Performance Evaluation of Lightweight Cryptographic Algorithms for IoT in Healthcare

Tserendorj Chinbat

A thesis submitted to the Faculty of Design and Creative Technologies Auckland University of Technology

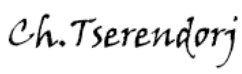
In partial fulfilment of the requirements for the degree of
Master of Information Security and Digital Forensics

School of Engineering, Computer and Mathematical Sciences

Auckland, New Zealand, September 2022

Declaration

I hereby declare that this submission is my work and that, to the best of my knowledge and belief, it contains no material previously published or written by another person nor material which to a substantial extent has been accepted for the qualification of any other degree or diploma of a University or other institution of higher learning, except where due acknowledgement is made in the acknowledgements.



Tserendorj Chinbat

September 2022

Acknowledgements

This thesis work is devoted to my beloved Teachers, Family, and Friends. I feel special gratitude for my beloved parents, wife, and two children. I would like to thank my research supervisor, Dr. Samaneh Madanian, for her valuable assistance and feedback throughout the process of this thesis.

Abstract

The significant number of objects interconnected to the Internet has grown as the Internet has become a more critical aspect of today's society. Network access, such as the Internet, is no longer restricted to personal computers, laptops, or data centers. It is now found in household items, automobiles, camera systems, implanted devices, as well as other items.

The healthcare industry has challenged securing and effectively collecting patients' medical data. Medical data is gathered from the patient's body utilising sensors or Internet of Things (IoT) devices, and securely transmitted to the healthcare system. Even though these medical devices are connected to the network, they must follow Information Security standards, such as confidentiality, integrity, and availability to secure their data. Furthermore, the healthcare service must respect patients' privacy and ensure sufficient protection for their data and information.

To avoid unauthorised access, it is necessary to establish data confidentiality from the beginning of the clinical treatment. As a result, medical data encryption is required from IoT medical devices, however, because of the limitations in their power, memory, and processor speed where traditional cryptographic algorithms are recognised as totally impractical. This has resulted in Lightweight Cryptography (LWC) compared to other traditional encryption methods, which can perform in devices that have limited resources, such as IoT medical devices.

This study has three main points. The first is to investigate potential IoT privacy and security issues in healthcare. And the second is to determine the most critical performance factors of LWC algorithms for IoT medical devices. Finally, the last main point is to evaluate the performance results of selected LWC algorithms using their experimental performance test results. The study determines the best candidate LWC algorithm for the healthcare system.

Table of Contents

List Of Figures

List of Tablets

List of Abbreviations

ACK	Acknowledgement
AES	Advanced Encryption Standard
BLE	Bluetooth Low Energy
CoAP	Constrained Application Protocol
CPU	Central Processing Unit
DDoS	Distributed Denial-of-Service
DoS	Denial-of-Service
DTLS	Datagram Transport Layer Security
HTTP	Hypertext Transfer Protocol
HTTPS	Secure Hyper Text Transport Protocol
ICT	Information and Communications Technology
IEEE	Institute of Electrical and Electronics Engineers
IoT	Internet of Things
IP	Internet Protocol
IPS	Intrusion Prevention System
6LoWPAN	Low-Power Wireless Personal Area Network
LoRaWAN	Long-Range Wide-Area Networks
LTE	Long-Term Evolution
LWC	Lightweight Cryptography
MFA	Multi Factor Authentication

MitM	Man in the middle
MQTT	Message Queuing Telemetry Transmission
NFC	Near-Field Communication
NIST	National Institute of Standards and Technology
OS	Operating Systems
RAM	Random Access Memory
REST	Representational State Transfer
ROM	Read Only Memory
RF	Radio Frequency
RFID	Radio Frequency Identification
WSNs	Wireless Sensor Networks
Wi-Fi	Wireless Fidelity

Chapter 1: Introduction

1.1 Background and Motivation

The Internet has become an essential part of a human's everyday life due to mobile devices' evolution and smartphone introduction. As data has become more widely available, a trend has grown for more objects accessible from anywhere around the world. Internet of Things (IoT) was first described in 1999 as uniquely recognised interconnecting networked objects employing Radio Frequency Identification (RFID) technology (Li et al., 2015).

Numerous communication technologies have been developed since then. IoT is the result of technological innovation and integration. It combines contemporary concepts such as Wireless Sensor Networks (WSNs) and Radio Frequency Identification (RFID) with cutting-edge technologies such as Big Data, Cloud Computing, and blockchain (Gill et al., 2019; Landaluce et al., 2020). Although technical improvements continue, the IoT definition has been developed to include them. Using these concepts, the IoT could be defined as everyday objects with recognising, sensing, networking, and processing abilities that allow them to interact with other equipment and services across the Internet to accomplish a meaningful goal (Whitmore et al., 2015).

Consumers are enthusiastic about the IoT, and the market is rapidly expanding. Over 18 billion IoTs, such as wireless sensors and interconnected objects, have been sold and interconnected via cloud servers by the end of 2020. 75 billion of IoT devices are anticipated to be operational by 2025, with a 300 percent increase in only five years (Abed et al., 2021).

New networking and communication technologies have been established as part of this expansion to provide integrated devices with more capabilities (Li et al., 2015). However, as a result of this growth, several new challenges have emerged, including scalability, information security, and organisational policies (Tim, 2016). These issues arise as a result of security and privacy concerns, as well as other considerations for power consumption and performance of IoT devices.

IoT devices routinely collect data from sensors, wearables, and smart-home appliances, increasing the risk of such devices becoming security threats (Rizvi et al., 2020). The majority of these sensitive devices endanger their users. Household smart appliances, such as refrigerators, microwaves, dishwashers, and webcams are vulnerable. Researchers discovered that 100,000 webcams could be potentially exploited (Palmer, 2017), in addition to children's smartwatches that can be monitored, tracked, and eavesdropped on conversations (Greenberg, 2020).

Security standards and protocols are still being developed and can be inconsistent. When designing and manufacturing secure IoT devices, manufacturing companies experience practical challenges such as the difficulty of implementing standard security measures due to resource constraints inherent in small, low-cost products (Lindqvist & Neumann, 2017). In the context of information security, the security issue at hand is data security, or data confidentiality. Data confidentiality ensures that authorised users have access to the data; no one else should have access to it (Gibson, 2014).

To address this problem, cryptographic methods are deployed to protect confidential data from viewing by unauthorised individuals; however, this comes at the expense of computationally expensive mathematical operations. These calculations are less challenging for equipment such as desktop computers, servers, and laptops. Because these devices have enough processing resources such as memory, processor speed, storage, and power. (Nishant et al., 2017). Furthermore, those devices can spend more resources on encryption processes while minimising the impact of other activities on the system.

Traditional cryptography in IoT devices faces challenges such as limited memory of Random Access Memory (RAM) and Read-Only Memory (ROM), low computational power, a limited physical area to construct design, and low-battery power (Thakor, 2021). For these reasons, classic cryptographic algorithms cannot be effectively used in the restricted environment of the IoT and thus are not acceptable options for presenting cryptographic solutions for IoT.

To solve the existing issues highlighted above, Lightweight Cryptography (LWC) is employed to provide countermeasures such as data integrity and data confidentiality in situations requiring efficient execution of cryptographic methods in resource-constrained devices, such as IoT devices. The National Institute of Standards and Technology (NIST) has standardised LWC algorithms for implementation in resources constrained areas where the functionality of the NIST cryptographic standards is insufficient (NIST, n.d.).

The main motivation of this study is to identify the best appropriate LWC algorithms for IoT devices in the medical environment in comparison to security and privacy needs and criteria established based on security requirements or standards. Lightweight Cryptographic (LWC) Algorithms of IoT medical devices are a significant problem since the landscape of these devices is developing quickly. As a result, it is necessary to utilise a specially designed LWC algorithm that offers the best security and performance for IoT devices like RFID and medical sensors.

Personal motivation for researching this area arises from conversations with friends frequently concentrate on the confounding growth of today's technology. My observations have led me to believe that many people are concerned about their information security in a completely integrated world. But, lack the comprehensive understanding to thoroughly verify whether the concerns are reasonable, what vulnerabilities of their IoT devices could be, and how they can avoid those. As a father of two children, I am motivated to learn more about this topic since I have an innate protective desire to keep my family safe from harm.

Each Internet-connected IoT device in healthcare represents a potential security vulnerability. Their vulnerability to cyber-criminal attempts can jeopardise patients' personal safety, expose patients' private information, and disrupt other critical healthcare services.

IoT security and privacy are essential because most people in our society utilise them to be safe from future threats posed by the continually changing online world. Therefore, among different areas, this thesis is motivated to analyse the characteristics of several LWC algorithms to get an insight into security and privacy situation of the IoT in the healthcare sector and determine if they have any limitations. Because of the structure of healthcare devices, it is necessary to utilize the right LWC algorithm for IoT in healthcare. The IoT devices utilised in medical industry have slow processing, memory, and bandwidth. It is necessary to choose LWC algorithm that considers all the algorithm's performance and physical functionalities. Due to the engagement of multiple performance characteristics relating to lightweight cryptography, the criteria for choosing the most suitable LWC algorithm for IoT in the medical sector has not been properly defined.

1.2 Research Objectives and Research Questions

The objectives of this thesis are to explore the potential IoT security and privacy issues in healthcare, to identify the most critical performance factors of LWC algorithms for IoT medical devices, and to run experimental performance tests of encryption and decryption procedures of selected LWC algorithms in terms of encryption/decryption execution time, energy usage, memory utilisation (RAM and ROM), and throughput for various payloads.

The following are the research questions that this thesis aims to determine:

Research Question 1 (RQ1): What are the main IoT security and privacy issues in healthcare?

Research Question 2 (RQ2): What are the most important performance factors of Lightweight Cryptographic (LWC) Algorithms for IoT in healthcare?

Research Question 3 (RQ3): Which Lightweight Cryptographic (LWC) Algorithm would produce the best performance results?

1.3 Research Approach and Findings

Answering mentioned RQs, two separate research methodologies were used and are outlined in Chapter 3.

Firstly, a Systematic Literature Review (SLR) was undertaken to gain a good comprehension of IoT security and privacy challenges in the healthcare sector. The SLR has two sections and the first section was designed to identify current challenges like the security and privacy problems of IoT in healthcare, and the results illustrated the leading security and privacy problems. Those issues are divided into three IoT layers, including the perception layer, network layer, and application layer. The second part of the SLR was developed to identify the important performance factors of the LWC algorithms for IoT devices in the healthcare industry.

Secondly, eight LWC algorithms were evaluated to recognise which algorithm had produced the best results in IoT medical environment. The experimental performance testing research methodology was employed to examine four performance factors of LWC algorithms in the IoT device, such as encryption/decryption execution time, energy consumption, memory usage (RAM and ROM), and throughput.

1.4 Thesis Structure

This thesis is presented in 6 chapters. The first chapter presented the thesis topic and gave the current situation on the thesis topic's origins and the existing study situation. The purpose and the importance of this study were discussed. The research methodologies utilised in this research were reported in the first chapter.

The background of IoT, IoT security, Cryptography and IoT, and Lightweight Cryptography are covered in Chapter 2, the literature review. This chapter describes the evolution of IoT, cutting-edge technologies have been created for the IoT, and the models of architectures presented. Existing information security goals like confidentiality, integrity, and availability are significant issues in IoT healthcare, but many additional problems make meeting these goals challenging. Healthcare security and privacy, as well as healthcare IoT security challenges are also described. The second chapter finishes by reviewing the literature on Lightweight Cryptography and IoT. The literature review revealed knowledge gaps, such as a limited number of studies of Lightweight Cryptography for IoT in healthcare.

The research questions that this thesis attempts to answer in the gaps in the current research are identified in Chapter 3. The research methodologies chosen for this study and the development process from prior research and related research methodologies are described in Chapter 3.

Research findings are explained and are covered in Chapter 4. The results of each of the research methodologies are also provided. Answering the research questions given by this thesis, Chapter 5 further analyses and reflect the research results from Chapter 4 and compares them to the literature review. This chapter also discusses the findings' consequences and ideas for strengthening IoT security and privacy in the healthcare sector.

Chapter 6 summarises the findings of this study and provides an overview of potential future study areas that could help expand the general understanding of the security and privacy of IoT medical devices.

Chapter 2: Literature Review

2.1 Introduction

The importance of understanding the impact of the widespread use of IoT on daily human life has been addressed (Rivas, 2017; Kliarsky, 2017). For instance, IoT devices in healthcare are frequently used by patients who might not be able to fully protect their security and privacy in the cyber environment, this should be addressed (Pradhan et al., 2021).

This chapter aims to summarise current knowledge on the security and privacy of IoT in the medical sector and recognise potential gaps in the body of literature that require further investigation. This chapter covers existing studies on the present condition of healthcare security and privacy, IoT security and privacy issues in the medical system, and current IoT lightweight cryptography. The significant issues in delivering a secure and confidential environment for IoT users in healthcare that lead to the development of the research questions for this study are covered.

Chapter 2 is divided into six subsections. Subsection 2.2 provides an overview of the IoT ecosystem concentrating on the existing studies that discusses the design of the IoT and defines the novel technologies in this field. Subsection 2.3 focuses specifically on research about IoT in healthcare and outlines the existing state of knowledge of these devices, security-related events faced by the IoT, and the recognised security and privacy issues in healthcare. The current studies of potential countermeasures to the problems experienced in this field are then addressed.

Subsection 2.4 provides a summary of cryptography and IoT, attempting to secure IoT devices in the healthcare environment. Subsection 2.5 considers the literature on LWC algorithms of IoT in healthcare, and subsection 2.6 summarises the literature review.

2.2 Overview of IoT

The Internet of Things (IoT) has no universally accepted definition due to its relative freshness and comprehensive nature. Kiran, D. (2019) chose the following definition “a global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies” (p. 495) to describe it (Kiran, 2019). As stated in Whitmore et al., (2015), everyday objects can be provided with identifying, sensing, networking, and processing capabilities that will allow them to communicate with other devices and services on the Internet to achieve some meaningful goal (Whitmore et al., 2015). The Cambridge Dictionary defines “objects with computing devices in them that are able to connect and exchange data using the Internet” (Internet of Things, 2022). On

the other hand, most definitions of IoT contain a similar idea: the concept of various systems, devices, and objects and the idea of communicating and linking with other nearby objects.

According to Stout & Urias (2016), the components that build the IoT could be grouped into four types. The first group includes switches, routers, personal computers, servers, and standard information technology equipment. The second category includes real-time monitoring systems, medical equipment, and other functional systems. Smartphones and tablets are included in the third category, and particular customer devices such as refrigerators and automobiles are included in the fourth. (Stout & Urias, 2016). Each category's devices may have sensors that monitor and capture various data from their surroundings and the ability to communicate with one another and to the Internet. (Alaba et al., 2017).

Different industries can benefit from IoT technology adoption in various ways, including increased performance, more extraordinary consumer experience, and faster growth. IoT devices can help organisations reduce vulnerability by offering novel approaches to working, like employing combination technologies such as Wireless Sensor Networks (WSNs) and Radio Frequency Identification (RFID) to track goods and equipment in large remote places. IoT is already being used in various areas, including transportation, healthcare, agriculture, and infrastructure. Companies that use IoT technology actively are expected to be 10% more profitable by 2025 than those that do not. (Tankard, 2015; FTC, 2015).

Technological improvements in wireless sensors and nanotechnology-based designs have driven IoT expansion. Numerous experts forecast a rapid increase in the IoT, including Abed's study, which predicts that the number of interconnected IoT devices would achieve 75 billion by 2025. (Abed et al., 2021). IoT's widely used applications drive more widespread connectivity and potentially compromise our daily lives to new threats. According to the Unit 42 research team, the expected growth will cause the IoT environment to carry the interactions of billions of devices. Over half of all IoT devices are sensitive to moderate and serious attacks (Unit 42 research team, 2020). Many traditionally essential devices including computational capabilities are used by consumers who may be unaware of these risks (Rivas, 2017). This leads to new threat vulnerability and the expected fast expansion highlights the need to recognise the IoT's underlying vulnerabilities and risks (Kliarsky, 2017).

2.2.1. IoT Architecture

Novel architecture concepts and hardware-software innovations have been established to manage IoT. However, there is currently no single IoT standard architecture that has been defined and approved. Numerous researchers and institutions have different concepts and models, such as the three-layered IoT architecture, displayed in Figure 2.1, which is the simplest and the most widely recognised (Alaba et al., 2017; Calihman, 2019; Sethi & Sarangi, 2017).

