KHAZAR UNIVERSITY

School of Science and Engineering

Department of Computer Science

MASTER THESIS

“Assessment of Security Threats on IoT Based Applications: Cyber Security Case Study in Cloud-Based IoT Environment Using the Example of Developing Cloud Information Security Technology in Banking”

By

Oruj Dursunzade

Supervisor:	DR. Saeed Saeedvand
Assistant Supervisor:	PhD con. Behnam Kiani

This thesis is submitted for the degree of Master of Computer Engineering

Abstract

The main objective of this master’s thesis is to emphasise on internet cyber security viewpoint on the appliances and the environment of the internet of things (IoT). In recent studies, there has been an exponential rise in the number of IoT devices and the usage rate of these devices is frequent because they are used in everyday life. Hence, the need to secure these IoT devices is becoming more and more crucial. The specified research methodology was sub-divided into two main parts. The first part of the research was about investigating and studying the environment and the IoT architectural viewpoint. Also, what is currently available in the market, the different types of IoT appliances commonly utilised, and their purpose. This part also clearly emphasises the basic rules used to protect devices in such an environment against the most common forms of cyber-attacks.

Study Design. The study adopted a mixed-method research design utilising case study and pragmatic philosophical reasoning, the exploratory approach was deemed appropriate because it enabled the research to be conducted by emphasising various aspects of the case under review. The study found out that the common vulnerabilities on IoT are malware, outdated software, weak passwords, storing data in clear texts. The vulnerabilities are exploited by cyber attackers to cause a denial of service and other forms of attacks that have caused millions of losses in the banking industry. Improved technology has also lead to increased cyber security risks in the banking industry. Therefore, the banking industry needs to take much care in regards to this and prevent cyber-attack directed to them as high as possible by being on guard always. To overcome the vulnerabilities counter measures must be put in place. Some of the counter measures are regular software updates, installation, and constant checks using antiviruses. Developing automated patching software to mitigate the vulnerabilities.

Keywords: Internet of Things, IoT, cyber security, network, attack vector, privacy

Acknowledgements

Thank you to my father, İlgar Dursunov, EEE engineer himself, for his assistance and guidance in making this work possible throughout my research programme.

Dedication

I dedicate this work to my family and many friends. A special feeling of gratitude to my loving parents, whose words of encouragement and push for tenacity ring in my ears. My sister, who has never left my side and is very special.

I also dedicate this dissertation to my many friends, and one special friend, who have supported me throughout the process. I will always appreciate all they have done,

I dedicate this work and give special thanks to everyone who has been there for me throughout the entire master's programme.

"The Biggest Adventure You Can Ever Take,

Is to Live the Life of Your Dreams"

Declaration

This dissertation is the result of my own work and includes nothing, which is the outcome of work done in collaboration except where specifically indicated in the text. It has not been previously submitted, in part or whole, to any university or institution for any degree, diploma, or other qualification.

Signed:____

Date:____

Oruj Dursunzade

Table of Contents

Abstract i

Acknowledgements iii

Dedication iv

Declaration v

1. **Chapter One:** Introduction 1

    1.1 Background to the study 1

    1.2 Problem Statement 5

    1.3 Research Questions 7

    1.4 Aim and Objectives 7

    1.5 Significance of the Study 7

    1.6. Structure of the Study 8

2. **Chapter Two:** Literature Review 9

    2.1 History of IoT Technology 10

    2.2. Common Exploit Points in IoTs 13

    2.3. Cyber-Security and IoTs' Security 19

    2.4 Theoretical Framework 21

    2.5 Emerging Gaps 23

3. **Chapter Three:** Methodology 25

    3.1. Introduction 25

3.2. Research Approach 26

3.3. Research Method 26

3.4. Research Philosophy...27

3.5. Research Design 28

3.6. Data Collection..29

3.6.1. Case Study Description 30

3.7. Data Analysis 33

3.7.1 Quantitative Analysis..33

3.7.2 Qualitative Analysis..34

3.8. Ethical Considerations 35

3.9. Chapter summary 35

4. **Chapter Four:** Analysis and Results 36

4.1 Scope of the Case Scenario 36

4.1.1 Experiment 1: Apache Server Deployment on a Virtual Machine 38

4.1.2. Experiment 2. Apache Server Deployed in A Kubernetes Cluster.............................38

4.1.3. Security Attack Vector Implementation Case Scenarios 39

4.2 Qualitative analysis 42

4.2.1 Vulnerabilities in IoT...43

4.2.2 Security mitigation practices 48

4.3 Quantitative analysis of secondary data 50

4.3.1 Figure 4.6: sample losses incurred by banks 50

4.3.2 Penetration test analysis of the common vulnerabilities 51

4.3.3 Internal network vulnerabilities 53

5. **Chapter Five:** Interpretation and discussion 58

5.0. Introduction 58

5.1. vulnerabilities from qualitative and quantitative analysis 58

5.1.1. Malware, outdated software and operating system vulnerabilities findings and discussion 59

5.1.2. Weak passwords and device accessibility findings and discussion 60

5.1.3. Data storage vulnerability 61

5.2. Vulnerabilities from case study discussion. 61

5.3. Vulnerabilities interpretation and discussion. 62

5.4. Vulnerabilities mitigation interpretation and discussion 63

5.5. Limitation of the results 63

5.6. Chapter summary 64

6. **Chapter Six:** Conclusion and recommendation 65

6.1. Conclusion 65

6.2. Recommendations for future studies 67

6.3 Chapter summary 68

References 69

1. Chapter One: Introduction

1.1 Background to the study

Gai et al. [1] established that the banking sector has attracted numerous financial technologies, making it a robust and dynamically developing industry in the global technological market. It is necessary to access confidential financial information and various payment transfer methods, including credit cards, SIM cards, and digital currencies, without fear that someone has stolen data or stealing your data. Therefore, automating banking services should maintain the integrity and confidentiality of data. The banking sector is heavily relying on automation developed using the Internet of Things [IoT] technologies. However, such an advanced technology comes with many risks. According to Somasundaram and Reddy [2], financial institutions and their customers are exposed to security concerns often perpetrated by fraudsters who utilise insecure IT infrastructures when accessing personal user data via unstable IoT platforms. However, due to idea drift and data imbalances, one of the enormous technological hurdles that influence the implementation of IoTs is limiting fraudulent and harmful actions.

The twenty-first century has experienced robust transformations in digital revolutions and expansions. For instance, Information and Communication Technologies [ICTs] are being used in enhancing productivity, efficiency, and service delivery [3]. Technology, especially IoTs, has had a tremendous impact on the banking sector after introducing microchips and cloud computing, which rely on internet communication [4]. According to PwC 2018 [5] report, IoT technologies are already becoming a reality. Businesses that have adopted the technology are gaining a competitive advantage through cost reduction and the development of new income sources due to full automation [5]. As computer-integration increases globally, detecting cyber-attacks in sensitive sectors like the banking sector is becoming more complex, developing more sophisticated techniques and further research into how fraudsters exploit IoT technologies. Subsequently, the connection of IoT devices for efficiency is drawing increased attention and significance in the banking sector because every financial institution struggles to make its services more efficient and available to clients [6]. The struggle is associated with the risks that the industry faces in terms of internet money laundry, as fraudsters keep track of almost all systems accessible to the users to explore loopholes in them.

Consequently, the increase in the connection of IoT devices has resulted in a subsequent rise in cyber-attacks because most of the applied technologies are not thoroughly tested to ensure they are not fully vulnerable to attacks [6]. Therefore, in most cases, the technologies have loopholes in them that the attackers have always tried to exploit. The major cause of this is the overreliance on innovations brought by computer programming, which has aided innovation and the development of new applications. According to Castiglione, Pop, and Ficco [7], the application development process involves coding, and the process at times leaves some programming bugs. When hackers identify such bugs, they may exploit them and launch attacks on such applications and even on the entire device.

Analysing cyber-attacks in an IoT network flow with numerous devices accessing and processing different forms of data has become challenging for malware intrusion detection systems [8]. Moreover, the contemporary world is increasingly integrating the use of IoT networking in every aspect of life, thereby becoming over-reliant on the use of the internet. According to Khan and Salah [9], IoTs are computing environments of interconnected devices, systems, and networks comprising distinctive features that enhance or facilitate the transfer of data across varied multiple networks without necessarily involving or relying on human input known as man-to-man interactions. Borkar et al. [10] further note that Internet-connected devices and systems using IoT technology provide users with platforms where they can initiate or facilitate communication with each other and send relevant data without the assistance of human intervention. Thus, IoT-connected devices have been enabled to create real-time data that can be analysed and used to create business projections and results. However, one of the major problems faced by IoT systems is security breaches resulting from numerous vulnerabilities to malware attacks [3]. According to Khan and Salah [9], because over 90% of IoT data is stored in the clouds, there is a high likelihood that cloud providers will always be under attack necessitating the need to mitigate malicious attacks from hackers and security threats from data breaches especially in blockchains and other sensitive financial technologies which attract many fraudsters due to the financial gain.

IoT technologies and devices continue to attract numerous users, and the number of electronic and computerised devices increases as well as the reliance of these devices on the IoT networks increase [11]. Hackers mainly target IoT devices because they lack inbuilt security features. The majority of the user of IoT technologies lack the required knowledge to use the platforms, thereby making weak login credentials within the development cycle and use of the systems. Additionally, contemporary malware developers have changed their malware design approach and developed malware to avoid detections [11]. Newer and advanced techniques have been used to change the internal detections of the malware and avoid exposures, for instance, the Intuition Detection Systems (IDS) cannot do many detections nowadays[3]. Initially, the IDSs were used because they were accurate and provided timely alerts whenever security breaches occurred besides offering useful and illegal information about user activities [10]. According to Mahdavinejad et al. [12], most of the malware available today in IoTs is characterised by camouflaging behaviours and sets of changing features. As a result, techniques such as signature-based are likely to fail in their attempts to detect new malware. New malware should always be distinguished from old malware since thousands of malware are being released each day. Effendy et al. [13] note that there are limited techniques to examine and describe IoT malware. Although few are available, they have poor malware detection accuracy or attract high machine learning costs, yet separating new and old malware decreases system protection ability. This implies that there is a need for the development of new techniques in detecting IoT threats and increasing protection against threats.

Austin [14] established that having a totally secured system is not realisable and practical in the current computing environment because man is prone to making mistakes, and the technology environment is not yet stable. Traditional security techniques are no longer reliable and should not be relied upon when managing and securing IoTs because IoT platforms incorporate various technologies, including mobile networks, regular internets, fog computing, and non- I.P. network, in their data processing. For instance, Austin [14] recommended that because flow-based anomaly detectors work faster and efficiently than state-full protocol and packet-based anomaly detectors, they should be used in malware detection in IoT. Similarly, Sun et al. [13] suggested that flow-based IDS that use TCP flow, using Benford's Law, were vital and effective in detecting malicious behaviours that are commonly used in malware detection in IoT environments. The results and analysis of Sun et al. [15] indicate that every IoT attack has a unique pattern that can be used to identify abnormal and normal flows. Therefore, studying and analysing network flow attacks is an essential challenge for malware intrusion detection systems and requires a more holistic approach to malware detection in IoT networks.

1.2 Problem Statement

The continuous adoption of technology in every aspect of life has led to increased adoption and integration of the internet in the contemporary age making IoT the next phenomenon in the world of data transfer and communication. Borkar et al. [10] established that there is a steady increase in the adoption and use of IoTs in blockchains and financial institutions globally. The increase in the adoption of unstable IoT technologies in financial sectors has led to numerous cyber-security attacks on both the institutions and users to explore security vulnerabilities of IoT systems and devices. Lohana [16] noted that hackers target IoTs in financial systems and devices due to the lack of built-in security frameworks to protect the devices or the systems themselves from malware intrusions. Additionally, Mahdavinejad et al. [11] established that many surplus IoT devices and systems exist in the current market that malware developers efficiently target to initiate attacks such as the build botnets, which have the ability to interact as decoys with the real user and execute full-scale functions as real users. Furthermore, the introduction of scalable cloud computing solutions, increased adoption of automated sensors, and distributed microprocessor systems offer breakthrough solutions for contemporary modes of life in transportation, agriculture, industrial, healthcare, social, and household sectors. As a result, every sector is turning its attention towards integrating IoT ideas and technologies to implement business ideologies to improve operations and find new opportunities without the available threats they face from the use of IoT. With thousands of new malware released each day into IoT networks, it is imperative to perform an IoT-based cyber-risk assessment to predict cyber-attacks on IoT networks and develop compromise indicators that will be used to detect attacks in an IoT network.

Accenture [17] conducted a study in 2018 on 30 key banking applications and discovered that all 30 had flaws ranging from unsafe data storage to insecure verification and code manipulation. And a similar investigation found that 85% of the evaluated web apps were vulnerable to cyber assaults against their consumers. Insecure data storage, poor cryptography, and other issues make online banking portals and apps a security risk. Boston Consulting Group assessment on cybersecurity, banks and financial institutions face 300 times the risk of a cyberattack as other organisations [17]. These dangers cost financial institutions a lot of money because of the attacks and the consequences that follow. IBM X-Force Threat Detection Index indicated that the banking industry was the most targeted for the third year in a row by 2018. In 2018, it was responsible for roughly 20% of all cyberattacks, regardless of industry [17]. These statistics indicate why there is a continuous need for more study on this topic to explore more on the vulnerabilities and ways to mitigate them hence developing better-secured applications to use the internet of things.

1.3 Research Questions

From the background information and the stated problem, this research provides insights to the question: "how vulnerable are IoTs to cyber-attacks, and what approaches and techniques can be used in mitigating security vulnerabilities in IoT networks?"

1.4 Aim and Objectives

This research emphasised the need to have cyber internet security in cloud computing applications in IoT technology. As such, the guiding objectives were:

i. To identify the available IoT security threats and use their characteristics to determine how financial institutions adopting IoT and cloud computing are to IoT-related cyber-attacks.

ii. To develop artificially intelligent process indicators to identify and mitigate cyber-attacks in IoT environments used in financial institutions.

1.5 Significance of the Study

With increased cyber-attacks in cloud-based IoT networks, there is a need for robust and sophisticated mechanisms in mitigating malicious cyber-attacks and security threats on IoT networks. This investigated and provided more information about malware behaviours and vulnerabilities in cloud-based IoT networks and derives approaches of identifying and mitigating malware attacks in IoT networks. As a result, the findings of this study provide a point of reference for all IoT users, technicians, security systems developers, policymakers, and security systems researchers, especially in the financial sectors, about cyber security risks they face and how they can identify and mitigate potential threats in their systems. The results further enhance a deeper understanding of various malware programmes available in IoTs, thereby providing security managers more insights into the tricks hackers use to avoid detection. The research findings also provide an approach meant to analyse IoTs network traffic and identify potential malware threats and security breaches in cloud computing environments, enabling network managers to mitigate threats in a timely manner. The study adds to the existing body of literature on IoT malware characterisation, behaviour, and mitigation to inform future researchers.

