THE COLLOQUIUM -A Multi disciplinary Thematc Policy Journal
www.ccsonlinejournals.com
Volume 10 , Number 1 , 2022 Pages 93 - 101
CC-BY-NC-SA 4.0 International Print ISSN : 2971-6624 eISSN: 2971-6632

EVALUATING CYBERCRIME BASED ON INTERNET OF THINGS TECHNOLOGY AND LEVEL OF READINESS FOR SOLUTIONS IMPLEMENTATIONS IN RIVERS STATE

[1]AGBO, Okechukwu Chuks, [2]UGWUANYI, Stephen & [3]ISAAC, Udoka C. N. Ph.D
[1,3] Department of Electrical/Electronic Education,
Federal College of Education (Technical), Omoku,Rivers state.
[2] Department of Computer Science Education,
Adeyemi College of Education ,Ondo State.
Corresponding Email : okechukwu.agbo@fcetomoku.edu.ng

Abstract

This paper aims at evaluating cybercrimes based on Internet of Things (IoT) Technology, emanating from the issues of IoT devices such as challenging management environment, different technology profile, processing capabilities, use-cases and physical locations and levels of readiness for solutions implementations in Rivers State, Nigeria. Two research questions supported the study with one null hypotheses which were tested at 0.05 level of significance. A descriptive research design was used for the study. The research population was made up of 92 male and female Information and communication Technology (ICT) based business operators randomly selected from twenty three local government of Rivers State. Ten items structured questionnaire titiled "Cybercrime Based on Internet of Things Technology and Level of Readiness for Solutions Implementations Questionnaire (CBIoTREIQ) was used for the survey. The instrument was validated by three experts in Federal college of education (Technical) Omoku. The Pearson product Moment Reliability Co-efficient was used to obtain a correlation value of 0.87. Data related to the research questions were analyzed using mean and standard deviation while t-test analysis was used to test the null hypotheses at 0.05 level of significance. The research surveys cybercrimes considering the following aspects; identity theft, false alert, dating and romance scam and online shopping scam. The investigation shows the highest value representing 30% of involvement in identity theft category with the lowest value representing 10% of involvement in online shopping scam. It further reveals that a high record of web based applications representing the mode of operation and the level of readiness of operators for solution implementation is low in Rivers State. It was recommended that while awaiting the full utilization the vast potentials of IoT devices and their vulnerability to commit their crimes, the Nigerian government and relevant authorities must be proactive to develop preventive measures to this impending danger.

Keywords: *Cybercrimes, IoT devices, network, Cybersecurity*

Introduction

Activities of man including ease of communication, business operation, health care management, education delivery, environmental monitoring, etc. have become very easy with technological advancements. The high dependence on technology has made man open to various kinds of threats resulting from illegal use of technology such as the Internet of Things (IoT) technology. The number of use of IoT devices is

Cite this article as

Agbo, O. C., Ugwuanyi, S., & Isaac, U. C. N. (2022). Evaluating cybercrime based on Internet Of Things technology and level of readiness for solutions implementations in Rivers state.*THE COLLOQUIUM*, 10(1), 93 -101

estimated to hit 20 billion in 2020 and 50 billion in 2030 (Alisdair, 2018) but will give rise to new cybersecurity threats. The illegal use of technological devices results to Cybercrime as evidenced in Furnell (2020). The levels to which these interconnected devices are utilized in committing cybercrimes have not been established especially in the developing countries. Cybercrime involves the use of electronic devices to further illegal ends which includes financial fraud, child trafficking, promotion of pornography materials, intellectual property theft, identities theft or privacy violation. In Karie, Shari and Haskell-dowland (2020), cybercrime is described as a type of crime perpetuated by criminals who employ computers as tools and internet connection to achieve series of objectives including illegal downloading of music files and films, piracy, spam mailing , etc. Referencing the ITU and Budapest Convention on cybercrime, it is considered to focus on real-world critical information technology facilities (Security, 2017). In the real- life settlements, policies, laws and regulations including insurance and legal implications are also needed to curtail the cyber-security cases emanating from over dependent on modern IoT technology devices (Alisdair, 2018). Intrusion and threat detection systems are on increasingly demand to protect user' data and privacy breaches.

