A Proactive Defence Framework for Internet of Things (IoT) Networks Security for Digital Health

By

Gihan Yasith Indunil Ranga Gunasekara

(BSc (Hons) in Computing and Information Systems, Master of Business Administration, MSc in Computer Science)

Thesis
Submitted to Flinders University
for the degree of

Doctor of Philosophy

College of Science and Engineering
27/09/2024

DECLARATION

I certify that this thesis does not incorporate without acknowledgment any material previously submitted for a degree or diploma in any university and that, to the best of my knowledge and belief, it does not contain any material previously published or written by another person except where due reference is made in the text.

Signed.....

Date : 27/09/2024

ACKNOWLEDGEMENTS

I am grateful to everyone who helped me in numerous ways and capacities to accomplish my PhD research.

First and foremost, I would like to express my most profound appreciation to Professor Trish Williams for being my principal supervisor and for her invaluable supervision, continuous support, and patience during my PhD studies. I would also like to thank my secondary supervisor, Professor Giselle Rampersad, for her treasured support, inspiration, and advice.

I could not have undertaken this journey without my lovely wife, Gayani. With her tremendous understanding and continuous encouragement over the past few years, it would have been impossible for me to complete my PhD studies. Also, for my kids Ranu, Dinu and Dinon, who made me stronger, better and more fulfilled than I could have ever imagined.

Words cannot express my gratitude to my parents for their unconditional love and support throughout my life. Thank you both for giving me the strength to reach for the stars and chase my dreams.

I sincerely thank Ms Ginger Mudd for her friendship, empathy, and encouragement and for helping me with academic writing.

ABSTRACT

Digital health can be described as the use of digital technologies to improve access to healthcare and care delivery and provides numerous benefits to patients and healthcare service providers. The Internet of Things (IoT) plays a significant role in these systems. IoT devices have been applied in many ways in digital health, such as implantable devices, wearable devices, activity trackers, indigestible devices and monitoring devices. IoT devices are increasingly deployed to improve individuals' health, health monitoring, healthcare and personal safety. Security of IoT networks is a challenge because of the limited computational power in IoT devices, the lack of standards for IoT device manufacturing, the evolving nature of the IoT technology and healthcare as primary targets for cybercriminals. As health-related data is sensitive, additional protective measures need to be applied. According to industry reports and literature studies, security breaches in digital health systems can be catastrophic, compromising patient safety, privacy, reputation and can have financial implications. Indeed, medical data is a target for cybercriminals due to its scientific and commercial value.

Reactive security measures deployed in Information and Communication Technology (ICT) systems have failed to reduce the time taken to identify security incidents and contain security breaches. As a result, the total cost of recovery, system downtime and legal penalties are high. This research aims to develop a framework for the Proactive Defence of IoT networks, specifically for IoT technologies used in Digital Health. Proactive Defence means creating a framework that caters to the constant evolution of security threats. The objective of being proactive is to pre-identify security risks and address them, to be in front of attacks to minimise them and to increase the level of protection of digital health systems. Being proactive increases patient safety, improves productivity, improves business continuity and minimises financial loss.

The primary research question is ‘How can a framework be developed and applied for proactive defence for IoT network security in digital health?’. A “Design Science” Research Methodology is used to investigate the problem and to develop the framework.

This research makes an important theoretical contribution. Unlike static models, this research provides a theoretical contribution to the digital health literature through an adaptable framework for the proactive defence of IoT networks.

This research offers a valuable contribution by providing a proven and adaptable framework for defending IoT networks. It enables network architects to design IoT networks with a high level of security, leading to an effective and efficient operational IoT network.
This framework also provides a valuable solution that can be used by other IoT security researchers, healthcare service providers, designers of smart technologies, IoT system implementers and those responsible for securing healthcare infrastructure.

This security framework is designed to provide end-to-end security and a multi-layer secured architecture for IoT networks in digital health systems. It's not just about protection but also about preparing for constantly evolving threats and vulnerabilities. The framework's technology-agnostic and vendor-neutral nature allows to adapt to these challenges by choosing the technologies that best suit and match the needs. It also included a detailed, step-by-step guide on applying the security framework to an IoT network, ensuring a smooth and effective implementation. This framework provides comprehensive visibility of all connected devices, including the type of devices used, where they are deployed, device connectivity, network connectivity, and technologies used in the IoT network, mapped to the IoT architecture.

TABLE OF CONTENTS

Table of Figures

Table of Tables

1. INTRODUCTION

IoT devices are increasingly deployed to improve healthcare systems as well as the health and safety of individuals. Such devices include wearables, implantable devices, monitoring systems, fall detection and vital sign monitoring. World Health Organization (WHO) describe Digital Health as "harnessing the power of digital technologies and health innovation to accelerate global attainment of health and well-being". Similarly, the Australian Institute of Health and Welfare (AIHW) defines digital health as "an umbrella term referring to a range of technologies that can be used to treat patients and collect and share a person's health information". Further, the Food & Drug Administration (FDA) – USA define digital health as "The broad scope of digital health includes categories such as mobile health (mHealth), health information technology (IT), wearable devices, telehealth and telemedicine, and personalized medicine".

Security failures of IoT technology used in digital health can be catastrophic because they are used for healthcare purposes. For instance, unauthorised access to confidential data and compromised IoT devices can pose risks to the associated networks, information systems and ultimately patient care. Additionally, denial-of-service attacks can make essential network services and resources unavailable temporarily or indefinitely. Whether innovative or adapted from existing approaches, new methods to secure IoT devices are crucial and demand the design of secure IoT networks in digital health systems.

1.1. Background

It is important to visualise the enormity of IoT growth compared with the growing cyber security issues impacting healthcare. The global IoT market was worth US $151 billion in 2018 and is expected to grow to US $1567 billion by 2025 (Lueth, 2018). The Internet of Medical Things (IoMT) market shows similar growth. It was valued at US $44.5 billion in 2018 and is predicted to grow to US $254.2 billion by 2026 (Global Internet of Medical Things (IoMT) Market, 2020). In addition, the number of devices was 8.0 billion in 2018 and is predicted to grow to 30.9 billion by 2025 (Lueth, 2020). The number of IoT platforms has risen from 260 in 2015 to 620 in 2019 (Lueth, 2019, Liu, 2021). These statistics show that the growth of IoT is

significant. Concerningly forecasts indicate that over 25% of known attacks will involve IoT by 2020 (Leading the IoT, 2017). Even though technological measures have been widely implemented in information and communication technology systems, securing healthcare data is an ongoing challenge. Data breaches continue to occur, and the incidents are growing rapidly. The PROTENUS "Breach Barometer" report shows that the number of affected patient records is increasing exponentially (Protenus, 2020). Table 1 summarises healthcare disclosed incidents and breached patient records from 2016 to 2021 (2021 Breach Barometer | Protenus, 2022).

Table 1 – Healthcare disclosed incidents and breached patient records summary

Year	Breaches reported	Patients' records affected
2016	450	27,314,647
2017	477	5,579,438
2018	503	15,085,302
2019	572	41,404,022
2020	758	40,735,428
2021	905	50,406,838 (only for 700 incidents)

Table 1 shows that the number of patient records affected by security incidents tripled from 2017 to 2018 and from 2018 to 2019. As the number of affected records grows, the cost associated with the breaches also increases. Figure 1 shows the average cost of significant breaches comparing 2020 to 2022 measured in US$ millions (IBM Security - Cost of a Data Breach Report, 2022).

Figure 1 – Average cost of mega breaches (IBM Security - Cost of a Data Breach Report, 2022)

Further (IBM Security - Cost of a Data Breach Report, 2022) indicates that the average healthcare data breach cost is approximately US$ 10.10 million, the highest compared to other industries.

1.1.1. Data Breaches

The data breach life cycle is defined as the time between the first detection of a breach and its containment. Calculating the time expected to identify a breach and the time to contain it is crucial. Containing means resolving the breach and restoring the system to normal. The longer the breach cycle time, the greater the damage and the higher the costs. According to the (IBM Security - Cost of a Data Breach Report, 2020,), the average data breach life cycle was 280 days in 2020.

Figure 2 shows the average days to identify and contain an incident during 2015 – 2020 in all industries.

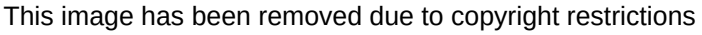


Figure 2 - Days to identify and contain an incident during 2017 - 2023 in General (IBM Security - Cost of a Data Breach Report, 2023).

Figure 2 shows that the number of days increased from 2017 to 2021. Figure 3 shows the days to identify and contain an incident during 2015 – 2020 according to industry. Figure 3 shows the healthcare industry's average data breach life cycle is 329 days, taking 236 days for detection and 93 days for containment. The report also highlights US $1.12 million in savings if a breach can be contained in less than 200 days. Moreover, federal laws mandate that patients be informed within 60 days of any patient related data breach (McLeod & Dolezel, 2018). It is a massive challenge for healthcare organisations to meet the legal requirements as the breach life cycle is far greater than the notice period provided by the law. In addition to the financial losses, these breaches reduce patient safety and cause a loss of reputation.

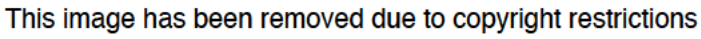


Figure 3 - Days to identify and contain an incident during 2020 based on the industry (IBM Security - Cost of a Data Breach Report, 2020).

In conclusion, the global IoT market is growing. IoT devices are getting added, and the number of IoT platforms is rising. Similarly, the growth of cyber security incidents and breaches are increasing. Additionally, the cost involved in data breaches and recovery is significant. Since 2020, data breach costs in the healthcare industry have increased by 53.3% and, for the 13th year in a row, have been reported as the most expensive data breach, which averages US $ 10.93 million (IBM Security - Cost of a Data Breach Report, 2023).

Moreover, cyber security incidents and breaches lead to high legal requirements, reduce patient safety, and cause a loss of reputation. Even though technological measures have been widely implemented in information and communication technology systems, securing healthcare systems is an ongoing challenge. Therefore, a strategy that can protect these systems in a proactive rather than reactive manner is needed.

1.1.2. Digital Health Systems

There are increasing demands for the healthcare industry to be more innovative in its delivery of healthcare services in a timely, patient-centred, pervasive and affordable manner. To meet these demands, the healthcare industry is adopting more digital technologies (Jayaraman et al., 2020). The Australian Institute of Health and Welfare (AIHW) defines Digital Health as an umbrella term for applying emerging technologies: Internet of Things (IoT), Artificial Intelligence, Big data, Data Analytics, Cloud, Fog and Edge Computing and their capabilities in advancing effective and flexible healthcare systems. Within such emerging technologies, IoT can support many areas in digital health, including real-time remote monitoring, chronic disease management using wearable and implantable devices, remote care, remote diagnosis, smart elder care facilities and health and fitness programmes to help the seamless information collection, transmission and sharing across multiple platforms in healthcare systems (Janjua et al., 2009; Volk et al., 2015).

1.1.3. Increasing Importance of Digital Health Systems

Information technologies are increasingly applied to minimise human errors, reduce medical treatment errors, reduce administration inefficiencies and improve clinical outcomes (Alotaibi & Federico, 2017). Where traditional healthcare practices are not viable, as was the case during the COVID-19 pandemic, the presence of digital health enables continuous patient care. Digital health as a component of an integrated solution also provides quality and comprehensive healthcare in rural and remote areas with workforce shortages, poor transportation facilities and geographical isolation. IoT is increasingly used to transform healthcare to digital health and address these challenges (Hermes et al., 2020). Yet, it needs a high level of security and assurance that patient data is protected.

1.2. Research aim

Forecasts indicate that IoT will involve more than 25% of the known attacks. Further, IoT will increase the attack surface as the devices are always connected to the internet. The existing evidence shows that the healthcare industry's average data breach life cycle is 329 days, taking 236 days for detection and 93 days for containment, which is almost closer to a calendar year to recover from a breach. Therefore, maximum protection is needed in IoT

networks proactively rather than reactively to minimise the potential loss, damage, or destruction it can cause to digital health systems.

This research aims to develop a framework for the Proactive Defence of an IoT network, specifically for using IoT technologies in Digital Health. Proactive defence means a framework that caters for the constant evolution of security threats.

The use of IoT based healthcare methods has the potential to improve the quality of a patient's life by using biosensors, wearable devices and other medical devices to collect and combine data about vital signs, remote health monitoring, elderly care, chronic diseases, health and fitness programmes and the effectiveness and efficiency of the treatments and tests (da Costa et al., 2018; Nogueira & Carnaz, 2016). As IoT devices are increasingly deployed to improve individuals' health, health monitoring, healthcare and personal safety, security failures of IoT technology can be catastrophic. For instance, unauthorised access to confidential data, compromised IoT devices posing risks to the associated networks and denial of service attacks can make essential network services and resources unavailable temporarily or indefinitely. Whether innovative or adapted from existing approaches, a comprehensive method to secure IoT devices is critical to designing a secure IoT Network.

1.3. Research questions

How can a framework be developed and applied for proactive defence for IoT network security in digital health?

1.4. The proposed framework

Nelson (1994) elaborates that "framework helps developers provide solutions for problem domains and better maintain those solutions". It provides a well-designed and thought-out infrastructure so that when new pieces are created, they can be substituted with minimal impact on the other pieces in the framework. The framework in this research aims to provide a set of methods and techniques that can be applied to a secure IoT network for digital health. As patients' lives must not be put at risk at any time, it is the responsibility of all healthcare service providers and care professionals to understand the security of digital health systems and to safeguard such systems from cybercriminals. In this context, this research study is

focused on developing a security framework for IoT networks in Digital Health systems that will function proactively.

1.5. Research Methodology

This research aims to develop a proactive defence framework that caters for the constant evaluation and evolution of security concerns and threats. Identifying framework elements to address contemporary IoT security concerns in digital health systems is broad and complex. Defending IoT security proactively is challenging. This research is part of the Information System research domain as the development of such framework involves an in-depth analysis of literature and industry publications, the development of new insights, assessment of current security systems, identification of improvements and new areas to develop and contribute to the body of knowledge. The study will investigate the contemporary security postures of digital health systems built upon IoT networks, security solutions, failures and proactive defence mechanisms. Proactive defence means a framework that caters for the constant evolution of security threats. It is essential to use an appropriate methodology to support constructing artifacts for a result oriented and technological solution to the research problem. Design Science Research Methodology is used as the research approach. As proposed (Peffers et al., 2007a), the Design Science (DS) methodology can be used to construct and present superior Design Science Research in information systems. The underlying elements of Design Science Research are conceptual principles, practice rules, and processes that bring out the meaning of the research, how the research is conducted, and how the research findings can be presented in a systematic manner (Peffers et al., 2007a). Further (Hevner, 2007) , highlights that the DS methodology is a problem-solving and solution-oriented process. The research design and methodology are discussed in detail in Chapter 3 - Methodology.

1.6. Significance of the research

Proactive defence aims to minimise cyber security incidents and breaches. This research applies a proactive strategy, rather than a reactive one, to be in front of attacks and minimise potential loss, damage, destruction, or impact from cyber security incidents. Pre-identifying and addressing security risks limit the opportunity for hackers to get into a network and detect and take early actions when an incident happens.

The digital healthcare space is critical and complex because multiple systems are integrated and interconnected to deliver the required services and care. According to the Australian Institute of Health and Welfare (AIHW), these systems include mobile health and health applications, electronic prescribing, electronic health records, telemedicine, telehealth, wearable devices, robotics and artificial intelligence. These systems produce a vast amount of sensitive data that has personal, clinical, scientific, financial, and commercial value (Yeng et al., 2021). Hence, these digital systems are associated with security and privacy risks as cyber hackers and criminals target these systems due to the demand for personally identifiable data of individuals such as name, address, contact numbers, social security numbers, medicare numbers and driver's license details on the dark web, long-term value of knowing medical conditions and treatment histories of individuals and weak defences. Other motivations include political gain and impact on patients' lives in cyber warfare (Coventry & Branley, 2018). According to a report published by the Federal Bureau of Investigations (FBI Cyber Division, 2014), cybercriminals sell partial medical information for approximately $US50. In contrast, a stolen social security number is only worth US $1. Once a social security number or a credit card is stolen, the card can be cancelled, or the relevant authorities can be notified, and necessary actions can be taken within a short period, but healthcare data theft lacks standard remediation procedures (Ibrahim et al., 2016). Further, stolen credentials are used to access health services, prescribed medicines and insurance claims (Coventry & Branley, 2018). The healthcare industry was top on the list for the last thirteen years (2010 - 2023) compared to other industries, averaging US $ 10.93 million for a data breach (IBM Security - Cost of a Data Breach Report, 2023).

The significance of the research is discussed from two perspectives: general and specific benefits. To elaborate on the benefits, the following sub-sections are structured to identify

who it will impact and benefit, how better theoretical models can be built using the research findings, and how the research findings can contribute to research gaps. Figure 4 illustrates the significance of the research on various levels which will be discussed further in the following sections:

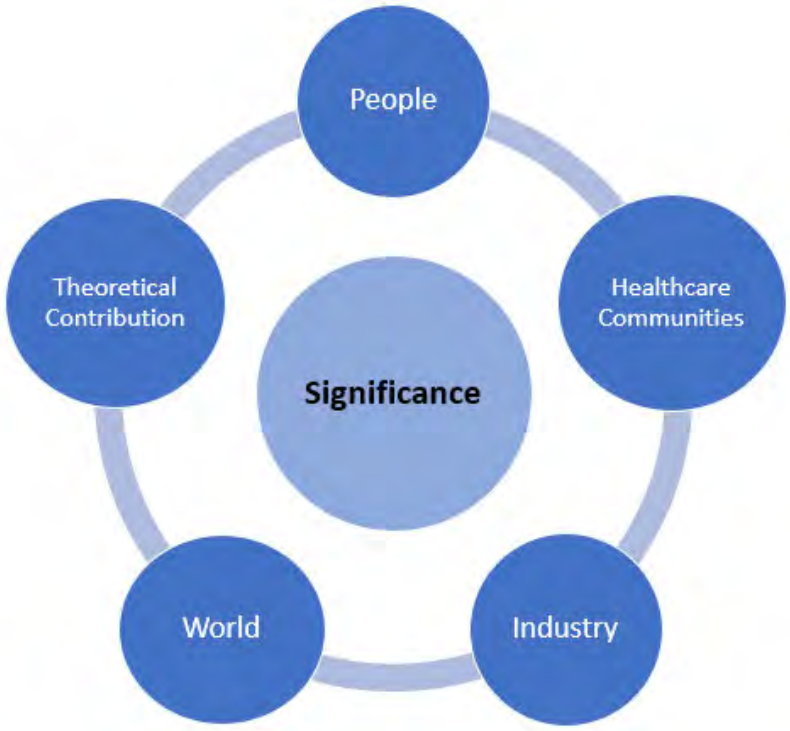


Figure 4 - Significance of this research on various levels

People

Through this research, securing healthcare IoT networks will provide people with safer access to healthcare. When medical data is safe and secure, it provides accurate monitoring of individual health conditions through bodily sensors such as glucose and heart rate monitors. Timely access to reliable data, such as insulin delivery or vital-sign emergency alerts, is essential for automation and leads to better healthcare, ensuring the safety of people's lives. Fundamentally, this means less money is diverted to recovering from security breaches and spent as intended on staff, equipment, research and improving healthcare. The benefits of securing healthcare IoT networks are better healthcare outcomes and increased trust in digital health systems.

Healthcare Communities (Hospitals, Clinics, Healthcare Service Providers)

This security framework supports healthcare communities by preventing unauthorised access, tampering, or denial of access, thus protecting information, data, and ICT systems and ensuring the highest levels of confidentiality, availability and integrity. Ultimately, this enables the healthcare communities to provide accurate, timely and better patient care. Poor security postures increase the risk of cyber incidents and breaches. Adopting this security framework improves the security posture, strengthening the defence against known and unknown potential threats; it limits the opportunities for hackers, preventing breaches.

Preventing security breaches eliminates the high costs of investigations, containment, recovery, and legal liabilities. Ultimately, it prevents the diversion of money away from the capacity to provide and improve quality healthcare. This capacity includes infrastructure, human resources, ambulance services, and research. This is especially important in communities that rely on public funding. In addition to the direct costs of a security breach, the loss of reputation is hard to measure in terms of people's trust and confidence in healthcare.

World

The healthcare industry in low and middle-income (LMIC) countries are challenged by financing in general, not only in cyber security. This security framework is built using existing resources and available current technologies. None of the security elements in this framework use proprietary or specific technology. The framework was developed in a vendor-neutral and technology-agnostic manner. Therefore, it can assist LMIC countries in implementing cost-effective cyber security for their IoT networks in digital health systems.

Industry

The industry demands innovative and results-oriented solutions for security issues. While this security framework is developed focusing on IoT networks in digital health systems, it could be applied to other IoT industries as the framework's implementation is based on the selected architecture and not on any specific technology, platform, or commercial product. The

framework is built upon the nature of IoT devices and considers the security concerns of the related architecture, platforms, networks, and communication. Following the implementation phases, this framework can be applied to any other industry.

Theoretical Contribution

The study makes an important theoretical contribution by providing a proactive, comprehensive security framework to provide end-to-end security for IoT networks in digital health systems. This framework caters to the constant evolution of security issues and prevents the rise of actual incidents. Unlike the security approaches that are reactive, this study is ~~critical~~ significant as it uses a proactive approach of pre-identifying security risks and addressing them before they can become incidents, being in front of attacks to minimise them, and increasing the level of protection of digital health systems.

One of the main objectives of this research is to use existing resources and current technologies to develop a security framework rather than spending time and money on developing novel components. As this artifact was developed as a framework rather than a model, any modifications, including adding new elements or excluding existing elements, can be accommodated to meet future requirements without changing the original research objectives.

Key Contributions to developing the framework

The key contributions in developing the security framework across various areas. The key areas,

- Understanding the criticality and complexity of the digital healthcare space, as multiple systems are integrated and interconnected to deliver the required services and care.

- Implementing a proactive security solution to an IoT network is not just a task, it's a necessity. It requires a thorough understanding of the IoT ecosystem: IoT devices, how they are interconnected, network media used, software and hardware components and technology used in the network, and end-to-end data flow.

- A comprehensive approach was taken to identify the security elements of the framework. Elements were identified through the scoping review, analysis of the academic literature and analysis of grey literature and industry security reports. This thorough research provided a deep understanding of the security posture of IoT-based digital health systems, the current and constantly evolving security landscape, security incidents and breaches, trends of threats and vulnerabilities, the common attack surfaces, security challenges and the present cyber security situation.

- During the application and implementation phase, a conceptual view of the security elements, the relationship between each element, and a proper step-by-step guide with a six-phase framework implementation process was presented.

- This research covered end-to-end comprehensive security coverage to be proactive in many dimensions: identifying relevant threats and mapping them to IoT networks, secure communication between layers, data security, continuous monitoring, digital forensics, and information sharing. Ultimately, it provided a layered security approach for maximum protection.

1.7. Study Limitations

The potential limitations of this research are categorised into the scope and method limitations.

Scoping limitations

Using a case study is not representative of the security posture in all instances. Data collection involves highly confidential and sensitive security information, so disclosing such information may be limited. This may impact analysis by not capturing the whole image of a digital health system. Due to the evolving nature of security threats and technology, the final framework may include outdated technologies. However, the security framework was developed to accommodate this, and it is technology-agnostic and vendor-neutral. Before completing the final thesis, review the content for any technology changes that will be undertaken.

Methodological limitations

The success of the artifacts produced from the research will depend on the evaluation. The evaluation tests the artifacts in different contexts iteratively (Peffers et al., 2018). This research uses expert reviews and interviews to evaluate the artifacts and a desk study to demonstrate the implementation. Therefore, this study may be limited to a specific context, such as the knowledge of the experts, simulation model, or selected case study.

1.8. Summary

Security failures of IoT technology used in digital health can be catastrophic because it is used for healthcare purposes. For instance, unauthorised access to confidential data and compromised IoT devices can pose risks to the associated networks, information systems, and patient care. Additionally, denial-of-service attacks can temporarily or indefinitely make essential network services and resources unavailable. Whether innovative or adapted from existing approaches, new methods to secure IoT devices are crucial and demand the design of secure IoT networks in digital health systems

The technology landscape is evolving. One of the objectives of this security framework is to be flexible and agile in responding to technological changes, such as changes in IoT platforms, operating systems, communication technology (Wi-Fi, Bluetooth, Zigbee), different platforms, and vendors. None of the security elements use any proprietary or specific technology in this security framework. The framework was developed in a way that is vendor—and technology-neutral. Therefore, the framework can respond to any technological changes as it is not tied to a single technology, is cost-saving and is easier to integrate.

Data security, with a strong emphasis on data privacy, is not just a priority but a necessity for the digital healthcare industry. It is a fundamental requirement that cannot be overlooked. The main objective of data security is to preserve confidentiality, integrity, and availability. These were significant priorities during the framework's construction. Specifically, to achieve this purpose, security elements, access control, data security, and Information Security Policies & Standards were included in the framework. Access control plays a vital role in IoT networks by implementing identification, authentication, authorisation, and accountability for devices and limiting network access and communication only to legitimate entities. Implementing access control mechanisms and proper authentication processes for users and

objects can eliminate unauthorised access. The "Capability-based Access Control" proposed in this research addresses the device identification, authentication, and authorisation requirements. Data security is considered during transmission and output to preserve confidentiality, integrity, and availability. The main information security pillars, confidentiality, integrity, and availability, have been ensured by positioning security elements in each IoT architectural layer.

This research aimed to develop a framework for the Proactive Defence of an IoT network, specifically for using IoT Technologies in Digital Health. Proactive defence is a framework that caters to the constant evolution of security issues and prevents the rise of actual incidents. The objective of being proactive is to pre-identify security risks and address them, be in front of attacks to minimise them and increase the level of protection of digital health systems. Being proactive increases patient safety, improves productivity, improves business continuity and minimises financial loss.

Structure of the Thesis

This PhD thesis consists of eight chapters. A brief outline is given for each chapter below.

Chapter 1 – Introduction to the Research

This chapter explains the IoT network in digital health, including the IoT architecture, infrastructure, technology, and system operation. It also presents the background of the study, the research aims, the research questions, the significance of the study, and the study limitations, including scoping and methodological limitations. This chapter provides the rationale for conducting this research.

Chapter 2 - Literature Review

The literature review provides the background to the inherent security issues in using IoT. Current overarching security measures are discussed. Also, this includes a scoping review of existing security models to critique the target of these models and to identify where proactive defence measures are included. A review of framework development methods is also presented. The literature review concludes by identifying the gap in research on IoT defensive security measures and presents the research aim and questions to be answered. This chapter provides the context for this research.

Chapter 3 – Methodology

This chapter describes the research design paradigms and methods. It also discusses the use of Design Science Research (DSR) in Information Systems (IS) and the application of Design Science Research Methodology (DSRM) to this research. Further, the research design aligns with the Design Science Research Process Model, and its suitability is presented.

Chapter 4 - Design and Development

This chapter presents an overview of the proposed security framework. The chapter explains each security element's rationale and relationship within the framework. Further, this chapter presents a conceptual view of the proposed security framework. Also, this chapter presents the application and implementation of the proposed security framework.

Chapter 5 – Demonstration of the Framework

This chapter demonstrates the framework for the selected context, a "Remote Health Monitoring System." The demonstration was carried out as a desk study, and working examples were provided. Further, challenges faced during the demonstration were discussed.

Chapter 6 – Evaluation

This chapter describes the evaluation process of the proposed security framework using expert interviews. The evaluation process is discussed in detail, and results from a thematic analysis are presented.

Chapter 7 – Discussion

The Discussion chapter presents a discussion of the proposed security framework, which encompasses nine security elements accompanied by detailed descriptions, purposes, and outputs, all of which are designed to address the research questions and gaps identified in the literature. . Furthermore, the discussion chapter includes the intellectual knowledge gained by the researcher, lessons learned, and future directions for this research.

Chapter 8 – Conclusion

The conclusion chapter highlights the research's background, problem, questions, and key characteristics. It also presents evidence of how the research questions have been answered and outlines the key findings. Finally, the chapter provides the conclusion of this research.

2. LITERATURE REVIEW

This literature review provides the background to the Internet of Things (IoT), including the evolution of IoT architecture. IoT common concepts, key terms, and overarching security measures are presented. Also, this chapter describes the initial framework using literature. The term “Framework“, the main artifact type developed in this research, is also explained in detail. The difference between the terms “framework” and “model” is described using academic literature, as these terms are frequently used in research publications interchangeably. Further, the chapter includes a scoping review of existing security models with an extensive analysis to critique the target of these models and to identify where proactive defence measures are already in existence. In response to the thesis examiners' comments, an additional section is added to present in the scoping review additional research papers from the period 2021 to 2024. The initial scoping review covered the period from 2015 to 2020.

A review of framework development methods is also presented. The literature review concludes by identifying the gap in research on IoT defensive security measures and presents the research aim and research questions to be answered.

2.1 Internet of Things (IoT)

Physical objects connected to the Internet to control and communicate are known as the Internet of Things (IoT) (Ray, 2016). Objects are getting connected to the Internet at a rapid pace. These objects range from simple temperature readers to medical-grade sensors, artificial intelligence-driven robots, autonomous cars, and highly classified military sensors. These devices fall into three categories: Consumer, Enterprise, and Industrial (Harsha et al., 2019) (Higginbotham, 2019). With the intensive growth of the IoT and IoT networks embedded with smart technologies, people are attracted to the adoption of such intelligent technologies in their lives without paying much attention to the security aspects. For example, robot vacuum cleaners, smart bulbs, smart heaters, air conditioners, watches, fitness equipment, health monitors, and microwaves. Cyber attackers are cleverer than ever before. They study the target environments more carefully than the manufacturers to identify

weaknesses or loopholes, seeking opportunities to launch an attack. A simple weakness is an opportunity for an attacker to launch an attack in a matter of seconds or minutes.

Deploying IoT without proper security measures may create huge risks to the network. It creates an avenue for attackers to exploit weaknesses, resulting in disaster, such as a complete loss of a business. Most IoT devices are built for a specific purpose with much less memory and computational power (Chattopadhyay et al., 2019; Kouicem et al., 2018). This poses a challenge to secure IoT devices and IoT networks.

2.1.1 Evolution of the IoT Architecture

There is scant coverage in the literature about a standard architecture for IoT. There are many factors to consider: scalability, performance, security, interoperability, and how the devices are connected to the internet. IoT architecture depends on the domain: wireless sensor networks (WSN), healthcare, cloud services and smart cities (Ray, 2018). Researchers have proposed different architectures including three-level architecture, five-level architecture, cloud and fog-based architecture, social IoT architecture, and machine-to-machine (M2M) architecture (Sethi & R. Sarangi, 2017). The three-layer architecture is considered the basic architecture (Ammar et al., 2018; Wu et al., 2010). It consists of 3 layers: the perception, network, and application layers. The perception layer identifies the objects and senses, gathers information, and sends the gathered information to the next layer (Patel et al., 2016). The network layer transmits and processes information. The application layer delivers application-specific services to the user, including vital sign monitoring and environmental sensing (Sethi & Sarangi, 2017). Five-level Architecture consists of five layers: (1) perception, (2) transport, (3) process, (4) application and (5) business. Sensor data is captured by the perception layer and transmitted to the process layer by the transport layer. Storing, analysing and processing data is done in the processing layer. Management of all applications, business models and profit models is done by the business layer (Sethi & Sarangi, 2017) (Wu et al., 2010).

Cloud and Fog-based Architecture – as (Sethi & Sarangi, 2017) describe, in cloud architecture, the top level is allocated to applications, the middle level is for cloud services: infrastructure, platform, and software, and the bottom level is for the network of smart things. Fog

architecture is considered an extended version of cloud architecture (Bonomi et al., 2014). Social IoT Architecture – The social relationship: “parent object relationship”, “co-location object relationship” and “co-work object relationship” of the objects is taken into consideration and the architecture is based on a server-side and an object side (Atzori et al., 2011). Social relationships have analogies with how humans form social relationships according to work, workplace, and living area. The server side has three layers: the base layer, component layer and application layer, while the object layer has two layers: the object layer and object abstraction layer (Sethi & Sarangi, 2017).

2.1.2 Common concepts of IoT and associated key terms

This section discusses common concepts of IoT and associated key terms. Knowing these key concepts and terms helps to understand the broader picture of the IoT space.

IoT Devices

IoT devices include sensors, actuators, appliances, gadgets, medical implantable devices and machines that can connect to networks and the internet (Chattopadhyay et al., 2019) (Sethi & Sarangi, 2017). These can be a simple environmental sensor to gauge temperature, a medical implantable sensor to measure the blood glucose level of a patient, or a military-grade device such as an inertial navigation system (INS) fitted to missiles and submarines.

IoT Data

The IoT data refers to any data collected by IoT devices (Arya & Gore, 2020). As an example, simple environmental sensor to gauge temperature reading from a room, medical implantable sensor to measure the blood glucose level of a patient and feed the data to the monitoring device.

IoT Network

A collection of interconnected IoT devices, such as sensors, actuators and machines, that communicate using wired or wireless communication channels (Tahir et al., 2020). For instance, Radio Frequency Identification (RFID), Cellular, Local Area Networks (LAN), Personal

Area Networks (PAN), Body Area Networks (BAN), Low Power Wide Area Networks (LPWAN), and Mesh Networks.

IoT Platform

An IoT platform is the central backbone of the IoT infrastructure where multi-layer technology facilitates provisioning, managing and automating the connected devices (Fahmideh & Zowghi, 2020).

IoT Communication

The communication of IoT includes person-to-person (P2P), machine-to-machine (M2M) and machine-to-person (M2P) (Bradley et al., 2015).

IoT Capabilities

The healthcare industry is adopting the latest technologies to provide optimal care and to deliver the best services. Innovative solutions will maintain and improve healthcare system efficiencies. The capabilities of IoT, such as monitoring, controlling, optimising, and automating, can be applied to healthcare services to achieve these innovations (Porter & Heppelmann, 2014).

2.2 What type of security has been implemented to protect IoT networks?

As the threat landscape evolves, security solutions must adapt. Applying a single security solution is not appropriate and is not sufficient.

The distributed, fragmented, and always-connected nature of IoT networks presents a larger attack surface than traditional networks. This means that there are more potential points of entry for cyber threats, making IoT networks more vulnerable to attacks. (Islam & Aktheruzzaman, 2020). In a basic three-layer architecture, attacks on IoT networks can be expected at different layers: perception, network, or application. The following are some examples of attacks that can take place in each layer.

- Perception layer – Unauthorised access, Eavesdropping, Radiofrequency jamming, Spoofing attacks.
- Network Layer: Denial of Service Attacks (DoS), Distributed Denial of Service attacks (DDoS), Sniffing attacks, Replay attacks, and Man-in-the-middle attacks.
- Application layer – Code injection attacks, Buffer overflow attacks, Phishing attacks, SQL injection attacks,

More than one security solution must be implemented in multiple layers to provide the highest level of security. For instance, a combination of firewalls, intrusion detection systems, and encryption can be used. These security solutions must identify and model threats and vulnerabilities in advance, enforce access control and apply data security. In addition, monitoring network traffic for intrusions, digital forensic investigations, sharing security information, and information security policies need to be embedded to make a comprehensive solution that provides end-to-end security.

At present, most of the security strategies implemented to safeguard IoT networks can be categorised as reactive approaches. A reactive approach pertains to dealing with something that has already occurred. Most of the security solutions that are deployed in IoT networks are software firewalls, hardware firewalls, virus guard solutions, Intrusion Detection Systems (IDS), Intrusion Prevention systems (IPS), Software-defined networks (SDN), Moving Target Defence (MTD), Network monitoring systems using Artificial Intelligence. This section covers a general description of these security solutions, their failings and benefits.

2.2.1 Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS)

IDS and IPS are security technologies that are used to protect networks. IDS detects unauthorised access to a system or network (Santos et al., 2018). An IDS structure consists of three modules: a data gathering module to collect data, an analysing module to analyse collected data, and a reporting module to make alerts (Asharf et al., 2020). The data-gathering module collects data and passes it to the analysing module. If the analysing module detects any suspicious or unauthorised activity after processing the collected data, the reporting module will produce alerts (Zarpelão et al., 2017). There are two types of IDS based on their operation: Host-based intrusion detection systems (HIDS) and Network-based intrusion detection systems (NIDS). The host-based systems identify the attacks on the device they have been installed on (Gyamfi and Jurcut, 2022), and the network-based systems monitor

the network traffic to detect any malicious activities. A comparison of the NIDS and HIDS is presented in Table 2.

Table 2 – Comparison of the NIDS and HIDS (Gyamfi & Jurcut, 2022).

	Host-based IDS	**Network-based IDS**
Data source	System call logs, running processes, file system changes, application logs	Network traffic
Detection rate	The detection rate is low and less capable of detecting new attacks	The detection rate is high, capable of detecting new attacks
Threats traceability	Based on the system call	Network addresses, time stamps,
Limits	Rules created can be obsolete, depending on the operating system, and unable to detect network attacks.	Monitor only network traffic within subnets.

Further, IDS are classified according to their placement strategies and detection methods. There are three main placement strategies: “Centralised”, “Distributed”, and “Hybrid” and three detection methods: “Signature-based”, “Anomaly-based”, and “Specification-based”. The Centralised placement strategy refers to placing the IDS in a central location where the incoming and outgoing network traffic can be monitored for intrusions (Gyamfi & Jurcut, 2022), E.g., a Border Router (BR) or a dedicated device. The distributed strategy places the IDS in the network's IoT devices; therefore, the selected IDS must be lightweight (Gyamfi & Jurcut, 2022). The Hybrid placement strategy uses a mix of centralised and distributed approaches.

The detection methods are described as follows;

- Signature-based approach – Known signatures are stored in a database. When an attack is matched with a signature, the system generates alarms. This approach can detect known threats only. It is accurate and effective for known threats (Santos et al., 2018).

- Anomaly-based approach – Compares the system activities in a given time with normal behaviour. If the comparison exceeds the pre-defined threshold values, then an alert is produced. It is efficient in detection. However, anything that fails to match the expected behaviour is detected as an intrusion. Therefore, this approach usually results in a high rate of false positives (Santos et al., 2018). Statistical and machine learning techniques are used to create normal behaviour profiles (Santos et al., 2018). For easy detection, anomalies can be further classified into three categories (Chandola et al., 2009).
    - Point anomalies – Data instance differs from the usual pattern.
    - Contextual anomalies – when the data instance behaves anomalously in a given context.
    - Collective anomalies – Similar data instances behave anomalously.
- Specification-based approach – A set of rules and thresholds for network components defines the expected behaviour. For example: - routing tables, protocols, and nodes. This method is capable of identifying any deviations from normal behaviour. A human defines rules and thresholds; therefore, the false positives are minimal (Santos et al., 2018).

Manual specifications result in low false positives compared to machine-defined specifications. Placement strategies and detection methods of IDS are explicitly designed for IoT networks (Zarpelão et al., 2017). The taxonomy used to classify the IDS is based on the attributes: “detection method”, “placement strategy”, and “security threat” (Zarpelão et al., 2017). Once intrusions are detected, preventive actions need to be taken. As manual actions may take longer, the need for automated actions arose due to the limited time available for defenders. This is where the Intrusion Prevention Systems (IPS) were introduced (Fuchsberger, 2005). IPS work actively and can control the intrusion activity or limit the propagation to minimise the damage. IPS is capable of responding to denial-of-service attacks, network worms, and port scanning.

IPS are classified into three categories: rate-based, signature-based and anomaly-based. Rate-based systems focus on network traffic load and analyse the packets. Corrective actions are taken if anything is beyond the threshold values, including blocking or mediating traffic

(Fuchsberger, 2005). Signature and anomaly-based classification are identical to the IDS's signature and anomaly classification. IDS and IPS can be deployed as standalone or combined solutions (Fuchsberger, 2005).

However, applying traditional IDPS is not straightforward to IoT networks due to resource constraint nature and is a challenge (Santos et al., 2018; Zarpelão et al., 2017). According to Table 1, implementing a network-based intrusion detection system has benefits such as placement strategy, detection rate and limitations over the host-based. This research seeks to find applicable network-based IDPS for IoT networks. Further, this type of protection needs to be deployed in IoT networks to detect any intrusion or suspicious activities. Failure to implement IDS will lead to intrusions undetected in the network. Failure to implement IPS will lead to intrusion detected but not actioned to prevent it. Once detected and actioned, this supports the start of a digital forensic investigation for the security incident. Such digital forensic investigation results can feed the next element, "Information Sharing". Further, this information feeds into "Threat intelligence". These feeds support keeping threat intelligence sources up to date. Up-to-date threat intelligence sources are essential during the "Threat landscaping" and "Threat Modelling". Moreover, newly generated IDPS data sets can be used to create new data sets to train new AI-driven models.

2.2.2 Access Control (AC)

Access control in ICT networks can be referred to as preserving the CIA triage: Confidentiality, Integrity, and Availability using identification, authentication, authorisation and accountability mechanisms (Ouaddah et al., 2017; Samarati & de Vimercati, 2001; Whitman & Mattord, 2022). Further, access control ensures secure access to users, devices, applications, and services (Ragothaman et al., 2023). The development process for an AC consists of three components: Security policy, Security model, and Security mechanism (Samarati & de Vimercati, 2001). There are many access control models discussed in the literature. A comparison of each model is shown in Table 3.

Table 3 – Details of AC methods with Pros and Cons

AC Model	Details	Pros	Cons
Discretionary access control (DAC)	A primary access control technique uses an access control matrix or an access control list (Ragothaman et al., 2023). Based on the identity, rules are to allow or not allow access and are always coupled with an administrative policy (Samarati & de Vimercati, 2001).	Once access is granted, it remains permanent until administrators revoke access.	DAC is a static model unsuitable for dynamic environments such as IoT (Ragothaman et al., 2023). Prone to vulnerabilities that bypass the access control system using "Trojan horse" embedded malicious programs (Samarati & de Vimercati, 2001).
Mandatory access control (MAC)	An identity-based access control method (Ravidas et al., 2019). A central authority mandates the regulations for access control (Samarati & de Vimercati, 2001).	Only the administrator can modify the security labels of objects and highly suitable military applications (Andaloussi et al., 2020).	Difficult to maintain and expensive to implement (Andaloussi et al., 2020).
Role-based access control (RBAC)	Based on the users' role in the system, access is granted (Samarati & de Vimercati, 2001).	Suits highly centralised systems (Pal et al., 2020).	Not suitable for distributed or highly dynamic systems (Pal et al., 2020).
Organization-based access control (OrBAC)	This is an extension to the RBAC. Adding "Organization" as a dimension.	Suits where multiple organisations play a role or single organisations with many subdivisions (Ragothaman et al., 2023).	Not suited for dynamic and heterogeneous environments like IoT (Ragothaman et al., 2023).
Attribute-based access control (ABAC)	Access control decisions are based on the attributes.	Provides significant flexibility to make access control decisions as this is based on the attributes and supports the scalability aspect of IoT (Pal et al., 2020). Suits large-scale projects. Eg – smart grids (Ragothaman et al., 2023).	High in complexity due to the centralised architecture (Ragothaman et al., 2023). Does not support systematic management of policies (Pal et al., 2020).

Usage control access control (UCON)	A framework to protect digital resources consists of three main concepts: authorisation, obligation and condition (Ragothaman et al., 2023).	Provides high dynamicity, and continuous access monitoring and can revoke the access when required (Ragothaman et al., 2023).	Follows a centralised architecture (Ragothaman et al., 2023).
Capability-based access control (CapBAC)	CapBAC logic is embedded into the device. Therefore, devices are capable of doing authorisation and executing decisions. (Samarati & de Vimercati, 2001)	It supports the distributed nature and resource-constraint nature of IoT (Pal et al., 2020).	Does not support systematic management of policies and establishing trust is a challenge (Pal et al., 2020).
Relationship-based Access Control (ReBAC)	Granting permission is based on the relationship between entities. E.g., user to device, device to device, and user to user (Ragothaman et al., 2023).	Support dynamic environments.	Fairly new.
Blockchain-based access control (emerging)	A distributed ledger technology. An emerging decentralised security technology to support security and privacy issues (Mohanta et al., 2021).	Suits distributed nature and aspect of delegation (Muthusamy Ragothaman & Wang, 2021).	New to IoT and still needs to mature (Muthusamy Ragothaman & Wang, 2021).

