Cybercrimes in Southern Nigeria and Survey of IoT Implications

Stephen Ugwuanyi
Department of Electrical and Electronic Engineering
University of Strathclyde
Glasgow, United Kingdom
stephen.ugwuanyi@strath.ac.uk

Agbo Okechukwu
Department of Electrical & Electronic Education
Federal College of Education (Tech.)
Omoku, River State, Nigeria
okechukwu.agbo@fcetomoku.edu.ng

Ohia Prince
Department of Computer Science
Federal College of Education Technical
Omoku, River State, Nigeria
opwservices@yahoo.com

Ndukwe Ogechukwu
Department of Computer Science
University of Port Harcourt
Rivers State, Nigeria
ogeking2004@yahoo.com

James Irvine
Department of Electrical and Electronic Engineering
University of Strathclyde
Glasgow, United Kingdom
j.m.irvine@strath.ac.uk

***Abstract*—This study comprises of a survey on the cybercrime situational awareness in the southern part of Nigeria and the readiness for IoT implications resulting from the challenges of IoT technology adoption for consumer and industrial use cases. We considered cybercrimes in the forms of identity theft, data theft, false alert, dating and romance scam and online shopping scam. The analysis shows among others, 84% of involvement in identity theft and 20% of involvement in data theft with the mode operation being highest through web-based applications. Although cybercriminals are yet to fully utilize the vast potentials of emerging IoT technology and their vulnerability to commit cybercrimes in the region, the rate is on the increase. Also presented is a generic background study on IoT security concerning device capabilities, threat landscape, policy frameworks and applications from which cybercrime trend mitigations and recommendations to reduce the impending dangers of IoT cybercrimes were proposed.**

Keywords—cybercrimes, internet of things (IoT), network, cybersecurity

I. INTRODUCTION

The advent of technology has made the human life easy with its use in almost every human activity ranging from ease of communication, conducting business transactions, health care management, education delivery, environmental monitoring, etc. The heavy reliance on technology has made humans susceptible to various kinds of threats associated with wrongful use of technology like the Internet of Things (IoT) technology. The use of IoT devices is estimated to reach 20 billion in 2020 [1] and 50 billion in 2030 [2]but with new cybersecurity threats. Cybercrime is as a result of the wrongful use of technological devices as evidenced in [2] and [3]. The extent to which these connected devices are used to execute cybercrimes has not been established especially in the developing countries. Cybercrime involves the use of electronic devices to further illegal ends, such as committing financial fraud, child trafficking, promoting pornography materials, intellectual property theft, stealing identities or violating privacy. In[4], cybercrime is seen as a type of crime committed by criminals who make use of a computer as a tool and the internet as a connection to reach a variety of objectives such as illegal downloading of music files and films, piracy, spam mailing and the likes. With reference to the ITU and Budapest Convention on cybercrime definition[5], cybercrime is focused on real-world critical information technology facilities. In the real-life scenarios, laws and regulations in additions to the insurance and legal implications outlined in [6] are however needed to reduce the cyber-security level resulting from the heavy reliance on modern IoT technology devices. Intrusion and threat detection systems are increasing sort after to protect IoT user' data and privacy breaches [7].

According to a report by the Nigerian National Information Technology Development Agency (NITDA), there are over 97 million internet users in Nigeria in 2017. This figure surpassed 100 million users in 2019. This is possible due to the increase in the use of smartphones in Nigeria and the availability of internet facilities, hence, the high reliance on computers and the internet for the everyday activity such as messaging, business transaction, banking operations and other business activities. The use of the internet has brought about various forms of crime known as cybercrime and cybercriminals in Nigeria are mostly regarded as *"Yahoo Boys"*. This involves Automatic Teller Machine (ATM)frauds, phishing, identity theft etc. According to a report by NITDA in 2017, about 14% of the total internet users in Nigeria have experienced cybercrime of different scale and magnitude. It was proven that 39.6% African users of the internet are Nigerian, hence, the high increase in the rate of internet crime in Nigeria[3]. In Nigeria, people of all ages involve on different kinds of cybercrimes because of the high rate of unemployment in the country which is currently 23.1% in 2019 according to the National Bureau of Statistics[8].

According to an analysis carried out by KPMG forensic service in Nigeria, there is an increase in cyber-related offences between 2013 and 2015 as a result of the adoption of various forms of technology [9] with targets of financial gains. This study involves a survey carried out through an online questionnaire, administered to1700 active computer users in 17 southern states of Nigeria to determine the levels of involvement of the respondents on the various type of cybercrime such as identitytheft, malicious spamming, data theft, false alert, and online shopping scams with discussions on IoT implications on cybercrime, aiming at determining its level of involvement in cybercrime. The survey also

examines the mode of operations through which these crimes are committed.