1.6. Structure of the Study

This study was organised into six chapters. The first chapter, Introduction, provided the background, research problem, research question, aim, objectives, and study significance. The second chapter, Literature Review, provides literature and theoretical analysis and identifies gaps on the research topic. The third chapter, Methodology, describes methods used in data collection, analysis, and ethical considerations. The fourth chapter, Results, presents case study analysis and research findings. The fifth chapter discussion provides an interpretation and discussion of results by comparing case study findings to existing literature and further discussion of the theories before outlining limitations of the research. The sixth chapter, Conclusion, provides a conclusion of the study and recommendations for future research.

2. Chapter Two: Literature Review

Appreciating earlier efforts in this field fulfilled three aims. First, it prevented data overload during the project's first data collection stages by giving guidance on creating data collection instruments. Another benefit of conducting a systematic evaluation of existing research was that it helps keep the study focused on the big picture. Finally, when the research reached the data analysis stages, this activity provided an opportunity for expressing a critical examination of the actual "meaning" of the obtained data. This chapter provided a review of past literature and theoretical models on IoT malware, detection, and mitigation, including; IoTs and their characteristics, IoT networks, vulnerabilities commonly used to initiate attacks, and mitigation approach used in safeguarding IoT networks.

2.1 History of IoT Technology

According to Liu, Xu, and Yung [18], research on IoT integrations and implementations as adequate information and technology security solutions is not new. The idea that devices and systems can exchange information on their own without human intervention dates back to the late 1970s during the invention of the "pervasive computing" concept, which was fully integrated into Artificial Intelligence (A.I.). The findings of Wirtz et al. [19] show that it took technologies like A.I. a few decades of development before the introduction of the IoT concept. In technical contexts, the phrase Artificial Intelligence had been well established since its invention in 1956 when scientists at Dartmouth College used it to refer to the ability of computerised devices to have intelligence human-like behaviours such as the ability to understand, learn, act, and making conclusive decisions [20]. On the contrary, Tzafestas [21] established that IoT incorporates research ideologies from psychology, computing, engineering, formal data analytics with proportional logic, thus does not entirely rely on A.I. However, in the mid-1990s, Kevin Ashton exploited the radio-frequency identification (RFID) technology to enable devices to communicate on their own as a remedy to slow optimisation of data and transfer of information between humans inventing the IoT concept. As such, Russell and Norvig [22] conclude that IoT was derived from the exploitations of Kevin Ashton and exists in two main categories. First, IoTs can be categorised based on their ability to apply A.I. and execute functions and show intelligent behaviours like human beings [23]. Secondly, IoTs can be categorised based on its ability to show rational behaviour and actions towards achieving predetermined goals [23].

The findings of Sun and Medaglia [18] show that although it took almost a decade for the phrase "Internet of Things" to become part of everyday life, by the beginning of the 21st century, IoT had become the cutting edge of information technology development. As a result, in 2008, the IPSO Alliance created an alliance of companies that supported developing technologies related to the Internet of Things. According to Sage University [39], in 2012, during the largest Internet conference in Europe's history, LeWeb, the main points of discussion concentrated on the importance of integrating IoT technology, and major multinational corporations began implementing IoTs while major magazines in business analysis, including the Forbes magazine, Fast Company, Wired among others started using the term "Internet of Things" more actively. In 2013, IDC published a study predicting that the IoT market would grow to $8.9 trillion by 2020 [39]. As established in the analysis of Wang et al. [3], the IoT market had surpassed $12.5 trillion by 2019, especially with the introduction of Chatbots in communication in Chinese, American, and European markets.

According to Khan and Salah [9], IoTs refer to a consignment of interconnected electronic devices having different identifiers for enhanced data transfers and do not require human interaction to facilitate end-to-end data encryption, data transfer, and data decryption. As a result, IoTs need various technological integrations to prevent malware attacks and cyber-attacks [9]. The broad adoption of IoTs is attributed to the fact that IoTs have essential advantages over other breakthrough technologies. Similarly, Wang et al. [3] found out that IoT technology is widely used to serve consumers and businesses in general [22]. Additionally, Wang et al. [3] established that to start using IoT, there is already infrastructure being ready to some extent, namely, mobile and fixed networks, and its further implementation parameters like sensors, applications, and platforms are pretty cheap. Likewise, Vangelista et al. [32] established that the spread of IoT in the world has been made possible due to four technological trends, including (1) the decline in the expenditure on computer power, memory, processor, and storage. (2) the decrease in the cost of data transmission. (3) The growth of cloud-based solutions and advanced analytics have made adaptable data storage and analytic software available, enabling information management easier despite the steady increase in the amount of information received. As the number of connected devices increases, a technological ecosystem is needed to support it, as well as a number of suggestions for data collection, transmission, and aggregation, as well as a framework to allow the analytics of this data and the use of it to execute these recommendations.

According to Khan and Salah [9], the continual and growing interchange of data necessitates the creation of new technologies that link us to the real world. These services must also be developed on new business models and deliver new cash flows. There is some evidence to suggest that the adoption of IoT technologies is influenced by the country's economic, technological, regulatory, geographic, and cultural factors [3]. The findings of Wang et al. [3] show that in the consumer market of some countries, the main deterrent of IoT exploration is the low-income level of the population. Conversely, as established in the findings of Vangelista et al. [32], even in abled commercial companies and stable economies, there are still numerous challenges in the adoption of IoT due to prolonged decision-making process during implementation of new technologies, complexities in changing the internal processes, lack of IoT standardisations, and difficulties in integrating IoT technologies into the existing I.T. environments.

The findings of Vangelista et al. [32] show that many firms are adopting IoTs due to the perceived importance they provide, especially with the automation of services, when in reality, they are required to understand the costing aspects and approaches used in securing IoT devices without seeking assistance from third party companies. For instance, Vangelista et al. [32] further identified IoT device management technologies, including Low-Power security encryptions and decryptions, wide-area range networks, short-area range networks, operating systems, IoT processors, IoT ecosystems, and event-streaming processes as IoTs used by different device manufacturers. Yet, they are poorly secured and can be exploited easily by hackers and malware developers. In addition, IoT technology is widely used in Cyber-Physical Systems [CPS] because of the ability of IoTs to monitor physical objects in CPS and act on their own through A.I. and machine learning [ML] techniques to take security measures whenever changes are detected. Similarly, Vangelista et al. [32] postulate that IoT is believed to be the critical enabler in empowering the fourth industrial revolution and, as a result, critical sectors including the health sector, manufacturing sectors, transportation sectors, agriculture, construction sector, financial sectors, supply chain, retail, and energy sectors are heavily integrating IoTs. However, as pointed out by Yoon et al. [33], financial institutions, especially banks, tend to focus on automation of processes and empowerment of the inanimate physical objects to make users' experience more interactive while ignoring key security aspects of the system. Therefore, there is a need for a robust and all-inclusive approach to malware detection to enable support and system developers in the IoT environment to avert the threats.

2.2. Common Exploit Points in IoTs

According to Pozzolo et al. [4], contemporary business demands for financial services have made financial service providers change their service delivery approach and adopt numerous IoT solutions in their automation and service delivery. Similarly, Pasquale established that the integration of technology to ease business transactions has led to the generation of big data compared to the phased out traditional manual transactions. As a result, fraudsters use abnormal coding strands that differ from usual codes creating loopholes for multiple exploit points in devices and IoT systems. Pozzolo et al. [4] further found that because many datasets are generated over time, assimilation of anomalies and malware datasets may take longer to detect, leaving the financial dataset owners vulnerable to cyber-crime activities. Additionally, Lucas and Jurgovsky [8] found that transitioning from physical, financial transactions to multi-channelled digital services provides an excellent operational ground for black hackers to operate. For instance, credit cards technology is a widespread payment option in online markets, and due to their large numbers, they have attracted an increased number of fraudulent activities [21]. Therefore, there is a need to ensure that their security is maintained through different technologies.

Borkar et al. [10] state that interconnecting IoT multiple devices in IoT networks continue to attract more attention because of an increased level of security threats and risks from increased exploit points for malware attacks instigated by hackers who rely on larger datasets. There is a rapid increased generation of big data and cyber-attacks globally, necessitating security system developers and managers to improvise methods that can detect malware in IoT networks and devices in real-time. As established in the study of Broker et al. [10], it is important to characterise IoT malware based on their nature and most vulnerable IoT device to understand malware behaviours and easy identification of malware in IoT environments. Similarly, a study by Kumar and Lim [24] established that malware programmes are engineered based on the nature of data in targeted networks, network administrators' and controllers' communications, and characteristics of attack vectors to be exploited. However, Cozzi et al. [25] established that system managers and security experts have focused on vulnerabilities in specific operating systems since time immemorial. For instance, as established in the analysis of Barr-Smith et al. [26], more research on cyber threats exists, although in most cases, the studies concentrate on exploit points in Microsoft-based systems and android based devices because the two operating systems are widely used globally. Although established by Kumar and Lim [24], IoTs access and use different operating systems, which share similar traffic kernels. Ignoring other operating systems' vulnerabilities in research exposes IoT environments to more cyber-attacks. Subsequently, Smith et al. [26] further note that ignoring other operating systems and devices when studying the malware landscape makes them more vulnerable and easy targets for malicious activities.

Over the past two decades, the number of computer devices has spontaneously risen thanks to the numerous advantages of adopting internet of things paradigms in most aspects of life [22]. To make IoT devices and systems secure, Nayak et al. [27] conclude that developers use three main encryption algorithms: asymmetric, symmetric, and hash functions. According to the findings of Nayak et al. [27], although asymmetric cryptographic algorithms are flexible, they require more power, more memory. They consume more energy, making them unsuitable for securing IoT applications. Symmetric cryptographic functions subsequently comprise stream and block cyphers, which are faster and use simple operations, making them suitable for IoT applications [27]. However, streaming cyphers are fast but suitable for data streaming, while block cyphers are more flexible in their application.

Similarly, Barakhtian et al. [28] observe that block cyphers, such as simple permutation, double permutation, single key permutation, and so on, have been proposed by scientists to protect resource-limited devices in IoT applications. For example, AES is a widely used block cypher to provide security in IoT applications such as IEEE802.15.4, LoRaWAN, Zigbee, Sigfox, ZWave, and it has off-the-shelf hardware accelerators built into commercial products that enable them to protect vulnerable devices. Barakhtian et al. [28] further implemented and evaluated block cyphers based on 8-bit, 16-bit, and 32-bit microcontrollers, focusing on the widely used tinyAES algorithm and other algorithms suitable for embedded platforms. The study emerged that when code size and RAM space do not matter, AES is a strong candidate for securing small devices.

Popov [29] further shows that AES is a symmetric key encryption algorithm that converts data into ciphertext during encryption, and decryption converts the ciphertext back into plaintext. As shown in figure 1, typical AES requires initialisation and involves several steps during encryption and decryption.

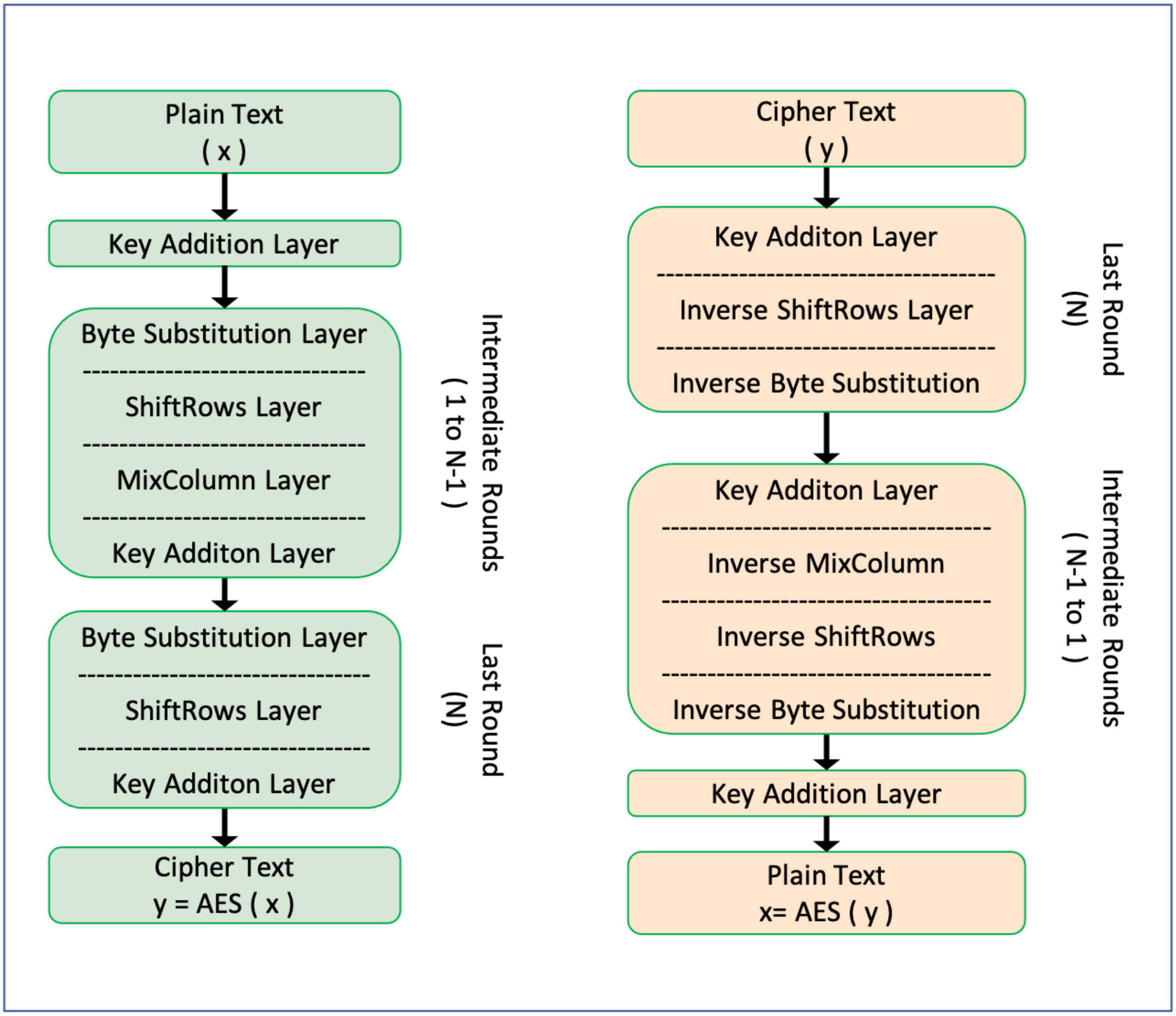


Figure 1: AES encryption processes [Popov, 2020]. (Compiled by the Author)

During the initial stages, key expansions and initial rounds are performed, followed by series of encryptions using the expanded keys from the key expansion step. After various rounds, encrypted texts are passed through to the final round evaluations are done to ensure the number of rounds increases in the form of 10, 12, 14, and so on, along with the subsequent key sizes of 128, 192, 256 bits, respectively. The keys used for each round are generated from the original key during the key expansion phase. Thus, different keys generated from the original key are used for each round. Conversely, Costin and Zaddach [30] established that IoT devices are vulnerable to cyber-attacks because they do not have proper security attributes due to over-simplified networks and device designs that make it easy for hackers to exploit the networks. For example, in their study on analysis of IoT malware framework, Costin and Zaddach [30] found out that when designing IoT systems, developers fail to consider the modularity and extensibility of the systems. Since more energy is required for data transfer, the transfer durations ought to be minimised for adequate encryptions to occur. But since less attendance is driven towards sensors and micro-controllers by developers, hibernations are preferred to reduce power consumption instead of lightweight encryptions algorithms. Yet, they provide the necessary security and privacy at all levels while ensuring low latency and power consumption [5]. Similarly, Barakhtian et al. [28] argue that the AES-256 provides adequate security but limits system resources such as time, memory, and energy, preventing developers from using low-power peripherals in their respective IoT applications.