According to a report by the Nigerian National Information Technology Development Agency (NITDA), 97 million internet users recorded in Nigeria in 2017. This figure is above 100 million users which were recorded in 2019. This is results from the increasing level of use of smart devices in Nigeria and high level internet connectivity. This led to the high dependence on computers and the internet for daily activity which includes messaging, business transaction, banking operations, etc(Tabassum et al., 2018). Increasing dependence on internet has led to various forms of cybercrime which includes this ATM Frauds, Phishing, Identity theft etc. NITDA reported in 2017 that about 14% of the total internet users in Nigeria have been involved in cybercrime at different scales and magnitudes. It was established that 39.6% African users of the internet are of Nigerian extracts, resulting in increased rate of internet crime in Nigeria (Tabassum et al., 2018). Nigerians of various ages involve on different kinds of cybercrimes due to increasing number of unemployment people in the country(Tabassum et al, 2018).Young Nigerian cybercriminals are tagged "Yahoo boys" depicting the name of the search engine and e-mail service provider called Yahoo.The analysis of KPMG forensic service in Nigeria reveals an increase in Cyber related offences between 2013 and 2015 as a result of the adoption of various forms of technology with the aim of financial benefits (Tabassum et al., 2018).

This study includes a survey conducted through an online questionnaire that is administered to 1700 active computer users in Rivers state, Nigeria to determine the levels of involvement in the various type of cybercrime which includes IdentityTheft, Malicious Spamming, Data Theft, False Alert, Dating and Romance Scam, and OnlineShopping Scam from the selected respondents on the level of readiness to implement an IoT based solutions for cybersecurity. The survey investigates the mode of operations through which these crimes are perpetuated.

Statement of the Problem

Reports show cybercrime as one of the major challenges of network based communications in the globe with several countries of the world making policies to reduce its increase (Broadhurst, 2017). Furthermore, the advent of IoT technology with so many attendant problems yet to be completely solved have become the concerns of communication experts who utilise the opportunities for the perpetuation of the crimes (Furnell,2020). Therefore, the researcher deemed it fit to evaluate cybercrimes based on IoT and the readiness for the solutions implementations in Rivers State.

Purpose of the Study

The main purpose of this study is to evaluate cybercrimes based on IoT and the readiness for the solutions implementations in Rivers State Specifically, the study sought to determine:

1.The Level to which male ICT Based Business Operators are ready for the implementation of IoT based solution for cybercrime in Rivers state.

2.The Level to which female ICT Based Business Operators are ready for the implementation of IoT based solution for cybercrime in Rivers state.

Research Questions

The following research questions guided the study:

1.To what level to do the male ICT Based Business Operators ready for the implementation of IoT based solution for cybercrime in Rivers state?

2.To what levels to do the female ICT Based Business Operators ready for the implementation of IoT based solution for cybercrime in Rivers state?

Hypothesis

The null hypothesis was tested at 0.05 level of significance:

H_{01} : There is no significant difference in the respondents' means ratings of both male and female ICT Based Business Operators' on the readiness for the implementation of IoT based solution for cybercrime in Rivers state based on gender.

Related Literature

Tasks and events in the world today are performed through information systems and communication networks, facilitating among others, crucial activities which includes financial transactions, shopping, education and research (Furnell, 2020). However, growth in knowledge in these areas, there is a sharp rise in criminal activities which negates the original operational principles the profession. Perpetuating these illegal activities through information and communication technology devices has also registered a sharp rise and has resulted in the increase in the cost of maintaining the global communication infrastructure (Broadhurst, 2017). Most of the techniques recommended by researchers to tackle these illegal acts need constant update due to the dynamic nature of cyber-attacks. Cybercrime exists in different forms, making it difficult to categorize (Security, 2017). Some of the present solutions consists of the use of encryption techniques and development of Radio Frequency Identifier (RFID) to provide authentication and integrity for the communication between RFID tags(Karier et al.,2020). In Security(2017), a design thinking approach to cybersecurity awareness among young people was carried out in Malaysia with IoT, cyber-attack, password, privacy and safer society identified as the key terms in cybersecurity research. The findings of the research indicated that that IoT devices support cyber-attacks, but the experiences are not uniform across organizations. With the continuous emergence of new consumer IoT devices, some are not supervised and are tagged "Cyber Debris" (Alisdar, 2018). The failure to properly manage the devices also makes up the cyber vulnerability. Practical investigation of IoT solution is the ideal approach for identifying vulnerability surfaces as observed in the Wifi experimentation in a city in Denmark (Tabusca et al., 2019). A global approach to tackling cybercrime has been put forward since it is an international concern (Tabassum et al., 2018). The research profiled the developing countries to be more vulnerable and recommended global strategic joint effort for secured cyberspace. For clear understanding of the concept of cybersecurity as obtainable in Nigeria, cross examine the evidence on the direct effect of cybercrime on foreign investments and national development. This leads to trust issues and reduces national credibility. 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 (Furnell, 2020).