II. Related Literature

Today, tasks and events globally are connected through information systems and communication networks, enabling among others, critical activities such as financial transactions, shopping, education and even research[11].However, as the knowledge in these areas deepens, criminal activities become imminent as against its original operational principles[12]. Transmitting these criminal activities using information and communication technology devices has consistently been on the rise and has resulted in the hike of the cost of maintaining the global communication infrastructure [11]. Some of the techniques implemented by researchers to tackle these menaces need constant update due to the dynamic nature of cyber-attacks. Cybercrime comes in different forms and is generally difficult to categorize [10]. Some of the solutions include;[13] the use of encryption techniques and development of Radio Frequency Identifier (RFID) to provide authentication and integrity for the communication between RFID tags.

In [11], a design thinking approach to cybersecurity awareness among youth was conducted in Malaysia with IoT, cyber-attack, password, privacy and safer society identified as the key terms in cybersecurity investigations. The findings, however, showed that IoT devices aided cyber-attacks, but the experiences varied across organizations. As new consumer IoT devices continue to emerge, some are left unsupervised and referred to as "*Cyber Debris"* in [12]. The inability to properly manage the devices also constitutes a cyber vulnerability. Practical testing of IoT solution is the optimal approach to identifying vulnerability surfaces as seen in the Wi-Fi experimentation in a city in Denmark [13]. A global approach to tackling cybercrime has been proposed since it does not respect national boundary [14]. The study profiled the developing countries to be more vulnerable and recommended global strategic collaborative effort for sustainable cyberspace.

To understand the concept of cybersecurity in the Nigerian context and its impact on the national development, we made the following observations; that the evidence exists on the direct effect of cybercrime on foreign investment and national development. It also creates trust issues and damages national credibility[15].Data security and digital privacy protection are identified as a key driver in the NCC 2020 -2024 strategic plan with regulatory frameworks intended outcome of reducing the incidence of cybersecurity and data breaches [16].

III. Methodology

A survey design was adopted for the study. The researchers considered this design appropriate for this study since it intended to collect data from the population of people who operate online/internet-based transactions in the southernregion in Nigeria. One thousand (1700) people who do online transactions were randomly selected from the six (6) states of the south-south region of Nigeria consisting of one hundred (100) respondents. The instrument for data collection was a structured questionnaire titled "*Survey of Internet of Things(IoT) Implication on Cybercrime*(SIOTIC)''. Qualtrics statistical tool was used to administer the survey and the results analyzed using classic report feature. The research focused on addressing three key research questions: What are the types of IoT cybercrimes?;How frequently are the different IoT cybercrime committed?;and How are such cybercrimes evolving with time among different groups?. We adopted this research method because it provides a detailed opinion about IoT and its security implications.

Figure 1. Societal and Technological IoT Solution Model[17]

The framework above depicts the required multi-facets fights against cybercrime which is expected in our society. With the emergence of technologies such as IoT into basic activities of man, it becomes paramount that technology may have to interface with law, ethics and attitude awareness to check online security.

IV. Government Policies on Cybercrime

On the 15th May 2015, the Nigerian Government enacted the cybercrime bill into law, summarized in [15], which allows for Prohibition, Prevention, Detection, Prosecution and Punishment (PPDPP) of Cyber related offences in Nigeria. The 2015 cybercrime act is the first of such in Nigeria that deals with cybersecurity. One of the objectives of the 2015 cybercrime act is to promote cybersecurity and protect computer systems and network electronic communications, data and computer programs, intellectual property and privacy rights.

The 2015 Nigeria cybercrime act prescribes a jail term of up to 5 years and a fine of up to 10 million Naira for internet fraudsters that perpetuate their act by sending electronic mails with the purpose of defrauding an individual, government or organization[18].It also identifies identity theft and gives a punishment of 7 million or a 3-year jail term or both. Identity theft is when a fraudster pretends to be someone else on the internet for financial gain or to cause other damages.

The Nigerian Economic and Financial Crimes Commission(EFCC) was enacted in 2002 and started full operation in 2003 with the sole aim to investigate and prosecute all financial criminal cases which includes cybercrime. The following are some of the internet related offences and crimes in Nigeria.

A. Credit Card or ATM Fraud

This is the process of stealing credit/debit card information by hackers when the user enters credit/debit card information when performing an online transaction on a

webpage. Another form of the electronic card fraud is the fake and unauthorized messages sent by Fraudsters requesting for an update of the Bank Verification Number (BVN). In such cases, personal information and debit card information are collected from the victims and in some cases phishing sites are sent to the victims. According to a report by the Central Bank of Nigeria (CBN), commercial banks in Nigeria have lost about 199billion Naira to e-fraud alone between 2000 and 2014.

B. Advance Fee Fraud

In Nigeria, fraudulent activities are popular with the use of technology and the internet. The proliferation of scams associated with IoT in Nigeria may be difficult to compare to other countries. In Nigeria, cybercrime involves the use of spam to unleash various dubious gimmick propositions like sending an e-mail to various people asking them to transfer a sum of money to an account for non-existing products and services. In another dimension, cybercrime victims are promised a percentage of a huge sum of money for third-party activities. After the money has been transferred, they never hear from the person again. The Advance Fee Fraud and other Related Offences Act, Criminal Code Act, The Financial Crimes Commission Act and Money Laundering Prohibition Act of 2016 are the regulatory frameworks available to combat fraudulent activities known as "419" in Nigeria[41]. Given the available frameworks, the prevalence of internet scams in Nigeria is however due to lack of enforcement.