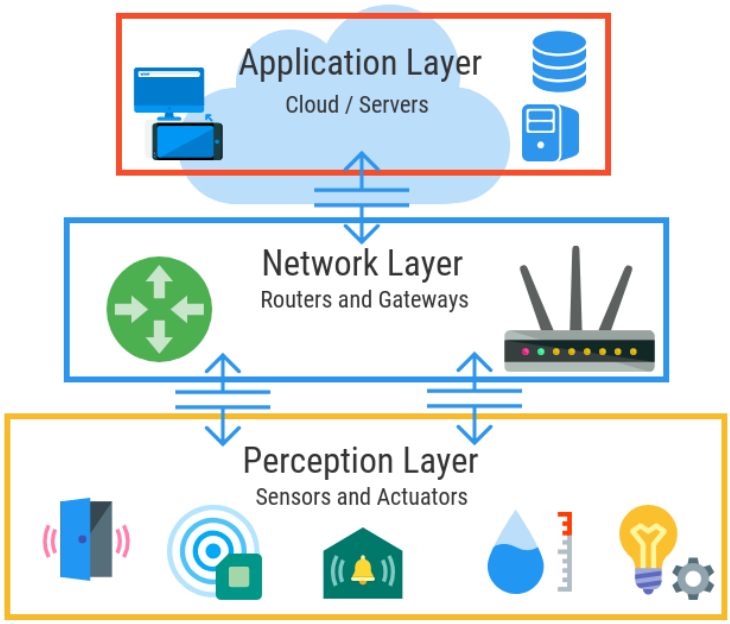


Figure 2.1 *Three-layered IoT architecture (Adapted from Calihman, 2019)*

The following is a description of the three-layered model:

The Perception Layer: This layer combines several IoT devices and is responsible for device communication and data gathering. Smart sensors, such as RFID tags and detectors, are used to collect data (Sethi & Sarangi, 2017). Real defence of any object and authentication and data integrity are security implications because IoT at this layer is sensitive to numerous attacks (Aarika et al., 2020). Sensor nodes, for example, are vulnerable to DoS, jamming, and Sybil attacks (Patil & Chen, 2017). DoS, repudiation, eavesdropping, counterfeiting, and spoofing attacks are all possible with RFID tags (Anca et al., 2019). Wireless technology is frequently used to communicate this layer to the network layer (Patil & Chen, 2017). Killer Bee, Packet manipulation, and key exchange issues concern ZigBee, while Bluetooth is vulnerable to DoS, bluejacking, and eavesdropping (Alaba et al., 2017).

Network Layer: Data is transmitted through the network layer, containing functionalities like device identification, packet switching, forwarding, and security protocols. The perception layer collects data, which the network layer functions and transmits to the application layer. It is the most critical layer of IoT architecture because it combines different communications methods that enable the interconnection of IoT devices. At this layer, security is comprised of a varied set of constantly developing requirements and innovations (Radovan et al., 2017). ZigBee, Bluetooth low energy (BLE), Low-Power Wireless Personal Area Network (6LoWPAN), and Long-Range Wide-Area Networks (LoRaWAN) are the most extensively used communication technologies (Tara & Raj, 2017). Network security risks, Denial-of-Service (DoS), Distributed Denial-of-Service (DDoS) attacks, and Man-in-the-middle (MITM) attacks are all examples of issues at this level.

Application Layer: The network layer obtains the data from the application layer, providing the appropriate offerings to IoT consumers (Sethi & Sarangi, 2017). It can be used for many applications, such as smart homes, smart retail, and smart grids. These activities can occur anywhere in the cloud or even on a mobile interface. The most common application layer protocols are Constrained Application Protocol (CoAP) and Message Queuing Telemetry Transmission (MQTT) (Almheiri & Maamar, 2021). Authentication challenges, access control, and information leakage are security issues at this level (Burhan et al., 2018).

2.2.2. IoT Technologies

IoT is supported by many technologies that interact across a broad selection of environments, many of which are geographically separated, highlighting the role of efficient, secure, and consistent communication. Wireless Fidelity (Wi-Fi), Long-Term Evolution (LTE), and cellular technology are all examples of communication technologies utilised in the IoT (Alem et al., 2021). These standard networks can be used by applications that demand high data rates over long distances; however, this only represents a small segment of the IoT infrastructure. IoT networks are not the same as conventional networks. IoT devices are generally built on Low-power and Lossy Networks (LLN) with limited processing power, energy, and memory (Radovan et al., 2017). As a result, new protocols and standards must be developed to be established to solve the significant problems in order to meet security and privacy requirements in the IoT ecosystem.

IoT devices typically interact via Radio Frequency (RF) signals or the Internet connection. They could access the network using the Internet Protocol (IP) or non-IP routes; however, each method faces its own set of issues. The standard IP stack is complicated and resource-intensive, making it unsuitable for most IoT devices. Near-Field Communication (NFC), Bluetooth, and RFID are non-

IP communication methods with a restricted range. Signal eavesdropping is challenging for all RF protocols (Alaba et al., 2017). Those issues have motivated scholars to improve, respond, and build new methods for secure connectivity. Figure 2.2 represents some of the available IoT technologies.

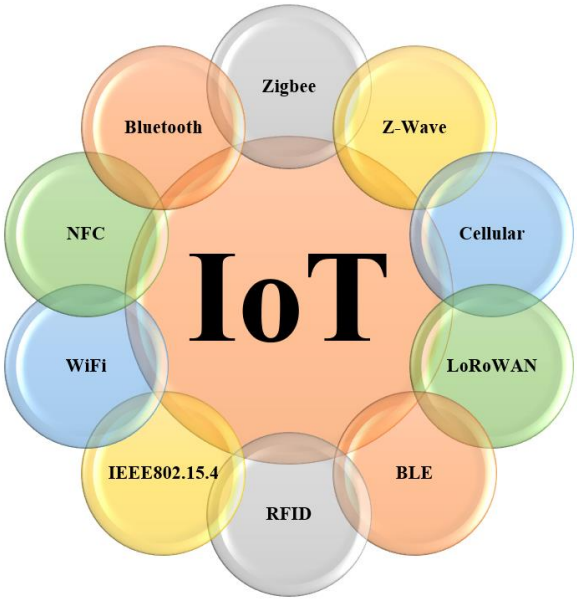


Figure 2.2 *IoT Enabling Technologies*

The following subsections discuss the most popular IoT technologies and the challenges they experience.

Radio Frequency Identification (RFID)

Radio Frequency Identification (RFID) utilises wireless communication to transfer identification data from a microchip to a receiver (Xu et al., 2014). Due to its ability to detect, track, and monitor objects, RFID technology is a key component of the IoT (Jia et al., 2012). It enables radio signals to send data across a short distance (Gubbi, 2013). RFID tags or transceivers, along with sensors or transceivers, enable data to be stored and accessed remotely.

Tags connected to IoT devices store data that a reader collects through a 2-way signal, allowing individual objects to be monitored. This technology has advantages that include a tiny design, inexpensive price, and reliability when utilised as a non-contact procedure to detect and track items in the IoT environment; it is suitable for short-range utilization because it facilitates data transmission via radio signals (Lin et al., 2017). The RFID system comprises radio signal tags that store the object's remarkable identity and the tag reader that uses radio waves to recognise the device (Ajami & Rajabzadeh, 2013; Vaniotis, 2018). As

shown in Figure 2.3, the tag reader sends the object's identification number to a computer, tracking and monitoring it.

Figure 2.3 *Radio Frequency Identification (RFID) system (Adapted from Vaniotis, 2018)*

This technology is gaining traction in various areas, including trade, logistics, and other tracking-related industries (Li et al., 2015). Organizations can use RFID to monitor and track products automatically, minimizing the need for direct intervention. Tracking data could be provided for scanning. RFID scanners could be recognised as the first IoT devices based on network connectivity functionalities in those applications (Xu et al., 2014). In the healthcare industry, for instance, RFID significantly reduces the probability of providing incorrect prescriptions, enables the clinical trial process much easier, increases the accuracy of patient identification, improves patient tracking, and eases inventory management (Pal et al., 2021).

Wireless sensor networks (WSNs)

Wireless sensor networks (WSNs) are collections of separate nodes which interact wirelessly across a constrained capacity and have been utilised in several areas, such as traffic monitoring, armed services tracking, and healthcare (Xu et al., 2014; Yick et al., 2008). While WSNs are an essential part of the IoT environment, several issues regarding securing them are acknowledged (Kocakulak & Butun, 2017). Because of significant resource limits, such as low processing capabilities and limited memory, they cannot deal with typical cryptographic procedures and are vulnerable to standard wireless security threats. Sharma et al. (2012) outlined and evaluated known symmetric, asymmetric, and hybrid architectures and an overview of suggested cryptographic algorithms for usage in WSNs. No single way is indicated as the best and finding the proper method for each network is challenging.

The WSNs sensors are employed in the healthcare sector to monitor, track, and record patient data, including blood pressure, heart rate, temperature, and other vital indicators (Kocakulak & Butun, 2017). It enables medical workers and caregivers to track and record patient health data

continuously. While RFID and WSNs are the key technologies that drive IoT, numerous additional innovations have been created as components. These newest contributions to the IoT include software and hardware improvements.

Near Field Communication (NFC)

One of the novel technologies brought to the IoT field is Near Field Communication (NFC), enabling devices to interact when they are paired (Whitmore et al., 2015). NFC is a short-range wireless telecommunication technique depending on RFID that enables data to be exchanged among two NFC-enabled objects over a small range. It provides two-way interaction and could protect transfers such as payments. It is commonly found in smartphones (Kevin et al., 2012; Sethi & Sarangi, 2017). This technology intends to establish a singular functionality for processing the data from several equipment, allowing developers to quickly launch new services without worrying about data transformation (Whitmore et al., 2015). Because data transfer requires proximity, it has a restricted application (Sethi & Sarangi, 2017).

Constrained Application Protocol (CoAP)

Constrained Application Protocol (CoAP) is an application layer protocol for resource-limited devices like IoT (Al-Fuqaha et al., 2015). CoAP changes various Hypertext Transfer Protocol (HTTP) protocols to allow IoT device communication, while Datagram Transport Layer Security (DTLS) provides security. As a result, the protected deployment is contingent on DTLS flaws being resolved. (Sethi & Sarangi, 2017). CoAP is built on the Representational State Transfer (REST) architecture, as illustrated in Figure 2.4.

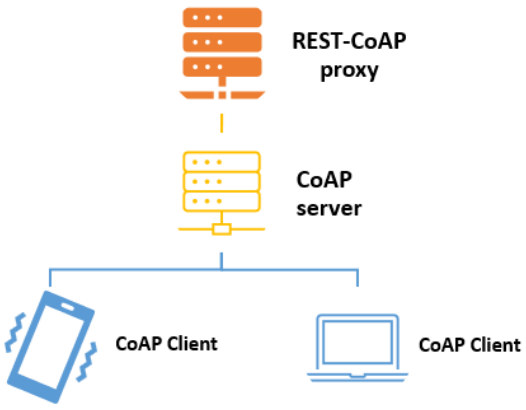


Figure 2.4 *The Constrained Application Protocol architecture (Adapted from Al-Fuqaha et al., 2015)*

CoAP was created with IoT devices in mind, including HTTP functionality. Because IoT devices have limited resources, the HTTP protocol, due to its complexity, is not ideal for power-limited devices (Shelby et al., 2014). The server could maintain several devices not enabled with HTTP. It has capabilities like push notification, where the server transfers notifications to the objects. The four messages available are acknowledgement, confirmable, non-confirmable, and reset.

IEEE 802.15.4

IEEE 802.15.4 is a technical standard and Medium Access Control (MAC) layer protocol for Wireless Personal Area Networks (WPANs). This protocol enables connecting devices in the personal area while consuming low energy and provides protection solutions such as authenticity, data confidentiality, and replay defense (Al-Fuqaha et al., 2015). It was developed by the Institute of Electrical and Electronics Engineers (IEEE). NULL security, Unencrypted Acknowledgement (ACK) frames, and no timed frame monitors are challenges to this protocol. (Alaba et al., 2017).

ZigBee and Z-Wave

ZigBee is a wireless connection technology rooted in the IEEE 802.15.4 requirement and is designed for short-range communications (ZSO, 2006). It is reliable, secure, and flexible and operates at 2.4GHz with low data rates of 250Kbps over a 100-meter distance (Taleb et al., 2021). End-devices in a star topology are straightforwardly linked to the coordinator, whereas intermediate routers extend the network in tree or mesh networks.

Smart houses, monitoring devices, and smart healthcare are possible usage areas. The network layer uses cluster-tree and customized on-demand range linear schemes to distribute data (Li et al., 2010). Its compatibility is limited because a ZigBee device can only connect to other ZigBee devices.

Z-Wave is comparable to ZigBee because it provides low-cost, low-energy, and reliable short-term connectivity. While it has a more straightforward design to install than ZigBee, the various nodes that is in the system is severely constrained. (Lin et al., 2017).

Low-Power Wireless Personal Area Network (6LoWPAN)

6LoWPAN is merged with the Internet protocol (IPv6) and Low-Power Wireless Personal Area Network (LoWPAN) (Montenegro et al., 2007). It was created by the Internet Engineering Task Force (IETF) (Montenegro et al., 2007), and utilise various frequencies across multiple platforms while providing a unique IP address to practically every connected

device. It allows IoT devices with restricted resources to send data over IPv6 wireless channels and promotes mobility. Smart homes, healthcare, smart agriculture, and industrial IoT are the most common 6LoWPAN use cases (Radovan et al., 2017). For instance, in the healthcare industry, 6LoWPAN enables the connection of limited wireless wearable sensors to the IP world to measure the patient's physiological data and regularly update physicians and specialists on the patient's situation (Touati et al., 2016). Unlike ZigBee, a 6LoWPAN device could communicate with another 6LoWPAN device or an IEEE 802.15.4 device. It can also connect to an IP-based network, such as Wi-Fi, as shown in Figure 2.5.

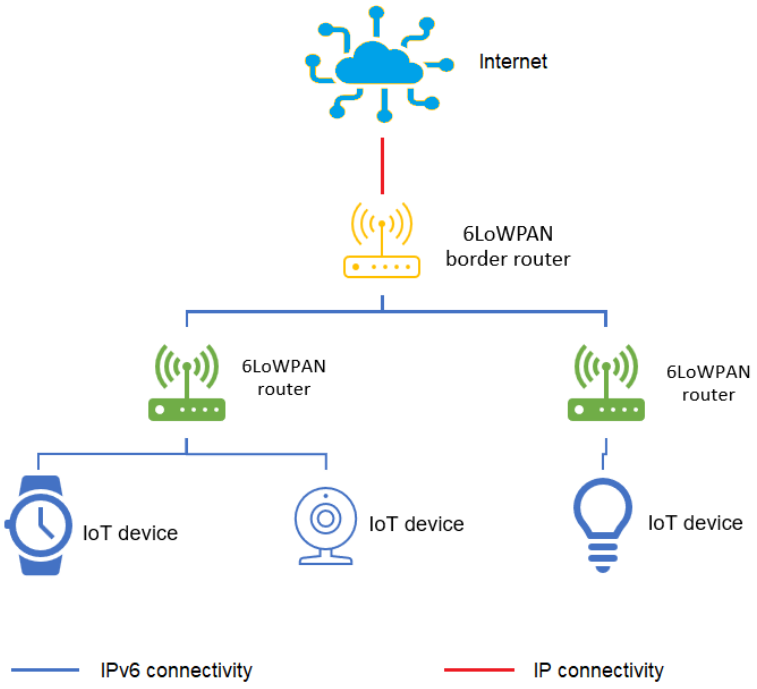


Figure 2.5 *6LoWPAN architecture (Adapted from Radovan et al., 2017)*

LoRaWAN

LoRaWAN is a Long-Range Communication Technology designed for low-power IoT applications (LoRa Alliance, 2017). LoRaWAN network comprises routes and a separate server in star-of-star architecture (Yasmine et al., 2021), as illustrated in Figure 2.6.

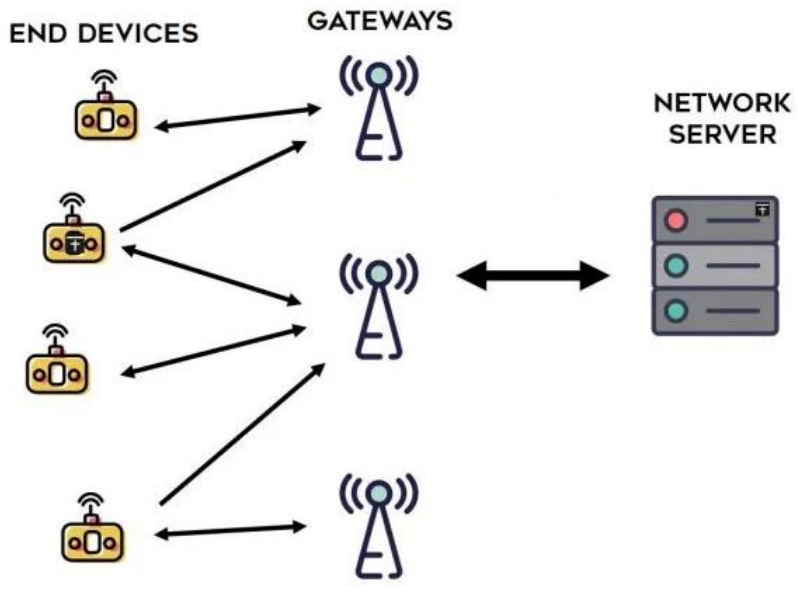


Figure 2.6 *LoRaWAN architecture (star-of-star topology) (Adapted from Yasmine et al., 2021)*

Through one-hop connectivity, devices can interact with one or more gateways. This Internet protocol is utilised to communicate the ports to the network server.

Datagram Transport Layer Security (DTLS)

Many security standards suggest the Transport Layer Security (TLS) protocol for providing network communications security; but it is impractical for resource-limited fields, such as the IoT. DTLS has been presented as a solution for these conditions and is currently widely used in the IoT environment. (Nguyen et al., 2015). Problems occur when implementing DTLS in the IoT environment since DTLS involves the key-agreement procedure, typically accomplished using the public key infrastructure. However, most IoT objects lack the necessary resources to handle this key authentication approach, leaving only non-scalable alternatives. (Raza et al., 2016).

Bluetooth Low Energy (BLE)

Bluetooth Low Energy (BLE) is a low-energy, short-range data transmission system that requires fewer resources than standard Bluetooth (SIG Bluetooth 2015). It uses a range of 50–150 metres at 1 Mbps of RF communication to save energy while operating at 2.4GHz (Sultania et al., 2020). BLE technology employs adaptive frequency hopping, allowing it to communicate consistently in RF systems like those found in homes and factories (Townsend et al., 2014). IoT devices have limited resources that integrate security procedures like intrusion detection and employing RF

communication methods like BLE could bring different issues. Because these procedures sometimes require specific technologies still in development.