Specifically, IoT represents the new industrial slogan for connecting intelligent and unintelligent devices including actuators, sensors, and other devices to the web. Presently, a lot of organizations are considering Industrial IoT as a tool for their business success strategies and evaluation through advanced data analytics in industrial domains (Thiuchadai, Padmavathis and Hemarnanalini, 2020). A major component in such a system is the ability of heterogeneous devices to effectively connect and communicate. It demands that material objects now have communications and computation capabilities and automatically identify themselves using standard protocols and architecture, employing the Internet open system as their foundation (vestergaard,Kasenburg and Jorgensu, 2020). This development is due to the deployment of the IP version 6 (IPv6) . Notwithstanding that IoT enables machines to communicate with each other and smart devices; there are potential security and privacy challenges which happen at the application arena of IoT. In the area of analysis and detection, providers can adopt signature-based and anomaly-based approaches to detect intrusions. Ultimately, IoT will make our world smarter, easier and more efficient.

Nigerian Government made policies on Cybercrime

The Nigerian Government enacted the cybercrime bill into law on the 15th May 2015 which provides for Prohibition, Prevention, Detection, Prosecution and Punishment (PPDPP) of Cyber related offences in Nigeria(The Nigerian Cybercrime Act, 2015). This is the first of such law in Nigeria that provides regulations for cybersecurity. One aim of the 2015 cybercrime act is to enshrine cybersecurity and protect computer systems and network electronic communications, data and computer programs, intellectual property and privacy rights (Furnell, 2020). The cybercrime act provides for a jail term of up to 5 years and a fine to a tune of 10 million Naira for internet criminals that commits such offenses. It also proscribes a punishment of 7 million or a 3-year jail term or both for internet theft. Another type of theft regarded ad identity theft occurs when a fraudster pretends to be someone else on the internet for financial gain or to cause serious damages. With the enactment of the Nigerian Economic and Financial Crimes Commission(EFCC) in 2002 which started full operation in 2003 with the singular function of investigating and prosecuting all financial criminal cases which cybercrime is one of them, the activities of the fraudsters are continually monitored (Tabassum et al, 2018). Some of the internet related offences and crimes in Nigeria are provided below:

1.Credit Card or ATM Fraud

This involves the stealing of credit/debit card information by hackers when the user enters credit/debit card information when carrying out an online transactions on the internet. This can also be in the form of the fake and unauthorized messages sent by these criminals requesting for an update of the Bank Verification Number (BVN) or any of such financial information. In such situations data collected from the unsuspecting users or phishing sites are used against the victim (Security,2017).

2.Advance Fee Fraud(419)

This is a type of cybercrime that involves the fraudsters who sends an unsolicited e-mail to various users requesting them to send a particular sum of money to an account number for purposes they will never fulfill with a huge fake promise that they will present to be real. (Karier et al,2020).

3.Phishing Attacks

A phishing attack involves cloning or duplicating a webpage including social media page, e-commerce store and bank websites to collect sensitive personal financial data of customers. Following the increase in mobile phones usage and mobile banking application in Nigeria e-fraudsters use many fake applications which looks like the originals to fetch and extract user's personal data(Furnell, 2020).

4.Online Sale Fraud

The online sale fraud involves the sale of products that are not in existence. It is usually difficult for users to clearly differentiate between the real e-commerce site and a fake one (Tabassum et al., 2018).

5.Cybercrime On Iot/Trends Of Crime

IoT and its Evolving Technology

The evolvement of internet started from interlinked hypertext into a network of people, applications and devices. There is a constant increment in the number of devices currently connected to internet from millions to billions with a total estimate of **six** billion devices (Alisdair, 2018). This gave rise to the need for an autonomous communication of devices to be created. That solution today is the Internet of Things (IoT). The internet of application evolved to the internet of people giving rise to social networking. The internet of people gave metamorphosed into IoT (Alisdair, 2018). IoT is made up networks which connects devices, transmit and receives data through the internet with the help of sensors.Cisco estimated that IoT Connection will get up to 50 billion in 2020. This raises a serious challenge as a result of security and vulnerability in IoT by most businesses and organization who rely on IoT technology for their businesses (Lin et al., (2017).

6.Fraud

Following the poor control of devices in most IoT network, serious damage can be experienced. According to a report by Forrester, fraudsters are now targeting IoT devices for financial gain and no longer for social or political reason. This is as a result of sensitive business data which is held by most IoT devices, such as, a smartwatch and phone containing some user sensitive data which includes; name, address, health information and debit/credit card information.

