National College of Ireland

Importance of IoT Security & Privacy to Mitigate Cyberattacks

MSc Research Project
MSc in Cybersecurity

Umesh Vinaykumar Khurana
Student ID: x20107013

School of Computing
National College of Ireland

Supervisor: Imran Khan

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name: ……Umesh Vinaykumar Khurana……

Student ID: ……x20107013……

Programme: ……MSc in Cybersecurity…… **Year:** ……2021-22…..

Module: ……MSc Research Project……

Supervisor: ……Imran Khan……

Submission Due Date: ……16/12/2021……

Project Title: …Importance of IoT security & privacy to mitigate cyberattacks….

Word Count: ……9974…… **Page Count**…..29……..

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.
ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature: …Umesh Vinaykumar Khurana……

Date: ……14/12/2021……

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

Attach a completed copy of this sheet to each project (including multiple copies)	□
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	□
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	□

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

Importance of IoT Security & Privacy to Mitigate Cyberattacks

Umesh Vinaykymar Khurana
x20107013

Abstract

The Internet of Things (IoT) is the next technology leap that will greatly improve a variety of aspects of human life, notably healthcare, business, and transport. Despite the fact that technology may lead to positive individual and financial outcomes, artefact and user Security and privacy protection are still major issues that have arisen. Specifically, information flow must now be monitored and regulated by security mechanisms. This study looks into the origins of (a) various security and privacy issues, (b) challenges faced in defending infrastructure and technology based on IoT, (c) appropriate security measures, and (d) types of secrecy that are most suited and necessary for different features of Internet-of-Things-driven apps. This study proposed an emerging IoT layers strategy. With security and privacy characteristics, as well as layer id, it is general and expandable. The planned IoT system with cloud/edge support has been developed and tested. The IoT nodes produced as Amazon Web Service Virtual Machines (AWS)as Amazon Web Service Virtual Machines (AWS) constitute the bottom layer. The intermediate layer (edge) was built using hardware for the Raspberry Pi 4and AWS' Greengrass Edge Environment. We used AWS' cloud-enabled IoT to create the top layer. Environment (the cloud). Safety protocols and critical organisational activities were developed across all of these layers to ensure the privacy of the clients' data. To allow data movement between the planned cloud/edge empowered IoT paradigm's layers, we built security certificates. The suggested system model not only eliminates potential security vulnerabilities but can also be utilised in conjunction with the best security strategies to mitigate the cybersecurity risks that each of the layers, cloud, edge and IoT face.

Keywords: Internet of Things, security and privacy, cloud IoT system, IoT layer model, Raspberry Pi 4, AWS Greengrass, cybersecurity

Table of Contents

1. INTRODUCTION

1.1 Background

The term "Internet of Things" (IoT) refers to a system of interconnected objects and gadgets. This is either a wired or a wireless internet connection. The Internet of Things has grown in popularity, despite the fact that it is utilised for various objectives such as networking, mobility, research, and commercial expansion. The Internet of Things (IoT) created hyperconnectivity by allowing corporations and individuals to communicate with one another from a distance. Kevin Ashton invented the name "Internet of Things" in 1999 to advocate the RFID (Radio Frequency Identification) theory, which incorporates interconnected Intelligent devices and sensors. However, the idea was first proposed in the 1960s. At the time, the terms "extensive computing" and "embedded internet" were used to describe the concept. The Internet of Things (IoT) was suggested by Ashton as a way to optimise supply chain systems. The IoT's varied capabilities, on the other hand, have supported its climb to prominence since its inception in the summer of 2010.

The Chinese government established a five-year programme with the Internet of Things as a core goal. Currently, there are around 26.66 billion IoT devices on the earth **(The IoT history and future - Itransition, 2019)**. With the introduction of smart homes, wearable technologies, and intelligent power metres in 2011, the mainstream boom began. Businesses have benefited from the rapid expansion of IoT in a variety of ways, including improved market research and corporate planning. Likewise, the Internet of Things has improved people's communities by providing self-service technologies. However, such unconstrained growth has sparked concerns about confidentiality and protection.

1.2 General findings

Internet-of-Things-capable technologies have been employed in industrial contexts and for a number of commercial objectives **(Makhdoom et al., 2019)**. Such software helps these companies obtain a strong position over their competitors in the market. Unfortunately, Most leaders are concerned about information security intrusions, which interrupt operating procedures, actions, and core networks, resulting from the successful completion of diverse, intelligent devices with data exchange and execution. To preserve seized assets and maintain business sustainability, experts should improve these concerns and develop robust security workflows. For example, attackers might exploit linked bright kitchen house IoT enabled gadgets to gain access to corporate and/or individual sensitive information, as well as disrupt and impact commercial activity.

Excessive identity utilisation, a failure to update credentials, and a dearth of technical improvements have raised cybersecurity concerns, permitting corrupted PCs to view confidential material on IoT devices. Privacy violations and other dangers are more probable as a result of inadequate security practices. Because of its weak security processes and laws, most security experts believe IoT is a susceptible area for cyber-attacks. Even though a variety of security techniques for protecting IoT devices from cyber-attacks have been **developed (Conti, Dehghantanha, Franke and Watson, 2018)**, as a result, end-users could not take steps to prevent data breaches. Since the beginning of 2008, hackers have begun building viruses to attack IoT applications. They devised a number of phishing methods in order to get workers or individuals to provide crucial information **(Aldwairi and Tawalbeh, 2020)**. As a response, serious cyberattacks often compromise the integrity of organisations and individual gadgets. By thoroughly evaluating cyber threats, device engineers and security professionals may build efficient protective strategies to stop or counteract cyber-attacks.

Every day, new technologies arise, and old ones are improved. Take a look at the most current developments in the 5G network. In IoT technologies, The importance of 5G has been identified. It attracts investigators due to its wide frequency range, which piques their interest in possible security and privacy issues. Conversely, short-wavelength technology necessitates a shift in infrastructure, needing extra entry points to cover the same area as prior technology for wireless communication. Fake base stations certainly, pose a greater hazard under this new setup. It is critical to be aware of security threats and possible solutions.

1.3 Novel Aspect and Existing approach of the project

In this work, I aim to provide an overview of the IoT applications, benefits, and potential risks. Additionally, to build a framework to study and further develop best security practices by either implementing and analysing current existing schemes or developing new ones. Based on the findings, I provide recommendations to avoid such risks and to remedy the possible security vulnerabilities. This work will guide regulatory agencies to continue enforcing policies, educating end-users and entities, and stakeholders involved in IoT to develop and apply more appropriate security and privacy measures.

I built this model using Amazon Web Service (AWS) as proof of concept, which later translated to actual physical systems of sensors nodes mimicking general IoT structure. By making the system, I can deploy and study different security approaches by building real sceneries and benchmarks.

I adopted a narrative review methodology to explore the history and background of the IoT systems, their security and privacy issues, and the corresponding countermeasures. I proposed my own view of the generic and stretched IoT model and its privacy and security concerns. I built and studied a cloud/edge supported IoT model consisted of a virtual machine (sensors), and edge node (Raspberry Pi), and cloud services (AWS). This setup was designed to evaluate the model we proposed in the following sections in this paper. Our work does not provide details on the different IoT applications (smart health, smart cities, supply chain, transportations, etc.); their features, advantages, and challenges, or the possible security risks or threats among these applications.

1.4 Report Format

This study focuses on understanding the Internet of Things (IoT) and its applications, benefits, and concerns. Even so, by implementing and reviewing existing mechanisms or developing unique ones, a framework for investigating and enhancing optimal security processes will be established. We make suggestions based on the findings for preventing such attacks and correcting any security weaknesses. This study would help state officials define criteria, engage individuals and customers, and support IoT technicians in developing and formulating better acceptable confidentiality precautions.

Amazon Web Service was utilised to build the model as a demonstration of the idea, which was subsequently interpreted into the exact structural sensor node systems that matched the overall IoT architecture. By building the system, I would be decided to examine and apply security measures by creating plausible scenarios and measurements.

The rest of this study is outlined into different sections: the next part introduces a research subject supported by evidence. In Section 3, IoT security and privacy problems were used to assess a literature review. Section 4 discusses the future of the Internet of Things. Section 5 presents the preferred cloud/edge supported IoT layered models. General and extended with

privacy and security components and layers identification. The suggested approach is implemented in Section 6 using AWS cloud and edge settings, as well as the Raspberry Pi 4 kit. Section 7 wraps off this project and looks ahead to what is next.

2. RESEARCH QUESTION

THE STUDY WILL BE CONDUCTED WITH THE GOAL OF RESPONDING TO THE FOLLOWING QUESTION:

How critical are the security and privacy of the Internet of Things (IoT) technologies in mitigating modern-day cyberattacks on small and medium-sized enterprises (SMBs)?

