**JOSEPH CHAT AYUBA**

**BU/22C/PGS/7636**

**BAZE UNIVERSITY**

**TOPIC: VUNERABILITIES IN INTENET OF THINGS (IoT): A CYBER-SECURITY GUIDE**

**CHAPTER ONE**

**INTRODUCTION**

* 1. **Background to the Study**

The emergence of the Internet of Things (IoT) represents a notable advancement within the realm of communication technology. According to Leloglu (2017), the term "Internet of Things" refers to the interconnectedness of computing devices that are embedded in physical objects, enabling the collection and exchange of data. There exists a vast multitude of wirelessly connected devices, numbering in the billions. Distributed, grid, and vehicular networks represent a subset of the diverse range of devices, infrastructure, and applications that stand to gain advantages from the implementation of the Internet of Things. The Internet of Things (IoT) employs a combination of sensors, processors, and communication hardware to acquire data from the physical environment. Subsequently, these data are subjected to various operations (Dean & Agyeman, 2018). The Internet of Things (IoT) refers to a comprehensive and continuously expanding network of interconnected computing devices that possess the ability to perceive and react to their physical environment. Numerous enterprises often fail to recognize the extent of their utilization of Internet of Things (IoT) devices, thereby remaining unaware of the potential cybersecurity and privacy risks associated with such devices.

The phrase "Internet of Things" (IoT) is employed to denote the interconnected network of devices capable of autonomously collecting and exchanging data, as well as performing tasks, owing to their embedded software, processing capabilities, sensors, network connectivity, and other technological components. IoT devices utilize wireless protocols such as Bluetooth and Wi-Fi for inter-device communication. The aforementioned protocols facilitate the exchange of data between devices and their integration with diverse cloud platforms for the purposes of data storage and processing (Yadav & Vishwakarma, 2018). The emergence of the Internet of Things (IoT) has brought about the aspiration to achieve the highest level of automation in the computing era. The term "Internet of Things" (IoT) pertains to a network comprising interconnected wireless devices capable of autonomously exchanging data without requiring human intervention. In the context of the Internet of Things (IoT), peripheral devices establish connections with a central hub, which may be hosted in a cloud environment. Subsequently, these devices are programmed and accessed through the hub, aligning with the specific requirements of the user. The principal objective of the Internet of Things (IoT) is to enhance the efficiency and effectiveness of frequently utilized devices. The concept of the Internet of Things (IoT) was initially introduced and coined by Kevin Ashton in 1999. The proliferation of the Internet of Things (IoT) is steadily increasing as an increasing number of machines, sensors, and cameras are interconnected with the internet (Gupta, 2019).

 The Internet of Things (IoT) has emerged as one of the most cutting-edge technologies currently available, according to recent research by Radanliev, De Roure, Maple, Nurse, Nicolescu, and Ani (2019). The Internet of Things (IoT) refers to a network of physical devices that are interconnected and capable of communicating with each other via the Internet. This term refers to computers that are capable of sensing, collecting, and transmitting information while being connected to the internet. The Internet of Things (IoT) has a wide range of applications, one of which is the remote management of appliances (Choudhary, Umamaheswari, & Kumawat, 2021). The Internet of Things (IoT) enables the connectivity of various objects to the internet. The Internet of Things (IoT) is poised to have a profound impact on our societal norms and daily routines. Currently, the industry is experiencing significant growth and success. According to analysts, there is a projected acceleration in the growth of Internet of Things (IoT) products and services in the foreseeable future. The term "Internet of Things" (IoT) pertains to a collection of interconnected devices that have the ability to exchange and receive data over a network autonomously, without the need for human involvement. Given the widespread adoption of the Internet of Things (IoT), it is imperative that connected devices provide adequate security measures. In the present era, the imperative to develop a secure device has become increasingly paramount due to the substantial amount of personal data that is stored in digital form. The primary focus in any system is the protection of data due to the increased susceptibility of internet-enabled devices to hacking (Choudhary, Umamaheswari, & Kumawat, 2021).