Moreover, Karanja et al. [31] explain that most of the current IoT networks are complex and more sophisticated. As a result, many networks vary greatly from traditional personal computer networks. Thus, malware developers modify the three main properties used in detecting malware in traditional networks and use the modifications interchangeably to exploit

IoT networks in the current operational environments [31]. Vangelista et al. [32] identified the use of brute-force attacks to access IoT devices, IoT ports like the HTPPs, telnet, and FTPs, and Distributed Denial-of-Service [DDoS] attacks as the most used modifications used interchangeably to initiate IoT attacks. All three can be implemented by the IoT software specially programmed malware without human intervention. Vangelista et al. [32] further note that, typically, viruses in IoT networks and devices spread too fast for the unsuspecting user to realise their existence [37]. For example, Khan and Salah [9] established that IoT viruses in the Mirai family are silent and have the ability to affect IoT devices in a very span of time adversely. Mirai virus exploits open Telnet ports to access IoT networks, and after entering the network, they initiate multiple attacks on vulnerable devices by tampering or duplicating login credentials. This provides a DDoS attacker with the chance to access and exhausts server properties as well as initiate surges to the website's load timers.

Yoon et al. [33] further concluded that when a DDoS attack is actualised in a website, it can lead to poor performance issues such as the website failing to respond to users' commands or errors in network connectivity. In another case, Weaver et al. [50] established that the central processing unit [CPU] of devices, as well as the device's memory, may also crash when a severe DDoS attack occurs. As such, cyber-attacks initiated or implemented through IoT devices are the most severe attacks and lead to huge disruptions in business operations. According to Yoon et al. [33 pp 354] findings business operations are largely affected because the attackers completely disable internet network connections of affected devices or crash the devices, thereby interrupting normal organisation functions and activities and, in some instances, personal data may be accessed by unauthorised personnel, leaked out, altered, or erased in the event. Researchers have been able to identify vulnerable points of attacks in IoTs and the potential devices to be attacked when IoT security breaches are orchestrated. However, it is unclear how the attacks are initiated to determine how to differentiate or prevent the attacks.

2.3. Cyber-Security and IoTs' Security

The emergence of IoT devices has dramatically expanded the list of devices connected to the internet. According to Khoshhalpour and Shahriari [34], hackers can freely access and isolate the most vulnerable devices from the highly secured devices and use them to learn their security system. However, Humayun et al. [10] found that, unlike conventional servers where it was not possible to initiate an attack unless remotely executed and have specialised protection systems, IoT devices are more vulnerable to unauthorised access because they rely on cloud computing. The widespread distribution of IoT devices means that if one device is compromised, the manufacturer will not be able to quickly recall all devices and update their security system [10]. Similarly, Khoshhalpour and Shahriari [34] established that hackers easily infiltrate IoT networks because one unsecured device can provide access to a wide range of other devices on the network enabling access to sensitive data, from bank details to medical records, and even crucial corporate information, given that many people use varied devices both at home and work. According to Kumar and Lim [24], cyber-attacks are initiated in phases while avoiding detection using unsecured devices to exploit networks of more secured devices and systems.

Kumar and Lim [24] further established that the first stage of a cyber-attack is infection and propagation, where the botmaster concentrates on infecting other bots via a new host on a local network or by tricking device users through page redirects. In the second stage, the botnet concentrates on concealing its presence and deactivates the protection systems. In this case, it deactivates or disables the anti-virus software. Once the security of the device is compromised, the bot moves to the third stage and concentrates on connecting to the command and control

[C&C] server, and if in a distributed system network, it sends SYN commands to other devices to establish a connection and command over other devices in the network as part of the botnet family. In the fourth stage, the malicious bot concentrates on maintaining stable communication while obtaining valuable information about the network and concealing the information. Once reliable data and information have been acquired, the malicious bot moves to the remove and release stage, where it initiates the threat and attack to escape the network without detection through the unsecured devices. In a similar view, Kolias et al. [36] postulate that Mirai family malware imitators and variants were identified to have been used in the first major Distributed Denial of Service attack in History in August 2016. Further research and analysis by Kumar and Lin [24] showed that malware families like the Mirai family of malware existed for a long time because their built-up designs are based on pre-existing IoT botnet malware like the Bashlite, making them hard to detect. The functionality of such replicating malware families is straightforward because they spread by connecting with randomly identified insecure devices via Telnet ports and modification of login credentials in a hard-coded list.

Similarly, Lee et al. [35] established that Mirai malware spread faster through unsecured network devices such as printers, routers, cameras, and digital video recorders (DVRs). However, according to Kolias et al. [36], malware mutations are generated daily and cause real damages to devices because they can proliferate continuously. The continuous proliferation process renders device manufactures and vendors' chronic neglect in the wake of applying security practices. It also emerged in the study of Kolias et al. [36] that, Bashlite or LizardStresse as commonly referred to is a notorious IoT bot that replicates behaviours of IoT malware and engraves its code in other malware to avoid detection or confuse the anti-virus software to believe it has dealt with the real malware when it has deleted the decoy [83-84]. Similar findings were in the reported analysis of Munchester [37] who identified Hajime to be another family of IoT malware families that spread in IoT networks by emulating the behaviours of other malware like the Mirai family of malware does. According to Munchaster [37], Hajime viruses are non-centralised but just like the Brickerboot, they rely on fully distributed communications and exploit the network by bricking the devices to destabilise them before using them as bricking bricks. As such, similar to Mirai, the Hijame malware family initiates DDoS attacks in IoT devices by erasing all files from the device's memory and later defaces the device's firmware [37]. Munchaster [37] also states that behaviour emulating malware families Hijame and Mirai families are dangerous because they are engineered to specifically implement financial binary attacks. These types of malware are designed to alter financial data including user account data and credit card information. According to the findings of Kolias et al. [25] behaviour emulating malware, families are commonly used in initiating attacks in financial IoT-based networks because they can be used as toolkits and purchased or easily deployed by anyone for specific purposes. Thus, since they self-replicate themselves, it makes it easier for this malware to insert itself into other files and remain silent for long and without detection cause huge damages to users' files or programmes.

2.4 Theoretical Framework

According to Sáenz-Royo et al. [23], the diffusion of innovation theory [DOI] provides a good conceptual framework for understanding what motivates organisations' I.T. managers towards adopting new and emerging technologies. Developed by Rogers in 1962, the DOI theory is established on five pillars of innovations. According to Sanni et al. [20], the first pillar of DOI theory is compatibility and refers to the ability of the emerging technology to adapt to the existing systems and operational environment. The second DOI theory pillar is the relative advantage conceptualisation and deals with the extra benefits that are or can be gained by the implementing institution compared to the existing technology [40]. Sáenz-Royo et al. [23] identify trialability as the third pillar of the DOI theory. This pillar addresses issues related to the new technology's ability to be tested or piloted before adoption. According to Sanni et al. [20 pp 257], the fourth DOI theory pillar is observability, which refers to the resulting effects of adopting the new technology. Yung-Ming [40] identifies the final pillar of DOI as complexity, which addresses the difficulties that users may face while learning the new technology.

According to Sáenz-Royo et al. [23], the basis and suitability of the DOI theory to research on the threats provided by IoT relies on the ability of IoT technology to provide firms with a relative advantage over existing technologies but be compatible, able to be assessed, and less complex to implement so that hackers and unauthorised users cannot find easy loopholes to exploit the technology. Similarly, Penjor and Zander [39] state that not only should new technologies be compatible, but they should also be experimented on through trials and observed by adopting firms to ensure they are not complex to the users. Yung-Ming [40] notes that the most integral part in the adoption of new technology is to ensure the devices are secured in a way that they cannot breach privacy while at the same time ensuring the devices used are reliable for the adoption of the technology. The objective of the current research was to cyber-security issues, how privacy breaches are initiated, and reliability strategies in mitigating security threats in IoT technologies adopted in the banking sector. Therefore, the DOI theory was used to understand the motivations that drive I.T. leaders in the banking sector to adopt IoT. However, Panagiotopoulosa et al. [41] conversely identify that the DOI theory's major weakness is that it only concentrates on the diffusion of the new technology to effectively adapt to the existing environment and not the value of the new technology for digital governance.

To deal with the weaknesses of the DOI theory, Bannister and Connolly [1] postulate that the public value theory provides a better understanding of how the management of resources and services are delivered by emphasising service delivery, costing, efficiency, and security. Moore developed the public value theory in 1995 and as postulated by Panagiotopoulosa et al. [41] it assesses the impact of management initiatives in providing and delivering social and economic outcomes that reflect the expectations of the targeted users. As such, Bannister and Connolly [46] argue that although the public value theory does not account for digitalisation initiatives [11], the constructs of this theory provide strong foundations when studying the impact of technology in public management [9] and achievement of a win-win scenario for both the firm and the public using the technology [31]. Therefore, the public value theory is a more encompassing approach to account for complexities in transformation, which is necessary during the transition from focusing on service delivery to fulfilment of users' expectations in the public domain like the banking sector.

2.5 Emerging Gaps

As observed in this review, research on the integration of IoT technologies is still limited and scarce, while available studies largely concentrate on the expected effects of IoT adoption. It also emerged that research on IoTs' impact is more speculative. Researchers tend to relate the potential impact of IoT across multiple sectors without narrowing the research to specific sectors because the operational environments in every sector with the adoption of technology differ significantly. From the review, it is also evident that there is no proper understanding of the categories and families of IoT cyber threats orchestrated through cloud computing as the majority of the researchers concentrate on malware attacks while there are many ways through which IoT devices can be used to initiate cyber-attacks like through cyber-physical exploits of cloud computing platforms. Although different researchers have investigated the types of malware in IoTs, there is a lack of practical proof on how this malware can be used to initiate cyber-attacks in IoT-enabled cloud computing environments, which is a fundamental step in understanding the severity of the threats posed by different malware. Additionally, no empirical evidence is available to account for the cyber-threat threshold in IoTs used in the public sector like the banking sector, which is a very important public domain. Therefore, to enforce proper IoT network analysis, malware threat categorisation, and implementation of a structured IoT network security restriction, this research provided a practical case study approach on how security exploits can be initiated in IoTs used in the banking sector to under understand how cyber-attacks are orchestrated and develop artificially intelligent process indicators for identification and mitigation of cyber-attacks in IoT environments.

3. Chapter Three: Methodology

3.1. Introduction

Methodology forms a critical part of any research as it articulates how the research will be conducted. For the most part, this chapter explains how the study was conducted. It gives details on the research approach used and explains why it was chosen for this particular project. The chapter also discusses the various stages of the research, such as the selection of participants, the data gathering method, and the analysis of data. As such, the chapter discusses the preferred types of data types and adopted strategies used while conducting the research, including the used philosophies, research designs, choice of the method, data collection approach, data analysis systems, and ethical considerations.

3.2. Research Approach

The research employed both inductive and deductive reasoning design to find out how vulnerable are IoTs to cyber-attacks and the approaches and techniques that can be used in mitigating security vulnerabilities in IoT networks. Inductive reasoning was fundamental in analysing real-life experiences as observed in the experimentation with the codes to show how cyber-attacks are initiated. As observed by Herman [47], inductive reasoning meant that inferences can be drawn from the evidence as observed in the coding experiment and case study analysis. Subsequently, deductive reasoning was fundamental in deducing facts from critical analysis of published information and views about the case to develop an informative inference. According to Creswell and Creswell [42, 43], it is important to limit the choice of the preferred research design to options compatible with the preferred philosophy and approach because harmony between the two is critical in helping the researchers collect the most appropriate data for analysis.

3.3. Research Method

To answer the question, 'how vulnerable are IoTs to cyber-attacks and what approaches and techniques can mitigate security vulnerabilities in IoT networks?', it was important to analyse numerical data and key themes emerging from qualitative data. This is important as the frequency of cyber-attacks could be analysed from the qualitative data as well as using the numeric data to give a visualisation of data. This is important for getting the extent of cyber-attack damages [22]. As such, mixed-method research was adopted for the study because it utilises both quantitative numerical data and qualitative reasoning and views to make sense of a research phenomenon. According to Creswell [42], the mixed-method research method is suitable for scientific research because it allows for the inclusion of both qualitative and quantitative data, thereby broadening the perspectives used during data collection and analysis and, as a result, robust conclusions were realised from the study. Additionally, the mixed-method is suitable for case analysis in scientific studies because it contributes to the achievement of more concise answers through comparison of both factual numerical findings and themes emerging from different views and experiences of the phenomenon.

As established in the literature review, there are numerous studies that have experimented and investigated cyber-attack prevention mechanisms for IoT environments without achieving the desired acceptable threshold. Some of the critical aspects for this research were the specific effects that cyber-attacks pose to the security decision-making processes of IoT users, especially those manufacturing IoT devices for use in the banking sector. The mixed method allows for analysis of numerical data obtained from the case analysis and experimentation using the coding process. This information was key in evaluating the truce in qualitative data that was obtained after the available interventions failed or successfully mitigated cyber-attacks in the IoT environment to develop themes.

3.4. Research Philosophy

According to Howell, pragmatism gives prominence to the main problem under study by giving priority to the practical results [48]. Pragmatic philosophical reasoning was fundamental in this research because it enabled the adoption and utilisation of practical data obtained through a mixed-method design in answering questions on current ways of mitigating cyber-attacks in IoT networks. Additionally, it was important to focus available data on secondary sources for further evaluation of the case scenario because they give an in-depth exploration of the cyber security cases [28]. Understanding how cyber-attacks are orchestrated in IoTs and malware behaviours in IoT networks was beneficial as it provided the basis and background information for the implementation of corrective mitigation approaches such as ML and A.I. to safeguard IoT networks. Howell [48] states that pragmatic reasoning in a mixed-method research design provides an appropriate avenue to obtaining the best research findings because they enable a researcher to manipulate independent variables representing the causes and measuring dependent variables representing the effects controlling the extraneous variables. Thus, pragmatism was fundamental in keeping the research within the desired scope.

3.5. Research Design

Since the study adopted a mixed-method utilising case study and pragmatic philosophical reasoning, the exploratory approach was deemed appropriate because it enabled the research to be conducted by emphasising various aspects of the case under review. There are numerous studies on the mitigation of security threats in IoT, which makes the choice to be viable for this study [23]. Moreover, the exploratory research approach allowed for an investigation into the specific cyber-attacks targeting IoTs and initiated through cloud computing to understand behaviours of malware used, categorise the malware, and determine how hackers exploit IoT devices in banking IoT environments. This is important for this study as it will enable the researcher to be able to answer the research questions adequately. According to Ganin et al. [44], the exploratory design is important when analysing cyber activities because it eliminates the possibility of incorporating or relying on existing assumptions in research to make conclusions about the phenomenon. Franklin [45] further states that an exploratory research design also expands on the scope that a researcher can rely on while addressing issues that emerge during a case study or experimental study. As such, the approach also allowed for the utilisation of existing tools of experimentation and augmentation to analyse the factual information about the case and draw comparisons to various topics presented in research before making conclusions

[46]. In the current research, these tools were fundamental in analysing specific cyber-attack mechanisms and malware intrusion behaviours during IoT attacks.