2.1 Motivation:

The Internet of Things (IoT) anticipates a semi-future in which objects could interact with each other via the Internet and actively contribute from any location and at any time. Sensors, actuators, the Internet, cloud computing, and various communication infrastructures are all part of the Internet of Things. This technology is employed in a multitude of fields, including energy, health care, and transportation **(Atzori, Iera and Morabito, 2017)**. According to Gartner, over 30 billion IoT devices will connect to the Internet by 2025 **(Newsroom, Announcements, and Media Contacts | Gartner, 2013).**

However, the IoT, like any other communication network, is prone to many flaws and security problems. Security is a primary priority since It is a modernised version of the old unprotected Internet. This paradigm encompasses wireless sensor networks (WSNs), optical networks, wireless data, and 2G/3G communication networks. Each of the technologies discussed above is vulnerable to various security risks **(Gartner, 2013)**. Furthermore, IoT devices have the capacity to interact with their environment in a dynamic and autonomous manner, without the need for external supervision, raising a number of security and privacy problems.

For the reasons stated above, it is vital to examine and analyse the privacy of IoT technologies. Regardless of how substantial and compelling these efforts are, the continual growth of cyberattacks necessitates the parallel research of adequate remedies, making thorough survey surveys necessary and profitable.

2.2 Justification

Even though the Internet of Things (IoT) promises a brighter future for its users, it offers a security risk like other technological breakthroughs. In this day and age, privacy is becoming increasingly crucial to the general population. The security of the Internet of Things must be enhanced before being used in people's daily lives. The performance of the Internet of Things is dependent on its security. The Internet of Things (IoT) is a fairly recent phenomenon. The lack of a very well and extensive system security and regulations stifle the expansion of IoT **(Kabir, 2021)**.

The Internet of Things includes WSNs, RFID systems, wireless networks, 3G technology, WiMAX, personal area networks, and other innovations, as opposed to traditional networks. Security challenges become more sophisticated than any present network architecture as the IoT ecosystem expands in complexity. Given the fact that the Internet of Things has a

promising future and is essential, the issue of if IoT applications can be widely adopted persists. The following factors, at the very least, cast doubt on this idea **(Kabir, 2021)**.

1) Security: The Internet of Things connects more networks than conventional networks, which raises security concerns.
2) Privacy: WSN devices are unlikely to be able to survive all types of assaults (physical and cyber). Sensitive information or location privacy may be jeopardised.

To find answers to the research, IoT devices will undoubtedly grow more prevalent in the future. Privacy issues, on the other hand, are still a hot topic today. Ensuring the protection and lowering storage capacity all across the planning stage of an IoT ecosystem is undeniably a key step into more anonymity.

2.3 Research Question Conclusion

IoT enabled devices have been used in industrial applications and for multiple business purposes. The apps help these businesses to attain a competitive edge over their competitors. However, due to the excessive adoption of various smart devices with data sharing and integration, the privacy and data breach becomes a significant concern to most businesses, as it interrupts the flow of work, activities, and network services. It is essential to have professionals to overcome these threat concerns and develop comprehensive security measures and policies to protect their business assets and ensure services continuity and stability. For example, smart kitchen home IoT enabled appliances connected to the local network can be a source of the breach for hackers to get access to the business and/or personally sensitive data or to manipulate and interrupt the business workflow.

Every day new technologies emerge, or changes are made to existing ones. Consider the latest advances in the 5G network, for example. 5G is expected to play an essential role in the IoT systems and applications. It is getting the researchers' attention and curiosity about the possible security and privacy risks, with its high frequency and bandwidth. Yet, the short wavelength imposes a change in the infrastructure, hence the need for more base stations to cover the same area covered by other wireless technology. This new structure imposes more threats, such as fake base stations. It is essential to understand the security risks and potential solutions.

3. LITERATURE REVIEW

The purpose of this section is to provide a complete assessment of the literature on IoT as well as to highlight the important themes and patterns that have emerged from recent studies on the subject. This section presents the theoretical material of previous studies in this area of IoT. The literature review includes academic journals, conference proceedings, books, and edited volumes. The study delves into the privacy and security concerns raised by this technology. Relevant content was discovered by searching databases for terms like "Internet of Things," "IoT," and "security and privacy."

Considering the Internet of Things' enormous benefits to its users, unique issues must be addressed. Two of the most critical themes mentioned are cybersecurity and privacy concerns. These two produce a slew of issues for corporations and government entities alike **(Leloglu, 2017)**. The dangers of IoT technology have been highlighted by recent high-profile cybersecurity incidents. Novel security measures are necessary because network connection in the Internet of Things gives internet access from an unauthorised and unverified source. However, when it comes to implementing an IoT security solution, it is vital to emphasise the standards and basic concepts of the IoT Cyber Security Framework **(Leloglu, 2017)**.

3.1 Related Works

A.-R. Sadeghi, C. Wachsmann, and M. Waidner wrote: "Security and privacy considerations in the industrial internet of things" (2015).

From vital infrastructure to modern autos to crucial infrastructure, smart mobile and cyber-physical platforms are becoming increasingly popular. According to **(Sadeghi and Waidner, 2015)**, With strong connectivity and the effective utilisation of new tiers of wireless systems, Industry 4.0 and the Internet of Things (IoT) give great innovative concepts and technology frameworks. These devices produce, analyse, and disseminate a vast amount of useful data. Cyber-attacks are a tantalising proposition for the Internet of Things system because of the heightened security and personal values that make them appealing. They cause harm to others and make life tough for them. Since they can constitute a risk, cybersecurity and visibility are vital. Because of the intricacies of current technology and the potential implications of cyber-attacks, connected business IoT devices are now facing extra hazards. To address security and privacy concerns in commercial IoT networks, standard safety mechanisms can be implemented. The current state of IoT systems makes it difficult to deliver the needed functionality **(Sadeghi and Waidner, 2015).**

Basu, S. S., Tripathy, S., and Chowdhury, A. R., "Design challenges and security issues in the Internet of Things" (2015).

Some of the most critical IoT security issues include the verification and authenticity of devices. Due to the vast diversity of devices in the IoT, determining and verifying a single object is challenging. It is difficult to verify that an organisation's information flow includes everything it is supposed to include without identification. S Basu, S Tripathy, and S Chowdhury discussed how an authorisation that is linked to authentication might be challenging. Some form of access control is essential to ensure that not everyone on a network has access to everything **(Basu and Tripathi, 2015).**

Gordon et al., "The Economics of Information Security Investment" (2002).

Ponemon et al., 'Cost of data breach study: global analysis' (2015).

Organisations have overspent on the highest firewalls, antivirus programs, email spam filtering, and complicated security networks for a long time. **Gordon (2002)** performed research to determine the right amount of resources that organisations need to expend in their information technology security measures. "The cost to expend in information security rises in direct proportion to the quantity of danger associated with such information," he argues. This means that the greater the risk, the greater the investment necessary to mitigate the defects. **Ponemon (2015)** conducted research on the "Costs of Data Breach," discovering that the average cost of a data breach to a corporation increased from $3.52 million in 2014 to $3.79 million in 2015.

A. Skarmeta and M. V. Moreno's "Internet of Things" (2013).

"IoT security, privacy, and trust must be considered as basic designs of radar systems," says the report according to **Skarmeta (2013),** citing "serious complex challenges confronting the IoT concept" According to a recent IoT security study conducted by **Brophy (2016)** for IOActive, According to about 50% of all security experts questioned, less than 10% of all IoT options on the market offer adequate security.

L. Atzori et al., "The Internet of Things: A Survey" (2010)

According to **Atzori (2010),** daily items pose greater security threats, and the IoT has the potential to disseminate those dangers considerably more widely than the Internet has done thus far. The linked nature of IoT devices, according to **Rose (2015)**, means that Any unprotected element that is linked has the potential to endanger the global security and resilience of the Internet. According to the FTC's 2015 study, IoT devices can assist high-volume assaults on other systems.

Andrea, I., Chrysostomou, C., and Hadjichristofi, G. "Internet of Things: Security vulnerabilities and challenges" (2016).

Andrea and Abomhara also discover some trust relationships. Trust is required at each layer of the Internet of Things **(Andrea, Chrysostomou, and Hadjichristofi, 2016)**. Interactions and level shifts must be secure and hidden. For security and privacy, each layer demands trust, which implies that each IoT level should be retained in any scenario. Finally, there should be some kind of connection between the individual and the IoT network. Other aspects of IoT trust management include the creation of innovative distributed trust models, the installation of networking devices for cloud computing, and the application of new ideas based on link security, which are all important goals of IoT trust research. They recommend that trust assessments be conducted in a conscious and computerised manner.

Khoo, "RFID as an Enabler of the IoT: Issues of Security and Privacy" (2011).

The writers explored the enabling technology RFID, which has the capability of identifying devices, tracking their location, exchanging information, and taking safeguards if necessary. They also talked about some of the obstacles that RFID technology faces, such as security and privacy concerns. The authors of this research have developed a strategy for dealing with security challenges by inserting a tag in a sleeping position **(Kho, 2012)**.

