inflicts damage to the victim(s).

Cyber Defamation

Cyber defamation is an act conducted using the internet to slander, tort or defames mostly important personalities in societies, which has not yet been labeled a criminal offenses, but it depends on the country where such activity is been committed, as the cyber-laws varies from nation to nation. Punishments for 'Cyber defamation' is different from country to country, as indicated by the fundamental rights enshrined in the "UN Declaration of Human Rights" and "European Union Fundamental Human Rights".

Hacking

Hacking is unauthorized access to a computing device to view, copy, or create data with a trace with the intention of not destroying the data or damaging the computing device. Humans live in a globally connected cyber environment where almost all devices are interconnected either directly or indirectly via the network of networks "the internet". Unfortunately, no system is 100% secure from a security threat, some internet users just make it easy for hackers and attackers to infiltrate into their systems. They forget that they (users) and cybercriminals use the same source (internet), where they are exploited knowingly or unknowingly. A hacker is anyone with the technical knowledge and expertise who intrudes into a system in an unauthorized manner. A security hacker is someone who uses his/her knowledge to break into a computer system. They are also known as crackers (Lee, M. 2015). This normally results in substantial financial loss and identity theft. These hackers deploy malicious malware in various forms to take away important credentials, steal valuable information, search for a systems' back door, or "use you" to make an even a bigger gain, they must first get you or your computer to do something maliciously, like executing a code (Taylor et al, 2015).

Cracking

Cracking is the act involving the unauthorized permission to a computer to inflict damage to it, and those engaged in such activities are called "cracker".

E-Mail Spoofing

Email spoofing is common nowadays in electronic communications. Online Fraudster design email messages to falsify the sender's address, to get the receiver to respond, thereby completing the attack. Once the recipient accepts the challenge, the cybercriminal launches an attack.

SMS Spoofing

SMS spoofing, which is somewhat a new innovative technology, utilizes the "Short Message Service" (SMS), using "mobile phones" and "Personal Digital Assistants" (PDAs), to trick people as if the messages are coming from whom it should come from, by hiding the original mobile number (Sender ID)

with alphanumeric text. It has both positive and negative effects.

Spoofed Domains

It usually occurs as a result of either compromising a DNS or due to typographical errors deployed to exploit online users. Just typing a wrong letter turns a website into a hostile ecosystem. Failing to realize such a mistake, will expose your systems' vulnerabilities which hackers will capitalize on and hack into your systems.

Carding

It is a kind of online fraud where a credit card is stolen and used to charge pre-paid cards. Carding normally implicates the holder of the stolen card buying store-branded gift cards, which can then be sold or used to secure other goods to castoff, and those involved in such activities are called "carders".

Bot Networks

A botnet network is infected networks that compromise several computers allowing an attacker to control them. Some malware tends to transform a victims' computer into zombies and use the infected machine to launch an attack against other systems. Sometimes, they will result in colossal denial of service attacks, they might be used to break into other machines either through brute force or distributed cracking.

Intellectual Property Crimes

Intellectual property (IP) theft is the act of stealing copyrighted materials including trade secrets, trademarks, and other vital copyrighted. A copyright is a lawful right accorded to the owner of original work, such as publisher, storybook, composer, artists or musicians, to replicate it, normally for a limited time.

Cybersquatting

Cybersquatting (domain squatting) by the U.S Federal Law called "Anti-Cybersquatting Consumer Protection Act", register, transfer in, or use the internet domain name to extort benefit from the benevolence of someone's trademark. The cyber-squatter normally bargains to trade the domain to the person or organization owning the trademark enclosed within the name at a magnified rate.

Cyber Vandalism

Vandalism is the intentional act to destroy or damage a property belonging to others, and cyber vandalism referred to the act of destroying or damaging data on a network when is stopped or disrupted. It may comprise any type of physical mischief done to someone's computer. Such acts include stealing someone's computer, a computer part or a peripheral attached to the computer.

Cyber Trespass

Trespassing refers to entering into someone's property without his/her permission. It normally involves a deliberate act to commit a crime by encroaching or infringing people's assets (land or property) without due permission. Criminal trespass involves the act to commit a crime, and that involves using cyberspace is called a "Cyber Trespass".