The complex nature and wide range of technology and data that IoT systems use present security challenges (Lee, 2020). The expeditious resolution of security issues on the Internet of Things is imperative. In an Internet of Things (IoT) environment, ensuring the security of data and services necessitates the incorporation of fundamental features such as confidentiality, accuracy, completeness, authentication, access control, availability, and privacy. In the realm of cybersecurity, the Internet of Things (IoT) possesses distinctive idiosyncrasies and limitations. Consequently, there is a continuous emergence of novel attacks and threats pertaining to the Internet of Things (IoT) on a daily basis (Kandasamy, Srinivas, Achuthan, & Rangan, 2020). Hence, it is imperative that we acquire a comprehensive comprehension of the hazards presented by this technology and formulate strategies to mitigate them. It is imperative to possess a comprehensive understanding of the diverse manifestations of attacks and the corresponding strategies employed to mitigate them. The frequency and severity of cybersecurity attacks targeting Internet of Things (IoT) systems are on the rise, leading to a multitude of challenges for both individuals and businesses.

Vulnerabilities refer to inherent weaknesses present in a system or its design that can be manipulated by an unauthorized individual to illicitly obtain access to information, compromise the system's integrity, or initiate a denial-of-service attack (Skarmeta, 2015). The IoT infrastructure presents numerous potential vulnerabilities that can be exploited by hackers. According to Kizza (2013), vulnerabilities can exist within the hardware, software, policies, procedures, and user components of a system. The proliferation of Internet of Things (IoT) technologies, such as smart grids, patient monitoring systems, the banking industry, environmental monitoring, smart manufacturing, and smart logistics, has resulted in a rise in cyber attacks. The complexity of ensuring security in the Internet of Things (IoT) arises from the dynamic and ever-changing nature of device connections, the diverse range of actors involved in IoT systems, and the limited availability of resources (Pahlevanzadeh, Koleini, & Fadilah, 2021).

* 1. **Statement of Problem**

The Internet of Things (IoT) refers to a network comprising physical and virtual devices that are interconnected and capable of gathering and exchanging data through the internet. This technology facilitates the connectivity and interaction between numerous devices and individuals, allowing for the seamless exchange of information and the provision of personalized experiences, thereby streamlining our daily routines. Although the Internet of Things (IoT) offers numerous benefits, it is important to acknowledge that its deficiency in ensuring data security may present a significant concern (Rudner, 2013). The global expansion of Internet of Things (IoT) devices has led to a rise in the presence of malevolent entities seeking to illicitly acquire personal information and infringe upon users' privacy. Safeguards are necessary to uphold the integrity, privacy, availability, and authenticity of data and services within the Internet of Things (IoT) ecosystem. The Internet of Things (IoT) poses distinct cybersecurity challenges as a result of its unique characteristics and limitations. As a result, a variety of threats consistently target the Internet of Things (IoT) (Kozik & Choras, 2013).

There are several factors that contribute to the heightened susceptibility of Internet of Things (IoT) applications to security vulnerabilities in comparison to traditional computer systems. Firstly, it is important to note that there is a diverse array of Internet of Things (IoT) devices, platforms, communication channels, and protocols available for selection. Furthermore, it should be noted that Internet of Things (IoT) systems are not primarily intended for online interaction. Instead, their main purpose is to establish connections between different physical networks through the utilization of interconnected "things." Furthermore, due to the mobility of users and devices, Internet of Things (IoT) systems exhibit a perpetual state of evolution and possess limited delineations. Ensuring the security of the Internet of Things (IoT) against potential cyber threats poses significant challenges. To begin, it is imperative for Internet of Things (IoT) devices to possess the capability to accommodate an extensive range of protocols, standards, and operating environments. Administrators will encounter heightened challenges in safeguarding these entities from potential assailants (Restuccia, D'Oro, & Melodla, 2018). Furthermore, it should be noted that not all Internet of Things (IoT) devices will derive equal advantages from a uniform security solution. Consequently, there is no universally effective solution for safeguarding the Internet of Things. Additionally, a large number of businesses are involved in the creation, distribution, and installation of IoT devices. Who, then, will assume responsibility for ensuring the security of Internet of Things (IoT) devices? Furthermore, Internet of Things (IoT) devices possess compact dimensions and exhibit constrained storage and processing capabilities.