Roman, R., Najera, P., and Lopez, J. Securing the Internet of Things (IoT)

Many privacy-related options are provided by Roman et al. One of the concepts is confidentiality by architecture, which suggests that individuals would have control over

their data. Another important factor is transparency. Transparency in the Internet of Things entails people becoming conscious of who handles their information and how and when it is utilised. The final solution they recommend is data management. It is up to you to figure out who is in command of the secrets **(Roman, Najera and Lopez, 2018)**. A variety of data policy measures, as well as a method for enforcing such policies, must be in place. UPECSI (User-driven Privacy Assurance for Cloud-based Services in IoT), on the other hand, is a strategy developed by Henze et al. for handling IoT data in cloud settings. Consumers have control over their personal information before it is transmitted to the cloud via UPECSI.

Ayyash et al. "IoT: A Survey on Enabling Technologies, Protocols and Applications" (2015).

The researchers discussed IoT (Internet of Things), which is a combination of the Internet, sensors, and M2M technologies. They also covered a variety of IoT-related use-cases for various protocols. The authors of this paper look at the interaction between IoT and popular automation technologies, including big data analytics, cloud services, and fog nodes (**Al-Fuqaha et al., 2015)**.

Mahmoud, R., Yousuf, T., Aloul, F., and Zualkernan, I "Internet of things (IoT) security: Current status, challenges and prospective measures" (2015).

Several authentication systems have been proposed for IoT. Shieh S et al. offer verification models, encryption tokens, access control chain, and authorisation trust tree. Mahmoud R et al. have also created security mechanisms and suggest a one-time, one-cipher technique based on a request-response system **(Yousuf, Mahmoud, Aloul and Zualkernan, 2015)**.

Zhu et al. "Green IoT for Smart World" (2015).

The investigations have addressed a green IoT solution that uses less energy. They have also completed an architecture outline for IoT and Green IoT. In this article, the study explains sensors to the cloud, which is a distinct ideal in green IoT conception. **(Zhu, Leung, Shu and Ngai, 2015)**.

Nguyen, K. T., Laurent, M., and Oualha, N. "Survey on secure communication protocols for the Internet of Things"(2015).

Only a few existing security systems integrate features like access control and privacy protection. The intrusion detection service, according to K. M. Laurent, T. Nguyen, and N. Nguyen, is critical in the Internet of Things. They point out that server-based protocols with an authorisation server are often used to provide this capability **(Nguyen, Laurent and Oualha, 2015)**.

Weber and Boban, "Security challenges of the IoT" (2016).

The authors concentrated on the challenges of Information devices in the domains of anonymity and security amid diversity, as well as limitations in controlling devices as they grow by the second. The writers of this research analysed and contrasted two technologies: IoT and M2M. **(Weber and Boban, 2016).**

Zhang, C., and Green, R. (2015). Communication Security on the Internet of Things: Preventive Measure and Avoid DDoS Attack over IoT Network.

A Learning Automata (LA) has been proposed as a response to DDoS attacks in IoT networks. The LA would intelligently adjust the packet reference signal, according to **Zhang C and Green R**. Each endpoint's DDoS protection element would analyse the requests it gets during feature extraction. If a specified storage limit were surpassed, it

would send a DDoS notice to neighbouring nodes. The IP would be sampled by the devices. Address the problem and find the culprit as soon as the alarm goes off. After the attacker has been discovered, other nodes will be notified, and communications from the suspect's IP address will be removed. Depending on this technique, Zhang presents their innovative methodology for analysing and halting a DDoS attack in an IoT network. Another other option is to replicate the sink node (It gets sensor-generated information). This communication link would serve as a backup connection, undertaking some of the sink node's operations. This method is thought to be outlay**(Zhang and Green, 2016).**

Gupta and Shukla, "IoT: Security Challenges for Next Generation Networks" (2016).

The writers have explored how the Internet of Things (IoT) is maturing and has a number of security concerns. The authors of this article revealed that IoT applications had low computing power and impaired memory administration, both of which are significant issues in the networking sector **(Gupta and Shukla, 2016).**

Liu, X.; Zhao, M.; Li, S.; Zhang, F.; Trappe, W. A "Security framework for the internet of things in the future internet architecture" (2017).

Terminating a contract, including several components and routing protocols, is one of the most crucial tasks to consider. "Guidelines inequalities impede the implementation of various service agreements and are key components that must be incorporated in any Internet of Things" cybersecurity architecture," says the report **(Liu et al., 2017)**. He emphasised that a number of basic steps must be performed to assist reduce IoT cybersecurity challenges and ensure the IoT framework's security dependability. Trappe et al. further demonstrated that the cybersecurity Internet of Things system requires adaptability **(Liu et al., 2017)**. According to analysts, the Internet of Things architecture must be resilient in order to address a billion Internet and cybersecurity problems.

Chaudhary et al. "The IoT: Challenges & Security Issues" (2014).

(Matharu, Upadhyay, and Chaudhary, 2014) explored the overall layer architecture of the Internet of Things, as well as its future characteristics and constraints. The authors of this study presented a secure IoT framework development by addressing privacy concerns at every level of the IoT platform.

Zhao et al. "A survey on the internet of things security" (2013).

According to **Zhao (2013)**, The Internet of Things is a "merger of disparate networks" that has not just the same security concerns as conventional networks but also privacy concerns, problems with authentication, and access control issues. The primary social demands for the Internet of Things, according to **Uckelmann (2011)**, are open governance, security, privacy, and trustworthiness.

Rahman, M., et al. "Secure Management of Low Power Fitness Trackers" (2016).

A substantial number of security design issues in typical fitness trackers were uncovered in a previous investigation by Rahman p.449 of the IEE Computer Society. The following attack strategies were identified in the study: "1. Inspect attacks: the attacker listens in on tracker, base, and web server connections." **(Rahman, Carbunar, and colleagues, 2016, p. 449)** "2. Insertion strikes: the opponent exploits remedy weaknesses to update and introduce data into the network, as well as to interrupt present interactions." "3. Capturing strikes: the attacker obtains trackers or target bases"

3.2 Research Niche

As stated in Table 1, the table below comprises an overview of all literature as well as an explanation of how the suggested approach differs.

References	Research Topic	Characteristics	Analysis
Skarmeta (2013)	Internet of things	IoT products, privacy and trust	Only around ten percent of all IoT products on the market, according to almost half of all security specialists polled, provide appropriate protection.
Atzori (2010)	A review on the Internet of Things	IoT cloud risks	Due to the general interconnected nature of IoT devices, every poorly secured object that is attached has the potential to undermine global Internet security and resilience.
Andrea, Chrysostomou, and Hadjichristofi (2016)	Internet of things: security vulnerabilities and challenges	Trust management	Creating creative models for decentralised trust, as well as installing network components for cloud computing, are all aspects of IoT trust management.
Canedo and Skjellum (2016)	Using machine learning to safeguard IoT systems	IoT framework solution	Researchers Proposed a machine learning algorithm and a strategy for creating testbeds.

Gordon (2002)	The economics of information security investment, cost of data breach study: a global analysis	Spamming solution	They have conducted some studies about the best amount of resources businesses should invest in their IT security systems.
Razzak (2012)	Spamming the IoT	Authentication	Using encryption keys to validate the information in 2D barcodes is one way to avoid IoT fraud.
Kho (2012)	RFID as an IoT enabler: security and privacy concerns	RFID security	Various obstacles in the RFID system, such as security and privacy concerns, were discussed.
Roman, Najera and Lopez (2018)	Securing the IoT	IoT security	Provide a plethora of privacy-related options.
Al-Fuqaha (2015)	The Internet of Things: an overview of enabling technology, methods, and services	IoT protocols	The Internet of things (IoT) was discussed, which is a mix of Internet, sensors, and M2M technologies.
Singh (2016)	Twenty cloud-based IoT security concerns.	Regulatory solution	Certificate-based role-based access control regulations demand a cross-domain architecture for certificate validation.
Khorshed (2015)	Combining IoT with the processing power of the cloud	IoT Cloud environment	According to the results of 18 distinct

	and the expertise of big data analytics.		cyberattacks, the random forest algorithm had the best success rate.
Granjal, Monteiro and Sa Silva (2015)	Security for the Internet of Things: A review of existing standards and outstanding research questions	IoT sensors	For better connection, IPV6 has been used.
Yousuf, Mahmoud, Aloul and Zualkernan, (2015)	IoT security: present state, issues, and potential solutions	Access control	The models that have been proposed include verification, encryption token, access control chain, and authorisation trust tree.
Zhu, Leung, Shu and Ngai (2015)	Green IoT for an intelligent world	Cloud sensor	Sensor cloud, a cutting-edge idea in green IoT, was explained.
Nguyen, Laurent and Oualha (2015)	A survey on secure communication methods for the Internet of Things is being conducted.	Secure Protocols	The intrusion detection service, according to the claim, is critical in the Internet of Things.
Stampar and Fertalj (2015)	In network intrusion detection, artificial intelligence is used.	IDS system	Perspective is a method based on artificial intelligence, a subset of machine learning whose primary goal is to learn from data.
Basu and Tripathi (2015)	IoT design challenges and security concerns	Identification and Authentication	The problem with an authorisation that is linked to authentication has