IoT devices are diverse. There are a multiplicity of makes, models, and network mediums used for connecting and communication and built with limited resources: less computational power, low power, limited built-in memory, legacy operating systems running on devices, no built-in security features, difficulties in updating or upgrading the software (Hossain et al., 2015). Due to the limitations of resources in IoT devices, applying traditional access control models to IoT networks is a challenge (Ouaddah et al., 2017). Further, due to the heterogeneous and diverse nature of IoT devices' hardware and software configuration, designing and implementing access control is very complicated (Ragothaman et al., 2023) As identified in Table 1, there are pros and cons of each access control model and, therefore, it is problematic to rely on a single access control method in an IoT network. Therefore, this research looks into applicable access control methods that can be used in IoT networks to provide comprehensive security coverage. Specifically, how to enforce these access control methods in each IoT architectural layer to provide maximum protection.

2.2.3 Data Security

Data is one of the most valuable assets to an organisation and is susceptible to intentional attacks (Whitman & Mattord, 2022). As data travels through the network, from a source to a destination, data security is an area that needs to be paid attention to. Further, data security is critical to any organisation due to many other reasons such as legal requirements, reputational damages, system downtime and financial losses. Therefore, security measures need to be implemented to secure the data to preserve confidentiality, integrity and availability. As suggested (Eaton & McNett, 2020; Whitman & Mattord, 2022), security measures can be implemented physically, technically and administratively. Physical security refers to protection from physical actions and natural disasters, which is not discussed in this research. Technical security refers to the use of technology, and Administrative security refers to policies and procedures organisations can develop to safeguard the data.

IoT devices generate vast amounts of data based on their deployment in a network. The collected data from IoT devices travel through a specific path until it reaches its destination. As an example, from the perception layer to the application layer – from a sensor to a website. In search of security measures to apply, there are widely used technological methods to

secure data. The conventional methods to implement data security are cryptography, access control, network security, hardware-based security and data backups (Thapa and Camtepe, 2021). As an emerging technology, Blockchain is also used to secure the data (Lockl et al., 2020; Ray et al., 2021; Uddin et al., 2020). In fact, IoT networks are implemented with low resources, such as energy, memory and computational power (Alaba et al., 2017). Due to this resource constraint and the heterogeneous nature of IoT devices, implementing data security using conventional security methods is not straightforward, as these methods need high computational power, memory and storage (Sharma and Arya, 2022; Roman et al., 2011). Therefore, lightweight solutions need to be used in IoT networks to secure the data in transit, use, and storage. Authors (Alaba et al., 2017) suggest that lightweight encryption technology, which uses lightweight cryptography algorithms, suits IoT devices in the perception layer.

2.2.4 Security enabled Software Defined Networks (SDNs)

As an emerging technology, Software Defined Networks (SDN) are becoming popular within the industry and academia because of their network management flexibility, power, lower operational cost and ease of use compared to traditional network hardware device configuration (Gupta et al., 2023; Shin et al., 2016). SDN technology has been used in monitoring network traffic, threat diagnosis, network forensics, security policy management, etc (Ahmad et al., 2015).

Using a software-based programmable entity called a “Controller”, SDNs control the network traffic. Consequently, network intelligence can be centralised, and the physical network devices behave as forwarding devices because a software component will control dedicated hardware devices used to control the traffic (Ja’fari et al., 2021). Applications running in controllers can enforce high-level network policies, collect flow statistics, analyse statistics, and produce real-time network status (Sahay et al., 2019). The OpenFlow (OF) protocol is the first SDN standard originally defined (Lim, 2019). SDN Architecture consists of a “Data plane”, a “Control plane”, and an “Application plane”, also known as the management plane. Network devices act as intrusion detection systems responsible for forwarding and filtering traffic positioned in the data plane. Protocols and rules reside in the Control plane, and the Application plane contains the network and the security policies for managing the network (Sahay et al., 2019).

This emerging technology, SDNs, is widely used for IoT application deployment because of its dynamic behaviour, cost-effectiveness, flexibility, and adaptability (Zemrane et al., 2019). The positive side of the SDN is that it can be implemented with inbuilt security mechanisms. (Lim, 2019) has implemented an intrusion detection system using machine learning in an SDN-based environment where the Open Network Operating System (ONOS) is controlled. A further study by (Edwin Raja S & Ravi, 2020) implemented phishing attack detection using deep machine learning in an SDN environment. While security-enabled SDNs are used in IoT networks, SDNs also have drawbacks. The whole network will be unavailable if the central software-driven controller fails, or attackers can get full access to the network by gaining access to the controller. (Omar et al., 2019) point out that SDNs are vulnerable to DDoS attacks. They further explain that the "Controller" of the SDN will be unavailable due to a DDoS attack because incoming data packets will be sent to the controller, and the process will overload. As a result, computer resources may be drained, and the controller will fail to process legitimate data packets. Further, SDNs are prone to "Topology Poisoning attacks", "Side Channel Attacks" and "Botnets" (Gao et al., 2018; Ja'fari et al., 2021). Considering the drawbacks that can be caused by the SDNs, implementing security-enabled SDNs in IoT networks as a single solution is not enough as it also creates security risks.

2.2.5 Cyber Deception Technology

With the drawbacks of security technologies implemented in networks, most industries in the digital age demand more advanced and hybrid strategies to overcome security threats and vulnerabilities. As a result, the concept of "Deception": deceiving attackers has been applied to Cyberspace. As explained by (Steingartner et al., 2021), deception does not entail eliminating existing security controls in place. Deception complements and enhances security controls and provides more visibility of attack paths, activities and threat intelligence, providing robust protection using planned, methodical and managed actions. Some of the benefits of this technology are early post-breach detection, scalability, automation, reduced false positives and decreased risks (Steingartner et al., 2021). The Moving Target Defence (MTD) is an emerging cyber deception technique that increases the complexity of the network by making constant changes to the attack surface (Ge et al., 2020). This technique uses three approaches: *Shuffling* – which changes the network configuration by IP address

randomisation, device migration, and topology reconfiguration; *diversity* – which employs many implementations for the same functionality, e.g., different operating systems for servers; and *Redundancy* – replications of the network devices to increase the reliability. *Honeypot* is another mechanism used as cyber deception to trap attackers. In this mechanism, imitated physical and virtual devices are used to represent the actual devices and facilitate close monitoring and log activities, which helps defenders identify the attacks, study them, and implement countermeasures (La et al., 2016). Cyber deception technology can be used in IoT networks to mitigate potential attacks as a proactive solution to keep real resources such as sensors, communication links, and data sources away from intruders. As an example, implementing honeypots in an IoT network. As a drawback, there are no universal solutions for cyber deceptions, and the success and effectiveness of cyber deception techniques solely depend on the person's knowledge and capabilities who develop them (Dmytro S. Morozov et al., 2023).

2.3 Overview of the Frameworks

The terms framework and model appear frequently in information systems research publications. In general, these two terms seem similar, but not in theory. Many models are referred to as frameworks, and frameworks are referred to as models. So, this section provides a differentiation between a framework and a model.

As described (Haig, 2010), there is a vast variety of models in science: scale models, analogue models, mathematical models and theoretical models. A scale model refers to a construct of a selected object in a miniature size, with limited features and properties to its original (Haig, 2010). "*Scale models are usually built to present the properties of interest in the original object in an accessible and manipulable form*" (Haig, 2010). E.g., A model aircraft or military tank. Analogue models are used to express the relationship between the analogy and the selected reality, where requirements for modelling come from the need to learn about inaccessible entities hypothesised by theories, and these models are important in building scientific theory (Haig, 2010). E.g., a computational model of the mind or a molecular model of gases. A mathematical model is described as a model that "*offers an abstract symbolic representation of the domain of interest*" (Haig, 2010). Further authors (Haig, 2010) explain that the mathematical models are often considered "formal theories", and sometimes these

mathematical models are presented as mathematical equations in behavioural and social sciences. E.g., factor analysis. As described (Haig, 2010), "*Theoretical models typically describe an object by ascribing to it an inner mechanism or structure*". Theoretical models are created and described using the researcher's imagination, and these models are non-physical objects that consist of a set of assumptions of the object and inform the subject matter through their properties (Haig, 2010): E.g., Markov models of human and animal learning and Watson–Crick model of the DNA molecule.

A framework is descriptive, showing relevant concepts and components, how they relate to each other, and how important they are to the goal of solving a problem. A framework is a powerful technique for reuse (Aguiar, 2000). According to (Johnson & Foote, 1988), a framework can be described in three different ways: "*a sum of components and patterns*", "*reusable design of a whole system or parts of a system that represents a set of abstract classes, and the interaction between the classes*" and "*skeleton of an application that can be customized*". Further, (Stamer et al., 2016) define a framework in Information Systems as "*A framework is a structure underlying 'something' serving a specific purpose*".

Due to the constant evolution of security threats, any artifact (main research output of this PhD research) that develops to protect IoT networks must accommodate this (constant evolution). An artifact that can be re-used, which shows the relationship with each identified security element, capable of updating or adding new elements to improve the expected results without affecting the original structure, needs to be selected in this research. Therefore, a "framework" is chosen over a model as the main artifact in this research.

2.3.1 Frameworks

In academia, the term "framework" appears often. It is hard to find a universal, precise, or absolute definition of a framework in Information systems (Stamer et al., 2016). The authors explain that the term "Framework" has been used inconsistently across the domains and differently interpreted in the publications. A framework is considered a powerful technique that can be reused (Aguiar, 2000). Frameworks are developed to provide a solution for a specific problem domain, can respond to constant changes, and can be updated without

impacting the existing components (Nelson, 1994). Further (Ammar et al., 2018) explain the concept of a framework as identifying a structure that is a set of rules and regulations that coordinate and control the elements' processes. Per the systematic literature review conducted by (Stamer et al., 2016), the authors categorised the frameworks based on characteristics such as purpose, development process and structure. Six categories of frameworks were identified based on purpose. Four categories are based on the development process. The development process was supported by interviews, the author's experience, case studies and field studies. Seven categories were identified based on the structure of the framework. Table 9 summarises the six categories of frameworks based on purpose. Table 10 summarises the four categories of frameworks based on the development process, and Table 11 summarises the seven categories of frameworks based on structure.

Table 4 – Categories of the frameworks based on purpose (Stamer et al., 2016).

Framework category	**Description**
Green Information System Framework	The environmental aspect of the information system is the focus of this type of framework.
Test Framework	The purpose is to test the implementation of the Information system.
Development Framework	Supports the development of information systems or new system features from either a technical perspective, general perspective, or both.
Research Framework	Focus on theoretical topics with little practical application.
Evaluation Framework	It is to evaluate an information system or certain aspects of the information system.
Mixed Purpose Framework	Combination of two or more framework categories based on the purpose of the framework

Table 5 – Categories of the frameworks based on the development process (Stamer et al., 2016).

Framework category	Description
Literature Review Developed Frameworks	Frameworks are developed through an academic literature review.
Research Developed Frameworks	Frameworks are developed using existing research. E.g., existing theories, models and frameworks.
Requirements Developed Frameworks	Frameworks are developed to fulfil identified requirements.
Mixed Developed Frameworks	Frameworks are developed using multiple categories. E.g., Literature review + Research developed approach.

Table 6 – Categories of the frameworks based on structure (Stamer et al., 2016).

Framework category	Description
Layered Structured Frameworks	These frameworks have a layered structure where each layer describes the system features on each level.
Technical Structured Frameworks	These frameworks consist of technical components and their detailed description.
Sequence Structured Frameworks	These frameworks consist of activities that are performed in a sequence.
Category Structured Frameworks	These frameworks structure a studied phenomenon into different categories, each with different characteristics.
Factors-outcome Structured Frameworks	These frameworks consider relevant factors and determine how these factors impact the outcome.
Component Structured Frameworks	These frameworks have component-based structures, and components describe the framework and their interrelationship.
Mixed Structured Frameworks	These frameworks show a mix of structures used to develop the framework.

Table 4, Table 5 and Table 6 give a clear understanding of how the frameworks can be identified in the field of information systems. Considering the categorisation based on purpose, development process and structure presented in Table 4, Table 5 and Table 6, when positioning this research of developing the proactive defence framework for IoT network security, based on the purpose, the proposed framework falls into the "development framework" category as it develops an information system in both technical and general perspectives. Based on the development process, the proposed framework falls into a "mixed developed framework" as it uses the literature review, research developed, and requirements developed categories. Looking at the Structure, the proposed framework uses the "mixed structure framework", which uses the "technical" structure as it consists of technical components, "sequence" structure as it consists of activities that are performed in a sequence and component" structure as it consists of a component-based structure with the interrelationships.

In addition to the security solutions discussed in section 2.2, further search is continued to find how researchers have conducted academic studies on protecting IoT networks, data, and digital health systems from security attacks, specifically about security frameworks introduced and implemented to protect against and overcome security issues. These findings aim to contribute valuable, concrete information, solutions and new ideas to identify critical security elements to include in this research framework to build an advanced, robust, result-oriented, usable and comprehensive security framework to protect IoT networks from security threats and attacks. Therefore, a scoping review has been conducted to achieve this purpose. The next section describes the scoping review.

2.4 Scoping Review

This section presents the findings from the scoping review conducted to investigate the existing security frameworks in IoT networks.

Security frameworks are a central component of this research. Therefore, a scoping review was necessary to ensure that existing frameworks are captured comprehensively from the literature. An extensive search strategy, the “PRISMA” method, was used. The scoping review was conducted using four electronic databases: Scopus, ScienceDirect, IEEE Explorer and PubMed, with pre-defined search queries. The overall search was focused on the research question, “How can a framework be developed and applied for proactive defence for IoT network security in digital health?”. The search focused on finding the security and security frameworks around using the terms “IoT Network Security”, “Framework for IoT Network Security”, “IoT in Digital Health”, “IoT Network Security in Digital Health”, and “Proactive defence for Internet security”. The results of the database search are shown in Table 7. The searches were limited to English language results and studies published between 2015 and 2020. Data was extracted using Microsoft Excel and multiple spreadsheets to filter relevant studies. Strict inclusion and exclusion criteria were set during the screening process.

Method:

A. Identify the following search queries
    a. IoT Network Security
    b. Framework for IoT Network Security
    c. IoT in Digital Health
    d. IoT Network Security in Digital Health
    e. Proactive defence for Internet security

B. Multiple electronic databases, *Scopus*, *Science Direct*, *IEEE Xplore* and *PubMed*, were used to search the relevant published studies using search queries from peer-reviewed academic journals and conference proceedings.

The following combinations of search terms were used during the electronic database search:

- IoT network Security, searched as “IoT network security”
- Framework for IoT Network Security searched as (“Framework for IoT” OR “IoT Framework”) AND “Network Security”
- IoT in Digital Health, searched as “IoT” AND “Digital Health”
- IoT Network Security in Digital Health searched as "Digital Health" AND "IoT" AND "Network Security"
- Proactive defence in IoT Networks, searched as “Proactive defence” AND “Internet security”

Table 7 – Number of papers found for each database searched.

Search terms	Scopus	Science Direct	IEEE Xplore	PubMed
IoT Network Security	23	24	38	10
Framework for IoT Network Security	41	64	17	17
IoT in Digital Health	27	83	22	36
IoT Network Security in Digital Health	22	9	44	4
Proactive defence for Internet security	20	10	44	1
Total (556)	**133**	**190**	**165**	**68**

Inclusion criteria

The following criteria were used for paper inclusion.

- Existing frameworks developed for the Internet of Things (IoT) security, Internet of Things (IoT) Networks OR
- Internet of Things (IoT) security Issues and challenges OR
- Application of AI/ ML/ DL/ NN/ DM in digital health systems for security OR
- Proactive defence against security threats, vulnerabilities, and techniques in IoT networks

Exclusion criteria

The following criteria were used to exclude papers.

- IoT devices focusing on energy efficiency, management
- IoT - Interoperability, Flexibility, Usability, Design Requirements, workflow management

- Traditional Networks, Sensor technologies, Sensor networks, Cloud – Fault diagnosis, troubleshooting, improvements, management
- Software platforms, Application development, Protocols Design
- Human sensing, body movement identification, tracking
- Clustering, Dynamics and scalability - large-scale mobile ad hoc networks
- Data transmission techniques, performance improvement
- General workplace Security, physical security, health and safety
- Big data, data analytics, analytics techniques – not security perspective
- Health diagnostics, assessments, therapeutics, and monitoring
- General policies, regulations, and guidelines related

After the papers were selected from the initial search, the total was 558. Duplicate records (n=83) were removed, leaving 475 for title and abstract screening. After the title and abstract screening, 211 studies were full-text reviewed, and 164 were included in the final study. Figure 5 shows the PRISMA flow diagram for the literature search.

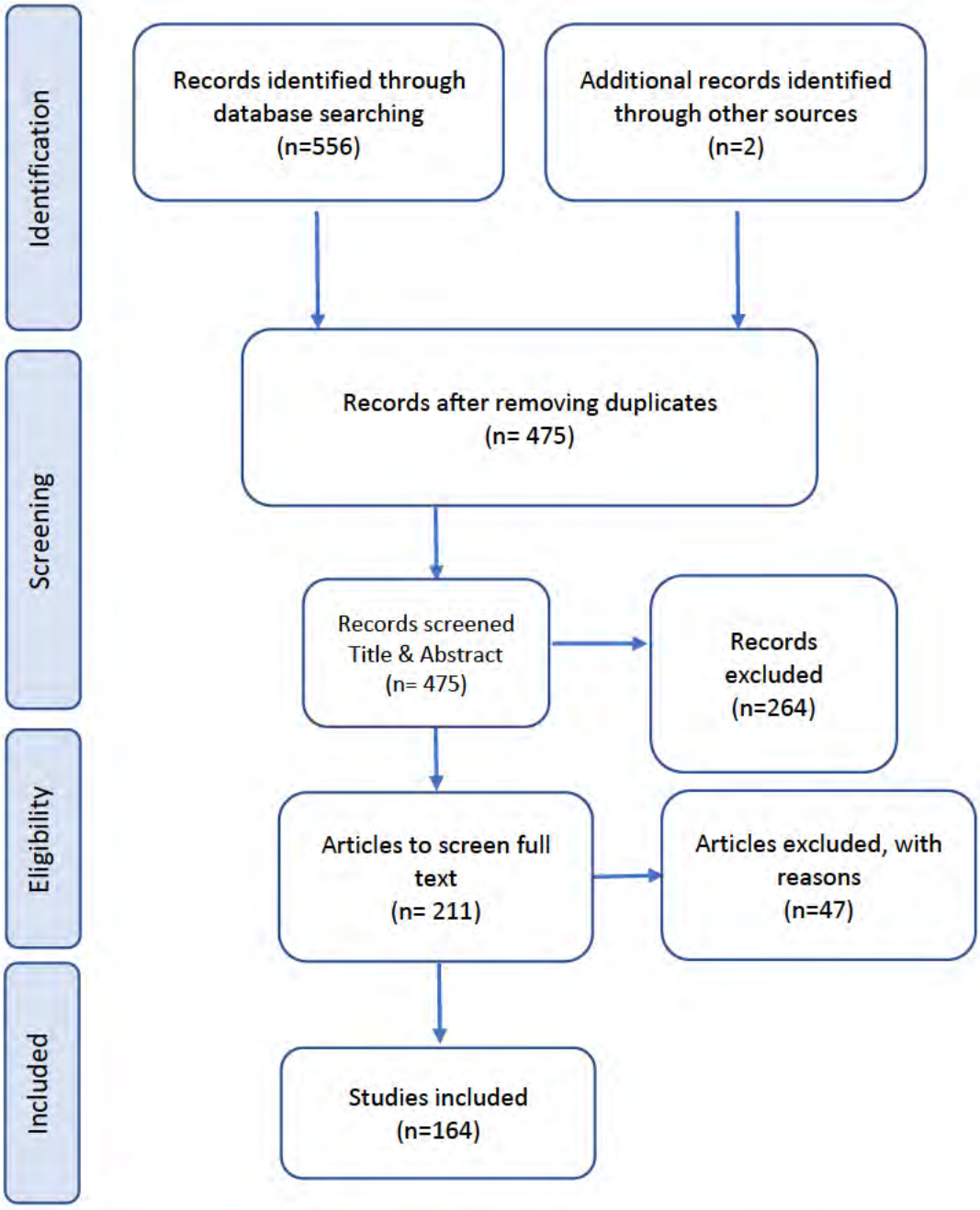


Figure 5 – PRISMA flow diagram for study selection

Out of 164 papers, 37 papers on frameworks related to IoT networks, digital health, and proactive defence were found during the scoping review process. These frameworks were categorised into "framework based on", "framework focus on", and "Model/Process" for further analysis. Framework-based helps to understand what technology, techniques or mathematical functions have been used in the framework. Framework focus helps uncover

the security framework's area, aspect or specific component. The last column is used to identify the process frameworks.

Table 8 summarises the 37 frameworks found during the scoping review process related to IoT networks, Digital health and Proactive Defence.

Table 8 – Summary of the 37 Frameworks

Year	Authors	Title	Framework based on	Framework focus on	Process Framework
2019	A. Ahuja; H. Gandhi; R. Shorey; D. Kulkarni; J. Tew	PlumeWalk: Towards Threat Provenance Localization for IoT Networks	Graph theoretic threat provenance identification	To provide a fast and accurate topological characterisation of threat provenance as implied by the network traffic and the network configuration.	Not a Process FW
2019	A. Ashtari; A. Shabani; B. Alizadeh	A New RF-PUF Based Authentication of Internet of Things Using Random Forest Classification	Based on RF-PUF (radio frequency - Physical unclonable functions)	Authenticate wireless nodes	Process FW
2019	A. H. Ahmed; N. M. Omar; H. M. Ibrahim	Secured Framework for IoT Using Blockchain	Blockchain	IoT monitoring applications	Not a Process FW
2016	A. H. Moon; U. Iqbal; G. M. Bhat	Lightweight Authentication Framework for WSN	Lightweight Authentication for WSN	Supports node registration, entity authentication, key establishment, new node injection and broadcast authentication of messages diffusing from the base towards nodes in WSN	Not a Process FW
2019	Abubakar Sadiq Sani, Dong Yuan, Jiong Jin, Longxiang Gao, Shui Yu, Zhao Yang Dong,	Cyber security framework for Internet of Things-based Energy Internet	Identity-based security mechanism	security and privacy in integrated internet-based smart grids	Not a Process FW a Model
2018	Ansari A.M., Hussain M.	Middleware-Based Node Authentication Framework for IoT Networks	Lightweight Authentication - Middleware Based	IoT node authentication	Not a Process FW a Model/ technique
2018	B. B. Gupta; M. Quamara	Multi-layered Cloud and Fog-based Secure Integrated Transmission and Storage Framework for IoT-based Applications	Cloud and Fog	IoT Transmission and Storage IoT Applications	Process FW
2019	Chattopadhyay A.K., Nag A., Ghosh D., Chanda K.	A secure framework for IoT-based healthcare system	security protocols - HTTPS-SSL - AES-256 and SHA-3	Secure communication	Not a Process FW

2017	G. Varshney; H. Gupta	A security framework for IOT devices against wireless threats	Blockchain	Security and management of data on the Internet	Process FW
2020	G. Yadav; K. Paul; A. Allakany; K. Okamura	IoT-PEN: A Penetration Testing Framework for IoT	server-client architecture	Penetration testing	Not a Process FW
2017	Hadar N., Siboni S., Elovici Y.	A lightweight vulnerability mitigation framework for IoT devices	Cloud-based Security Appliance	IoT network traffic flow	Process FW
2018	Hsu R.-H., Lee J., Quek T.Q.S., Chen J.-C.	Reconfigurable Security: Edge-Computing-Based Framework for IoT	Edge computing	Protocol layers, including multiple applications on an IoT device (reconfigurable security framework	Not a Process FW
2018	J. Pacheco; C. Tunc; S. Hariri	Security Framework for IoT Cloud Services	Anomaly behaviour analysis, IDS	IoT Cloud-based applications and services	Process FW
2019	K. Albalawi; M. M. A. Azim	Cloud-based IoT Device Authentication Scheme using Blockchain	Blockchain	IoT device authentication	Process FW
2019	Kavitha S, Alphonse PJA, Reddy YV.	An Improved Authentication and Security on Efficient Generalized Group Key Agreement Using Hyper Elliptic Curve Based Public Key Cryptography for IoT Health Care System	Hyper Elliptic curve based public key cryptosystem	Ensure entity authentication and secure group communication	Not a Process FW
2019	Kim Y., Nam J., Park T., Scott-Hayward S., Shin S.	SODA: A software-defined security framework for IoT environments	SDN - IoT Gateway	To protect IoT-sensitive and private information	Not a Process FW
2018	Krishnan K.N., Jenu R., Joseph T., Silpa M.L.	Blockchain-Based Security Framework for IoT Implementations	Blockchain	Secure communication and authentication of the data across IoT networks	Process FW
2018	M. A. Hakim; H. Aksu; A. S. Uluagac; K. Akkaya	U-PoT: A Honeypot Framework for UPnP-Based IoT Devices	Honey pot based	Capturing attacks on IoT devices that use Universal Plug and Play (UPnP) protocol	Not a Process FW
2019	M. Nobakht; C. Russell; W. Hu; A. Seneviratne	IoT-NetSec: Policy-Based IoT Network Security Using OpenFlow	policy-based and fine-grained traffic monitoring	Traffic monitoring of the IoT network segments	Not a Process FW
2020	Md. Ashraf Uddin, Andrew Stranieri, Iqbal Gondal, Venki Balasubramanian,	Blockchain leveraged decentralised IoT eHealth framework	Blockchain	Medical data to ensure reliable, secure and private communication	Process FW

2020	Murthy S., Kavitha C.R.	A smart and secure framework for IoT device-based multimedia medical data	Multimedia decryption and encryption techniques	Secure way to share multimedia medical data over the internet in IoT devices	Not a Process FW
2019	Myers J., Babun L., Yao E., Helble S., Allen P.	MAD-IoT: Memory anomaly detection for the internet of things	Machine Learning	IoT Memory Anomaly Detection	Process FW
2018	Nwafor E., Campbell A., Hill D., Bloom G.	Towards a provenance collection framework for Internet of Things devices	Data provenance (data lineage) techniques	IoT data objects	Not a Process FW
2019	Rashid M.A., Pajooh H.H.	A security framework for IoT authentication and authorization based on blockchain technology	Blockchain	A multi-layer security network model for IoT network	Not a Process FW
2019	S. Behrad; S. Tuffin; E. Bertin; N. Crespi	Network Access Control for the IoT: A Comparison Between Cellular, Wi-Fi and LoRaWAN	General comparison	Access control architectures in the different communication technologies (cellular, Wi-Fi and LoRaWAN)	Not a Process FW
2019	S. Chakraborty; S. Aich; H. Kim	A Secure Healthcare System Design Framework using Blockchain Technology	Blockchain	Maintaining the privacy of the patient's data and also the process of laying out real-time accurate and trusted data to the medical practitioners	Not a Process FW
2019	Salman O., Elhajj I.H., Chehab A., Kayssi A.	A machine learning-based framework for IoT device identification and abnormal traffic detection	Machine Learning	Device identification and abnormal traffic detection	Process FW
2019	Satamraju K.P., Malarkodi B.	Design and Evaluation of a Lightweight Security Framework for IoT Applications	Lightweight security mechanisms	Security for the data transmitted from the device	Not a Process FW
2018	Setikere S., Sachidananda V., Elovici Y.	Out of kilter: Holistic exploitation of denial of service in the internet of things	Network traffic analysis	DoS or a DDoS attack on a specific IoT device	Not a Process FW
2018	Shailendra Rathore, Jong Hyuk Park,	Semi-supervised learning based distributed attack detection framework for IoT	Machine Learning - Extreme learning machine (ELM) based Semi-supervised Fuzzy C-Means (ESFCM) method	Fog-based attack detection	Process FW
2017	Sridhar S., Smys S.	Intelligent security framework for IoT devices: Cryptography-based end-to-end security architecture	Lightweight Asymmetric cryptography, Lattice-based cryptography	To secure IoT service gateway, Broker devices/Gateway and cloud services.	Not a Process FW
2019	Weijie Han, Jingfeng Xue, Yong Wang,	MalInsight: A systematic profiling-based malware detection framework	Systematic profile based	IoT Malware detection	Process FW

	Zhenyan Liu, Zixiao Kong,				
2020	Xu L., Chen L., Gao Z., Fan X., Suh T., Shi W.	DIoTA: Decentralized-Ledger-Based Framework for Data Authenticity Protection in IoT Systems	A decentralized ledger-based lightweight data authentication mechanism	To facilitate IoT devices and data management	Process FW
2020	Yahya Al-Hadhrami, Farookh Khadeer Hussain,	Real-time dataset generation framework for intrusion detection systems in IoT	Real time data collection from IoT Networks	New training datasets for IDS	Process FW
2019	Zarca AM, Garcia-Carrillo D, Bernabe JB, Ortiz J, Marin-Perez R, Skarmeta A.	Enabling Virtual AAA Management in SDN-Based IoT Networks	novel policy-based and cyber-situational awareness	Authentication, Authorization, Accounting (AAA) as well as Channel Protection virtual security functions in IoT networks	Process FW
2016	Zeb K., Saleem K., Al Muhtadi J., Thuemmler C.	U-prove based security framework for mobile device authentication in eHealth networks	Token-based security concept	Mobile device authentication and authorization in the eHealthcare	Process FW
2020	Zubair A. Baig, Surasak Sanguanpong, Syed Naeem Firdous, Van Nhan Vo, Tri Gia Nguyen, Chakchai So-In,	Averaged dependence estimators for DoS attack detection in IoT networks	Average Dependence estimator-based scheme	Intelligent Denial of Service (DoS) attack detection	Process FW

Thirty-seven (37) papers were examined to identify the type of framework. As a result of this exercise, 17 papers were identified as process frameworks that were based on blockchain and focused on data security, communication security and access control, machine Learning network anomalies, attack detection, device identification, Cloud-based IoT applications, anomaly behaviour analysis, real-time data collection from IoT networks, creating new training data sets, systematic profiles for malware detection, token-based access control and policy-based cyber security awareness.

Table 9 shows the categorisation of the remaining 127 papers that do not relate to frameworks.

Table 9 - Categorisation of the remaining 127 papers.

Category	Topic	Number of studies
1	Access Control	15
2	Artificial Intelligence, Machine Learning, Deep Learning, Neural Network	14
3	Blockchain	18
4	Attack detection, security assessments, Protocol, Cryptography	14
5	Proactive defence – Data security, Moving Target Defense, IDS, IPS, Honey Pot	14
6	Survey studies	26
7	Systematic reviews	3
8	Cyber defence, Data security, IoT and Cloud, Risk assessment, Security Awareness	23
	Total	127

As an emerging technology, “Blockchain” has been used by 18 papers to implement access control mechanisms to identify, authenticate and authorise users, IoT devices and wireless nodes and to apply security to data in use, data in transit and data in storage. Most blockchain studies focus on information exchange, access and transaction management, trust, continuous integrity, tamper proof, provenance and data traceability (Ahmed et al., 2019).

Artificial intelligence, machine learning, deep learning, and neural networks (AI, ML, DL, NN) have been used in 14 studies to discuss access control, network traffic analysis, attack detection, and implementing intrusion detection systems. Intrusion Detection and Prevention Systems are heavily used and discussed in the literature. Various techniques, including AI, ML, DL, NN and other mathematical functions, are used to analyse the network traffic and patterns to detect abnormalities.

Data encryption and decryption techniques such as cryptography, pseudonymisation and anonymisation, hyperelliptic curve-based public key cryptosystem, lightweight asymmetric cryptography and lattice-based cryptography have been used for access control and data security. Software Defined Networks (SDN) have been used to implement IoT gateways and policy-based internet traffic monitoring in IoT networks.

Cloud, fog and edge technologies are used to implement security in IoT networks, IoT applications, data transmission, storage and IoT network traffic analysis. Further, Cloud, fog and edge-based solutions are used to control IoT network traffic flow, identify policy violations, protect IoT services from attacks and ensure the security and privacy of IoT by deploying software-based appliances.

Fourteen papers that were focused on proactive defence were found. Seven of these discussed a Moving Target Defence (MTD) concept, which increases the complexity of the network by making constant changes to the attack surface (Ge et al., 2020). MTD is used for attack prevention, tolerance, and early identification of attacks such as DDoS attacks. Further studies use cyber threat intelligence, software-defined networks and moving target defence techniques in cloud-based applications to provide proactive defence mechanisms.

Twenty-six survey studies discussed different areas in IoT networks and network security-related aspects in digital health systems. The focus areas were security and privacy issues, security challenges, security requirements, secure communication and routing, security vulnerabilities, threats, attacks, AI and IDS, blockchain in IoT, encryption and decryption techniques, cryptography and IoT trust models. Three systematic literature review studies were discussed regarding enforcing security in IoT, information security and different security frameworks. Fourteen papers discuss protocol design about privacy, lightweight critical establishment and routing.

Finally, twenty-three papers focused on software security models, software security solutions, Intrusion detection systems, security assessments, prototype architectures, risk assessments, impact analysis, attack detection and general data security concepts.

The initial scoping review covered the period 2015 to 2020. The following section presents the research papers from the period 2021 to 2024. The original search terms and the same review process described in Section 2.4 were followed to obtain the results shown in Table 7 A. The "Covidence" web-based software was used to conduct the review.

Table 10 A– Number of papers found for each database searched for 2021 - 2024.

Search terms	Scopus	Science Direct	IEEE Xplore	PubMed
IoT Network Security	31	18	143	4
Framework for IoT Network Security	1	84	10	13
IoT in Digital Health	4	21	4	56
IoT Network Security in Digital Health	7	1	16	0
Proactive defence for Internet security	1	4	16	1
Total (435)	**44**	**128**	**189**	**74**

After the papers were selected from the initial search for 2021 - 2024, the total was four hundred thirty-five (435). Thirty-eight duplicate records were removed, leaving three hundred ninety-seven (397) for title and abstract screening. After the title and abstract screening, 121 studies were full-text reviewed, and 91 were included in the final study. Figure 5 A shows the PRISMA flow diagram for the literature search.

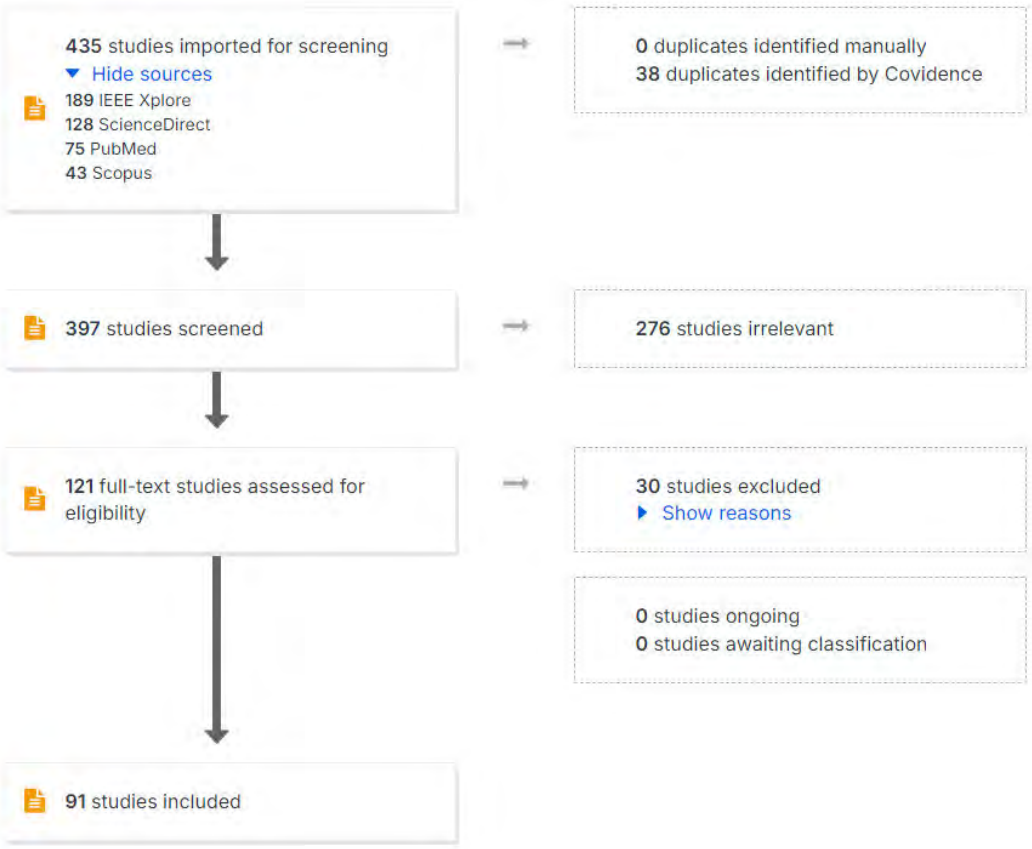


Figure 6 A – PRISMA flow diagram for study selection 2021-2024

Out of ninety-one studies, thirteen papers discussed IoT security frameworks, summarised in Table 7 B. Nine studies of these IoT security frameworks discussed Artificial Intelligence, Machine Learning, Deep Learning, and Neural Networks. These have been used in threat landscaping and modelling, intrusion detection, detecting malicious traffic, and anomaly detection in network traffic. Two studies were about moving target defense and cyber deception technologies to provide IoT network security by detecting DDoS attacks. One study employed blockchain concepts, using clever contracts and virtual contracts to implement policies and conditions to grant access to the networks, while another focused on the Stackelberg game model to analyse IoT packet sampling against DDoS attacks to overcome the computational overhead that occurs in networks when inspecting all packets online for DDoS detection.

Table 11 A– Summary of the 13 Frameworks

Year	Authors	Title	Framework based on	Framework focus on
2021	B. Ikharo; A. Obiagwu; C. Obasi; S. U. Hussein; P. Akah	Security for Internet-of-Things Enabled E-Health using Blockchain and Artificial Intelligence: A Novel Integration Framework	Artificial Intelligence (AI), Internet-of-Things (IoT) and Blockchain (BC)	Security of e-health data, secured e-health services
2024	K. Shrivastava; S. Singh; P. Chaudhary; R. Singh; B. K. Saraswat; A. Garg	An Improved Blockchain Based Security Framework for IoT Enabled Wireless Network	Blockchain - Clever contracts, virtual contracts, validating transactions	IoT wireless networks
2024	Garah, Abdelhamid; Mbarek, Nader; Kirgizov, Sergey	Enhancing IoT data confidentiality and energy efficiency through decision tree-based self-management	Lightweight cryptographic ciphers, decision tree technique	Deployment of lightweight encryption solutions
2021	Tsogbaatar, Enkhtur; Bhuyan, Monowar H.; Taenaka, Yuzo; Fall, Doudou; Gonchigsumlaa, Khishigjargal; Elmroth, Erik; Kadobayashi, Youki	DeL-IoT: A deep ensemble learning approach to uncover anomalies in IoT	Deep and stacked autoencoders to extract handy features for stacking into an ensemble learning model, deep feature extraction with a deep ensemble learning model	Class imbalance, dynamic attack detection, and data heterogeneity problems together in Software-Defined Networking (SDN) enabled IoT anomaly detection
2022	Aslam M; Ye D; Tariq A; Asad M; Hanif M; Ndzi D; Chelloug SA; Elaziz MA; Al-Qaness MAA; Jilani SF	Adaptive Machine Learning Based Distributed Denial-of-Services Attacks Detection and Mitigation System for SDN-Enabled IoT.	Adaptive Machine Learning based SDN-enabled Distributed Denial-of-Services attacks Detection and Mitigation (AMLSDM)	Denial-of-Services attacks Detection and Mitigation
2024	Sunanda, N.; Shailaja, D.K.; Kandukuri, P.; Rao, V.S.; Godla, S.R.	Enhancing IoT Network Security: ML and Blockchain for Intrusion Detection	Machine learning, specifically Red Fox Optimization (RFO) for feature selection and Attention-based Bidirectional Long Short-Term Memory (Bi-LSTM).	Intrusion detection

2024	Tyagi, K.; Ahlawat, A.; Chaudhary, H.	IoT Network Security: NetFlow Traffic Analysis and Attack Classification Using Machine Learning Techniques	Machine learning balancing technique was created to solve the issue of class imbalance, which provides the best results after implementing Machine Learning(ML) models	Real-time anomaly detection
2024	Osman, Musa; He, Jingsha; Zhu, Nafei; Mokbal, Fawaz Mahiuob Mohammed	An ensemble learning framework for the detection of RPL attacks in IoT networks based on the genetic feature selection approach	Ensemble Learning-based	Intrusion Detection System (IDS)
2021	Hussain F; Abbas SG; Shah GA; Pires IM; Fayyaz UU; Shahzad F; Garcia NM; Zdravevski E	A Framework for Malicious Traffic Detection in IoT Healthcare Environment.	Open-source IoT data generator tool - IoT Flock	detect malicious traffic in IoT
2022	X. Chen; L. Xiao; W. Feng; N. Ge; X. Wang	DDoS Defense for IoT: A Stackelberg Game Model-Enabled Collaborative Framework	Stackelberg game model to analyse the collaborative IoT packet sampling	Detect DDoS attacks
2022	H. Galadima; A. Seeam; V. Ramsurrun	Cyber Deception against DDoS attack using Moving Target Defence Framework in SDN IOT-EDGE Networks	Moving Target Defense (MTD) technique based on SDN	Detect DDoS attacks
2021	Y. Zhou; G. Cheng; S. Yu	An SDN-Enabled Proactive Defense Framework for DDoS Mitigation in IoT Networks	Moving Target Defense (MTD) techniques	Detect and mitigate DDoS attacks

2024	Thakur, Pankaj; Goel, Shubham; Puthooran, Emjee	Edge AI Enabled IoT Framework for Secure Smart Home Infrastructure	Cost-effective, lightweight Edge, AI based	Secure Smart Home Infrastructure

Table 7 C categorises the remaining 78 papers that do not relate to frameworks.

Table 12 A - Categorisation of the remaining 78 papers.

Category	Topic	Number of studies
1	Access Control: Blockchain	3
2	Artificial Intelligence, Machine Learning, Deep Learning, Neural Networks, Threat landscaping and modelling	46
3	Attacks and Solutions in the IoT Network, Survey	1
4	Blockchain; IoT Networks - Security solution, data security	5
5	Data Security; SDN	6
6	Forensics; IoT Networks - Security solution	1
7	IoT Networks - Security solution; Threat landscaping and modelling, IDS and IPS	11
8	Moving target defense and cyber deception IoT Networks - Security solution DDoS detection	2
9	Security Prediction	2
10	Zero Trust	1
	Total	78

The research study about “Zero Trust” attempts to prevent advanced persistence attacks (APT) in local area networks from IoT devices. The study's primary focus is the local area network, not the IoT network, and it uses the traditional network security concepts of micro-segmentation and the next-generation firewall in conjunction with the zero trust concepts. Two studies have discussed security predictions. Security prediction refers to predicting the future security of the IoT network using mathematical models based on IoT historical data and network status (Xiao et al., 2022; Yang et al., 2022). If needed, this can be easily integrated into the proposed security framework’s threat landscaping and modelling to include future predicted threats and vulnerabilities. Further, Chapter 4, Section 4.5.3.1 explains that developing a threat landscape involves using threat intelligence. These future predictions can be considered threat intelligence.

The papers from 2012 to 2024 do not show any comprehensive security framework developed to protect IoT networks proactively. Compared to the initial scoping review, the findings show no significant change other than two terms: security prediction and zero trust. All other topics are in line with previous findings.

2.4.1 Summary of Scoping Review

The analysis of each framework/ paper used in the initial point of the research is discussed in Chapter 4.