3.6. Data Collection

The purpose of this research was to assess the safe operation of IoT cloud-based network equipment and software for banking services through assessment of the information risks levels. As such, a case study approach was adopted for empirical data collection procedures on how cyber-attacks are initiated and executed within the context of a banking system using multiple IoT devices within the public domain [50]. To successfully implement and detect cyber-attacks or malware attacks to an IoT network or device in real-time, it was imperative to design a security threat detection model in a simulated environment. ML and A.I. algorithms would be implemented to learn and detect intrusions in real life. Additionally, primary and secondary data comprising of published interviews from stakeholders in the banking sector, grey data from policy documentations, excerpts and printouts from cyber-attack penetration tests, presentations in the banking sector, and key analysis from IoT device manufacturers and technology firms were consulted. The data was obtained from ptsecurity.com, and cyber hunter solutions, and science.gov websites. These published secondary materials of data were important in ascertaining the truth level in the primary data obtained during the simulated experimental processes [50]. The quantitative data was mainly obtained from the simulated case scenario experiment and secondary data from published penetration tests, which is a test done by organisations for vulnerabilities identification, testing, and highlight. The qualitative data was obtained from secondary materials including published interviews from stakeholders in the banking sector, grey data from policy documentations, excerpts and printouts from general users' interviews, presentations in the banking sector, and key analysis from IoT device manufacturers and technology firms. The topic “vulnerability in the banking industry” was searched on sciencedirect, google scholar, and science.gov, and a sample of studies was selected for thematic analysis.

3.6.1. Case Study Description

In this study, it was considered that technology for cloud service implementation in banking is determined by the presence of a number of limitations. As such, the processes of collecting, processing, and storing banking data are subject to the manifestation of information risks. Thus, the premises where server equipment is located should meet special security requirements, including controlled accessibility, use of certified software and hardware equipment, and adoption of cryptographic protocols for remote access communication channels to virtual servers. However, most cloud service providers cannot provide the level of information security required for banking operations. This leads to the implementation of cloud solutions using IoTs by the banks themselves using their own resources, which are unsecured and pose a huge cyber threat.

In this case, the "Software as a Service" [SaaS] model of cloud computing was implemented using the "Private" model. Thus, a simulated model environment was adopted where virtualised servers were installed in data centres hosting client information for a commercial bank. Users were allowed to communicate to the bank via IoT devices through cloud computing services from different locations and other means of communication. After authorisation, users went through authentication procedures before being allowed access to all the bank's applications and services to its clients. The virtual banking office model in figure 2 was adopted to simulate a commercial bank with multiple remote location branches all accessing one cloud-based Server based on PaaS cloud service. The public hybrid cloud-based server service was installed with virtual desktops equipped with preinstalled operating systems, a set of office applications, a client module of the CRM system, a scoring programme, a mailing module, and other tools, the composition of which is agreed with many banks.

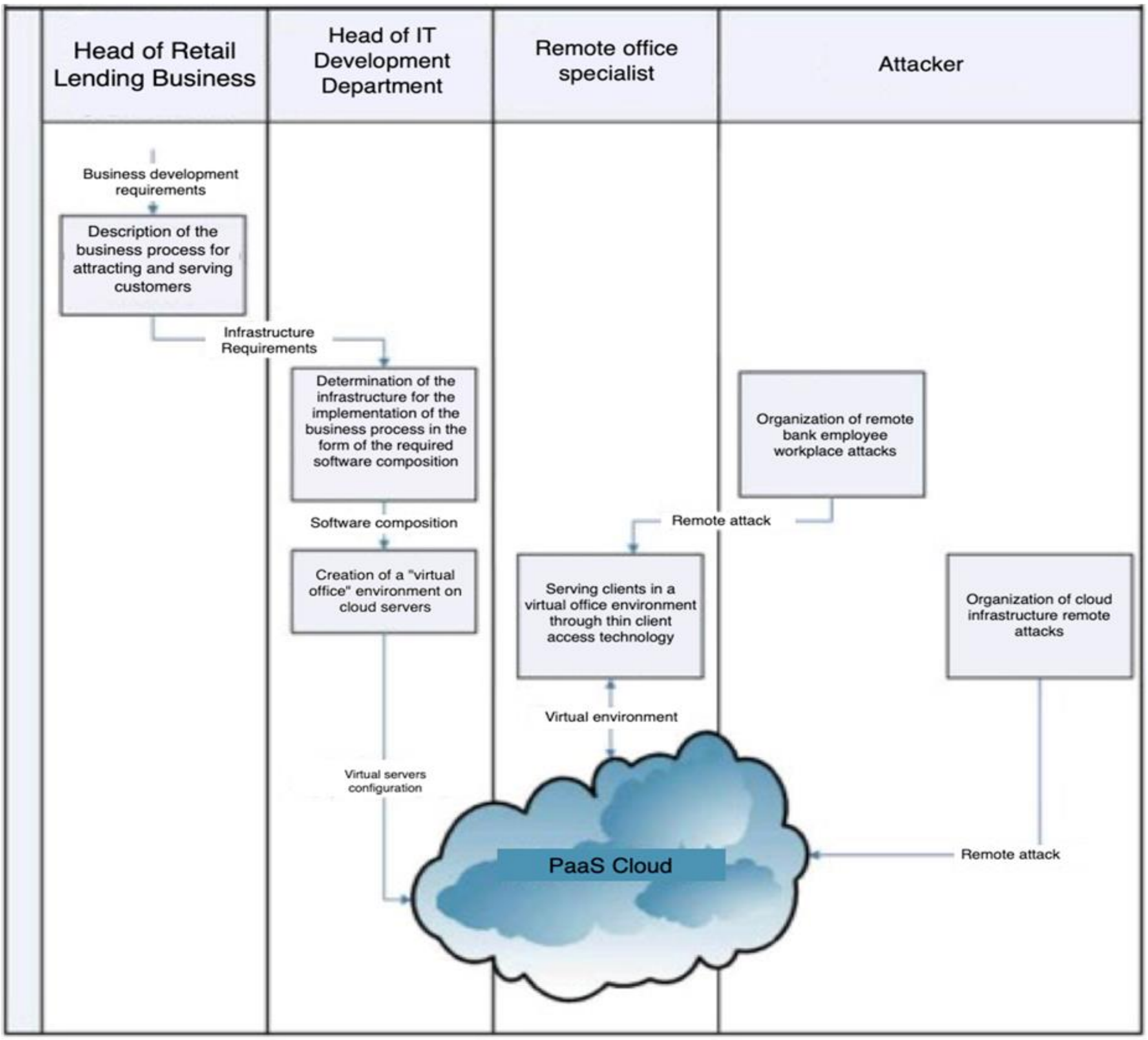

Head of Retail Lending Business
Head of IT Development Department
Remote office specialist
Attacker
Business development requirements
Description of the business process for attracting and serving customers
Infrastructure Requirements
Determination of the infrastructure for the implementation of the business process in the form of the required software composition
Software composition
Creation of a "virtual office" environment on cloud servers
Virtual servers configuration
Organization of remote bank employee workplace attacks
Remote attack
Serving clients in a virtual office environment through thin client access technology
Virtual environment
Organization of cloud infrastructure remote attacks
Remote attack
PaaS Cloud

Figure 2: Simulated cloud banking service process "Virtual Workplace." [Source: Compiled by Author]

When opening a new remote workstation, all a person needs is a network connection to the Internet and a terminal to access the cloud server. Users and new branches were not allowed to use a fully-featured personal computer, additional licenses, and information security tools. The cloud service was implemented using PaaS technology with virtual office deployed in the bank's internal private cloud to enable the main bank to physically control the security of the server equipment. Banking services provided directly to customers had the following properties: reliability, security, accessibility, and scalability, all of which are common when customers make electronic payments, as indicated in figure 3.

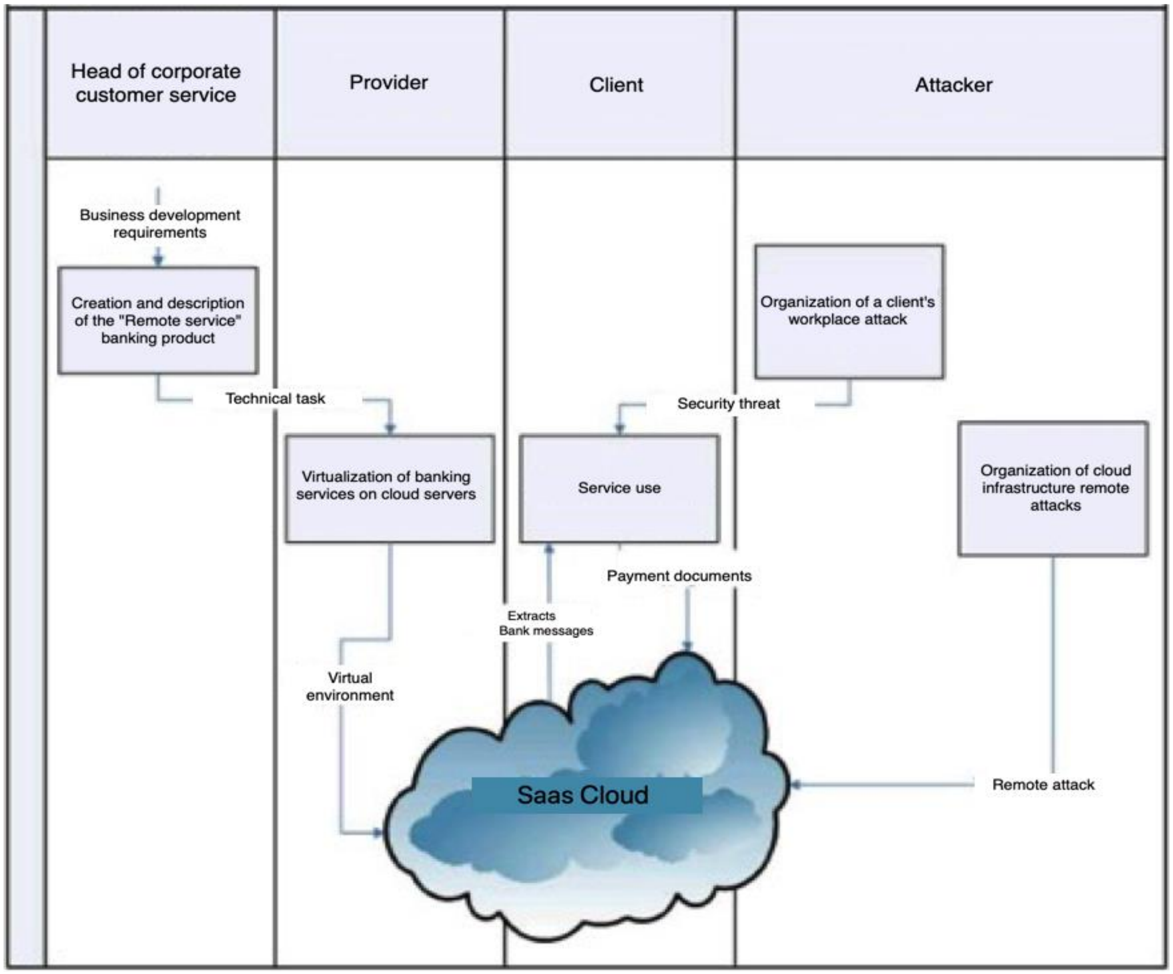

Head of corporate customer service
Provider
Client
Attacker
Business development requirements
Creation and description of the "Remote service" banking product
Technical task
Virtualization of banking services on cloud servers
Organization of a client's workplace attack
Security threat
Service use
Organization of cloud infrastructure remote attacks
Payment documents
Extracts Bank messages
Virtual environment
Saas Cloud
Remote attack

Figure 3: Simulated remote banking service organisation. [Source: Compiled by Author]

It was also assumed that SaaS technology from a third-party provider is used when providing remote service to corporate clients. The bank in question used rentals for software installed in the public cloud, which was developed by another company, Centre for Financial Technologies [23]. The bottleneck in this scheme of work is that it is necessary to develop a technology to migrate data from cloud servers to the bank's automated system and CRM system, which are completely inside the organisation. Providers on the market offer other SaaS solutions: business intelligence systems, KPI analysis and control systems, and project and portfolio management systems. The developer of the software that was based on SaaS services can be the bank itself or a third-party vendor with access to the bank's critical data [28]. The system is installed on cloud servers of the data centre of a third-party provider. Client access is organised by SaaS technology which can be exploited by a hacker easily.

Performing real experiments on these cloud computing technologies such as SaaS is expensive and may cause problems such as decrease in speed of execution [32]. Therefore, a simulation was vital to ensure that the aim of the research is attained [26]. The simulation that was used in this experiment was to install HTTP apache server and Kubernetes cluster on virtual machines. The virtual machine was then used to experiment with the impact of hacking the Virtual machine on request processing. The data from the experiment was collected for the purpose of analysis

3.7. Data Analysis

There are rapidly changing cyber-attack mechanisms, malware, and specimens in the current contemporary IoT environments. For this study, data analysis combined both quick reporting through static analysis and opcode features through dynamic analysis to implement a more robust simulated system.

3.7.1 Quantitative Analysis

According to Cherrington et al. [51], if the input data is numerical and the outcome is categorical, as was the case in this study, the analysis of variance [ANOVA] is the most suitable statistical analysis tool for testing the data and if the data used and the output is categorical, the Chi-Squared should be used. The current study involved experimentation where numerical data was used in the first incidence as the input data during the simulated experiment. After the application of the filter method to identify malware attack vectors, categorised data was used as input data in the simulated model. As such, both ANOVA and Chi-Squared tools were used for quantitative data analysis. The analysis was done descriptively through trend analysis of malware intrusion performance based on speed, attack vector populations, and the effect on the device performance using tables and figures.

3.7.2 Qualitative Analysis

After the identification of key secondary materials, qualitative data was obtained and analysed thematically according to its appropriateness in evaluating the performance of the simulated algorithm. Manual thematic analysis using codes was used because it allows the researcher to develop themes from the secondary [21]. A two-step coding process as designed by Castleberry and Nolen [56] was adopted. The first-round coding aimed at identifying specific sub-themes on cyber-attacks in IoTs and the challenges that banks face in securing IoTs as they implement them in the public domain where numerous IoT devices exist. The second coding process involved regrouping the sub-themes into abstract codes to synthesise them into more distinctive classes of themes. As such, the research materials were read to have an acquaintance with the content. The materials were re-read to have a better understanding of the data and codes generated. After understanding the research content, data from the studies were categorised based on emerging sub-themes, authors' observations, and original participants' and experimental accounts. Finally, a connection was made between the research findings, researchers' accounts, and recommendations to establish the thematic contribution of the studies to the current research.