			been addressed.
Weber and Boban (2016)	The Internet of Things presents a number of security problems.	Confidentiality	IoT and M2M are two technologies that have been compared.
Gupta and Shukla (2016)	The Internet of Things poses security issues for next-generation networks.	Security concern	It was determined that IoT devices had low processing power and memory management, which is a major worry in the networking business.
Liu (2017)	Future Internet architecture will include security mechanisms for the Internet of Things.	IoT architecture	It was stressed that some basic steps must be performed to assist reduce IoT cybersecurity challenges and ensure the IoT framework's cybersecurity dependability.
Matharu, Upadhyay and Chaudhary (2014)	The Internet of Things: Challenges and Security Concerns	IoT limitations	They have Dealt with security problems at each tier of the IoT framework to ensure secure development of the IoT building.
Zhao (2013), Uckelmann (2011)	A poll on the security of the Internet of Things	IoT privacy and security	According to the research, the major societal expectations for the Internet of Things are open governance, security, privacy,

			and trustworthiness.
Rahman, Carbunar (2016)	Low-power fitness trackers must be managed securely.	Secure communications	Many security design issues in popular fitness trackers have been discovered.
Sadeghi and Waidner (2015)	Industrial IoT security and privacy issues	IoT attacks	By utilising new layers of portable systems and providing new creative models and software platforms, you may provide new ones.

Table 1: Literature review research niche summary

3.3 Literature Gaps:

At the moment, there must be at least two subjects that require more investigation. Device clusters will be the next iteration of Internet of Things devices. Cluster validation, or the evaluation of such systems, is still in the works. Another problem that deserves further investigation is secure device management for IoT devices. Because of the expanding number of devices on the market, appropriate security measures cannot keep up. A secure, private IoT architecture is still needed. Existing solutions are considered too complex for the Internet of Things' low-resource devices. According to the researchers, IoT systems require a short technique without relying on expensive symmetric matching.

3.4 Expected Contribution:

The examination and analysis of various security risks in the IoT have become extremely important. One of several primary purposes of IoT Security controls is to offer consumers privacy and integrity by assuring increased protections, access, and verification of the existence of more IoT services. As a result of multiple computational methods and varied technology systems, work in various IoT security is acquiring critical traction.

A new perspective on IoT models was offered as a result of this research: general and extended, encompassing aspects of privacy and security and layer authentication and isolation. A cloud/edge-enabled IoT system is created to implement the specified IoT models. As an outcome, the broad and extended methods are designed first, followed by a detailed of a more in-depth understanding of the application and installation environment (layered model development). The results will be discussed and given.

4. RESEARCH METHODOLOGY

4.1 IoT Security and Privacy challenges

The Internet of Things has provided several benefits to people, but it has also had a lot of problems. Intellectuals and defence specialists are most concerned about cybersecurity and privacy issues. Because of these two issues, several companies and organisations are at risk. Consistently high infringements have spotlighted the drawbacks of IoT technology. The Internet of Things' network connectivity poses a vulnerability that allows access from the unknown and insecure Internet, necessitating creative security measures **(Tawalbeh, 2017)**.

4.1.1 Security

The Internet of Things varies from conventional computers and technology equipment in several ways, making it more susceptible to security threats **(Alaba and Hashem, 2017)**:

- Many Internet of Things devices are designed to be industrially in enormous quantities. Sensors are an excellent example of this.
- In most situations, an IoT deployment contains a number of sensors with comparable or almost identical capabilities. Because of this resemblance, every security vulnerability that impacts a large number of them has a higher impact.
- Similarly, several organisations have developed risk analysis criteria. The number of parameters linking IoT devices is projected to skyrocket as a result of this approach. Many of these detectors can automatically connect to other devices and engage with them. This requires an examination of modern IoT security technology, strategies, and procedures.

When it relates to confirmation, IoT is particularly sensitive to a range of defects, which remain to be among the biggest complex difficulties in ensuring security in diverse applications. Because it only protects against a certain sort of attack, like DoS or replays attempts, the access control used is limited. Due to the prevalence of dangerous apps in the IoT ecosystem and their inbuilt complexity of data collection, information assurance is one of the most vulnerable areas in IoT authentication. Take the problem of NFC credit cards. These cards may be used to investigate login details and identity without requiring ID verification.

Among the most common cyber threats in the IoT is the man in the middle attack. A network operator compromises a communication channel in order to counterfeit the identities of genuine network nodes involved in a network exchange. Because the adversary is not required to be aware. The purported suspect's identity, the MITM attack, effectively hacks the bank system and accepts the payment as an actual occurrence **(Khan and Salah, 2018).**

4.1.2 Privacy

How well the Internet of Things can fulfil private personal data has an impact on its long-term viability. Security concerns and possible threats linked with IoT could play a major role in slowing IoT's successful adoption. It is crucial to acknowledge that client trust and faith in IoT technologies are essential; connected devices and other technological components are based on privacy and data security rights. Much effort is being made to ensure that the Internet of Things (IoT) functions effectively. However, the IoT affects confidentiality, such as increased eavesdropping and surveillance. Pervasive cognition connected things, where the survey approach and content exchange in IoT can be done almost anywhere, raise privacy problems. Understanding this issue also requires an understanding of resource efficiency via Internet access. Unless a unique approach is created, it will be much easier to obtain sensitive information from anywhere globally **(Bugeja, Jacobsson and Davidsson, 2016)**.

4.2 Future of IoT

Network connection and computational power are now available to devices and technologies, as well as the capacity to communicate with other connected items and devices **(Personal data breaches and securing IoT devices, 2019).** Increasing the channel's capability to include any physical site possible would improve our lives while saving energy and money. Getting onto the network, on the other hand, necessitates dealing with potential cyber dangers. Cybercriminals prey on objects with internet connections. The growth of the IoT business increases the number of possible dangers to employment, device security, and, as a result, our privacy. Cyber-attacks have grown significantly, according to research. Sixty percent have happened in the United States alone since 2015. **(Digital Identity and Security, 2020)**. According to studies undertaken in Japan, Canada, the United Kingdom, Australia, the United States, and France, 63 percent of Internet of Things (IoT) users consider these devices are frightening due to a lack of security. 90 percent of clients are sceptical about IoT security, according to a survey **(Maple, Watson, and Tiwari, 2016)**.

The present study examined a number of unique ways for decreasing cyber-attacks and enhancing privacy protection. A few of the ideas discovered throughout the investigation are given below.

Implementing encryption mechanisms: As a result of the employment of solid and higher encryption methods and mechanisms in both cloud and device configurations, hackers would be unable to exploit the worthless protected datasets**(Jose and Singh, 2016)**.

Updates should be made more frequently: Device manufacturers should focus on little repairs rather than major updates. Using this method, patch installation may be made easier. Furthermore, customers will benefit from frequent updates in averting cyber-attacks from a number of sources **(Sohal, Sandhu, Sood and Chang, 2018)**.

To raise security awareness, develop written user guidelines: Insufficient technical involvement is the root of the bulk of data breaches and IoT cyber-attacks. Customers seldom consider safety measures or restrictions while purchasing IoT devices. Users can avoid these issues if gadget manufacturers correctly disclose the potential dangers of IoT.

There will be light in a huge number of cities. New horizons will open up due to the use of IoT in city planning. The widespread use of IoT will result in improved road management, with no traffic jams on the highways, less pollution in communities, and the greatest degree of safety.

5. IMPLEMENTATION

5.1 Proposed IoT Layered Models

This study looks at both broad and diverse IoT architectures, taking into consideration privacy protection concerns, as well as layer classification and division. A cloud/edge enabled system is intended to implement the IoT concepts defined. As a result, the basic and extended models will be addressed first, followed by a description of the evaluation approach and implementation setting (layered model construction). Lastly, the results will be presented and discussed.

5.1.1 Data Fusion Model with Generic IoT Layers

Figure 1 depicts the overall layout of the Internet of Things network, which includes the device, cloud, and end-user levels. The app's tier is composed of a collection of detectors that are securely networked, data gathering chips, and communication techniques for transferring data to local or distant computing storage. These technologies enable users to collect data in real-time at various intervals.

Detector information is saved in the cloud layer for further analysis, reduction, semantic segmentation, and customisation. This information is then forwarded to a prediction model, which makes a health-related decision based on complex data collecting and machine learning.

The receiver, which is part of the end-user layer, can take many different forms. Smart devices are a cause of worry due to the security and privacy issues they bring. To maintain the recommendation platform's robustness, a list of parts or subsystems is placed inside the limitations of these three tiers.

The proposed method incorporates edge computing features capable of making such informed choices while also stashing a backup of the data and conveying it to the cloud layer for handling elongated storage to confirm information is recorded and analysed fast enough to make a crucial decision that cannot wait until the statistics are uploaded to the cloud. Some wearables may require instructions or directives from time to time to increase their rate of acquisition or functionality; this will need the usage of a variety of interfaces and data security.