2.5 Summary of the literature findings

Technology continues to develop rapidly, but improvement in security in the healthcare industry cannot be seen. It is evident from Figure 2 that the number of days to identify and contain a security incident has not improved in the last seven years (2017-2023), and according to the global incident data, the healthcare industry is at the top of the list (Figure 3). The number of patient records breached has tripled (Table 1), indicating that current healthcare security systems are weak or inadequate. Furthermore, it is predicted ("Leading the IoT", 2017) that 25% of future breaches will be due to IoT technology.

The global average time to identify and contain a security breach is 280 days. In five years (2015 to 2020), this number has been reduced by a mere five days. The time to contain in the healthcare industry exceeds the global average. In the seven years, technology has not contributed in any significant way to reducing the rate of incursions or improving discovery. The security solutions discussed in the literature and currently deployed have also provided no considerable impact on breach events. These solutions are primarily reactive. In the face of increasing security and privacy challenges, digital health systems will remain most vulnerable unless security measures are applied in a defensive and preventative manner.

While most of the studies in this scoping review use the term “framework”, however specific elements of each framework are not present. Generally, the studies target a particular security area and are not comprehensive. Comprehensive means end-to-end security for IoT. E.g., from sensing to application. The “process frameworks” identified in this review address discreet areas of security and do not offer a comprehensive framework that can be used to develop secure IoT networks for digital health systems. This review found no comprehensive

security framework for use as a base to build a robust, highly secured IoT network in digital health.

A comprehensive security framework must include a wide variety of security concepts in addition to other technologies such as artificial intelligence (AI), feedback loops, and Interrelated security elements that contribute to each other to improve their function and to increase the level of defence. The application of in-depth vulnerability assessment, threat modelling and mapping them to IoT architecture is not discussed or applied to IoT in digital health systems.

Due to the nature of IoT devices, applying traditional security measures is challenging and not straightforward. IoT networks use different ways to connect and use different protocols depending on the application. Without rich visibility of all connected devices, including the type of devices used and where they are deployed, device connectivity, network connectivity and technologies used in the IoT network mapped to the IoT architecture will fail to implement any security solution to provide end-to-end protection. There is no universal fit, common language, or ready-made solution that can be used or applied for IoT networks. Therefore, applying a single security solution does not suit nor is sufficient and demands a layered security approach where security can be strengthened in each architectural layer in the IoT network and supported by an In-detail application process for the security of an IoT network.

Additionally, a technology-agnostic and vendor-neutral security framework is needed, where the IoT network security implementors can use open-source or vendor-specific technology to implement a security element based on their circumstances. Deploying IoT networks without proper security may create security risks to the greater network. It allows attackers to exploit weaknesses and get into the main network. Therefore, the IoT security framework must be robust and cater to constantly evolving threats and the need to minimise the security risk for the greater network.

This chapter provided a background to the Internet of Things (IoT), including the evolution of IoT architecture, a literature review discussion, scoping review findings and the identified gaps. The next chapter presents the research methodology.

3. METHODOLOGY

This chapter begins with a general introduction to research and research methodologies used in information system research. The selection of the research method to answer the research questions is described. The disciplines of Information Systems (IS), Design Science Research (DSR), and Design Science Research Methodology (DSRM) are explained in detail. “Design Science Research” is the overarching research methodology and describes the Design Science Research Methodology (DSRM) Process Model in the research design to address the research questions.

3.1 Research Paradigms

As pointed out by (Shanks et al., 1993), the two paradigms, “positivism” and “interpretivism”, which are based upon philosophical assumptions about the science and the nature of social reality, need to be considered when selecting a research approach. Positivism refers to “seeking to explain and predict what happens in the social world by searching for regularities and causal relationships between its constituent elements” (Morgan, 1979; as cited in (Shanks et al., 1993)). Interpretivism is “the systematic analysis of socially meaningful action through the direct detailed observation of people in natural settings to arrive at understanding and interpretations of how people create and maintain their social world” (Neuman 1991; as cited in (Shanks et al, 1993)). There is a third research paradigm: critical theory. Critical theory is described as “a theory of society and a meta-theory of social science (Fay 1987 cited by Grimes 1992). It may apply to the topic of technology where there is a “threat to the human agency” or in the development of public policy as it relates to technology or in “social theories of modernity” (Fouche et al. 2017). The two paradigms act differently within information systems research. Positivism is interested in research that confirms validity by replicating it. Interpretivism is about making the results clear, coherent, consistent, and understandable within the context (Williams, 2006). Therefore, the intrinsic investigation into information systems includes how humans interact with and function with others and technology (Williams, 2006). Interpretivism may be a suitable investigative paradigm over positivism in this information system research.

3.2 Research Approaches

Information Systems researchers are equipped with a range of research approaches, from experiments to conceptual studies (Williams, 2006). The continuum of research approaches proposed by the authors is demonstrated in Figure 6. In addition to these approaches, authors (Galliers, 1991) identified further approaches: "Theorem Proof", "Engineering", "Reviews", "Longitudinal", and "Forecasting/ Future Research". When making an informed decision to select a research approach or scholarship, Information systems researchers need to consider many factors: relevance, philosophical framework, research stage, purpose and approach (Shanks et al, 1993).

Figure 7 – A Continuum of Approaches to Research (Williams, 2006)

Further, (Shanks et al., 1993) presented "A Model of the Discipline of Information Systems", shown in Figure 7, which the researchers can use to conduct IS research. This model illustrates the relationship between "*Research*"," *Scholarship*" and "*Practice*" while highlighting how other reference disciplines provide grounding theory and research approaches.

Figure 8 - A Model of the Discipline of Information Systems (Shanks et al., 1993).

"Scholarship" is defined "as the process of systematising existing knowledge relevant for a discipline" (Shanks et al, 1993). Systematising existing knowledge can be accomplished by surveying the literature, including grey literature, published industry security reports and web resources. Then, the gained knowledge can be used to develop new insights, hypotheses, frameworks, and feeds. "Research" is defined as "a systematic process of acquiring new knowledge" that can generate new and revised theories, and the research results can feed into "Scholarship" and "Practice" (Shanks et al., 1993). Practise refers to using "Scholarship" and "Research" to improve the practice.

3.3 Research Approach Justification

The main research question, "How can a framework be developed and applied for proactive defence for IoT network security in digital health?" can be subdivided into "How to develop?" and "How to apply?". Regarding development, identifying framework elements to address contemporary IoT security concerns in digital health systems is broad and complex. Development of such a framework involves an in-depth analysis of literature and industry publications, assessment of current security systems, development of improvements, new

insights, and new areas. The application of such a framework needs a deep understanding of the IoT environment, including devices, architecture, platforms, networks, and current technologies, as well as the researcher's knowledge and experience in the field. This research is considered applied research as it aims to improve a specific concern, "security", in IoT networks in digital health systems. This research falls into the Information System research domain as it is systemising the existing knowledge, the "scholarship", follows a process to acquire new knowledge, the "research", and improves the "practise" by proactively defending the IoT networks and enabling network architects to design IoT networks with a high level of security leading to effective and efficient operational IoT networks. This research uses a mixed approach to developing the framework as a conceptual study, applying it using a desk study, and validating it by expert interviews.

3.4 Research and Research Methodology

In their book "Design Research in Information Systems: Theory and Practice", the authors (Hevner & Chatterjee, 2010) suggest that our knowledge is incomplete and problems are waiting to be solved. To solve these problems, questions are to be asked, and answers are to be found. To find answers, it is necessary to follow a suitable method. Furthermore, the authors emphasise the "role of research" is to provide a method to find answers. (Kuhn 1970; Lakatos 1978, as cited in (Hevner & Chatterjee, 2010) defining research "*as an activity that contributes to the understating of a phenomenon*". A similar definition (Oates et al., 2022) for research is the "*Creation of new knowledge, using an appropriate process, to the satisfaction of the research users*". And (Shanks et al., 1993) define research as "*a systematic process of acquiring new knowledge*". Accordingly, it is clear that "research" is a process to find an answer to a question, a resolution for a problem or a greater understanding of a phenomenon, and this process is called "*Research Methodology*" (Hevner & Chatterjee, 2010).

3.5 Design Science Research Justification

The design science history goes back to the 15th century (Dresch et al., 2014). In 1969 "(first published in 1969 and third edition in 1996), the author Herbert A. Simon explained the idea of the "Science of Design" in his book "The Science of the Artificial" and highlighted the

difference between natural science and design science (Teperi et al., 2021). Moving forward, it is better to understand the science, design science and how design science evolved as a methodology and as a process model throughout the research community.

According to (Simon, 1996), the traditional goal of "Science" is to develop knowledge about what exists through discoveries and analysis of existing objects. Furthermore, (Hegenberg 1969; as cited in (Dresch et al., 2014)) explains that science can be classified as: "factual science" and "formal science", where "*Factual science explores, describes, explains, and predicts phenomena and is validated when it provides some empirical evidence*" while "*formal science encompasses subjects such as logic and mathematics*". The authors also elaborate that factual science is divided into "natural science " and "social science". Physics, chemistry and biology disciplines are included in natural science and sociology, politics, economics, anthropology and history subjects are included in social science. The main goal of natural science is to understand a complex phenomenon, and the knowledge generated is descriptive and analytical, and this knowledge is valid for building a hypothesis (Romme, 2003, as cited in (Dresch et al., 2014)). Further, natural sciences mostly use positivist methods for extensively developing and testing theories (Venable, 2006). On the other hand, "*social sciences seek to describe, understand and reflect on human beings and their actions*," and social science research maintains proximity to the object of study, which is people (Romme 2003 as cited in (Dresch et al., 2014)). Due to the complexity and subjectivity of social reality, social science employs various methods, from positivism and interpretivism (Venable, 2006). Considering both social science and natural science research, they share a common mission to search for the truth, a goal to explain, describe and predict to improve the knowledge in a selected area of study (Denyer et al 2008 as cited in (Dresch et al., 2014). So, in nature, natural science starts with a "hypothesis", collects data and ends up approving or disapproving the hypothesis, which eventually leads to developing a theory (Hevner & Chatterjee, 2010).

The need for an alternative science, such as "Design Science", arose when researchers realised that conducting research using natural science or social science has limitations when the research goal is to study a design, construction or creation of a new artifact, as these sciences result in studies more focused on exploring, describing, explaining or predicting a phenomenon and their relationship (van Aken 2004; Gibbons and Bunderson 2005; Manson 2006; as cited in (Dresch et al., 2014)). Furthermore (Le Moigne; as cited in (Dresch et al.,

2014) highlighted that science that only engages in explaining a natural phenomenon is inadequate for the progression of science and knowledge. A similar idea (Hevner and Chatterjee, 2010) shares the problems that require creativity and novel and innovative solutions not sufficiently supported by natural science research. On this basis, "Design Science" was recommended as a new epistemological paradigm for the research community rather than natural science and social science (van Aken 2004; March and Smith 1995; Le Moigne 1994; Romme 2003; Simon 1996; as cited in (Dresch et al., 2014)). Table 7 shows the comparison between these sciences.

Table 13 - Synthesis—natural sciences, social sciences, and design science (Dresch et al., 2014)

Characteristic	Natural sciences	Social sciences	Design sciences
Purpose	To understand complex phenomena. To discover how things are and to justify why they are this way.	To describe, understand, and reflect on human beings and their actions.	To design, produce systems that do not yet exist; to modify existing situations to achieve better results. The focus is on solutions.
Research goal	To explore, describe, explain and predict.	To explore, describe, explain, and predict	To prescribe. Research is oriented toward solving problems.
Examples of areas that usually employ each of these scientific paradigms	Physics, chemistry, biology	Anthropology, economics, politics, sociology, history	Medicine, engineering, management

Authors (Hevner & Chatterjee, 2010) define design science research as "*a research paradigm in which a designer answers questions relevant to human problems via the creation of innovative artifacts, thereby contributing new knowledge to the body of scientific evidence. The design artifacts are both useful and fundamental in understanding that problem*". Fundamentally, design science research is considered a problem-solving paradigm (Hevner et al., 2004). The main goal is to produce an artifact that must be built and evaluated. The design process consists of a sequence of expert activities that build the artifact, and the

evaluation process of the developed artifact provides feedback information and the understanding of the problem to improve the quality of the artifact and the design process (Hevner et al., 2004). The knowledge created from design science research lets the researcher know how the developed artifact can be improved, is better than existing solutions, and efficiently solves the identified research problem (Vaishnavi & Kuechler, 2004). Design science creates innovative ideas, products, best practices and technical capabilities via analysis, design, implementation and management (Denning 1997; Tsichritzis 1998; as cited in (Hevner et al., 2004)). Furthermore, (Hevner, 2007) elaborates design science research contains three important research cycles: “Relevant Cycle”, “Design Cycle”, and “Rigor Cycle”, as shown in Figure 8.

- Relevant Cycle - bridges the gap between contextual environment and the design science activities in the research.
- Design Cycle - an iterative activity iterating between “Build Design Artefact and Process” and “Evaluation” of the research.
- Rigor Cycle - The knowledge base: scientific theories and methods, experience and expertise, Meta artefacts and the design science activities.

Figure 9 - Design Science Research Cycles (Hevner, 2007)

(Hevner, 2007) Suggest that these three cycles must be presented and identifiable in any DSR project. A motive of design science is to produce new or innovative artifacts and the processes to develop these artifacts to improve the environment (Simon 1996; as cited in (Hevner, 2007). The environment is where the problem & opportunity can be observed or lie in the

selected phenomenon, including the people, organisations and technology. The knowledge base is the existing body of knowledge that other researchers have contributed or developed previously in the form of theory or artifacts (Dresch et al., 2014). Design Science Research is between the “Environment” and “Knowledge Base”.

Relevance cycle –The environment initiates the researcher's need or problem. Then, the researcher frames the research activities to address the need or to find solutions to problems. In theory, the results generated by the “artifacts” can be used by the people attached to the organisation to improve their practice, meet their needs, or solve their problems. (Dresch et al., 2014). So, this journey assures the research’s relevance. Further, the relevance cycle allows research and an opportunity to evaluate the results (Hevner & Chatterjee, 2010).

Design cycle – This is an internal component of the design science research project. This cycle iterates within the construction of the artifact and evaluation of the developed artifact (Hevner, 2007). The evaluation cycle’s results feed into the design to refine and ensure that the original requirements are met in the design (Hevner, 2007).

Rigour Cycle -The rigour cycle refers to the quality of the research, which is detailed, accurate, and carefully conducted, and the completeness of the research. So, the research is valid and reliable and contributes to the existing body of knowledge or to improve it (Dresch et al., 2014).

Considering the three cycles, the relevance cycle enables the identification of problems from the environment and provides requirements as input to the design cycle to design the artifact, while the rigour cycle provides the theories and methods to evaluate the design from the knowledge base (Hevner, 2007). Moreover, (Hevner, 2007) highlights that the most challenging work of design science research lies in the design cycle. The outputs of DSR, the “artifacts” include constructs, Models, Frameworks, Architectures, Design Principles, Methods, Instantiations and Design Theories (Vaishnavi & Kuechler, 2004). Table 8 shows the outputs of DSR the “artifacts”.

Table 14 - Outputs of Design Science Research (Vaishnavi & Kuechler, 2004)

#	Output	Description
1	Constructs	The conceptual vocabulary of a domain.
2	Models	Sets of propositions or statements expressing relationships between constructs.
3	Frameworks	Real or conceptual guides to serve as support or guide.
4	Architectures	High-level structures of systems.
5	Design Principles	Core principles and Concepts to guide design.
6	Methods	Sets of steps used to perform tasks—how-to knowledge.
7	Instantiations	Situated Implementations in specific environments that do or do not operationalise constructs, models, methods, and other abstract artifacts: in the latter case, such knowledge remains tacit.
8	Design Theories	A prescriptive set of statements on how to do something to achieve a specific objective. A theory usually includes other abstract artifacts such as constructs, models, frameworks, architectures, design principles, and methods.

To enrich the design science research, (Peffers et al., 2006) suggest that it is adequate to have a conceptual model for researchers to conduct the research and a mental model or a template for readers to understand the research as well as for reviewers to evaluate the research. To fulfil this, (Peffers et al., 2006) presented the DSRM Process Model, which consists of six steps: Identify the Problem & Motivation, Define the Objectives of a Solution, Design &Development, Demonstration, Evaluation and Communication. Figure 9 shows the Design Science Research Methodology (DSRM) Process Model.

Figure 10 - Design Science Research Methodology (DSRM) Process Model (Peffers et al., 2007b).

The attractiveness of this process model is that it provides an avenue for the researcher to enter the process model in four possible research entry points: “Problem Centred Initiation”, “Objective Centred Solution”, “Design and Development Centred Initiation” and “Client/ Context Initiated”.

The specific steps involved in the DSRM process model’s six steps are further explained below based on (Peffers et al., 2007).

1. Problem identification and motivation
    a. Define the specific research question/ questions
    b. justify the value of a solution
2. Objectives of a solution
    a. Infer the objectives of a solution from the problem definition
3. Design and development
    a. Create the artifactual solution. Such artifacts are potentially, with each defined broadly, constructs, models, methods, or instantiations
4. Demonstration

    a. Demonstrate the artifact's efficacy in solving the problem. This could involve using it in experimentation, simulation, a case study, proof, or other appropriate activity.
5. Evaluation
    a. Observe and measure how well the artifact supports a solution to the problem. This activity involves comparing a solution's objectives to observed results from using the artifact in the demonstration.
6. Communication
    a. Communicate the problem and its importance, the artifact, its utility and novelty, the rigour of its design, and its effectiveness to researchers and other relevant audiences.

3.6 Research Methodology Justification

This research focuses on the phenomenon of "IoT network security in Digital Health Systems," specifically, how to secure IoT networks proactively in digital health. A proactive Defence Framework is a framework that caters for the constant evolution of security threats.

Considering the research relevance, the environment, in this case, is the "Digital Health Space" where People, Organisations and Technology provide the opportunity to identify the problem "How to secure the IoT networks in digital health proactively?". People include users, implementers, and healthcare personnel. Organisations are the Healthcare service providers such as Clinics, Aged care facilities, SMART elder homes, and hospitals. The technology refers to Internet of Things (IoT) devices, architecture, platforms, networks, and communication, including both hardware & software components, technologies used and the end-to-end data flow. The design cycle provides the opportunity to design the artifacts to address the research questions and the evaluation to ensure the design meets the original requirements of the research. The rigour is addressed using the appropriate approach to evaluate the developed artifact as a desk study (1st pass) and feed the results to improve the design. Also, use the expert interview approach for further evaluation and a theoretical contribution to the digital health literature through an adaptable framework for the proactive defence of IoT networks. DSRM provides the nominal process to conduct the research step by step with four possible entry points. Academic literature, industry security reports, and grey literature were used to identify the research problem. Therefore, the "Problem Centred Initiation" entry point was used in this research. On the other hand, the mental model provides the structure to present the research output.

3.7 Research Design

The research design consists of five major phases: Identifying security elements for the framework, Draft Framework, Demonstration of the framework, Validation and Final framework. Following the DSRM process model with six steps and the four possible entry points, the "Problem Centred Initiation" entry point was selected as the academic literature, industry security reports and grey literature were used to initiate the research problem.

Each primary phase consists of activities and sub-activities. Figure 10 shows the detailed research design with a mapping of the DSRM process steps.

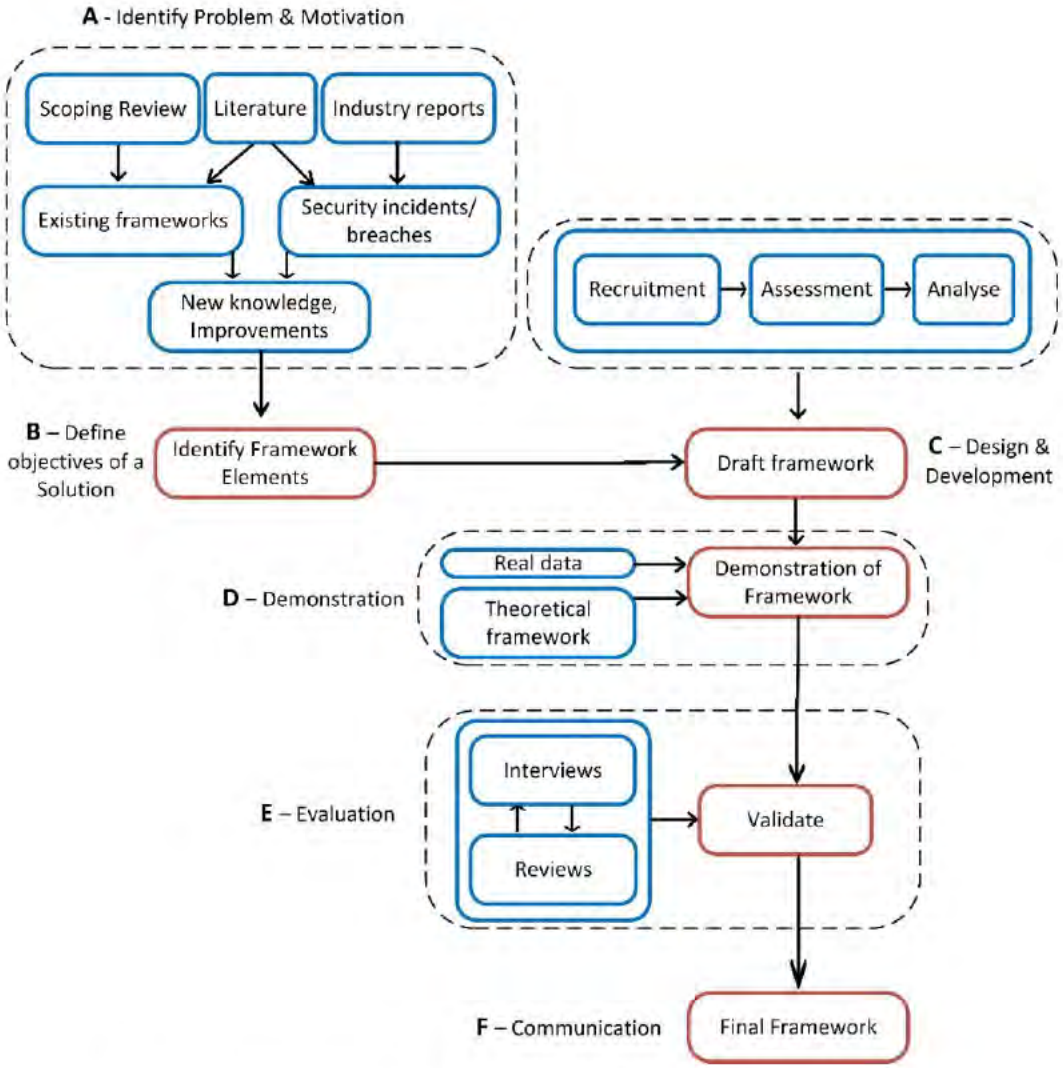


Figure 11- Detail design of the proposed research design.

Identify framework elements – The main objective of this phase is to identify the framework's elements. Results of the scoping review and existing literature are used to understand the security posture of the IoT-based digital health systems, the nature of the existing security frameworks developed, the focus and target of such frameworks, the kind of proactive mechanisms/ techniques and the type of technologies used. Leading industry report data is used to understand the current and evolving security landscape, an overview of the security incidents/ breaches, the trends of threats and vulnerabilities, the common attack surfaces, and the global cyber security outlook. Analysing literature, including grey literature and industry data, will pave the way to understanding the gaps, the direction of new knowledge discovery, and the improvements needed.

Draft framework – This phase positions the identified security elements in the framework and organises them logically into a view that builds upon highlighting the relationship between the elements and the flow.

Demonstration of the framework – Using a desk study. The main objective of this phase is to prepare and validate the framework. This will incorporate the theoretical framework applied to real-world IoT networks in digital health systems selected from academic literature.

Validate – In this phase, the framework is validated through expert reviews.

Final framework – Finalise the framework based on validation results.

Figure 11 shows the phases of the research design aligned with the design science research methodology process model.

Figure 12 – Research Design Phases Aligned with Design Science Research Methodology

3.8 Research Methodology challenges and limitations

The methodology relies on iteration, and the Evaluation and Communication activities often identify where revision in design is necessary. Thus, the whole design science process creates a cyclic re-iteration loop with the design, and the method can result in persistent revisions if the scope is not well defined. Further, Carlsson (2005) suggests that consideration of real-world applications and events, as in critical realism, is needed during the research process to discern between the theoretical and practical application of the methodology.

The success of the artifacts produced from the research will depend on the evaluation, which tests the artifacts in different contexts iteratively (Peffers et al., 2018). This research uses expert reviews and interviews to evaluate the artifact and a desk study to demonstrate the implementation. Therefore, this study may be limited to a specific context, such as the knowledge of the experts, the number of experts recruited and the case study selected. Using a case study may limit the generalizability to other real-world settings. Further, such

evaluation may involve collecting highly confidential and sensitive security information, so disclosing such information may be limited. Further evaluation of the artifact can be complex if it needs to be tested in a real-world environment due to time and resource barriers. This may impact analysis by not capturing the whole image of a digital health system.

Summary

This chapter discussed research, research paradigms, and research approaches in general. Specifically, information system research, design science research and design science research methodology are presented, and their use in this research is justified. This research is based on interpretivism philosophy, utilising a mixed approach. The design science methodology is used as the overarching methodology to conduct the research.

The next chapter presents the design and development of the main artifact, the security framework.

4. DESIGN AND DEVELOPMENT

This chapter presents the proposed framework. The rationale behind each element of the framework and their relationship within the framework is explained. Further, each element identified in the framework is described using the design science activity two, “Define the Objective of a Solution”.

4.1 Overview of the Framework

Given the framework categories discussed in literature review section 2.4, characteristics of purpose, development process and structure matched the research question, “How can a framework be developed and applied for proactive defence for IoT network security in digital health?

Purpose - Development Framework - Supports the development of information systems or new system features from either a technical perspective, general perspective, or both.

Proactive Defence means catering to the constant evolution of security threats. Developing such a framework needs to consider preventing cyber security incidents, and where an incident happens, detect and prevent it from a technical perspective. In addition, the protection of IoT networks in digital health systems needs to be looked at from a general perspective about patient safety, improving productivity, improving business continuity, and preventing financial losses. Therefore, this supports developing an information system from technical and general perspectives.

Development process – Mixed-developed Framework, Supports the development of framework using multiple development categories.

Regarding the development process, identifying framework elements to address contemporary IoT security concerns in digital health systems is broad and complex.

Development of such a framework involves an in-depth analysis of literature and industry publications, assessment of current security systems, development of improvements, new insights, and new areas. A mix of Literature Review Developed, Research Developed and Requirements Developed is used.

Literature Review Developed Frameworks – Frameworks are developed through an academic literature review. A scoping review was conducted to capture the necessary information from the academic literature about existing security frameworks. An extensive search strategy was carried out using four different academic electronic databases.

Research Developed Frameworks - Frameworks are developed using existing research. E.g., existing theories, models and frameworks. Further analysis of academic literature, grey literature, and web resources was used to deeply understand the IoT environment, including devices, architecture, platforms, networks, current IoT technologies, and security solutions.

Requirements Developed Frameworks - Frameworks are developed to fulfil identified requirements. Leading industry reports/ publications were used to understand the current and evolving security landscape, an overview of the security incidents/ breaches, the trends of threats and vulnerabilities, the common attack surfaces and the cyber security outlook globally to identify the requirements to fulfil in a proactive defence security framework.

Structure - Mixed structure Framework

The proposed security framework uses a mix of technical, component, and sequence structures described below.

Technical Structured Frameworks - These frameworks have technical components and detailed descriptions. The identified framework security elements consist of technical components, and their roles are well described in the framework development process.

Component Structured Frameworks - These frameworks have component-based structures, and components describe the framework and their interrelationship. The conceptual view of the proposed framework highlights the relationship between the framework's security elements, and three main components can be seen. The interrelationship within these components is explained later in the chapter.

Sequence Structured Frameworks - These frameworks consist of activities performed in a sequence. Applying the framework, a step-by-step process and a list of activities to perform sequentially can be seen in this framework.

4.2 Overview of the Proposed Security Framework

Securing digital healthcare IoT networks presents challenges. The space is critical and complex because multiple systems are integrated and interconnected to deliver the required services and care. This complexity contributes to the lack of visibility in the IoT Network. This includes a poor understanding of the type of devices used, where they are deployed, device connectivity, network connectivity, and technologies used. The proposed security framework is crucial in addressing the challenges of securing digital healthcare IoT networks. Its application process, particularly in the "Identification" and "Mapping" phases, contributes to identifying the IoT Network Segments and Components and mapping them to the IoT architecture. This enables the visibility of the IoT Network. The rich visibility gained by mapping the IoT network segments and components to IoT architecture ensures the framework security elements are applied to IoT network components in every layer, providing a multi-layer secured architecture.

The following section describes the proactive defence security framework construction, security elements of the security framework and the relationship between these elements. Elements were identified through the scoping review, analysis of the academic literature and analysis of grey literature and industry security reports. The mix of these sources provided the opportunity to understand the security posture of the IoT-based digital health systems, the current and constantly evolving security landscape, security incidents and breaches, trends of threats and vulnerabilities, the common attack surfaces, security challenges and the cyber security outlook globally. These understandings paved the way to identify the gaps in frameworks found in literature, the direction of new knowledge discovery, and the improvements needed to strengthen the security of IoT networks.

To construct the draft framework for this research, findings from a scoping review, academic literature, industry security reports and grey literature were used. Security concerning the Internet of Things (IoT) devices, architecture, platforms, networks and communication were focused on to identify the potential elements for the framework. One of the main

expectations was to use the existing resources and current technologies rather than invest in developing new or novel components. Opportunities have been examined to enhance existing resources and use current technologies to improve and increase the framework's effectiveness. The main areas of IoT security, as well as IoT security weaknesses and failures, were considered during the framework's development.

The framework is anticipated to apply to existing and new IoT networks. New networks would be able to follow the framework during the design phase of the network. The three main characteristics of information security: confidentiality, availability, and integrity were major priorities during the framework's construction.

The proposed framework consists of nine elements: Threat Landscaping, Threat Modelling, Access Control, Data Security, Intrusion Detection and Prevention, Security Forensics, Security Information Sharing, Security Policies and Standards, and Security Gap Analysis. Figure 12 shows the proposed proactive defence security elements.

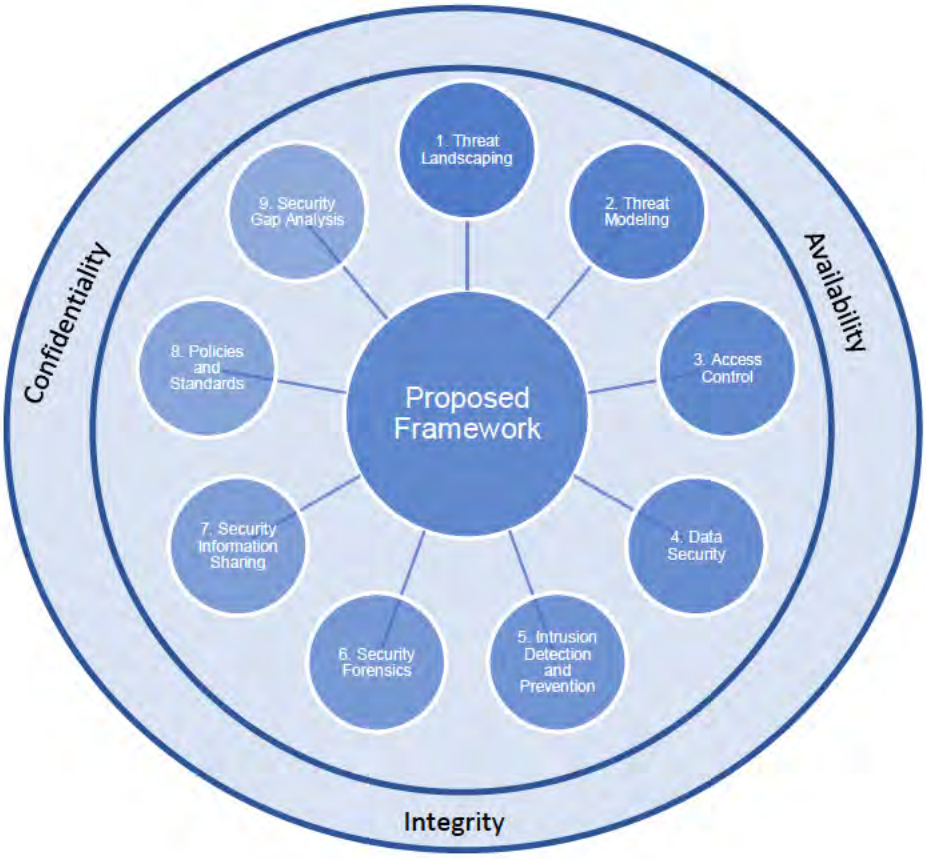


Figure 13 – Proactive Defence Security Elements

To be proactive in cyber defence, it is essential to ensure the strength of Information and communication technology systems against threats and vulnerabilities. Identifying the associated threats and vulnerabilities in a given context and addressing them is challenging without the correct mechanisms.

1. **Threat landscaping** refers to the complete understanding of existing, most recent (classified as unknown incidents) potential threats, their behaviour, and how they can affect the network system and knowing these facts in detail will help understand the threat environment and the risks (Chatzis & Stavrou, 2022; Pirc et al., 2016). The findings from this activity provide the necessary information for security element "Threat modelling".

2. **Threat modelling** is defined as “a process that can be used to analyse potential attacks or threats and can also be supported by threat libraries or attack taxonomies” (Uzunov & Fernandez, 2014). The key expectation of threat modelling is to eradicate, prevent, minimise or mitigate the impact that can happen to an ICT system from threats (Xiong & Lagerström, 2019). With a sound understanding of the impact on information and communication technology systems, threat classifications and test cases can be developed in the threat modelling activity by identifying threats from the threat landscaping activity (Aufner, 2020). Based on the testing results, decisions can be made to implement preventive actions. Threat modelling is a challenge as the threat landscape is constantly evolving. Therefore, threat modelling is iterative (Kamatchi & Ambekar, 2016). Various modelling methods are discussed and used: manual, automatic, formal and graphical (Xiong & Lagerström, 2019). Formal modelling methods are based on mathematical models and graphical modelling using tables, attack trees and graphs (Xiong & Lagerström, 2019). Several threat modelling methods are available, but applying them to IoT is limited as they focus on application development (Aufner, 2020). It is hard to find a tailor-made method to suit IoT networks. Therefore, a method or combination of methods needs to be investigated to apply and customise to meet the requirements. The focus can be on IoT architecture throughout the data acquisition, transmission, processing, and application phases. An approach proposed by (Tatam et al., 2021), which focuses on four areas: “asset-centric, system-centric, threat-centric and data-centric” can be adopted based on the IoT network. Figure 13 shows the threat modelling approach focusing on the four areas. The next security element is “Access Control”.

Figure 14 - Threat modelling approach (Tatam et al., 2021)

3. **Access Control.** IoT networks are defined as a collection of interconnected devices, such as sensors, actuators and machines that communicate using wired or wireless communication channels (Tahir et al., 2020). In each architecture, three-layer or five-layer or the Cloud and Fog of the IoT network, devices in each layer or the stage play multiple roles: sensing, identification, acquisition, communication and management. Implementing appropriate security measures for IoT devices, communication channels, and associated data is crucial (Pal et al., 2020). Therefore, Access Control plays a vital role in IoT networks as it needs to implement identification, authentication, authorisation and accountability for the devices to preserve confidentiality, integrity and availability (Li et al., 2016; Pal et al., 2020). The main objective of implementing access control at various levels is to limit network access and communication only to legitimate entities (Pal et al., 2020; Ravidas et al., 2019). A combination of policies, programmes and technologies can be used to implement Access Control (Whitman & Mattord, 2022). Access control can be implemented in the device, user, communication, data, and location or based on capabilities (Khan et al., 2017) or based on Discretionary access control (DAC), Mandatory access control (MAC), Role-based (RBAC), Attribute-based (AAC) or Rule-based (RuBAC) (Whitman & Mattord, 2022). The next security element is “Data security”.

4. **Data Security**. Data obtained from IoT devices in a healthcare setting are used to make clinical decisions, treatments, diagnoses, drug management and improve patient experience (Abouelmehdi et al., 2017; Li et al., 2010). Therefore, data cannot be lost, tampered with, or damaged as it affects their usage. Failure to obtain CIA-preserved data will prevent a patient from being treated effectively or even lead to incorrect treatments (Li et al., 2010). Worse case scenarios include compromised treatments, such as incorrect dosage of medications and delay in treatment, which can cause serious harm or loss of life (Abouelmehdi et al., 2017). Therefore, Data Security is an area that needs to be paid attention to, and security measures must be applied during the data acquisition, transmission, processing, application and storage phases. Also, healthcare service providers need to adhere to the data protection laws imposed by the government (Abouelmehdi et al., 2017; Tomašić et al., 2017). The next security element in the proposed security framework is "Intrusion detection and prevention systems".

5. **Intrusion Detection and Prevention Systems**. Threat landscaping and threat modelling help to identify the existing threats but limit the opportunity to identify potential threats. It is very important to detect and prevent attacks in IoT in digital health systems because failure in this space may impact the patient's life. This is where IoT networks need technology-driven solutions to identify any anomalies or malicious intrusions. **Intrusion Detection Systems** can be used to detect anomalies or malicious intrusions or new attacks in an IoT network and to make alerts (Elrawy et al., 2018). Detecting suspicious activities and new attack trends contributes to threat intelligence, updating the threat landscaping and threat modelling. On the other hand, **Intrusion Prevention Systems** need to be implemented in IoT networks to take preventive actions where possible once the detection system is alerted of a possible intrusion without human involvement (Fuchsberger, 2005). Artificial Intelligence (AI), Machine Learning (ML), Deep Learning (DL), Neural Networks (NN) and Software Defined Networks (SDNs) have been used to develop intrusion detection and prevention systems (IDPS) (Chang & Hsieh, 2018; Hodo et al., 2016; Myers et al., 2019). As IoT devices are incapable of running software programs by themselves due to low processing power and memory constraints, network-based IDPS systems need to be

used. These should focus on implementation across different layers and target the data transmission process using various methods and techniques. The next security element is “Security forensics”.

6. **Security Forensics.** Once an intrusion or suspicious activity is detected or prevented by the IDPS, it is important to investigate the incident further. This is where Security forensics needs to be conducted to find more information about the incident. Even though this is a reactive activity, the main objective is to input the findings of such investigation to the security information sharing and for research purposes to identify potential threats and to feed the threat intelligence. The next security element is “Security Information Sharing”.

7. **Security Information Sharing.** The threat landscape is evolving. To keep up with this situation, sources that provide information about existing and potential threats must be updated as soon as new information is available. Therefore, Security Information Sharing is important to keep the information sources updated and available for access (Pirc et al., 2016). The main objective of this security element is to share threat information internally and externally and to use such information to take preventive actions and to improve the security posture. Also, threat information sharing will contribute to expanding threat intelligence and continuous improvements to be proactive by knowing the facts before and being immune to the IoT networks. Moreover, the latest security information can be used by security policymakers/ developers to update existing policies or introduce new ones. The next security element is “Security Policies and Standards”.

8. **Security Policies and Standards** are an integral part of any organisation to state how the CIA triad is treated. Security policies provide directions to handle security issues and how technology can be used to accomplish this (Whitman & Mattord, 2022). Importantly, policies are focused on the CIA, overlooking the sensitive data and meeting the regularity requirements. Once the policies are in place, standards are to accompany the policies to comply with them by providing detailed statements (Aly et

al., 2019; Whitman & Mattord, 2022). The next security element in the proposed security framework is “Security GAP Analysis”.

9. Security GAP analysis

A GAP analysis is conducted to identify differences between a current and a targeted state of concern: technology, process, market, product, etc (Rasmussen et al., 2018). A security GAP analysis is an in-depth review to identify gaps in the organisation’s current security posture in ICT systems. A GAP analysis is conducted using industry best practices for comparison. The results of a security GAP analysis highlight whether the level of security in the organisation is low compared to industry best practices.

A failure to secure the primary network presents a vulnerability. A security GAP analysis of the primary network infrastructure is proposed in this framework as a recommendation. While the security of the primary network is extremely important, ultimately, it is outside the scope of this research other than to highlight the need to be proactive about the security of the primary network.

The key steps in a security Gap Analysis are listed below.

1. Select a security standard
2. Evaluate people and processes
3. Gather data
4. Analysis

A conceptual view, presented through three major viewpoints, is designed to guide the practical implementation of the proposed security framework. As shown in Figure 14, this conceptual view shows the logical arrangement of the security elements. Further, these security elements were allocated to four implementation stages, as shown in Figure 15. Additionally, a six-phase implementation guide is introduced to facilitate and streamline the implementation of the proposed security framework. This process is further elaborated in Section 4.5 and Chapter 5—Demonstration with working examples.

4.3 The conceptual view of the proposed framework

The elements identified in Figure 12 can be logically organised into a conceptual view that builds upon highlighting the relationship between the elements and the flow. Figure 14 shows the conceptual view of the proposed security elements in the framework. Three major viewpoints can be seen.

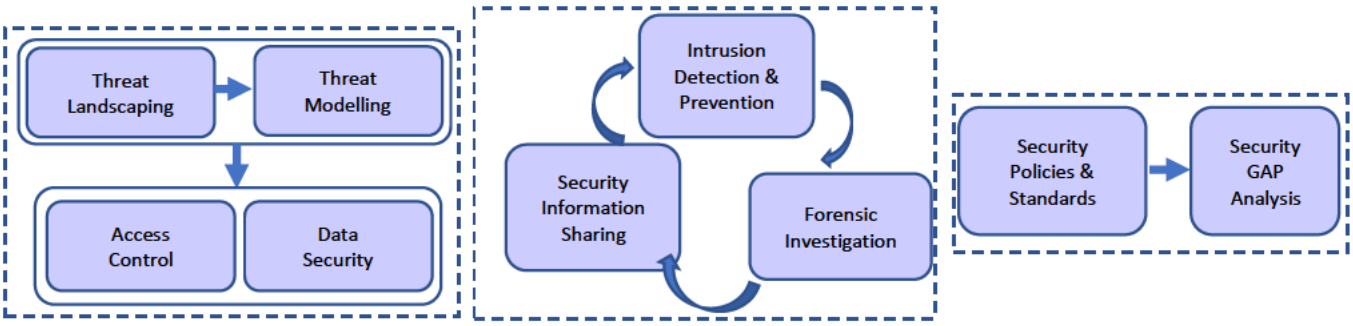


Figure 15 - Conceptual view of the proposed security elements in the framework

Due to the resource-constrained nature of IoT devices, which includes low processing power, less storage, battery life, and limited memory, some framework elements may not apply directly to IoT devices. Therefore, transforming the conceptual view (Figure 14) into a practical implementation requires stages of implementation. Four stages were introduced to fulfil this requirement: Preparation, Active monitoring and actioning, Contributing, and Strengthening. The arrangement between the security elements and the implementation stages is shown in Figure 15. Figure 15 highlights the relationship between each element and how the individual elements contribute to other elements within the framework to improve its functions and be more result-oriented. e.g., Threat landscaping contributes to threat modelling, forensic investigation findings contribute to information sharing, and information sharing will feed into threat intelligence.