A comparison of these protocols is presented in Table 2.1.

Table 2.1 *Comparison of IoT Wireless Technologies*

Wireless Technology	ZigBee	BLE	6LoWPAN	LoRaWAN
Topology	star, tree, mesh	Star	Star, mesh	star, star-of-star
Range	10-20m	<100m	10-20m	3-5km
Application	smart home, smart meters, smart healthcare	Smart vehicle	smart home, smart agriculture, smart industry	Smart city
Interoperability	No	No	Yes	Yes
Security	Yes	Yes	No	Yes
Scalability	Yes	No	Yes	Yes

2.3 IoT in Healthcare

2.3.1 Healthcare Security and Privacy

Security and privacy are two essential characteristics of any system, and their role in healthcare cannot be underestimated (Arora et al., 2014). Medical data, including patient healthcare data, is classified as sensitive and generally confidential since it may include personal information such as medical history, health issues, and emergency contacts (Virtual Mentor, 2012). Because it comes to physiological wellness, sickness, and drug addiction, this information becomes even more sensitive when it includes private health data that patients usually refuse to discuss with anyone except their physicians. Furthermore, patients' health records collect huge volumes over the period, including medical history, nutritional and genetic information, and even relatives' health backgrounds (Bouayad et al., 2017).

Security and privacy problems could prevent the widespread utilisation of Information and Communications Technology (ICT) in the healthcare environment. Compared to the previous two decades, healthcare data and information are now vulnerable to a broader range of security and privacy threats. The major problem is that vulnerabilities and technologies in healthcare are not adequately integrated. The challenge of security and privacy is increased by adopting innovative technologies in the healthcare system, such as mobile devices, cloud services, and remote applications (Nureni & Charles, 2019).

Furthermore, increased technology usage also raises the risk of public health data, making citizens' healthcare information vulnerable to different types of threats and exploitation, which might have

severe consequences for both patients and medical organisations (Argav et al., 2020). The absence of security and privacy considerations in healthcare ICT technologies also restricts the healthcare system's ability to reach its full potential and utilise technologies to address some of the issues (McGraw & Mandl, 2021; Argav et al., 2020). In this regard, the concepts of security and privacy should be well defined, and their objectives in healthcare should be clearly explained. Although these two concepts in healthcare can be defined differently based on people's views, the following definitions were used in this study.

Security is described as "a condition that outcomes from the formation and preservation of prevention strategies that allow an organisation to accomplish its purpose or essential operations despite risks to its use of information systems" (Paulsen & Byers, 2019). Privacy means "controlling user access or reliant party information following national regulations and organisation policy" (Paulsen & Byers, 2019).

Statistics show that breaches in healthcare records create financial concerns, psychological harm, medical identification fraud, and potential social stigma or prejudice against people with a specific condition (Seh et al, 2020). Victims' health credentials are hijacked in some situations for medical treatment, which causes financial losses for healthcare institutions and could also have health effects for the individuals owing to the alteration of their medical files (Seh et al, 2020). Even inadvertently leaking healthcare data can affect patients' privacy (McGraw & Mandl, 2021; Abouelmehdi et al., 2018) and expose them to additional issues, like those described above.

As a result of those mentioned above and the fact that health data breach is the second most reported breach (Hasan, 2020), two-thirds of The United States (US) adults are concerned about the security of their healthcare information. At the same time, 75% of US patient populations are concerned about health websites where their data being shared. Furthermore, security breaches such as healthcare theft or loss are estimated to cost the US healthcare business USD 7 billion yearly (Hasan, 2020). Figure 2.7 the number of healthcare data breaches in the US from 2009 to 2020.

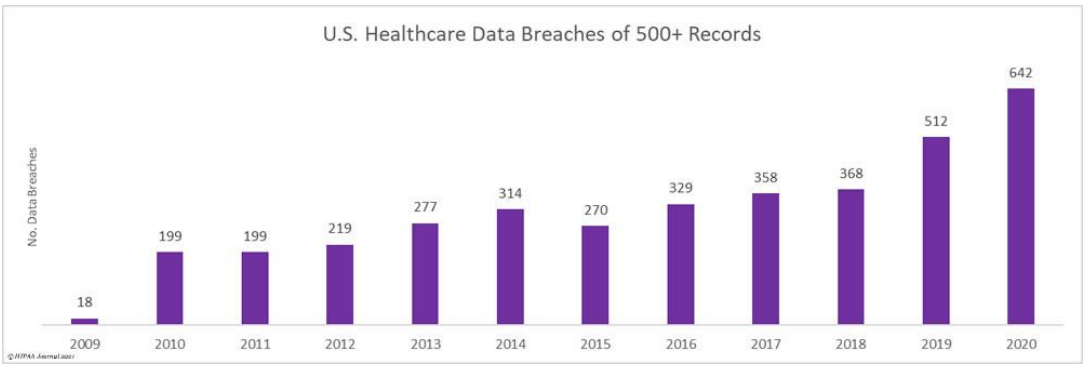


Figure 2.7 *Healthcare Data Breaches, 2009-2020 (Adapted from* Hasan, 2020*)*

Different organisations have established and developed principles, legislation, policies, guidelines, and protocols to improve security for technology service providers in the health sector. The regulations' long-term goals are to protect systems from any purposeful or accidental threat (Argav et al., 2020). This is to take advantage of various technologies to provide people with efficient and cost-effective medical services while also reacting to growing concerns about clinical information security and privacy and minimizing the strong growth of cyber-attacks in healthcare.

The US's Health Insurance Portability and Accountability Act (HIPAA), State Alliance for eHealth, and National Governors Association Centre for Best Practices are just a few organisations that provide internationally accepted principles and regulations for using technology in healthcare. The deployment and utilisation of technological advancements in healthcare exceed the guidelines and standards set even by the abovementioned organisations. As a result, new technologies and methods are becoming progressively sensitive to security and privacy threats, despite improving the healthcare system significantly (Elhoseny et al., 2021).

2.3.2 IoT Security and Privacy Challenges in Healthcare

Although utilising IoT devices for healthcare purposes can bring enormous advantages for medical specialists and the healthcare business, it is essential to highlight that security impedes IoT implementation (Maple, 2017). When everything becomes interconnected, additional security and privacy challenges appear, including the confidentiality, authenticity, and data integrity generated and received by objects (Hurrah et al., 2019). Furthermore, most of these problems are the consequence of traditional computer systems that have been changed for usage in portable devices.

The most technologies or networks are vulnerable to security and privacy concerns, especially in healthcare, because personal and private information is involved (Hurrah et al., 2019). The data security transferred from a patient's device to wireless media, which compromises unencrypted patient data, is a significant issue (Verry et al., 2020). Because a large percentage of devices and their activities are wireless, users may not gain value from the advantages of IoT in the medical sector because of the breaches of privacy concerns stated (Kelly et al., 2020). The variety of capabilities and network heterogeneity has worsened IoT devices' challenges (Imran et al., 2020). IoT is made up of heterogeneous networks such as sensor nodes, wireless communication networks, and the Internet; the same security and privacy vulnerabilities that affect each network significantly impact IoT devices (Panagiotis et al., 2019).

Due to the rising confidence and widespread acceptance of IoT technology in healthcare, the quality of services supplied by healthcare organisations will significantly improve, resulting in better public health (Kelly et al., 2020). However, users are unwilling to support IoT-based medical services due to the security and privacy mentioned above. However, technology adoption is expected to improve if the challenges are identified and resolved by reducing the psychological and social conflict associated with IoT adoption.

There are multiple types of IoT security and privacy issues that can be physical, information and management, or system and information. These risks can come in the form of either passive or active threats. Attackers can acquire data without affecting network behaviour in passive threats; however, in active threats, intruders can block or slow down service administration (Thomas, 2020). As shown in Figure 2.8, a categorisation of IoT security and privacy threats is divided by layers, purposes, and responses. This section concentrates on the three layers of IoT security and privacy vulnerabilities in healthcare.

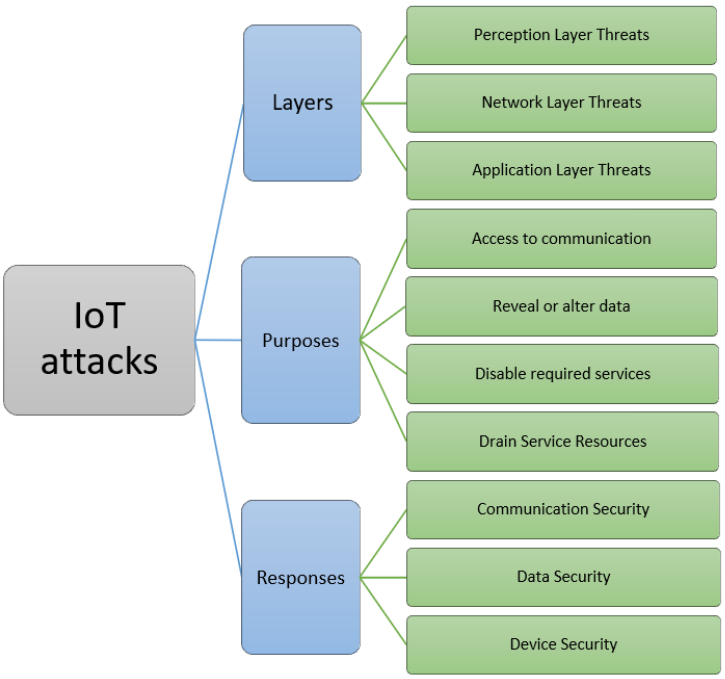


Figure 2.8 *IoT attacks based on layers, purposes, and responses*

Perception Layer

The perception layer is a sensing layer that connects perception hardware and data collection (Aarika et al., 2020). This layer's object/human recognition and sense experiences are used for the IoT system. IoT is an arrangement of several networks. It has convergence problems, which affect various security threats frequently (Burhan et al., 2018). This layer's security concerns include physical devices and data collection. Therefore, hardware limitations compromise the main security and privacy issues of this layer (Yao et al., 2021). Most IoT sensors have little external security or protection, so such advanced security and public encryption methods or frequency hopping interaction cannot be addressed. Some systems also accept short passwords, compromising device confidence management (Mahanty et al., 2018). The weaknesses of IoT devices, such as memory, computational, and energy limitations make them vulnerable to physical interference and jamming activities (Li et al., 2020).

Additionally, other limitations, such as the variety of IoT devices, make incorporating a single and unified security design burdensome (Domb, 2019). Also, variations in IoT devices can result in data aggregation, posing a danger to data integration. This issue is counted as one of the most severe threats to public health (Kelly et al., 2020).

On the other hand, IoTs are likely to be the most important for protection in healthcare applications, as one of the most common attacks at this layer to reduce physical/device manipulation is IoT device exploitation (Elhoseny et al., 2021). Many devices are vulnerable to severe attacks because they are deployed without additional security or interaction in the patient's environment. Through this attack, attackers will search the collection devices to exploit and steal patient data. For the IoT healthcare systems to remain safe, node authentication is the first crucial step in recognising malicious nodes due to physical threats (Pradhan et al, 2021). Because many types of healthcare equipment have been created and developed to record, retain, and protect individual health records, physical or device exploitation in healthcare can be significant (Devibala, 2019).

Because of the IoT devices' resources (battery power, memory, and Central Processing Unit (CPU)) limitations, Lightweight Cryptographic (LWC) algorithms are appropriate in IoT (Thakor et al., 2021).

Network Layer

Providing sufficient security and privacy in this layer while maintaining the flexibility and expandability of the IoT network is a difficult task (Ren et al., 2017). Multiple IoT devices frequently use different sources and, as a result, use other network protocols for data transmission (Alsubaei et al., 2017). Therefore, determining or including a single security protocol that matches all network types (wired and wireless) is complex, and even the traditional security model has vulnerabilities.

The security considerations for multiple protocols, including 4G access networks, Ad hoc, and Wi-Fi networks, among many other network systems, should be defined and handled in all media (Chacko & Hayajneh, 2018). This is essential to note that the security and privacy problems discovered in this layer may be the same as those in traditional network security challenges. This layer is vulnerable to Trojan horses, malware, and spam, resulting in data leakage. Data is transmitted wirelessly due to the extensive usage of multiple wireless networks in IoT, making wireless communication vulnerable to data eavesdropping. Several network risks exist at this layer, including packet spoofing, route falsification, and flooding attacks (Shrivastava & Namdev, 2020).

Attackers can manipulate medical data and disable their alarms connected with healthcare systems or even interfere with the WSN, so sensors can send false information, which means physicians will make inadequate decisions. Hackers may also submit spam and launch Denial of Service

(DoS) attacks or hijack network source points. DoS in IoT can be disastrous, as malicious IoT nodes can enable secure resources to make valid IoT nodes in the network inaccessible. However, if malicious IoT nodes interrupt the configuration data, a harmful DoS attack causes network topology to be insecure (Nausheen & Begum, 2018).

The use of a combination of security and privacy protocols and mechanisms is an efficient and systematic approach for protecting the network against security threats due to the heterogeneity of the entire network. This enables the network to be encrypted and manipulated by attackers to ensure authenticity, confidentiality, integrity, and availability.

According to Anil & Thaier (2018), DoS attacks can be a crucial problem for multi-domain infrastructure and, therefore, for IoT medical applications. DOS attacks can jeopardise IoT servers and lead to the retrieval or destruction of many saved security contexts in a restricted domain. This attack could destroy the health system and patients because it could damage critical health services and put patients' lives at risk. Several researchers have suggested solutions to this problem, such as IoT decentralised architecture and firewalls to filter DoS attacks. However, it is challenging to detect and prevent all DoS attacks by detecting any potential DoS attacks, but not enough research is underway in this direction. More searching for this form of attack is therefore required. Besides attack detection, good authentication and filtering mechanisms are also essential to guarantee the protection of IoT data.

Application Layer

The high number of IoT applications and their complexity could be viewed as the main reason for the security issues of IoT caused by system integration. Therefore, the system providing an interface between users and IoT devices can relate to several security challenges in this layer. IoT device limitations and difficulties deploying potential issue solutions are two common underlying reasons for security problems in the application layer (Nausheen & Begum, 2018).

The first is generated by weak network protocols of the IoT operating system, which involves a limited safety module that cannot provide complete application layer protection (Abdullah et al., 2019). Dynamic security patch installation for IoT devices, because of the difficulties in manually upgrading programs on many remote appliances, is challenging, if not impossible. In addition, the potential for installing updates is restricted (Devibala, 2019).

Due to the high diversity in IoT applications that use various interfaces and data sharing models, numerous security problems remain issues (Zeadally et al., 2020). Certain aspects such as data protection, authentication, and data breaches.

More importantly, it is recommended to explicitly identify and use the medical data access policy to confirm the user's credentials with the authorization to enter this IoT layer of healthcare services, verification, and access monitoring (Mahanty et al., 2018). In addition, healthcare works with sensitive patient information, and specific data protection measures should be developed for its datasets. An additional layer of safety with encryption algorithms is also suggested for patient data protection.

Table 2.2 presents different security issues in the IoT healthcare environment.

2.4 Overview of IoT and Cryptography

The IoT devices could fulfill Confidentiality, Integrity, and Availability (CIA)'s security requirements. Encryption and decryption are used to accomplish this. Cryptography is the strategy used to ensure confidentiality and integrity. It changes data to an unreadable format via cryptography, and individuals who have a secret key could access it (Kumar et al., 2016).

The procedure of converting an understandable message to an unreadable form is called encryption (Gurpreet & Supriya, 2013). The understandable text is recognised as plaintext, while the unreadable version is called ciphertext. Transforming ciphertext is termed plaintext as decryption (Gurpreet & Supriya, 2013). To generate the ciphertext, the cryptographic algorithms used for encryption apply substitutions and transformations on the plaintext and a comparable operation to generate the ciphertext to the plaintext (Gurpreet & Supriya, 2013). A key is used to decipher ciphertext (Kumar et al., 2016). Cryptographic algorithms could be classified as symmetric or asymmetric, depending on a set of the keys.

Only one key is utilized in the encryption and decryption of the symmetric cryptographic algorithm (Kumar et al., 2016). It employs two keys in asymmetric encryption: the public key and the private key. The public key is for message encryption and is distributed to anybody (Peterson & Davie, 2012). The key's owner holds the private key, the only key capable of decryption (Peterson & Davie, 2012). Asymmetric cryptographic algorithms are substantially slower than symmetric cryptographic algorithms, which could be a challenge for processing huge volumes of data (Patil et al., 2016). Asymmetric cryptographic algorithms are utilised session keys because of the performance difference; symmetric encryption techniques are then used for encryption and decryption (Peterson & Davie, 2012).