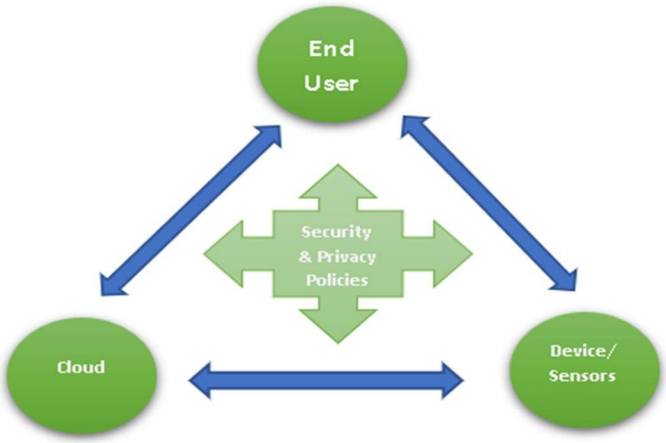

Figure 1: Regulations for Security and Privacy in a Generic Model.

5.1.2 Security and Privacy regulations

Cloud-based services that enable data storage, processing, and sharing are widely regarded as the IoT's critical infrastructure **(Singh et al., 2016)**. Hackers and cybercriminals target Internet of Things (IoT) information systems and terminals that keep or send critical information. Because of patient data and computerised medical documentation, the healthcare business, for example, is potentially exposed to hackers. While enforcing regulations concerning security and privacy, and processes, each level of the proposed ecosystem presents a security risk. Sensor readings are relayed to the edge, fog, and eventually the cloud in the device layer, for example. Authorisation and credentials that authenticate particular servers are required to thwart these attacks. Firmware privacy, physical address identification, and other features are available; Conversely, since many wireless-enabled items, including wearables, are fuelled by cells, this comes at a cost in terms of energy consumption. In order to accomplish both secrecy and resource restrictions, such security measures must be studied.

At the cloud layer, the authentication method between edge and fog nodes, as well as between detectors, must be safeguarded. Due to the apparent basic communication technique, point-to-point encryption, and authentication, data interception and recording may be minimised. Long-term digital information and legitimate analysis of data must be safeguarded against SQL injection attacks, sniffer attacks, and phishing scripting attacks at the workflow and end-user levels provided the service certificate is kept up to date and fulfils HIPPA standard (in health systems) **(The HIPAA Privacy Rule, 2018)**. Attackers might utilise machine learning to discover a new technique to identify a person, resulting in a data breach. Traditional security procedures are becoming increasingly complex. When IoT devices come and exit a collection of devices, and data sets, new intelligent and adaptable security techniques are formed **(2015).**

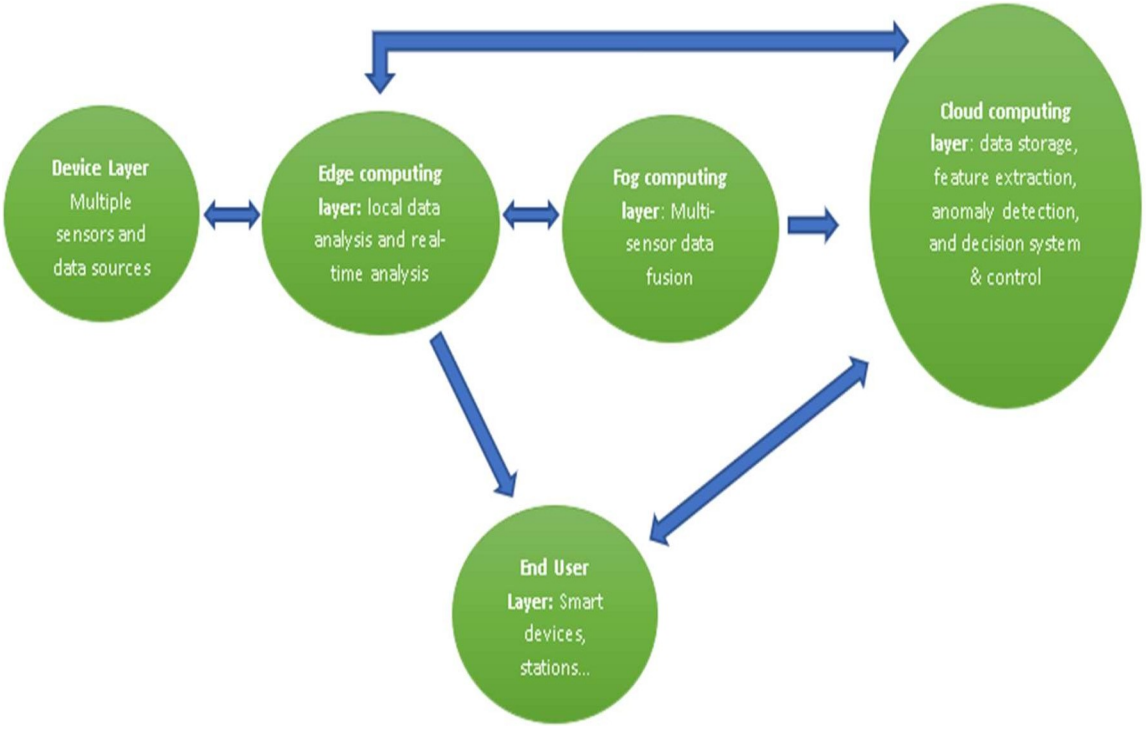

Figure 2: Extending the IoT Model

Figure 2 shows an expanded version of the overall model. There are two new layers, edge and fog, that may be seen. By depending on cloud layer objects and making timely judgments, both levels may be willing to surmount technical glitches. Cloud technology occurs on computers that are linked to or near devices. They provide you with complete empowerment over your data sets while interacting with other elements to offer info for integration, collecting, and statistics. The fog computing layer physically separates information and data streams from edge computing operations, which are relocated to a more constructive processing capacity tied to the local area network. As a result of these additional features, there are more security and privacy issues.

5.2 Proposed Layered Cloud-Edge-IoT Model

This work plan guarantees that security safeguards are in place before integrating IoT capable devices into a dedicated server, guaranteeing that They may converse and transmit information in a secure manner while protecting data privacy using encryption. The hardware, software, and connectivity concepts are summarised in Figure 3. AWS serves as the primary cloud, with Virtual Machines serving as IoT systems and the Raspberry Pi 4 serving as an Edge Node. The proposed layered design made use of an AWS premium version to give me full access to all AWS resources, including such security and encryption keys, authorisation, and identification.

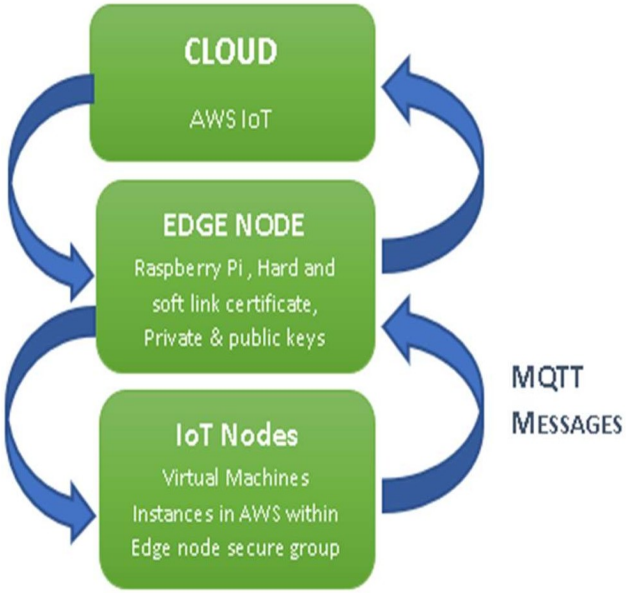

Figure 3: Model of the proposed system.

In this strategy, the AWS Identity and Access Management web service (IAM) from the AWS accessible resources will be employed. The users' access will be controlled by giving each user their own IAM account. Due to security concerns, the AWS Root account will not be used rather than generating an IAM user with administrative privileges. The AWS Greengrass Core instantly connects to the cloud and works the same way as a Raspberry Pi as an edge node. The Raspberry Pi will be set up to make a link between AWS and the Raspberry Pi by providing Linux hard and soft link security mechanisms. The AWS Greengrass core will be utilised to create a group that will include the primary sensor as well as all other Internet of Things devices that will communicate to the edge.

To authenticate all devices using AWS, certificates will be required. To provide a critical link between the edge and AWS, I have generated private and public keys certificates. AWS generated the core certificates once we formed the Greengrass group, as illustrated in Figure 4 below. We began the Greengrass Core after downloading the created files to the Raspberry Pi.