According to Restuccia, D'Oro, and Melodla (2018), the implementation of security countermeasures on IoT devices poses a significant challenge due to the reliance on computationally intensive algorithms and protocols with high overhead. Wireless security attacks, such as eavesdropping, denial of service, spoofing, message injection, and jamming, pose significant concerns for the Internet of Things (IoT) due to its distributed nature and heavy reliance on wireless data transmission. Consequently, this study aims to investigate vulnerabilities in internet of things (IOT) using cyber-security as a guide.

* 1. **Research Questions**

The following questions are stated to guide the study

1. What are the major vulnerabilities associated with internet of things (IOT) in the Nigerian fintech industry?
2. In what way(s) has IOT vulnerabilities affected the safety of vital information resources and data of institutions in the Nigerian fintech industry?
3. What are the cyber-security strategies adopted by fintech firms to checkmate or address vulnerabilities associated with internet of things?
4. How effective are cyber-security strategies adopted by fintech firms to address vulnerabilities associated with internet of things in the Nigerian fintech industry?

* 1. **Objective of the Study**

The main objective of this research is to investigate vulnerabilities in internet of things (IOT) using cyber-security as a guide. Specifically, the objectives of the study are to

1. examine major vulnerabilities associated with internet of things (IOT) in the Nigerian fintech industry,
2. investigate ways through which IOT vulnerabilities has affected the safety of vital information resources and data of institutions in the Nigerian fintech industry,
3. identify cyber-security strategies adopted by fintech firms to checkmate or address vulnerabilities associated with internet of things, and
4. investigate cyber-security strategies adopted by fintech firms to address vulnerabilities associated with internet of things in the Nigerian fintech industry.
   1. **Research Hypothesis**

The following hypothesis are stated

H01: Vulnerabilities associated with IOT has significantly affected safety of information in the Nigerian fintech industry

H02: Cyber-security strategies adopted by fintech firms to address vulnerabilities associated with IOT in the Nigerian fintech industry are effective

* 1. **Significance of the Study**

The results of this study are expected to contribute to a better understanding of the characteristics and extent of the risks presented by both institutional and espionage-related actors. In order to ascertain the invulnerability of the security solution against malicious attacks, it is imperative to initially identify the potential threats to the system as well as the inherent vulnerabilities within the system. This research is centered on the examination of cyber-security risks and issues within the context of the Internet of Things (IoT). The primary objectives of this study are twofold: (1) to identify and analyze the diverse threats and vulnerabilities that emerge in the IoT domain, thereby pinpointing the associated risks and issues; and (2) to compile the countermeasures and solutions proposed by scholars and authorities to address these risks and issues. These countermeasures encompass both technical approaches and the implementation of security policies. The outcome of this research is expected to be of relevance to financial institutions, fintech users, governments and IoT developers as it will aid in coming up with cyber-security strategies to address vulnerabilities associated with IOT in the Nigerian fintech industry.

* 1. **Scope of the Study**

This study focused on investigating the vulnerabilities in Internet of Things (IOT) using cyber-security as a guide. The research will focus on Fintech institutions in Nigeria due to numerous trend of attacks on information facilities and resources of these institutions.

Create a section called Limitation of study

**1.8 Organization of the Study**

The present study will be structured into five distinct chapters. The first chapter of this thesis will provide an introduction to the topic and present the statement of the problem. The document also delineated the study's aims, research inquiries, significance, and structure. Chapter two will present the review of related literature, while chapter three will discuss the methodology of the study. Chapter four will focus on the presentation, analysis, and discussion of data. Chapter five of this research paper will provide a comprehensive overview of the key findings and outcomes derived from the study. Additionally, it will present a concise summary of the research, followed by a well-supported conclusion. Finally, this chapter will offer valuable recommendations based on the research findings, which can serve as practical guidelines for future endeavors in this field.