Internet Time Thefts

It is related to hacking, involving the use of the internet to ascribe browsing hours to others by accessing the ISP user ID and password illegally without the other person's knowledge.

Online Gambling

Online gambling is a big business around the world where a bet is placed, received or channeled via the internet, but which does not involve the performance of the customary doings of a financial transaction provider, or computer service or telecommunications provision.

Fraud and Financial Crimes

Computer frauds are any mischiefs or fraudulent activities trigger to cause harm or prevent harm from happening. It can provide benefit by:

- Unauthorized data manipulation – It normally occurs with skilled and talented employees who illegally manipulate data in their favor before having access and/or use unauthorized processes.
- Manipulate, alter, destroy, suppress, or steal sensitive data generally to hide unlawful transactions without been detected.
- Changing or deleting stored data.

Cyber Extortion

Cyber extortion happens when a website, e-mail server, or computer device is experienced a constant denial of service and/or other attacks inflicted by mischievous online criminals. It is similar to the ransomware attack, where the cyber-extorters demand a financial reward and promise to halt the attack and to provide "protection".

Computer Virus

A computing system infected with a virus (s) should never be trusted because it has already been compromised or breached. For most sysadmins, the appropriate action is to dust off and nuke it from high orbit; meaning format and reimage the machine. Essentially, a computing system should always be backup to prevent breakdowns in operations. A virus is released onto a computing system when malicious online users target their victims.

Phishing

Phishing attacks occur when malicious attackers insert malware into someone's machine with the help of the internet. Luckily, it can be easily be stopped if users would carefully pay attention. Phishing attacks are frequent with the fact that they are most successful. Sometimes clicking on malware especially when you want to download a file or software on the internet, it redirects you to another webpage before downloading. It almost always occurs daily.

Cross-Site Scripting

Cross-site scripting attack allows online fraudsters to insert client-side scripts into weak web pages upon clicking grants their browser to execute the scripts. Hackers deployed them to snip personal data or download and install malware.

Malicious Links

The majority of the internet users normally click on malicious hyperlinks in their emails, webpages or forum post. Attackers sometimes insert a malicious link into a discussion thread and wait for a possible victim to click on it. It may sometimes be attack-free or execute malicious code into a webpage.

Network Sniffer

A network sniffer is a tool used to detect network problems thereby allows an individual to capture and view the packet level data on the network. According to the International Space Station (ISS), it is a tool that exploits the network interface of a computer to intersect data packets meant for other computers. It is also known as network monitors and analyzers, and also collect packet-level data and information.

Owned Websites

Some websites are usually owned by malicious online fraudsters designed to lure people into trusting such websites or hack into genuine websites to cause mayhem. They either motivate users to visit their fate websites or are already hacking into those websites via their homepage, favorites, and bookmarks.

Malicious Scripts

Most webpages contained JavaScript with malicious code making the browser vulnerable and thereby granting admin rights to the users provided the browser lacks proper anti-malware software installed. Therefore, for you to be on a safer side, without you permitting attackers to compromise your machine, you need to first install anti-malware software to prevent an attacker infiltrating into your machine. Modern internet does not require a specific scripting engine that downloads and runs the code. The user needs just to visit a page. You execute JavaScript nearly every time you visit a website.

Infected Files

Most internet users in Sierra Leone and elsewhere sometimes download malicious links containing malware that infect their files; such links or sites include screensavers and media codecs to name a few that hackers post containing malicious code. When internet user downloads and runs them, they immediately become prone to attack and they are referred to as a “potential victim”.

Embedded Media

Webmasters always insert media archives that online users normally click, and in turn, infects the whole webpage and make it vulnerable to attacks. Media players just like an OS regularly require an update. Unfortunately without proper patch implementation, it would be almost not feasible for users to keep their systems up-to-date.

Credit/Debit Card Fraud

Credit card fraud is an online theft and fraud done via an online payment card (credit or debit cards), with a fraudulent intention in an online transaction. The key motive is to acquire goods without payment or to get unauthorized funds from an account.

Identity Theft

Identity theft is the act of stealing or amassing enough information about someone’s identity including email address, name, date of birth, place of birth, residential address to commit identity fraud. Identity theft may occur either the victim is alive or deceased.