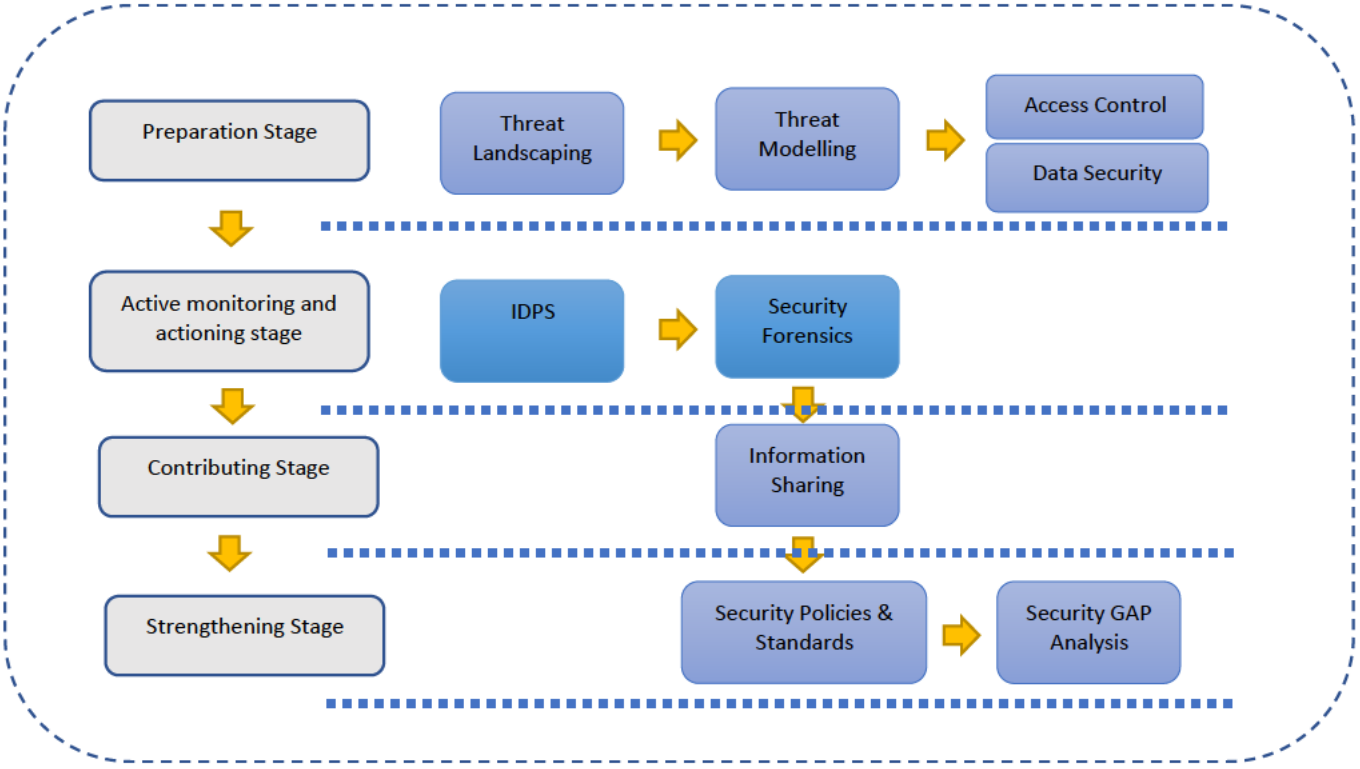


Figure 16 – Translation of Conceptual View Into Framework Security Elements Process and Stages

Preparation stage – This is the initial stage of applying the framework. This stage consists of four framework elements: Threat landscape, Threat modelling, Access control, and Data security. The main objective of this stage is to prepare each IoT architecture layer for proactive defence. Each IoT network infrastructure component will be closely looked at to find the relevant threat landscape. Threat classifications and test cases can be developed in the threat modelling activity based on the Threat Landscape. Threat modelling is to increase the defence. Identify weak areas and address them. The next element is to implement Access Control followed by Data Security.

Active monitoring and actioning stage – This stage consists of two framework elements: Intrusion Detection and Prevention (IDPS) and Forensic Investigations. IDPS is the active monitoring. Once IDPS detects any intrusion or takes any preventive measures, further investigations about the incident must be carried out. This is the activity of performing forensic investigations. The positioning of IDPS will be tactically looked at due to the resource limitation of IoT devices, as explained before.

Contributing stage – This stage consists of the "Security Information Sharing" framework element. The outcome of "Forensic Investigations" must be shared with other similar healthcare service providers and relevant security agencies. Sharing such Security Information contributes to keeping the security information sources updated and available for access. This information is needed to take preventive actions and to improve the security posture of the IoT networks. Also, Security Information sharing will contribute to developing threat intelligence.

Strengthening stage (next level) – This stage consists of two framework components: Security policies and standards and security GAP analysis. Policies are focused on security, overlooking sensitive data and meeting regularity requirements. Once the policies are in place, standards are to accompany the policies to comply with them. A security GAP analysis provides an in-depth review to identify gaps in the current security posture in ICT systems using industry best practices for comparison. The results of a security GAP analysis highlight the level of security compared to industry best practices.

This section explains the proposed proactive defence security framework elements and their interrelationship. The next section presents the application and implementation of the framework.

4.4 Application and Implementation of the Proposed Framework

To apply the security framework, it is first necessary to understand the general IoT architecture in digital health. This chapter describes a general IoT network in digital health in detail. The IoT network's architecture, infrastructure, technology and system operation are explained using figures. Further, applying and implementing the framework step by step is described using tables, figures and diagrams.

4.4.1 What does an IoT network in digital health look like?

The terms: Internet of Health Things (IoHT), Healthcare Internet of Things (HIoT), Internet of Medical Things (IoMT) and Mobile Internet Devices (MIDs) are used when IoT is used in the healthcare space. Also, the term "Wireless Body Area Network (WBAN)" is widely used in digital health as it is used for remote patient monitoring, assisted living, and vital sign

monitoring. WBAN integrates sensor nodes into the human body to acquire readings from body functions (Saleem et al., 2011). IoT-enabled assistive technologies have also assisted people with disabilities (Pal et al., 2020). IoT devices range from simple environmental sensors to bedside sensors, wearables, fitness trackers, gyroscopes, motion, vibration, and implantable and ingestible sensors. These devices have been used in many areas of digital health systems: simple room temperature monitoring to indoor occupancy monitoring, real-time remote monitoring, chronic disease management using wearable and implantable devices, remote care, fall detection, vital sign monitoring, disease detection, automated insulin delivery, connected inhalers, remote diagnosis, SMART elder care facilities, assisted living for differently-abled people, navigation systems with real-time guidance for blind people, health and fitness programmes (Istepanian, 2011; Pal et al., 2020). IoT devices can be deployed to collect, transmit, and share information across multiple platforms (Janjua et al., 2009; Volk et al., 2015). The core connection builds on a combination of People, Things and Data: P2P - person to person, M2P - machine to person and M2M - machine to machine (Bradley et al., 2015). These devices enable remote monitoring, remote care, and remote diagnosis, enhancing the service providers' capabilities, such as real-time data acquisition, processing, quick decision-making, and disbursing real-time treatments and care while ensuring patient safety. Also, using IoT devices in digital health systems contributes to reducing healthcare costs as it avoids hospital visits. On the other hand, these devices benefit people as they can monitor their personalised metrics, such as their fitness levels, heart rates, and steps from fitness bands or smart watches. Also, they can get real-time alerts about their specific health conditions, such as blood glucose readings or heart rate readings from the wearable or implanted device, and alert carers if support is needed. This promotes not only wellbeing but also patient safety. Moreover, IoT devices deployed for environmental monitoring, such as temperature and humidity monitoring in a drug storeroom or refrigerator in a healthcare facility, to alert to any changes in the controlled environment.

4.4.2 IoT Architecture

As described in sections 1.5 and 1.6 of Chapter 1, "Introduction," the digital healthcare space is critical and complex because multiple systems are integrated and interconnected to deliver the required services and care. Also, IoT security concerns in digital health systems are broad and complex. Implementing a proactive security solution to an IoT network requires a

thorough understanding of the IoT ecosystem: IoT devices, how they are interconnected, network media used, software and hardware components and technology used in the network and end-to-end data flow. On the other hand, to understand the IoT ecosystem, need to have a clear picture of the architectural structure of the IoT network. Therefore, a layered architecture is required to explain and understand the operation of an IoT network. As described in section 2.1.1 (Evolution of the IoT Architecture, Chapter 2), the three-layer architecture is considered the basic architecture for IoT networks. The five-layer architecture extended from the three-layer architecture by introducing the transport, process and business layers. For the purpose of explaining and understanding the broadness and complexity of IoT networks in this research, the basic architecture, the three-layer, the extended architecture, and the five-layer were selected. The core relation of the layers, segments and data flow of an IoT network is demonstrated in Figure 16.

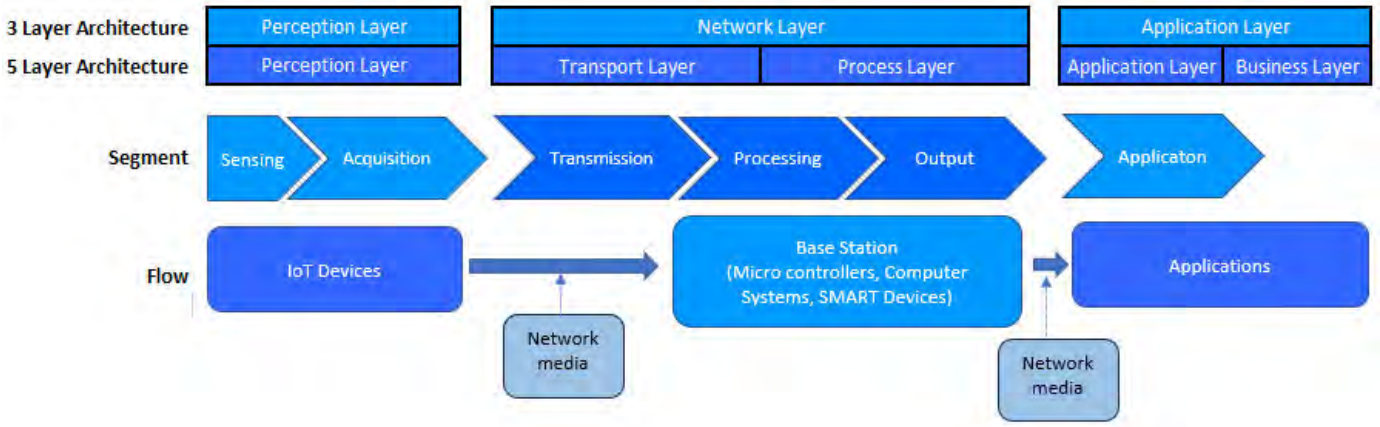


Figure 17 – Relation between the Layers, Segments and Data Flow of an IoT Network

4.5 Applying the Proposed Security Framework

Applying the proposed security framework, as shown in Figure 15 (Section 4.3), consists of six phases. Figure 17 shows the six phases of applying the proposed security framework.

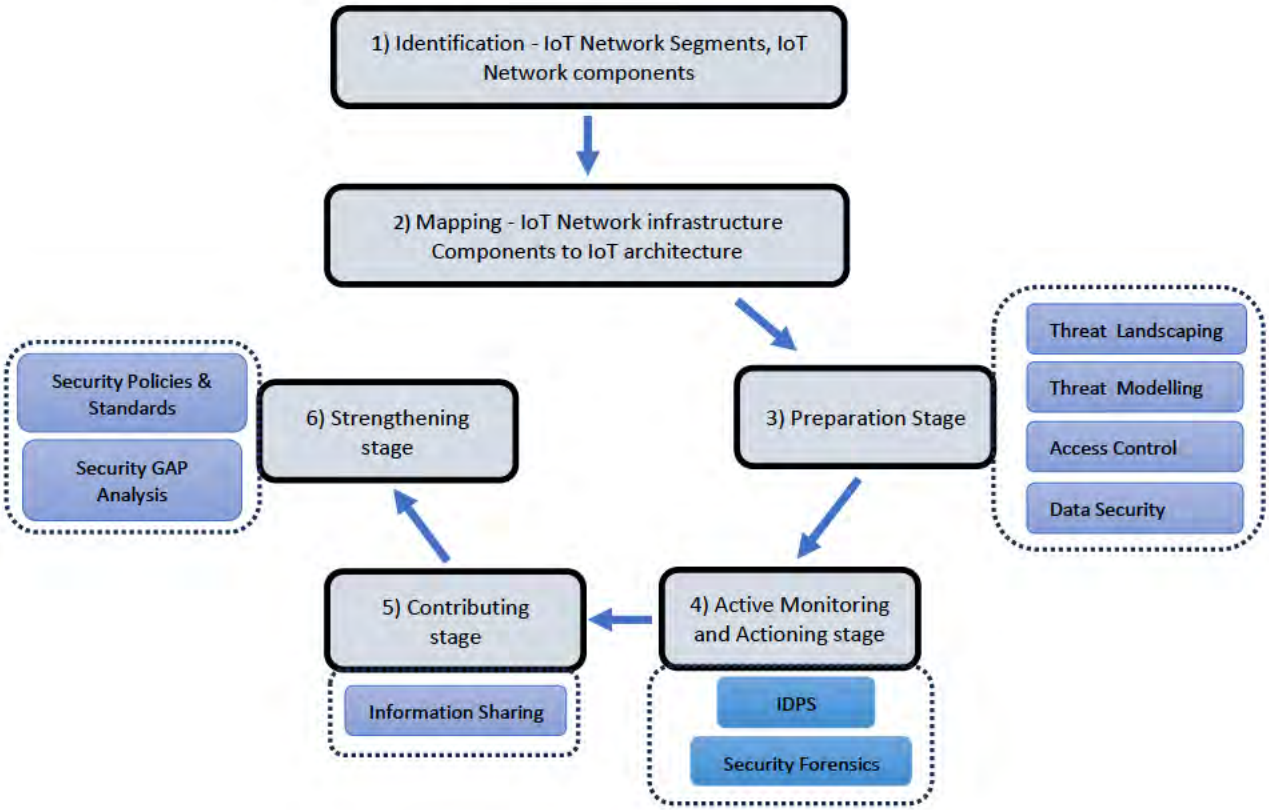
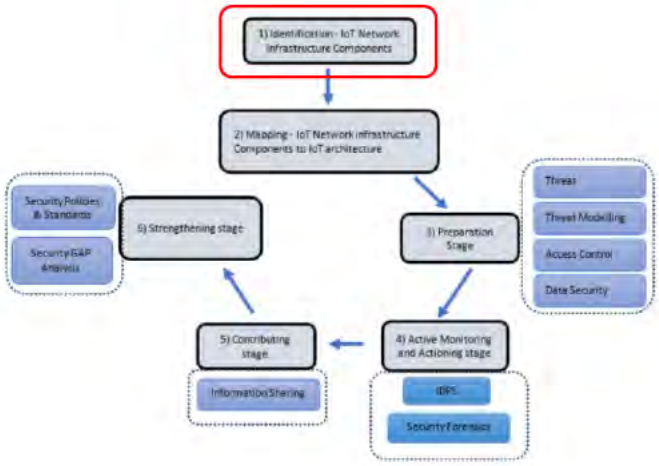


Figure 18 – Main Phases of Applying the Framework

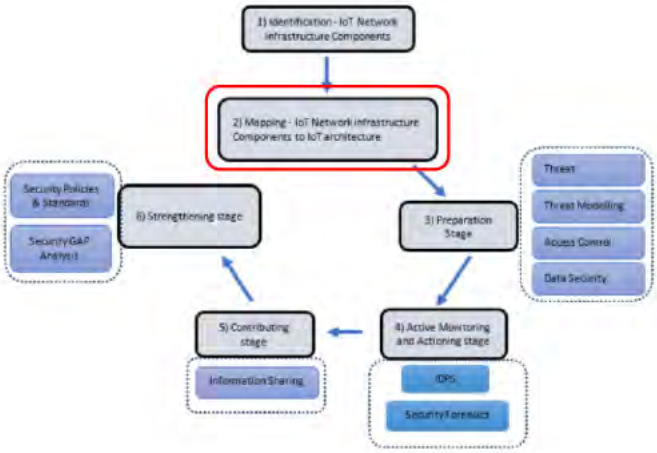
The six phases are explained in the following section. Chapter 5, "Demonstration of the Framework", provides a workable example of the proposed security framework.

4.5.1 Identification - IoT Network Segments and IoT Components



This is the starting point for applying the proposed security framework. A thorough understanding of the target IoT network is essential. As Steve Alder (2019), chief editor of HIPAA Journal, pointed out, *"One of the main problems with securing IoT devices is a lack of visibility into all connected devices, which is especially poor in the healthcare industry".* The visibility can be gained by identifying the segments of the IoT network, its underlying hardware and software components, the technologies used, and the end-to-end data flow. This creates visibility of the whole IoT network infrastructure and effectively enables the practical application of the proposed security framework. Visibility is essential as it gives a rich understanding of the IoT environment, including the type of devices used, where they are deployed, device connectivity, network connectivity and technologies used. “Effectively” means to produce the expected results from the security elements by placing them in the right position.

4.5.2 Mapping - IoT Network Infrastructure Components, Segments to the IoT Architecture



The IoT network segments and underlying components identified must be mapped to the IoT architecture. This will give a picture of the components and their position mapped to each architecture layer. This will ensure the framework security elements are applied to IoT network components in every layer, providing a multi-layer secured architecture. The framework can apply on a component basis on each layer based on the three- or five-layer architecture. For instance, for a sensor in the perception layer, wireless technology in the network layer, and a website in the application layer.

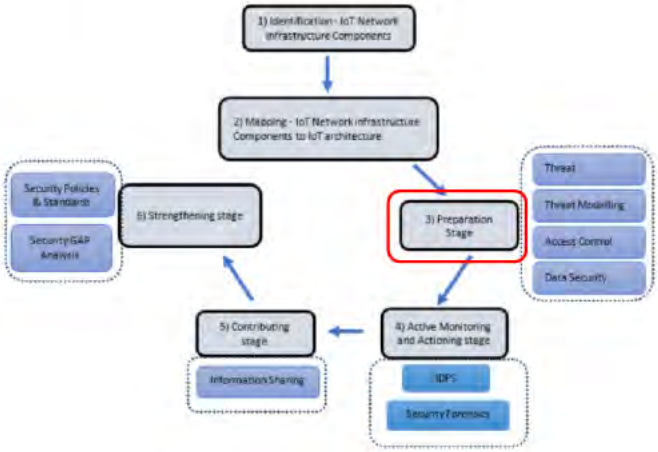
In an IoT network, the possible IoT network segments, components and the IoT architectural layers are positioned as illustrated in Table 12 together with examples. The network components include both hardware and software. E.g., IoT devices, network media, servers, desktop PCs, laptops, tablets, mobile phones, microcontrollers, programming languages, messaging protocols, communications protocols, operating systems, software programs, mobile apps, websites, etc.

Table 15 – Examples of typical IoT Network segments based on the IoT architectural layers.

3 - Layer	5 - Layer	Segment	Details
Perception	Perception	Sensing	Wearable devices – SMART watches, location sensors, heart monitoring sensors, etc. Implantable devices – Blood glucose monitors, swallowable capsule cameras, and embedded cardiac sensors (Alsubaei et al., 2017). Ambient devices – Sensors: temperature, humidity, motion, vibration etc. Stationary devices – Imaging devices (CT, X-ray, MRI), ECG, etc.
Perception	Perception	Data Acquisition	Gathering data from the physical phenomena by sensors
Network	Transport	Transmission	3G, 4G, 5G, Wi-Fi, Mesh, WiMAX, ZigBee, Bluetooth, RFID, Wired Message queues – Constrained Application Protocol (CoAP), Message Queue Telemetry Transport (MQTT), Rabbit MQ
Network	Processing	Base station	Microcontrollers - Arduino boards, Raspberry Pi, Photon Computer systems – Desktops, Laptops, Servers, Cloud applications Smart devices – tablets, mobile phones
Network	Processing	Processing	Data processing
Application	Application	Application	Data storage – Database management systems. I.e., MySQL, SQL, MongoDB etc Monitoring – Fall detection, Glucose monitoring, Visualising – Patterns Alerts – Care person Diagnosing – Disease
Application	Business	Business application	Data analytics – big data applications Business intelligence – decision making, automation SMART homes

Once the identification and mapping are completed, the framework can be applied to the selected IoT network. The process starts with the Preparation stage, then the Active Monitoring and Actioning stage, the Contributing stage and finally, the Strengthening stage. These stages are described in the following sections of this chapter.

4.5.3 Preparation Stage



The preparation stage consists of four security elements from the proposed security framework: threat landscaping, threat modelling, access control and data security. Figure 18 shows the IoT architectural layers of the three- and five-layer models and the four framework security elements. The perception layer identifies objects and senses, gathers information, and sends the collected data to the next layer. The network layer transmits and processes information. The application layer delivers application-specific services to the user. The order maintained throughout the research is the perception, network, and application layers.

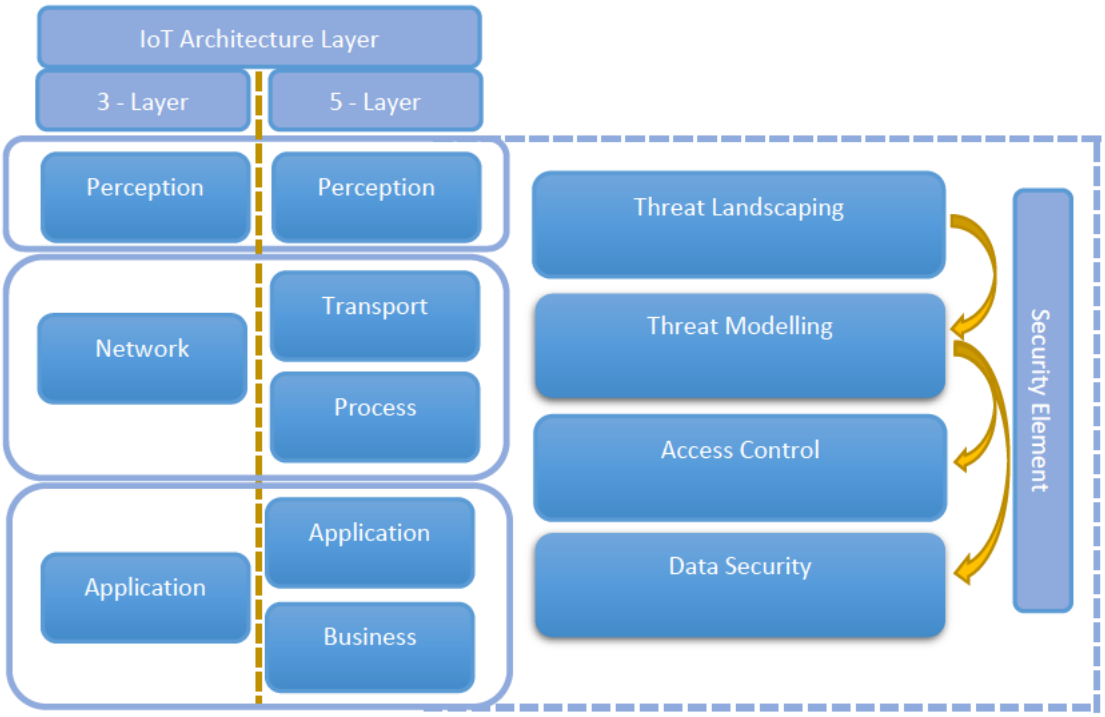
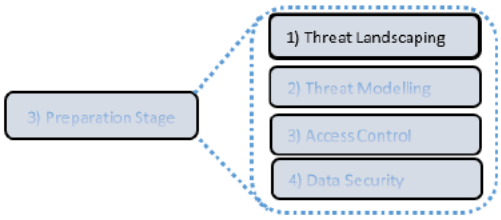


Figure 19 – IoT Architectural Layers and the Four Framework Elements

The four security elements are organised in a logical sequence in the preparation stage. Each security element can be applied to each architectural layer. For instance, apply the "Threat landscaping" for sensors in the perception layer. Then, the identified threats to the sensors will be modelled. The arrows show a direction but are not necessarily linear. For example, once threat landscaping and modelling are completed, access control or data security can start. For better protection, iteration and revision within elements is essential.

4.5.3.1 Threat Landscaping



The preparation stage (phase 3 in the application of the framework) starts with "Threat landscaping". Knowing state-of-the-art threat information is essential as the threat landscape evolves. Threat information refers to existing, most recent, and potential threats, their behaviour and how they affect an IoT network. Obtaining this threat information will be challenging without the correct mechanisms. Figure 19 shows these mechanisms and

how a threat landscape can be developed using information sources, threat intelligence and human expertise. Website addresses are sources where the content can be downloaded to complete the "Threat Landscape" using common vulnerability exposures (CVE) databases and web resources.

Figure 20 - Threat Landscape Information Sources

Publicly disclosed Threats and Vulnerabilities

Publicly disclosed cybersecurity threats, vulnerabilities, and exposures can be found in literature, including grey literature, published industry security reports, common vulnerability exposures (CVE) databases, and web resources. A common vulnerabilities exposures (CVE) database contains threat catalogues for identified and defined threats. These CVEs are built upon once organisations worldwide discover, assign, and publish vulnerabilities (www.cve.org). These databases, referred to as catalogues, are accessible from www.cve.org. The National Vulnerability Database (NVD) is another publicly accessible source. This service is provided by the National Institute of Standards and Technology (NIST) and is accessed from the website www.nvd.nist.gov/vuln.. Further information about publicly disclosed cybersecurity threats, vulnerabilities and exposures can be obtained from government websites (https://www.cyber.gov.au/about-us/view-all-content/alerts-and-advisories/2022-top-routinely-exploited-vulnerabilities, https://www.cisa.gov/known-exploited-vulnerabilities-catalog), vendor-specific websites (https://resources.trendmicro.com/2022-Public-Vulnerability-Market-Report.html), etc.

Threat intelligence – This is gaining rich evidence to discover reliable information on potential threats, threat patterns, revealing motives, techniques and tactics of adversaries and attack trends as attacks become more extensive and complex—e.g., Intrusion detection and prevention systems, Online sources such as “www.crowdstrike.com”, https://flare.io and “www.cisecurity.org”. This information is essential as IoT devices expand the attack surface due to their heterogeneous nature and are integrated with other network devices and are always connected (Schiller et al., 2022).

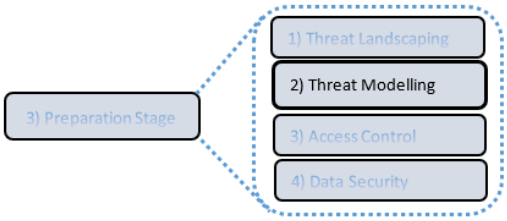
Human expertise – This is the use of threat intelligence by subject experts to predict attacks, attack trends, or patterns. Understanding of potential attacks and their patterns can be used to create security rules in firewalls, increase defence, filter IoT-specific threats, and increase threat response. i.e., edit specifications in intrusion detection systems enable high accuracy of detections. Early detection reduces the mean time to detect (MTTD) and mean time to respond (MTTR) for potential security incidents.

To develop a threat landscape for an IoT network, Table 13 was developed using the academic literature. The basis for Table 13 (Chen et al., 2018b; Kumar & Lee, 2012; Schiller et al., 2022), was those who used a similar approach to list the IoT security threats based on architecture. Subsequently, this research added the "segment" and "component" fields to the Table. These additional rows indicate the identified threats and where they sit in the IoT network.

Table 16 – IoT network threats mapped to architecture, segment and component.

3 Layer	Perception	Network		Application	
5 Layer	Perception	Transport	Process	Application	Business
Segment	Sensing & Acquisition	Transmission	Processing	Output & Application	Application
Component	X	Y	Z		
Security Threat, vulnerability	A, B, C,	A1, B1, C1	A2, B2, C2	Not in Scope	Not in Scope

4.5.3.2 Threat Modelling

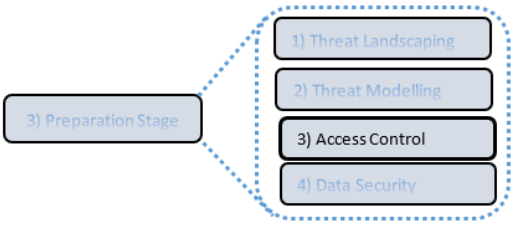


Once the threat landscape is developed, the next step is to start the threat modelling activity. Table 14 was designed to model the threats identified in threat landscaping with further details: "How this can happen—possibilities" and "Potential prevention action." Use a separate table for each layer to gain an in-depth understanding of the threats and their impact. This would reduce the complexity of threat modelling in all layers simultaneously and enable progress layer by layer.

Table 17 – IoT network threats and details.

Architecture layer – Perception/ Network/ Application		
Threat	**How this can happen - possibilities**	**Potential prevention action**
A	a)	
B	a)	
	b)	
C	a)	
	b)	

4.5.3.3
4.5.3.4 Access Control



The inclusion of Access Control ensures secure access to users, devices, applications and services (Ragothaman et al., 2023).

As shown in Figure 20, an access control system has three main components: the access control policy, the access control model, and the access control mechanism (Gouglidis et al., 2018; Hu & Scarfone, 2012; Samarati & de Vimercati, 2001).

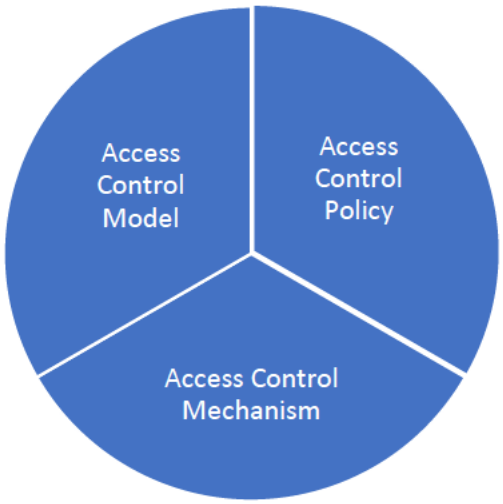


Figure 21 - The Three Main Components in an Access Control System.

- Access Control Policy – The policy defines the authorisation requirements and is enforced through an access control mechanism (Gouglidis et al., 2018; Samarati & de Vimercati, 2001).
- Access Control Model – The model provides the policies' presence and evaluation (Samarati & de Vimercati, 2001).
- Access Control Mechanism – The mechanism defines the implementation of the control (Samarati & de Vimercati, 2001).

Therefore, an access control solution consists of a set of governing security policies, an architecture with components and an access control model (Muthusamy Ragothaman & Wang, 2021). Due to the nature of IoT networks, there are many criteria to consider when choosing an access control model. Authors (Ragothaman et al., 2023; Ravidas et al., 2019; Rotondi & Piccione, 2012) suggest that certain criteria should be satisfied when adopting access control models to IoT applications. Further literature was reviewed to find studies about access control criteria related to IoT networks. Table 15 shows each study's summary and the authors' access control criteria. The number of studies is limited to seven as it

provides sufficient information to understand the requirements for a resource-constrained environment as in IoT network.

Table 18 – Criteria to be Satisfied when Adopting Access Control Models to IoT Environments

Author		(Ravidas et al., 2019)	(Ragothaman et al., 2023)	(Rotondi and Piccione, 2012)	(Pal et al., 2018)	(Andaloussi et al., 2018)	(Alramadhan and Sha, 2017)	(Hernández-Ramos et al., 2013)
Criteria	1	Dynamicity	Automation	Auditability	Distributed Nature	Flexibility	Adaptability	Distributed Nature
	2	Interoperability	Coherence	Delegation	Heterogeneity	Scalability	Generality	Delegation
	3	Performance	Downtime	Dynamicity	Lightweight	Usability	Lightweight	Efficiency and Lightness
	4	Reliability & Availability	Facilitation of Users	Easy to use	Scalability	Distributed Nature	Scalability	Flexibility
	5	Scalability	Granularity	Flexibility				Heterogeneity
	6	Usability	Handling Complexity	Granularity				Interoperability
	7		Interoperability	Scalability				Revocation
	8		Policies' Specification	Security				Scalability
	9		Resolving Identities	Understandability				Usability
	10		Resource Constraints	Distributed Nature				
	11		Scalability					
	12		Security					

Considering the features listed in Table 4, this research aims to fulfil the most important, essential and addressable criteria that can be used in IoT networks to provide comprehensive security. Table 16 summarises the common criteria that should be accommodated in IoT network access control, summarised from Table 15.

Table 19 – The number of times each feature appeared in Table 15.

Criteria	#
Scalability	7
Complexity, Easy to use, Lightweight	5
Distributed Nature	4
Interoperability	3
Delegation	2
Dynamicity	2
Granularity	2

Table 16 shows that Scalability, Complexity, Ease of use, Lightweight, Distributed Nature, and Interoperability have been identified frequently in literature as essential criteria for access control for IoT networks. Therefore, these features need to be considered when selecting an access control model. To assist in choosing the most suitable access control model for an IoT environment, Table 17 was developed using (Muthusamy Ragothaman & Wang, 2021) published work. Table 17 shows the access control models and their support for the most common criteria from Table 16.

Table 20 – Access Control Models and their Criteria

Access Control Model / Criteria	Discretionary Access Control (DAC)	Role Based Access Control (RBAC)	Attribute Based Access Control (ABAC)	Organisation Based Access Control (OrBAC)	Capability Based Access Control (CapBAC)	Usage Based Access Control (UCON)	Blockchain (BC)
Scalability	No	No	Yes	No	Yes	Yes	Yes
Complexity	More	More	More	More	Less	More	More
Distributed Nature	No	No	No	No	Yes	No	Yes
Interoperability	No	No	Yes	Yes	Yes	No	Yes
Delegation	No	No	No	No	Yes	No	Yes
Dynamicity	No	No	Yes	No	Yes	Yes	Yes
Granularity	Coarse	Coarse	Fine	Coarse	Coarse	Fine	Fine

The comparison presented in Table 17 for each access control model indicates that the CapBAC and Blockchain support most of the requirements for an IoT environment. Blockchain is an emerging technology that can be used for access control in IoT networks (Mohanta et al., 2021). It provides decentralised computation and storage facilities for IoT data (Ray et al., 2021). However, implementing blockchain technology in a resource-constrained environment remains a significant challenge (Ray et al., 2021) and (Muthusamy Ragothaman & Wang, 2021) highlights that it still needs to be thoroughly explored for its applicability to IoT environments. In the Capability Based Access Control (CapBAC) model, a capability refers to a key, ticket or token, which is a communicable artefact of authority (Patel et al., 2016). A definition given by (Gouglidis et al., 2018) CapBAC is "*permissions are assigned with subjects and thus support one-to-many relationships between subjects and objects. Subjects and objects refer to the users and resources of a system (in a similar way to RBAC). Permissions are authorised operations that can be performed by a subject on an object*". The CapBAC authorisation approach has been developed according to the capability-based authorisation model (Gusmeroli et al., 2013). The "capability" has a value that refers to an object coupled with a set of access rights (Patel et al., 2016).

Considering the "Complexity", (Muthusamy Ragothaman & Wang, 2021) it was highlighted that Blockchain is more complex than the CapBAC. Many blockchain platforms exist, and they are constantly changing. The constant change can be a drawback, as blockchain-based access control models need to be continuously updated. E.g., Qtum, Ethereum, Neo, Wanchain, Lisk, Ark, Eos, Stratis, and Waves. Another major drawback is the hash algorithms running in Blockchain, which need intensive computational power (Ray et al., 2021). The CapBAC is proposed for IoT networks as this has low requirements to place on IoT devices (Pal et al., 2018) and is proposed as a functional, realistic approach for IoT networks (Patel et al., 2016). Further (Gong, 1989) emphasises that CapBAC supports the least privilege principle and securing subsystems.

Compared to all the access control models presented in Table 17, the CapBAC model is selected in this research to implement in IoT networks as it supports the scalability, complexity, distributed nature, interoperability, delegation and dynamicity.

CapBAC implementation in IoT network

In CapBAC, the User (also referred to as the accessor or Subject, e.g., human) prepares a token. The token contains its capabilities and presents them to the accessing Asset (also referred to as a resource or object, e.g., a device or database file). The Asset makes the access decision based on the token received and the access policy it is operating. The User handles the capability list, and the Asset holds only the accessing policy. Figure 21 shows an example of the CapBAC model. Capability examples: Read (R), Write (W), Execute (X), Delete (D), Change Access Permissions (P), Take Ownership (O) etc. The capability describes a set of access rights for an asset (Mahalle et al., 2012).

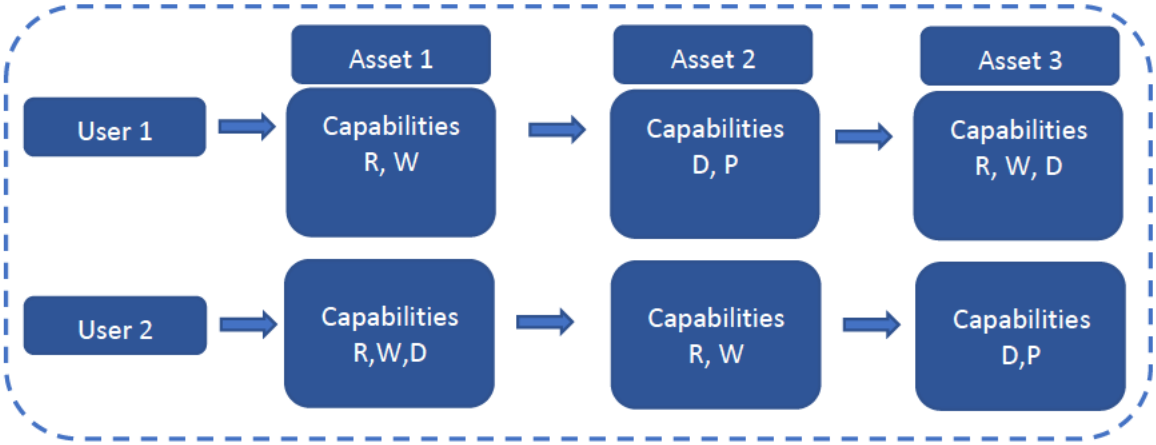


Figure 22 - The CapBAC Model Example

The "User" is associated with a list of capabilities that stores their access rights to all related "Assets" (Gong, 1989). As an example, the capabilities of user1 and user2 can be represented as;

- User 1 capabilities = (Asset 1 (R, W), Asset 2 (D, P), Asset 3 (R, W, D)).
- User 2 capabilities = (Asset 1 (R, W, D), Asset 2 (R, W), Asset 3 (D, P)).

CapBAC's Capabilities are designed as a data structure and include the following information:

A couple of data structure examples are presented below.

- Capability (Object, Rights, Random) (Gong, 1989). Where:

  Object – the name of the object

  Rights- set of access rights

  Random – Random number generated using a one-way hash function

- CBAP = (Device identity, Permissions, Discriminator, DelegabilityBit, IssuedTime, ExpiryTime) (Patel et al., 2016). Where:

  Device identity – the Identity of the object

  Permissions – permitted operation

  Discriminator – a unique random value

  DelegabilityBit – a value set to 0 or 1 to use in an access delegation scenario

  IssuedTime – capability issue time

  ExpiryTime - capability expiration time

- CAP_i = (*O, AR,C,* Rnd_i) (Anggorojati et al., 2018). Where:

  $Rnd_i = f(S_i, O, AR, Rnd_0)$

  Rnd_o *- f(O, AR)*

  O – name of Asset (object or resource) to be accessed

  AR- Access rights

  C – Context information

  Rnd - Random number generated using a one-way hash function

  S_i - identifier of Subject *I* requesting access

The terms "*Random*," "Discriminator," or "Rnd" refer to a random number generated using a one-way hash function to prevent forgery and used in the capability structure as a security mechanism (Gong, 1989; Mahalle et al., 2012; Patel et al., 2016).

Considering the above representation of capabilities, the following structure is adopted for this research study.

Cap = (ID, CL, Rnd) Where:

ID = Device identifier, i.e., Device Name, MAC address, etc

CL = Capability List, i.e., Read (R), Write (W), Execute (X), Delete (D), Change Access Permissions (P), Take Ownership (O), etc

Rnd = Random number to prevent tampering

Based on (Fotiou et al., 2022; Gusmeroli et al., 2013; Hernández-Ramos et al., 2013; Kain & Landwehr, 1987; Liu et al., 2021; Mahalle et al., 2012; Xu et al., 2018), Figure 22 shows the proposed Capability-based access control diagram for an IoT network.

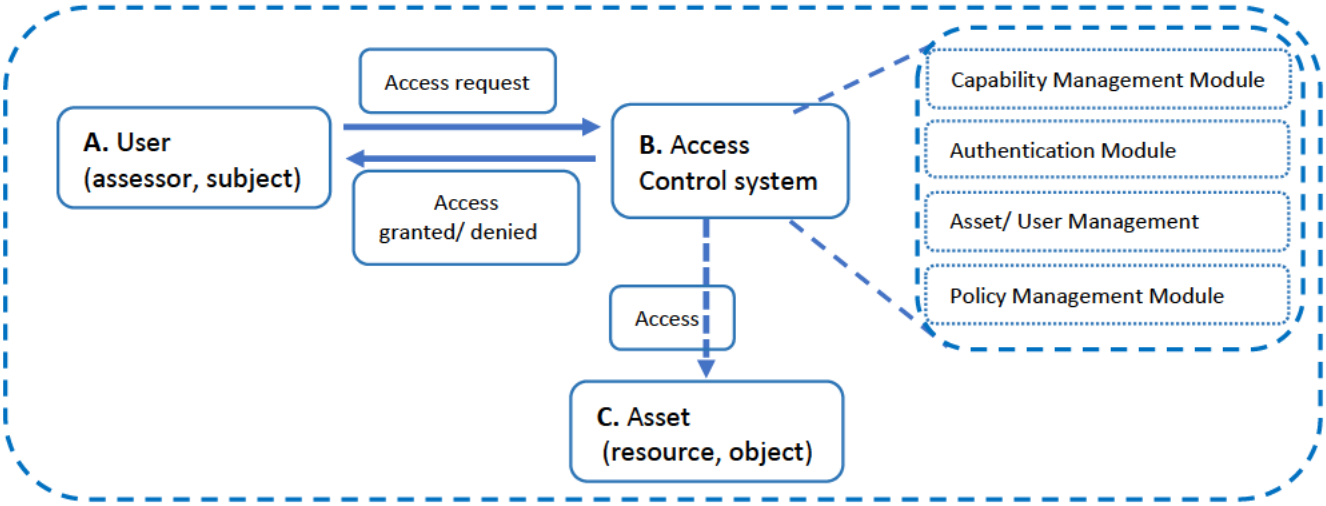


Figure 23 - Capability-Based Access Control Diagram

A. The user is also referred to as the accessor or subject.

B. Access Control system consists of the following modules.

- Capability management module – Propagation, Capability generation, capability verification, capability revocation.
- Authentication module – authentication services
- Asset/ User management – User registration, asset registration
- Policy management module – Policy Information Point (PIP), Policy Administration Point (PAP), Policy Decision Point (PDP), Policy Enforcement Point (PEP).

C. Asset is also referred to as a resource or object.

A "User" requests access to an "Asset" via the Access control system. The system verifies the capabilities assigned to the "User," authentication and authorisation requirements, "User" and "Asset" registration details and policy details against the request.

The decision to grant or deny access to the requested "Asset" will be based upon satisfaction with the user's capabilities, authentication, authorisation and policies stored in each module.

Access control in the Perception layer

The "Assets" and "Users" are registered with the "Asset/ User Management" module with their respective details. The "Capabilities" are assigned to Users accordingly.

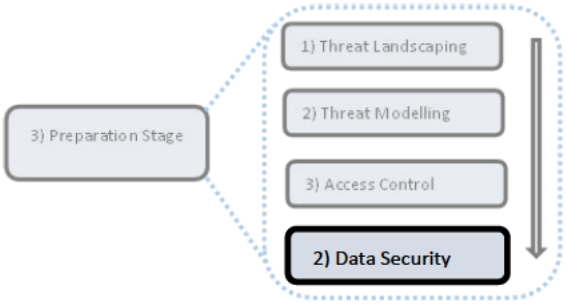
Access control in the Network layer

As the assets and users are registered with the "Asset/ User management module", the User can request access to an asset. The access control system can check the User's details from the Asset/ User management module, refer to the capability and policy and grant or deny the requested permission.

Access control in the Application layer –

The aspects (endpoints) of an IoT network, i.e., end user and edge processing, are considered out of scope as they become part of the traditional network or elements of the traditional networking environment. As such, they are not included in the proposed security framework.

4.5.3.5 Data Security



IoT data travels from a source to a destination in an IoT network—e.g., from a sensor to a database in the cloud. Data security is an essential part of this journey, as security measures must be applied where possible during the data transmission, processing, application, and storage phases. The main objective of securing data is to preserve confidentiality, integrity and availability.