3.8. Ethical Considerations

The study adopted a case study analysis using a simulated computer environment and published secondary data as primary sources. Thus, this research did not necessitate any ethical approvals. However, since the study is part of academic discourse, academic requirements with regard to submission of plagiarism-free academic work were followed. Therefore, all materials referred to or consulted during the research process were acknowledged at point in-text reference and thereafter included in the work cited list herein at the end.

3.9. Chapter summary

In summary, the research will adopt a mixed methodology that combines both qualitative and quantitative analysis. In addition, the research employed inductive and deductive methods in its approach. Qualitative data was analysed through thematic analysis, while quantitative data was analysed using data analysis software to give a visualisation of the results of all the analyses. The study ensured that all ethical issues were followed to the letter to avoid interfering with people's privacy.

4. Chapter Four: Analysis and Results

4.1 Scope of the Case Scenario

This research aimed at investigating the operations of the IoT device protocols in a simulated implementation of an edge local cloud computing environment. The basic "HTTP" protocol was chosen because it is the universal protocol used to design and build IoT applications and resources used in IoTs' communication. To study the performance of the modelled network in figure 4.1, two comparative experiments were conducted, and the server response time was used as the key performance measurement indicator. Subsequently, a python developed script was used to describe how to send the get-requests with session creation servers using aiohttp and asyncio libraries to provide multi-threaded request generation, which has increased the performance of requests per second compared to the traditional urllib libraries. Requests were generated based on the rates of requests made per second between 10 and 50 requests per second with a sequential increment interval of 10 requests. An iperf3 tool was run on both ends of the client-server connection for the duration of the traffic generation to load the communication channel with TCP connections. The client started with the following parameters: 100 concurrent requests and a read/write buffer length of 10000 kB. These parameters reflect the actual load from the Internet of Things devices. The duration of each step was 2 hours, which minimises the measurement error.

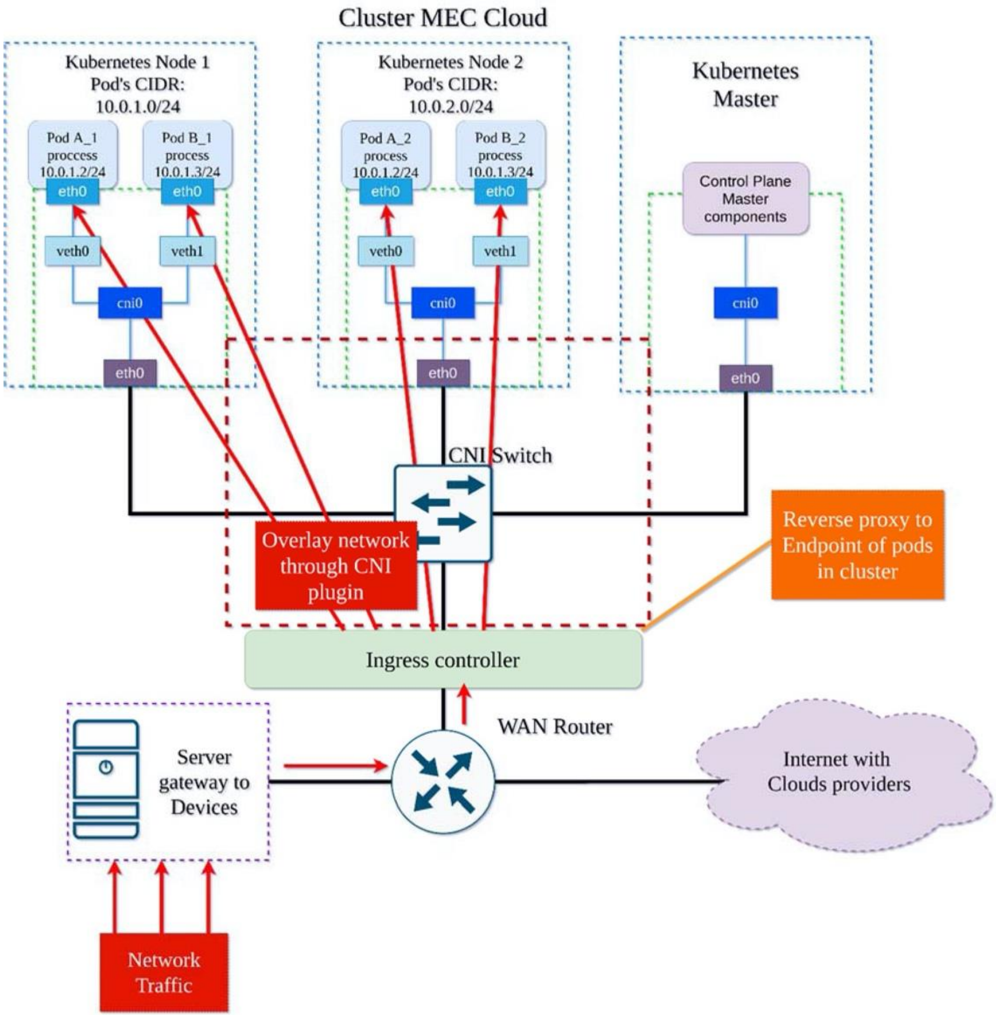


Figure 4.1 Simulated traffic flow model [Author's compilation: Adopted from Bouet and Conan, 2018]

4.1.1 Experiment 1: Apache Server Deployment on a Virtual Machine

In this experiment, the client was considered a laptop or device IoT device creating a load of TCP connections through the iperf3 tool and generating HTTP get-requests to the Server, as indicated in figure 4.2. Logically, the client and the Server are in the same LAN segment. As such, the client and the Server were implemented on the interface with a bridge connection.

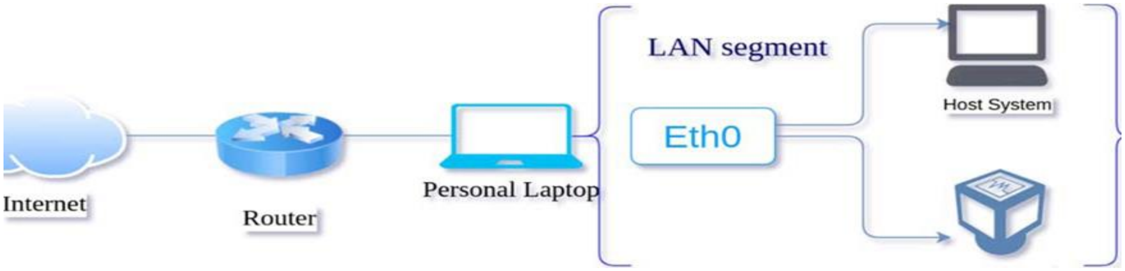
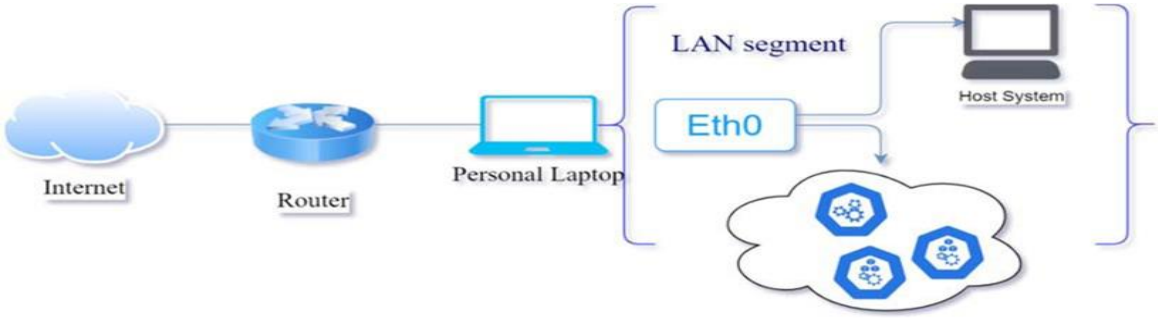


Figure 4.2: VM Apache for the local network connection [Author's compilation: Adopted from Bouet and Conan, 2018]. During the experiment data was collected for use in the case analysis shown in figure 4.4.

4.1.2. Experiment 2. Apache Server Deployed in A Kubernetes Cluster

The implementation of the local network for the Kubernetes cluster section was similar to the first experiment. The cluster is comprised of three nodes running as Virtualbox virtual machines. The control node and two working nodes were connected by CNI- plugin Flannel, which operates in host-gw mode. Ingress was used to access the webserver. Traffic was evenly



distributed between the two Apache replicas distributed between each operating node in the cluster. Figure 4.3 illustrates the LAN layout for the second experiment.

Figure 4.3: VM Apache for the Server Deployed in A Kubernetes Cluster [Author's compilation: Adopted from Bouet and Conan, 2018]

During every testing stage, packages were captured using the TCPdump utility. Wireshark was then used to determine the time the request for each response took, and then calculated the average value of the resulting parameter throughout the entire testing phase. The resulting parameters were recorded in excel sheets and stored for further analysis as shown in figure 4.5

4.1.3. Security Attack Vector Implementation Case Scenarios

To simulate a real cyber-security threat for IoT networks, it was necessary to consider all the probable attack vectors faced in IoT environments. As such, the zero-day vulnerability analysis in Palmer was considered. According to Khan and Salah [9], zero-day attacks are exploits of computer appliances initiated before the exploit point is known. As such the system security administrators need to think of the possibility of an attack. Such vulnerabilities can be discovered by analysing the IoT environment, testing the environment, reporting documented analysis, and analysing mitigation effects. The simulated environment in this case consisted of physical devices including sensors, servers, and network data paths. When physical immunity is compromised, it was considered that it provided a considerable risk that IoT appliances would be exploited and used as botnets to affect other appliances in the worst scenario. Two main attack vectors were experimented on in the current case scenario: the physical attack vector and the application-based attack vectors.

4.1.3.1. Scenario 1: The Physical-Based Attack Vectors

In this attack, an attacker gains physical access to an IoT device and tampers with the device's configuration data. Once the security parameters are tampered with, the attacker reconfigures the device and uses it to send malicious data over an IoT network as a botnet. In this experiment, a compromised device was used to feed incorrect measurement information to the system to cause physical damage to other devices and have uncontrolled changes to the configurations, which can enable malicious firmware and microcode upgrades to other IoT devices without the knowledge of the user.

4.1.3.2. Scenario 2: The Application-Based Attack Vectors

In this study, the application-based attack vectors were based on the OWASP 2017 report because the report covers the most recent attack vectors used to exploit IoT devices and systems. Additionally, there are numerous application-based attacks, and therefore it was important to use the documented and approved source of information on the most dangerously known attack vectors. The common application-based attack vectors and which were used in this case study experiment included: broken authentications, data exposure, security misconfigurations, cross-site scripting, use of components with known vulnerabilities, insufficient Loggins and monitoring, manipulation of user data held by tenants inside the IoT frameworks, denial of service, and man-in-the-middle attacks. The results of the experimentation was analysed below.

Using the tcpdump programme, packages were captured at every level of testing. According to the results obtained, Wireshark generated an average value of each parameter based on how long it took from request to response. Figure 4.4 compares the average server response time between the two studies. The analysis is important to determine the effect of the attack relating to the physical access and the malware that was installed on the machine to affect its performance.

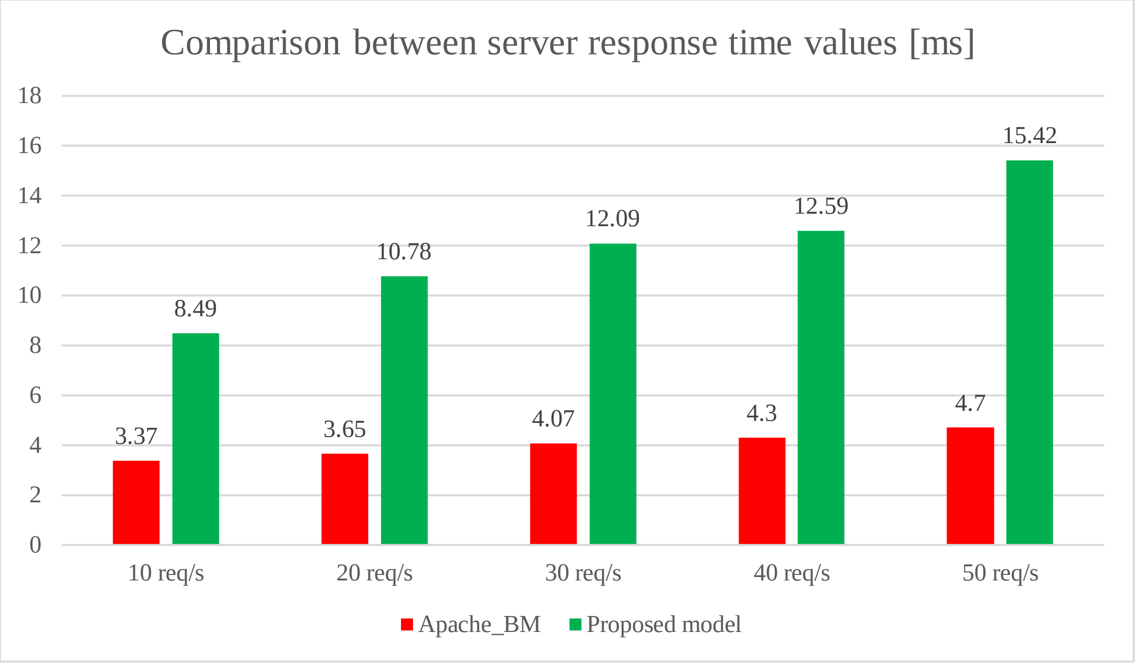


Figure 4.4. Test results, first deployment option [Source: compiled by Author]

Both trials showed that Apache applications deployed in the Kubernetes cluster were inferior to those deployed on a single server in conventional configurations. Due to iperf3's requirement for a large amount of CPU time in order to create parallel queries, the results do not reflect what we would like them to be. Minikube can be used to lessen the burden on the system and improve performance on the experimental client and Server. Kubernetes clusters can be deployed locally out of the box using Minikube, which is a smaller but less flexible alternative to Kubernetes. This shows that a new application or malware would cause increased response time that, according to figure 3.5 would continue to rise in comparison with the number of requests.

When we execute the second scenario [Figure 4.6], the cluster configuration will be identical to what we used in our first scenario. A KVM hypervisor is used to deploy the cluster's virtual machine, which has 4 VCPU and 3 GB of RAM. In this setup, less vCPU capacity is required, as well as less RAM space.