Cyber Bullying

Cyberbullying is the act of using electronic communications to intimidate or bully their victims, and it is done by transmitting intimidating or threatening messages to the oppressed victims (Richard Donegan, 2012).

Cyber Terrorism

Cyber terrorism is a kind of terrorist activity triggered via the use of the internet, mostly premeditated or politically motivated mischiefs against information, computing systems, and programs, resulting in chaotic situations against civilians perpetrated by malicious sub-national groups or individuals.

Harassment via E-Mails

Email harassment normally occurs when malicious online users continuously send unwanted electronic messages to others, and most often threatening. There isn't always an exact definition of what a message has to look or sound like to be harassing. It's usually a matter of circumstance since what one person finds offensive or harmful may not come off that way to someone else.

Pirated Software

Software piracy is the unauthorized copying, dissemination, transfer, or use of the software. It is a lucrative business prompting several organized crime groups around the world.

Child Pornography

Child Pornography is a criminal offense punishable by law in many countries. It is any pictorial representation relating to the use of a minor, or one appearing to be a minor, engaging in sexually clear conduct. Since technology moves much faster than legislation, crimes committed via social media are often prosecuted by applying existing statutes.

Several studies have been conducted relating to the potential effect of online pornography concerning the youth, assuming the high rate of exposure, and vulnerabilities among the youth including depression, interpersonal victimization, and delinquent tendencies, have more exposure.

Denial of Service Attacks

A denial-of-service (DoS) attack occurs when a cybercriminal attempts to make a machine or network inaccessible to its legitimate operators by temporarily or indefinitely disrupting services of a host linked to the internet. DoS attacks are normally done by "flooding" the resource with a large number of requests (Anand Kumar Shrivastay, Dr. Ekata, 2013). This limits the server to reply to some or all authorized requests. Legitimate users who want to utilize the pool of resources are denied access to those resources. A single DoS attack is easy to manage, and a distributed denial-of-service attack (DDoS attack) originating from several sources. DDoS attacks involve several computer users willingly joining hands together to take an active part in the attack. The DDoS attack is generally orchestrated using botnets - networks of breached computers whose users are unaware that their machines are partaking in an attack.

Malicious online users normally attach high profile web servers, sites or services – online payment methods with credit card facilities, banking facilities, revenue collection departments, or blackmailing (Prince, Mathew, 2016) with malicious software installed on computers that grant a third-party total control of the system.

Website Defacement Attack

A website defacement attack is a technique that manipulates a website content without prior knowledge of the web administrator. This happens when an attacker disrupts a particular website, modifies its contents to deceive people who visit the site. It is electronic vandalism to motivate cyber protesters or hacktivists (Romagna, M.; Van

Den Hout, N. J. 2017). Several religious and government websites are breached by political or religious-inspired cybercriminals to spread political or religious beliefs to deface the views and beliefs of others.

SQL injection technique occurred in website defacement intrusion. The invader inserts malicious data in a web form according to Thomas Steinbrenner. Traditionally, SQL injection is easy to protect, as a result of a programming error on the website. However, in practice, several websites are exposed due to negligent security practices. In contrast, in DDoS attacks, a website defacement refers to a situation in which an intruder gains access to a target computing system. However, gaining access to an organization's web server is different from breaking into that organization's internal network, because webservers are normally hosted on a different network.

Other Break-Ins

Break-ins is a process where an attacker breaks into a system than a webserver or break into webservers that store data than a public website. Such break-ins happen using methods analogous to those applied in website defacement. It depends on the level of IT security on the intended computer. Once an intruder is granted access to a computing system, he will be granted access to other computers within the same network stealing sensitive data, and install malicious apps that turn the machines into zombies for a botnet, or cause other destructions.

Cyber Attackers

Several governments are faced with numerous challenges with regards to Cybersecurity. Findings indicate a surge in hacks and breaches of data globally. Studies further indicate that most organizations' data are not protected as a result of poor cybersecurity practices, and make them vulnerable to data loss (Saroj Mehta & Vikram Singh, 2013).

Hacktivism

Hacktivism originates from two terms "hacking" and "activism". The online criminals who participate in hacking activities to penetrate computing systems or networks illegally for either social or political gain.