In a three-layer architecture, data flows from the perception layer to the network layer and then to the application layer. Data acquired by the IoT devices in the perception layer is transmitted wired or wireless via the network layer. Depending on the nature of the IoT system, further processing and data storage may occur in the network layer. Then, the data will move to the application layer for further processing. In a five-layer architecture, data flows from the perception layer to the transport layer, the process layer, the application layer, and the business layer. Data acquired by the IoT devices in the perception layer is transmitted wired or wirelessly via the transport layer. Processing and data storage occurs in this layer, and processed data moves to the application layer. Finally, it moves from the application layer to the business layer for further use in business applications.

Figure 23 shows the data flow mapping for an IoT network based on a three-layer and five-layer architecture.

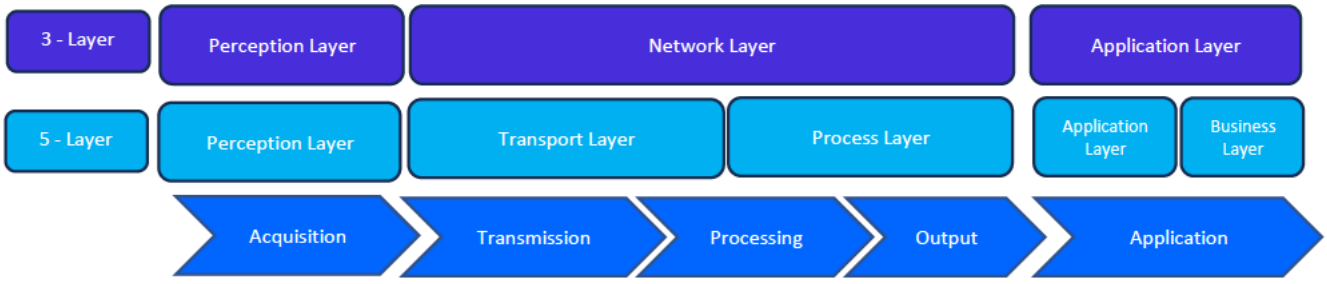


Figure 24 - Data flow mapping for IoT network based on three- and five-layer architecture.

Data security is looked at during transmission and output to preserve confidentiality, integrity and availability. To explain and understand the broadness and complexity of IoT networks in this research, the basic architecture, the three-layer, the extended architecture, and the five-layer were used. The architectural layers “Application” in 3-layer and “Application” and “Business” in 5-layer are involved with the aspects (endpoints) of an IoT network, i.e., end users, edge processing, cloud applications, big data analytics, and business intelligence are considered out of scope as they become part of the traditional network or elements of the traditional networking environment.

The initial data transmission occurs when the IoT devices pass the data they collect from the perception layer to the network layer. This transmission can be via a wired or wireless connection. In general, IoT devices in the perception layer are resource-constrained and unable to apply heavy encryption algorithms and other frequency-hopping communication security techniques (Hou et al., 2019; Suo et al., 2012). In this case, IoT devices require lightweight encryption algorithms that the devices can handle with the resources they are built with.

How to preserve data confidentiality and secure data from unauthorised access

Unauthorised access can be eliminated by implementing access control mechanisms and proper authentication processes for the users and objects (Miorandi et al., 2012). The "Capability-based Access Control" proposed in this research addresses the device identification, authentication and authorisation requirements.

How to preserve data integrity and ensure data is not modified or tampered with

Data encryption is another method of securing data from unauthorised access (Abouelmehdi et al., 2017). Encryption refers to a process that uses a cryptographic algorithm to convert an original message, which is in plain text, into a form that unauthorised users cannot read (Whitman & Mattord, 2022). These cryptographic methods can secure the data from being modified or tampered with and in the event of unauthorised access (Thapa & Camtepe, 2021). Cryptographic algorithms are of two types: symmetric or asymmetric. Examples of symmetric algorithms are Data Encryption Standard (DES), Triple DES, and Advanced Encryption

Standards (AES); examples of asymmetric algorithms are Rivest-Shamir-Adleman (RSA), Elliptic Curve Cryptography (ECC), Diffie-Hellman, Digital Signature Algorithm (DSA).

In the symmetric approach, a common secret key is used to encrypt the plain text and decrypt the cipher text. In this case, both sender and receiver must share the same key, which must be sent to the receiver securely to decrypt the cipher text. The key needs to be shared before the communication between the receiver and sender, and attackers can intercept it during the key transmission (Arya & Gore, 2020). Therefore, this raises a challenge of how to deliver the key securely (Whitman & Mattord, 2022). In the asymmetric approach, two different keys are used to encrypt and decrypt, while one key is a private key and the other is a public key. The private key is kept secretly, and the public key is stored in a public place where the receiver can access it, and this eliminates the challenge of delivering the key securely (Whitman & Mattord, 2022). The public key is stored in a public place where parties can access it. Asymmetric encryption is called "public-key encryption" (Whitman & Mattord, 2022). The asymmetric cryptographic solution was investigated for this research to avoid the challenge of secure key delivery and the distributed nature of IoT devices. However, either method could be used.

As mentioned, asymmetric algorithms RSA, ECC, Diffie-Hellman and DSA are used in public-key cryptography (PKC) (Dhillon & Kalra, 2016). Further literature was reviewed to select a suitable PKC for resource-constrained environments. Academic literature (Anggorojati et al., 2018; Chakraborty et al., 2018; Kumari et al., 2020; Lara-Nino et al., 2020; Patel et al., 2016; Sowjanya & Dasgupta, 2019; Sowjanya et al., 2021) highlighted that "Elliptic Curve Cryptography" (ECC) suits resource-constrained devices like IoT. A detailed comparative analysis (Dhillon & Kalra, 2016) shows that the ECC provides an equivalent security level to other asymmetric algorithms, consuming a low memory and power as it uses a smaller key size. ECC uses a 256-bit key, while RSA uses a 15360-bit key to provide the same security level. Simon Francia et al., 2022) also highlight that ECC needs less execution time, less memory usage, and runs with lower computational cost, which were the main reasons to use ECC in IoT security. Therefore, to encrypt the data, public-key cryptography using ECC is proposed during the transmission from the perception layer to the network layer. The proposed encryption method using PKC and ECC is shown in Figure 24.

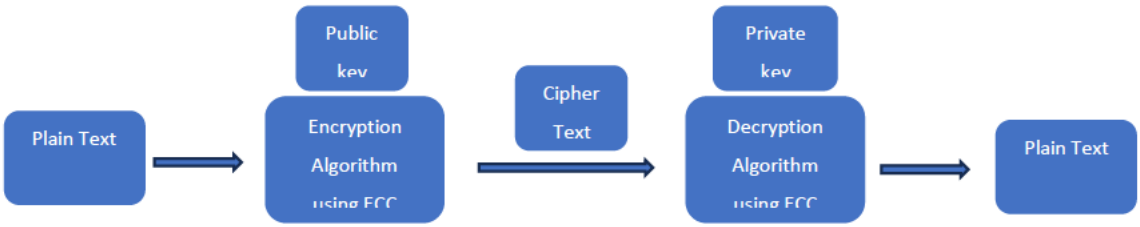


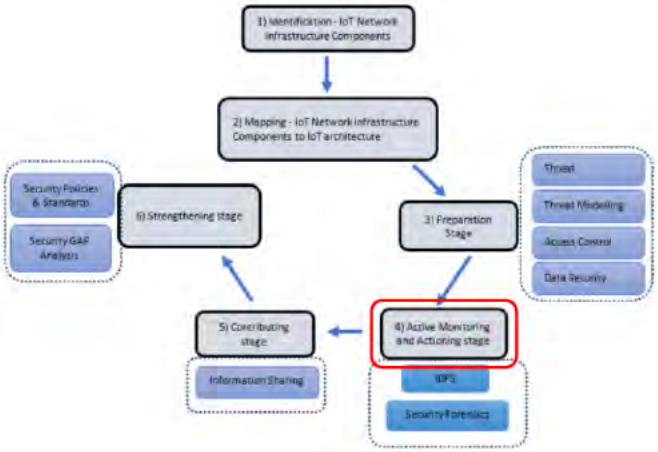
Figure 25 - Proposed Encryption Method Using PKC and ECC

How to preserve data availability for accessibility of data when and where needed

Data availability refers to ensuring the availability of data for its intended use when and where it is needed. For example, a patient's blood glucose readings may be collected hourly to be analysed by a clinician. The data collected needs to be available at the time of analysis. The unavailability of data due to accidental or intentional deletion, erasure or corruption would mean the clinician could not complete the analysis as scheduled. Therefore, the unavailability of data causes failures as the end users or applications cannot access it. In healthcare, the availability of patient data is critical as this data is used to provide preventive and reactive care for patients (Vargheese & Viniotis, 2014). Data backup and recovery are suggested to overcome data unavailability from accidental loss, erasure, corruption or even after a cyber-attack (Yeh & Meskaran, 2022).

In general, backup is keeping a separate copy of the original dataset to recover in the event of loss of the original data. The data backups must be encrypted, and access must be restricted only to authorised personnel. As a best practice, apply an extra layer of security for personally identifiable data to de-identify the individual sensitive information (Abouelmehdi et al., 2017). Data masking is also a de-identification technique that uses an unidentifiable value to replace a sensitive data element where true Identity cannot be revealed (Varadharajan & Bansal, 2016).

4.5.4 Active Monitoring and Actioning Stage



This stage comprises two framework elements: Intrusion Detection and Prevention System (IDPS) and Forensic Investigations (FI). IDPS is the active monitoring of the IoT network. Once IDPS detects any intrusions or implements preventions, further investigation about an incident needs to be carried out. This is the action of performing a forensic investigation.

4.5.4.1 Intrusion detection and prevention

IoT networks are exposed to cyber-attacks as they increasingly connect and integrate users, devices, applications, and communication networks (Thamilarasu & Chawla, 2019). Therefore, detecting intrusion attacks on a network is essential as they can result in interruptions, damages, and increased network downtime (Oh & Chae, 2008; Thamilarasu & Chawla, 2019). As a technological solution, intrusion detection systems detect intrusions in information and communication technology networks. An Intrusion Detection System (IDS) is a software application used in networks to detect any intrusions to network or host systems and make alerts about the intrusion (Santos et al., 2018; Whitman & Mattord, 2022). When intrusion prevention technology is incorporated into an intrusion detection system, such systems are commonly known as Intrusion Detection and Prevention Systems (IDPS) (Whitman & Mattord, 2022). However, applying these traditional IDPS is not straightforward for IoT networks due to resource constraints (Santos et al., 2018; Zarpelão et al., 2017). Therefore, further literature was reviewed to find specific IDPS techniques that can be applied to IoT networks. In search of this, research conducted by (Asharf et al., 2020; Butun et al.,

2014; Santos et al., 2018; Zarpelão et al., 2017) for IDS for IoT paradigms presented their findings focusing on attributes: "IDS placement strategy", "detection method" and "security threats". These research papers provide important insight into IDS for IoT environments. These insights are summarised in Table 18 based on (Santos et al., 2018; Zarpelão et al., 2017).

Table 21 – IDS based on the attributes

Placement strategy	Detection method	Security threat
• Centralised • Distributed • Hybrid	• Anomaly-based • Specification-based • Signature-based • Hybrid	• Man-in-the-middle attacks • Routing attacks • Denial of Service attacks • Conventional attacks • Botnets

The application process of a network-based IDPS to an IoT network is looked at based on the IoT architecture: perception layer, network layer and application layer. Based on "Figure 16 - Relation between the Layers, Segments and Data Flow of an IoT Network ", applying the IDPS in the network layer was decided. This decision was based on the following:

- The base station in the network layer consists of Microcontrollers: Arduino boards, Raspberry Pi, Photon, computer systems: desktops, Laptops, Servers, Cloud applications, or Smart devices: tablets, mobile phones, where the resources: memory, storage, and computational power required to deploy IDPS are available.
- Positioning the IDPS in the network layer, the following network traffic can be monitored centrally.
    - From the Perception layer to the Network layer
    - From the Application layer to the Network layer

This research does not cover outbound traffic from the application layer to external networks as it becomes part of the traditional network or elements of the traditional networking environment.

The proposed IDPS deployment method is shown in Figure 25 and is based on three- and five-layer IoT architecture.

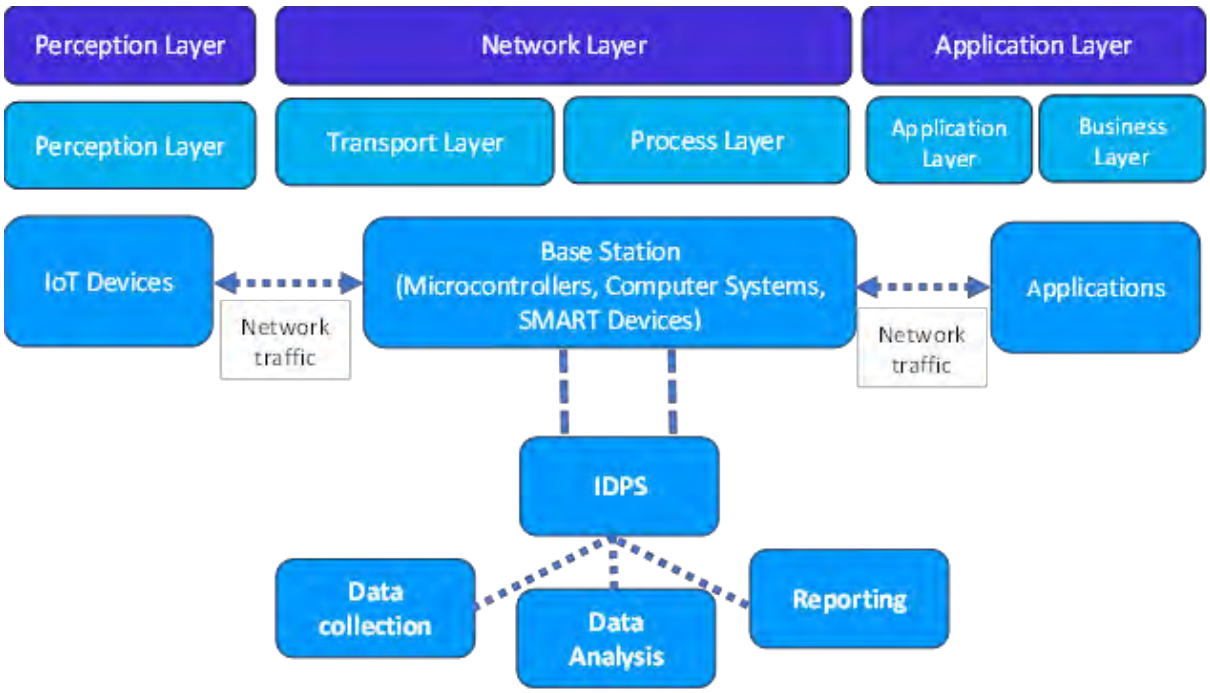


Figure 26 - The proposed IDPS deployment method based on three- and five-layer IoT architecture.

Selection of the "placement strategy", "detection method", and "security threats" depends on the diverse nature of the IoT network, including the architecture used, the type of IoT devices (environmental sensors to bedside sensors, wearables, fitness trackers, gyroscopes, motion, vibration, and implantable and ingestible sensors), network access media (Bluetooth, Zigbee etc.), the technology used (type of operating system, software), network devices (microcontrollers, smartphones, computers etc.), network infrastructure and the size of the network. For example, a centralised placement strategy can be used in the IoT network's base station, where both inbound and outbound traffic can be monitored. Referring to Figure 25, the base station can be used to deploy the IDPS. Upon completing the threat landscaping and threat modelling activities in the preparation stage (phase 3), based on the threats identified, an appropriate detection method can be chosen. For example, a signature-based detection method can be implemented to detect known attacks, an anomaly-based detection method for unknown attacks, or a hybrid approach can be implemented. Therefore, the implementer can select a detection method based on the threat landscape results.

4.5.4.2 Digital Forensics Investigation

In this research, the digital forensic investigation is performed after an alert is generated from the IDPS in an IoT network. The main objective is to better understand the incident and find any root causes for the alert. Thus, any potential intrusions can be prevented by taking preventive actions.

Digital forensics is a branch of traditional forensics science that involves a process of identification, collection, recovery, analysis, and preservation of electronic data as evidence obtained from electronic devices (Stoyanova et al., 2020). A definition given by the NIST for digital forensics is the "*application of science to the identification, collection, examination, and analysis of data while preserving the integrity of the information and maintaining a strict chain of custody for the data*" (Kent et al., 2006). The term "IoT Forensics" is used when digital forensics procedures are applied in IoT paradigms (Kent et al., 2006; Zawoad & Hasan, 2015). IoT forensics is a subdivision of digital forensics, a relatively new and unexplored security area (Kruger & Venter, 2019; Stoyanova et al., 2020).

In the event of evidence collection, digital forensics and IoT forensics fundamentally differ based on the sources that they obtained (Stoyanova et al., 2020; Surange & Khatri, 2021). For example, digital forensics collects from servers, routers, switches, computers, etc. IoT forensics collect forensic data from a wide range of sources, including devices (environmental sensors to bedside sensors, wearables, fitness trackers, gyroscopes, motion, vibration, and implantable and ingestible sensors), internal network (base station, gateways, routers) or from the cloud (Stoyanova et al., 2020). Therefore, IoT forensics is divided into three schemes: "Cloud forensics", "Network forensics", and "Device-level forensics" (Kent et al., 2006; Stoyanova et al., 2020; Surange & Khatri, 2021). Device-level forensics involves collecting data from the IoT device's local memory (Zawoad & Hasan, 2015). Network forensics refers to collecting data from the communication networks where IoT devices are connected, and cloud forensics refers to accumulating evidence from the cloud environment, as most of the IoT-based applications are integrated with cloud services (Kebande & Ray, 2016; Surange & Khatri, 2021).

The application process of a forensics investigation to an IoT network is based on the IoT architecture: three- and five-layer architecture. The proposed forensic investigation is based on " Figure 16 - Relation between the Layers, Segments and Data Flow of an IoT Network". The three IoT Forensics schemes and the Digital forensic processes recommended by the NIST integrated into the layered architecture are shown in Figure 26.

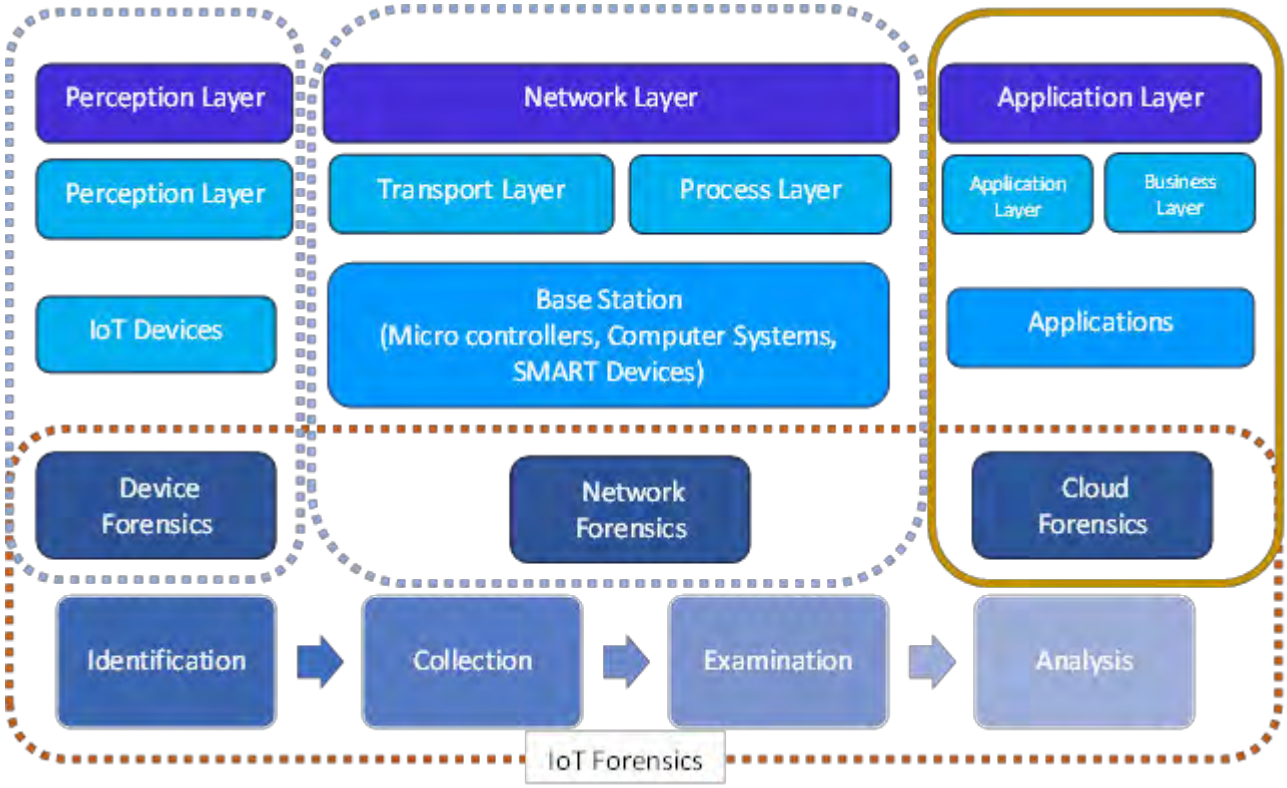


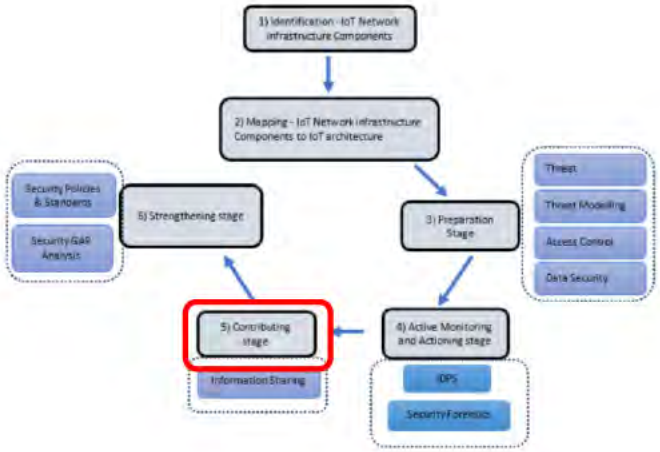
Figure 27 – Proposed Forensics Investigation for IoT Network

A brief description of the four processes is as follows.

- Identification – This refers to two things: Identification of a security incident or an event of interest and identification of sources involved in the incident (Kent et al., 2006; Zawoad & Hasan, 2015).
- Collection – Extraction of evidence from the identified sources. This can be from devices and networks.
- Examination – Examine the collected evidence.
- Analysis – Concluding based on the examination results.

The digital forensic security element in stage 4, the “active monitoring and actioning stage”, covers the perception and network layers in the IoT network. The application layer is out of scope as it connects outside the IoT network.

4.5.5 Contributing stage

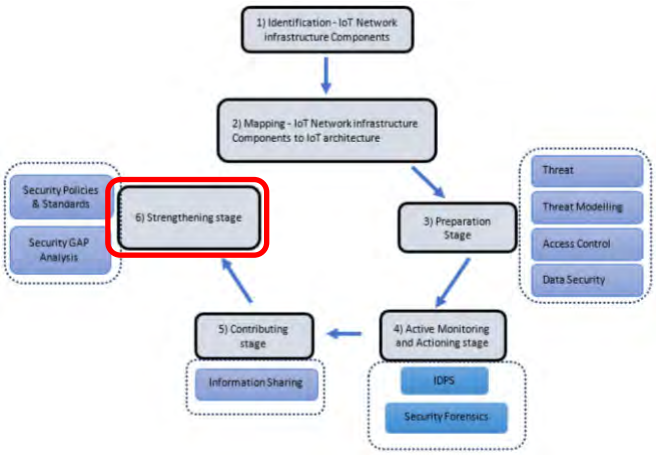


This stage consists of the "Security Information Sharing" framework security element. Any findings from the "Forensic Investigations" must be shared with the organisation internally and other similar healthcare service providers and relevant security agencies externally. The main objective of this security element is to share threat information internally and externally and to use such information to take preventive actions and to improve the security posture. According to (NIST, 2016), exchanging security threat information can be used by organisations to increase their knowledge and understanding of the security threats that they may face. It can take preventive actions: strengthening threat detection techniques and planning mitigation strategies. Further, sharing this information within similar organisations is highly beneficial because they may face common threats when using similar software, hardware, ICT systems, network services and data (Chadwick et al., 2020). The proposed model for security information sharing is presented in Figure 27.

Figure 28 – The Proposed Ways of Sharing Security Information via Different Sources.

Website bulletin boards will enable a group of people to interact with each other and promote awareness of security incidents. This will also facilitate sharing their experiences and how they can use such information within their organisation to prevent or mitigate threats or vulnerabilities. Feeding security threat information to threat-intelligent sources will keep it up to date. Organisations can access these intelligent sources to prepare for the latest security threats and keep their defences current. Providing security threat information to government agencies enables keeping threat and vulnerability databases up to date. So, threat landscaping using such databases will provide the latest information.

4.5.6 Strengthening stage



This stage comprises "Policies & Standards" and "Security GAP Analysis" framework elements.

4.5.6.1 Information Security Policies & Standards

Security Policies and Standards are an integral part of any organisation to state how Confidentiality, Integrity and Availability (CIA) are treated. Security policies provide directions to handle security issues and how technology can be used to accomplish this (Whitman & Mattord, 2022). Importantly, policies are focused on the CIA, overlooking the sensitive data and meeting the regularity requirements. Once the policies are in place, standards are to accompany the policies to comply with them by providing detailed statements (Aly et al., 2019; Whitman & Mattord, 2022).

Information Security policy refers to "*Written instructions provided by management that inform employees and others in the workplace about proper behaviour regarding the use of information and information assets*" (Whitman & Mattord, 2022). Information security policies can be presented in three basic types: Program policy, Issue-specific policy and System-specific policy (Nieles et al., 2017). The Program policy is a high-level policy that defines the purpose and scope, focuses on compliance issues, and assigns implementation responsibilities and other related responsibilities within the organisation at the strategic level (Nieles et al., 2017).

The Issue-specific policy addresses areas of relevance and concern to an organisation. This policy type aims to provide specific instructions and guidance on the proper use of the systems within the organisation, which needs regular review if there are any technological changes (Nieles et al., 2017). The system-specific policy focuses on a particular system within the organisation and provides information and directions on what actions are permitted on that system. Further, system-specific policies mandate the required security configuration for the specific system and guide the responsible personnel for the security to implement such controls (Nieles et al., 2017).

The main objective of this research's system-specific security policy is to outline how IoT networks in digital health systems are configured. Due to the time limitations of this research, only directions to create such a security policy are discussed.

Example 1 – In the selected IoT example, “Remote Health Monitoring System”, some sensitive, personally identifiable data is involved. Information Security Policy can be developed to state “how to handle sensitive information?”. How do employees handle such data? How patients are informed about the data collected and stored.

Example 2 – How are users and devices registered with the “Asset/ User Management” module in the Capability access control system?

Example 3 – Security mode configuration in Bluetooth modules (Mode 1, 2, 3 or 4) in Sensors.

Example 4 - Intrusion Detection System’s signature database updates.

A system-specific security policy template is proposed to cover the security configurations in this research based on the NIST Special Publication 800-12 R1. The system-specific security policy consists of a two-level model: Security objectives and Operational security rules (Nieles

et al., 2017). Security objectives need to be specific, well-defined, concrete and clearly stated to achieve them (Nieles et al., 2017). Operational security rules identify and document the rules for managing and operating the defined security objectives. This type of security policy guides the configuration of the selected system-specific aspect. An example is the creation of a database user with access rights. The proposed template, which was adopted from NIST, is shown in Figure 28.

System-specific security policy	
Security policy Name	
Security policy version	
Security policy created – dd/mm/yyyy	**Security policy last edited** – dd/mm/yyyy
Security objective	
Operational security rule	
Created by -	**Designation -**

Figure 29 - The Proposed System-Specific Security Policy Template

4.5.6.2 Security GAP Analysis

While applying this framework could potentially increase the security of an IoT network, failing to secure the primary network presents a vulnerability. This framework proposes a security GAP analysis of the primary network infrastructure. A GAP analysis is conducted to identify differences between a current and a targeted state of concern: technology, process, market, product, etc (Rasmussen et al., 2018).

A security GAP analysis is an in-depth review to identify gaps in the organisation's current security posture in ICT systems. It is conducted using industry best practices for comparison. The results of a security GAP analysis highlight whether the organisation's level of security is low compared to industry best practices.

The key steps in a security Gap Analysis are listed below.

1. Select a security standard
2. Evaluate people and processes
3. Gather data
4. Analysis

While the security of the primary network is extremely important, ultimately, it is outside the scope of this research other than to highlight the need to be proactive about the security of the primary network.

Security GAP analysis for the primary network infrastructure strengthens security from threats and vulnerabilities. It's important to remember that unsecured networks can pose a significant risk to the connected IoT network. Applying this proposed security framework could potentially increase the security of an IoT network; failing to secure the primary network presents a vulnerability. While the security of the primary network is critical, ultimately, it is outside this research's scope other than highlighting the need to be proactive about its security.

This chapter presented the proposed security framework. It explained the security elements, their interrelationship and the application process of the proposed security framework. The next chapter presents the Demonstration of the framework using an example.

5 DEMONSTRATION OF THE FRAMEWORK

This is the "Demonstration" phase of the design science methodology, where the developed artifact is applied to a selected context (Step D, Figure 11 – Research Design Phases Aligned with Design Science Research Methodology). This exercise was carried out using a desk study to test. The selected context is a "Remote Health Monitoring System" from academic literature.

The name of the academic paper – is "*Data Flow and Collection for Remote Patients Monitoring: From Wireless Sensors through a Relational Database to a Web Interface in Real Time*" (Tomašić et al., 2017).

The main reason for selecting this example is that the IoT network representation is straightforward and linear. The basic three-layer or five-layer architecture can be identified easily in the presented architecture. Further, the authors did not discuss the security aspects of the architecture in detail or applied, so it is an opportunity to demonstrate the application of the proposed security framework.

The selected remote monitoring system consists of sensors, a local server with a relational database, a web server and web interfaces. Figure 29 shows the overview of the selected real-time remote monitoring system (as shown in the original research paper).

Figure 30 – Overview of the Remote Health Monitoring System (Tomašić et al., 2017)

In this remote health monitoring system, the “Shimmer3 ECG” sensor kit collects data from the human body and streams them to the local server via Bluetooth. The data is inserted into the relational database configured in the local server. The web server queries the data from the relational database and provides it to the web interfaces.

The basic three-layer and the extended five-layer architecture are mapped to the selected context, as shown in Figure 30.

Figure 31 - Remote Health Monitoring System mapped to the IoT Architecture.

5.1 Getting started

Applying the framework to a selected scenario consists of six phases. Figure 31 shows the phases. (As originally presented in Chapter 4, Section 4.5, Figure 17 - Main Phases of Applying the Framework)

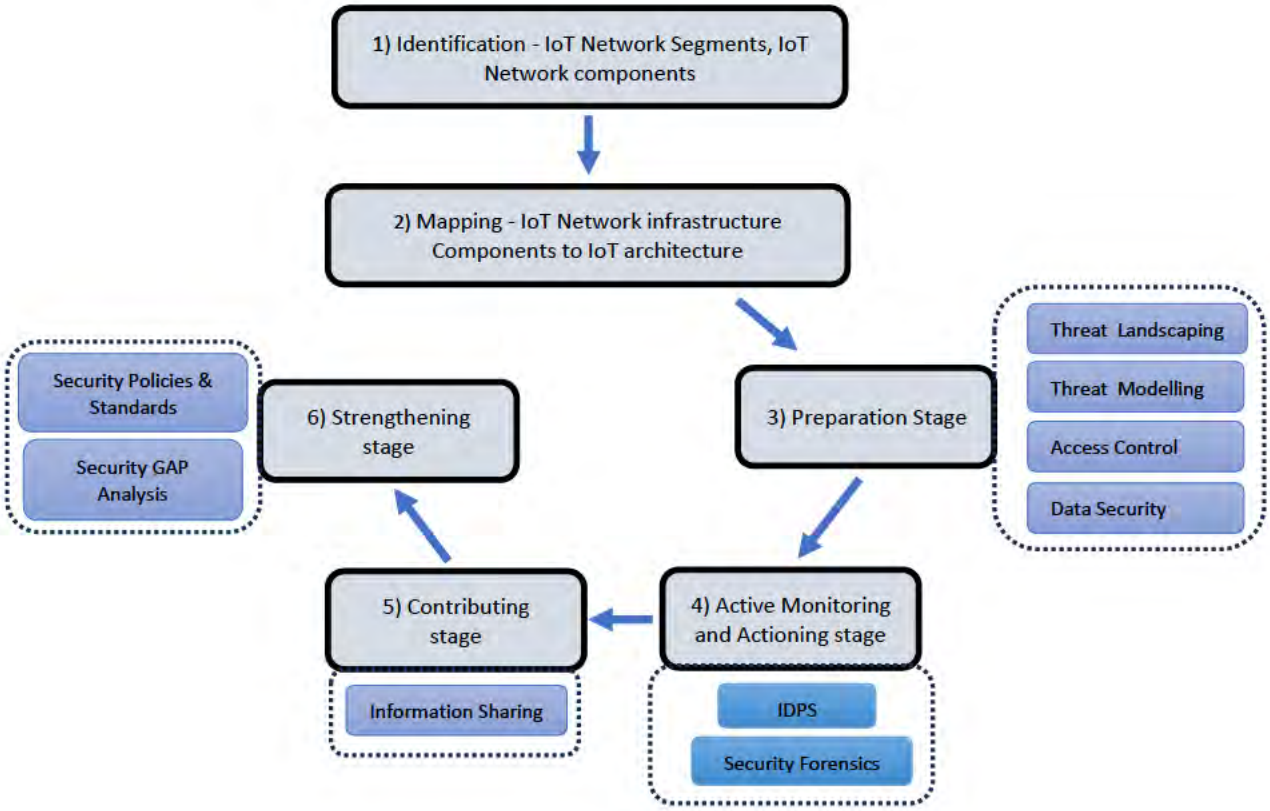
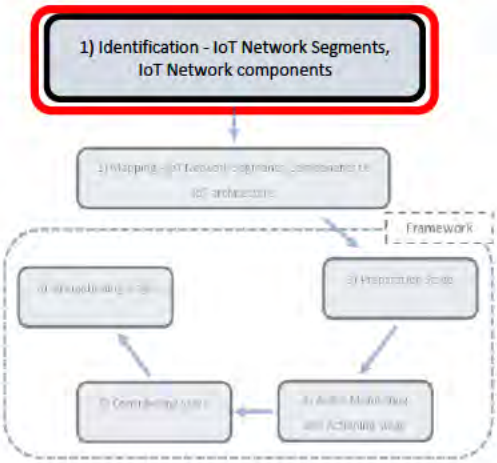


Figure 32 – Main Phases of Applying the Framework.

5.1.1 Identification - IoT Network Segments and IoT Network Components



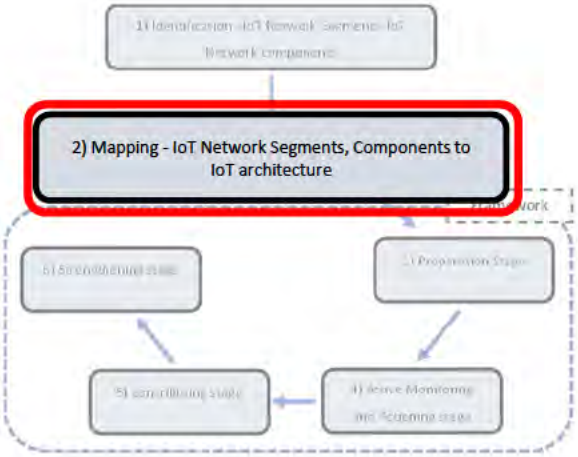
This is the starting point of the proposed security framework. This phase involves identifying the IoT network's segments, underlying hardware and software components, technologies used, and end-to-end data flow. The identified IoT network segments, components, and other details are given in Table 19.

Table 22 – Details of the IoT network segments and components

Segment	IoT Network Components	General Details	Technical details
Sensing and Acquisition	Sensor kit	Name – Shimmer3 Electrocardiogram (ECG) unit Provides an inertial measurement unit (IMU) including an accelerometer, gyroscope, and magnetometer. Generated signals streamed via Bluetooth to the PC.	Wireless – Class 2 Bluetooth 2. 1 + Enhanced Data Rate (EDR), Bluetooth RN 4678 Chip Memory - integrated 8GB microSD card slot, Battery - 450 mAh rechargeable Li-ion, Processor - TI MSP 430 microcontroller (24mHz, 16Bit), Sampling frequency 8kHz, experimented with a 200-500 Hz frequency.
Transmission	Network media	Collect data from the Shimmer nodes using Bluetooth.	Class 2 Bluetooth ver 2.1 + Enhanced Data Rate (EDR)
Processing & Output	Process and Storage	Prepare data for storage, analysis and presentation using MATLAB, LabView and C#.NET Using a relational database structure. MySQL Community Server (GPL)	MATLAB C#.NET ver Ver 5.7.12. Default InnoDB storage engine.
Application	Base Station	Local Server - Apache HTTP Server, PHP web interface	Computer running Windows 10 Pro 64 (Intel Core i7-6820HQ Quad-Core, 16 GB RAM (2133 MHz, DDR4 1 DM), 512 GB SATA-3 Self Encrypted OPAL2 Three Layer

			Cell Solid State Drive)
Application	User devices	SMART phones, Tablets, PCs	Apple and Android mobile phones, iPads, Laptops, Desktop PCs etc.

5.1.2 Mapping - IoT Network Infrastructure Components and segments to the IoT architecture



This is phase two of the proposed security framework. It involves mapping identified IoT network segments and components to the IoT architecture. The mapping output shows the components and their position in each architecture layer. This will ensure the framework security elements are applied to the IoT network in every layer, providing a multi-layer secured architecture. Table 20 gives the mapping output for three- and five-layer architecture. Further, this mapping output is used to develop the threat landscape in each layer in the preparation stage.

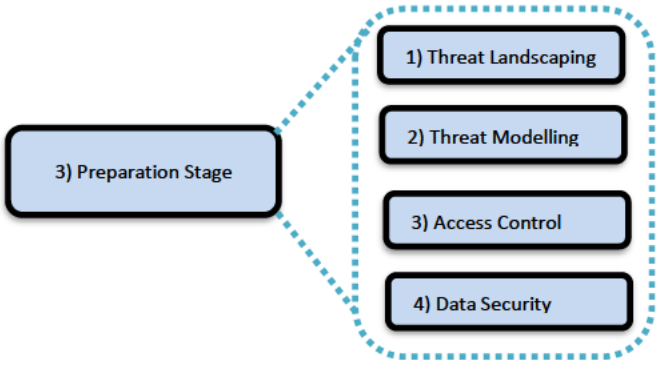
Table 23 – Segments and components mapped to the IoT architecture layers.

3 Layer	Perception	Network		Application	
5 Layer	**Perception**	**Transport**	**Process**	**Application**	**Business**
Segment	Sensing & Acquisition	Transmission	Processing	Output & Application	Application
Components (Included items)	Sensor kit	Bluetooth Wired & Wireless	Relational DB	HTTP Server, Web service	User devices

Upon completion of identification and mapping, the proposed security elements can be applied to the components in the IoT network, for instance, a sensor in the perception layer, wireless technology in the network layer, and a website in the application layer.

5.1.3 Preparation stage

This is phase three of the proposed security framework. The preparation stage consists of four security elements: threat landscaping, threat modelling, access control and data security.



5.1.3.1 Threat Landscaping

As described in Chapter 4, section 4.5.3.1, to develop a threat landscape for the selected IoT network, literature studies and publicly disclosed databases were used to identify threats and vulnerabilities. The security threats and vulnerabilities in Tables 21, 22, and 23 were identified using academic studies (Abdul-Ghani et al., 2018; Alaba et al., 2017; Alsubaei et al., 2017; Chen et al., 2018a; Habib et al., 2015; Islam & Aktheruzzaman, 2020; Jain et al., 2018; Khiangte et al., 2017; McGowan et al., 2021; Nawir et al., 2016; Schiller et al., 2022; Williams et al., 2022; Williams et al., 2019) and common vulnerability exposures at

https://cve.mitre.org/index.html. Threat landscaping activity uses the Table format which was developed (Chapter 4, Table 13). The results of mapping segments and components to the IoT architecture, shown in Table 20, were used to propagate the threat landscape in each layer. A separate table for each layer is used to gain an in-depth understanding of the threats. Table 21 gives the threat landscaping output for the perception layer, and Table 22 provides the landscaping output for the network layer.

Table 24 – IoT network threats mapped to Perception layer, segment and components.

3 Layer	Perception
5 Layer	Perception
Segment	Sensing & Acquisition
Components	Sensor Kit (Shimmer3)
Security Threat	1. Unauthorised access 2. Spoofing attack 3. Node replication attack 4. Denial of Service (DoS)

Table 25 – IoT network threats mapped to the Network layer, segment and components.

3 Layer	Network		
5 Layer	Transport		Process
Segment	Transmission		Processing
Components	Bluetooth	Wireless	Relational DB
Security Threat	1. BT Eavesdropping 2. BT Man-in-the-middle attack	3. Eavesdropping, 4. Man-in-the-middle attack 5. Rogue access point	6. SQL Injection attacks 7. DDoS attack

Threat Landscaping – Application layer

The threat landscape was not developed for the architectural layers “Application” in 3-layer and “Application” and “Business” in 5-layer, which are involved with the aspects (endpoints) of an IoT network, i.e., HTTP Server, Web services, and User devices. They are considered out of scope as they become part of the traditional network or elements of the traditional networking environment.

Table 26 – IoT network threats mapped to the Application layer, segment and components.

3 Layer	Application		
5 Layer	Application		Business
Segment	Output & Application		Application
Components	HTTP Server	Web service	User devices
Security Threat	Beyond the Scope		Beyond the Scope

5.1.3.2 Threat Modelling

Threat modelling activity using the Table format developed in Chapter 4, Table 14.

Using the results of the threat landscaping in Tables 21 and 22, the threat modelling was completed using the table format developed in Chapter 4, Table 14. Likewise, in the threat landscaping, a separate table for each layer is used to understand the threats and their impact on this activity. Further details such as "How this can happen—possibilities" and "Potential prevention action" are presented using literature, grey literature and online resources. The results of the threat modelling activity are shown in Tables 24 for the perception layer and 25 for the network layer.

Threat Modelling – Perception layer

Table 27 – Threat modelling in the perception layer

Layer	**Perception**	
Threat	**How this can happen - possibilities**	**Potential prevention action**
• Unauthorised access	The attack aims to gain unauthorised access to the nodes. (e.g., sensors, IoT devices)	• Access control (Node identification, Node Authentication)
• Spoofing attack	The attack aims to gain unauthorised access to the nodes and then to the network using a malicious node. If successful, the Adversary can feed the incorrect data to the system.	• Access control (Node identification, Node Authentication), • IDS
• Node replication attack	A malicious node can be added to the network.	• Access control (Node identification, node registration checks before adding to network)

Threat Modelling – Network layer

Table 28 – Threat modelling in the network layer

Layer	**Network**	
Threat	**How this can happen – possibilities**	**Potential prevention action**
• BT Eavesdropping	A passive eavesdropper can intercept the transmission between sender and receiver (paired Bluetooth devices).	• Data encryption • Access control • IDPS
• BT Man-in-the-middle attack	An adversary pretends to be a legitimate entity, and the legitimate sender and receiver are connected to the adversary (paired Bluetooth devices).	• Data encryption • Access control • IDPS
• Eavesdropping	An adversary listens to or captures data transmitted between a sender and receiver over wireless channels.	• Data encryption • Access control • IDPS

• Man-in-the-middle attack	An adversary intercepts the communication between sender and receiver over the wireless channels.	• Data encryption • Access control • IDPS
• Rogue Access Point	Dynamic Host Control Protocol (DHCP) attacks: DHCP Starvation attacks DHCP Spoofing attacks	• Configure Data Link Layer security (between network layer and application layer if DHCP enabled)
• SQL Injection attacks	An adversary interferes with input data from a client-side to the application. This applies to websites or web applications using structured query language (SQL) and SQL databases.	• Use SQL vulnerability scanners • Implement safe programming techniques for SQL-based applications
• DoS attack	Make services unavailable to legitimate users by flooding unwanted traffic to services.	• Intrusion detection and prevention systems

Threat Modelling – Application layer

The threat modelling was not conducted for the architectural layers “Application” in 3-layer and “Application” and “Business” in 5-layer, which are involved with the aspects (endpoints) of an IoT network, i.e., HTTP Server, Web services, and User devices. They are considered out of scope as they become part of the traditional network or elements of the traditional networking environment.