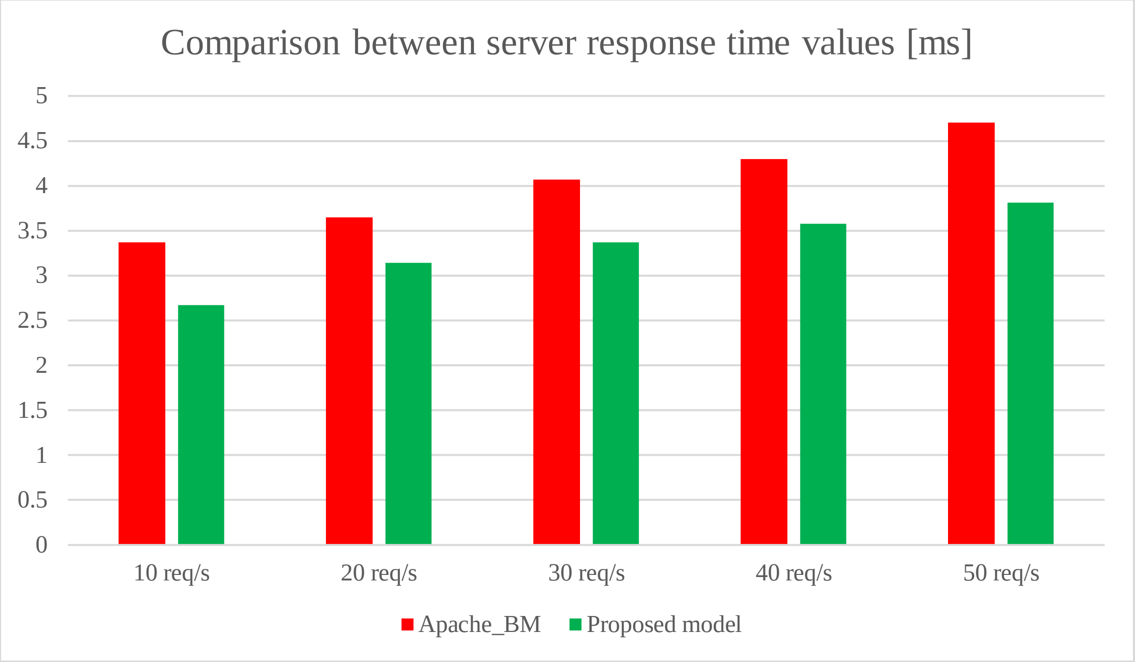


Figure 4.5 Second option for testing the proposed model. [source: compiled by Author]

Load balancing reduces response time, and the Kubernetes orchestrator allows us to simply expand and alter cluster application parameters based on the findings. This value is supplied in the deployment object manifest file, which is part of the control plane, and uses the application operates as a declarative definition of the number of replicas. It also made use of a config map to pass configuration to and from within the container while configuring HTTP-server with the application.

4.2 Qualitative analysis

After searching the databases 9 relevant articles were selected for thematic analysis. The selection was based on the relevance of the material to the research topic and objectives. The studies summary is attached appendix.

4.2.1 Vulnerabilities in IoT

The study materials' analysis also found out that several themes arose that were vital for the study under this theme. The themes that arose are malware, weak passwords, insecure interfaces, insufficient data protection, poor IoT device management, Denial of service

4.2.1.1 Malware

By introducing a rogue service instance or virtual machine into the cloud, the hacker can perform data change, gain control, and run a malicious piece of code [52–53]. It is stated, "attackers copy and upload a victim's service instance, but when some service asks the victim's instance, the malicious instance answers "[60]. As a result, the hacker can have access to data on sensitive services. The study by Fernandes et al. [60] supports this by indicating that 6 out of the 8 employees interviewed could easily click links sent to them, and in most cases, it realises that it has impacted the devices they use [54]. In most cases, the antiviruses stored on the system have played a key role in preventing the malware from running. This indicates that malware is a vulnerability on the internet of things.

4.2.1.2. SQL injections

A poorly constructed application may be vulnerable to attacks by incorporating SQL statements in the input data like files [54]. Attackers use these SQL statements to perform writing, reading, and deleting activities. This type of attack can obtain the user's personal information and is dangerous to the entire database system. In the case of SQL injection attacks on Web applications, the page on view may display different results than the genuine information [55]. SQL injection is associated majorly with programmers with ill motives in the banking industry. The major aim of the injection can be to steal given data from the system, or even cause authorise modification of data in the system.

4.2.1.3. Weak passwords

Implementing robust authentication procedures across various interfaces in the IoT ecosystem, such as mobile, cloud, and online makes it more secure. "Through weak credentials and account enumeration, the adversary targets these insecure interfaces". The study by Sanni et al. [54] found, “If anyone can gain access to the IoT nodes without going through identity checks or circumventing the poor authentication scheme, the adversary can abuse the system in a variety of ways” [59]. The adversary might conduct a denial-of-service attack, and seize complete control of the system, and steal data. These indicate how attackers can use the weak passwords to access the banking system in to attack the system in various ways

The verification procedure is important to the preservation of IoT cybersecurity. The current authentication solutions are unable to provide a fine-grained verification. For example, when applications are updated, malicious payloads can be downloaded and used by cybercriminals to remotely influence a device [57, 60]. While this is going on, the authorisation model is flawed. Unchecking the "Use all available permissions" box will provide access to information even if none of the permissions is needed [60]. This makes the IoT application vulnerable to hackers.

In addition, if an attacker has inappropriate access to a directory or file, they can unleash a wide range of cyberattacks [59]. The smart card has remote access flaws that could lead to leaks and modification of user information in a past work situation [51]. This may be the reason for the increasing cyber-attacks on IoT systems are increasing with time.

4.2.1.4 Insufficient data protection

As a result of the vulnerability, an attack called sensitive data tampering can be carried out. In this attack scenario, critical data is accessed and altered without authorisation, resulting in privacy violations for the users [52]. In most cases, this exploit takes the use of authorisation model design flaws [59]. Attackers have used authorisation model flaws to take control of smart home applications, culminating in issues like break-ins and theft [54]. In addition, previous studies [51] looked into the events used to interact between SmartDevice and SmartApp. Smart devices and SmartApps, it should be mentioned, present a particularly complex data protection scenario. A SmartDevice uses events to convey sensitive data to a SmartApp, and the SmartApp uses events to monitor the SmartDevice. However, a lack of appropriate event security may result in event leakage and even more devastating harm to the user. Moreover, users' security may be violated due to a lack of adequate user input protection [59]. A system for securing sensitive data by defining intended data flow patterns was created

4.2.1.5 Web browser attack

The Shodan search engine has evolved into a difficult-to-overcome information security threat. Shodan was designed to examine computer system and network security and conduct penetration tests [pentesting]. "The deadliest search engine," according to CNN Business Journalist David Goldman, and "a huge security disaster" according to Information Security Expert and CEO of Rumble Network Discovery HD Moore labelled Shodan in 2013.

One can use the system for free or for business purposes by paying a fee. Free access severely restricts the user's options. By not paying the monthly subscription, a person will have full access. A .edu email address is required, and a university can only issue these. There are, however, ways to obtain it illegally [60]. The vast majority of people who utilise Shodan do it in precisely this manner. As a result, one of the most devastating information assault tools is available to absolutely anyone at no cost. People that are looking into Internet-connected device vulnerabilities might use the Shodan search engine as a key tool for their investigation.

Additionally, large corporations use the system to ensure the security of gadgets they make or use. The Shodan user will get several forms of information after entering the IP address of a device or establishing filters based on that device's attributes in the search box. These include the target's general location, open network ports, a list of installed access protocols and their connection details, as well as names and descriptions of vulnerabilities discovered. As a result, detecting and fixing vulnerabilities is made much simpler by the system. This is a priceless ability. At the same time, attackers who want to take control of the victim's devices or acquire sensitive data receive the same data. Particularly vulnerable are systems of control and surveillance.

4.2.1.6 Poor IoT device management

The study by Sanni et al. [56] indicated that most of the hackers' main target is to access the devices that are used in the banking industries. They believe that access to the device will be critical in aiding them to hack the system either by using phishing practices on the device that would be vital to getting the passwords that the banking IoT uses. “Lack of security support on devices deployed in production, including asset management, update management, secure decommissioning, systems monitoring, and response capabilities is one of the factors contributing to hacking” [56]. It shows that most of the workers allow others to access the devices they use for the banking services. “The common attacks were related to access device is the smartphones. The hackers, in some cases, trick the users into sharing vital information which they try on the system and at times gain access to the IoT environment hence cause attacks.

Internet-connected devices use embedded sensors to collect data and, in some situations, influence them. A smart home that automatically changes heating and lighting, or a smart factory that monitors industrial machines for issues and then automatically adjusts them to avoid failures, are two examples of Internet of Things applications [58]. People can communicate with gadgets, and devices can communicate with each other, adjust to changing environments, and make decisions without human input. First, the devices collect data - such as apartment temperature or user heart rate - then that data is transferred to the cloud. There, it's handled by the programme. Once notified, the system can wait for the user to respond, or it can act immediately. More than 25 billion Internet of Things [IoT] devices are currently in use, raising security. Because they are connected to the corporate network invisibly, most Internet of Things devices is shadow devices. Protecting Internet of Things [IoT] devices is difficult due to the fact that these gadgets are designed with little consideration for security. Verizon reported the result of this cyberattack on a major U.S. university in 2019. [the name of the educational institution was not disclosed]. The perpetrators launched the attack simultaneously from 5,000 devices on the campus. All of these devices were compromised by hackers, who used them to send DNS queries. This was the first attack on a smart device that local security experts had seen, and they were unable to rapidly figure out how to restore control of the hijacked gadgets. After further investigation, it was discovered that a botnet had been responsible for the attack and had taken control of the network. Password brute-forcing allowed hackers to take over the devices one by one.

4.2.1.7 Denial of service

IoT nodes have the potential to be used as bots to target DDoS attacks. This easiness introduces a risk to the internet in the form of spread attacks. The availability of a large number of 24/7 unsecured IoT devices and their inadequate maintenance and barely engaging user interfaces attracts the attention of intruders. Mirai and its variations are examples of such assaults. The Mirai malware was initially discovered in August of 2016. Two DDoS assaults utilising the Mirai malware were launched in September 2016 against the websites of Brain Krebs, a computer security consultant, and the French web provider [57]. The following month, it targeted the service provider Dyn, causing several websites to go offline for several hours, including Netflix, Twitter, GitHub, and Reddit. Mirai launches a DDoS attack against target servers by assembling a network of poorly configured IoT devices [52]. This shows how this attack can have an adverse effect on the organisation.

4.2.2 Security mitigation practices

Based on this theme, two sub-themes were established on the research relevant to answering the research question. The first theme was automated patch generation and access control methods, which other studies proposed for mitigation practices. Automated patch generation aims at fixing vulnerabilities, while access control aims at fixing unauthorised access and malware.

4.2.2.1. Automated patch generation

The automatic patch generation technology described in this article is not explicitly directed at the Internet of Things (IoT) but rather is an augmentation of the current security field. Security flaws are often repaired at the source level by the vendor software development. In the wake of receiving an external vulnerability report, they duplicate the trigger condition and research the vulnerability method to close the hole. It is claimed that automatic patch generation will fix software errors without programmers manually finding, comprehending, and correcting them.

IoT devices require the capability to capture and upgrade their software, which is provided by technical requirements. A team of software engineers recommended studying the correct C [53,54], Java [55], and other source code languages to produce the patch automatically, which achieved a set of comprehensive results. They were successful. You can also change the programme's appearance only, which has the advantage of not affecting its functionality. GenProg [58] makes use of a more advanced form of genetic programming to build a programme version that is both functional and impervious to a specific fault. Mutation techniques are unpredictable, and this might lead to bizarre results. Long and Rinard [57] developed the Pattern-based Automatic Programme Repair to overcome existing issues. For the Android platform, Long, Amidon, and Rinard [60] presented Adapt patch, an adaptive kernel hotfix framework, and LuaKpatch, which inserts a type-safe dynamic language engine into the kernel to execute patches. These solutions solve the issue that the Android platform's patch chain is too long, fragmentation and ecological layout are not matched, and subdivision repair is not quick. However, they do not plan to address the issue of automatic hotfix development in the cross-CPU architecture. They must still be written by hand based on the subject of knowledge and experience. DARPA's Cyber Grand Challenge [CGC] [58] encourages academics to create automated security solutions at the binary c level. There were a few exceptions: binary code strengthening [56, 57], boundary checking, and pointer patching were all widely used in these approaches [59].

4.2.2.2. Access control method user or platform side to avoid or stop harmful attacks.

Requirements concerning technology: User or cloud-based scalability.

A study by Shoshitaishvili et al. [60] looked at the security of a programme named SmartThings for the first time. These researchers found that most apps have excessive privileges because of their coarse-grained capabilities and the devices they use to connect asynchronously with applications via occurrences, which do not sufficiently secure events that transmit top secret information like lock credentials.

4.3 Quantitative analysis of secondary data

Data for the sake of this analysis was obtained from the ptsecurity.com website, and cyberhunter.solutions, and science.gov

4.3.1 Figure 4.6: sample losses incurred by banks

Secondary data on the losses that different companies have incurred due to cyber security threats can be summarised in figure 1 below.

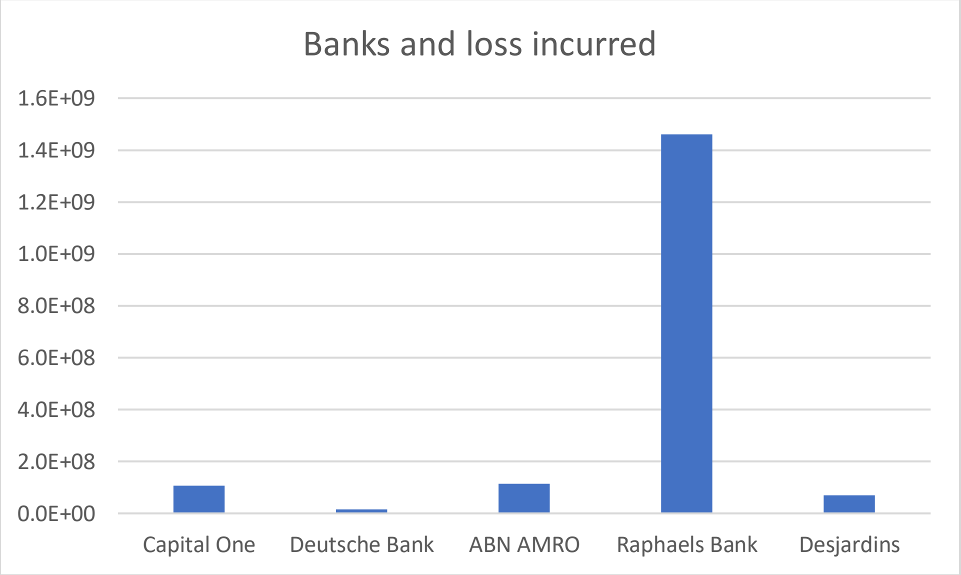


Figure 4.6. Bar chart of different banks and losses incurred relating to cyber attack. [source: Author using data from cyberhunters.solutions]

Figure 4.6 above shows that different companies have incurred losses due to cyber security breaches. Most of the companies were fined after the bank had undergone cyber-attacks. From the data, it is clear that Raphael's bank was the one that suffered the most from the fine due to cyber-attacks. The data indicated that the banks' main attack was due to technical issues that led to the Denial of service. The Desjardins bank suffered the loss because the intruder received information from one of the employees [62]. The hacker, therefore, used the credentials to cause an attack on the system hence leading to the loss. It indicates that the hackers could gain information from the workers, which they can use to cause an attack on the system. Capital one bank attack was associated with a data breach where massive individual information was breached, causing millions of losses.