7.Data Theft

Trojan VPN filter was found in 2018 to have been used in extracting sensitive information which includes username and password and other important data from users. However, the adoption of IoT devices by the public, the issue of privacy of data became a thing of concern to many.

8.Malicious Spamming

This involves sending malicious emails to unsubscribed individuals. Even in the case where the smart devices are infected with a trojan, they still go ahead to send malicious messages except taken offline or a security update is quickly made.

9.Identity Theft

Fraudsters can get access to personal information of users which includes bank account details, credit and debit card information and use them for financial transaction in the victim's name. This is due to vulnerability of IoT devices.

Methodology

A descriptive design was adopted for the study. The researchers employed this design appropriate for this study since it intended to collect data from the population of people who operate ICT-based Business in the Rivers State, Nigeria. Ninety two (92) ICT based business operators were randomly selected from the twenty three (23) local government areas (LGA) of Rivers state, Nigeria consisting of four (4) ICT based business operators respondents from each LGA of Rivers State. The instrument for data collection was a structured questionnaire titled "Cybercrime Based on Internet of Things Technology and Level of Readiness for Solutions Implementations Questionnaire (CBIoTREIQ), decision rule based mean rating of 2.0 was used. Therefore, items with mean rating of 1.5 – 2.0 were regarded as high level, items with mean rating of 1.0 – 1.49 were regarded as moderate level and items below 1.0 were regarded as low level. In testing the hypothesis, a null hypothesis was accepted where the calculated t-value is less than critical value of t. it means that there is no significant difference and the hypothesis will not be rejected. Conversely, where the calculated t-value is equal to or greater than the critical t-value, it means there is significant difference and the hypothesis will be rejected

Result analysis of the Survey

Analysis of the respondents responses, shows that 30.01% high involvement in identity theft and 10.3% lower in online shopping scam in Rivers state, Nigeria as presented in Table 1 which shows the different levels of percentages involvements in the listed cybercrimes in Rivers State, Nigeria. The survey results shows the state of cybercrime in Rivers State, Nigeria based on respondents' responses. The findings will be to enable the relivant authorities to decide on the most secured security architecture while implementing IoT based solutions.

Table 1. Percentages of involvements in cybercrime

Types of Cybercrime	Percentage of Involvement
Identity Theft	32.01%
Malicious spamming	10.02%
Data Theft	20.01%
False Alert	13.04%
Dating and Romance	17.0%
Online shopping scam	10.3%.

The data gathered from the research was used in determining the levels of percentages of modes of operation of cyber-related crimes in Rivers State, Nigeria as shown in Table 2. The mode of operation showed that web-based applications recorded 34.6% high while Text messaging recorded 7.7% low.

Table 2. Percentage of Mode of Operations

Types of Cybercrime	Percentage of Operations
Web-based application	34.6%
Social Networking	33.0%
Text messages	7.7%
Mobile Application	10.0%
E-mail	15.1%

Research Question 1

1.To what level to do the male ICT Based Business Operators ready for the implementation of IoT based solution for cybercrime in Rivers state?

Table 1: mean responses of male on the Level of ICT based business operators' readiness for IoT solutions for cybercrime in Rivers State.(N_1 = 41)

S/N	Type of Cybercrime	Mean	Level of Readiness
1	Web-based App	0.81	low
2	Social Networking	0.54	low
3	Text message	0.92	low
4	Mobile App	0.55	low
5	email	0.48	low
	Mean of means	0.66	low

The result of the study in table 3 shows that all the items had their means below 1.0 with mean scores of 0.66. Therefore, all the male ICT based Business Operators used for the study are at low level of readiness for IoT solutions for Cybercrimes in Rivers State.

Research Question 2

To what level to do the female ICT Based Business Operators ready for the implementation of IoT based solution for cybercrime in Rivers state?
Data collected in the second research question were analyzed and presented in table 4.

Table 4: mean responses of female on the Level of ICT based business operators' readiness for IoT solutions for cybercrime (N_2=41)

S/N	Type of Cybercrime	Mean	Remark
1	Web-based App	0.95	low
2	Social Networking	0.81	low
3	Text messages	0.45	low
4	Mobile App	0.38	low
5	e-mail	0.51	low
	Mean of means	0.62	low

The result of the study in table 4 shows that all the items had their means below 1.0 with mean scores of 0.62. Therefore, all the female ICT based business operators used for the study are at low level of readiness for IoT solutions for Cybercrimes in Rivers State.