The rise of hate speech or radicalism through digital and social platforms across the globe has negative consequences: the Arab Spring of the Middle East, the green revolution in France (2019), several mass shootings (Texas and Ohio, 2019) in the U.S, the in the Sri Lanka bombing in April 2019, the Christchurch mosque massacre in New Zealand are perpetrated using live stream using social networking sites (Periscope, Facebook, Twitter) with online users participating in the online debate. Mayor Ada Colau of Barcelona amassed massive online support approximately 6,000 people for his electoral campaign in the public assemblies, with the establishment of the network of cyber activists.

They attack influential and powerful people's computer networks anonymously and sometimes terrorize organizations. The Panama Papers exposures by WikiLeaks and Edward Snowden are referred to as "hacktivism". Her documents are amassed, leaked and spread through the internet with political ramifications. The Panama leaks orchestrated massive protests making the Iceland Prime Minister quit office and calls for similar action in the U.K.

Cyber Espionage

Espionage is an effort made by either an individual or state to extract sensitive information from a rivalry state or individual organization. Cyber espionage is acceptable behavior as compared to cyber-attack, which is unacceptable behavior per international law.

Several objections have been among the world powers against unacceptable cyber espionage prompting fear of a new era of informationalization and digitalization war. Furthermore, the U.S has been advocating for new standards for cyber espionage, permitting nations to practice it only for traditional intelligence purposes to make critical national security actions. Cyber espionage is becoming a normal order of the day among the world powers. An ex-CIA agent pleaded guilty spying for China, according to the U.S justice department in May 2019, as the main reason believed for dismantling the U.S espionage network.

Prosecutors indicated that Jerry Chun Shing Lee was financially motivated to disclose information on the U.S covert assets. About 20 informants were murdered or jailed between 2010 and 2012 becoming most catastrophes in the U.S intelligence in modern times.

4. Discussions and Results

Sierra Leone, which is an emerging and third world country along the west coast of Africa has little foundation in sciences and technology. It just started embracing technological innovations immediately after the civil war that ravaged the country for 11 years in 2002. The government in the last decade has embraced technological innovations and sciences, which is evident in all government ministries having a separate department for IT officers, web administrators and software analysts to design, develop, store, maintain, monitor, and protect data about those departments or institutions.

Cybercrime is a global phenomenon and has no boundary when it comes to cyber-attack. Even the most advanced nations are not exempted from being inflicted by cybercriminals. Cybercriminal may even be your very employee, or business partner and/or your rivalry institution. This means it is very difficult to prevent it from occurring 100%. It should involve all stakeholders in the society including government, civil society, private sector, GSM operators, and the citizens of the global village. Furthermore, massive cyber education is required to better prepare internet users in the country to learn the basic techniques on how to protect their online data and activities. Cyber courses should also be introduced in schools, colleges, and universities to raise cyber awareness among online clients.

Based on the research conducted, about 80% of online clients in Sierra Leone lack the basic skills and techniques to protect their online activities against cybercriminals and hackers. Only 10% of people who frequently used the internet know the basic knowledge and impact of cybercrimes. About 10% of online users remain neutral.

For the government of Sierra Leone to protect the country's cyberspace, strong cyber-laws should be enacted, and perpetrators of such an act should be severely punished with fines and imprisonment. Moreover, those agencies in charge of protecting the nations' information, should be given the required training and education to be able to fight cybercrimes and cybercriminals. Also, a global cyber – laws that could encourage all nations to fight the common enemy; cybercrimes and cybercriminals.

Figure 1 Cyber perception in Sierra Leone

Category	Percentage (%)	Comments
No cyber knowledge	80%	Population with no knowledge on the impacts of cybercrime
Cyber knowledge	10%	People with cyber knowledge
Neutral	10%	People who have either knowledge or no knowledge of cybercrimes in the country

Survey result of 2019

5. Conclusion

The world today is a hostile cyber environment where individual or entity and/or individual nations conduct espionage activities either to gain competitive advantage or for financial gain. Most nations in Africa including Ghana, Kenya, Uganda, South Africa, Nigeria, and the industrial world have applied tougher policies to fight cybercrimes. Sierra Leone as a nation needs to move at a faster pace to provide a safe and secure cyber ecosystem that will fascinate prospective investors into the country.