Table 29 – Threat modelling in the application layer

Layer	**Application**	
Threat	**How this can happen – possibilities**	**Potential prevention action**
Beyond the Scope	Beyond the Scope	Beyond the Scope

5.1.3.3 Access control

In the selected "Remote Health Monitoring" System, the proposed capability-based access control (CapBAC) solution (Chapter 4, Figure 22) can be installed on the local server. The CapBAC solution modules are described in Table 27. The access control system in the proposed CapBAC consists of four modules: capability management, asset/ user management, authentication, and policy management. Table 27 shows each module's contents in relation to the selected IoT network. For example, an asset/ user management module registers the IoT network's assets and users, and a policy management module can manage policies, including administration, decision-making, and enforcement. Working examples are given in Table 27.

Table 30 – The CapBAC modules

CapBAC module	**Involves**	**Example**
Asset/ User management	1. Register Shimmer sensors 2. Register Users – Insert data into the relational database 3. Register Users – to access Web service	The "Assets" and "Users" are registered with their respective details. 1. Shimmer sensor registered as Device ID – [Shim1+mac address] Eg - [Shim001:00:06:66:42:24:18] Device Name – Shimmer3 GSR+ 2. User to insert data: Username - LabView 001 User ID - WeivBal0007 Password – "**********" 3. User to read data: Username - WebServ 001 User ID - VresBew0009 Password – "**********"
Authentication module	Authenticate devices, users	Using credentials
Capability management module	1. Generate capabilities according to the system requirements. 2. Capability verification – Capability request against Capability assigned 3. Capability revocation – in case user/ asset changes	The user inserts data "Write" Web service reads data "Read" Generate CapBAC data structures (*Cap = (ID, CL, Rnd*) Refer to Figure 32 and 33
Policy management module	1. Policy information 2. Policy administration 3. Policy decision 4. Policy enforcement	1. Name of the policy, the purpose of the policy 2. Edit, delete, update 3. Access granted/ denied 4. Enforce the decision

The CapBAC data structure can be implemented in the selected IoT network for the following two scenarios.

a. Scenario 1 - Once the connection between the Shimmer sensor and the local server is established, the "LabView" and "C#.NET" interfaces insert data into the relational database.

Cap_2 = (ID, CL, Rnd) Where,

ID = User ID,

CL = Write (W)

Rnd = Timestamp + User ID + (Secret Number Generated)

Cap_2 = *(*WeivBal0007, *Write, (*Timestamp + User ID + (Secret Number Generated))*)*

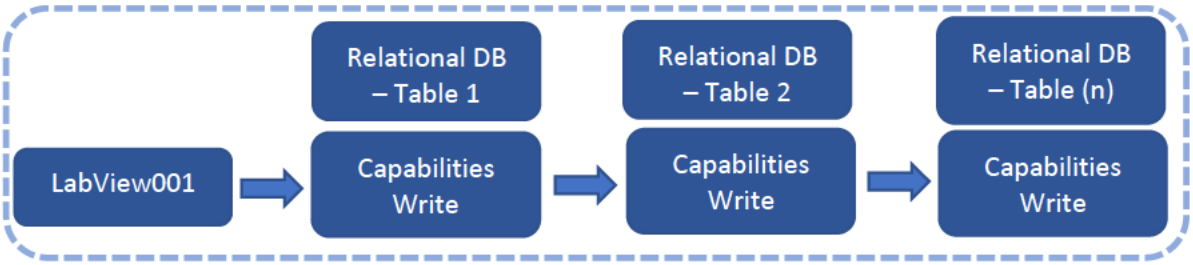


Figure 33 – The CapBAC Orientation for the "LabView" User

b. Scenario 2 - The Web service queries the data from the relational database and displays the data. Web service as a user,

Cap_3 = (ID, CL, Rnd) Where,

ID = User ID,

CL = Read (R)

Rnd = Timestamp + User ID + (Secret Number Generated)

Cap_3 = *(*VresBew0009, *Read, (*Timestamp + User ID + (Secret Number Generated))*)*

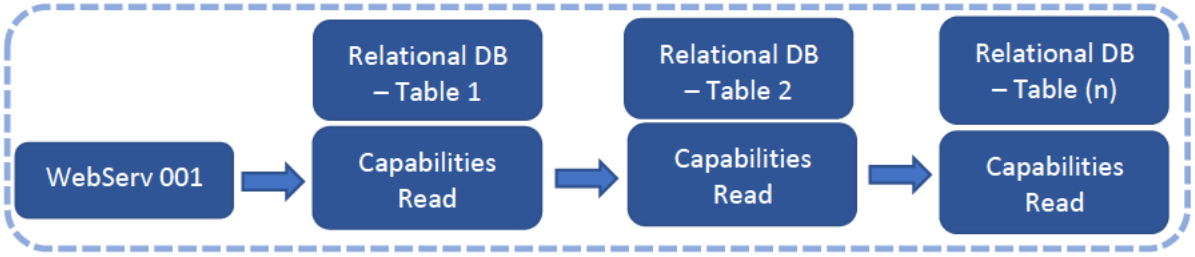


Figure 34 – The CapBAC Orientation for "WebServ" user

Overall, figure 34 shows how the decision tree of the proposed access control system is expected to work. As Figure 22 - Capability-Based Access Control Diagram explains in Chapter 4, - A “User” requests access to an “Asset” via the Access control system. The system verifies the capabilities assigned to the “User,” authentication and authorisation requirements, “User” and “Asset” registration details and policy details against the request. The decision to grant or deny access to the requested “Asset” will be based upon satisfaction with the user's capabilities, authentication, authorisation and policies stored in each module.

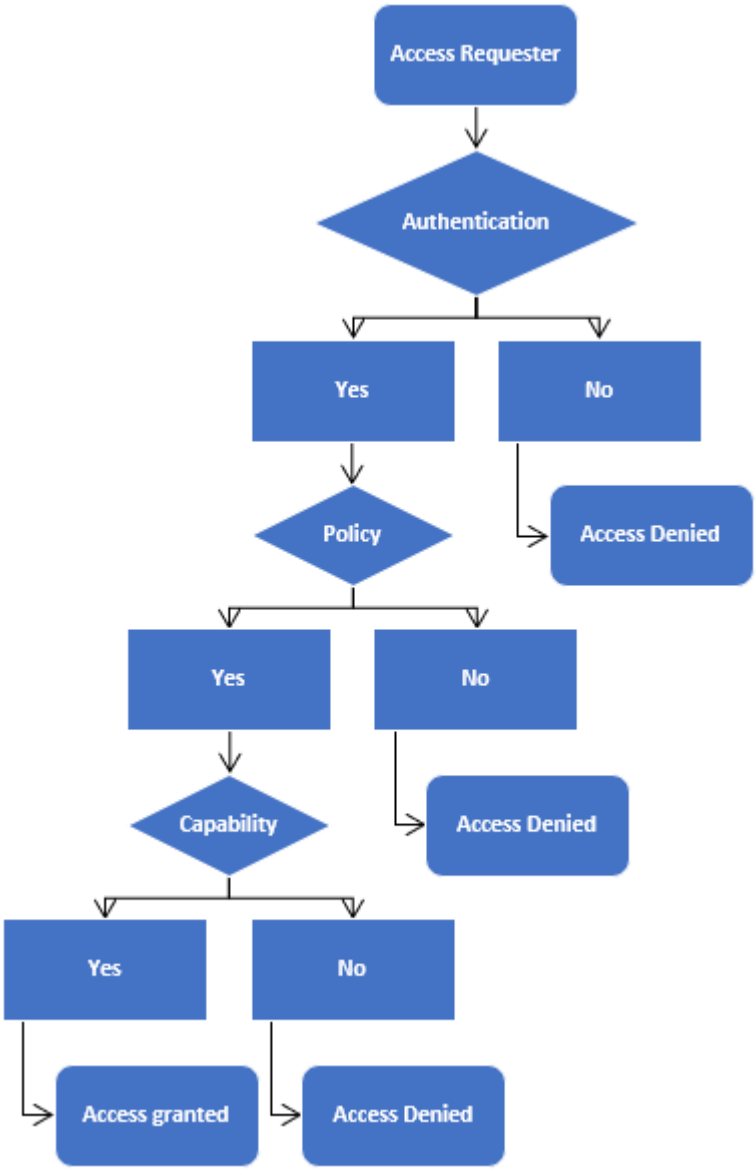


Figure 35 - Access Control System Decision Tree

The access requester can be a device or user. E.g., Bluetooth device, a user to access a database.

5.1.3.4 Data security

After the initial pairing process, communication occurs between the local server and the Shimmer sensor. The Shimmer sensor transmits the data to the local server's relational database. During this transmission, data needs to be encrypted to mitigate any data modification or tampering.

Data security from the Shimmer sensor to the relational database in the local server

In addition to security modes provided by Bluetooth, it also offers ways to encrypt the data exchanged between the paired devices (Chen et al., 2013; John et al., 2022). The encryption modes are:-

- Mode 1 - Traffic not encrypted at all
- Mode 2 - Encrypted using encryption keys on individual links, broadcast traffic is not encrypted.
- Mode 3 - Using a master link key, all traffic is encrypted.

The Bluetooth Encryption modes 2 and 3 use either "E0 Stream Cipher" or "Advanced Encryption Standard Counter with Cipher Block Chaining-Message Authentication Code (AES-CCM)" encryption mechanisms, which are symmetric cryptography. The Bluetooth Basic Rate (BR) and Enhanced Data Rate (EDR) devices use E0 stream cipher, and Bluetooth Low Energy (BLE) devices use AES-CCM. In the selected IoT network, the Shimmer sensor uses Class 2 Bluetooth 2.1 + Enhanced Data Rate (EDR), so E0 Stream Cipher is the inbuilt encryption method for data transfer. Therefore, data transmission from the Shimmer sensor to the relational database in the local server can be encrypted using E0 Stream Cipher.

According to the technical specifications, the Shimmer sensor uses the "RN-4678" module for communication, which supports AES128 encryption. Therefore, the E0 Stream Cipher can use

an AES 128 encryption mechanism between the Shimmer sensor and the relational database in the local server.

Data security from the relational database in the local server to the Web

In the selected IoT network, data obtained from the Shimmer sensor is stored in the relational database, and the Web Service queries the relevant data from the relational database and provides the data to web interfaces. In this scenario, two events can be seen: data at rest in the database and data in transit from the database to Webservice. According to the technical details, the relational database is installed in MySQL Community Server (GPL) - Ver 5.7.12. default InnoDB storage engine, webserver running on Apache HTTP Server and web interfaces are developed using PHP language.

Data at rest in the database

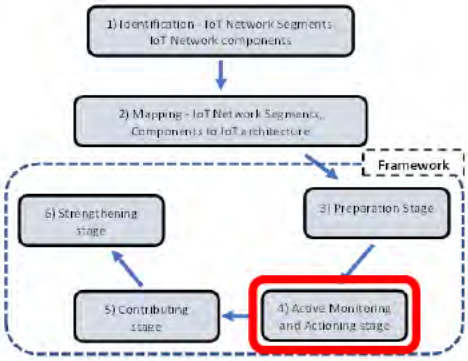
Based on the MySQL 5.7 reference manual, the MySQL InnoDB version (5.7.12) supports Advanced Encryption Standard (AES256) block-based encryption for data in the rest. This encryption feature relies on a “keyring” plugin and can be enabled during the table creation or alteration. The “keyring” plugin must be installed and configured first to use the encryption feature. Therefore, data at rest can be secured by applying AES encryption.

Data in transit from the database to Webservice

Based on the MySQL 5.7 reference manual, the MySQL InnoDB version (5.7.12) supports encryption connections between clients and the server using Transport Layer Security (TLS). The encryption connections are created per connection during the database user creation process. Therefore, data in transit between local databases and web services can be secured by making encrypted connections.

Phase three of the proposed security framework, the “preparation stage,” covered the security elements of threat landscaping, threat modelling, access control, and data security. The next section presents phase four, the “active monitoring and actioning stage,” which covers the security elements: intrusion detection and digital forensic investigations.

5.1.4 Active Monitoring and Actioning Stage



This is phase four of the proposed security framework. The active monitoring and actioning stage consists of two security elements: intrusion detection and prevention and digital forensic investigations. The IDPS system monitors the IoT network traffic to detect malicious activities and alert users. Once the IDPS generates an alert, digital forensics investigates the cause of the alert.

5.1.4.1 Intrusion Detection and Prevention

The "centralised" placement strategy is used in the selected IoT network, as there is a powerful node, the local server, to deploy the IDPS. Placing the IDPS centrally, the inbound and outbound network traffic can be monitored centrally by the local server, as shown in Figure 35.

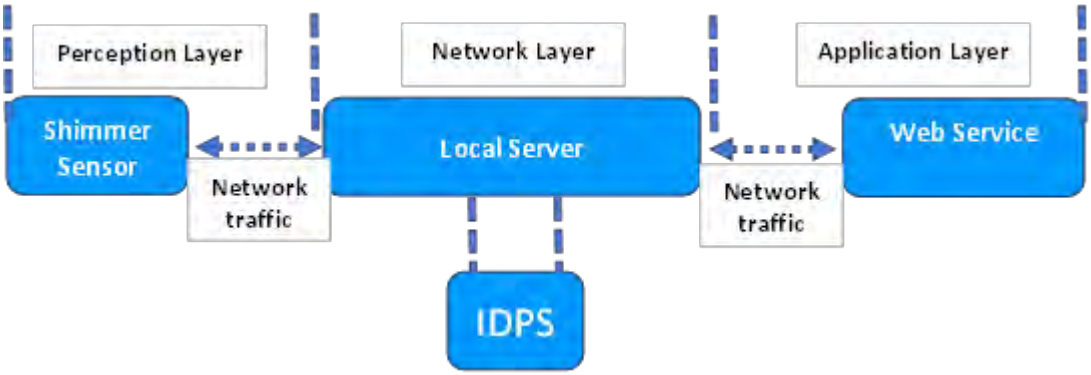


Figure 36 – IDPS Deployment in the Local Server

In selecting a detection mechanism for the selected IoT network, the "signature-based" approach is chosen as this is capable of detecting known attacks. During the Threat Landscaping activity, potential threats and attacks to the selected IoT network were identified in Tables 21 and 22 in section 5.1.3.1. For example, spoofing attacks in the perception layer and man-in-the-middle-attack in the network layer. The signature-based approach detects attacks when network behaviour matches an attack signature stored in the database inside the IDPS. Signature-based detections are accurate and efficient in detecting known attacks, as the available attack signatures are stored in the signature database (Khraisat et al., 2019; Loulianou et al., 2018; Santos et al., 2018; Zarpelão et al., 2017). Figure 36 shows how IDPS functions in the selected IoT network.

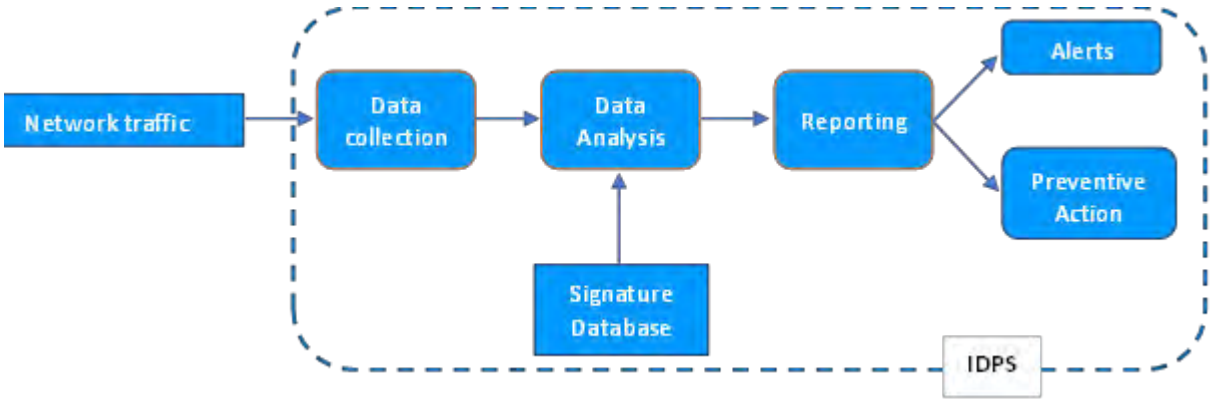


Figure 37 – IDPS Functioning in the IoT Network

The network traffic between architectural layers, perception layer to network layer and application layer to network layer (Figure 35) is fed into the "Data collection" component in the IDPS. Then, the data is forwarded to the "Data Analysis" component for analysis. This process compares collected data with the stored attack signatures in the local database. Any matches will inform the "Reporting" component. The reporting component generates alerts to security administrators and will launch preventive actions, e.g., a text message to a phone or temporarily disconnecting a suspected node.

5.1.4.2 Digital Forensics Investigations

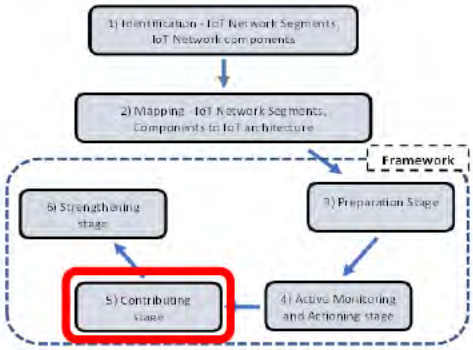
As proposed in Chapter 4 (Figure 26), the digital forensic process consists of four phases: Identification, Collection, Examination and Analysis.

Hypothetical scenario - The IDPS has generated an alert. An incident has occurred.

A. Identification:
    1. Identification of the incident – The alert generated by the IDPS
    2. Identification of the sources—Identify the devices and communication technologies involved in the incident (device and network forensics). This can be easily achieved through the rich visibility of all connected devices and technology used in the selected network. Table 19 in section 5.1.1, "Details of the IoT network segments and components," and Table 20 in section 5.1.2, "Segments Mapped to the IoT Architecture Layers," provide this visibility.
B. Collection – Collect the relevant data from the identified sources, e.g., shimmer sensor and local server.
C. Examination – Examine the collected data from the sources to identify any positive clues.
D. Analysis – Conclude results based on the examination. Determine whether a security incident or the IDPS has generated a false alarm.

Phase four of the proposed security framework, the "active monitoring and actioning stage", covered the security elements of intrusion detection and digital forensic investigations. The following section presents phase five, the "contributing stage," which covers the "information sharing" security element.

5.1.5 Contributing Stage



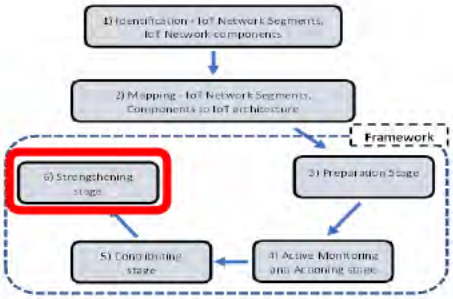
This is phase five of the proposed security framework. The contributing stage consists of information sharing security elements. The information sharing is about how the findings from digital forensics can be shared.

5.1.5.1 Information Sharing

Findings from the "Digital Forensic Investigations" about a security incident must be shared with the organisation internally and other similar healthcare service providers and relevant security agencies externally. The main objective of this security element is to share threat information internally and externally and to enable the use of such information to take preventive actions and improve the security posture. As proposed in Chapter 4 (Figure 27), sharing such security incident information can be done via website bulletins, feeding into threat intelligence sources and informing government agencies and healthcare service providers.

Phase five of the proposed security framework, the "contributing stage", covered the security elements of information sharing. The following section presents phase six, the "strengthening stage," which covers the "security policy" and "GAP analysis" security elements.

5.1.6 Strengthening Stage



This is the last phase of the proposed security framework. The strengthening stage comprises two security elements: information security policy and GAP analysis. The main objective of information security policy is to outline how IoT networks in digital health systems are configured. Security GAP analysis for the primary network infrastructure to strengthen the security from threats and vulnerabilities.

5.1.6.1 Information Security Policy

As proposed in Chapter 4, section 5.5.6.1 Figure 28, the system-specific security policies can be created in the following areas within the selected IoT Network example. In this worked example, the access control security element uses an "Asset/ User Management" module in the Capability access control system. A system-specific security policy can be created to register users and devices. Figure 37 shows how devices registered with the "Asset/ User Management" module in the Capability access control system.

System-specific security policy	
Security policy Name	Registration of IoT devices
Security policy version	Version 1.0
Security policy created – 20/12/2024	**Security policy last edited** –
Security objective	Only registered devices can operate in the IoT Network.
Operational security rule	A device ID is created as [CCCC+N+MAC address]" where CCCC - four characters, N – number, MAC address - MAC address of the device

	Example: The first four characters are from the name of the IoT device (Shimmer - shim) Number – number of the sensor MAC address – MAC address of the sensor Device ID – [Shim001:00:06:66:42:24:18]
Created by – John Smith	**Designation –** IoT Network Architect

Figure 38– Device Registration Example in Access Control System

5.1.6.2 Security GAP Analysis

The proposed security framework included the security element “security GAP analysis” for the primary network. Unsecure networks can pose a risk to the connected IoT network. Applying this proposed security framework could potentially increase the security of an IoT network, failing to secure the primary network presents a vulnerability. While the security of the primary network is critical, ultimately, it is outside this research's scope other than highlighting the need to be proactive about its security.

Phase six of the proposed security framework, the “strengthening stage,” covered the security elements of information security policies and GAP analysis. The six phases in the proposed security framework, which consisted of nine security elements, were carried out using a desk study in the demonstration exercise to test it in the selected “Remote Health Monitoring System” context. The following section discusses the challenges while demonstrating the proposed security framework for the selected IoT network.

5.2 Demonstration Challenges

A number of challenges were faced during the demonstration of the proposed security framework for the selected IoT network. These challenges included giving further direction where in-depth research is needed to overcome them.

As the threat landscape evolves, developing a threat landscape manually for any given network is challenging, as skimming through the sources requires a lot of time.

The Shimmer sensor device must be initially paired with the local server to transfer data from the sensor to the local server. This is the pairing process via Bluetooth in this instance. Then, the communication between the local server and the Shimmer sensor occurs. Bluetooth devices support multiple data rates: Basic Rate (BR), Enhanced Data Rate (EDR) and High Speed (HS), where BR supports up to 1 megabit per second, EDR supports up to 3 megabits per second, and HS supports up to 24 megabits per second (Chen et al., 2013; John et al., 2022). Bluetooth BR, EDR and HS define the authentication and encryption security procedures to enforce between pairing devices during different communication stages (John et al., 2022). As per (Cäsar et al., 2022; Chen et al., 2013; John et al., 2022), the Bluetooth Basic Rate, Enhanced Data Rate, and High-Speed specifications define four security modes:

- Mode 1 – Non-secured
- Mode 2 – Security mode enforced by the service level after link establishment.
- Mode 3 – Security mode enforced by the link level before link establishment. This mode mandates the authentication and encryption for all connections.
- Mode 4 – Security mode enforced by the service level after physical and logical link establishment. Further, mode 4 uses “Secure Simple Pairing” (SSP,) which utilises the Elliptic Key Diffie-Hellman key agreement for link key generation.

Security mode 4 was introduced for Bluetooth 2.1 + Enhanced Data Rate (EDR) (Chen et al., 2013). The Shimmer sensor uses the Class 2 Bluetooth 2.1 + Enhanced Data Rate (EDR) module. Therefore, security mode 4 can be utilised. The “Secure Simple Pairing” improves security using Elliptic Key Diffie-Hellman public key cryptography for pairing key generation. Thus, “Secure Simple Pairing” mitigates man-in-the-middle attacks and passive eavesdropping during the pairing process (John et al., 2022).

During the connection establishment between the local server and the shimmer sensor kit, integrating the inbuilt Bluetooth security features and proposed CapBAC solution is a technical challenge. To overcome these needs over right inbuilt security in Bluetooth programming. One of the objectives of introducing access control at the device level is to increase the security level of devices in the IoT network and to avoid malicious nodes getting connected to the IoT network. For example, device registration and ID checks prevent malicious nodes from getting connected and control their access to resources based on defined capabilities. Moreover, inbuilt security modes depend on the class of the Bluetooth and the data rate it uses. Therefore, not all Bluetooth devices have the same built-in security features. Therefore, when selecting sensors with Bluetooth, it needs to consider at least Bluetooth 2.1 + Enhanced Data Rate (EDR) so security Mode 4 can be implemented.

This research proposes the Public key cryptography (PKC) encryption method (Chapter 3.4) for data encryption. However, the Shimmer sensor uses a symmetric cryptography mechanism: “E0 stream Cipher”. E0, a stream cipher, is prone to attacks (John et al., 2022). To achieve a high security level to protect sensitive information, it needs to investigate how to apply the proposed PKC encryption protection instead of Bluetooth's built-in security encryption.

The selected database management system for this example is MySQL InnoDB version 5.7.12. According to (Amazon Web Services, 2023), the version is coming to its end of life and ends the standard vendor support by February 2024. The users of the 5.7 version need to upgrade to the latest released version, 8.0. It is important to upgrade to the new version, as vendors do not provide further security patches, vulnerabilities, or bug fixes.

IoT networks are vulnerable to attacks due to the heterogeneous devices used, the communication technology stack and their distributed nature. Therefore, detecting only known attacks is not sufficient. Detecting potential attacks also needs to be considered. In this situation, not only “signature-based” but also a possibility of “Anomaly-based” detection mechanisms or a hybrid model need to be implemented for better protection. Further

research would need to be done to determine whether it is possible to create options for such hybrid models.

In intrusion detection and prevention security element, preventive actions must be closely examined based on the IoT network and its purpose. For instance, disconnecting or shutting down a suspect node may disrupt a service. An example is shutting down a smoke sensor due to a false alarm by the IDPS.

The attack signature database must be updated once new signatures are released. Failure to update the signature database will leave the IDPS outdated, so it needs regular updates.

In the example IoT network, IDPS is deployed on the local server. According to the local server's technical specifications, it is a powerful machine with the required computational power, memory, and storage to deploy the IDPS. However, devices with limited storage may be challenging as the known attack signatures must be stored in a local database (Elrawy et al., 2018).

The required knowledge to conduct a digital forensics investigation in an IoT network can be challenging as not all information and communication technology personnel are trained explicitly for this purpose. Therefore, an Immediate response to an alert generated by the IDPS cannot be made.

The complexity of the investigation may increase due to the devices used, communication technologies used and the distributed nature of the IoT network compared to a traditional network.

The availability of IoT-specific forensics tool kits for ICT professionals needs further research. This may be future research to develop a basic IoT forensics tool kit.

Business continuity during digital forensics can be challenging, as IoT devices are sometimes used 24/7. For example, temporarily stopping the services of a fall detection system requires a replacement system during the investigations.

Information published through the organisation's website or as bulletins must be limited to general details. Publishing specific details may cause a security threat (disclosure of information to attackers). The availability of a trusted platform only allows healthcare service providers to share and access confidential security incident information.

This chapter demonstrated the proposed security framework in the selected “Remote Health Monitoring System” as a desk study. The demonstration covered six phases, from the preparation stage to the strengthening stage. Working examples were provided in each phase. Further, challenges faced during the desk study were discussed. The next chapter presents the evaluation of the proposed security framework.

6 EVALUATION

This is the “Evaluation” phase of the design science methodology. This chapter presents the evaluation of the proposed security framework. The evaluation results were based on the desk study (demonstration phase) and expert interviews. Expert interviews were used to capture the specialist advice of security professionals in the industry to evaluate the proposed security framework against a set of evaluation criteria.

6.1 Evaluation

An evaluation examines a developed artifact to assess its worth and deviation from expectations (Oates et al., 2022). Other reasons mentioned (Hevner & Chatterjee, 2010) for evaluation are: “promotional”, ”scholarly”, and” practical”. “Promotional” promotes the adoption of information systems and proves its usability, effectiveness, reliability and other characteristics to intended clients (Hevner & Chatterjee, 2010). “Scholarly” is how well a proposed technology or Information System has been evaluated or compared to similar systems' structure, function or impact in a scientific discipline (Hevner & Chatterjee, 2010). “Practical” is about understanding what works well and what does not through evaluating the Information System (Hevner & Chatterjee, 2010).

Most importantly, understanding the failures contributes to the body of knowledge so other researchers in the same discipline can learn from them (Hevner & Chatterjee, 2010). Evaluation provides feedback for further development, assures the research rigour and shows the relevance of the practice of the developed artifact (Mdletshe et al., 2023).

Evaluation in design science is defined as *“Evaluation of design artefacts and design theories is a key activity in Design Science Research (DSR), as it provides feedback for further development and (if done correctly) assures the rigour of the research”* (Venable et al., 2016). Also, (Woodall et al., 2016) point out that evaluation is needed to determine the quality and validity of the produced artifact. To evaluate an artifact, evaluation criteria need to be used

to measure the success of the artifact developed (Mdletshe et al., 2023; Oates et al., 2022; Prat et al., 2014; Woodall et al., 2016). Therefore, relevant evaluation criteria need to be developed to evaluate the produced artifact. Evaluation criteria for development and use in design science research have been discussed in studies (Hevner & Chatterjee, 2010; Mdletshe et al., 2023; Oates et al., 2022; Prat et al., 2014; Woodall et al., 2016). (Hevner & Chatterjee, 2010) highlights that the researcher can evaluate the technical or socio-technical aspects of the developed artifact using different techniques such as analytical modelling, simulation, actual measurements, quantitative surveys or qualitative interviews. (Mdletshe et al., 2023) emphasise that evaluation in design science research is to investigate the artifact's accomplishments by showing the utility, quality and efficacy. (Prat et al., 2014) Their in-depth study of artifact evaluation in design science research presented a hierarchy of criteria for artifact evaluation. The proposed hierarchy (Prat et al., 2014) is organised according to the dimensions of an Information System: goal, environment, structure, activity and evolution. Further, (Oates et al., 2022) suggest criteria: functionality, accuracy, consistency, performance, usability, completeness, aesthetics, and fit with the organisation to evaluate an artifact.

In view of the above, the proposed security framework needs to evaluate its promotional, scholarly, and practical aspects. The practical aspect was covered during the desk study, which led to an understanding of what worked well and what did not. To evaluate the promotional and scholarly aspects, evaluation criteria and semi-structured questions were developed using the academic literature, and expert interviews were conducted. The developed evaluation criteria and semi-structured questions were used to evaluate the proposed security framework discussed in the next section.

This research study used a design science research approach and produced the proposed security framework as the main output. The design output of design science research in Information systems can be considered a system (Prat et al., 2014). Viewing the designed output as a system, the evaluation criteria can be organised according to the fundamental dimensions: goal, environment, structure, activity, and evolution of such a system (Prat et al., 2014). Table 28 shows the details of the criteria according to the dimensions used to evaluate the proposed security framework. The dimensions and criteria adopted were based on the "*Hierarchy of criteria for IS artifact evaluation*" proposed (Prat et al., 2014).

Table 31 – Criteria to evaluate the artifact

	Artifact dimension	**Evaluation criteria**
Proposed Security Framework	Goal	Efficacy - *the degree to which the artifact produces its required effect*
		Validity - *the degree to which the artifact works correctly*
		Generality – *generality of the goal*
	Environment	People – *consistency with people (understandability, ease of use)*
		Organisation - *consistency with organisation (fit with the organisation)*
		Technology - *consistency with technology (use of up-to-date technology)*
	Structure	Completeness – *being whole*
		Simplicity – *easy to understand*
		Clarity – *being clear*
		Level of detail – *enough details to understand*
		Consistency – *the degree of the firmness*
	Activity	Completeness – *amounts to functionality*
	Evolution	Robustness – *low failure, response to change*

Semi-structured questions were developed to evaluate the criterion. Table 29 presents the mapping of the semi-structured questions to the evaluation criteria used to capture answers from the expert interviews.

Table 32 – Mapping of the Evaluation Criteria and Semi-Structured Interview Questions.

Artifact dimension	Evaluation criteria	Question	Q#
Goal	Efficacy	Do you think this framework delivers its expected protection?	C7
	Validity	Do you think this framework achieves its expected protection correctly? (*reliability?*)	C6
	Generality	For each framework element: Do you think this element is needed in a comprehensive IoT security solution? Are the elements described consistently?	B1,B5
Environment	People	(*Understandability and ease of use*) Do you think healthcare service providers and IoT network implementers would easily understand the framework?	C5
	Organisation	(*Utility*) Do you think this security framework would fit your organisation?	C4
	Technology	(*harnessing of recent technologies*)Do you think that the security elements are up to date in terms of current security measures?	C3
Structure	Completeness	Do you think the security framework is comprehensive enough to cover end-to-end protection?	C2
	Simplicity	Are the security elements described enough? Is the framework easy to understand?	B3
	Clarity	Are the security elements described correctly for an IoT environment?	B4
	Level of detail	Are the security elements' roles clearly described?	B2
	Consistency	Are the elements described consistently?	B5
Activity	Completeness	Do you think any security elements are missing from the framework?	C1
Evolution	Robustness	Do you think the framework would work as technology changes?	C8

A list of healthcare security professionals was obtained from the supervisor's potential participants, who were contacted via email to conduct the interviews. The interviews were scheduled for one hour, and data was collected via online one-to-one meetings. Participants were provided with the consent form, proposed framework description and the questionnaire at least two weeks before the interview. Initially, six healthcare security professionals were contacted, and three interviews were conducted. Interviews were conducted using Microsoft Teams, and the discussions were recorded. Answers were captured for the questions.

6.2 Interview Results

Answers were captured for the questions, and Table 30 shows the summarised answers for the questionnaire.

Table 33 - Summarised Answers for the Questionnaire.

Interview Question	Interviewee 1	Interviewee 2	Interviewee 3
A1. Do you currently use a framework for IoT security?	1a. No formal framework was used. 1b. Application framework used. 1c. Development framework used.	Yes, NIST, Essential Eight (https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/essential-eight)	1a. No formal framework. 1b. Not responsible for IoT
A2. Thinking about the new proposed framework, how many of the security elements in the framework have you implemented in your IoT network deployments?	Skipped by the expert	Most of them	All.
A3. Looking at the proposed framework as a whole, do you think that using such a framework would be useful?	Yes, it would be useful. Actually, it's quite useful on its own.	It is a great idea to have an IoT Security framework.	Yes, as long as it is accessible to the people using them.
A4. Do you see any challenges to implementing such a framework?	Capability, quality, Interoperability, implementation, workforce, knowledge.	No, it needs guidance on how to implement it.	Yes, implementing a framework requires knowledge, training, funding and interpretation of the framework. It needs to be accessible, understandable, and at an abstract level.
B1. For each framework element: Do you think this element is needed in a comprehensive IoT security solution?	They are all relevant.	Yes, to everything. As long as it is tried and tested	Yes, it is.
B2. Are the security elements' roles clearly described?	Yes. In a summary form.	Yes	Yes, well described.
B3. a). Are the security elements described in enough detail? b). Is the framework easy to understand?	Yes, it is easy to understand.	Yes	Relatively clear. It is better to accommodate the implementation guide.
B4. Are the security elements described correctly for an IoT environment?	Skipped by the expert, currently not in IoT Specific.	Not captured	Yes.
B5. Are the elements described consistently?	Suggestion - Need to improve the writing style to bring the meaning up.	Not captured	Yes.
C1. Do you think any security elements are missing from the framework?	From the provided summary, it is ok.	Maybe IT standards, catalogue of IT Standards.	Something that comes to mind is "Education."
C2. Do you think the security framework is comprehensive enough to cover end-to-end protection?	Yes, with the feedback loop from each stage.	Yes, it will cover 80%. It is 100% better to have the "Standards" catalogue included.	Yes, I think it is sufficient.
C3. Do you think that the security elements are up to date in terms of current security measures?	Skipped by the expert	Yes	Yes,

C4. Do you think this security framework would fit your organisation?	Skipped by the expert, currently not attached to the organisation.	Yes, After testing, piloting or proof of concept	Yes, it would. Bring it to the next level – application and useful.
C5. Do you think healthcare service providers and IoT network implementers would easily understand the framework?	Yes, they would understand it. To make it meaningful, add examples, if possible.	Yes, I think so. Clinical engineering and Bio-medical engineering will.	Healthcare service providers – not so much. IoT network implementers should.
C6. Do you think this framework achieves its expected protection correctly?	When the security elements interact iteratively and provide feedback to each other, they are effective.	The intent is there, the framework is there, so it can.	Certainly, it will help people guide them, implement, and improve.
C7. Do you think this framework delivers its expected protection?	When the security elements interact iteratively and provide feedback to each other, they are effective.	The intent is there, the framework is there, so it can.	It is insufficient by itself; other factors include workforce, skills, knowledge, and funds.
C8. Do you think the framework would work as technology changes?	Yes, with clear distinctions between the conceptual model and the implementation.	Yes, it may depend on the "Standards" catalogue. Thinking of standards ten years ago and now.	Think so. The strategies do not target a particular technology.

The first set of questions (A1-A4) was included to capture information about existing IoT security frameworks used for security protection, the type of IoT security elements used in such frameworks, the usefulness of an IoT security framework, and any implementation challenges for security frameworks. The experts' responses are discussed below.

The answers from the interviewees to the question "*Do you use a framework for IoT security*?" showed that interviewees have not used a specific framework for IoT security but have used frameworks in ICT security, application development, and software development. One interviewee mentioned the "NIST" and "Essential Eight" security frameworks that he has used. Responses highlight that interviewees are familiar with frameworks and have value in a specific security framework for IoT networks.

Answers to the question *"Thinking about the new proposed framework, how many of the security elements in the framework have you implemented in your IoT network deployments?"* highlighted that most of the security elements or all of them have been implemented based on their experience. This reveals that the security elements in the framework are relevant and valid to provide protection.

Answers captured for the "Looking at the proposed framework as a whole, do you think that using such a framework would be useful?" responses were very positive: *"Yes, would be useful. Actually, quite useful on its own", "Great idea to have an IoT Security framework.".* One of the interviewees commented that the framework is beneficial not only for IoT Networks but also for other ICT networks. Another interviewee commented that make the framework accessible to people who can use it.

Answers to the "Do you see any challenges to implementing such a framework?" highlighted that other than the technological needs, there are other factors such as workforce, implementation guidelines, interoperability, funding, accessibility, knowledge and skills required to implement a security framework successfully.

The next set of questions (B1-B5) was included to capture the information about the generality, level of detail, simplicity and clarity of the proposed IoT security framework, as shown in Table 31.

Table 34 – Questions B1 – B4 with Artifact Dimension and Evaluation Criteria

Artifact dimension	**Evaluation criteria**	**Question**
Goal	Generality	B1. For each framework element: Do you think this element is needed in a comprehensive IoT security solution? B5. Are the elements described consistently?
Structure	Level of detail	B2. Are the security elements' roles clearly described?
	Simplicity	B3. a). Are the security elements described in enough detail? b). Is the framework easy to understand?
	Clarity	B4. Are the security elements described correctly for an IoT environment?

Focusing on the artifact dimension "goal" and evaluation criteria "generality," answers for the B1 complement the included security elements in the framework, which was comprehensive to provide security. In answers for the B5, an interviewee suggested improving the writing style to bring meaning to the elements, while another interviewee is happy with the descriptions.

Responses for the B2 regarding the clear description of the security element's role to evaluate the level of detail, interviewees shared a view: "Yes, roles are well described".

Question B3, parts (a) and (b), about the simplicity of the individual elements and framework as a whole, responses highlighted that the framework is easy to understand and relatively clear. Further, the interviewee commented that it is better to accommodate an implementation guideline for the proposed framework. (This was already addressed in the demonstration)

Regarding question B4, one interviewee responded “yes”. Another skipped the question as he is specifically not in the IoT security area.

The last set of questions (C1-C8) was included to capture the information about the completeness, technology, organisation, people, validity and efficacy of the proposed IoT security framework, as shown in Table 32.

Table 35 – Questions C1 – C8 with Artifact Dimension and Evaluation Criteria

Artifact dimension	**Evaluation criteria**	**Question**
Activity	Completeness	C1. Do you think any security elements are missing from the framework?
Structure	Completeness	C2. Do you think the security framework is comprehensive enough to cover end-to-end protection?
Environment	Technology	C3. Do you think that the security elements are up to date in terms of current security measures?
	Organisation	C4. Do you think this security framework would fit your organisation?
	People	C5. Do you think healthcare service providers and IoT network implementers would easily understand the framework?
Goal	Validity	C6. Do you think this framework achieves its expected protection correctly?
	Efficacy	C7. Do you think this framework delivers its expected protection?
Evolution	Robustness	C8. Do you think the framework would work as technology changes?

The question “C1” ensures that any essential security elements are missing in the framework. Responses made by the interviewees did not comment on missing security elements that they could think of. Further, interviewers suggested that including any “IT Standards Catalogue” and “Education” elements in the framework would be better.

Responses gathered to evaluate the completeness of the framework structure from C2 clearly showed that the security framework can provide end-to-end protection. Further, the interviewee highlighted the importance of "feedback loops" within each framework stage, which were already discussed in Chapter 4.

Focusing on the artifact dimension "Environment", responses captured in C3, C4 and C5 for technology, organisation and people highlighted that security elements included in the security framework are state-to-art with the current security measures and would fit any organisation after bringing it to the next level by testing, piloting and providing a proof of concept. (This was addressed in the demonstration, and practical implementation was discussed in the future direction). Negative comments were not made regarding understanding such a framework by the healthcare services providers or the IoT network implementers.

Responses from C6 and C7 suggest that the framework would achieve the expected protection as long as the security elements interact iteratively and provide feedback to each other. The framework should be supported by a workforce, skills, knowledge, and funds to deliver the expected protection.

Responses to the question "Do you think the framework would work as technology changes?" indicated that as the security elements included in the security framework were not focused on any particular technology, there are no anticipated changes to the framework with technology changes.

6.3 Interview Results Analysis

Further, a six-phase thematic analysis was conducted according to the outline (Braun and Clarke, 2006). Each phase is presented below.

Phase 1: Familiarising yourself with your data—The interview transcripts were downloaded from the recorded video in Microsoft Teams into Word documents. A thorough back-and-forth reading of the transcripts was done to familiarise the transcripts and identify potential themes.

Phase 2: Generating initial themes—Twenty–four themes were initially identified from the transcriptions, as shown in Table 33.

Table 36 – The Themes identified from the Interview Transcriptions

Interview data	Theme
How do you make sure the whole environment is secure?	IoT Environment and Visibility
How to implement it? Guidelines?	Implementation Guidelines
How do people know what they are getting or not getting?	Workforce, Knowledge, Sills
Threat landscape – macro or micro view?	Access to Information
How to apply Threat Landscape, Modelling	Access to Information
How to automate Threat Landscape, Modelling	Process automation and AI Integration
IoT picture as a whole in a network. Similar to the OSI 7-layer model	IoT Environment and IoT Architecture
Feedback loops within elements	Interrelationship of Security Elements
Security Framework to work autonomously	AI Integration
Real-time protection	Security Assurance
Applicability to other industries	Wide Application
Deal with technology, different platforms, and vendors.	Technology agnostic
How this framework deals with standards	ICT Standards
AI Integration management of workflow	AI Integration
Framework implementation support	Implementation Support ($)
IoT Device Testing	ICT Standards for IoT Devices
Security coverage	Security Assurance
Planning, designing, implementation, Value chain to FW	Implementation Guidelines
Expanding the FW, does it support	Future support
Level of security sophistication, people with knowledge and skill	Workforce, Knowledge, Sills
Who can apply this FW? Small, medium or large organisations	Target audience (Small, Medium, Large)
Framework accessibility	Accessibility
People to access information (threats) and Information Sharing, Crowdsourcing	Access to Information
People's thinking patterns sharing information, reputation loss, trust	Mindset

Phase 3: Searching for themes – Twenty-four themes were identified in the search for themes from the extracted interview transcripts and the initial themes.