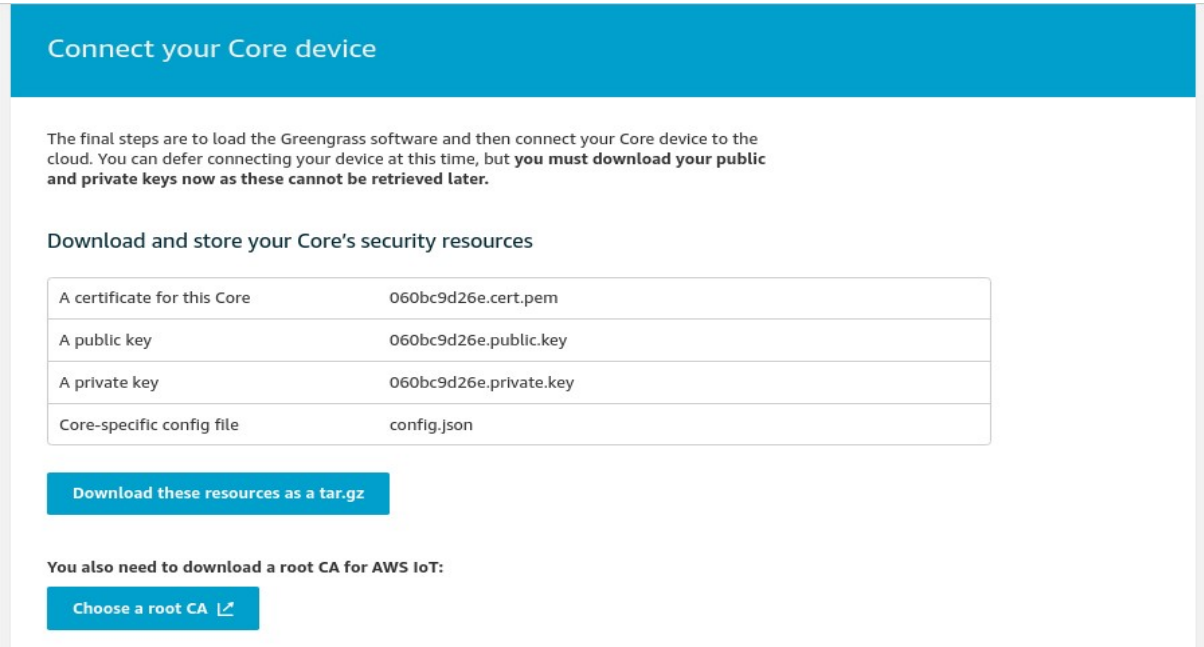

Figure 4. Certificate, Private and Public keys.

6. EVALUATION & ANALYSIS

I have designed a simple scenario in which two Embedded devices communicate with one another via our edge computing platform. The IoT devices were built up as virtualisation in AWS and connected to the Greengrass core, as shown in Figure 5. During the design phase, each device collects a specific credential, public and private keys, and is authenticated with AWS and the Greengrass Core device. A message broker was utilised to securely connect between these two devices using the MQTT protocol **(What is AWS IoT? - AWS IoT Core, 2019).** Finally, Figure 6 shows that both IoT nodes and Edge nodes communicated effectively, with data transmissions completed at predefined times.

The below are some critical points to remember about our AWS working environment and design:

- AWS IoT Core connects IoT devices to one other and the cloud in the general paradigm.
- I added the premise of the edge to this architecture by utilising AWS' Greengrass IoT fundamental idea and modelling it with Pi. Consider it an extra intermediary between IoT devices and the AWS IoT Core, and then the cloud.
- For each device, a certificate, private key, and CA Root certificate are required (this is the AWS IoT certificate). There are several sorts of CA Root certificates available depending on the type of IoT device.
- Each device requires a policy, which specifies which activities it may execute (connect/receive/publish/subscribe, for example).

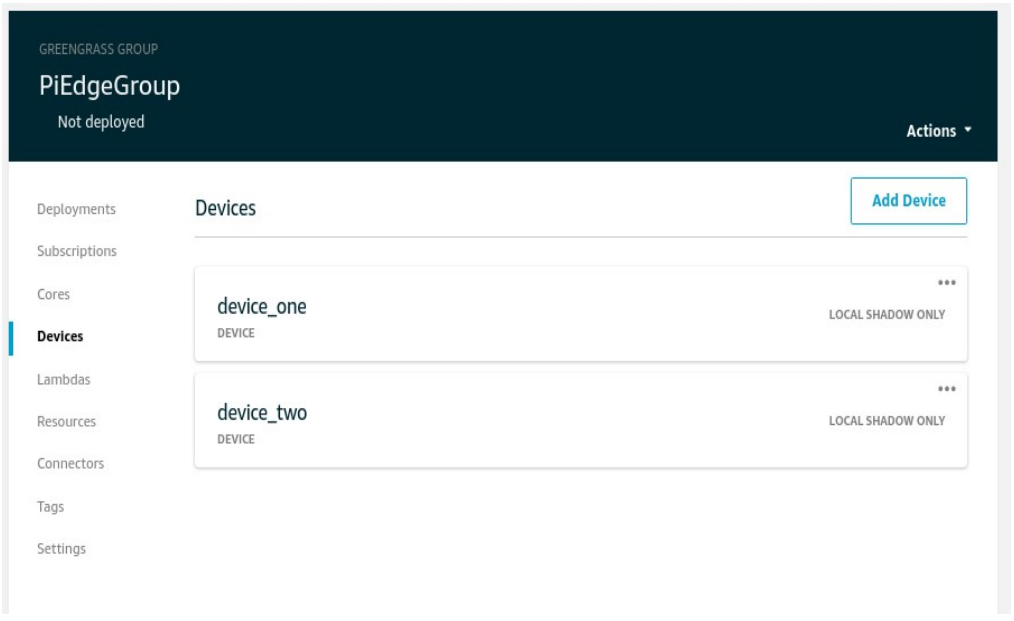

Figure 5. Nodes with IoT capabilities.

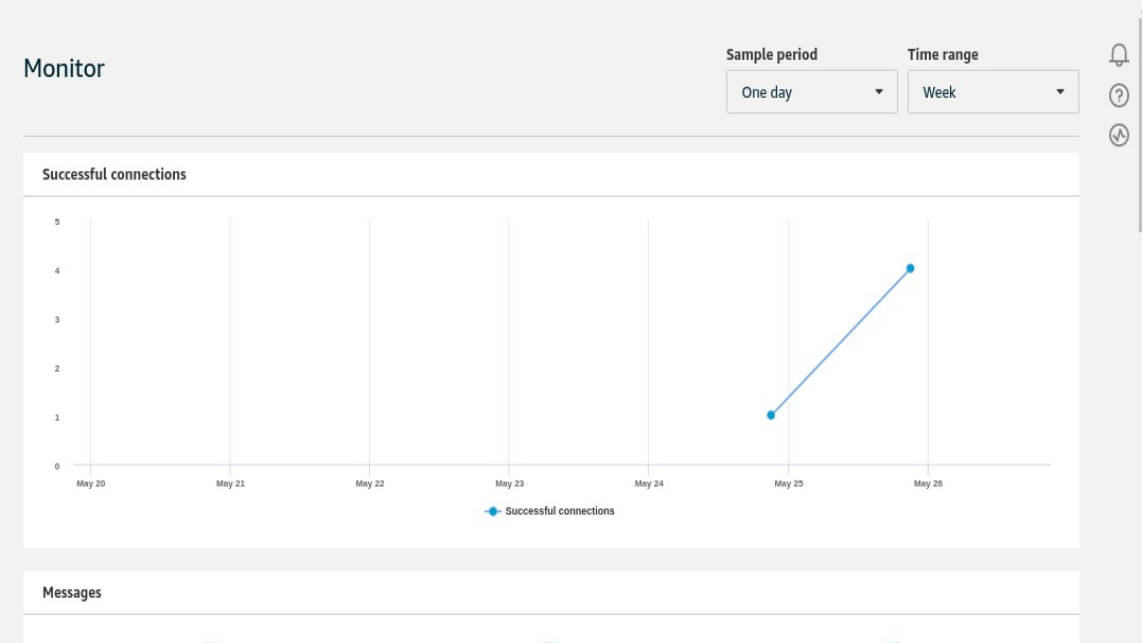

Figure 6. Communication and data exchange between nodes are successful. The x-axis shows the number of days in the month, while the y-axis reflects the number of connections.