C. Phishing Attacks

A phishing attack involves cloning of a webpage such as social media pages, e-commerce store and bank websites to collect sensitive personal information such as smart card information, username and password etc. Due to the increase in the use of mobile phones and banking application in Nigeria e-fraudsters deploy many fake applications which are used to fetch and extract user's personal information. Palo Alto networks indicated that Nigerian phishers used a trojan-spy called Key base to lodge an attack with the major industrial companies as targets. According to an estimate by the Federal Bureau of Investigation (FBI), the damages done by Nigerians through phishing activities from 2013 to 2016 exceeds US$3 billion with an estimate of 22,143 companies across 79 countries[19].

D. Online Sale Fraud

This is a type of cybercrime that involves the sale of products that do not exist. The problem with online shopping is that users sometimes cannot differentiate between a genuine e-commerce site and fake websites. The various forms of social media scams include; the beneficiary of a will scam, charity funds, cyber-stalking, blackmailing scam, and social hijacking[20]. An account number is displayed sometimes on the advertisement and users are asked to pay for the product to be delivered. This scam is possible because people are asked to make full or part payment before the item is delivered.

V. IoT AND SECURITYEVOLUTION

The internet has evolved from interlinked hypertext into a network of people, applications and devices. The total number of devices currently connected to the internet has increased from millions to billions with an estimate of six billion devices connected to the internet[21]. As a result of too many devices connected to the internet, there is a need for adequate security in every section of the communication infrastructure. The IoT application evolved to the internet of people, regarded as social networking. The internet of people gave birth to the IoT[21].IoT is a network of connected devices through the internet which receives and sends data. The internet connects servers; the IoT network connects devices which are made smart by sensors - from thermostats, light bulbs, fridges to container ships and beyond. As seen in figure 1[22], the security evolution of IoT has been linear

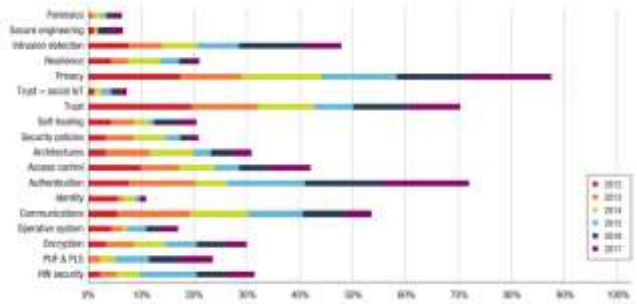

Figure 2. Security evolution of IoT

over since 2012. Trust, identity and social sides of IoT security remain relatively lower than other bold security approaches.

VI. APPLICATIONS OF IoT TECHNOLOGIES

The Internet of Things has various applications ranging from, home automation, smart banking, education and training services, advancing manufacturing, transportation and agriculture to e-government. They all present a different set of challenges, some of which are presented in [23].Data security and privacy remain critical requirements as discussed in the following IoT use cases:

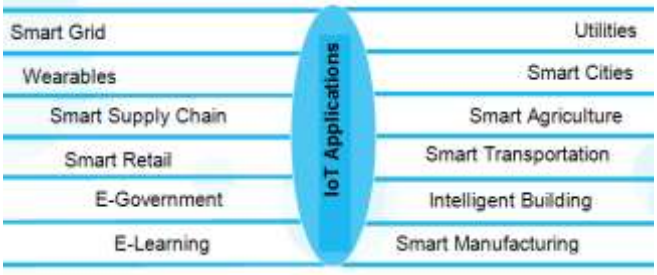

Figure 3. IoT Applications and Use cases

A. Home Automation/Intelligent Building

IoT devices are used to build a smart home which comprises of a smart lighting system, security, heating and air-conditioning system controlled by an application. An example of such application is the Amazon Echo and Google home smart speakers, which are mostly based on Wireless Sensor Networks [24]. Their use, however, is accompanied by huge privacy and security vulnerabilities. According to [25], the hardware, software and the network analysis of

home and industrial IoT solutions revealed that they are prone to different attacks types as a result of IoT adoption. Solutions such as multipath and split channel Onion IoT gateway proposed in [26]are used to filter connections at the gateway level. The choice of cybersecurity solutions like multiple authentication and encryption system lies in a compromise between cost and performance due to factors such as increased data overhead.