Phase 4: Reviewing themes—The themes were reviewed to identify any similarity to collapse themes. As an example, for "Security elements to function automatically" and "Can the process be automated?", the theme is "AI Integration and Automation." Thirteen themes were collated and the collated results are shown in Table 34.

Table 37 – Collated Themes

Interview data	**Theme**
Threat landscape – macro or micro view? (T) (access to security information)	Access to Security Information
How to apply Threat Landscape, Modelling (T) (access to security information)	Access to Security Information
People to access information (threats) (D) (Information Sharing) (Crowdsourcing)	Access to Security Information
FW accessibility (D) (Accessibility of the resources)	Accessibility
How to apply Threat Landscape, Modelling (T) (Automation with AI)	AI Integration
Security Framework to work autonomously (T) (AI Integration)	AI Integration
AI Integration (L) management of workflow	AI Integration
Feedback loops within elements (T) (Relationships) (Automation)	Feedback loop Interrelationship
Expanding the FW, does it support (L) (yes, can add)	FW - Flexibility, adjustability, changeability
How this framework deals with standards (L) (standards)	ICT Standards
IoT Device testing (L) (Standards)	ICT Standards
How to implement? Guidelines? (T)(Implementation Guidelines)	Implementation Guidelines
Planning, designing, implementation (L) (Value chain to FW)	Implementation Guidelines
Framework implementation support (L) (Funds)	Implementation Support ($)
IoT picture as a whole in a network. Similar to the OSI 7-layer model. (T) (IoT Architecture and visibility)	IoT Environment and visibility
How do you make sure the whole environment is secure? (T) (IoT architecture)	IoT Environment and visibility
People thinking pattern sharing information, reputation loss (D) (trust)	Mindset
Real-time protection (T)	Security Assurance
Security coverage (L) (level of Assurance)	Security Assurance

Who can apply this FW Small, medium or large org (D) (applicability)	Target audience (Small, Medium, Large)
Deal with technology, different platforms (L) (Technology agnostic, vendor-neutral)	Technology agnostic
Applicability to other industries (L) (wide application)	Wide Application
How do people know what they are getting or not getting? (T) (Knowledge, skills)	Workforce, Knowledge, Skills
Level of security sophistication, people with knowledge and skill (D) (workforce)	Workforce, Knowledge, Skills

Phase 5: Defining and naming themes – The final thirteen themes are presented in Table 35.

Table 38 – The Finalised Themes

Code #	Themes
1	Access to Security Information
2	Accessibility of the Framework
3	AI Integration and Automation
4	Feedback loop Interrelationship
5	Implementation Guidelines
6	IoT Environment and Visibility
7	Technology agnostic
8	Security Assurance
9	Target audience (Small, Medium, Large)
10	Workforce, Knowledge, Skills
11	Wide Application
12	FW - Flexibility, adjustability, changeability
13	ICT Standards

Phase 6: Producing the report -

The three interview transcriptions found that these thirteen themes were significant concerns when adopting a security framework. These themes are related to the research question of "how to apply a security framework?" and the sustainability of such a framework.

 # 1 Access to security information – This theme is about how the users of the proposed security framework can access the necessary security information. For example, to conduct the “Threat Landscaping”, how can the users of this security framework obtain the threat information? The process of obtaining the necessary information uses information sources such as publicly disclosed threat and vulnerability databases, threat intelligence and human expertise. This was discussed in detail in Chapter – Application and Implementation of the Framework, Figure 19 - Threat Landscape Information Sources.

 # 2 Accessibility to the framework—How is this framework accessible to people who wish to access it? As part of this research, in addition to the thesis publication, and as fulfilment of the “Communication” in DSRM methodology, scholarly and professional publications of this research are planned. This will enable the public to access the security framework in the broader community.

 # 3 AI Integration and Automation—Automation is widely applied in ICT systems to increase efficiency and productivity. Additionally, AI can support self-learning and decision-making. There is plenty of room for improvement in this research study, using AI and Automation techniques to bring this security framework to the next level and not be limited by any barriers. Due to the time and scope, this is for future research directions and opportunities.

 # 4 Feedback loop Interrelationship – This theme is about how each element of the security framework is interrelated and provides a feedback loop to each element. The conceptual view of the security elements (Chapter 3, Figure 14) shows the security elements' logical arrangement, highlighting the relationship and the flow. For example, the “Intrusion detection system” to generate alerts for any intrusions, “forensics investigation” to find a possible cause for the alert, and any results to share in “information sharing”. Further, as shown in Figure 38, “Information Sharing” loops back to the “Threat Landscape” by providing the information for public databases and threat intelligence.

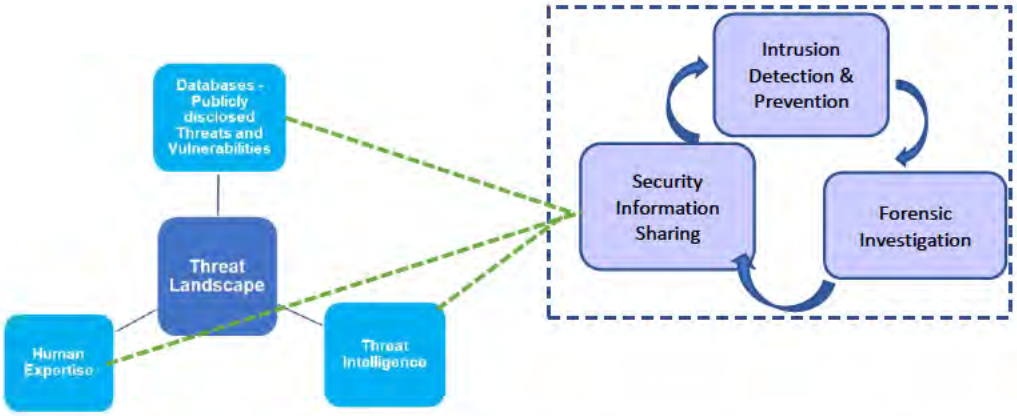


Figure 39 – Example of a Feedback loop and Interrelationship

 # 5 Implementation Guidelines – This was from the end user's perspective to implement this security framework and as a value chain to this framework having a complete set of implementation guidelines. This was discussed in detail using six phases in Chapter 4 -Design and Development, Section 4.5 - Applying the proposed security framework. Each phase is individually explained step-by-step using figures and tables, and the framework's practical implementation is further demonstrated as a desk study in Chapter 5 - Demonstration of the Framework, using a worked example.

 # 6 IoT Environment and Visibility – Compared to the Open System Interconnection (OSI) 7-layer model in traditional networks, the way the IoT environment can be seen was raised. The "Application and Implementation" process includes identifying IoT Network segments and IoT Components and Mapping to the IoT architecture. This gives a rich understanding of the IoT environment from an architectural view, including the type of devices used, where they are deployed, device connectivity, network connectivity, technologies used and end-to-end data flow. This provides a complete visibility of the IoT Environment.

 # 7 Technology agnostic—This theme refers to how this security framework is ready to respond, is flexible, and agile regarding technology changes, such as IoT platform changes, Operating systems, Communication technology (Wi-Fi, Bluetooth, Zigbee), etc. None of the security elements use any proprietary or specific technology in this security framework. The

framework was developed in a way that is vendor and technology-neutral. Therefore, the framework is capable of responding to any technological changes.

 # 8 Security Assurance – This theme concerns the confidence level after implementing such a security framework against cyber threats and vulnerabilities. The three main characteristics of information security: confidentiality, availability, and integrity were major priorities during the framework's construction. Security elements were identified to provide comprehensive security coverage through the scoping review, analysis of the academic literature, grey literature and industry security reports. Further, Security concerning the Internet of Things (IoT) devices, architecture, platforms, networks and communication were focused on to identify the security elements for the framework. The rich visibility gained by mapping the IoT network segments and components to IoT architecture ensures the framework security elements are applied to IoT network components in every layer, providing a multi-layer secured architecture. The framework can be used for each layer based on the architecture. As an example, a sensor in the perception layer, wireless technology in the network layer, and a website in the application layer. As another example, the data security element - The security of data in an IoT network is looked at the end-to-end flow. Security measures are applied during the data transmission, processing, application and storage phases. Further, this framework recommends the primary network by proposing a "Security GAP analysis" to minimise the security risks that can pose to the IoT network. As a norm, not 100% security is guaranteed in any security solution due to the constant evolution of the threat landscape, sophisticated and more intelligent tools used by cybercriminals and human errors. However, security elements included in the security framework are promising as it proactively attempts to provide security defence. Furthermore, security assurance is adequately met by the rich visibility of the IoT network and layered security architecture.

 # 9 Target audience (Small, Medium, Large) – Regarding the target audience, no specific target market has been identified. Anyone interested in being proactive in IoT network security can adopt the proposed security framework.

 # 10 Workforce, Knowledge, Skills—This theme refers to the required workforce, knowledge, and skills to implement such a security framework, as Cybersecurity is one of the most demanded fields globally. The required skills and knowledge need to be addressed at a

broader level to implement this security framework and the whole Cybersecurity space. Due to the time and scope, this is for future research directions and opportunities.

 # 11 Wide Application—The theme is applying the security framework to other industries, such as agriculture, transportation, etc. During the construction of the framework, IoT architecture was considered. The implementation of the framework is based on the selected architecture and not on any specific technology or platform or a particular commercial product. This framework can be applied to any other industry following the implementation phases.

 # 12 Framework - flexibility, adjustability, changeability – This theme highlights the capability towards the security framework's flexibility, adjustability and changeability to meet future requirements. The main objective of this research is to develop a “framework” to accommodate this need over a “model”. These capabilities were discussed in detail in Chapter 2– Literature Review and Section 2.3 - Overview of the Framework. As this artifact was developed as a framework rather than a model, any modifications, including adding new elements or excluding existing elements, can be accommodated to meet future requirements without changing the original research objectives.

 # 13 ICT Standards – The theme is about accommodating existing information and communication technology and IoT standards to the proposed security framework. Due to the outdated nature of standards, specific standards were not targeted in the security framework, leaving it to the implementer to select the valid standard at the time of implementation.

6.4 Evaluation Results Discussion

This research study used a design science research approach and produced the proposed security framework as the main output. The qualitative methods employed provide a comprehensive understanding of the proposed security framework, including its elements and their intended purpose, through expert knowledge and experience. This approach ensures that the evaluation is thorough and informative. The qualitative results, gathered directly from the feedback and perspectives of the actively involved interviewees, provide a clear understanding of whether the framework is suitable for its intended purpose. They also help provide context-specific information, in this case, about IoT networks. The interview results, capturing the perspectives of the interviewees, particularly those with extensive experience and knowledge in the field, provide a comprehensive understanding of the security elements included in the framework.

After analysing the evaluation results, no deviations from the research objectives were found. The results complement the proposed security framework and provide thoughts on future enhancements.

The results highlighted the importance of access to security information. Access to current and reliable security information is vital as it contributes to threat landscaping and modelling. Creating a secure platform to access security information needs to be addressed at a broader level. At least one platform focuses on the healthcare industry. If such a platform exists, the proposed security framework's security element, "Information sharing," is to feed the current threat information. Further results suggest the potential of automation and integrating artificial intelligence into security elements. For example, compiling a complete list of threats from multiple sources may be time-consuming in threat landscaping. Gathering this information is also an ongoing process as the threat landscape evolves. This may be an essential factor to consider in future research to find or develop security tools to automate this process. Also, the results highlighted the need for defined roles, responsibilities, and expertise to implement the proposed security framework. Based on the organisation's capabilities, roles and responsibilities can be identified throughout the implementation phases. This framework does not target a specific organisation, leaving it to the implementer to assign roles and responsibilities throughout the course of implementation.

No changes were made to the proposed security framework, as the evaluation results' analysis is in line with the research objectives. The themes identified in the evaluation provide thoughts on future enhancements and research.

6.5 Limitations of the Evaluation

The evaluation focused on its goal, environment, structure, activity, and evolution, as presented in Table 28, along with evaluation criteria. The intended purpose of this artifact is to provide proactive security defence for IoT networks in digital health systems.

Two methods were employed for the evaluation: desk study and expert interviews. The semi-structured interview questions were designed to gather qualitative insights from industry experts with a wealth of healthcare security experience and were selected from the supervisor's extensive contacts.

The expert interview results indicate that the proposed security framework meets its objectives and goals.

Further experts suggest that implementation guidelines could be beneficial for users to implement such a framework accurately. The chosen evaluation methods, the desk study, and the expert interview methods have inherent limitations. Understanding these limitations is essential as it guides future evaluations. The limitations and challenges of the desk study are discussed in Chapter 5 Demonstration, Section 5.2 Demonstration Challenges. The following section presents the limitations and challenges of the expert interviews.

Selection of experts for the interviews and the failures of the recruitment method. An example is the snowball method used in this study. Employing the snowball method, these experts were asked to forward the invitation to other experts in their network. The objective was to conduct at least ten interviews. The expectation was that six people forwarding the invitation could generate an additional 6 contacts. This would bring the total of potential reviewers to 12. It seems that the Snowball method is beyond the control of the researcher. Alternatively, the number of initial contacts should be much larger to succeed with the

Snowball method. Six initial contacts resulted in 2 interviews and a third interview was conducted using the Snowball method.

Further, incomplete data can lead to incomplete conclusions. As an example, the interviewer didn't answer the question. Another limitation is financial limitations. As this evaluation didn't pay money to experts for their participation, many of them didn't accept the invitation to participate.

Time constraints: interviews were limited to one hour. Further, conducting interviews and transcribing is time-consuming. Scheduling interviews was challenging because the experts were busy with their work. The recruited subject experts may have biases or personal opinions for their responses. This may affect evaluation data. The sample size used in this research study is small. Therefore, this is not representing a broader context.

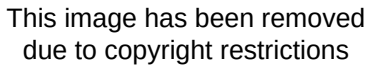
If possible, addressing these limitations will help achieve higher evaluation outcomes. For instance, increasing the number of initial contacts for the snowball method or providing compensation for expert participation could help mitigate some of the identified limitations.

This chapter presented the evaluation of the proposed security framework. The analysis of the interview results was presented. The next chapter presents a Discussion of this research study.

7 DISCUSSION

This chapter presents a detailed discussion of the proposed security framework, which encompasses nine security elements. Each element is accompanied by detailed descriptions, purposes, and outputs, all of which are designed to address the research questions and gaps identified in the literature. The chapter also provides a discussion on the application of this security framework. Furthermore, the discussion chapter includes the intellectual knowledge gained by the researcher, lessons learned, and future directions for this research.

This research employed the DSRM Process Model, a systematic approach that progresses logically through six steps: Identify the Problem & Motivation, Define the Objectives of a Solution, Design & Development, Demonstration, Evaluation and Communication. A brief summary is presented in each step, aligning with this research.



1. Identify the Problem & Motivation

The research process started with the analysis of academic literature, grey literature, and industry security reports to understand the security posture of IoT-based digital health systems, the current and constantly evolving security landscape, security incidents and breaches, trends of threats and vulnerabilities, the common attack surfaces, and security challenges. These understandings paved the way for identifying gaps in the literature and the improvements needed to strengthen the security of IoT networks.

2. Define the Objectives of a Solution

The primary research objective of the proactive security framework is to ensure end-to-end security for IoT networks in digital health systems. Proactive defence means a framework that caters to the constant evolution of security issues and prevents the rise of actual security incidents.

3. Design & Development

This research has developed a proactive defence security framework with nine security elements as the primary artifact. Four stages were incorporated to implement the proposed security framework: preparation, active monitoring and actioning, contributing, and strengthening. Further, a detailed step-by-step guide with six phases is included in the research to apply the proposed security framework to IoT networks.

4. Demonstration

The step-by-step guide was used to demonstrate the proposed security framework's practical application using a desk study providing working examples. The selected context is a “Remote Health Monitoring System” from academic literature.

5. Evaluation

The proposed security framework was evaluated using a desk study and expert interviews. The desk study covered the practical aspects, while expert interviews captured the specialist advice of security professionals in the industry. The proposed security framework was evaluated against a set of evaluation criteria.

6. Communication

In line with the communications step of the design science methodology, this research is documented as the PhD thesis of the researcher. Importantly, the results of this research will contribute to academic papers on proactive security in IoT networks in the digital health space.

7.1 Key Findings

7.1.1 Development of the Framework

This research developed a framework for the Proactive Defence of an IoT network, specifically for use in Digital Health, to prevent attacks and minimise potential loss, damage, destruction, or impact from cyber security incidents. To be proactive, such a security framework must consider many aspects, such as the constant evolution of the security landscape, pre-identification of threats and vulnerabilities, continuous security protection, and maintaining defence levels.

In developing the security framework, nine security elements were identified through the analysis of the academic literature, grey literature and industry security reports. The mix of these sources provided the opportunity to understand the security posture of IoT-based digital health systems, the current and constantly evolving security landscape, security incidents and breaches, trends of threats and vulnerabilities, common attack surfaces, and security challenges. These understandings paved the way to identify the gaps in existing frameworks found in literature, the improvements needed to strengthen the security of IoT networks and to build an advanced, robust, result-oriented, usable and comprehensive security framework to protect IoT networks from security threats and attacks.

One of the objectives was to use the existing resources and current technologies rather than developing new components. Opportunities have been examined to enhance existing resources and use current technologies to improve and increase the framework's effectiveness. The main areas of IoT security, as well as IoT security weaknesses and failures, were considered during the framework's development. The three main characteristics of information security; confidentiality, availability, and integrity were significant priorities during the framework's construction.

Table 36 presents the nine security elements included in the security framework, with descriptions, purposes, and outputs.

Table 39 – Security Elements Included in the Security Framework

Security element	Description	Purpose	Research outputs
1. Threat Landscaping	Threat Landscaping refers to understanding existing, most recent, and potential threats, their behaviour, and how they affect the IoT network.	• To obtain a solid understanding of the threats, vulnerabilities and the potential risk. • The findings from this activity provide the necessary information to input into the threat modelling activity (Security element #2).	• The development of a threat landscape using information sources, threat intelligence, and human expertise (Figure 19). • A table format was developed to conduct a threat landscape (Chapter 4—Application and Implementation of the Framework, Table 13). The resulting table maps threats to architectural layers, segments, and components (Chapter 5—Demonstration of the Framework, Table 21, 22, 23). • The findings from Threat Landscaping provide the necessary information for threat modelling security elements.
2. Threat Modelling	Threat Modelling is used to eradicate, prevent, minimise or mitigate the impact that threats can have on an ICT system. With a sound understanding of the impact by identifying threats from the threat landscaping	• Threat modelling will result in a sound understanding of the threats and their impact. • Threats can be mapped to the IoT architecture, preventive actions can be planned, and mitigation and countermeasures can be implemented.	• A table format developed to conduct threat modelling activity (Chapter 4—Application and Implementation of the Framework, Table 14). • The resulting table of 14 is a threat model according to the architecture and nature of the threat (Chapter 5—Demonstration of the Framework, Table 24, 25, 26).

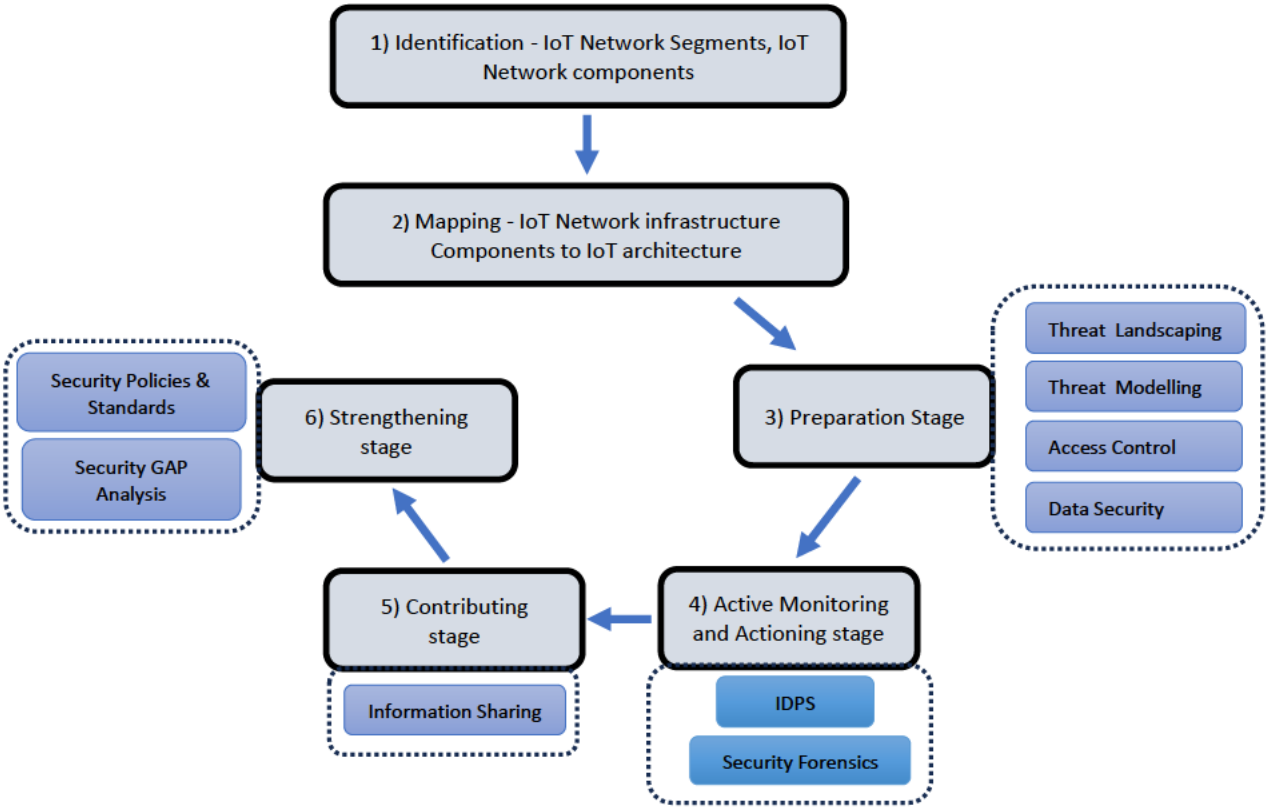
	activity, threat classifications and test cases can be developed in the threat modelling activity.		
3. Access Control	Access Control ensures secure access by users, devices, applications and services by enforcing identification, authentication, authorisation and accountability.	• To preserve confidentiality, integrity and availability in the IoT Network. • Limit the network access and communication only to authorised entities.	• A detailed discussion about the access control models for resource constraint environments. • A Capabilities-based access control model for IoT networks based on the IoT architecture (activity (Chapter 4—Application and Implementation of the Framework, Figure 22).
4. Data Security	Data Security secures the data during the IoT network's transmission, processing, storage and application phases.	• To preserve confidentiality, integrity and data availability in the IoT Network. • Prevent unauthorised access, tampering or damage until data reaches the destination.	• An approach to map an end-to-end data flow in a layered architecture for an IoT network (Chapter 4 – Application and Implementation of the Framework, Figure 23). • A method to encrypt data using public key cryptography and Elliptic curve cryptography (Chapter 4 – Application and Implementation of the Framework, Figure 24). • Recommendations include keeping encrypted backup onsite and off-site, data de-identification and data masking for data at rest.
5. Intrusion Detection and Prevention	Intrusion Detection and Prevention is to detect	• To detect known and new attacks.	• The intrusion detection and prevention system (IDPS) deployment method is based on the IoT architecture, where the inbound and outbound network traffic can be monitored centrally

	anomalies, malicious intrusions or new attacks on the network using various automated or manual methods and techniques. Prevention refers to implementing preventive actions once detected without human involvement.	• To use new attack information to create threat intelligence. • To feed the new attack details to update threat sources. • Use new attack details for "Threat Landscaping" activity.	(Chapter 4 – Application and Implementation of the Framework, Figure 25). • Important insights about IDPS's placement strategies, detection methods and security threats (Chapter 5 - Demonstration of the Framework, Figure 35). • The application process of an IDPS to an IoT network.
6. Digital Forensics	Digital Forensics is used to conduct further investigations after an incident alert is generated from the IDPS in the IoT network.	• This is to investigate and find the root cause for the incident triggered by the IDPS.	• Identify potential and new threats and attacks. • Update the new data with existing Intrusion detection data models. • The digital forensics investigation application process to an IoT network is done using a layered approach (Chapter 4 - Application and Implementation of the Framework, Figure 26). • Findings from digital forensics about potential and new threats feed into the "Information Sharing" security element and can be used as threat intelligence.
7. Information sharing	Information sharing is to share findings from digital forensics about potential and new threats and attacks internally and	• Use of such information to take preventive actions and improve the security posture of the IoT network	• Exchanging such security information among similar interested entities increases their knowledge and understanding of the security threats they may face.

	externally with similar interested parties.		• A proposed way to share security information (Chapter 4—Application and Implementation of the Framework, Figure 27).
8. Information security policy	Information Security Policy provides specific instructions for required security configuration and guidance on adequately using particular systems within the organisation.	• To guide the configuration of the selected system-specific aspect of an IoT Network.	• A template for documenting system-specific security configuration details (Chapter 4—Application and Implementation of the Framework, Figure 28).
9. GAP Analysis	GAP Analysis assesses the organisation's current security posture compared to an industry-best standard.	• To identify the security gaps in the existing security measures and to improve them.	• This framework proposes a security GAP analysis of the primary network infrastructure as a recommendation because failure to secure the primary network presents a vulnerability to the IoT network.

7.1.2 Application of the Framework

An understanding of the breadth, complexity, and visibility of an IoT network is needed to apply any security solution. To gain this understanding, a clear picture of the architectural structure of the IoT network, IoT devices, how they are interconnected, network media used, software and hardware components and technology used in the IoT network, and end-to-end data flow is needed. A layered IoT architecture was used to achieve this, and IoT network segments and components were identified and mapped to IoT architecture, as explained in Chapter 4, Section 4.5.



Further, the security elements were grouped, and four stages were introduced: preparation, active monitoring and action, contribution, and strengthening. The groups highlight the relationship between each security element and how the individual security element contributes to other elements within the framework to improve its functions and be more result-oriented. The objective of the preparation stage is to prepare each IoT architecture layer for proactive defence by applying the security elements: threat landscape, threat modelling, access control, and data security. The active monitoring and actioning stage aims to provide continuous security protection by monitoring the IoT network traffic. Intrusion detection and prevention (IDPS) and forensic investigations security elements are used to achieve this. The contributing stage is focused on how security information can be shared with service providers and relevant security agencies to take preventive actions. Sharing such security information contributes to keeping the security information sources

updated and available for access. The strengthening stage looks at increasing the defence level by introducing information security policies and highlighting the primary network's security level.

7.1.3 Intellectual knowledge gained during the research

Gaining visibility of an IoT network was achieved by developing table formats to capture IoT network segments and components (IoT infrastructure details) and mapping them to the IoT architecture. Resulting tables and mapping outputs enable the implementation of security elements in the IoT architectural layers to strengthen defence. Data security in the perception and network layers is an example.

The interrelationships and feedback loops within the security elements have been identified to improve their functionality and achieve better results, such as IDPS, Digital Forensics, and Threat Intelligence. The security elements have been grouped, and the stage approach has been introduced to achieve this.

The need for a proper step-by-step framework implementation process was understood during the application and implementation phase: “How do I apply the framework?” To accomplish this, a step-by-step guide with six phases was introduced. Further, the staged approach was embedded in phases three to six, as described in Chapter 4, Section 4.5, Figure 17).

In addition to the above, further knowledge was gained through the challenges faced during the demonstration phase as a desk study, discussed in Chapter 5, Section 5.2.

7.1.4 Lesson Learned

Conducting expert interviews for artifact evaluation: Six industry experts were contacted and invited to review and participate in an evaluation of the proposed security framework resulting from this research. Employing the snowball method, these experts were asked to forward the invitation to other experts in their network. The objective was to conduct at least ten interviews. The expectation was that six people forwarding the invitation could generate an additional 6 contacts. This would bring the total of potential reviewers to 12. It seems that the Snowball method is beyond the control of the researcher. Alternatively, the number of initial contacts should be much larger to succeed with the Snowball method. Six initial contacts resulted in 2 interviews and a third interview resulted from the Snowball method. Therefore, based on these numbers, a much larger sample size of initial contacts is needed to generate 10 interviews. For example, 2 contacts generated 1

snowball contact. Thus, 18 initial contacts could result in 6 initial acceptances and 3 snowball acceptances total of 9 interviews. In this case, 20 initial contacts would more likely have produced a larger sample of interviews.

Implementing security mechanisms in IoT networks in the real world is a challenge, especially when compared to traditional ICT networks. A comprehensive understanding of the security requirements is not just important, it's essential. It needs to be based on the type of devices used, where they are deployed, device connectivity, network connectivity, and technologies used. The need to gain comprehensive visibility of the IoT network is realised. To achieve this, necessary table formats were developed to capture the IoT infrastructure details and map them to the IoT architecture.

7.1.5 Future Directions

Testing any security framework for applicability, feasibility, reliability, and quality before deployment is essential. Future research should consider applying and testing the proposed security framework and security elements' functions in other IoT networks. This will address any issues arising during the application. This PhD research focused on IoT networks in the digital health space. Applying this security framework to any other industry in future work could resolve issues with broad applicability.

Future research should incorporate the proposed security framework and a routine checklist, indicating where each phase and security element is completed, how often it is revisited, and how frequently it is updated. For example, Phase 1— “Identification of IoT Network Segments and IoT Network Components”. This will ensure that any IoT devices are added later to the network and that their details are captured in the records. Revisiting and updating threat landscaping and modelling security elements would ensure they are up to date with the evolving threats and vulnerabilities.

Future research on the proposed security framework could include more expert interviews to gather feedback on the evaluation from different perspectives, such as academics, chief information security officers (CISOs), penetration testers, etc. Feedback during the interview process suggested the potential of automating and integrating artificial intelligence (AI) into security elements, and this could be explored future. This may include developing a threat landscape, modelling it to an IoT network, and auto-updating is an area for possible automation. As artificial intelligence (AI) can

support self-learning and decision-making processes, integrating AI into intrusion detection and prevention security elements can increase detection accuracy and speed.

Further, expert interviews highlighted the need to include and define the roles, responsibilities, and expertise needed to implement the proposed security framework. This represents future research to identify and clearly define roles and responsibilities that any organisation can then apply or implement within their organisational structure.

Also, a mechanism should be incorporated into the framework to communicate with IoT device manufacturers about the need to update with findings from forensic investigations to improve the IoT device's operating system security or security flaws.

Further, five future projects have been designed for postgraduate students to conduct as their masters thesis projects. These include applying and implementing the framework security elements: threat landscaping, threat modelling, access control, data security and intrusion detection and prevention. Three of these projects are underway in Semester 1, 2024. The following results are expected:

a) encryption of IoT data streams in an IoT network in digital health systems (data security)
b) an open-source intrusion detection system in an IoT network in digital health systems (IDPS)
c) a zero-trust approach in an IoT network in digital health systems (access control).

8 CONCLUSION

This chapter summarises the proposed security framework's research background, problem, questions, and key characteristics. It provides evidence of how the key research questions are answered and outlines the key findings. Further, it discusses the research's impact on practice, theory, and literature. Finally, it provides the conclusion of this research.

8.1 Research background, problem and research questions

The Internet of Things (IoT) connects many heterogeneous devices to build an always-connected and intelligent world. IoT and its applications are adopted by people in their day-to-day lives, such as SMART watches, fitness trackers, blood glucose monitors and so on. Also, IoT applications are now used in industries such as SMART cities, healthcare, transportation, manufacturing, and agriculture.

Today, people have come to a point where they are dependent on technology. Information technologies are increasingly being applied in the healthcare industry to minimise human errors, reduce medical treatment inefficiencies, administration inefficiencies and improve clinical outcomes (Alotaibi & Federico, 2017). IoT devices are deployed increasingly to enhance healthcare systems as well as the health and safety of individuals. Such devices include wearables, implantable devices, monitoring systems, fall detection and vital sign monitoring.

This research developed a security framework for the proactive defence of IoT networks, specifically for IoT technologies in digital health. This is a result of reactive measures that have failed to reduce the time taken to identify and contain security incidents. Proactive defence means a framework that caters to the constant evolution of security issues and prevents the rise of actual incidents. The objective of being proactive is to pre-identify security risks and address them before they can become incidents, be in front of attacks to minimise them and increase the level of protection of digital health systems. Being proactive increases patient safety, improves productivity, improves business continuity and minimises financial loss.

The main research question, ‘How can a framework be developed and applied for proactive defence for IoT network security in digital health?’ is answered in two sub-questions: “What would a

proactive defence framework look like?" and "How could a proactive defence framework be applied in practice?".

8.2 Key characteristics of the proposed security framework

- A comprehensive security framework to provide end-to-end security for IoT networks in digital health systems.
- A security framework that caters to constantly evolving threats and vulnerabilities.
- A security framework that is technology-agnostic and vendor-neutral.
- A security framework that ensures the security elements are applied in each IoT architecture layer to provide a multi-layer secured architecture.
- Interrelated security elements multiply their effect to improve their function and increase the defence level.
- A comprehensive visibility of all connected devices, including the type of devices used, where they are deployed, device connectivity, network connectivity, and technologies used in the IoT network, mapped to the IoT architecture.
- Detailed step-by-step application process of the security framework to an IoT network.

The digital healthcare space is complex because multiple systems are integrated and interconnected and critical to deliver the required services and optimum patient care. Deploying IoT networks without proper security measures in this environment may create substantial security risks. Most IoT devices are built for a specific purpose with much less memory and computational power. Therefore, traditional security solutions cannot be installed, and this poses a challenge to securing them and the networks on which they run. IoT supports many areas of digital health, including real-time remote monitoring, chronic disease management using wearable and implantable devices, remote care, remote diagnosis, SMART elder care facilities, and health and fitness programmes due to seamless information collecting, transmission, and sharing across multiple platforms in healthcare systems. Security failures of IoT technology can be catastrophic because they are used for healthcare purposes, as mentioned.

In cybersecurity, the main challenge is how secure the information and communication technology systems. Due to the nature of IoT devices, applying traditional security measures is challenging, not straightforward, and insufficient. IoT networks use different ways to connect and different protocols. Applying a single security solution does not suit and is not sufficient. There is no universal

fit, common language, or ready-made solution that can be used or applied for IoT networks. Therefore, IoT networks are more prone to security threats and vulnerabilities.

The proposed security framework gives comprehensive visibility to the IoT network and provides a layered security approach. The main information security pillars, confidentiality, integrity, and availability, have been ensured by positioning security elements in each IoT architectural layers. This research covered end-to-end comprehensive security coverage to be proactive in many dimensions: Identifying relevant threats and mapping them to IoT networks, secure communication between layers, data security, continuous monitoring, digital forensics, and information sharing. Further, this research looked at multiple perspectives to proactively provide a maximum level of protection to an IoT network. It is not a good practice to rely on a single security solution or mechanism. More than one security solution must be implemented in multiple layers to provide the highest level of security. Therefore, this research introduced multiple security levels in case one fails and another to protect systems. For example, applying security elements in the perception layer and network layer.

Further, the proposed security framework can be used as a foundation to build proactive security protection for any network. For example, developing and modelling a threat landscape to the IoT network. Additionally, a security framework that is technology-agnostic and vendor-neutral. Framework users can use open-source or vendor-specific technology to implement a security element of their choice based on their circumstances. As an example, “Suricata” is an open-source IDS/IPS software compared to “ManageEngine Log360” and “SolarWinds”.

The study is significant as it applies a proactive rather than a reactive strategy. This is to be in front of attacks and to minimise the damage. A simple weakness is an opportunity for an attacker to launch an attack in seconds or minutes. Pre-identifying and addressing security risks limits the opportunity for hackers to get into a network. Deploying IoT without proper security measures may create considerable risks to the greater network. It creates an avenue for attackers to exploit weaknesses, resulting in disaster, such as a complete loss of a business.

8.3 Implications of the Study

As this artifact was developed as a framework rather than a model, any modifications, including adding new elements or excluding existing elements, can be accommodated to meet future requirements without changing the original research objectives.

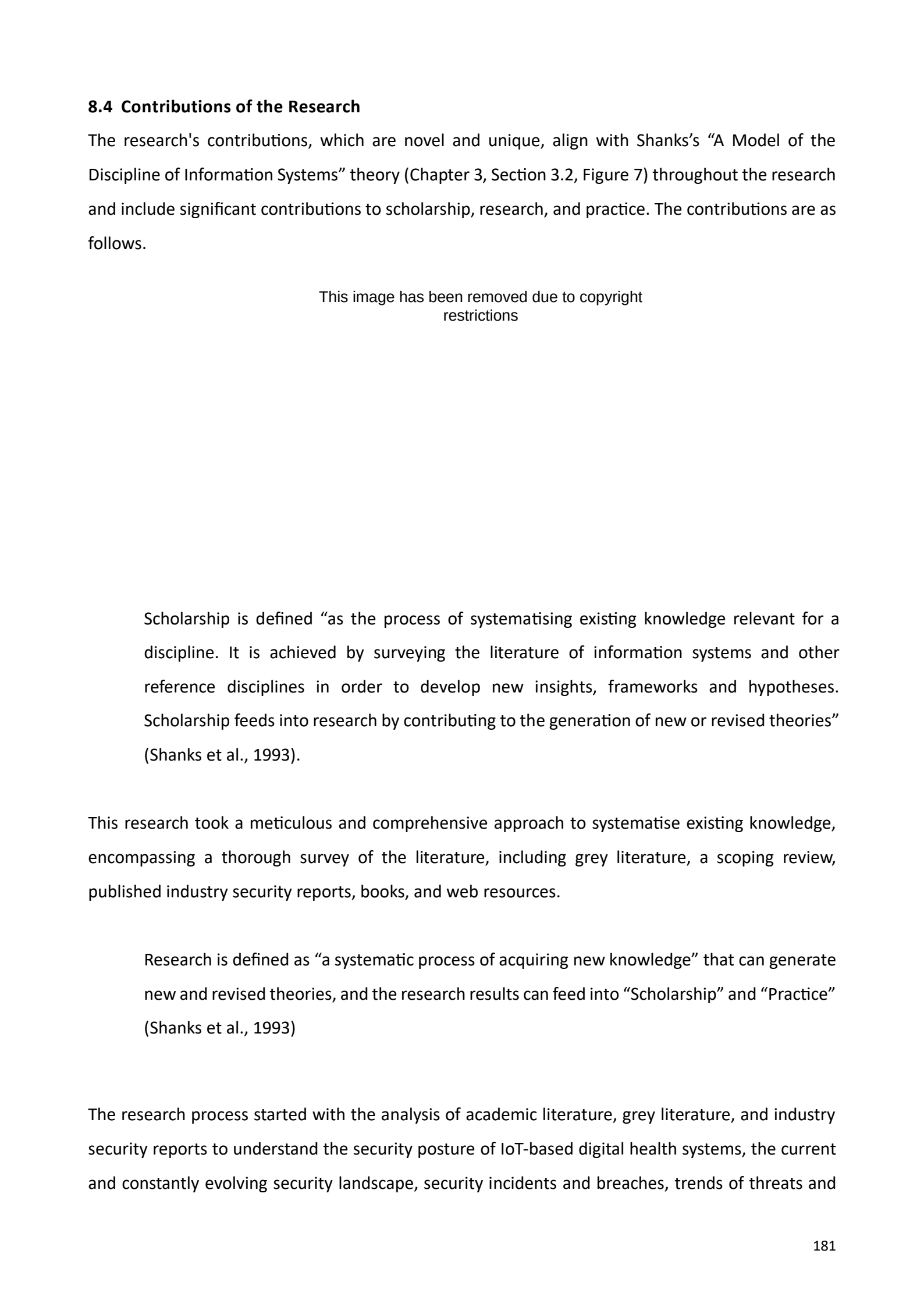
This research study leveraged existing resources and current technologies to develop a robust security framework, avoiding the need to invest time and money in developing novel components. Explored opportunities to enhance existing resources and utilise current technologies to improve and expand the framework's effectiveness. The development of the framework considered the main areas of IoT security, as well as IoT security weaknesses and failures.

Further, the proposed security framework is unaffected by technological changes. This refers to how this security framework is ready to respond, flexible, and agile regarding technology changes, such as IoT platform changes, Operating systems, Communication technology (Wi-Fi, Bluetooth, Zigbee), etc. None of the security elements use any proprietary or specific technology in this security framework. The framework was developed in a way that is vendor and technology-neutral. Therefore, the framework can respond to any technological changes and use open-source or vendor-specific technology to implement a security element of the user’s choice based on their circumstances.

Furthermore, this study also identified the need for step-by-step implementation to streamline the process, which covers layers and provides a multi-layer security architecture. It also included a detailed, step-by-step guide on applying the security framework to an IoT network, ensuring a smooth and effective implementation.

8.4 Contributions of the Research

The research's contributions, which are novel and unique, align with Shanks's "A Model of the Discipline of Information Systems" theory (Chapter 3, Section 3.2, Figure 7) throughout the research and include significant contributions to scholarship, research, and practice. The contributions are as follows.



> Scholarship is defined "as the process of systematising existing knowledge relevant for a discipline. It is achieved by surveying the literature of information systems and other reference disciplines in order to develop new insights, frameworks and hypotheses. Scholarship feeds into research by contributing to the generation of new or revised theories" (Shanks et al., 1993).

This research took a meticulous and comprehensive approach to systematise existing knowledge, encompassing a thorough survey of the literature, including grey literature, a scoping review, published industry security reports, books, and web resources.

> Research is defined as "a systematic process of acquiring new knowledge" that can generate new and revised theories, and the research results can feed into "Scholarship" and "Practice" (Shanks et al., 1993)

The research process started with the analysis of academic literature, grey literature, and industry security reports to understand the security posture of IoT-based digital health systems, the current and constantly evolving security landscape, security incidents and breaches, trends of threats and

vulnerabilities, the common attack surfaces, and security challenges. These understandings paved the way for identifying gaps in the literature and the improvements needed to strengthen the security of IoT networks. The deep analysis and understanding contributed to identifying the security elements to be included in the security framework. The three main information security pillars; confidentiality, availability, and integrity were significant priorities in determining the security elements for the framework.

> Practise refers to using “Scholarship” and “Research” to improve the practice (Shanks et al., 1993).

This study makes an important theoretical contribution by developing a proactive defence security framework for IoT networks in digital health systems. The proposed security framework consists of nine security elements and ensures that the security elements are applied in each IoT architecture layer to provide a multi-layer secured architecture. A step-by-step guide with six phases is included to implement the proposed security framework. The proposed security framework can readily be used as a foundation for building proactive security protection for IoT networks. This framework, with its practical implications, can provide end-to-end security protection, making it highly relevant and applicable in real-world scenarios.

8.5 Limitations of the Study

Considering the broad context of IoT Networks in the digital health space, this study’s evaluation is confined to a desk study and expert interviews. The limitations of these are discussed in detail in the respective chapters.

The desk study's selected case was “Remote Patient Monitoring.” Selecting more cases from different perspectives, i.e., wearables, implantable devices, monitoring systems, fall detection, and vital sign monitoring, would elaborate on the potential benefits and challenges of applying the proposed security framework in real-world scenarios.

Further, the use of a simulated attack and how the proposed security elements can contribute to safeguarding such attacks would have showcased the proposed security framework's real-time impact.