As a result, I built a device, a policy, and a certificate. The policy was then connected to the certificate, which was subsequently attached to the device. Figure 7 depicts a standard policy below:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "iot:*",
      "Resource": "*"
    }
  ]
}
```

Figure 7. AWS's default device policy.

- As per the standard policy, the device can do all actions (Action: IoT: *) from and to all other devices (Resource: *).
- I created a new approach to addressing the extra Greengrass layer in this framework.
- Additionally, action: greengrass: * specifies that the Greengrass group device may conduct all acts from and to other Greengrass group devices (Resource: *).

Figure 8 depicts the amended policy for our model. In this case, we communicate utilising the MQTT protocol, which is a machine-to-machine procedure. MQTT is used because it is compact (brief messages and power efficiency), making it appropriate for use in a confined environment (sensors as an example in real applications).

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "iot:Publish",
        "iot:Subscribe",
        "iot:Connect",
        "iot:Receive"
      ],
      "Resource": [
        "*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "greengrass:*"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```


Figure 8. Modified device policy to incorporate the edge layer in the proposed model.

Moreover, the AWS Sensor nodes are emulated as MQTT clients (if virtual, as in our case), and the MQTT clients communicate through an MQTT Topic. The relationship may be viewed as a secure channel between clients that have been formed, registered to, and utilised to broadcast messages by other clients.

Installing JAVA JDK8, Greengrass files, and contracts Entered software (depending on the device used—in our case, a Raspberry Pi 4) is now part of the Raspberry Pi setup process.

As seen in Figure 9, all of these files were transferred to the Raspberry Pi 4.

Figure 9. The Raspberry Pi 4 package installation.

I needed to extract the relevant files and modify several configuration files to match the created certificates and keys after transferring them to the Raspberry Pi 4.

Finally, the Greengrass core device was turned on. The raspberry device operated as an Edge successfully, as seen in Figure 10.

Figure 10. Greengrass is successfully running on the Raspberry Pi 4 kit.

After establishing the environment and confirming it was accessible, I created an MQTT matter in our instance and named it (my/topic). Then I created a system to become a subscriber to my/topic and another to become a publisher to my/topic. All endpoints (by default) may do all tasks with all other devices, and all interactions are properly relayed. Figure 11 displays the many aspects of interaction that occur in a single day. The connection time is influenced by a variety of factors, including network latency and the platform used.

The suggested IoT paradigm demonstrated that I could verify that privacy and security protections existed before allowing IoT enabled devices or nodes to communicate or exchange their data. I am confident that my assets will be safeguarded after successful implementation and setup. With fog/edge computing layers and sensor fusion, the paradigm proposed in this research may be leveraged to offer secure IoT environments and systems. This model has a wide range of real-world applications, including healthcare, military, disaster recovery, and many more **(Sethi and Sarangi, 2017).** Consider the healthcare scenario: by implementing the suggested policy-based approach, Customers are allowed to rely on their healthcare provider to give them protection, guaranteeing that they are adequately taken care of. Wearables are being invested in by healthcare firms in the hopes of improving staff productivity, reducing absenteeism, and lowering healthcare expenses. Another important aspect of The benefit of wearable devices is the certainty that they may offer to those who are visually impaired. For instance, an individual with exceptional needs will be able to enter commands and data by just sliding their finger up and down. The amount of security users who may apply to their accounts is a final way, but it is not the only one.

People might, for example, set restrictions on who can see their social media postings or create rules that highlight the significance of adding more excellent protection to their account (e.g., two-factor authentication) **(Liyanage, Kumar, and Ylianttila, 2018).**

While the developers of IoT apps (in this case, healthcare) strive to provide the best service possible to their consumers, some gaps still exist. One disadvantage would be how third parties keep and utilise the user's information. It is mostly the provider's responsibility to ensure that they develop guidelines and give a strategy that will keep them in great condition with vendors and users. The same can be stated for the clients' privacy. Third parties (such as insurance firms) are usually able to obtain user information if they "agree" to it, and determining whether or not it is accurate from there can be perilous.

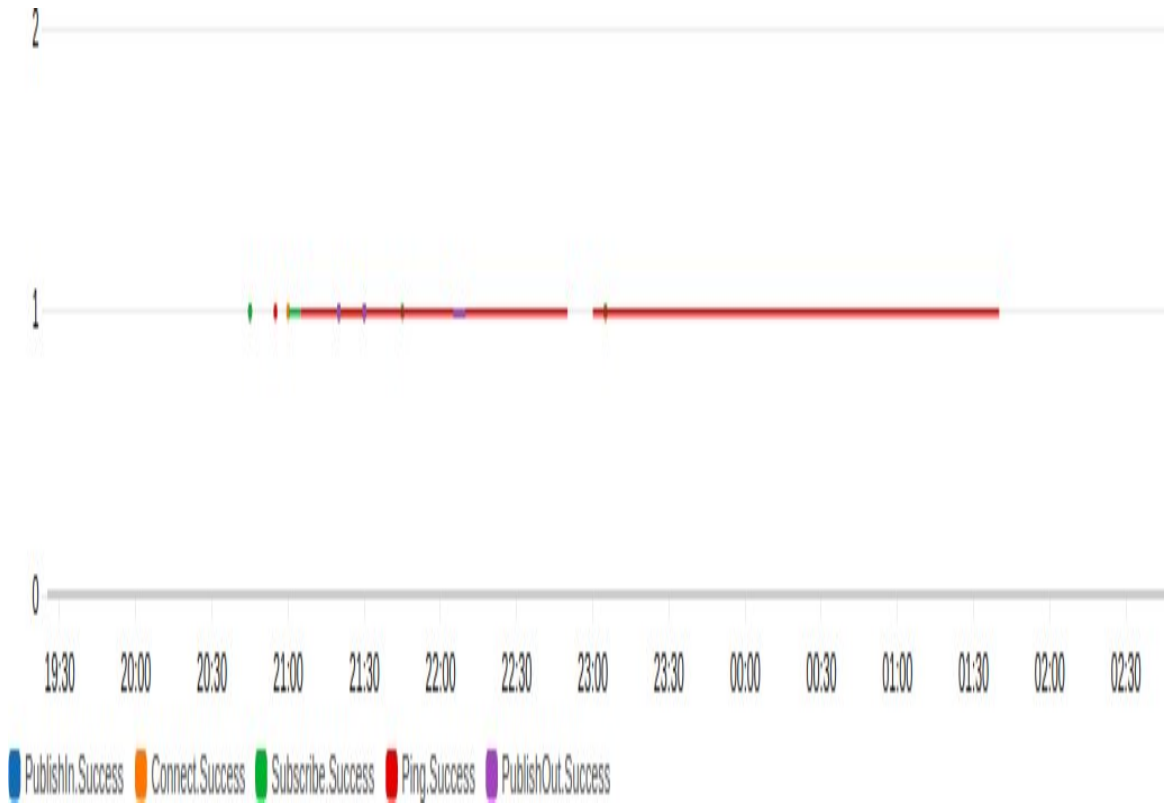

Figure 11. Messages of various sorts were successfully exchanged: Publish. Connect to achieve success. The subscription was a success. Ping, congratulations. Congratulations, Publishout. Success. The x-axis depicts the hours of the day, while the y-axis represents a single day.

7. CONCLUSION & FUTURE WORK

IoT gadgets have become much more prevalent in our regular lifestyle. IoT devices can be seen almost anywhere, including our homes, workplaces, shopping malls, schools, airports, and a number of other places, and they provide us with secure and on-demand capabilities.

The Internet of Things devices makes it easier to collaborate with customers and understand operational requirements and achievements. Furthermore, IoT-based insights and data analysis can assist corporate facilities in increasing production and efficiency.

Therefore, IoT applications are incorporating a number of significant technology improvements across a wide range of businesses. Several providers and companies utilise a range of limitations to protect their connected devices from unwanted attacks. As these kinds of devices link to our private networks and the Internet, greater privacy and security concerns have arisen. We have heard and read that our coffee machine is listening in on our talks and that our smart doorbell is transmitting photographs of our guests to the government. Many real-world examples demonstrate the significance of the security concerns associated with IoT devices.

In this research, I proposed new IoT layered models that are both broad and enhanced with confidentiality aspects, as well as layer recognition. The proposed IoT system with cloud/edge support was created and tested. The lowest layer is made up of IoT nodes generated by Amazon Web Service (AWS) as Virtual Machines. The intermediary layer (Edge) was created with the Raspberry Pi 4 hardware kit and AWS' Greengrass Edge Environment. The top layer, which is the cloud, is implemented using AWS's cloud-enabled IoT ecosystem. Security protocols and critical management activities were developed between each of these layers to ensure the privacy of the users' information. We created security certificates to permit data transmission between the levels of the proposed Cloud/Edge enabled IoT framework.

Future Work

Additional study should be carried in the future on strong encryption algorithms that are substantially more powerful enough to run on resource-limited IoT systems (Lightweight Crypto). It will help ensure that users of diverse degrees of expertise can reliably access and establish IoT devices, despite the fact that many of these IoT devices have terrible user interfaces. Additionally, there is an urgent need to unify the data collection and sharing methods utilised by Internet-connected IoT devices. Such guidelines will reduce the number of unforeseen vulnerabilities and associated assaults on non-homogeneous systems.