4.3.2 Penetration test analysis of the common vulnerabilities

An organisation's security is tested by mimicking what an actual invader would do in order to determine how secure it really is. When it comes to external testing, it is used to determine the likelihood of breaching a network perimeter, while internal testing is used to get full control over the infrastructure or access to important systems. Penetration testing was performed regularly for many companies. The result shown in figure 2 below was gathered from penetration tests that experts conducted that we're able to deploy a wide range of methodologies in 12 of the most instructional penetration tests we've conducted for banks over the past three years. The penetration test identified four areas of vulnerabilities and faults that affect the bank network perimeter: online application vulnerabilities, a lack of adequate network security, problems with server setup, and user account management. The researcher was able to employ a variety of strategies throughout the previous three years. Figure 4.7 shows the common network vulnerabilities that banking industries have been facing.

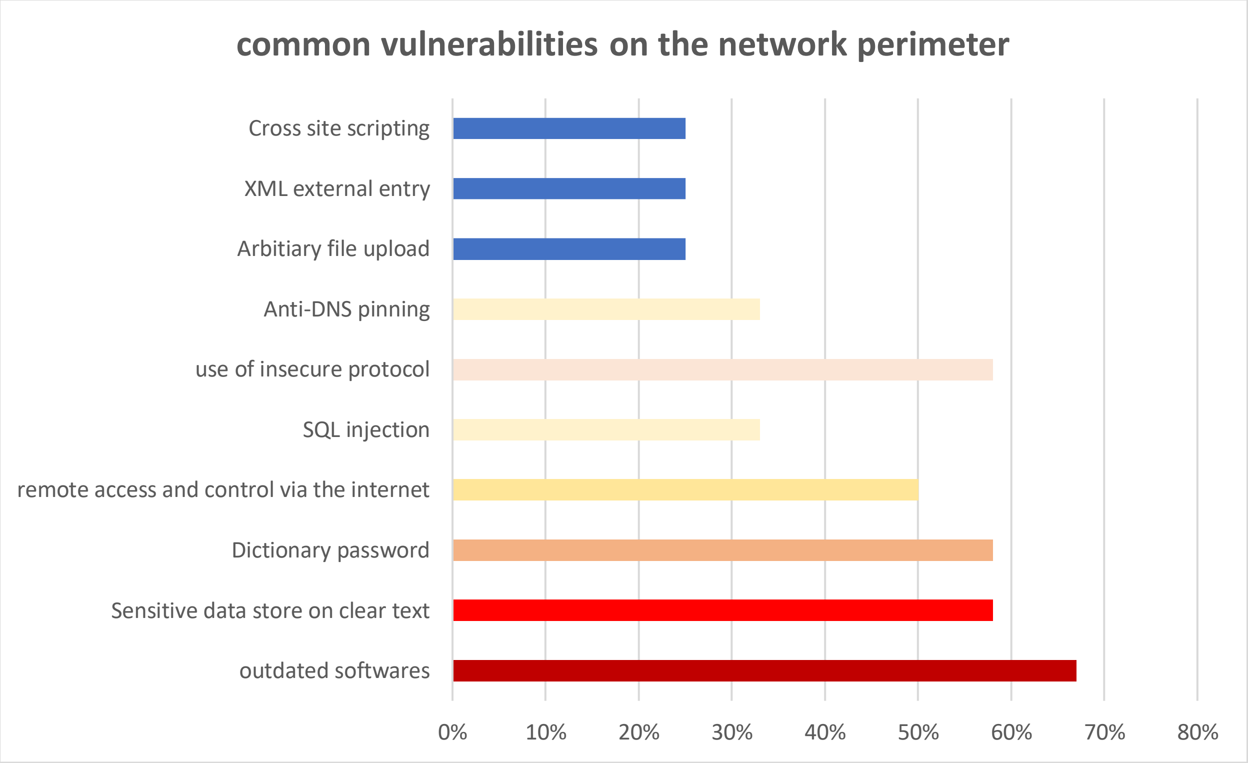


Figure 4.7 Common vulnerabilities on network perimeters. [Source: Author using data from ptsecurity.com of penetration tests done from 2015-2018]

The mere presence of security flaws on the system perimeter does not guarantee that their exploitation will allow access to the system's internal network. In general, banks' network perimeters are much more protected than those of other industries in terms of network security. As a result of external penetration testing in the last three years, 58 per cent of tests gained access to the internal network; this figure was only 22 percent for banks. There were flaws in web programmes that made it easy for an intruder to attain their aim with only one step, facilitating access in each situation. Figure 4.7 also shows that dictionary passwords, use o0f insecure protocols, storing sensitive data on clear text, and using outdated software are the top vulnerabilities in the banking system with 58, 58, 58, and 67%, respectively [64]. Other vulnerabilities are SQL injections that in most cases target the databases running on SQL, remote access via internet user, which is common with cloud computing, arbitrary file upload, cross-site scripting, and XML external entry

In another penetration test done by Costin, A. and Zaddach [5] to verify the employee's awareness of phishing activities, a link was sent to various employees via email, and a counter check was done to check the number of the employees who clicked the link. 75 per cent of bank employees opened a link in a phishing message, 25 per cent input their credentials in a phone authentication form, and 25 per cent ran a harmful attachment on their work computer during a security awareness assessment [63]. About 8% of bank users clicked on a phishing link, 2% ran a malicious programme, and fewer than 1% input their credentials.

4.3.3 Internal network vulnerabilities

Criminals get access to the banking infrastructure because of security weaknesses in the banking system. The following chart indicates the frequency of vulnerabilities exploited to acquire complete access over domain infrastructure during internal penetration testing. Password recovery via OS memory and weak password policies are the two most common attack vectors.

On the network perimeter of 50 per cent of banks, dictionary passwords are utilised. However, each system has a weak password policy on the internal network. When it comes to this, banks are no different from any other industry [62]. Users set weak passwords on half of the systems. Administrators often create default accounts when deploying database management systems, web servers, operating systems, or creating corporate accounts [with predictable passwords]. The majority of the time programmes either have excessive privileges or have known security flaws. Consequently, intruders can get administrative powers in just one or two actions.

Figure 4.8: common vulnerabilities in the banking industry

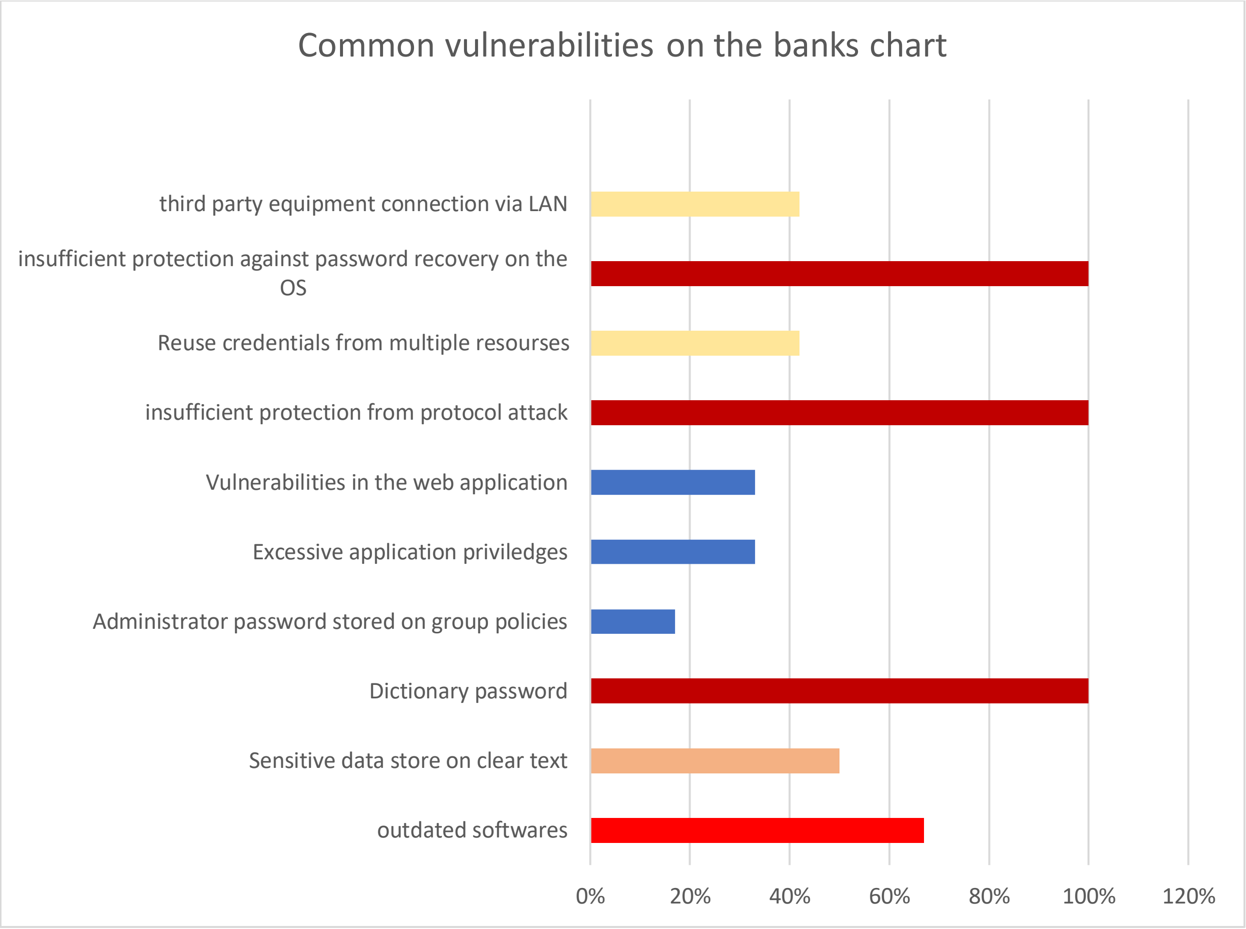


Figure 4.8 Common Vulnerabilities on banking sector [Source: penetration test data from ptsecurity.com done from 2015-2018]

Figure 4.8 shows some of the vulnerabilities that the banking industry faces. It shows that the highest vulnerability is dictionary passwords, insufficient protection from protocol attacks, and insufficient protection against password recovery by the operating system. These factors are mainly associated with the creation of password and password recovery mechanisms [62]. Hackers can easily access saved passwords from the system and use them to launch attacks. Outdated software is the third in the rank.

Figure 4.9 vulnerabilities in internal networks

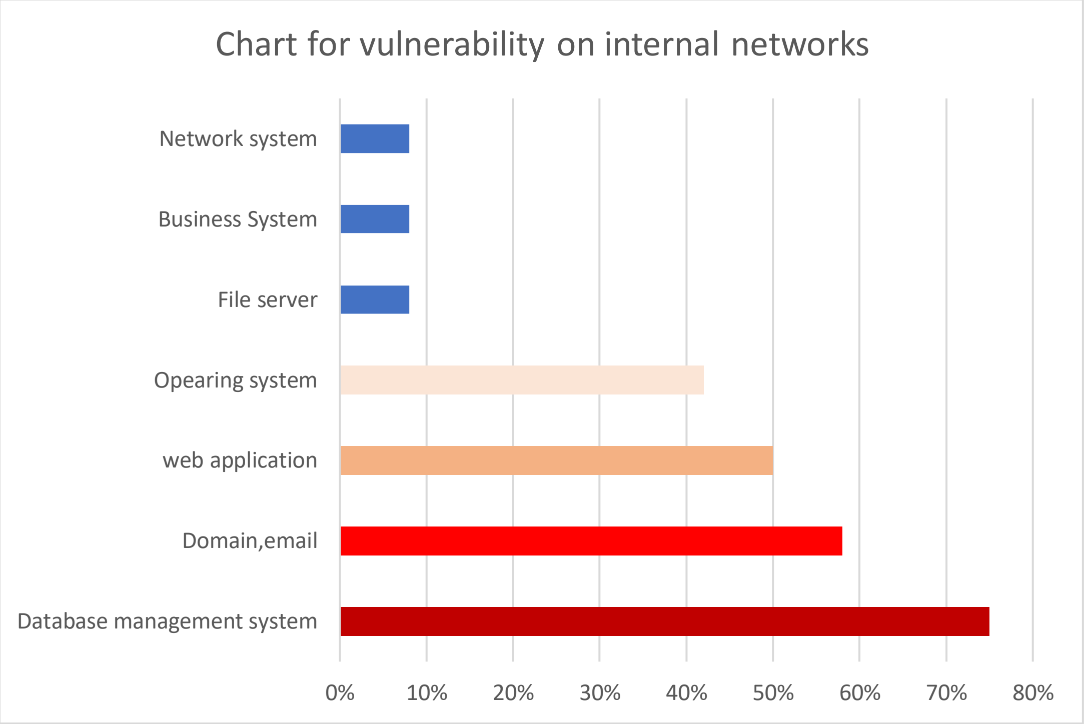


Figure 4.9. Vulnerabilities on internal networks bar chart. [Source: Auther using penetration test result from cyberhunter.solutions done from 2015-2018]

Figure 4.9 shows that the highest vulnerability on internal networks is the database management system. The reason for this might be associated with programming bugs that the hackers tend to exploit. Domain/ email is the second in the ranks. In most cases, hackers send emails containing malicious programmes that are executed when the user clicks on those links. Web applications and operating systems follow in succession. The reason for these two may also be associated with coding as they depend on programming.

For example, when it comes to securing service protocols, the research by Borkar et el. [10] often found minimal security measures or none at all. The NBNS protocol was not protected at any bank, and 70 per cent of banks did not have protection against LLMNR attacks. ARP Poisoning assaults affected almost 80 per cent of banks, according to a report by the FBI [63]. Meanwhile, hackers can successfully obtain information about the system by intercepting credentials passed across the network. It was possible to capture numerous NetNTLMv2 hash values of domain user passwords in Challenge–Reply format at various banks, for instance.