B. Smart Banking

IoT technology is also transforming how banking and financial services are conducted. IoT devices and applications are increasingly used to facilitate banking activities. In [27], the general view of adopting IoT in the banking sector focuses on transforming the IoT data into profitable financial gains. The data is acquired through IoT banking devices and analyzed through integrated analytics platforms. The customer data can be used to offer solutions and advice that can help the customer in making a secure and sound financial decision[28]. The layers of IoT framework must have unique security features. The data generation layer ranges from smartphone to token generators for initiating and validating banking transactions. The connectivity level ensures that the data gets to the banking server. Using public or private connectivity technology presents different cyber risks. The security of the data processing and the user interface layer depends on the tools and technologies established by the bank IT employees. The banking infrastructure, management, third-party service providers, employees and customers are different cyber-levels that also require adequate security mechanisms.

C. Transportation

The application of IoT in the transportation sector is driving services such assmart traffic control, smart parking, fleet management, vehicle control, etc. Some of the benefits are improved revenue, public safety, service on demand, and resource optimization like fuel consumption feedback and traffic route recommendation. With these new efficient and economic offerings, safety, security and privacy are the cybersecurity challenges associated with such smart city solution[29]. For instance, a smart packing system when compromised becomes underutilized and leads to economic wastages. Similarly, when a critical traffic control or fleets monitoring systems are compromised, the result is catastrophic and must be detected and mitigated using the alert scheme as proposed in [30].

D. Health Care

Smart health care is an application of IoT in the health care management system. It involves data collection and analysis for research and treatment purposes. IoT technology connects patients, medical professionals and healthcare resources intelligently. The condition of patients with medical devices such as heart rate monitors can be remotely diagnosed accurately and timely. With these capabilities, the pressure on the medical facilities use can be reduced through early diagnosis and detection of illnesses. We recommend the widespread use of this technology, especially in developing countries if the data security and privacy challenges of adopting IoT in the healthcare sector as recommended in [31]are addressed.

VII. Implications of IoT on Cybercrimes

IoT is the perfect recipe for cybercrime as it presents an opportunity for cybercrimes to be committed and the implications of its use have been understated. IoT as new and emerging technology requires stakeholders to pay more attention to security issues to drive market competitiveness. This has not been the norm and as a result, IoT devices are manufactured with security vulnerabilities, paving way for cybercrimes to be committed as new devices are introduced [32].As highlighted by Amy Webb of Future Today Institute that "Technology can be like junk food. We will consume it, even when we know it's bad for us" [33].The implications of the use of IoT devices is the vulnerability of data and privacy. IoT devices pose a high level of vulnerabilities, whichare present in IoT devices due to:

A. Poor Authentication

IoT manufacturers play a critical role in establishing the security features of IoT devices and their focus should include both ease of use and security. A return on the investment trade-off makes most IoT devices lack the proper authentication and other security features. Some IoT devices use the default security credential which is the same for similar or the same products. This makes it easy for an attacker to gain access to such a device. As IoT scales, lightweight authentication techniques using private and public keying infrastructure are needed to resolve these issues[34].

B. Unencrypted Messages Between IoT Devices

When the messages exchanged between two IoT devices are obscured from cybercriminals, confidentiality is guaranteed. The confidentiality of a network can be evaluated using either plaintext, encoded, or encrypted data types exchanged between devices or devices and servers[32]. Due to the ease of use of many IoT devices, the communication between these devices appears to be unencrypted, making it possible for a man-in-the-middle, side-channel and other data-driven attacks to take place. When a request is routed over the internet, it passes through various networked devices which are manned by different people and organizations. When these devices transmit the data as plain text (unencrypted) then it is possible for software on any of the devices to read such data [35].The threats also come from known operational inefficiencies like the inability to restrict access from a non-secure network, data mobility which leaves sensitive information in the attacker's domain, etc. In [36], a wireless radio network was vulnerable to a DDoS attack due to unencrypted data at the radio link level. Encrypted data does not mean absolute security. For instance, encrypted data tags available to an attacker can be used to obtain other information such as the number of people in a building [37].

C. Lack of Authentication

Enough validation of software, hardware and log activities ensures the authenticity and confidentiality of a network. Strong authentication pairs ensure secure access to the IoT network and prevent attacks like Distributed Denial of Service (DDoS) and replay attacks. If network access control and updates are not properly authenticated to know if the data is from a trusted source, then malicious programs can be installed in the guise of a genuine update. Usually, the firmware update will equip IoT devices with an upgrade

which will enable them to perform improved operational instructions without a corresponding upgrade in the hardware. The updated firmware will be able to bring new experiences in various functions of the devices such as security. IoT devices can take care of some of its security challenges if authentications of update of firmware are periodically made to ensure new security features in place [35]. This is common in edge computing level and in a training machine learning algorithm, where fake dataset or nodes are introduced early to deviate the system from learning valid model [37].

Future research in authentication should be focused on Android devices because wearable is on the increase. The combination of intrusion detection and authentication scheme; group authentication and key agreement; and electrocardiogram-based authentication with privacy preservation are the future research direction recommended for smart mobile devices in [38].