Testing the Hypothesis

Null Hypothesis H_{01}

There is no significant difference in the respondents' means ratings of both male and female lecturers on the usage of closed access computer applications for continuous assessment in tertiary institutions in Rivers state on the bases of gender. This null hypothesis was tested using t-test 0.05 level of significance.The results are indicated in Table 5

Table 5: Means, Standard Deviations and t-test for male and female ICT Based Business Operators' readiness for cybercrime solutions in Rivers state on the basis of gender.

Gender	N	Mean	SD	df	t-test	t-crit	α	Decision
Male	80	0.66	0.84					
				158	0.17	1.96	0.05	NS
Female	80	0.74	0.97					

Data in Table 5 shows that the t-test calculated of 0.17 is less than the t-critical value of 1.96 at 158 degree of freedom at 0.05 level of significance. Since the calculated value is less than the t-critical value, the null hypothesis is accepted. This implies, therefore, that there is no significant difference in the mean responses of male and female ICT based business operators on the readiness for IoT solutions for cybercrimes on the bases of gender. The null hypothesis was therefore accepted while alternate hypothesis was not retained.

Conclusion and Recommendations

The main aim of this study is to give an insight into cybercrime in Nigeria and also identify the potentials of IoT devices for cybercrime prevention in Nigeria. Although cybercriminals have not fully utilized the potentials of IoT devices and their vulnerability to attack and cause harm. There are indications that the new and emerging technology will be sought after by hackers and cybercriminals in Rivers State.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 law. Cyber laws should be made available to the public and proper enforcement should follow suit.
- The co-operation of international ccommunities: In the fight against cybercrimes in Nigeria especially in Rivers state, the international community has an important role to play especially for Crimes that require extradition of criminals. This is because most cybercrimes have an international dimension (Security,2017).

Cite this article as
Agbo, O. C., Ugwuanyi, S., & Isaac, U. C. N. (2022). Evaluating cybercrime based on Internet Of Things technology and level of readiness for solutions implementations in Rivers state.*THE COLLOQUIUM*, 10(1), 93 -101

- Education and sensitization of internet users in Nigeria on the dangers of cybercrimes should be taken seriously.

References

Alisdair, F. (2018).Evolution of fraud in the IoT era .https://www.techradar.com/sg/news/evolution-of-fraud-in-the-iot-era.

Broadhurst, R .(2017). Cybercrime in Australia In *The Palgrave Handbook of Australian and New Zealand Criminology, Crime and Justice*, Springer International Publishing.

Furnell, S. (2020). Technology Use, Abuse, and Public Perceptions of Cybercrime, In *The Palgrave Handbook of International Cybercrime and Cyberdeviance*. Springer International Publishing,

Lin,L., Yu,WZhang, N.; Yang,X., Zhang,H., & Zhao,W. (2017). A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications, *IEEE Internet Things J.*, 4(5),125–1142.

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

Tabassum,A; Mustafa, M. S. & Al Maadeed, S. A (2018). 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, pp. 1–6.

Tăbuşcă, A., Tăbuşcă,S.M., & Garais,G. (2019). IoT and EU Law – E-Human Security, *Valahian J. Econ. Stud.*, 9(2), 25–32

The Nigeria CyberCrimes (Prohibition, Prevention, etc) Act, (2015). ICT Policy Africa. https://ictpolicyafrica.org/en/document/h52z5b28pjr.

Thiruchadai, P., Padmavathi,S., & Hemamalini, N. (2020). Engineering Full Stack IoT Systems with Distributed Processing Architecture—Software Engineering Challenges, Architectures and Tools. *Intelligent Systems Reference Library*, 185, 71–87.

Karie,M.N; Sahri,N.M., & Haskell-Dowland,P. (2020). IoT Threat Detection Advances, Challenges and Future Directions, In Proceedings - 2020 Workshop on Emerging Technologies for Security in IoT, ETSecIoT, pp. 22–29.

Vestergaard,L.S., Kasenburg, N., & Jorgensen, M. S. (2019). Implications of conducting internet of things experimentation in Urban environments. Global IoT Summit, GIoTS 2019 – Proceedings.

Cite this article as

Agbo, O. C., Ugwuanyi, S., & Isaac, U. C. N. (2022). Evaluating cybercrime based on Internet Of Things technology and level of readiness for solutions implementations in Rivers state.*THE COLLOQUIUM*, 10(1), 93 -101