Furthermore, if strong cyber laws are legislated, it will help boost the economy and alleviate poverty, and also improve on the lives of average Sierra Leoneans. The government should also embark on massive sensitization on the use of the internet, and how to protect their personal and government sensitive information from cybercriminals.

6. Recommendation

The following recommendations are highlighted by the researcher as a way to mitigate cybercrimes within Sierra Leone:

1. Strong cyber – laws should be legislated and culprits punish per the laws of Sierra Leone;
2. The global community should also legislate universal cyber – laws that would govern all nations on planet earth;
3. Cyber education and awareness should be incorporated into schools, colleges, and universities by the Ministry of Basic Education, Ministry of Higher and Technical Education and Tertiary Education Commission of Sierra Leone;
4. Regular workshops/seminar/training should be conducted for all security apparatus within the country;
5. All GSM operators within the country should carefully monitor their clients' activities and report to the appropriate authorities if found wanting of any related cybercrime offenses;
6. IT officers should be incorporated in all government departments and private sectors within the country;
7. The central bank of Sierra Leone should monitor all online financial transactions conducted by the various banks in the country;
8. The government should also invest heavily in scientific and academic

researches and ensure that all universities in the country make research as a key aspect of teaching;

9. The government should finally identify potentials and awarded them scholarships to study abroad in world top universities and return home to implement those morals in our educational sectors.

References

Anand Kumar Shrivastav, Ekata, (2013) ICT Penetration and Cybercrime in India: A Review, International Journal of Advanced Research in Computer Science and Software Engineering, 3, 414-419.

Harpreet Singh Dalla, Geeta, (2013) Cyber Crime – A Threat to Persons, Property, Government, and Societies, International Journal of Advanced Research in Computer Science and Software Engineering, 3.

Hemraj Saini, Yerra Shankar Rao, Panda, T.C., (2012) Cyber-Crimes and their Impacts: A Review, International Journal of Engineering Research and Applications, 2, 202-209

Lee, M. (2015). The evolution of cybercrime: From Julius Caesar and Prince Philip to state-sponsored malware. International Business Times. Retrieved from: http://ibtimes.co.uk.

Prince, Mathew (2016). Empty DDoS Threats: Meet the Armada Collective". Cloudflare.

Richard Donegan, (2012) Bullying and Cyberbullying: History, Statistics, Law, Prevention, and Analysis, The Elon Journal of Undergraduate Research in Communications. 3, 33-42.

Romagna, M., Van Den Hout, N.J., (2017). "Hacktivism and Website Defacement: Motivations, Capabilities and Potential Threats". Proceedings of the 27th Virus Bulletin International Conference: 41 – 50.

Saroj Mehta & Vikram Singh, (2013) Study of Awareness about Cyber Laws in the Indian Society, International Journal of Computing and Business Research, 4.

Taylor, R. W., Fritsch, E. J., & Liederbach, J. (2015). Digital crime and digital terrorism. (3rd ed.). Upper Saddle River, NJ: Pearson.

Taylor, R. W., Fritsch, E. J., & Liederbach, J. (2015). Digital crime and digital terrorism. (3rd ed.). Upper Saddle River, NJ: Pearson.

Vineet Kandpal and Singh, R.K., (2013) Latest Face of Cybercrime and Its Prevention In India, International Journal of Basic and Applied Sciences, 2, 150-156.

Acknowledgments: The author acknowledges the supports of Prof. Edwin J. J. Momoh, Vice-Chancellor, and Principal of the Ernest Bai Koroma University of Science and Technology (EBKUST), Prof. Paul Abass Kamara, Chairman Board of trustee of the Institute of Advanced Management and Technology (IAMTECH), Prof. Prince Sorie Conteh, Director of Research at the University of Sierra Leone (FBC), and Prof. Roseline E. Uyanga, Chief Executive Officer at IAMTECH for promoting quality education, academic research and mentoring young talents in the country. Special gratitude goes to Mrs. Elizabeth Guma-Sawaneh for her moral supports.

Declaration of Interest: The Author has no conflicts of interest to declare that they are relevant to the content of this article.

Funding: No funding was received for conducting this study