VIII. Security Threats and Attacks in IoT Network

The security of IoT network is vulnerable to various attacks, this is since most IoT devices are installed in public places e.g. IP camera can be subject to cloning, replacement and other physical attacks. Most of these attacks can be categorized based on the structure of the IoT. The attacks and threat to IoT can be divided into four[39].

A. Physical Layer Attack

This is the most important part of the IoT network that must be protected from all forms of attacks. IoT devices are mostly made of various remotely interconnected nodes. In the physical layer attack, when the attacker exploits a vulnerable node to extract security information, the result is catastrophic and can lead to a total failure of the network. All forms of physical security are associated with IoT users. An overload attack is a type of physical layer attack on an IoT. This attack is used to decrease the strength of an IoT network. One of the ways to provide a solution to the attacks at this layer is by fixing strong physical layer security. Physical Unclonable Function (PUF) is physical layer security that provides IoT devices with fingerprint identification[22].

B. Perceptual Layer Attack

A perception layer is an attack on the various nodes responsible for the collection of data from the external world. These nodes are sensors and example are RFID and wireless sensor network. These attacks are possible since little or no security exists on the sensors hereby, they are prone to attacks. The solution to this kind of attack is to provide a means of authentication for each node or to allow for a node to node authentication, which is possible only if nodes becomes powerful to support parallel processing.

C. Network Layer Attack

The main security threat in the network layer consists of routing attacks such as malicious behaviour against right path topology and forwarding data, Distributed Denial of Service (DDoS) attacks, cyber-attacks across a heterogeneous network, asynchronous attacks, collusion attacks and the man-in-the-middle attacks[39]. Another type of attack is when a malicious node tries to drain network resources. Other attacks include node impersonation attack and it happens when a malicious node tries to gain access to a network in the guise of a genuine node. Spoofing attack; this type of attack occurs when an attacker tries to gain access to a device by pretending to be someone else. Replay Attacks; the attacker captures network data and replays it on the network to slow down the network operation. These types of attacks can be stopped by restricting traffic on each network node.

D. Support Layer Attack

The attacks on this layer include Denial of Service (DOS) attack, sessionattack and Denial of Access (DOA) attacks. The support layer attacks can be stopped by using security tools to detect malicious codes, such security tool can be an antivirus.The support layer performs two major roles;To confirm that information is sent by an authenticated user and protected from threats andto send information to the network layer through wireless or wired technology [29]. The verification of the user and the information can be done in various ways, likethe method of authentication which is implemented by using secret keys and passwords.

E. Application Layer Attack

The application layer is responsible for handling user data, management processes, control, visualization, etc. An attack on the application layer targets the user confidential information by compromising specific web service applications. Cybercriminals use complex DDoS like HTTP floods, and brute force attack to steal, destroy or modify the user data. The major concern for application-level security is the issue of data sharing. Other factors include passwords and key agreement. The attacker is likely to destroy privacy in the application layer by a known vulnerability.

IX. Cybercrimes Trends in IoT

IoT development comes with different sensing and control capabilities applicable to industrial and consumer solutions. It has been estimated by Cisco that IoT connection will reach 50 billion in 2020. This is a serious concern due to the security and vulnerability issues in IoT as most businesses and organization are relying heavily on smart devices. Any approach to IoT security must include availability, integrity and confidentiality if the following cybercrimes are to be mitigated.

A. Fraud

Due to the lack of control of infrastructure in most IoT devices, low-level infrastructure can be used to cause serious damage. An example is the first fraud of IoT that happened when a network of ATM used by the banks was attacked by fraudsters through the use of web-based control. And in most cases, it takes just one compromised node for fraudsters to gain access into an entire system. According to a report by Forrester, hackers are now targeting IoT devices for financial gain, it is no longer for social or political reason. This is because of any sensitive business data which is held by most IoT devices, for example, a smartwatch and phone can contain some user sensitive data such as; name, address, health information and debit/credit card information.

B. Data Theft

Between 2017 and 2018[40], a trojan VPN filter and other malware types were found to be used in extracting sensitive information such as username and password and extracting other important data from IoT users. With the adoption of IoT devices by the public, the issue of privacy of data is a thing of concern. Most IoT such as smartwatch and entertainment smart devices store user data and such data

give detailed information about an individual.Cybercriminals upon obtaining these data, use them to usurp the personality of the original data owners. Sometimes, the data is stolen and sold or directly used to enable them to act or operate in the capacity of the victims.

C. Malicious Spamming

IoT devices are now used by hackers as tools to cause attacks. An example was the use of over 100,000 devices which includes smart devices, routers and other devices that were manipulated by hackers into sending out more than 750,000 malicious emails.In a case where those smart devices are infected with a trojan, they will continue sending malicious messages except they are taken offline in some cases a security update from the manufacturer can stop the trojan.

D. Identity Theft

With IoT devices, cyber-criminals can gain access to personal information of victims such as bank account details, credit and debit card information through theft and tampering and are used for both cash and internet transaction in the victim's name. This is because IoT devices make current data readily available and store historical user data [7]. Due to the security vulnerability of IoT devices, hackers can easily access such information in the form of hijacking.