In closing, Cybersecurity is an area that needs constant attention. We must promote cybersecurity awareness, deeper discussions and research to accomplish security goals. Regardless of the organisation's size, security solutions that can provide end-to-end security must be applied to any IoT network to prevent catastrophic impacts, particularly in the healthcare industry. Understanding the evolving nature of the threats and vulnerabilities and addressing them is essential to develop defence strategies. A single security solution cannot provide a high level of security for an IoT network. The proposed security framework introduces proactive defence security by identifying threats and vulnerabilities and modelling them in advance, implementing access control and data security in multiple architectural layers, constantly monitoring the network traffic for intrusions, conducting digital forensic investigations, sharing security information, information security policies and recommending ways to secure the primary network.

9 REFERENCES

Abdul-Ghani, H. A., Konstantas, D., & Mahyoub, M. (2018). A Comprehensive IoT Attacks Survey based on a Building-blocked Reference Model. *International Journal of Advanced Computer Science and Applications*, *9*, Article 3. https://doi.org/10.14569/IJACSA.2018.090349

Abouelmehdi, K., Beni-Hssane, A., Khaloufi, H., & Saadi, M. (2017). Big data security and privacy in healthcare: A Review. *Procedia Computer Science*, *113*, 73-80. https://doi.org/https://doi.org/10.1016/j.procs.2017.08.292

Aguiar, A. (2000). A minimalist approach to framework documentation. 143-144. https://doi.org/10.1145/367845.368050

Ahmad, I., Namal, S., Ylianttila, M., & Gurtov, A. (2015). Security in Software Defined Networks: A Survey. *IEEE Communications Surveys & Tutorials*, *17*(4), 2317-2346. https://doi.org/10.1109/COMST.2015.2474118

Ahmed, A. H., Omar, N. M., & Ibrahim, H. M. (2019, 8-10 Dec. 2019). Secured Framework for IoT Using Blockchain. 2019 Ninth International Conference on Intelligent Computing and Information Systems (ICICIS),

Alaba, F. A., Othman, M., Hashem, I. A. T., & Alotaibi, F. (2017). Internet of Things security: A survey. *Journal of Network and Computer Applications*, *88*, 10-28. https://doi.org/https://doi.org/10.1016/j.jnca.2017.04.002

Alotaibi, Y. K., & Federico, F. (2017). The impact of health information technology on patient safety. *Saudi medical journal*, *38*(12), 1173-1180. https://doi.org/10.15537/smj.2017.12.20631

Alsubaei, F., Abuhussein, A., & Shiva, S. (2017, 9-9 Oct. 2017). Security and Privacy in the Internet of Medical Things: Taxonomy and Risk Assessment. 2017 IEEE 42nd Conference on Local Computer Networks Workshops (LCN Workshops),

Aly, M., Khomh, F., Haoues, M., Quintero, A., & Yacout, S. (2019). Enforcing security in Internet of Things frameworks: A Systematic Literature Review. *Internet of Things*, *6*, 100050. https://doi.org/https://doi.org/10.1016/j.iot.2019.100050

Ammar, M., Russello, G., & Crispo, B. (2018). Internet of Things: A survey on the security of IoT frameworks. *Journal of Information Security and Applications*, *38*, 8-27. https://doi.org/https://doi.org/10.1016/j.jisa.2017.11.002

Andaloussi, Y., Ouadghiri, M. D. E., & Robieh, Z. S. M. A. (2020). Access Control Models for Smart Environments. In *Lecture Notes in Networks and Systems* (Vol. 92, pp. 13-18). https://doi.org/10.1007/978-3-030-33103-0_2

Anggorojati, B., Prasad, N. R., & Prasad, R. (2018). Capability-Based Access Control with ECC Key Management for the M2M Local Cloud Platform [Article]. *Wireless Personal Communications*, *100*(2), 519-538. https://doi.org/10.1007/s11277-017-5216-x

Arya, K. V., & Gore, R. (2020). Data security for WBAN in e-health IoT applications. In A. K. Singh & M. Elhoseny (Eds.), *Intelligent Data Security Solutions for e-Health Applications* (pp. 205-218). Academic Press. https://doi.org/https://doi.org/10.1016/B978-0-12-819511-6.00011-X

Asharf, J., Moustafa, N., Khurshid, H., Debie, E., Haider, W., & Wahab, A. (2020). A Review of Intrusion Detection Systems Using Machine and Deep Learning in Internet of Things: Challenges, Solutions and Future Directions. *Electronics*, *9*(7), 1177. https://www.mdpi.com/2079-9292/9/7/1177

Atzori, L., Iera, A., & Morabito, G. (2011). SIoT: Giving a social structure to the internet of things [Article]. *IEEE Communications Letters*, *15*(11), 1193-1195, Article 6042288. https://doi.org/10.1109/LCOMM.2011.090911.111340

Aufner, P. (2020). The IoT security gap: a look down into the valley between threat models and their implementation. *International Journal of Information Security*, *19*(1), 3-14. https://doi.org/10.1007/s10207-019-00445-y

Bonomi, F., Milito, R., Natarajan, P., & Zhu, J. (2014). Fog Computing: A Platform for Internet of Things and Analytics. In N. Bessis & C. Dobre (Eds.), *Big Data and Internet of Things: A Roadmap for Smart Environments* (pp. 169-186). Springer International Publishing. https://doi.org/10.1007/978-3-319-05029-4_7

Bradley, D., Russell, D., Ferguson, I., Isaacs, J., MacLeod, A., & White, R. (2015). The Internet of Things – The future or the end of mechatronics. *Mechatronics*, *27*, 57-74. https://doi.org/https://doi.org/10.1016/j.mechatronics.2015.02.005

Butun, I., Morgera, S. D., & Sankar, R. (2014). A Survey of Intrusion Detection Systems in Wireless Sensor Networks. *IEEE Communications Surveys & Tutorials*, *16*(1), 266-282. https://doi.org/10.1109/SURV.2013.050113.00191

Cäsar, M., Pawelke, T., Steffan, J., & Terhorst, G. (2022). A survey on Bluetooth Low Energy security and privacy. *Computer Networks*, *205*, 108712. https://doi.org/https://doi.org/10.1016/j.comnet.2021.108712

Chadwick, D. W., Fan, W., Constantino, G., de Lemos, R., Di Cerbo, F., Herwono, I., Manea, M., Mori, P., Sajjad, A., & Wang, X.-S. (2020). A cloud-edge based data security architecture for sharing and analysing cyber threat information. *Future Generation Computer Systems*, *102*, 710-722. https://doi.org/https://doi.org/10.1016/j.future.2019.06.026

Chakraborty, M., Jana, B., & Mandal, T. (2018, 27-28 July 2018). Implementation Of An Efficient Security Scheme Through Elliptic Curve Cryptography Based Radio-Frequency Identification(RFID) In Context Of Internet Of Things. 2018 International Conference on Recent Innovations in Electrical, Electronics & Communication Engineering (ICRIEECE),

Chandola, V., Banerjee, A., & Kumar, V. (2009). Anomaly detection: A survey [Review]. *ACM Computing Surveys*, *41*(3), Article 15. https://doi.org/10.1145/1541880.1541882

Chang, T. Y., & Hsieh, C. J. (2018). Detection and analysis of distributed denial-of-service in internet of things-employing artificial neural network and apache spark platform [Article]. *Sensors and Materials*, *30*(4), 857-867. https://doi.org/10.18494/SAM.2018.1789

Chattopadhyay, A. K., Nag, A., Ghosh, D., & Chanda, K. (2019). A secure framework for IoT-based healthcare system. In *Advances in Intelligent Systems and Computing* (Vol. 811, pp. 383-393).

Chatzis, P., & Stavrou, E. (2022). Cyber-threat landscape of border control infrastructures. *International Journal of Critical Infrastructure Protection*, *36*, 100503. https://doi.org/https://doi.org/10.1016/j.ijcip.2021.100503

Chen, K., Zhang, S., Li, Z., Zhang, Y., Deng, Q., Ray, S., & Jin, Y. (2018a). Internet-of-Things Security and Vulnerabilities: Taxonomy, Challenges, and Practice. *Journal of Hardware and Systems Security*, *2*. https://doi.org/10.1007/s41635-017-0029-7

Chen, K., Zhang, S., Li, Z., Zhang, Y., Deng, Q., Ray, S., & Jin, Y. (2018b). Internet-of-Things Security and Vulnerabilities: Taxonomy, Challenges, and Practice. *Journal of Hardware and Systems Security*, *2*(2), 97-110. https://doi.org/10.1007/s41635-017-0029-7

Chen, L., Cooper, P., & Liu, Q. (2013). Security in Bluetooth Networks and Communications. In L. Chen, J. Ji, & Z. Zhang (Eds.), *Wireless Network Security: Theories and Applications* (pp. 77-94). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-36511-9_5

Coventry, L., & Branley, D. (2018). Cybersecurity in healthcare: A narrative review of trends, threats and ways forward [Review]. *Maturitas*, *113*, 48-52. https://doi.org/10.1016/j.maturitas.2018.04.008

da Costa, C. A., Pasluosta, C. F., Eskofier, B., da Silva, D. B., & da Rosa Righi, R. (2018). Internet of Health Things: Toward intelligent vital signs monitoring in hospital wards. *Artificial Intelligence in Medicine*, *89*, 61-69. https://doi.org/https://doi.org/10.1016/j.artmed.2018.05.005

Dhillon, P. K., & Kalra, S. (2016, 14-16 Oct. 2016). Elliptic curve cryptography for real time embedded systems in IoT networks. 2016 5th International Conference on Wireless Networks and Embedded Systems (WECON),

Dmytro S. Morozov, Tetiana A. Vakaliuk, Andrii A. Yefimenko, Nikitchuk, T. M., & Kolomiiets, R. O. (2023). Honeypot and cyber deception as a tool for detecting cyber attacks on critical infrastructure. *CEUR Workshop Proceedings*, *3374*, 81-96. https://ceur-ws.org/Vol-3374/paper06.pdf

Dresch, A., Lacerda, D., & Antunes Júnior, J. A. V. (2014). *Design Science Research: A Method for Science and Technology Advancement*. https://doi.org/10.1007/978-3-319-07374-3

Eaton, I., & McNett, M. (2020). Chapter Six - Protecting the data: Security and privacy. In M. McNett (Ed.), *Data for Nurses* (pp. 87-99). Academic Press. https://doi.org/https://doi.org/10.1016/B978-0-12-816543-0.00006-6

Edwin Raja S, & Ravi, R. (2020). A performance analysis of Software Defined Network based prevention on phishing attack in cyberspace using a deep machine learning with CANTINA approach (DMLCA) [Article]. *Computer Communications*, *153*, 375-381. https://doi.org/10.1016/j.comcom.2019.11.047

Elrawy, M. F., Awad, A. I., & Hamed, H. F. A. (2018). Intrusion detection systems for IoT-based smart environments: a survey. *Journal of Cloud Computing*, *7*(1), 21. https://doi.org/10.1186/s13677-018-0123-6

Fahmideh, M., & Zowghi, D. (2020). An exploration of IoT platform development. *Information Systems*, *87*, 101409. https://doi.org/https://doi.org/10.1016/j.is.2019.06.005

Fotiou, N., Siris, V. A., Polyzos, G. C., Kortesniemi, Y., & Lagutin, D. (2022, 22-26 May 2022). Capabilities-based access control for IoT devices using Verifiable Credentials. 2022 IEEE Security and Privacy Workshops (SPW),

Fuchsberger, A. (2005). Intrusion Detection Systems and Intrusion Prevention Systems. *Information Security Technical Report*, *10*(3), 134-139. https://doi.org/https://doi.org/10.1016/j.istr.2005.08.001

Galliers, R. (1991). Choosing Appropriate Information Systems Research Approaches: A Revised Taxonomy. *The Information Research Arena of the 90s*, 155–173.

Gao, S., Li, Z., Xiao, B., & Wei, G. (2018). Security Threats in the Data Plane of Software-Defined Networks [Article]. *IEEE Network*, *32*(4), 108-113, Article 8284050. https://doi.org/10.1109/MNET.2018.1700283

Ge, M., Cho, J.-H., Ishfaq, B., & Kim, D. (2020). Modeling and Analysis of Integrated Proactive Defense Mechanisms for Internet of Things. In (pp. 217-247). https://doi.org/10.1002/9781119593386.ch10

Gong, L. (1989, 1-3 May 1989). A secure identity-based capability system. Proceedings. 1989 IEEE Symposium on Security and Privacy,

Gouglidis, A., Salonikias, S., Mavridis, I., & Gritzalis, D. (2018). Access Control in Industrial Internet of Things. In. https://doi.org/10.1007/978-3-030-12330-7_5

Gupta, N., Tanwar, S., & Badotra, S. (2023, 2023//). Review of Software-Defined Network-Enabled Security. Computational Intelligence for Engineering and Management Applications, Singapore.

Gusmeroli, S., Piccione, S., & Rotondi, D. (2013). A capability-based security approach to manage access control in the Internet of Things. *Mathematical and Computer Modelling*, *58*(5), 1189-1205. https://doi.org/https://doi.org/10.1016/j.mcm.2013.02.006

Gyamfi, E., & Jurcut, A. (2022). Intrusion Detection in Internet of Things Systems: A Review on Design Approaches Leveraging Multi-Access Edge Computing, Machine Learning, and Datasets. *Sensors (Basel)*, *22*(10). https://doi.org/10.3390/s22103744

Habib, K., Torjusen, A., & Leister, W. (2015). *Security Analysis of a Patient Monitoring System for the Internet of Things in eHealth*.

Haig, B. D. (2010). Encyclopedia of Research Design. In. SAGE Publications, Inc. https://doi.org/10.4135/9781412961288

Harsha, B. R., Damodaran, A., Ranganath, S., Raut, V., & Holla, S. (2019, 20-21 Dec. 2019). An approach to enable secure and reliable communication on IoT Devices. 2019 4th International Conference on Computational Systems and Information Technology for Sustainable Solution (CSITSS),

Hermes, S., Riasanow, T., Clemons, E. K., Böhm, M., & Krcmar, H. (2020). The digital transformation of the healthcare industry: exploring the rise of emerging platform ecosystems and their influence on the role of patients [Article]. *Business Research*, *13*(3), 1033-1069. https://doi.org/10.1007/s40685-020-00125-x

Hernández-Ramos, J., Jara, A. J., Marin, L., & Skarmeta, A. (2013). *Distributed Capability-Based Access Control for the Internet of Things*.

Hevner, A. (2007). *A Three Cycle View of Design Science Research* (Vol. 19).

Hevner, A., & Chatterjee. (2010). *Design Research in Information Systems: Theory and Practice* (Vol. 22). https://doi.org/10.1007/978-1-4419-5653-8

Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design Science in Information Systems Research. *MIS Quarterly*, *28*(1), 75-105. https://doi.org/10.2307/25148625

Hodo, E., Bellekens, X., Hamilton, A., Dubouilh, P., Iorkyase, E., Tachtatzis, C., & Atkinson, R. (2016, 11-13 May 2016). Threat analysis of IoT networks using artificial neural network intrusion detection system. 2016 International Symposium on Networks, Computers and Communications (ISNCC),

Hossain, M. M., Fotouhi, M., & Hasan, R. (2015, 27 June-2 July 2015). Towards an Analysis of Security Issues, Challenges, and Open Problems in the Internet of Things. 2015 IEEE World Congress on Services,
Hou, J., Qu, L., & Shi, W. (2019). A survey on internet of things security from data perspectives. *Computer Networks*, *148*, 295-306. https://doi.org/https://doi.org/10.1016/j.comnet.2018.11.026

Hu, V. C., & Scarfone, K. (2012). *Guidelines for Access Control System Evaluation Metrics*.

Ibrahim, A., Mahmood, B., & Singhal, M. (2016, 4-7 Oct. 2016). A Secure Framework for Medical Information Exchange (MI-X) between Healthcare Providers. 2016 IEEE International Conference on Healthcare Informatics (ICHI),

Islam, M., & Aktheruzzaman, K. (2020). An Analysis of Cybersecurity Attacks against Internet of Things and Security Solutions. *Journal of Computer and Communications*, *8*, 11-25. https://doi.org/10.4236/jcc.2020.84002

Istepanian, R. s. H. (2011). *The potential of Internet of Things (IOT) for assisted living applications*. https://doi.org/10.1049/ic.2011.0040

Ja'fari, F., Mostafavi, S., Mizanian, K., & Jafari, E. (2021). An intelligent botnet blocking approach in software defined networks using honeypots [Article]. *Journal of Ambient Intelligence and Humanized Computing*, *12*(2), 2993-3016. https://doi.org/10.1007/s12652-020-02461-6

Jain, A., Singh, T., & Sharma, S. K. (2018, 29-31 Aug. 2018). Threats Paradigmin IoT Ecosystem. 2018 7th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO),

Janjua, N. K., Hussain, M., Afzal, M., & Ahmad, H. F. (2009, 1-3 June 2009). Digital health care ecosystem: SOA compliant HL7 based health care information interchange. 2009 3rd IEEE International Conference on Digital Ecosystems and Technologies,

Jayaraman, P. P., Forkan, A. R. M., Morshed, A., Haghighi, P. D., & Kang, Y. B. (2020). Healthcare 4.0: A review of frontiers in digital health [Review]. *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*, *10*(2), Article e1350. https://doi.org/10.1002/widm.1350

John, P., John, B., Mayank, B., Rhonda, S., Lily, C., & Karen, S. (2022). Guide to Bluetooth Security. In: Special Publication (NIST SP), National Institute of Standards and Technology, Gaithersburg, MD.

Johnson, R., & Foote, B. (1988). Designing Reusable Classes. *Journal of Object-Oriented Programming*, *1*, 22textendash35.

Kain, R. Y., & Landwehr, C. E. (1987). On Access Checking in Capability-Based Systems. *IEEE Transactions on Software Engineering*, *SE-13*(2), 202-207. https://doi.org/10.1109/TSE.1987.232892

Kamatchi, R., & Ambekar, K. (2016). Analyzing impacts of cloud computing threats in attack based classification models. *Indian J. Sci. Technol*, *9*(21), 1-7.

Kebande, V. R., & Ray, I. (2016, 22-24 Aug. 2016). A Generic Digital Forensic Investigation Framework for Internet of Things (IoT). 2016 IEEE 4th International Conference on Future Internet of Things and Cloud (FiCloud),

Kent, K., Chevalier, S., Grance, T., & Dang, H. (2006). Guide to Integrating Forensic Techniques into Incident Response. *NIST Special Publication*.

Khan, Z., Pervez, Z., & Abbasi, A. G. (2017). Towards a secure service provisioning framework in a Smart city environment. *Future Generation Computer Systems*, *77*, 112-135. https://doi.org/https://doi.org/10.1016/j.future.2017.06.031
Khiangte, C., Das, P., & Das, R. (2017). Security Management perspective for Internet of Things.

Khraisat, A., Gondal, I., Vamplew, P., & Kamruzzaman, J. (2019). Survey of intrusion detection systems: techniques, datasets and challenges. *Cybersecurity*, *2*(1), 20. https://doi.org/10.1186/s42400-019-0038-7

Kouicem, D. E., Bouabdallah, A., & Lakhlef, H. (2018). Internet of things security: A top-down survey. *Computer Networks*, *141*, 199-221. https://doi.org/https://doi.org/10.1016/j.comnet.2018.03.012

Kruger, J.-L., & Venter, H. (2019). State of the art in Digital Forensics for the Internet of Things. In (pp. 588-596). Reading: Academic Conferences International Limited.

Kumar, P., & Lee, H. J. (2012). Security issues in healthcare applications using wireless medical sensor networks: a survey. *Sensors (Basel)*, *12*(1), 55-91. https://doi.org/10.3390/s120100055

Kumari, A., Kumar, V., Abbasi, M. Y., Kumari, S., Chaudhary, P., & Chen, C. (2020). CSEF: Cloud-Based Secure and Efficient Framework for Smart Medical System Using ECC. *IEEE Access*, *8*, 107838-107852. https://doi.org/10.1109/ACCESS.2020.3001152

La, Q. D., Quek, T. Q. S., Lee, J., Jin, S., & Zhu, H. (2016). Deceptive Attack and Defense Game in Honeypot-Enabled Networks for the Internet of Things. *IEEE Internet of Things Journal*, *3*(6), 1025-1035. https://doi.org/10.1109/JIOT.2016.2547994

Lara-Nino, C. A., Diaz-Perez, A., & Morales-Sandoval, M. (2020). Lightweight elliptic curve cryptography accelerator for internet of things applications. *Ad Hoc Networks*, *103*, 102159. https://doi.org/https://doi.org/10.1016/j.adhoc.2020.102159

Li, F., Han, Y., & Jin, C. (2016). Practical access control for sensor networks in the context of the Internet of Things. *Computer Communications*, *89-90*, 154-164. https://doi.org/https://doi.org/10.1016/j.comcom.2016.03.007

Li, M., Lou, W., & Ren, K. (2010). Data security and privacy in wireless body area networks. *IEEE Wireless Communications*, *17*(1), 51-58. https://doi.org/10.1109/MWC.2010.5416350

Lim, S. B. (2019). Software defined network detection system [Article]. *International Journal of Recent Technology and Engineering*, *8*(3), 1391-1395. https://doi.org/10.35940/ijrte.B3549.098319

Liu, Y., Lu, Q., Chen, S., Qu, Q., O'Connor, H., Raymond Choo, K.-K., & Zhang, H. (2021). Capability-based IoT access control using blockchain. *Digital Communications and Networks*, *7*(4), 463-469. https://doi.org/https://doi.org/10.1016/j.dcan.2020.10.004

Lockl, J., Schlatt, V., Schweizer, A., Urbach, N., & Harth, N. (2020). Toward Trust in Internet of Things Ecosystems: Design Principles for Blockchain-Based IoT Applications. *IEEE Transactions on Engineering Management*, *67*(4), 1256-1270. https://doi.org/10.1109/TEM.2020.2978014

Loulianou, P., Vassilakis, V., & Moscholios, I. (2018). *A Signature-based Intrusion Detection System for the Internet of Things*.
Mahalle, P. N., Anggorojati, B., Prasad, N. R., & Prasad, R. (2012, 16-19 Dec. 2012). Identity driven capability based access control (ICAC) scheme for the Internet of Things. 2012 IEEE International Conference on Advanced Networks and Telecommunciations Systems (ANTS),

McGowan, A., Sittig, S., & Andel, T. (2021). *Medical Internet of Things: A Survey of the Current Threat and Vulnerability Landscape*. https://doi.org/10.24251/HICSS.2021.466
McLeod, A., & Dolezel, D. (2018). Cyber-analytics: Modeling factors associated with healthcare data breaches. *Decision Support Systems*, *108*, 57-68. https://doi.org/https://doi.org/10.1016/j.dss.2018.02.007

Mdletshe, S., Motshweneng, O. S., Oliveira, M., & Twala, B. (2023). Design science research application in medical radiation science education: A case study on the evaluation of a developed artifact. *Journal of Medical Imaging and Radiation Sciences*, *54*(1), 206-214. https://doi.org/https://doi.org/10.1016/j.jmir.2022.11.007

Miorandi, D., Sicari, S., De Pellegrini, F., & Chlamtac, I. (2012). Internet of things: Vision, applications and research challenges. *Ad Hoc Networks*, *10*(7), 1497-1516. https://doi.org/https://doi.org/10.1016/j.adhoc.2012.02.016

Mohanta, B. K., Jena, D., Ramasubbareddy, S., Daneshmand, M., & Gandomi, A. H. (2021). Addressing Security and Privacy Issues of IoT Using Blockchain Technology. *IEEE Internet of Things Journal*, *8*(2), 881-888. https://doi.org/10.1109/JIOT.2020.3008906

Muthusamy Ragothaman, K. N., & Wang, Y. (2021). A Systematic Mapping Study of Access Control in the Internet of Things.

Myers, J., Babun, L., Yao, E., Helble, S., & Allen, P. (2019). MAD-IoT: Memory anomaly detection for the internet of things. 2019 IEEE Globecom Workshops, GC Wkshps 2019 - Proceedings,

Nawir, M., Amir, A., Yaakob, N., & Lynn, O. B. (2016, 11-12 Aug. 2016). Internet of Things (IoT): Taxonomy of security attacks. 2016 3rd International Conference on Electronic Design (ICED),

Nelson, C. (1994). A Forum for Fitting the Task. *Computer*, *27*(3), 104–109.

Nieles, M., Dempsey, K., & Pillitteri, V. Y. (2017). An Introduction to Information Security - NIST SP 800-12 Rev. 1 [Publication]. (Revision 1).

NIST. (2016). *National Institute of Standards and Technology, Special Publication 800-150: Guide to Cyber Threat Information Sharing*. Retrieved from https://doi.org/10.6028/NIST.SP.800-150

Nogueira, V., & Carnaz, G. (2016). *An Overview of IoT and Healthcare*.

Oates, B. J., Griffiths, M., & McLean, R. (2022). *Researching Information Systems and Computing*. Sage Publications Ltd.

Oh, H., & Chae, K. (2008, 11-13 Nov. 2008). Real-Time Intrusion Detection System Based on Self-Organized Maps and Feature Correlations. 2008 Third International Conference on Convergence and Hybrid Information Technology,

Omar, T., Ho, A., & Urbina, B. (2019). Detection of DDoS in SDN Environment Using Entropy-based Detection. 2019 IEEE International Symposium on Technologies for Homeland Security, HST 2019,

Ouaddah, A., Mousannif, H., Abou Elkalam, A., & Ait Ouahman, A. (2017). Access control in the Internet of Things: Big challenges and new opportunities. *Computer Networks*, *112*, 237-262. https://doi.org/https://doi.org/10.1016/j.comnet.2016.11.007

Pal, S., Hitchens, M., & Varadharajan, V. (2020). Access control for Internet of Things—enabled assistive technologies: an architecture, challenges and requirements. In N. K. Suryadevara & S. C. Mukhopadhyay (Eds.), *Assistive Technology for the Elderly* (pp. 1-43). Academic Press. https://doi.org/https://doi.org/10.1016/B978-0-12-818546-9.00001-4

Pal, S., Hitchens, M., Varadharajan, V., & Rabehaja, T. (2018). Fine-Grained Access Control for Smart Healthcare Systems in the Internet of Things. *EAI Endorsed Transactions on Industrial Networks and Intelligent Systems*, *4*, 154370. https://doi.org/10.4108/eai.20-3-2018.154370

Patel, S., Patel, D. R., & Navik, A. P. (2016, 22-24 Jan. 2016). Energy efficient integrated authentication and access control mechanisms for Internet of Things. 2016 International Conference on Internet of Things and Applications (IOTA),

Peffers, K., Tuunanen, T., Gengler, C., & Rossi, M. (2006). The design science research process: a model for producing and presenting information systems research. *Proceedings Design Research Information Systems and Technology DESRIST'06*, *24*.

Peffers, K., Tuunanen, T., & Niehaves, B. (2018). Design science research genres: introduction to the special issue on exemplars and criteria for applicable design science research. *European Journal of Information Systems*, *27*(2), 129-139. https://doi.org/10.1080/0960085X.2018.1458066

Peffers, K., Tuunanen, T., Rothenberger, M., & Chatterjee, S. (2007a). A Design Science Research Methodology for Information Systems Research. *J. Manage. Inf. Syst.*, *24*(3), 45-77. https://doi.org/10.2753/mis0742-1222240302

Peffers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2007b). A Design Science Research Methodology for Information Systems Research. *Journal of Management Information Systems*, *24*(3), 45-77. https://doi.org/10.2753/MIS0742-1222240302

Pirc, J., DeSanto, D., Davison, I., & Gragido, W. (2016). 1 - Navigating Today's Threat Landscape. In J. Pirc, D. DeSanto, I. Davison, & W. Gragido (Eds.), *Threat Forecasting* (pp. 1-15). Syngress. https://doi.org/https://doi.org/10.1016/B978-0-12-800006-9.00001-X

Porter, M. E., & Heppelmann, J. E. (2014). How Smart, Connected Products Are Transforming Competition. *Harvard Business Review*, *92*, 18.

Prat, N., Wattiau, I., & Akoka, J. (2014). Artifact Evaluation in Information Systems Design Science Research ? A Holistic View. *Proceedings - Pacific Asia Conference on Information Systems, PACIS 2014*.

Ragothaman, K., Wang, Y., Rimal, B., & Lawrence, M. (2023). Access Control for IoT: A Survey of Existing Research, Dynamic Policies and Future Directions. *Sensors*, *23*(4), 1805. https://www.mdpi.com/1424-8220/23/4/1805

https://mdpi-res.com/d_attachment/sensors/sensors-23-01805/article_deploy/sensors-23-01805.pdf?version=1675669917

Rasmussen, J., Natsiavas, P., Votis, K., Moschou, K., Campegiani, P., Coppolino, L., Cano, I., Marí, D., Faiella, G., Stan, O., Abdelrahman, O., Nalin, M., Baroni, I., Voss-Knude, M., Vella, V. A., Grivas, E., Mesaritakis, C., Dumortier, J., Petersen, J., . . . Koutkias, V. (2018). Gap analysis for information security in interoperable solutions at a systemic level: The KONFIDO approach. IFMBE Proceedings,

Ravidas, S., Lekidis, A., Paci, F., & Zannone, N. (2019). Access control in Internet-of-Things: A survey. *Journal of Network and Computer Applications*, *144*, 79-101. https://doi.org/https://doi.org/10.1016/j.jnca.2019.06.017

Ray, P. P. (2016). A survey on Internet of Things architectures. *Journal of King Saud University - Computer and Information Sciences*, *30*(3), 291-319. https://doi.org/https://doi.org/10.1016/j.jksuci.2016.10.003
Ray, P. P. (2018). A survey on Internet of Things architectures. *Journal of King Saud University - Computer and Information Sciences*, *30*(3), 291-319. https://doi.org/https://doi.org/10.1016/j.jksuci.2016.10.003

Ray, P. P., Dash, D., Salah, K., & Kumar, N. (2021). Blockchain for IoT-Based Healthcare: Background, Consensus, Platforms, and Use Cases. *IEEE Syst J*, *15*(1), 85-94. https://doi.org/10.1109/JSYST.2020.2963840

Rotondi, D., & Piccione, S. (2012). *Managing Access Control for Things: a Capability Based Approach*. https://doi.org/10.4108/icst.bodynets.2012.250234

Sahay, R., Meng, W., & Jensen, C. D. (2019). The application of Software Defined Networking on securing computer networks: A survey. *Journal of Network and Computer Applications*, *131*, 89-108. https://doi.org/https://doi.org/10.1016/j.jnca.2019.01.019

Saleem, S., Ullah, S., & Kwak, K. S. (2011). A study of IEEE 802.15.4 security framework for wireless body area networks. *Sensors (Basel)*, *11*(2), 1383-1395. https://doi.org/10.3390/s110201383

Samarati, P., & de Vimercati, S. C. (2001, 2001//). Access Control: Policies, Models, and Mechanisms. Foundations of Security Analysis and Design, Berlin, Heidelberg.

Santos, L., Rabadao, C., & Gonçalves, R. (2018, 13-16 June 2018). Intrusion detection systems in Internet of Things: A literature review. 2018 13th Iberian Conference on Information Systems and Technologies (CISTI),

Schiller, E., Aidoo, A., Fuhrer, J., Stahl, J., Ziörjen, M., & Stiller, B. (2022). Landscape of IoT security. *Computer Science Review*, *44*, 100467. https://doi.org/https://doi.org/10.1016/j.cosrev.2022.100467

Sethi, P., & R. Sarangi, S. (2017). *Internet of Things: Architectures, Protocols, and Applications* (Vol. 2017). https://doi.org/10.1155/2017/9324035

Sethi, P., & Sarangi, S. R. (2017). Internet of Things: Architectures, Protocols, and Applications. *Journal of Electrical and Computer Engineering*, *2017*, 25, Article 9324035. https://doi.org/10.1155/2017/9324035

Shin, S., Xu, L., Hong, S., & Gu, G. (2016, 1-4 Aug. 2016). Enhancing Network Security through Software Defined Networking (SDN). 2016 25th International Conference on Computer Communication and Networks (ICCCN),

Simon, H. A. (1996). *The Sciences of the Artificial* (3rd ed.). MIT Press.

Sowjanya, K., & Dasgupta, M. (2019, 6-8 July 2019). Secure Ambient Assisted Living System using Elliptic Curve Cryptography based CPABE. 2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT),

Sowjanya, K., Dasgupta, M., & Ray, S. (2021). Elliptic Curve Cryptography based authentication scheme for Internet of Medical Things. *Journal of Information Security and Applications*, *58*, 102761. https://doi.org/https://doi.org/10.1016/j.jisa.2021.102761

Stamer, D., Zimmermann, O., & Sandkuhl, K. (2016). What is a framework? - A systematic literature review in the field of information systems. Lecture Notes in Business Information Processing,

Steingartner, W., Galinec, D., & Kozina, A. (2021). Threat defense: Cyber deception approach and education for resilience in hybrid threats model [Article]. *Symmetry*, *13*(4), Article 597. https://doi.org/10.3390/sym13040597

Stoyanova, M., Nikoloudakis, Y., Panagiotakis, S., Pallis, E., & Markakis, E. K. (2020). A Survey on the Internet of Things (IoT) Forensics: Challenges, Approaches and Open Issues. *IEEE Communications Surveys & Tutorials*, 1-1. https://doi.org/10.1109/COMST.2019.2962586

Suo, H., Wan, J., Zou, C., & Liu, J. (2012, 23-25 March 2012). Security in the Internet of Things: A Review. 2012 International Conference on Computer Science and Electronics Engineering,

Surange, G., & Khatri, P. (2021, 17-19 March 2021). IoT Forensics: A Review on Current Trends, Approaches and Foreseen Challenges. 2021 8th International Conference on Computing for Sustainable Global Development (INDIACom),

Tahir, M., Sardaraz, M., Muhammad, S., & Khan, M. S. (2020). A lightweight authentication and authorization framework for blockchain-enabled IoT network in health-informatics [Article]. *Sustainability (Switzerland)*, *12*(17), Article 6960. https://doi.org/10.3390/SU12176960

Tatam, M., Shanmugam, B., Azam, S., & Kannoorpatti, K. (2021). A review of threat modelling approaches for APT-style attacks. *Heliyon*, *7*(1), e05969. https://doi.org/https://doi.org/10.1016/j.heliyon.2021.e05969

Teperi, A.-M., Gotcheva, N., & Aaltonen, K. (2021). 16 - Design thinking perspective for developing safety management practices in nuclear industry. In A.-M. Teperi & N. Gotcheva (Eds.), *Human Factors in the Nuclear Industry* (pp. 309-326). Woodhead Publishing. https://doi.org/https://doi.org/10.1016/B978-0-08-102845-2.00016-8

Thamilarasu, G., & Chawla, S. (2019). Towards Deep-Learning-Driven Intrusion Detection for the Internet of Things. *Sensors (Basel)*, *19*(9). https://doi.org/10.3390/s19091977

Thapa, C., & Camtepe, S. (2021). Precision health data: Requirements, challenges and existing techniques for data security and privacy. *Computers in Biology and Medicine*, *129*, 104130. https://doi.org/https://doi.org/10.1016/j.compbiomed.2020.104130

Tomašić, I., Petrovic, N., Fotouhi, H., Lindén, M., & Björkman, M. (2017). *Data Flow and Collection for Remote Patients Monitoring: From Wireless Sensors through a Relational Database to a Web interface in Real Time*.

Uddin, M. A., Stranieri, A., Gondal, I., & Balasubramanian, V. (2020). Blockchain leveraged decentralized IoT eHealth framework. *Internet of Things*, *9*, 100159. https://doi.org/https://doi.org/10.1016/j.iot.2020.100159

Uzunov, A. V., & Fernandez, E. B. (2014). An extensible pattern-based library and taxonomy of security threats for distributed systems. *Computer Standards & Interfaces*, *36*(4), 734-747. https://doi.org/https://doi.org/10.1016/j.csi.2013.12.008

Vaishnavi, V., & Kuechler, B. (2004). Design Science Research in Information Systems. *Association for Information Systems*.

Varadharajan, V., & Bansal, S. (2016). Data Security and Privacy in the Internet of Things (IoT) Environment. In Z. Mahmood (Ed.), *Connectivity Frameworks for Smart Devices: The Internet of Things from a Distributed Computing Perspective* (pp. 261-281). Springer International Publishing. https://doi.org/10.1007/978-3-319-33124-9_11

Vargheese, R., & Viniotis, Y. (2014, 22-25 Oct. 2014). Influencing data availability in IoT enabled cloud based e-health in a 30 day readmission context. 10th IEEE International Conference on Collaborative Computing: Networking, Applications and Worksharing,

Venable, J. (2006). The role of theory and theorising in design science research. *First International Conference on Design Science Research in Information Systems and Technology*.
Venable, J., Pries-Heje, J., & Baskerville, R. (2016). FEDS: a Framework for Evaluation in Design Science Research. *European Journal of Information Systems*, *25*(1), 77-89. https://doi.org/10.1057/ejis.2014.36

Volk, M., Sterle, J., & Sedlar, U. (2015). Safety and Privacy Considerations for Mobile Application Design in Digital Healthcare [Article]. *International Journal of Distributed Sensor Networks*, *2015*, Article 549420. https://doi.org/10.1155/2015/549420

Whitman, M. E., & Mattord, H. J. (2022). *Principles of Information Security* (7th Edition ed.). Cengage Learning. https://books.google.com.au/books?id=59dUDgAAQBAJ

Williams, P. (2006). Making Research Real: Is Action Research a Suitable Methodology for Medical Information Security Investigations? *Australian Information Security Management Conference*.

Williams, P., Dutta, I. K., Daoud, H., & Bayoumi, M. (2022). A survey on security in internet of things with a focus on the impact of emerging technologies. *Internet of Things*, *19*, 100564. https://doi.org/https://doi.org/10.1016/j.iot.2022.100564

Williams, P., Rojas, P., & Bayoumi, M. (2019, 4-7 Aug. 2019). Security Taxonomy in IoT – A Survey. 2019 IEEE 62nd International Midwest Symposium on Circuits and Systems (MWSCAS),

Woodall, P., Borek, A., & Parlikad, A. K. (2016). Evaluation criteria for information quality research. *Int. J. Inf. Qual.*, *4*, 124-148.

Wu, M., Lu, T. J., Ling, F. Y., Sun, J., & Du, H. Y. (2010). Research on the architecture of Internet of Things. ICACTE 2010 - 2010 3rd International Conference on Advanced Computer Theory and Engineering, Proceedings,

Xiong, W., & Lagerström, R. (2019). Threat modeling – A systematic literature review. *Computers & Security*, *84*, 53-69. https://doi.org/https://doi.org/10.1016/j.cose.2019.03.010

Xu, R., Chen, Y., Blasch, E., & Chen, G. (2018). A federated capability-based access control mechanism for internet of things (IoTs). Proceedings of SPIE - The International Society for Optical Engineering,

Yeh, C. R., & Meskaran, F. (2022, 2-3 Dec. 2022). A Strategy for System Management Complexity: Availability on Data Backup and Recovery. 2022 IEEE 2nd International Conference on Mobile Networks and Wireless Communications (ICMNWC),

Yeng, P. K., Nweke, L. O., Woldaregay, A. Z., Yang, B., & Snekkenes, E. A. (2021). Data-Driven and Artificial Intelligence (AI) Approach for Modelling and Analyzing Healthcare Security Practice: A Systematic Review. In *Advances in Intelligent Systems and Computing* (Vol. 1250 AISC, pp. 1-18).

Zarpelão, B. B., Miani, R. S., Kawakani, C. T., & de Alvarenga, S. C. (2017). A survey of intrusion detection in Internet of Things. *Journal of Network and Computer Applications*, *84*, 25-37. https://doi.org/https://doi.org/10.1016/j.jnca.2017.02.009

Zawoad, S., & Hasan, R. (2015, 27 June-2 July 2015). FAIoT: Towards Building a Forensics Aware Eco System for the Internet of Things. 2015 IEEE International Conference on Services Computing,

Zemrane, H., Baddi, Y., & Hasbi, A. (2019). Improve IoT eHealth ecosystem with SDN. ACM International Conference Proceeding Series,

10 APPENDIX 1 – ETHICS APPROVAL

HUMAN ETHICS LOW RISK PANEL
APPROVAL NOTICE

Dear Mr Gihan Gunasekara,

The below proposed project has been **approved** on the basis of the information contained in the application and its attachments.

Project No:	6111
Project Title:	A Proactive Defence Framework for Internet of Things (IoT) Network Security for Digital Health
Chief Investigator:	Mr Gihan Gunasekara
Approval Date:	01/08/2023
Expiry Date:	22/12/2023
Approved Personnel:	Professor Trish Williams
Supervisory Panel:	Prof. Trish Williams, Prof Giselle Rampersad

Please note: *For all research projects wishing to recruit Flinders University students as participants, approval needs to be sought from the Pro Vice-Chancellor (Learning and Teaching Innovation), Professor Michelle Picard. To seek approval, please provide a copy of the Ethics approval for the project and a copy of the project application (including Participant Information and Consent Forms, advertising materials and questionnaires etc.) to the Pro Vice-Chancellor (Learning and Teaching Innovation) via michelle.picard@flinders.edu.au.*

RESPONSIBILITIES OF RESEARCHERS AND SUPERVISORS

1. Participant Documentation

Please note that it is the responsibility of researchers and supervisors, in the case of student projects, to ensure that:

- all participant documents are checked for spelling, grammatical, numbering and formatting errors. The Committee does not accept any responsibility for the above mentioned errors.
- the Flinders University logo is included on all participant documentation (e.g., letters of Introduction, information Sheets, consent forms, debriefing information and questionnaires – with the exception of purchased research tools) and the current Flinders University letterhead is included in the header of all letters of introduction. The Flinders University international logo/letterhead should be used and documentation should contain international dialing codes for all telephone and fax numbers listed for all research to be conducted overseas.

2. Annual Progress / Final Reports

In order to comply with the monitoring requirements of the *National Statement on Ethical Conduct in Human Research 2007 (updated 2018)* an annual progress report must be submitted each year on the approval anniversary date for the duration of the ethics approval using the HREC Annual/Final Report Form available online via the ResearchNow Ethics & Biosafety system.

Please note that no data collection can be undertaken after the ethics approval expiry date listed at the top of this notice. If data is collected after expiry, it will not be covered in terms of ethics. It is the responsibility of the researcher to ensure that annual progress reports

are submitted on time; and that no data is collected after ethics has expired.

If the project is completed *before* ethics approval has expired please ensure a final report is submitted immediately. If ethics approval for your project expires please either submit (1) a final report; or (2) an extension of time request (using the HREC Modification Form).

For student projects, the Low Risk Panel recommends that current ethics approval is maintained until a student's thesis has been submitted, assessed and finalised. This is to protect the student in the event that reviewers recommend that additional data be collected from participants.

3. Modifications to Project

Modifications to the project must not proceed until approval has been obtained from the Ethics Committee. Such proposed changes / modifications include:

- change of project title;
- change to research team (e.g., additions, removals, researchers and supervisors)
- changes to research objectives;
- changes to research protocol;
- changes to participant recruitment methods;
- changes / additions to source(s) of participants;
- changes of procedures used to seek informed consent;
- changes to reimbursements provided to participants;
- changes to information / documents to be given to potential participants;
- changes to research tools (e.g., survey, interview questions, focus group questions etc);
- extensions of time (i.e. to extend the period of ethics approval past current expiry date).

To notify the Committee of any proposed modifications to the project please submit a Modification Request Form available online via the ResearchNow Ethics & Biosafety system. Please note that extension of time requests should be submitted prior to the Ethics Approval Expiry Date listed on this notice.

4. Adverse Events and/or Complaints

Researchers should advise the Executive Officer of the Human Research Ethics Committee on at human.researchethics@flinders.edu.au immediately if:

- any complaints regarding the research are received;
- a serious or unexpected adverse event occurs that effects participants;
- an unforeseen event occurs that may affect the ethical acceptability of the project.

Yours sincerely,

Hendryk Flaegel

on behalf of

Human Ethics Low Risk Panel
Research Development and Support
human.researchethics@flinders.edu.au

Flinders University
Sturt Road, Bedford Park, South Australia, 5042
GPO Box 2100, Adelaide, South Australia, 5001

ResearchNow
Ethics & Biosafety