Table 2.2 *IoT Security Issues in the Healthcare Environment*

Attack	Description	Purposes	References
Replay attack	Eavesdrop the communication and retransmit the packets to the target node	Achieve the trust and confidence of the IoT structure and launch additional attacks	(Zhao & Ge, 2013; Rughoobur & Nagowah, 2017)
Node tampering	Physically replace the sensing node or a component of hardware parts	The accessibility of infrastructure is affected by connectivity to vulnerable data	(Zhao & Ge, 2013: Wei et al., 2021)
Node injection	Implement malicious nodes in the IoT system	Monitoring traffic, gaining access to personal information, and launching extra threats	(Anwar et al., 2015)
Node capture attack	Capture node from the network	Obtain sensitive information	(Bharathi et al., 2012)
Black hole attack	Send route replay messages to the source node to receive packets from the sender node	Access to private data and join the network	(Ali et al., 2018)
Sinkhole attack	Claim unrestricted capabilities to be chosen for WSN traffic transmission	Breaching the privacy of the data and activating extra threats	(Soni et al., 2013)
Wormhole attack	Create a false one-hoptransmission to deliver more data through the tunnel	Breach security and privacy and launch multiple extra attacks	(Lee et al., 2014)
Sybil attack	Pretend the identities ofmany nodes to be more than one location	Degrade data securityand resource utilization	(Zhang et al., 2014)
RFID Sniffing	Utilising numerous sniffing applications, break out or eavesdrop on the data stream in the RFID system	Sensitive information disclosure	(Khoo et al., 2011)
RFID Spoofing	To hide the attacker's identity, spoof or replicate legitimate RFID details and transmit data with the correct ID tag	Collect sensitive information and gain direct connections to the framework	(Andrea et al., 2015)
RFID Cloning	Duplicate data from an original RFID tag to generate a clone	Enter directly into the framework	(Andrea et al., 2015)
Man in the middle (MitM)	Intercept and possibly alter the communication betweentwo nodes	Get private information and launch additional attacks	(Alsubaei et al., 2017)
Eavesdropping attack	It is a subset of MTM where an attacker intercepts secretly the communications	Get private information	(Abomhara & Køien, 2014; Alraja et al., 2021)
Brute force attack	Attempt so many keys to obtain the appropriate key	Decrypt encrypted data	(Alsaadi & Tubaishat 2015)
Encryption attack	To discover the encryption key on IoT devices, employ methods such as timing, energy, malfunction, and other analysis	Break encrypted system to get private data	(Andrea et al., 2015)
Code injection	Insert malicious code thatwill execute the IoT	Monitor the entire system while negatively impacting data security and privacy	(Andrea et al., 2015)
Denial of Service(DoS)	Send a large number of data packets to the IoT ecosystem	Deplete the resources of the service supplier, disconnect the network, and negatively affect data transmission	(Alsaadi & Tubaishat 2015)
Node jamming	In a type of DoS attack, the attacker could interrupt or prevent signal transmission	Maliciously disrupt the infrastructure and deactivate it	(Zhao & Ge, 2013)
Phishing attack	IoT users may be fooled. Typically, this is accomplished by posing as a trustful organisation	Obtain confidential data	(Sameena, 2021)
Social engineering	Manipulate the users of the IoT, based on human interaction	Access to confidential information	(Andrea et al., 2015)
Malicious software	Infect or deactivate the IoT system using malicious tools like worms, viruses, and trojan horse	Damage interconnected IoT devices to get data	(Andrea et al., 2015)

Key management and key authentication are the main issues with using asymmetric encryption because the key is publicly revealed. As a result, anyone could transmit a message, but its source could not be verified. It also requires a public key infrastructure and certificate authority if it uses authentication. This increases complexity significantly and requires pre-configuring certificates on devices.

IoT devices can use these cryptographic algorithms in each layer depending on the techniques and protocols applied. Because the perception layer communicates the device and its sensors, they should be secured (Luhach & Kumar, 2016). This protects the data from unauthorised access and modification; encryption ensures the data's confidentiality and integrity at rest. Most existing operating systems include storage and file encryption; nevertheless, this has a performance cost (Shi et al., 2020) and depends on the utilised technology and its cryptography support for device sensors.

On the other hand, interactions among IoT devices still need to be encrypted to secure data during transmission (Suo et al., 2012). The Advanced Encryption Standard (AES) symmetric algorithm could be used to enable the data encryption process. The goal of the IoT network layer is to secure interaction pathways among the IoT device and the local or remote systems. The other layers are unnecessary to build their encryption because the data is protected at this layer; therefore, network devices may read data based on how effective interaction is protected (Suo et al., 2012). The IP Security (IPSec) protocol package can be utilised with various IoT devices which implement the standard IP versions. IPSec Encapsulating Security Payload (ESP) protocol provides confidentiality via encryption (Peterson & Davie, 2012). However, IPSec also provides alternative encryption methods that are less widely implemented.

Finally, the objective of the application layer is to secure data transferred between an IoT application or service, as well as conversely. This enables the application or the service to deliver complete encryption independently (Suo et al., 2012). The application can utilise cryptographic security or third-party protocols or frameworks to achieve this. The Transport Layer Protocol (TLS) is an example of the current third-party protocol. Other applications or services use this protocol to offer Secure Hyper Text Transport Protocol (HTTPS) (Peterson & Davie, 2012). TLS employs two protocols to provide security: the record and handshake protocols (Claeys et al., 2021). The source and destination utilize the handshake protocol to choose encryption settings, like the symmetric cryptographic algorithm and the keys. After the handshake is completed, the recorded protocol is employed to encrypt and send data, and it is received to decrypt the data at the endpoint (Claeys et al., 2021).

2.4.1 Advanced Encryption Standard (AES)

AES encryption offers confidentiality in various protocols. In 2001, NIST designated the standard symmetric method to replace the Data Encryption Standard (DES) (Gurpreet & Supriya, 2013). NIST describes the AES algorithm as a classified symmetric encryption algorithm that works with a particular size of data blocks (Fips, 2001). The block size for AES is 128 bits, and it can use keys of 128 bits, 192 bits, and 256 bits (Fips, 2001), because key recovery is the most practical attack on AES, a more powerful key increases its strength. The AES algorithm includes encryption and decryption, as shown in Figure 2.10 and Table 2.3 illustrating how many AES procedures on plaintext or ciphertext to find a key must be done.

Table 2.3 *AES Strength (Adapted from Daemen & Rijmen, 2003)*

AES version	Strength	Key Rounds
AES-128	2^{127}	10
AES-192	2^{191}	12
AES-256	2^{255}	14

Decryption is the reversal of encryption, with the opposite functions used during encryption, as illustrated in Figure 2.9. The encryption and decryption processes of AES complete 4 essential operations for each session, not including the final, and only accomplish three. SubBytes, ShiftRows, MixColumns, and AddRoundKey are the four functions used during the rounds; all but AddRoundKey have an inverse function utilised during decryption. The round is calculated by the key size, as illustrated in Table 2.4. Even before starting, the key and message are added together, and the key is extended, resulting in the 128-bit key for each round. The 128-bit text could be stored in a 4x4 byte array, which is termed the state, and on which all the operations are conducted (Gurpreet & Supriya, 2013).

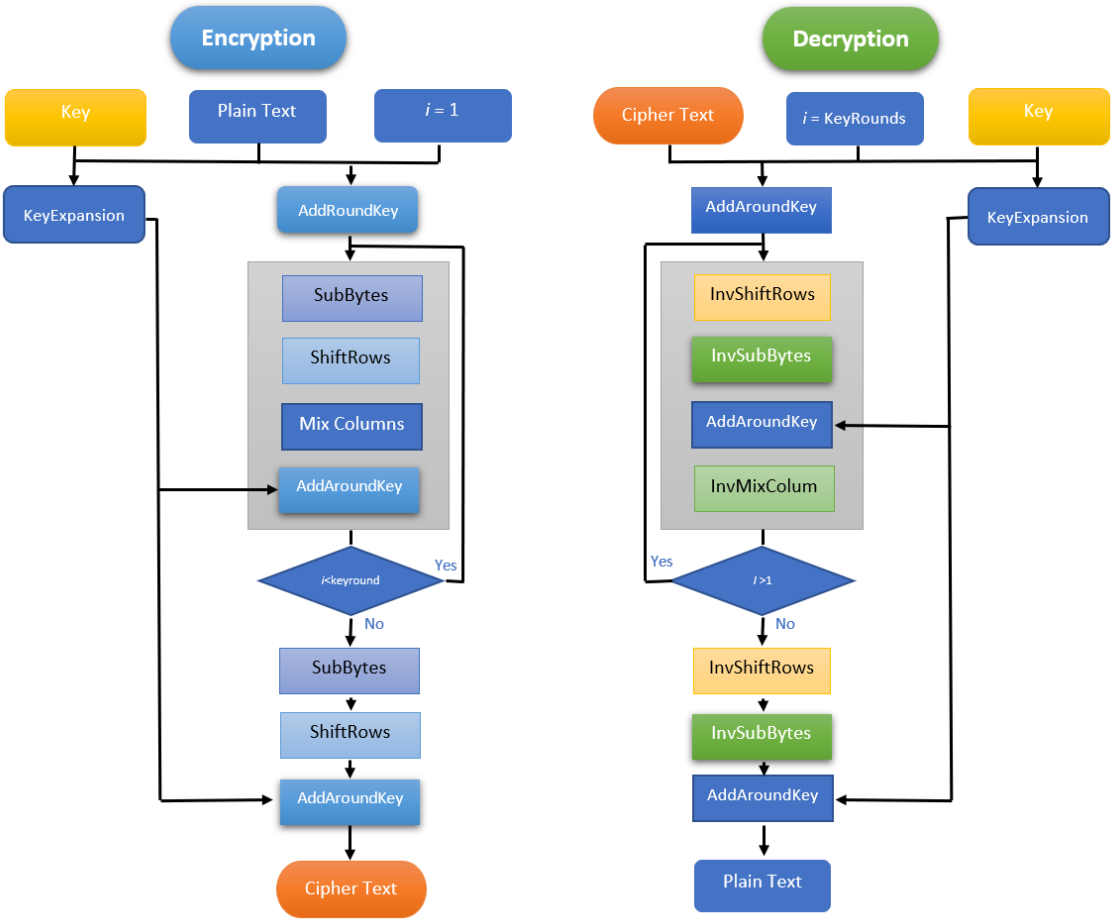


Figure 2.9 *AES encryption and decryption procedures (Adapted from Gurpreet & Supriya, 2013)*

Following is the encryption process description of the functionality provided by AES. The inverse functions are decrypted in a different sequence than their encryption counterparts, although they perform the same operation; this order is shown in Figure 2.9. The SubBytes process uses the Rijndael substitution box (Sbox) to conduct a conversion on every byte (Gurpreet & Supriya, 2013). Sboxes utilised during this function are shown in Figure 2.9 (inverse) (Fips, 2001). ShiftRows operation is next, which conducts the circular change to the last three. It shifted twice from the second row to the third row and three times in the fourth row (Fips, 2001). MixColumns function multiplies the repaired matrix by every column (using exclusive OR (XOR)); this procedure is not run in the last phase (Gurpreet & Supriya, 2013).

Hardware and software can both be used to implement AES. AES is made to take advantage of software optimisation in modern operating systems (Bui et al., 2017). Data processing and transmission delays along with an increase of power and energy utilization are relied on by AES software execution. High performance and throughput could be provided by hardware

implementations; however, these have a similar issue of significant energy usage, that could be harmful to the function of IoT devices. AES encryption requires too much computing power and energy for low powered devices like IoT, in order to maintain data security and privacy.

2.5 Overview of Lightweight Cryptography for IoT in Healthcare

Due to the medical sensors' resource limitations and their direct relation to the health and life of the patient, selecting the right encryption/decryption algorithm is challenging. It should be obvious that traditional cryptographic algorithms require a lot of resources and considerable computation. Whereas in the IoT, and specifically for a time-constrained system like e-health, an acceptable amount of sophisticated security while utilising the least resources is a need.

The cryptographic algorithm that is appropriate for systems with small resources, such as those found in healthcare sensors, RFID tags, and IoT medical equipment, is known as the Lightweight Cryptographic (LWC) Algorithm (Thakor et al., 2021). Its data security could be block-based or stream-based, however, it must provide an acceptable level of protection for instant usage (Yang & Johansson, 2021). LWC algorithms consume a small number of resources for real-time processing; it does not diminish the importance of the security and privacy of IoT devices (Thakor et al., 2021).

AES and several currently available cryptographic algorithms are considered standard cryptography (Kumar et al., 2017). These cryptographic algorithms are intended for use in various structures, including desktop computers, online services, and mobile phones, and have sufficient resources to execute cryptography procedures without degrading performance. These traditional cryptographic algorithms might not even be likely to be made, or their efficiency could be unacceptable on resource-limited objects like IoT devices in healthcare (Kumar et al., 2017). Researchers aim to find LWC algorithms that can work in constrained devices like IoT. These LWC algorithms reduce "weight" in software and hardware (Okelle et al., 2017).

The time and memory complexity of encryption define its software load. The time complexity refers to what time it requires the cryptography to accomplish, whereas the memory complexity refers to the amount of space, the cryptographic algorithm requires to perform its mission (Okelle et al., 2017). The cryptography's time complexity and energy usage affect the hardware weight. The power utilised by cryptography during operation defines the power consumption weight, and the time complexity is equivalent to software complexity. Although power usage is a hardware measurement, which also relates to software because many IoT devices have restricted capabilities (Okelle et al., 2017).

2.5.1 NIST Lightweight Cryptography Standardisation

In 2017, the National Institute of Standards and Technology (NIST) published a document on their existing LWC project and observations on the existing state of LWC (Kumar et al., 2017). The ISO/IEC 29129 standard includes LWC algorithms for several uses in the current form of lightweight cryptography, block ciphers (Kumar et al., 2017). PRESENT and CLEFIA are two ciphers now in use in the standard, both of which have outperformed AES (Kuznetsov et al., 2017).

NIST's LWC project aims to identify an appropriate algorithm that could be utilised based on the target characteristics. Unlike AES, a broad cryptographic algorithm, NIST has created a specific cryptographic algorithm, which will apply to different devices and applications (Kumar et al., 2017).

This section evaluates several LWC algorithms. These cryptographic algorithms meet NIST's proposed standards for LWC algorithms.

2.5.2 PRESENT

In 2007, the PRESENT application was introduced to work in restricted environments (Bogdanov et al., 2007). PRESENT can contain encryption and decryption when performed on a device, or it could be encryption-only with decryption performed elsewhere. It is made up of two algorithms that use either 80-bit or 128-bit keys and employs a 64-bit data block size (Bogdanov et al., 2007). PRESENT was compared to AES by Moriai (2015), although 80-bit was utilised, does not fulfill NIST's required key size. PRESENT-80 requires 284 calculations in terms of security, and while no formal linear cryptanalysis of PRESENT-128 has been done, it may be inferred that PRESENT-128 will be of a higher form (Dutta & Chakraborty, 2020).

Like AES, PRESENT encryption utilizes both substitution and rotations. The difference between PRESENT's encryption and decryption processes is the sequence and use of inverted operations for decryption. 64-bit STATE as well as 64-bit round key are used as initial and subsequent operations. The addRoundKey function applies an XOR between STATE and the round key. STATE is divided into four-bit parts in this function, and the units are processed in parallel using 16 Sboxes of the encryption process. Those sources identify the countermeasure mechanisms included in the Sbox to boost protection. The final operation is pLayer which changes the STATE bits utilising the given formula. This method is repeated 31 times, with phase 32 comprising only one addRoundKey (Bogdanov et al., 2007). The STATE now owns the ciphertext after this last session. The decryption procedure is similar to the encryption procedure. The encryption and decryption procedures used by PRESENT are shown in Figure 2.10; the difference is the usage of

opposite operations and the sequence in which they are performed.

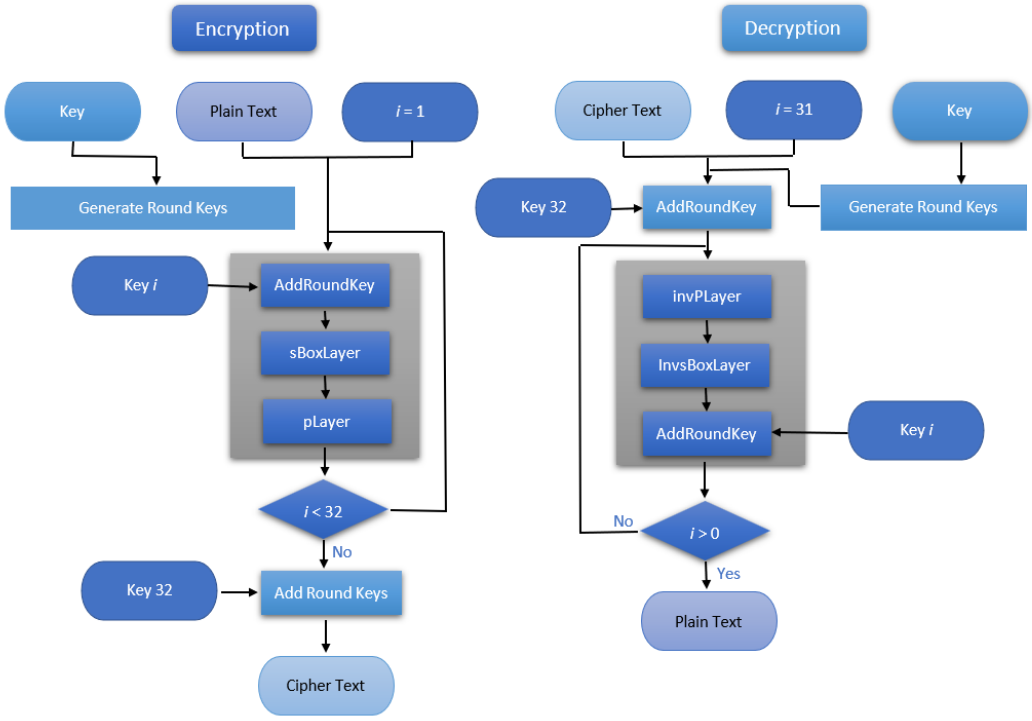


Figure 2.10 *PRESENT encryption and decryption processes (Adapted from Bogdanov et al., 2007)*

2.5.3 Modified Symmetric Encryption Algorithm (MSEA)

MSEA encryption was created in 2014 and gives users the option to select the number of rounds and plain text block size for the encryption process. (Kumar et al., 2014). MSEA supports varied data blocks and the changeable number of stages, and key lengths are rougher than the double-selected block size. They each have a significant level, as stated in Table 2.4 because they are all adjustable. The addition of unusual cycles and the diversity of stages and block sizes all contribute to a higher level of security. Modifying a single bit of plaintext impacts more than 50% of the cyphertext bits following nine rounds (Kumar et al., 2014).