X. Results and Analysis of the Survey

Based on the responses, the analysis of the results in **Error! Reference source not found.** reveals among others an 84% high involvement in identity theft and 20% lower in data theft in southern Nigeria. Figure 4 shows the different percentages of involvements in various cybercrime identifies in southern Nigeria. The survey results provide an overview of cybercrime in southern Nigeria and how frequently specific IoT devices have been used to commit cybercrimes. The implication of these findings is to enable faster design

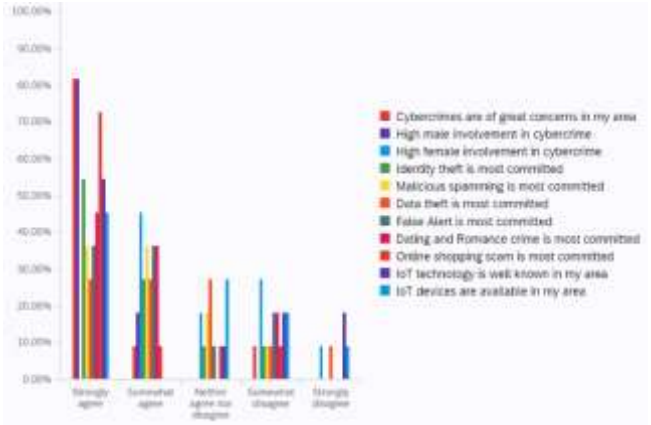

Figure 4. Percentages of involvements in cybercrime

and adoption of the best security architecture that will ensure confidentiality, integrity and availability of IoT services. It will also serve as the guide for creating a cybercrime awareness campaign and making necessary recommendations for IoT use and regulations.The data generated during the study was used in determining the percentage of modes of operation of cyber-related crimes in Southern Nigeria as shown in Table 1.

The types of cybercrime spread across the different modes of IoT operation. Web-based applications are the most common means of cybercrimesin southern Nigeria with 1.6% higher than social networking. While others like text messagingand mobile applications were lower, they are still as important as other aspects of IoT ecosystemnot captured in this study.

Table 1. Percentage of Mode of Operations

Mode of Operation	Percentage of Operations
Web-based Application	34.6%
Social Networking	33%
Text Messages	7.3%
Mobile Application	10%
E-mail	15.1%

XI. Future Directions

The IoT technology is a promising area of research which has been widely embraced across many fields. With the actual deployment figures very close to most of the growth forecasts, the security and privacy requirements and cybercrimes related to the use of this technology cannot be over emphasized. The emergence of this technology in virtually every area of human endeavours makes its security consciousness of interest to any concerned researcher and indeed the teaming users. The advances in IoT research in the future will take on the security direction. From the standardization of IoT product security approach down to the cybercrimes; the focus of this paper. The researchers project IoT to be enabling intelligent decision making if security is addressed at every layer of the architecture, including their role in the realms of cybercrimes.

XII. Conclusion/Recommendation

This study has revealed an increasing interest in IoT to advancing global interconnectedness. While IoT technology is available for consumer and industrial use for convenience and innovations, it has also become a tool for data breaches and a myriad of other cybercrimes. We reviewed IoT related service users in the southern part of Nigeria to gain an insight into how IoT devices are used to commit cybercrime. The focus was to understand the users' perception as it relates to cybercrimes in different locations. Although, the findings show that cybercriminals have not fully utilized the potentials of IoT devices and their vulnerabilities to attack and cause harm of great magnitude in this region. However, there are indications that IoT technology might be sought after by the hackers and cybercriminals in Nigeria.The following are put forward as recommendations from this study:

- Criminalize the Act of cybercrime: Although in Nigeria, all forms of internet-related offences are punishable according to the cybercrime Act of 2015. Cyber laws should be made available to the public and enforcement implemented.
- The co-operation of international communities: In the fight against cybercrimes, especially in southern Nigeria, the international community has an important role to play especially for crimes that require the extradition of criminals. This is because most cybercrimes have an international dimension. From the technology point of view, we recommend a global

approach to regulations and standardization since technology violates national boundaries.

- Research development / Specialized Training: Grants should be made available by the Federal Government of Nigeria specifically for interested researchers to embark on technological based research to curb the menace of cybercrimes and develop trust to resolve the present privacy issues
- Other recommendations: Education and sensitization of internet users in Nigeria on the danger of cybercrimes should be taken seriously, delegating more duties to Internet Service Providers (ISPs) such as the authority to report observed malicious communication, the introduction of cybersecurity module into Nigerian education curricula, and the setting up of a special anti-graft agency especially for cybercrime should be considered and quickly implemented.

ACKNOWLEDGMENT

The authors would like to appreciate those who responded to the study questionnaire and the Nigerian Petroleum Technology Development Fund (PTDF) for funding this research under the award number PTDF/ED/PHD/USO/1092/17.