**REFERENCE**

* Dean, A. and Agyeman, M.O. (2018) A Study of the Advances in IoT Security. The 2nd International Symposium on Computer Science and Intelligent Control , Vol. 15, 1-5. <https://doi.org/10.1145/3284557.3284560>
* Leloglu, E. (2017) A Review of Security Concerns in Internet of Things. Journal of Computer and Communications , 5, 121-136. <https://doi.org/10.4236/jcc.2017.51010>
* Gupta, A. (2019) The IoT Hacker’s Handbook: A Practical Guide to Hacking the Internet of Things. Apress, Walnut. <https://doi.org/10.1007/978-1-4842-4300-8>
* Restuccia, F., D’Oro, S. and Melodla, T. (2018) Securing the Internet of Things in the Age of Machine Learning and Software-Defined Networking. IEEE Internet of Things , 1, 1. <https://doi.org/10.1109/JIOT.2018.2846040>
* P. Yadav and S. Vishwakarma, “Application of internet of things and big data towards a smart city,” in 2018 3rd International Conference On Internet of Things: Smart Innovation and Usages (IoT-SIU), 2018, pp. 1–5. [Online]. Available: <https://ieeexplore-ieee-org.proxy.lnu.se/document/8519920>
* Radanliev, P.; De Roure, D.C.; Maple, C.; Nurse, J.R.; Nicolescu, R.; Ani, U. Cyber Risk in IoT Systems. Preprints 2019, 43, 2019030104. [CrossRef]
* Choudhary, Y.; Umamaheswari, B.; Kumawat, V. A study of threats, vulnerabilities and countermeasures: An iot perspective. Shanlax Int. J. Arts Sci. Humanit. 2021, 8, 39–45. [CrossRef]
* Kandasamy, K.; Srinivas, S.; Achuthan, K.; Rangan, V.P. IOT cyber risk: A holistic analysis of cyber risk assessment frameworks, risk vectors, and risk ranking process. EURASIP J. Inf. Secur. 2020, 2020, 8. [CrossRef]
* Lee, I. Internet of Things (IoT) Cybersecurity: Literature Review and IoT Cyber Risk Management. Future Internet 2020, 12, 157. [CrossRef]
* Pahlevanzadeh, B.; Koleini, S.; Fadilah, S.I. Security in IOT: Threats and vulnerabilities, layered architecture, encryption mechanisms, challenges and solutions. Commun. Comp. Inf. Sci. 2021, 267–283. [CrossRef]
* J. M. Kizza, Guide to Computer Network Security. Springer, 2013.
  + F. Skarmeta, J. Luis Hernández Ramos et J. Bernal Bernabe, « A required security and privacy framework for smart objects », ITU Kaleidoscope: Trust in the Information Society, Barcelona, Spain, décembre 2015
* Mazini, M.; Shirazi, B.; Mahdavi, I. Anomaly network-based intrusion detection system using a reliable hybrid artificial bee colony and AdaBoost algorithms. J. King Saud. Univ. Comput. Inf. Sci. 2018, 31, 541–553. [CrossRef]
* Schaad, A.; Binder, D. Ml-supported identification and prioritization of threats in the ovvl threat modelling tool. In Data and Applications Security and Privacy XXXIV; Singhal, A., Vaidya, J., Eds.; Springer International Publishing: Cham, Switzerland, 2020; pp. 274–285.
* M. Rudner, “Cyber-threats to critical national infrastructure: An intelligence challenge,” *International Journal of Intelligence and CounterIntelligence*, vol. 26, no. 3, pp. 453–481, 2013.
* R. Kozik and M. Choras, “Current cyber security threats and challenges in critical infrastructures protection,” in *Informatics and Applications* *(ICIA), 2013 Second International Conference on*. IEEE, 2013, pp. 93–97.