Table 2.4 *MSEA Parameter Values (Adapted from Kumar et al., 2014)*

Parameters	Minimum	Maximum
Key Size	256	4096
Rounds	1	63
Block Size	128	2048

Although it is not the only addition to cryptographic algorithms, AES and PRESENT have utilized the Substitution–Permutation Network (SPN) concept. The MSEA algorithm operates the variable combination, spin, and XOR (ARX) mechanism (Kumar et al., 2014). These different functions can be carried out without excessive expenditures because of substitutions or pairings.

The first step of the MSEA method is the generation of round keys, and the following phase is genuine encryption or decryption. Before proceeding, several features should be calculated the rounds, block size, exchange key, and master key (KM); recognised as the accumulating key because the sender and receiver share it (Kumar et al., 2014).

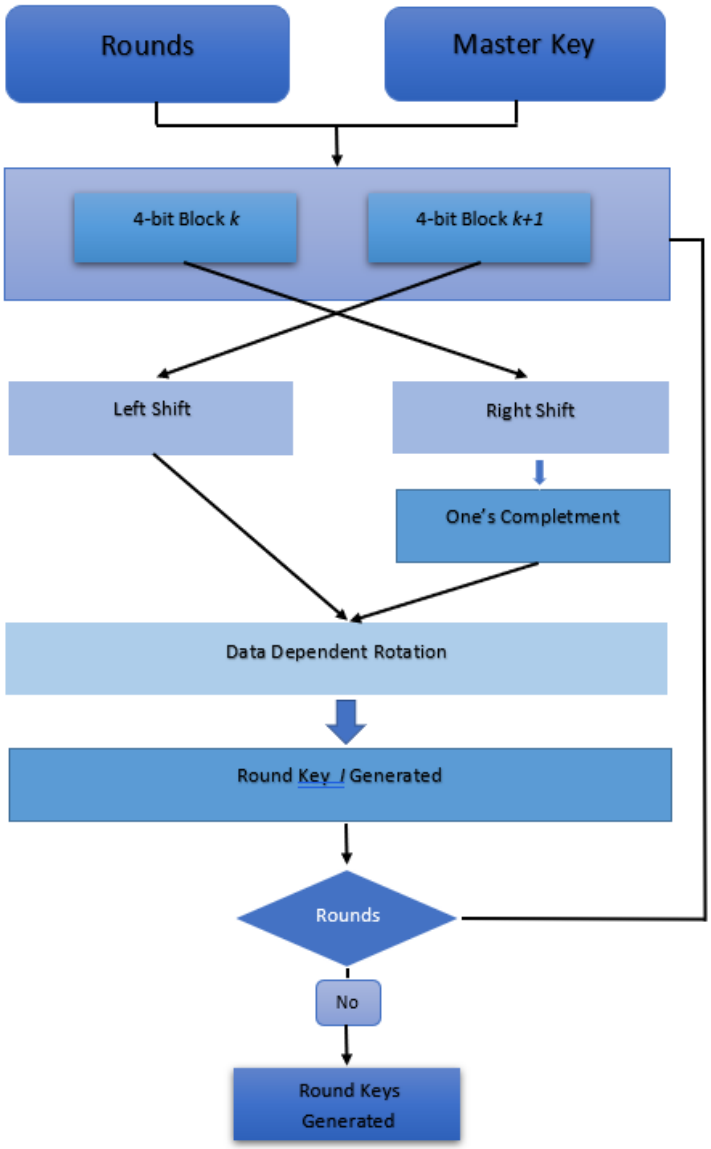


Figure 2.11 *MSEA Round Key Generation (Adapted from* Kumar et al., 2014*)*

The block size amount is the integer that indicates the quantity of bits in a data block. This number is multiplied by 8 and can vary from 128 to 2048. Based on the number of rounds, this number could range from 1 to 63 (Kumar et al., 2014). During the round key formation process, the exchange key is used, and the value of bits needed for this key is determined by calculating log2 s, which depends on the data block size. For the 128 bits block size, the key size is 7 bits (Kumar et al., 2014).

The master key, like AES and PRESENT, must be the double of bits in the data memory space, which is the third element. For a block size of 128 bit, the master key could be 256 bits (Kumar et al., 2014).

The round keys are created in the first stage utilising the parameters previously collected; Figure 2.11 shows the round key creation procedure. It will employ the number of rounds and the most significant aspects of this technique. In each cycle, the round key creation generates per round key with about the key length as the master key size (Kumar et al., 2014). 4-bit change is a direct action conducted on the master key or the earlier session key. This operation replaces the 4-bits block with the next 4-bits block. It turned one block to the left after the exchange, while the other is turned to the right, followed by one's counterpart. The result is inverted in a data-dependent fashion once all four 4-bit blocks have been handled. Log2's small bits regulate the formation; the first bit defines whether the function is right or left, and the succeeding bits determine the amount of spins (Kumar et al., 2014). Using this data, the outcome is turned right or left for the set of specified bits.

The round key can be applied for encryption or decryption. MSEA merely reverses the encryption technique, unlike AES or PRESENT, which involve reversal procedures for decryption (Kumar et al., 2014). Figure 2.12 depicts the encryption process, separated into three stages: message expansion, encryption rounds, and exchanges. The plaintext is split into 8-bit blocks, which are then enlarged to 16-bit blocks, resulting in text with an identical amount of key size bits. The four least significant bits are attached to the most significant bit.

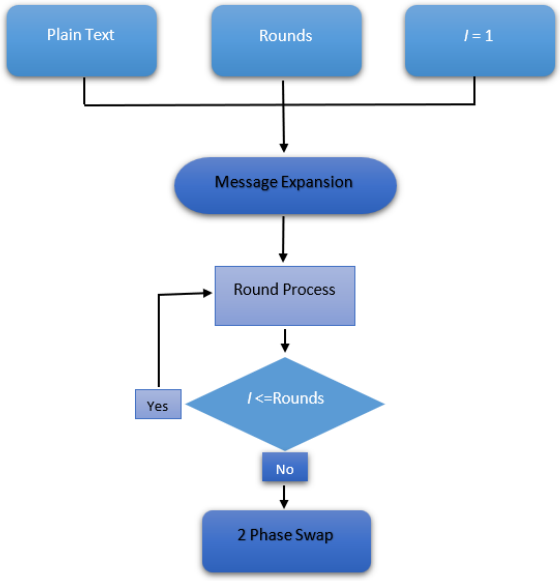


Figure 2.12 *Overall MSEA encryption process (Adapted from Kumar et al., 2014)*

In comparison, it attached the four most many bits before the least relevant bit to perform this multiplication (Kumar et al., 2014). After that, the 16-bit block goes through two data-dependent spins, like how keys are formed. The last four bits of the initial rotation are used to decide how the round will proceed. The direction, like previously, is the most critical bit, and the leftover bits represent the number of bits to rotate.

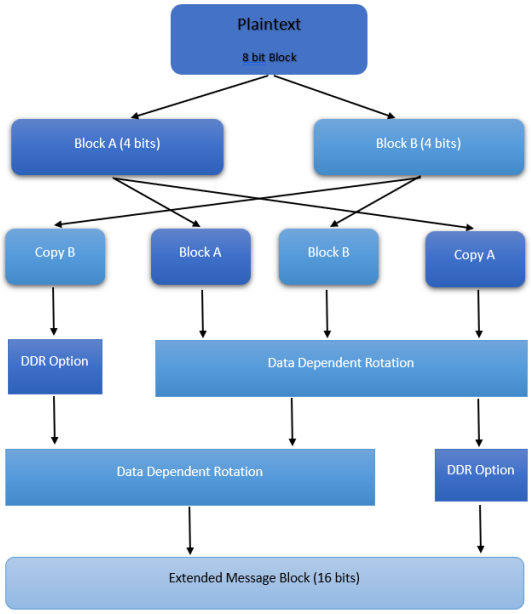


Figure 2.13 *Message expansion of MSEA (Adapted from Kumar et al., 2014)*

The first four bits are used in the next spin, following a similar procedure. Counterpart is applied to the blocks of 16-bit (Kumar et al., 2014). This procedure is repeated for the remaining blocks of 8-bit, resulting in extended text. Figure 2.13 depicts the message extension mechanism.

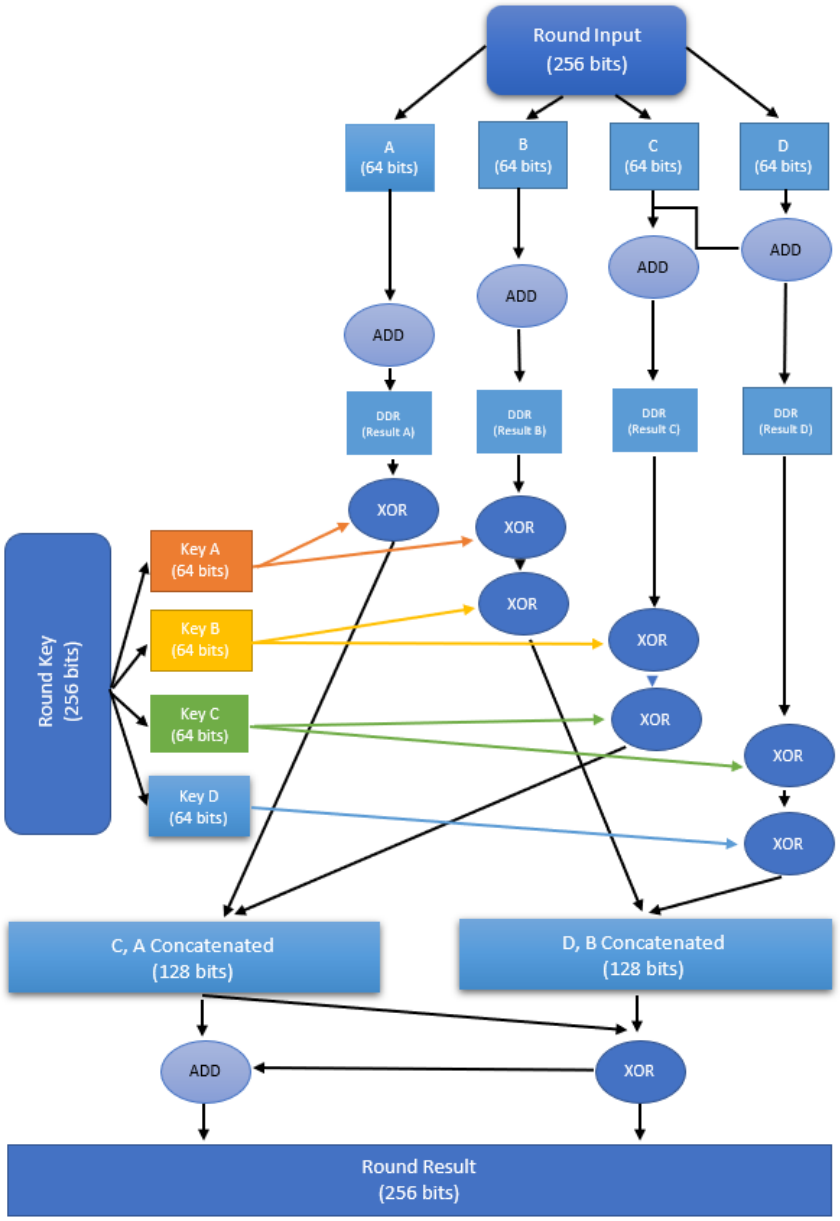


Figure 2.14 *Sending message in the encryption process (Adapted from Kumar et al., 2014)*

After the message has been extended, the encryption technique shown in Figure 2.15 is utilised to send the message. First, the raw message is divided into four equal sections, marked A, B, C, and D. These pieces will be sent through modular addition once they have been formed; D is the outcome of C and D, and C is the product of C and B, B is the outcome of B and A, and A is the

product of new D and A. Following this combination, the rotation is conducted utilising the final log2 m (m is the block size) (Kumar et al., 2014). The round key is divided into four keys designated $Kiia$, $Kiib$, $Kiic$, and $Kiid$ after turning the blocks. These keys are employed to function XOR ($\oplus$); The results from $A \oplus Kiia$, B is the result of $B \oplus Kiia \oplus Kiib$, C results from $C \oplus Kiib \oplus Kiic$, and D is the result of $D \oplus Kiic \oplus Kiid$. Then, in the provided order, blocks C, A, D, and B are combined to generate two new blocks, E and F (Kumar et al., 2014). Block F is XOR with E, and it saves the result in F; block E is modularly added to novel development in F, and the outcome could be saved in E. E and F are combined with a specified sequence, restoring the increased amount. This procedure is repeated as many times as the *r* argument identifies.

Following encryption procedures, it subjected the result from the final round to the two-phase change employing switch key *k*. Two steps compensate for this phase. Each *k*th bit is switched from 1 to 0 or 0 to 1 in the first phase. The next phase is the same as the 4-bit switch in the key creation, except that the swap is done on k-bits instead of 4-bits (Kumar et al., 2014). The encrypted message with an identical length as the key length results from the two-phase exchange.

2.5.4 LEA

LEA cipher is the encryption that was introduced in 2014. This algorithm uses two steps, the first phase is round key creation, and the second is encryption and decryption. The plaintext, ciphertext, and keys are all stored in arrays of 32-bit blocks in LEA (Hong et al., 2014). The plaintext/ciphertext, as well as the master key, are fed into the algorithm. The LEA utilises the values stated in Table 2.5, which are hexadecimal representations of the square root.

Table 2.5 *LEA Constants (Adapted from Hong at al., 2014)*

Constant	Value (hex)
δ[0]	0xc3efe9db
δ[1]	0x44626b02
δ[2]	0x79e27c8a
δ[3]	0x78df30ec
δ[4]	0x715ea49e
δ[5]	0xc785da0a
δ[6]	0xe04ef22a
δ[7]	0xe5c40957

The round keys are generated differently based on the key length specified for key generation. LEA-128 and LEA-192 versions utilise a comparable technique to key creation; however, LEA-

256 takes a specific strategy (Hong at al., 2014). To begin, it broke the master key into 32-bit blocks, these blocks are allocated as *T[x] = K[x]* (*K[x*] is the master key's *x*th block) (Hong at al., 2014). The round consistent is extracted for the first T block using ii mod 4, I is the existing round beginning at 0, and the variable is rotated by I bits. It modularly added the result of these spins with T[0] before being turned left by one bit (Hong at al., 2014).

Other blocks utilise the same technique; for the constant rotation, the number of bits to rotate is determined by I + block index, and in the configurable extension outcome, block 1 spins 3 bits, block 2 spins 6 bits, and block 3 spins 11 bits. The *i*-th key is the group of specified list; the next spin's entry could be the outcomes stored in T (Hong et al., 2014).

The next step is to encrypt or decrypt using the round keys that have been created. The encryption method is detailed in Figure 2.16, but the decryption is essentially the opposite of encryption.

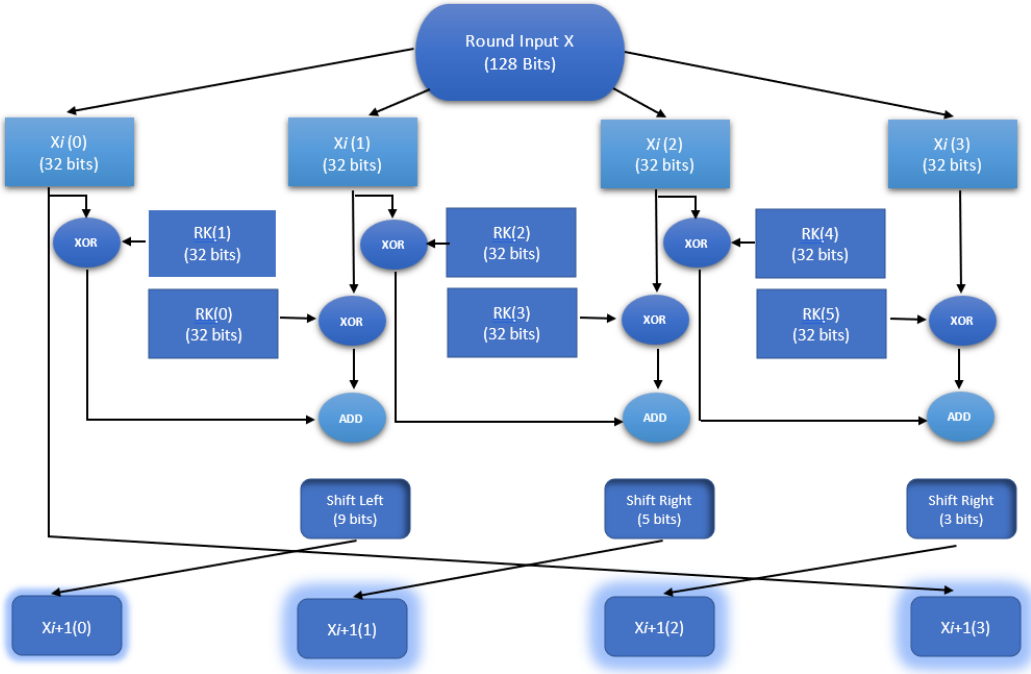


Figure 2.15 *LEA encryption process (Adapted from Hong at al., 2014)*

The purpose of LWC is to offer security solutions that can perform on devices with restricted resources by consuming less memory and less energy (Bhatt, 2020). In comparison to traditional cryptography, LWC is intended to be simpler and faster. These specific LWC algorithms might be suitable for IoT in healthcare. Because IoT devices have limited resources, suitable cryptographic algorithms are necessary for IoT-based healthcare systems. Before sending any data over a public network, it must be encrypted.