I investigate the benefits and drawbacks of the Internet of Things. With all of the positives, certain risks may be used to harm end-users by granting unauthorised access to confidential private data, allowing system attacks, and affecting personal security. After IoT - connected products are introduced to the market; we must ship them with appropriate security measures that influence their practicality, function, and compatibility with existing systems. With the help of researchers, we intend to develop a dynamic security framework that will minimise, rather than eliminate, security and privacy concerns while still being adaptable enough to respond to changes in new information and communication technologies and application deployment scenarios.

References

Itransition.com. 2019. *The IoT history and future - Itransition*. [online] Available at: < https://www.itransition.com/blog/iot-history > [Accessed 9 December 2021].

Makhdoom, I., Abolhasan, M., Lipman, J., Liu, R. and Ni, W., 2019. Anatomy of Threats to the Internet of Things. *IEEE Communications Surveys & Tutorials*, 21(2), pp.1636-1675.

Conti, M., Dehghantanha, A., Franke, K. and Watson, S., 2018. Internet of Things security and forensics: Challenges and opportunities. *Future Generation Computer Systems*, 78, pp.544-546.

Aldwairi, M. and Tawalbeh, L., 2020. Security techniques for intelligent spam sensing and anomaly detection in online social platforms. *International Journal of Electrical and Computer Engineering (IJECE)*, 10(1), p.275.

Atzori, L., Iera, A. and Morabito, G., 2017. *Understanding the Internet of Things: definition, potentials, and societal role of a fast-evolving paradigm*.

Gartner. 2013. *Newsroom, Announcements and Media Contacts | Gartner*. [online] Available at: < https://www.gartner.com/en/newsroom > [Accessed 9 December 2021].

Kabir, S., 2021. Internet of Things and Safety Assurance of Cooperative Cyber-Physical Systems: Opportunities and Challenges. *IEEE Internet of Things Magazine*, 4(2), pp.74-78.

Sadeghi, A.-R.; Wachsmann, C.; Waidner, M. Security and privacy challenges in industrial Internet of things In Proceedings of the 2015 52nd ACM/EDAC/IEEE Design Automation Conference (DAC), San Francisco, CA, USA, 8–12 June 2015; pp. 1–6.

Basu, S. S.,Tripathy, S., and Chowdhury,A. R. (2015). Design challenges and security issues in the Internet of Things, *IEEE Region 10 Symposium, IEEE*, 90–93.

Gordon, L. and Loeb, M., 2002. The economics of information security investment. *ACM Transactions on Information and System Security*, 5(4), pp.438-457.

Ponemon, L. (2015). "Cost of data breach study: Global Analysis." Poneomon Institute sponsored by IBM.

Skarmeta, A. and M. V. Moreno (2013). "Internet of things." Secure Data Management: 48-53.

Atzori, L., et al. (2010). "The internet of things: A survey." Computer networks **54**(15): 2787-2805.

Andrea, I., Chrysostomou, C., and Hadjichristofi, G. (2016). Internet of Things: Security vulnerabilities and challenges, *Proceedings – IEEE Symposium on Computers and Communications*, 180–187

Canedo, J. and Skjellum, A., 2016. Using machine learning to secure IoT systems. *2016 14th Annual Conference on Privacy, Security and Trust (PST)*,

Razzak, F., 2012. Spamming the Internet of Things: A Possibility and its probable Solution. *Procedia Computer Science*, 10, pp.658-665.

Rekleitis, E., Rizomiliotis, P. and Gritzalis, S., 2011. How to protect security and privacy in the IoT: a policy-based RFID tag management protocol. *Security and Communication Networks*, 7(12), pp.2669-2683.

Roman, R., Najera, P., and Lopez, J. Securing the Internet of Things (IoT), *IEEE Computer*, 44, 51–58.

Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M. and Ayyash, M., 2015. Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications. *IEEE Communications Surveys & Tutorials*, 17(4), pp.2347-2376.

Singh, J., Pasquier, T., Bacon, J., Ko, H. and Eyers, D., 2016. Twenty Security Considerations for Cloud-Supported Internet of Things. *IEEE Internet of Things Journal*, 3(3), pp.269-284.

Khorshed, M., Sharma, N., Kumar, K., Prasad, M., Ali, A. and Xiang, Y., 2015. Integrating Internet-of-Things with the power of Cloud Computing and the intelligence of Big Data analytics — A three layered approach. *2015 2nd Asia-Pacific World Congress on Computer Science and Engineering (APWC on CSE)*.

Airehrour, D., Gutierrez, J. and Ray, S., 2016. Secure routing for Internet of things: A survey. *Journal of Network and Computer Applications*, 66, pp.198-213.

Zhu, C., Leung, V., Shu, L. and Ngai, E., 2015. Green Internet of Things for Smart World. *IEEE Access*, 3, pp.2151-2162.

Nguyen, K., Laurent, M. and Oualha, N., 2015. Survey on secure communication protocols for the Internet of Things. *Ad Hoc Networks*, 32, pp.17-31.

Stampar, M. and Fertalj, K., 2015. Artificial intelligence in network intrusion detection. *2015 38th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*,

Weber, M. and Boban, M., 2016. Security challenges of the Internet of things. *2016 39th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*,.

Mahmoud, R., Yousuf, T., Aloul, F., and Zualkernan, I. (2015). Internet of things (IoT) security: Current status, challenges and prospective measures, *10th International Conference for Internet Technology and Secured Transactions (ICITST)*, IEEE, 336–341.

Zhang, C., and Green, R. (2015). Communication Security in Internet of Thing: Preventive Measure and Avoid DDoS Attack over IoT Network, *Proceedings of the 18th Symposium on Communications & Networking*, 8–15.

Liu, X., Zhao, M., Li, S., Zhang, F. and Trappe, W., 2017. A Security Framework for the Internet of Things in the Future Internet Architecture. *Future Internet*, 9(3), p.27.

Matharu, G., Upadhyay, P. and Chaudhary, L., 2014. The Internet of Things: Challenges & security issues. *2014 International Conference on Emerging Technologies (ICET)*,.

Zhao, K. and L. Ge (2013). A survey on the Internet of things security. Computational Intelligence and Security (CIS), 2013 9th International Conference on, IEEE.

Rahman, M., Carbunar, B. and Topkara, U., 2016. Secure Management of Low Power Fitness Trackers. *IEEE Transactions on Mobile Computing*, 15(2), pp.447-459.

Tawalbeh, L.A.; Tawalbeh, H. Lightweight crypto and security. In Security and Privacy in Cyber-Physical Systems: Foundations, Principles, and Applications; Wiley: West Sussex, UK, 2017; pp. 243–261.

Alaba, FA; Othman, M.; Hashem, I.A.T.; Alotaibi, F. Internet of Things security: A survey. J. Netw. Comput. Appl. **2017**, 88, 10–28

Khan, M. and Salah, K., 2018. IoT security: Review, blockchain solutions, and open challenges. *Future Generation Computer Systems*, 82, pp.395-411.

Bugeja, J.; Jacobsson, A.; Davidsson, P. On privacy and security challenges in smart connected homes. In Proceedings of the European Intelligence and Security Informatics Conference (EISIC), Uppsala, Sweden, 17–19 August 2016; pp. 172–175.

BetaNews. 2019. *Personal data breaches and securing IoT devices*. [online] Available at: < https://betanews.com/ 2019/08/13/securing-iot-devices > [Accessed 9 December 2021].

Thales Group. 2020. *Digital Identity and Security*. [online] Available at: < https://www.thalesgroup.com/en/markets/digital-identity-and-security > [Accessed 9 December 2021].

He, H.; Maple, C.; Watson, T.; Tiwari, A.; Mehnen, J.; Jin, Y.; Gabrys, B. The security challenges in the IoT enabled cyber-physical systems and opportunities for evolutionary computing & other computational intelligence. In Proceedings of the Evolutionary Computation (CEC), Vancouver, BC, Canada, 24–29 July 2016; pp. 1015–1021.

Al Shuhaimi, F.; Jose, M.; Singh, A.V. Software-defined network as a solution to overcome security challenges in IoT. In Proceedings of the Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO), Noida, India, 7–9 September 2016; pp. 491–496.

Sohal, A., Sandhu, R., Sood, S. and Chang, V., 2018. A cybersecurity framework to identify malicious edge device in fog computing and cloud-of-things environments. *Computers & Security*, 74, pp.340-354.

Singh, J., Pasquier, T., Bacon, J., Ko, H. and Eyers, D., 2016. Twenty Security Considerations for Cloud-Supported Internet of Things. *IEEE Internet of Things Journal*, 3(3), pp.269-284.

Jolt.richmond.edu. 2015. [online] Available at: < http://jolt.richmond.edu/v21i2/article6.pdf > [Accessed 9 December 2021].

Docs.aws.amazon.com. 2019. *What is AWS IoT? - AWS IoT Core*. [online] Available at: < https://docs.aws.amazon.com/iot/latest/developerguide/what-is-aws-iot.html > [Accessed 9 December 2021].

Sethi, P.; Sarangi, S. Internet of Things: Architectures, Protocols, and Applications. J. Electr. Comput. Eng. **2017**, 1–25.

Liyanage, M.; Braeken, A.; Kumar, P.; Ylianttila, M. IoT Security: Advances in Authentication; John Wiley & Sons: West Sussex, UK, 2020.