REFERENCES

[1] N. Gershenfeld, R. Krikorian, and D. Cohen, "The Internet of things", Scientific America, vol. 291, no. 4, pp. 76-81, 2004.

[2] S. Furnell, "Technology Use, Abuse, and Public Perceptions of Cybercrime," in The Palgrave Handbook of International Cybercrime and Cyberdeviance, Springer International Publishing, 2020, pp. 45–66.

[3] A. Bijik Hassan, F. David Lass, and J. Makinde, "ARPN Journal of Science and Technology::Cybercrime in Nigeria: Causes, Effects and the Way Out," *ARPN J. Sci. Technol.*, vol. 2, no. 7, 2012.

[4] O. Olusegun, "Impact of Immigration on Nigerian Economy," SSRN Electronic Journal, October, 2015.

[5] B. Akhgar et al., "Consolidated taxonomy and research roadmap for cybercrime and cyberterrorism," in Advanced Sciences and Technologies for Security Applications, Springer, 2016, pp. 295–321.

[6] A. Tăbușcă, S.-M. Tăbușcă, and G. Garais, "IoT and EU Law – E-Human Security," Valahian Journal of Economic Stududies, vol. 9, no. 23, pp. 25–32, Mar. 2019.

[7] N. M. Karie, N. M. Sahri, and P. Haskell-Dowland, "IoT Threat Detection Advances, Challenges and Future Directions," in Proceedings - 2020 Workshop on Emerging Technologies for Security in IoT, ETSecIoT 2020, 2020, pp. 22–29.

[8] Chris Ngige, "Nigeria's unemployment rate hits 33.5 per cent by 2020 – Minister | Premium Times Nigeria," May-2019. [Online], Available:https://www.premiumtimesng.com/news/top-news/328137-nigerias-unemployment-rate-hits-33-5-per-cent-by-2020-minister.html. [Accessed: 29-Jul-2020].

[9] KPMG, "Building Cyber Security & Resilience in a Digital Africa,"May, 2017. [Online], Available: https://home.kpmg/content/dam/kpmg/zm/pdf/2017/07/Building%20Cyber%20Security%20&%20Resilience%20in%20a%20Digital%20Africa-%20FINAL.pdf.[Accessed: 20-Jul-2020]

[10] R. Broadhurst, "Cybercrime in Australia," in The Palgrave Handbook of Australian and New Zealand Criminology, Crime and Justice, Springer International Publishing, 2017, pp. 221–235.

[11] M. Dorasamy, G. C. Joanis, L. W. Jiun, M. Jambulingam, R. Samsudin, and N. J. Cheng, "Cybersecurity issues among working youths in an iot environment: A design thinking process for solution," in International Conference on Research and Innovation in Information Systems, ICRIIS, 2019, vol. December-2019.

[12] I. Mizukoshi and A. Nakanishi, "Subscription; Remedy for Cyber Debris!?,"*2019 IEEE Social Implications of Technology (SIT) and Information Management (SITIM),* Matsuyama, Japan, 2019, pp. 1-6, doi: 10.1109/SITIM.2019.8910190.

[13] L. S. Vestergaard, N. Kasenburg, and M. S. Jorgensen, "Implications of conducting internet of things experimentation in Urban environments," in Global IoT Summit, GIoTS 2019 - Proceedings, 2019.

[14] A. Tabassum, M. S. Mustafa, and S. A. Al Maadeed, "The need for a global response against cybercrime: Qatar as a case study," in 6th International Symposium on Digital Forensic and Security, ISDFS 2018 - Proceeding, 2018, vol. 2018-January, pp. 1–6.

[15] The Communicator, "A Summary Of The Legislation On Cybercrime in Nigeria," Dec-2018. [Online]. Available: https://www.ncc.gov.ng/thecommunicator/index.php?option=com_content&view=article&id=899:a-summary-of-the-legislation-on-cybercrime-in-nigeria&catid=23&Itemid=179. [Accessed: 25-Jul-2020].

[16] NCC, "NCC Strategic Management Plan ASPIRE 2024," 2020. [Online]. Available: https://ncc.gov.ng/accessible/documents/886-ncc-2020-2024-strategic-management-plan-aspire-2024/file. [Accessed: 25-Jul-2020].

[17] M. M. Ali, "Determinants of preventing cyber crime: a survey research," *Int. J. Manag. Sci.*, vol. 2, no. 7, pp. 16–24, 2016.

[18] ICT Policy Africa,"The Nigeria CyberCrimes (Prohibition, Prevention, etc) Act, 2015,". [Online], Available: https://ictpolicyafrica.org/en/document/h52z5b28pjr. [Accessed: 24-Jan-2020].

[19] D. Gudkova, M. Vergelis, N. Demidova, and T. Shcherbakova, "Span and phishing in Q2 2016." Kaspersky Lab, August 2016.

[20] A. Esan, B. A. Omodunbi, P. O. Odiase, O. M. Olaniyan, and A. O. Esan, "Cybercrimes in Nigeria: Analysis, Detection and Prevention.," FUOYE Journal of Engineering and Technology, vol. 1, no. 1, 2016.