2.6 Conclusion

The literature review presented a summary of studies conducted in the IoT field as well as a growing collection of publications focusing on IoT security and privacy in healthcare. It reveals gaps in knowledge and illustrates that restricted research has been done in detailed sectors of IoT, such as IoT security and privacy challenges.

Section 2.2 provided an overview of the IoT. IoT was described, and the explanations for its rapid expansion were addressed. The advantages for both businesses and consumers, as well as the potential security and privacy threats posed by the IoT's increased widespread connectivity, were highlighted. Then, studies into structural models for the IoT were performed. Section 2.3 searched into IoT security. Finally, Section 2.4 concentrates on studies into IoT in Healthcare. Section 2.5 investigates the publications on LWC algorithms of IoT in healthcare.

Chapter 3 concentrates on creating the research approach to examine the security or privacy challenges related to IoT in healthcare and evaluating LWC algorithms for IoT. An appropriate process to research the potential IoT security and privacy challenges in healthcare, as well as the methodology to identify the critical factories of LWC algorithms, will be formed.

Chapter 3: Research Design and Methodology

3.1 Introduction

This chapter explains the adapted research methodologies for exploring security and privacy vulnerabilities associated with IoT and identifying a suitable approach for assessing LWC algorithms for IoT in the healthcare sector.

Various technical and other challenges regarding the security and privacy of IoT devices in healthcare were identified during the literature review in Chapter 2. Research questions mentioned in Section 3.2 were developed, stated, and explained using these challenges and gaps highlighted in the current set of research. To correctly answer these questions, it has been recognised that a methodological approach is required.

To answer these research questions, it is defined that two research approaches are needed. Sections 3.3 and 3.4 explain the methodologies chosen for each section of the research.

3.2. Research Questions

The literature review discussed in Chapter 2 highlighted that IoT devices in the healthcare industry have security and privacy problems that could compromise the safety and privacy of both patients' and organisations' data there is growing awareness about these issues (Elhoseny et al., 2021). This thesis intends to fill the research gap by studying and investigating the reported data from the Systematic Literature Review (SLR) and the Experimental Performance Testing. The Experimental Performance Testing method was implementing eight LWC algorithms using an IoT platform and ranks the LWC algorithms in a specific order for each evaluation metric, such as execution time, power consumption, memory usage, and throughput.

The research questions of this thesis will aim to answer are as follows:

Research Question 1 (RQ1). What are the main IoT security and privacy issues in healthcare?

A variety of IoT security and privacy threats can come in the form of either passive or active threats. Attackers can acquire data without affecting network behaviour in passive threats; however, inactive threats and intruders can block or slow down service administration (Kumar, 2016).

The Systematic Literature Review (SLR) research methodology indicated a rising concern from IoT in healthcare around security and privacy risks.

Research Question 2 (RQ2). What are the most important performance factors of IoT lightweight cryptographic algorithms in healthcare?

RQ2 was formulated to find the most important factors of IoT LWC algorithms in healthcare using the SLR research methodology.

Research Question 3 (RQ3): Which lightweight cryptographic algorithm would produce the best performance results?

RQ3 was formulated to address the performance evaluation of eight chosen LWC algorithms and identify the best performance results that should be considered for choosing the LWC algorithms for IoT in healthcare.

3.3 Research Approach

Two approaches were used for gatheringthe required data to answer these research questions.

Firstly, the Systematic Literature Review (SLR) methodology was employed to gather data to answer RQ1 and RQ2. The SLR systematically collects data from previous studies to present the background of IoT privacy and security issues as well as the most important performance factors of IoT LWC algorithms in healthcare. This SLR research methodology was chosen as a suitable approach for answering RQ1 and RQ2. Because to address a clearly stated question, the SLR research methodology identifies and systematically evaluates current research (Munn et al., 2018). SLR can be either quantitative or qualitative; the former provides a detailed review that uses numerical data, while the latter contains qualitative research that uses observation and analysis of interviews and verbal activities to obtain the data (Snyder, 2019). This SLR is defined as a quantitative systematic review.

Secondly, the Experimental Performance Testing research methodology was chosen to obtain the data needed to address RQ3. In terms of the research, quantitative data analysis is used. Quantitative data analysis is essentially the study of data that is based on numbers or that can be easily converted into figures without losing any value (Austin & Sutton, 2014). Following this methodology, eight LWC algorithms were compared to find the best LWC algorithm utilised the best performance. The result of this comparison points to choosing a suitable LWC algorithm regarding the shortest encryption/decryption time, and low resource consumption (energy, RAM, and ROM) of IoT devices in healthcare.

3.4 Systematic Literature Review (SLR) Research Methodology

The Systematic Literature Review (SLR) is described as "an analysis of the findings on a clearly defined question that employs systematic and specific methods to find, choose and objectively evaluate the significant independent study, and to explore and analyse data from the selected works" (Wright et al., 2007). The SLR research methodology was undertaken to answer RQ1 and RQ2 of this study.

3.4.1 Approach and Mode

The research approach, which was defined using SLR research methodology on studies that had already been published, focused on the IoT security and privacy in the medical sector. This research methodology was chosen for this study to answer RQ1 and RQ2 because the SLR analysis is appropriate when the research field has the overall view and supplying a typical concept is needed (Snyder, 2019).

This SLR is defined as a qualitative systematic review, which is a method for evaluating the results of qualitative research (Booth, 2016). After gathering the publications, a strict systematic review procedure is applied, and then a quantitative approach is used to evaluate them. A qualitative SLR often follows the same procedures as other systematic review guidelines, including the use of eligibility requirements in systematic reviews and the techniques for collecting and screening existing studies (Xiao & Watson, 2019). The SLR's final write-up, which summarises the findings and presents findings and conclusions, brings everything to a conclusion by tabulating the evidence into a summary of findings tables (Paré & Kitsiou, 2017). Using an integrated coding process, data collection from selected scientific databases was assembled in this research methodology. This SLR research methodology's phases are explained in the following subsections.

3.4.2 Data Collection

Google Scholar, PubMed, IEEE, Scopus, and Science Direct, were used to perform the SLR. This SLR was limited to studies published between 2017 and 2021 to gather more up-to-date background information on this field. All potential variations of the keywords searching phrases in all databases were included in search engines: "Internet of Things" OR "IoT" AND "Healthcare" OR "Health Care" AND "Security" AND "Privacy" OR "Lightweight Cryptography" AND "Performance Evaluation". In the first phase, 279 studies were obtained from various databases and placed into the dataset generated using Endnote software. Thirteen duplicate papers were found and removed during the initial screening of the paper titles. Then, after skimming the abstracts, 112 research papers were removed based on the exclusion criteria (Table 3.1). After scanning the full text of 154 articles and applying the specified exclusion criteria, 85 articles were excluded. After this, 69 articles met the requirements for inclusion and were considered for a detailed search and analysis. Figure 3.1 illustrates the overall procedure and details of the research paper selection procedure.

Table 3.1 Exclusion Criteria

	Exclusion criteria
1	Articles which are not in English
2	Studies with a purely technical focus
3	Book Chapter/Company report/Letter/Thesis/Abstract
4	Studies with a medical focus only
5	Smart home studies with no discussion on healthcare

3.4.3 A Pilot Test of the SLR Research Methodology

From 69 articles, 20 were chosen randomly for the pilot test. Articles were analysed using thematic analysis. The articles were thoroughly reviewed to identify IoT privacy and security issues in the medical sector as well as the most important factors of IoT LWC algorithms. The pilot test was done using the qualitative data analytical software NVivo.

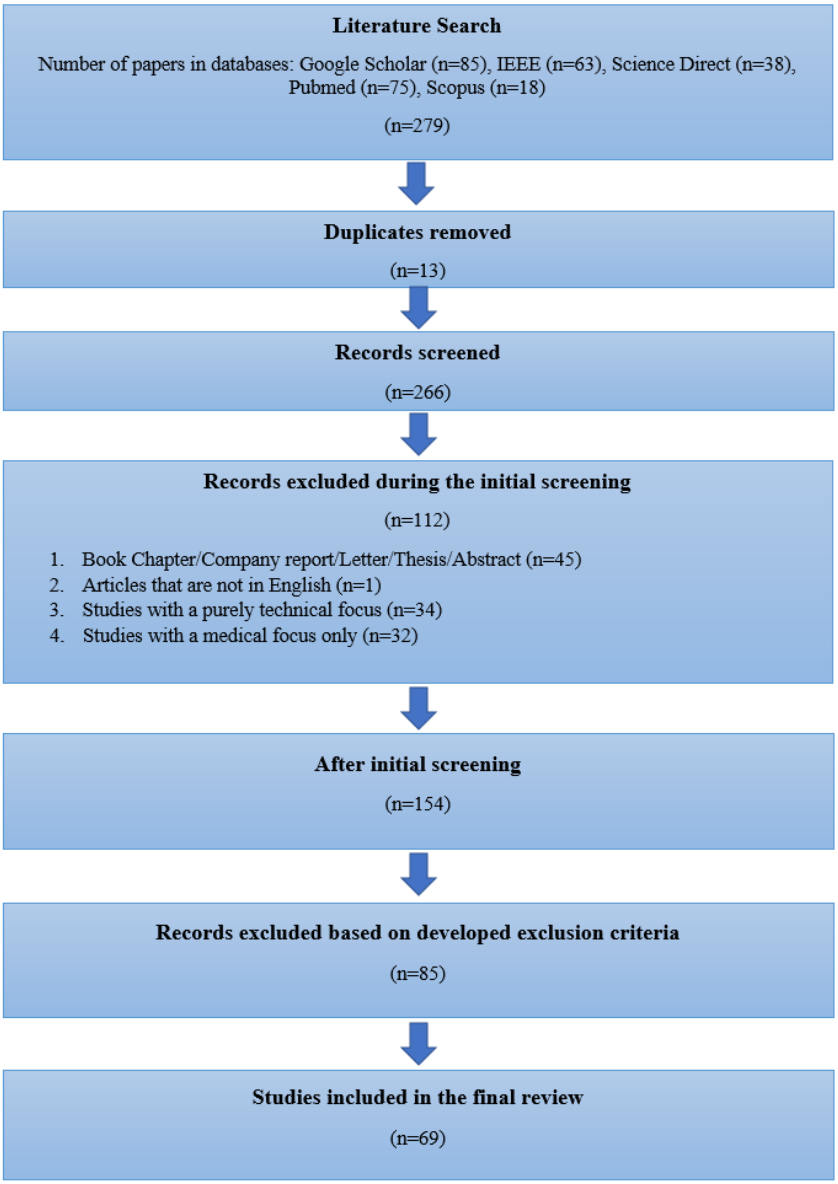


Figure 3.1 *Flow diagram of the SLR*

3.4.4 Coding and Data Analysis

This phase collected data from selected articles and assigned them to pre-determined groups. Several additional categories appeared at this step. Deductive and inductive coding is used in combination with this research method. Inductive coding is a non-pre-defined exploratory study, while deductive coding uses classifications as a guideline for the coding stage (Selvaraj & Sundaravaradhan, 2020).

The pilot test outlined three essential security and privacy areas: the perception layer, network layer, and application layer of IoT devices in healthcare, used as a pre-developed data set for

deductive coding. In addition, new application areas were identified and introduced as new codes during the coding process. The combined coding method assisted in the coding phase by using deductive coding and inductive coding to analyse the developing codes.

For data analysis, organising the coding, and data processing, NVivo software was used. The SLR aimed to gather qualitative data for the investigation to give a comprehensive overview of existing and potential IoT security and privacy problems in healthcare. Due to the big amount of data, SLR analysis can be challenging. However, the process is manageable since a methodical approach is taken. Simply capture the main conclusions of all included articles by study type, and then evaluate the collection refers to results based on the frequency of data, to create a summary of results from multiple qualitative studies.

3.5 Experimental Performance Testing Research Methodology

Several LWC algorithms are being developed for IoT data protection. Due to the sensitive nature of the medical field, not all of them might be suitable for IoT medical applications. The experimental performance testing research methodology was undertaken to answer RQ3, to choose eight LWC algorithms that were systematically tested and evaluated their performance for key performance factors for both encryption and decryption modes. These eight LWC algorithms are suitable and meet the requirements of security for IoT in healthcare.

Collecting quantitative data and doing statistical analysis for the study purpose, this experimental research methodology uses quantitative data analysis. Because the core of quantitative analysis is the statistical and numerical description and evaluation of objects. Through numerical variables and statistics, the quantitative analysis aims to analyse the data gathered for the phenomenon.

3.5.1 Research Design

Experimental performance testing is a systematic procedure in which experiments are designed to identify one or more factors of the provided element. Using SLR research methodology which was mentioned previously to answer RQ2 and to find the key factors of IoT LWC algorithms in healthcare. These results were used in the experimental performance testing methodology to determine which LWC algorithm had the best performance. The experimental procedure employed in this thesis is illustrated in Figure 3.2.

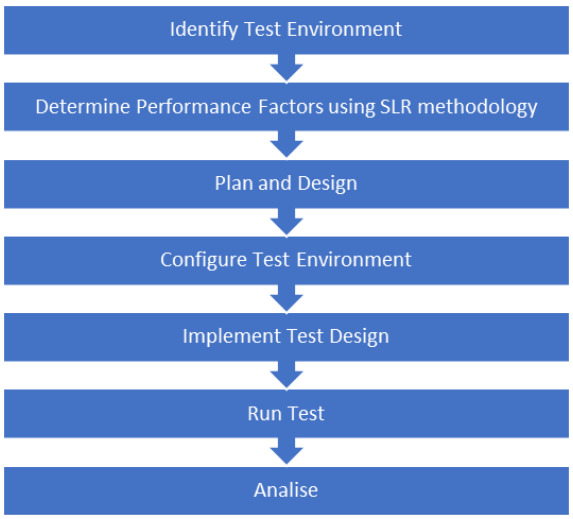


Figure 3.2 *Experimental Performance Testing Process*

This research chooses eight LWC algorithms based on their block size, key length, popularity, and operational potential of the IoT in the healthcare environment. And these LWC algorithms analysed their performance for battery usage, memory consumption, throughput, the execution time in various payloads. Choosing an LWC algorithm for low resource consumption (energy and memory) and providing acceptable security is the motivation to evaluate LWC algorithms in this thesis.

This research selected Raspberry Pi 3 as the IoT platform and the Google Drive cloud server as a file exchange to evaluate the eight lightweight algorithms over an IoT platform. Each experiment is repeated 5 times to obtain more accurate outcomes. On the sender side, the plaintext is encrypted using LWC algorithms, which is then transferred to the cloud for decryption; the Raspberry Pi 3 receives the file from the cloud and begins to decrypt it. Figure 3.3 shows the view of data transfer.

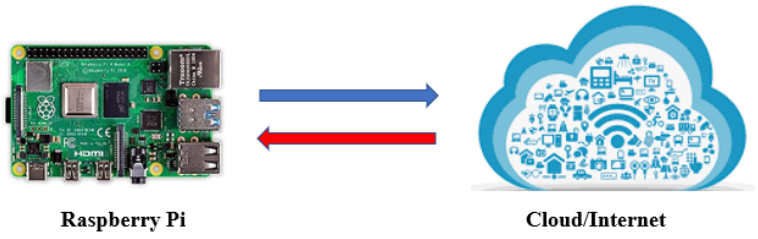


Figure 3.3 *Data exchange schema for the experiment*

3.5.2 Research Goals of Experimental Performance Testing

The specific factors addressed in this study to maintain the acceptable LWC algorithm for IoT medical devices are determined by the encryption/decryption execution time, memory consumption, energy usage, and throughput briefly mentioned below.

Encryption/Decryption Execution Time - The energy consumption can be reduced, and battery life can be increased by the quick execution of an LWC algorithm. The optimisation of all three metrics, namely energy consumption, memory usage, and execution time, is necessary and will be covered in more detail in the implementation and assessment section.

Memory Usage - IoT devices in healthcare have very little memory. For this reason, this study concentrated on determining how much RAM and ROM the LWC algorithm required.

Energy consumption - the amount of battery power required during encryption or decryption. The power usage represents the amount of electricity required to run the cryptographic operation. The lower the power consumption, the better for the algorithm. Most IoT medical devices are manufactured with limited energy or battery resources (Norah et al., 2017). The interaction and processing of the sensors, which have an impact on how much of the power is used for consumption, will determine which security measures may be applied (Schukat et al., 2016).

The throughput - is used for the quantity of plaintexts processed per second (bps). The higher throughput is the better for the algorithm performance.

Energy consumption, memory use, throughput, and execution time are the three interrelated characteristics. These characteristics will be used to identify the benefits and drawbacks of each cryptographic algorithm and where each cryptographic algorithm might be useful.

The following are the objectives of this study:

- Providing a fair evaluation for characteristics given in the literature such as power consumption, memory usage, throughput, and execution time by implementing eight lightweight algorithms via the cloud using an IoT platform.

- Examine and analyse data from operations, and rank the LWC algorithms mentioned for each comparison factor.

- Discuss the findings to choose the optimal LWC algorithm for all the numerous measures.

3.5.3 Data Requirements

The experimental performance tests will be analysed where all features can be measured, allowing for direct and comprehensive analysis of the data. As a result, a testing procedure where all of the elements could be tested and monitored. To avoid false data, an isolated environment could create better outcomes. This isolated system's purpose is to simulate a performance testing process that identifies the techniques used to collect data from the Raspberry Pi 3 device.