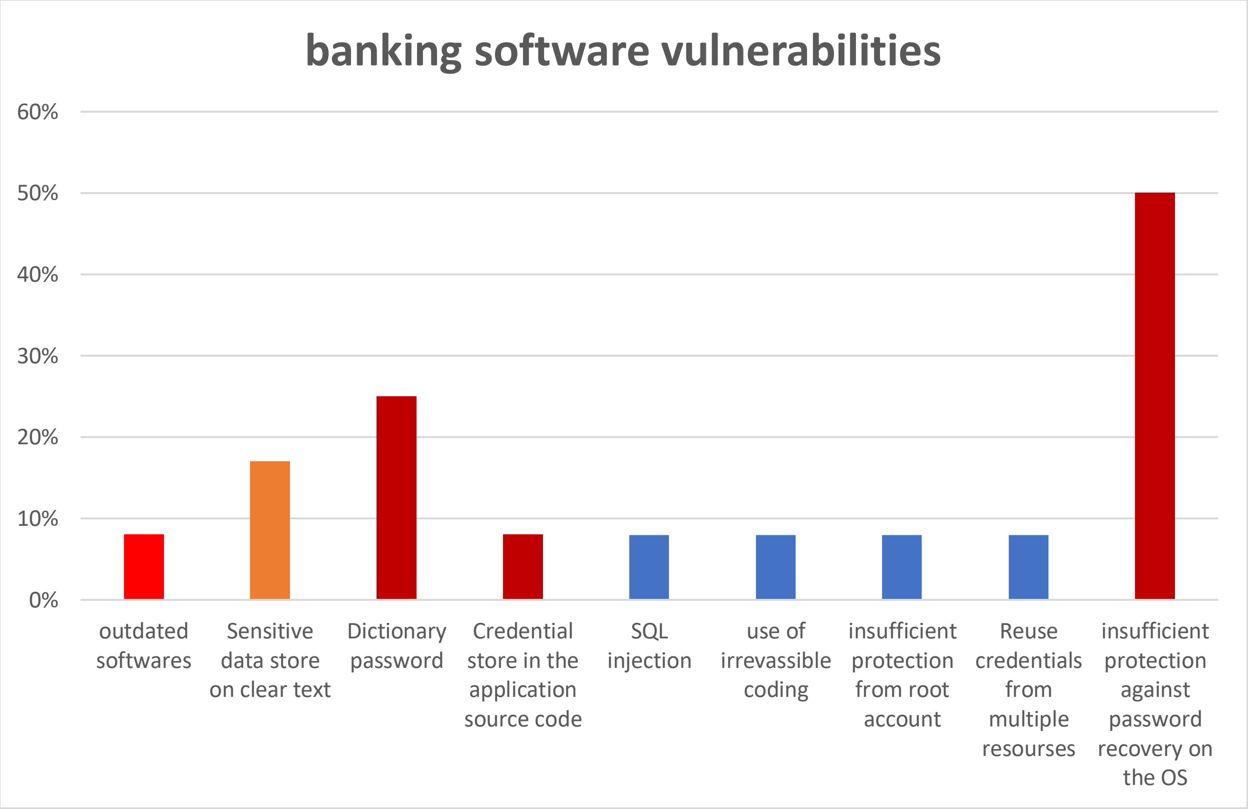


Figure 4.10. Vulnerabilities used to access banking software. [Source: Author with data from penetration test from psecurity.com done from 2015-2018]

As a result of a security breach indicated in figure 4.10, at 25% of banks, Cobalt could withdraw money from ATMs that had been compromised [61]. The penetration test found it easy to transfer funds to criminal-controlled accounts through interbank transfer systems at 17 per cent of institutions.

It is estimated that 17 per cent of banks' card processing systems are not fully protected, allowing attackers to manipulate the balances on their card accounts, as we witnessed in the case of assaults on Eastern European banks in 2017. With the ability to hack practically any banking application, the Carbanak gang could have stolen money from 58 per cent of banks [61]. To acquire access to a bank's electronic crown jewels, an attacker who has breached the bank's internal network often has to perform only four steps.

5. Chapter Five: Interpretation and discussion

5.0. Introduction

This chapter takes the results from the analysis and gives an interpretation of them. After interpretation, it discusses the relevance of the finding compared to those in the literature review. Therefore, it will illustrate the meaning of the results and limitations and discuss the importance of the results to the banking industry. It will entail a summary of the results, interpretation of the vulnerabilities, mitigation of the vulnerabilities, and limitation of the results.

5.1. vulnerabilities from qualitative and quantitative analysis

From the results, some vulnerabilities massively impact the banking industry. The vulnerabilities can be categorised into two types, that is external vulnerabilities and internal vulnerabilities. However, both the categories converge into the same types of vulnerabilities.

5.1.1. Malware, outdated software and operating system vulnerabilities findings and discussion

According to the results, malware vulnerabilities are connected to outdated software the hackers try to exploit in most cases. The finding affirms the study by Lucas and Jurgovsky [8] that also indicated that malware makes the banking IoT vulnerable to attacks. Malware and outdated software were the main vulnerability that hackers target Broker et al. [2]. Of course, using a single system for a longer time may pose a real danger to many organisations. A study of the software by the hackers for a more extended period would only suggest that some of the loopholes are realised; hence an attack could be launched on the system. This explains why the outdated software formed part of the target by the hackers in this study. The finding, therefore, supports the finding by Lucas and Jurgovsky [8], which added that the usage of credit cards for a long time had played a part in the identification of its vulnerabilities that are now identified by most of the hackers. This study identified that the hackers' main focus is the data they may want to steal or manipulate for their benefit. Therefore, the finding supports the study by Kumar and Lim [24], which indicated that the hackers engineer the malware based on the nature of the data on the target network they would wish to acquire. It also indicated that the operating system forms part of the focus area that attackers wish to exploit. The finding affirms Cozzi et al.'s [7] finding, which illustrated that from the time past, the system managers and security experts have continually focussed on the security vulnerabilities associated with the operating systems. The major cause of this, according to the study, is the massive data exchange that comes with the advancement of technology that leads to the development of IoT applications. This finding supports Khan and Salah's [9] finding, which indicated that data exchange requires new technologies to connect to the physical world. This may be the reason why attackers target banking systems as it entails a massive flow of data.

5.1.2. Weak passwords and device accessibility findings and discussion

Another vulnerability from the analysis is weak passwords. Both qualitative and quantitative analysis realised that the attackers use the weak password to guess and access the banking system hence launch their respective attacks. When administrators install database management systems, web servers, operating systems, or create corporate accounts, they frequently leave default accounts with predictable passwords behind. Applications are frequently either overly privileged or have security flaws that have already been publicly disclosed. So invaders can get administrative rights in just a couple of clicks now. Inadequate security precautions were found in the study and none when securing service protocols in many cases. At the same time, intercepting credentials sent across the network could be effectively utilised by adversaries to gather data from the system. These findings have supported the study by Humayun et al. [10] that indicated that employees form the soft sport for hackers as they use weak passwords that are easy to guess, especially with access to the user devices. The study supported Yoon et al. [33], which also indicated that the attackers majorly invade systems with a precise aim of accessing the devices. With the access, they can launch a denial of service attack on systems or even cause massive losses by making the system crash. The major cause of such attacks is data leakages and weak data that cybercriminals can exploit.

The finding also illustrates that access to devices and search engines can be exploited as a vulnerability in banking industries IoT. It indicates that the banking industry employees should be critical of the people they allow to access the devices and the browsers they use. The other finding indicates that the attacker targets the data majorly; therefore, the storage of data on explicit texts is a vulnerability for most of the attackers.

5.1.3. Data storage vulnerability

The study also established that storing data in clear texts forms a vulnerability that most hackers wish to exploit in most cases. Therefore, showing a need to have a better way of storing data. The finding, in a way, explains why data encryption technology has been on the rise recently. Though the current study never focused on encryption as a way of preventing data manipulation by hackers, it in a way supports the study by Popov [29] and Humayun et al. [10] that indicated that different algorithms are in place to ensure that data is encrypted before storage as it plays a key role in ensuring that data cannot be lost via easy access and read by the hackers.

5.2. Vulnerabilities from case study discussion.

The case study found that attacking the servers lowers the speed for the execution of requests from the server. The server is engaged with the hacker’s malware which makes it delay in processing requests. The decrease in speed lowers the efficiency in banking IoT application that is run on the cloud. At such a time of delay the finding by Tzafestas [21 indicated that the hackers can exploit by launching attacks that would lead to massive data losses. This finding supports the finding by Pozzolo et al. [4] that illustrated that the main purposed for attackers to focus on the cloud computing interface is because they can easily exploit vulnerabilities on such a system as it could be accessed from different places. The results by Cozzi et al.'s [7] also support this finding by indicating that the decrease in speed of processing requests is an indication that the system is attacked and data loss is the next stage of the attack.

5.3. Vulnerabilities interpretation and discussion.

The results indicate that the banking industry faces many attacks that exploit the above vulnerabilities. Most of the vulnerabilities exploit more about accessibility to the system. Therefore, hackers may use phishing to gain access or tease the workers to share their information to allow them to launch attacks on the system. Outdated software's and malware also presented a soft spot for the hackers. From there, it is evident the banking industries should understand these vulnerabilities and try to overcome each. This established the suggestion by Humayun et al. [10] that illustrated how the importance of building highly secured applications to use in the banking sector. Because from the study, the worker is targeted by malicious attackers, banks, organisations, and other financial institutions must educate their employees on the ways attackers can attack and the policies that will help them stay safe in the IoT this was also suggested by the study by Khan and Salah's [9]. They should be educated to ensure that their devices are protected from accessibility both at work and at home. They also need to be educated on the need to update system software's regularly to ensure that they are up to date and coding vulnerabilities are not allowed [8]. Password creation and storage should also form part of the education to ensure that they create strong passwords that may not be easy to predict. In addition, the passwords should be encrypted before storage to ensure that they are not easily viewed, which may lead to different forms of attacks this affirms the suggestion by Popov [29]. From the vulnerabilities, it is also evident that a continuous system check should be enhanced on banking industries to ensure that SQL injections and malware are identified on time and step undertaken to overcome them. The study also found two main methods that can be used to mitigate the attacks. The earlier study did not focus on these as they mainly focused on the vulnerabilities and how to overcome them. Therefore, a need to test and approve the two testing methods as they may assist in overcoming cyber security losses in case they are viable and practical. The mitigation practices will be discussed in the next section.

5.4. Vulnerabilities mitigation interpretation and discussion

The study also found that vulnerability mitigation also forms a key part in realising vulnerable systems; hence, prevention can be done. Many studies have not exploited the subject. However, two common mitigation practices were realised during the study: automated patch generation, which is key for the banking industries and organisations to implement as the method could help patch realise and patch any vulnerability associated with the system this differs from the suggestion in the study by Cozzi et al.'s [7] which mention antivirus as a method of mitigation. In doing so, attacks such as SQL injections, code injections, and malware will be realised before any massive infection is realised on the system. Access control method was also a technical practice that the study found to be vital for mitigating attacks. This differs from the previous studies by Khan and Salah's [9] and Humayun et al. [10] that suggested restricting access to the device only. The method, if applied effectively according to the study, will help the banking industries to realise access of an unauthorised person to the system faster. In doing this, the hackers would be quickly identified and be blocked from accessing and tampering with massive data as suggested by Liu, Xu, and Yung [18], These mitigation practices would help several banks from the massive losses that they have incurred relating to cyber-attacks.

5.5. Limitation of the results

One of the study's limitations is that the data used in the study, especially for penetration testing, was collected in the past three years. According to increased development in cyber security, some of the data may not provide a clear picture of the security vulnerabilities that the banking industry experience on the internet of things. The hackers, as the study has shown, continue to exploit systems to develop how they can access them. This leads to new techniques for attacking and new vulnerabilities. In addition, this field needs a more experimental approach to examine vulnerability in the banking industry. This can be done by performing attacks on different banks and systems to try and exploit the vulnerabilities of such systems. The practice requires extensive authorisation from the banks and policy agreements. This is not easy for most banks as they may fear data breaches and the losses that might occur. To the research, this endeavour would be too expensive. This limited the researcher to use secondary data, which may be outdated and might not give the current situation.

5.6. Chapter summary

The chapter indicates some of the study's vulnerabilities and their relevance for application in the current world. The chapter malware, weak passwords, SQL injections, outdated software, and devise accessibility Areas are some of the study's vulnerabilities. In addition, the study established automated patch generation and access control methods as the two methods that can be used to mitigate the cyber security attacks and either path them or report them. The use of antiviruses was also identified as a means that can be used to prevent malware infections that could lead to Denial of service.

6. Chapter Six: Conclusion and recommendation

6.1. Conclusion

The concept and aspects of IoT technology, its application, and implementation in cloud computing were one of the study objectives. Therefore, the study has shown that the devices' interconnection is how banks operate in the world today. They implement massive usage of servers that are run in SaaS or PaaS. However, the interconnection has brought some risk into the IoT, especially in banking. The study shows that cyberattacks are anticipated to affect the banking industry, especially the servers where data is stored. As a result of the inherent risk in this industry, financial institutions must be vigilant against the ever-increasing cyber threat. However, the sector deals with money which is a crucial aspect of life for the development of individuals and society. Many people have been left in the dark about modern-day technological advances, leaving them open to cyber-attacks like phishing and malware. Hackers can now steal data and money thanks to banks' open vulnerability and the knowledge chasm between them and their clients.

The study realised that banks need to have good defences against possible threats and vulnerabilities on their internal systems. By using a conventional method such as phishing to infect unknowing employees on the company network, hackers can simply circumvent the network's perimeter defences. For this to happen, malicious actors keep an eye out for emerging vulnerabilities, which they exploit to launch different attacks on the system. They use vulnerabilities such as weak passwords, outdated and unprotected systems, malware, SQL injections, and many others to launch attacks that would result in slow responses or total Denial of service

The intruders can also use well-known vulnerabilities and legitimate applications to their advantage while remaining undetected by network managers. In a matter of minutes, the intruders were able to seize control of the bank's infrastructure by exploiting holes incorporated in network protection, causing an attack called Denial of service. From the study, the intruders can be stopped if an attack is recognised and stopped quickly enough or if the vulnerabilities are patched. Losses can be avoided at any point by taking necessary precautions such as employee education. The use of antivirus on the systems can also be employed to ensure that malwares are not installed by the user in a scenario where the attackers use links containing malware. Another alternative to using only endpoint antivirus systems is checking email attachments in an isolated environment. As a result, security access must be tracked by access control software to notice any attack early and automated patching software that will be able to patch any vulnerabilities before exploitation, which greatly simplifies and improve the processing of information security events. It is also necessary that banks share information on industry attacks and learn more about key indicators of compromise to protect themselves better. They must also assist increase awareness within the sector by sharing information about cybercrime. In addition, vulnerability mitigation must be used to ensure the vulnerabilities are realised beforehand and kept at bay; the practice will help the banking industries realise their system's vulnerabilities and patch them before massive data transfer and manipulation.

Data transmission in IoT systems has a high chance of being intercepted. Suppose the system has a low resistance to identifying device spoofing. In that case, as shown by the information shown above, Changes in peripheral device characteristics impact how the system behaves, and this must be understood. Therefore, massive education is needed on the vulnerabilities realised in this study.

A clear understanding of the vulnerability indicated in the study will be necessary for the uses in the IoT environment to take caution of them. This will help maintain the system's security as the system's users will undertake no risks. In addition, the mitigation practices discuss in the study will help the organisation identify the flaws on a system before hackers exploit them, hence maintaining high-security standards in the IoT cloud computing environment.

6.2. Recommendations for future studies

The study recommends that banking industries educate the employees on cyber security and vulnerability practices on the internet of things. In addition, practices such as software updates and the use of antiviruses to protect the system should be enhanced by the companies as vast as possible. During the study, the researcher also realised that there are limited studies on this topic; therefore, more studies on the topic should be done to have a well-informed society in the future. The study also realised only two methods for mitigating vulnerabilities; therefore, there is a need for further study on the same and an innovative mindset to develop other means for mitigating vulnerabilities in systems.

6.3 Chapter summary

In summary, this chapter indicates the vulnerabilities identified during the study and how they can be mitigated. In addition, a few practices that enhance security are highlighted. Lastly, recommendations on researches that could be done are indicated. One of the research highlighted technologies that can be employed to mitigate threats as there is no study on this topic.

References