[21] Infosys, "Live enterprise." Annual report, 2018-19. [Online]. Available:https://www.infosys.com/investors/reports-filings/annual-report/annual/Documents/infosys-AR-19.pdf. [Accessed: 24-Jan-2020].

[22] R. Roman-Castro, J. Lopez, and S. Gritzalis, "Evolution and Trends in IoT Security," Computer (Long. Beach. Calif)., vol. 51, no. 7, pp. 16–25, Jul. 2018.

[23] S. Thiruchadai Pandeeswari, S. Padmavathi, and N. Hemamalini, "Engineering Full Stack IoT Systems with Distributed Processing Architecture—Software Engineering Challenges, Architectures and Tools," Intelligent Systems Reference Library, vol. 185, Springer, Cham, 2020, pp. 71–87.

[24] C. S. Abella et al., "Autonomous Energy-Efficient Wireless Sensor Network Platform for Home/Office Automation," IEEE Sensor Journal, vol. 19, no. 9, pp. 3501–3512, May 2019.

[25] J. Wurm, K. Hoang, O. Arias, A.-R. Sadeghi, and Y. Jin, "Security analysis on consumer and industrial IoT devices," 2016 21st Asia South Pacific Des. Autom. Conf., pp. 519–524, 2016.

[26] L. Yang, C. Seasholtz, B. Luo, and F. Li, "Hide your hackable smart home from remote attacks: The multipath onion IoT gateways," in Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 2018, vol. 11098 LNCS, pp. 575–594.

[27] R. S. Lande, S. A. Meshram, and P. P. Deshmukh, "Smart banking using IoT," Proceedings of the 2018 3rd IEEE International Conference on Research in Intelligent and Computing in Engineering, RICE, pp 1-4, January 2018.

[28] V. Dineshreddy and G. R. Gangadharan, "Towards an Internet of Things framework for financial services sector," in 2016 3rd International Conference on Recent Advances in Information Technology, RAIT 2016, 2016, pp. 177–181.

[29] A. S. Elmaghraby and M. M. Losavio, "Cyber security challenges in smart cities: Safety, security and privacy," Journal of Advanced research, vol. 5, no. 4, pp. 491–497, 2014.

[30] W. Li, H. Song, and F. Zeng, "Policy-Based Secure and Trustworthy Sensing for Internet of Things in Smart Cities," IEEE Internet Things J., vol. 5, no. 2, pp. 716–723, Apr. 2018.

[31] F. Nasri and A. Mtibaa, "Smart Mobile Healthcare System based on WBSN and 5G," International Journal of Advanced Computing Science and Applications, vol. 8, no. 10, 2017.

[32] F. Loi, A. Sivanathan, H. H. Gharakheili, A. Radford, and V. Sivaraman, "Systematically Evaluating Security and Privacy for Consumer IoT Devices," 2017.

[33] Alisdair Faulkner, "Evolution of fraud in the IoT era ," 22-Aug-2018.[Online],Available:https://www.techradar.com/sg/news/evo

lution-of-fraud-in-the-iot-era. [Accessed: 25-Jul-2020].
[34] K. Gupta and S. Shukla, “Internet of Things: Security Challenges for Next Generation Networks,” 1st International Conferenceon Innovation and Challenges in Cyber Security, ICICCS-INBUSH, pp. 315–318, 2016.
[35] G. Nebbione and M. C. Calzarossa, “Security of IoT Application Layer Protocols: Challenges and Findings,” *Futur. Internet*, vol. 12, no. 3, p. 55, Mar. 2020.
[36] D. Pishva, “Internet of Things: Security and privacy issues and possible solution,” *2017 19th Int. Conf. Adv. Commun. Technol.*, vol. 5, no. 2, pp. 797–808, 2017.
[37] A. Mohsen Nia and N. K. Jha, “A Comprehensive Study of Security of Internet-of-Things,” *IEEE Trans. Emerg. Top. Comput.*, vol. 5, no. 4, pp. 1–1, 2016.
[38] M. A. Ferrag, L. Maglaras, A. Derhab, and H. Janicke, “Authentication schemes for smart mobile devices: threat models, countermeasures, and open research issues,” *Telecommunication Systems*, vol. 73, no. 2. Springer, pp. 317–348, 01-Feb-2020.
[39] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao, “A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications,” IEEE Internet Things Journal, vol. 4, no. 5, pp. 1125–1142, 2017.
[40] I. Makhdoom, M. Abolhasan, J. Lipman, R. P. Liu, and W. Ni, “Anatomy of Threats to the Internet of Things,” *IEEE Commun. Surv. Tutorials*, vol. 21, no. 2, pp. 1636–1675, Apr. 2019.
[41] T. Oriola, "Advance fee fraud on the Internet: Nigeria's regulatory response," Computer Law & Security Review, vol. 21, no. 3, pp.237-248, 2005.