3.5.4 Lightweight Cryptographic (LWC) Algorithms Selection

Lightweight solutions assist in preserving memory and processor requirements as low as possible. Eight lightweight block cyphers are chosen and tested for performance in this paper. The following is a brief explanation of the eight LWC algorithms, AES, PRESENT, MSEA, LEA, XTEA, SIMON, PRINCE, and RECTANGLE, that were chosen because they were suitable, and all fulfill the requirements of NIST's LWC algorithm standards.

1. AES - It has 128 bits displayed by a 4*4 matrix, and the algorithm state is processed using four operations: Substitute Bytes, Shift Rows, Mix Columns, and Add Round Key (Heron, 2009). Sub-Bytes (A four-byte word is the SubByte return value), Shift Rows (State rows are cyclically shifted over different offsets), Mix Columns (State columns are expressed as polynomials and multiplied by modulo x4 + 1 with a constant polynomial c(x)), and Add Round Key (Dworkin et al., 2001). It is noticed that the AES shifting operation greatly assists in accelerating the algorithm's speed.

2. PRESENT - the architecture of this LWC algorithm is the model resource for many LWC algorithms. It has a bit-oriented SPN structure. Creating round keys, this algorithm functions the steps: addRoundKey (Involves the operation for $0 \leq j \leq 63$, $bj \rightarrow bj \oplus k^i$), sBoxLayer (Uses a single 4 × 4 S-box), pLayer (The *i*-th bit of STATE is moved to position P(i) due to specific mapping). It is recommended on hardware platforms (Bogdanov et al., 2007).

3. MSEA - allows for alternative combinations in rounds and block sizes, they could be limited to specified levels to stabilize the testing environment. The MSEA requirements are followed first, allowing the MSEA characteristics to be flexibly set, and the block is confined in the second. Because 256-bit keys are required, the block size is to be set to a minimum of 128 bits each. Because decryption is the inverse of encryption, algorithms will be the opposite of actual encryption. Finally, for additional security, the number of rounds will be set to 18, which will also be utilised for testing (Kumar et al., 2014).

4. LEA version - will take advantage of the bitwise functions given by C. Only the LEA-128 version will be examined because LEA can employ 128 bit, 192 bit, or 256 bit keys (Jap & Breier, 2015). The LEA design handles all other settings. It is a reversal of the encryption operation for the decryption function.

5. XTEA - are following the Feistel formation. It has a key size of 128 bits and a block size of 64 bits. The TEA system is a simple key schedule mechanism. Rearranging shifts, XORs, and adds operations have improved compared to XTEA. It also employs a more complicated key scheduling method. Both feature 128-bit key and 128-bit block sizes (Moon et al., 2002).

6. SIMON - is a Feistel structure for hardware systems. Its primary goal is data protection in environments with limited resources, such as the IoT in healthcare. The fundamental operations of the SIMON algorithm, which have an impact on the sensitive data that needs to be secured, can be seen as straightforward round functions of bitwise AND, XOR, and shifts. It is designed with hardware implementations to increase performance while running on hardware, however, it has been discovered to produce results that are acceptable for both software and hardware data cryptosystems. Key sizes range from 64 bits to 256 bits, depending on the situation. A block can have a specific value ranging from 32 to 128 bits. Round numbers could range from 22 to 34. Round function adding and XORing operations (Alassaf et al., 2019).

7. PRINCE - is built with FX, and no exact key scheduling technique of this algorithm could explain it; It acquires two of its 64-bit keys within the 128-bit master key, which serves as a whitening key, and the third one is XORed in the internal state during encryption. Per round contains the following stages: key addition (the 64-bit state is XORed with the 64-bit subkey), one Sbox-layer (a single four-bit Sbox is used), a linear layer (a 64*64 matrix is multiplied by a 64-bit state in this layer), and consistent round addition (The state is XORed with a 64-bit round constant) (Borghoff et al., 2012).

8. RECTANGLE - has SPN framework. This LWC algorithm has 25 rounds that include the following steps: SubColumn (S-boxes are implemented to 4 bits within a column), ShiftRow (A simple bitwise XOR is implemented to the medium state), AddRoundKey (To the medium state, a simple bitwise XOR is implemented), ShiftRow (Each row is rotated to the left at various variations). S-box for this LWC algorithm could be built using a series of twelve basic logical operations. The P-layer is made up of three rotations (Zhang et al., 2015).

Table 3.2 compares the eight chosen LWC algorithms.

Table 3.2 Comparison of Selected LWC Algorithms

Name	Block size (bit)	Key size (bit)	Structure	References
AES	128	128	SPN	Daeman & Rijmen, 1998
PRESENT	64	128	SPN	Bogdanov et al., 2007
MSEA	128	256	Feistel	Kumar et al., 2014
LEA	128	128	GFN	Jap & Breier, 2015
XTEA	64	128	Feistel	Moon et al., 2002
SIMON	64	128	Feistel	Ray et al., 2015
PRINCE	64	128	SPN	Borghoff et al., 2012
RECTANGLE	64	128	SPN	Zang et al., 2015

3.5.5 LWC Algorithm Implementation

Most of the LWC algorithms that will be examined and designs must be implemented to be explored. These algorithms will be implied in C and generated with the GNU Compiler Collection (GCC).

3.5.6 Testing Environment

On a Raspberry Pi 3, the LWC algorithms will be evaluated. This Raspberry Pi 3 model has 1 GB of RAM, and a quad-core processor, and runs at 1.2 GHz (Raspberry Pi, n.d.). A Broadcom BCM2837 64-bit CPU and a 64-bit ARM Cortex A53processor (Raspberry Pi, n.d.). It could be powered by a 5 V Micro USB or PowerBank. The Raspberry Pi 3 was powered by a 10,400 mA Power Bank. To control, the researcher connected the RaspberryPi 3 to a Dell Notebook via ethernet and USB ports. When measuring battery usage, a USB power meter was used. By measuring the USB power meter, the overall battery usage of the Raspberry Pi 3 during encryption and decryption could be calculated. Figure 3.4 shows the experiment setup.

Figure 3.4 *Experiment Setup*

3.5.7 LWC Algorithms Testing

As previously indicated, the LWC algorithms will be compared to execution time, memory usage, and energy consumption. Each of these resources would be investigated in various file sizes. The file sizes will be 16 KB, 64 KB, 256 KB, 512 KB, 1024 KB, and 2048 KB. Over the different data sizes, each of those encryption algorithms will be completed.

The monitoring software Massif will perform the encryption memory consumption. By default, this tool measures how much stack memory a method employs. The device can be applied to estimate how much memory a process uses, including codes. The RAM consumed during encryption and decryption will be monitored when Massif is used. This test will be conducted independently from the other resources due to the tool's structure, which executes slower simulations of a program's code.

Furthermore, the previously mentioned USB power meter will calculate battery utilisation. This experimental performance test will measure the voltage generated during an encryption process's encryption and decryption operations. As a result of this interaction, the execution time and charge usage tests will be done simultaneously.

3.5.8 Data Collection

The obtained data is the core of this research methodology. Each performance experiment will be conducted as follows.

• At the start of every experiment, all hardware will be turned off. Ensure that no information is saved on the physical components that can affect the data.

• The laptop will be turned on in the second stage.

• Based on the experiment requirements, modify extra hardware or software.

• A checklist will be utilised to document all of the parameters once the experiment is accomplished. Checking that they are arranged correctly for the experiment.

• After completing all the procedures, each device's goal would be changed to launch the experiment.

• Begin gathering data for additional assessment. Once the study has collected sufficient data, it would then be stored, and all devices would be turned off.

3.5.9 Data Analysis

During this phase, all study outcomes would be documented. After storing data, all settings will be adjusted to the available resources, including deleting data or disconnecting any equipment utilised for the experiment. During data analysis, those data will be examined for anomalies as well as errors. Misconfigurations or other errors may occur during the data collection or analysis phases, resulting in erroneous data that must be identified to repeat the test or pinpoint the problem. Similarly, certain studies will be run multiple times in order to compare data.

3.6 Conclusion

In Chapter 3, the adapted research methodologies for this study were discussed. This chapter highlighted the main research questions. The data collecting, analysis, and research methodologies were all discussed. The results of the systematic literature review and the evaluation testing procedures are presented in Chapter 4.

Chapter 4. Findings

4.1. Introduction

This chapter provides the outcomes obtained from the Systematic Literature Review (SLR) of IoT privacy and security problems and the evaluation of LWC algorithms of IoT in healthcare. Section 4.2 covers the findings of the SLR conducted to identify the main medical IoT privacy and security issues and the most important performance factors of LWC algorithms in the healthcare field. Section 4.3 presents the experimental performance evaluation testing findings of chosen eight LWC algorithms.

4.2 Systematic Literature Review Findings for RQ1

A visual and narrative description of the primary research results is provided. These outcomes contain the results of data analysis obtained from the records to recognise any relations and patterns within the collected data that may allow for a better comprehension of the study results and support them answering the research questions.

4.2.1 IoT Security and Privacy in Healthcare

While using IoT for healthcare can provide enormous potential for medical professionals and the healthcare industry, it is essential to note that security is a significant barrier to IoT adoption and implementation in healthcare.

The main issue is the security of data transmitted from a patient's device through wireless networks, which could reveal unencrypted patient data. Security and privacy are significant issues since most appliances and their applications are wireless. Users may not take full advantage of all the IoT opportunities provided to the healthcare system because of the violations or privacy issues addressed (Amaraweera & Halgamuge, 2019). Most media or networks are vulnerable to security and privacy concerns, especially in healthcare, since personal and private information is concerned. Furthermore, the diversity of resources and network heterogeneity have aggravated the issue of IoT devices (Ianculescu et al., 2020).

Although IoT is a combination heterogeneous networks, including sensors, mobile phone networks, and the Internet, which have the same security and privacy risks that could affect IoT (Alkhatib et al., 2018). Other security areas to further consider and investigate which are heterogeneous network authentication, privacy protection, access control, information management, confidentiality, and trustworthiness (Bajrić, 2020).

Users are hesitant to consider IoT-based healthcare services because of the security and privacy problems listed above. However, it is expected that if the problems are identified and solved, technology acceptance will improve by reducing psychological and social incongruity associated with IoT usage (Djenna & Saïdouni, 2018).

As a result of the increased trust and growing acceptance of IoT in healthcare, the quality of the service provided by medical institutions should significantly improve, leading to a better healthcare system. Attempts have been made to identify various security and privacy challenges in IoT in healthcare applications. By resolving them, technology suppliers and service providers could be advised to meet those requirements for potential advanced technologies growth.

IoT security and privacy risks are various, including physical information and administration, network, and data (Ren et al., 2017). These could be passive or active threats. At passive threats, attackers could collect information, while active intruders would interrupt or slow down the operation of the services without affecting network activity (Abdullah et al., 2019).

All these types of problems were investigated depending on the design of IoT in this study. Therefore, the IoT vulnerabilities in healthcare can be categorised into perception, network, and application layers are illustrated in Figure 4.1.

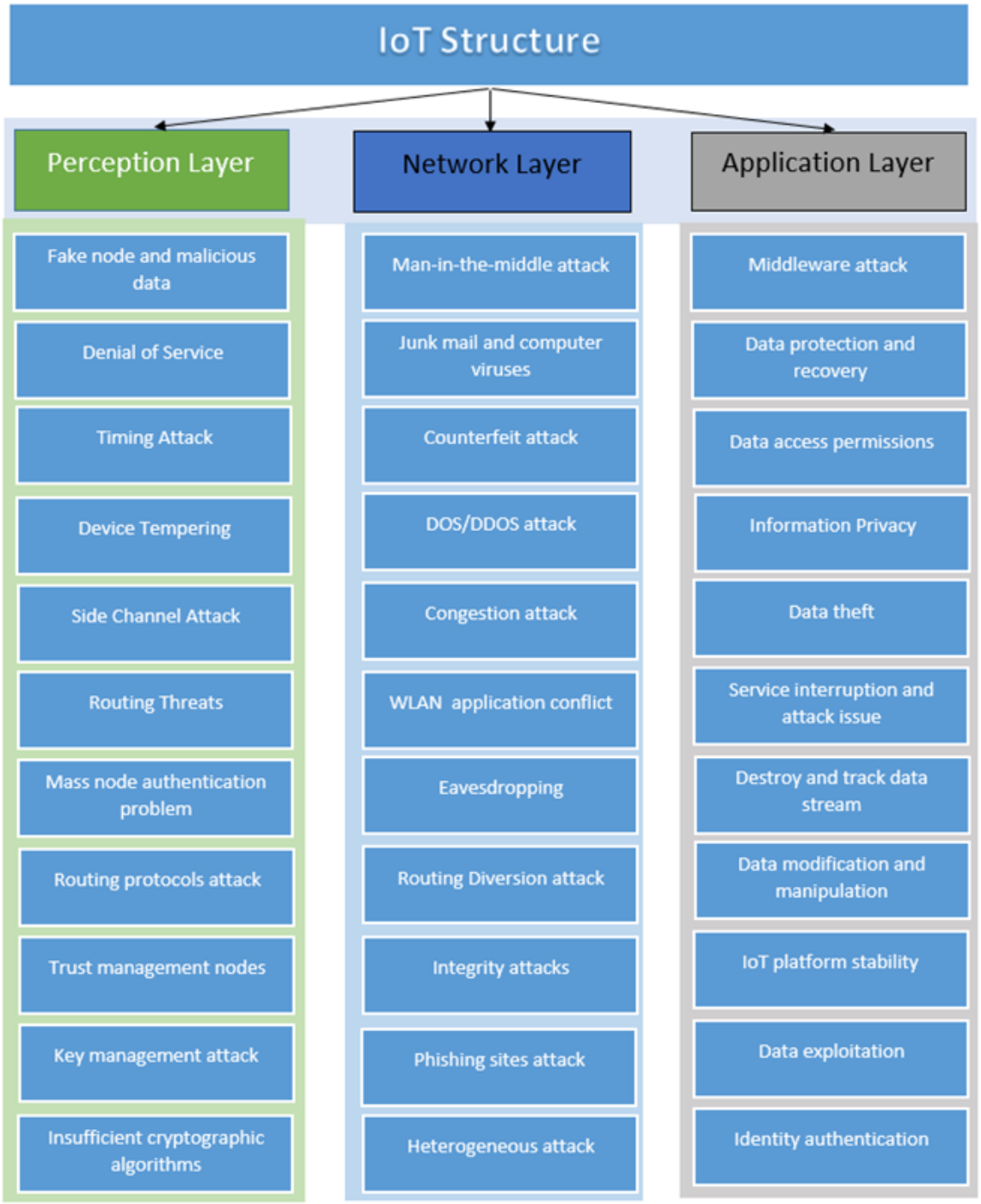


Figure 4.1. *IoT structure that addresses main security and privacy issues*

The core SLR research results of IoT security and privacy challenges in healthcare could be categorized into three groups: perception, network, and application. The following subsections go over each of these categories.

Perception Layer

The perception layer is a sensing layer that joins perception hardware and data collection (Aarika et al., 2020). The IoT system is used for this layer's object/human recognition and sense experiences. IoT is an arrangement of several networks. It has convergence problems, which affect various security threats frequently (Nasiri et al., 2019). The perception layer's security concerns include physical devices and data collection.

Therefore, hardware limitations compromise the security and privacy of this layer (Obogo, 2018). Most IoT sensors have little external security or protection, so advanced security and public encryption methods or frequency hopping interaction cannot be addressed. Some systems also accept short passwords, compromising device confidence management (Mahanty et al., 2018). Those weaknesses' memory, computational, and energy limitations make them vulnerable to physical interference and jamming activities (Li et al., 2020).

Furthermore, certain other limitations, such as various IoT devices, make it burdensome to incorporate a single and unified safety design (Alkhatib et al., 2018). For example, this layer has two RFID vulnerabilities: consistent coding and conflict interference (Alraja et al., 2021). The medical IoT security and privacy threats in Table 4.1 could be concluded that the integrity, authenticity, and confidentiality protections on IoT devices must be preserved.

However, in the case of IoT healthcare applications, probably the most critical tasks to protecting IoT devices resistant to physical/device tampering in healthcare applications, as it is one of the most common attacks in this layer (Selvaraj & Sundaravaradhan, 2020). Since many devices may be placed with no or minimum security or involvement in the patient's environment, they still are subject to severe attacks. Intruders will search the collection devices to exploit and steal patient data through this type of attack. Node authentication is the first critical step in identifying malicious nodes due to physical attacks on the IoT of healthcare systems to keep their safety. Physical or device exploitation in healthcare can be significant because many devices in healthcare have been designed and developed to record, store, and protect individuals' health records (Devibala, 2019).

In addition, data encryption requires protected distribution. LWC algorithms are suitable in cryptography. Because the resources of the IoT devices (battery power, memory, and CPU) are not drained rapidly when utilizing these algorithms.

Table 4.1 *Security and Privacy Challenges of IoT Perception Layer*

Issues	Explanation/Example
Denial of Service	This attack disables the entire system and restricts authorised individuals from having access. It can be accomplished by flooding the system with so many requests at one time, thereby flooding the network and stopping it from transmitting the standard service (Abdullah et al., 2019). According to Alsubaei et al. (2017), 162 attacks targeted healthcare businesses, affecting 900 clinics, hospitals, and organisations. Furthermore, these assaults involved almost 24 million patient records, a 670 percent rise from the previous year.
Distributed Denial of Service (DDoS) Attack	One type of attack is carried out on a huge scale. Utilizing many IoT nodes to send traffic to the target is the most challenging issue (Sharma et al., 2018). For example, there are suspicions that many IoT nodes were used in the DDoS attack known as "Mirai" that occurred in October 2016 (Alagar et al., 2018).
Timing attack	In a side-channel attack, the attacker attempts to breach the system by analysing its time to perform cryptographic algorithms (Bajrić, 2020).
Routing threats	Although it might also happen at the perception layer during the data transmission process, this is the most common IoT attack. An attacker can establish a routing loop, which causes the routing path to be shorted or extended, increasing the side delay and error messages (Alsubaei et al., 2017).
Side channel attack	Targets encryption devices by exploiting hardware information such as power dissipation, power consumption, execution time, and interference caused by equipment during the encryption on the chips where the system is implemented. This data could be analysed to find the secret keys utilised throughout the encryption procedure (Amaraweera & Halgamuge 2019).
Insufficient cryptographic algorithms	A widespread threat in devices that use encryption is incomplete cryptography or insecure cryptography usage. Because of insufficient cryptographic algorithms or weaknesses in the encryption process, an attacker can rebuild the encrypted code or sensitive data to its original (Mahanty et al., 2018).
Replay Attack	Without having the right to do so, data is saved and re-transmitted subsequently. These types of attacks are widespread against IoT authentication protocols (Yeole & Kalbande 2021).
Routing Protocols Attack	Cyber attackers conduct IP source route exploits to determine the route signals taken through a system. For example, the attacker can send an IP packet and utilize the patient's network responses to obtain information from the target device's or network device's operating system (Saba et al., 2020).
Node Capture	Nodes are easier to control for hackers (base node or gateway). Taking down a node allows an attacker to access encrypted keys and protocol information and duplicate and spread malicious nodes throughout the network, compromising IoT security (Yeole & Kalbande, 2021).
Key management	The administration or maintenance of data encryption for a cryptographic protocol is key management. It includes creating, security, maintenance, transfer, modification, and utilization of the keys consideration (Taiwo & Ezugwu, 2020). In addition, it allows selective limitation for specific keys with another sort of security technology integrated into massive cryptographic protocols.
Fake node and malicious data	The attacker could use fake nodes to create fake identities. The overall structure could produce incorrect data, or nodes periodically could get junk data and lose individual privacy (Singh & Chatterjee, 2019). The false nodes would send data to "authentic" nodes, enabling individuals to use up the capacity and bring the entire service down.
Denial of Sleep Attack	One of the fundamental challenges in the IoT is detecting the diverse nodes; each mainly provides factors like moisture, temperature, pulsation, and other variables at a selected time (Mahanty et al., 2018). Before resting for another interval of time to enable the nodes to perform for a lot longer. This attack addresses the node's electricity supply to increase energy usage and shorten the node's operation life by preventing the node from sleeping after transmitting the necessary sensor information (Ren et al., 2017).

Network Layer

The flexibility and expandability of the IoT network is a challenging task for providing sufficient security and privacy in this layer (Ren et al., 2017). IoT devices often employ various sources and therefore own network protocols for data transmission (Alsubaei et al., 2017). Consequently, it is challenging to determine or include a single security protocol that fits all network types (wired and wireless), and even the conventional security model has found such faults.

The security requirements for various networks should be established and addressed in all the media, including 4G access networks, Ad hoc, and Wi-Fi networks, among many other network systems (Chacko & Hayajneh, 2018). Note that the security and privacy vulnerabilities in this layer (network) may be identical to the conventional network security challenges. This layer is exposed to Trojan horses, viruses, spam, packet spoofing, route falsification, and flooding attacks causing disclosure of information (Shrivastava & Namdev, 2020). Since the use of various wireless networks in IoT is widespread, data is transmitted wireless, making wireless communication more open to eavesdropping.

Attackers can manipulate medical data and disable their alarms connected with healthcare systems or even interfere with the WSN, so sensors can send false information, which means physicians might make wrong decisions. Hackers may also submit spam and launch Service Denial (DoS) attacks or hijack network source points. DoS in IoT can be disastrous, as malicious IoT nodes can enable secure resources to make valid IoT nodes in the network inaccessible. However, whether malicious IoT nodes interrupt the configuration data, a harmful DoS attack causes network topology to be insecure (Nausheen & Begum, 2018). Some of the security and privacy issues of medical IoT in the network layer are presented and defined in Table 4.2.

The use of a combination of security and privacy protocols and mechanisms is an efficient and systematic approach for protecting the network against those threats due to the heterogeneity of the entire network. This enables the data to be encrypted and manipulated by attackers to ensure authenticity, confidentiality, integrity, and availability.

Table 4.2 *Security and Privacy Issues of IoT Network Layer*

Issues	Explanation/Example
Denial of Service (DoS) attack	This attack happens at the IoT network layer when a fake node blocks electromagnetic signals, disrupting data transmission or routing between nodes (Fazeldehkordi et al., 2019).
Man-in-the-Middle (MITM)	This attack combines with the Secure Socket Layer (SSL) attack, allowing hackers to monitor communication, capture it, and impersonate both endpoints of the communication (Shrivastava & Namdev, 2020).
Congestion attack	This attack succeeds by flooding networks with unprocessed responses until their period runs out. Then, the lane is restricted to transactions whenever the highest number of unsolved requests (HTLCs) is achieved (Ianculescu et al., 2020).
Eavesdropping sniffing	This attack enables the offender to monitor personal conversations across the data transmission (Alsubaei et al., 2017). The attacker could get valuable information like identities and node registration, contributing to other forms of issues (Cilliers, 2020).
Black Hole	The attacker creates a fake node that accepts network traffic by claiming to have the quickest route. Network traffic could be forwarded to the fake node, which is used as a proxy server or ignored (Saba et al., 2020).
Gray Hole	This attack is similar to a black hole attack; instead of destroying all signals, it just removes a selection of those (Karunarathne et al., 2021).
Worm Hole	By managing at least two network nodes or adding additional false nodes to the network, the attacker establishes a link between different parts of the network. The hacker gathers data from one point and replays it to the other after confirming the link (Cilliers, 2020).
Hello Flood	By sending a "Hello" connection request by a fake node, the attacker utilizes the strength of nodes in the system. Fooling all nodes in the system in a similar range, leading each to transmit information to its neighbours, led to massive network activity (Sadek et al., 2019). "Hello" signals are defined in various routing protocols, allowing nodes to communicate with their neighbours (Sadek et al., 2019).
Phishing sites attack	Social engineering techniques which are frequently employed to gather personal data from users, such as login details and banking information (Alkhatib et al., 2018).
Junk mail and computer virus	Some viruses steal contact details from an email application's address book and use them to deliver infected files from the device to all those contacts (Amaraweera & Halgamuge, 2019).
Forgery attack	An exploit leads an Internet browser to perform an inappropriate consumer application activity. A successful cyberattack can be catastrophic for both the patient and the healthcare organisation (Alsubaei et al., 2017).

According to (Chacko & Hayajneh, 2018), DoS attacks can be a crucial problem for multi-domain infrastructure and, therefore, for IoT medical applications. DOS attacks can jeopardise IoT servers and lead to the retrieval or destruction of many saved security contexts in a restricted domain. This attack could disrupt the health care system because it could damage critical health services and put patients' lives at risk. Several scholars have suggested solutions to this issue, such as IoT decentralised architecture and firewalls to filter DoS attacks. However, it is challenging to detect and prevent all DoS attacks by detecting any potential DoS attacks, but not enough research is underway in this direction. More searching for this form of attack is therefore required. Besides attack detection, good authentication and filtering mechanisms are also essential to guarantee the protection of IoT data.

Application Layer

The high number of IoT applications and their diversity and complexity could be considered the main cause of the security issues of the IoT caused by system integration (Selvaraj & Sundaravaradhan, 2020). Therefore, the system providing an interface between users and IoT devices can relate to several security challenges in this layer. IoT device limitations and difficulties deploying potential issue solutions are two common reasons behind application layer security problems (Nausheen, & Begum, 2018).

The weak network protocols of the IoT operating system generate a limited safety module that cannot provide complete application layer protection (Abdullah et al., 2019). Dynamic security patch installation for IoT devices is challenging. Because manually updating programs on many remote IoT devices might be challenging. In addition, IoT devices are resource-restricted such as storage, memory, CPU, and battery capacity, and the potential for installing updates is restricted (Devibala, 2019). Table 4.3 presents a variety of security issues in the application layer.

Due to the enormous amount of IoT applications that use various interfaces and data sharing models, numerous security problems remain in the topic presented in this paper (Yeole & Kalbande, 2021). Certain aspects such as data protection, authentication, and data breaches.

Table 4.3 *Security and Privacy Issues of IoT Application Layer*

Issues	Explanation/Example
Authentication, Data Accessibility	Unauthorized users could have a huge impact on the system's availability (Karunarathne et al., 2021). Because there are so many users, multiple permissions and security systems are required.
Data privacy and identity	IoT interconnect devices from various manufacturers demand the use of several authentications. Integrating multiple techniques to protect data privacy and identity is challenging **(**Shrivastava & Namdev., 2019).
Dealing with the Availability of Big data	The IoT interconnects many devices, resulting in a huge amount of data. This adds overhead to the application's data analysis, and significantly influences the application's service(s) accessibility **(**Ianculescu et al., 2020*).*
Information privacy	Authentication, identity, and device heterogeneity are the security and privacy challenges in IoT in healthcare. In addition, scalability, integration, ethical system designs, financial strategies, and monitoring are significant problems (Sadek et al., 2019).
Data protection recovery	The process of stopping important data from being exploited, damaged, or misplaced is known as data protection. The method of restoring data that has been lost, destroyed, corrupted, or otherwise become inaccessible is known as data recovery.

More importantly, it is recommended to explicitly identify and use the medical data access policy to accept the user's identity with the authorization to enter IoT in this layer of healthcare services, verification, and access monitoring (Alsubaei et al., 2017). In addition, healthcare works with sensitive patient information, and specific data protection measures should be developed for its datasets. An additional layer of safety with encryption algorithms is also suggested for patient data protection.

4.3 Systematic Literature Review Findings for RQ2

According to a literature search, there are three types of LWC algorithms: Substitution-Permutation Networks (SPN), Feistel Networks, and other variants. Comparing Feistel to SPN architectures, the round operation of SPN must be invertible, whereas, for Feistel, this is not required. Compared to the Feistel network, SPN offers a relatively higher level of security. In contrast, SPN uses up more resources. The encryption and decryption processes in a Feistel structure are typically similar and even comparable.

An evaluation of the different LWC algorithms utilising various characteristics is presented in Table 4.4.

Table 4.4 *Comparison of several LWC algorithms*

Name	**Block size (bit)**	**Key size (bit)**	**Number of rounds**	**Structure**	**Implementation environment**	**References**
AES	128	128, 192, 256	10, 12, 14	SPN	Hardware and software	Daeman & Rijmen, 1998
PRESENT	64	80, 128	31	SPN	Hardware	Bogdanov et al., 2007
MSEA	128	256	96	Feistel	Hardware and software	Kumar et al., 2014
LEA	128	128/192/256	24/28/32	GFN	Hardware and software	Jap & Breier, 2015
XTEA	64	128	64	Feistel	Software	Moon et al., 2002
SIMON	32 48 64	64 72/96 96/128	32 42/44	Feistel	Hardware	Ray et al., 2015
PRINCE	64	128	12	SPN	Hardware	Borghoff et al., 2012
RECTANGLE	64	80, 128	25	SPN	Hardware and software	Zang et al., 2015

When looking through the literature, performance comparison papers are typically divided into 3 categories: software, hardware, and software/hardware. In this section, the researcher examines similar works in the field of software and hardware.

The LWC algorithm is named NUCLEAR for use in 6LoW-PAN networks. Researchers chose the ARM 7 LPC2129 platform to examine the software metrics and evaluated the findings of nine LWC algorithms in the areas of memory, energy usage, throughput, and encryption/decryption execution time (Salunke et al., 2019). The Atmega128 microcontroller was examined to SPECK, SIMON, KLEIN, Piccolo, and TWINE LWC algorithms in characteristics for consumption of power and memory (Hosseinzadeh & Bafghi, 2017).

Singh et al., (2018) investigated the performance of six LWC algorithms for IoT devices. As testbeds, they selected the Beagle Bone Black and Raspberry Pi 3. The researchers assessed the algorithms based on how quickly they ran in the CBC and ECB formats. CBC is a well-known procedure in which every plaintext is XORed with the prior cyphertext even before encryption. The message in ECB is composed of blocks, and each block is separately encrypted.

Due to code size, battery usage, memory usage, and throughput, five LWC algorithms including Twofish, XTEA, Rijndael, RC6, and Serpent were evaluated by employing software on the Strong SA-1100 microprocessor (Großschädl et al., 2007). Over an Atmel Atmega128RFA1 microprocessor, XTEA and AES were evaluated according to a couple of payloads and parameters for power usage, execution time, and throughput (Botta et al., 2007). Based on characteristics such as Flash, RAM, throughput, and energy usage, Beaulieu et al., (2014) evaluated the performance of SPECK and SIMON algorithms in the AVR 8-bit Atmel Atmega128 microcontroller for the encryption operation.

LBlock, SIMON, PRESENT, SPECK, RECTANGLE, PRIDE, and PRINCE algorithms were tested on the Raspberry Pi 2 and Arduino UNO in characteristics of RAM/ROM usages, the execution time for encryption, and decryption (Tasnime et al., 2018).

The researchers examined the energy consumption, throughput, execution time, and RAM/ROM factors for the encryption of the three LWC algorithms: CLEFIA, PICCOLO, and TWINE. The studies were conducted on an STM32F401RE device, and the algorithms were tested with inputs of 512, 1024, 2048, and 3072 bytes of plain text (Ertaul, 2017).

Table 4.5 gives a detailed review of previous related publications for performance evaluation of LWC algorithms.

Table 4.5 *The Comparison of Previous Related Studies on Performance Evaluation*

Algorithms	***Evaluated factors***	***Platform***	***Comparison method***	***Mode***	***Reference***
RC6, Rijndael, Serpent, Twofish, XTEA	Code size, power consumption, throughput, memory (RAM and ROM) footprint	Strong ARM SA-1100	Block lengths of algorithms	Encryption and Decryption	Johann et al., 2007
XTEA, AES	Throughput, Energy usage, and execution time	Atmel ATmega128RFA1	Payloads - 1, 15, 16, 31, 32, 47, 48, 63, 64, 79, 80, 95, 96, 104 bytes	Encryption, Decryption	Botta et al., 2013
AES, XTEA, SEA, CLEFIA, DESXL, PRESENT, HIGHT, Noekeon, KATAN, Piccolo, KLEIN, TWINE, IDEA, Skipjack, KANTAN, LBlock, LED, MIBS, TEA	Cycle count, RAM/ROM usage	MSP430	Block length	Encryption, Decryption	Mickael et al., 2013
AES, PRESENT KATAN, TEA, SIMON, SPECK, PRESENT, SEA	RAM, Cycles, throughput, Energy	8-bit microcontroller	Block lengths of algorithms	Encryption	Michael et al., 2016
AES, PRESENT	Power usage, memory usage, time, throughput	Snapdragon 400 and Qualcomm MSM8926	Block length	Encryption, Decryption	Lara et al., 2016
SIMON, SPECK, AES, PRESENT	RAM usage, Code size, execution time	16-bit MSP and 8-bit AVR	Block length	Encryption, decryption	Kotel et al., 2016
AES, SPECK, SIMON, LED, PRESENT, TWINE	Throughput, TP/A, cycles/block, cycles/bytes	Xilinx Kintex-7 FPGA	Each algorithm	Software versus hardware	William et al., 2017
AES, TDES, DES, Twofish, RC2, Blowfish	Execution time in CBC and EBC modes	Raspberry Pi 3, Beagle Bone Black	Files in MB (1, 2, 4, 8, 16, 32, 64, 128 MB)	Encryption	Singh et al., 2018
AES,Camelia, IDEA, KASUMI, GOST, HIGHT, PRESENT, CLEFIA, DES, HB, Piccolo, Robin, TEA, XTEA, SEA, mCrypton, MIBS, TWINE, LBlock, LED, Klein, KATAN, KTANTAN, ITUbee, SIMON, SPECK, LEA, PRINT, PRINCE, PRIDE, Zorro	Energy usage, RAM/ROM, latency, throughput	8-bit, 16-bit, 32-bit micro controllers	Key size and block size	Software comparison versus hardware	George et al., 2018
PRESENT, SIMON, SPECK, RECTANGLE, PRINCE, Pride, LBlock	Execution time, RAM/ROM, Clock cycle	Arduino UNO and Raspberry Pi 2	Block length	Encryption, decryption	Tasnime et al., 2018
PRESENT, AES, HIGHT, Klein	Memory consumption and throughput	2019Arduino Uno, MATLB	Each algorithm	Software	Ankir & Margi, 2019
BRIGHT, RoadRunneR, SPECK, HIGHT, SPARX	Memory consumption, execution time, throughput	Intel Core i5-2430 M	Block ciphers	Encryption and decryption	Deepti &Nasib, 2019
AES, CLEFIA, SIMON, SPECK, PRESENT	Execution time, energy efficiency, power consumption	ODROID-XU3	64 MB plain text	Encryption	Lee et al., 2020

Based on the impact and opportunities of the LWC algorithms, NIST started the procedure in 2015 to standardize LWC algorithms that meet the specifications of resource-limited devices (McKay et al., 2016). To meet resource constraints, the following performance factors could be assumed when choosing an appropriate LWC algorithm in the IoT medical sector.

The key size is an important performance factor, because medical IoT devices, such as node sensors, have very little storage (Uslu et al., 2020). It is recommended to use the LWC algorithm that has a shorter key size and gives the same degree of protection. The performance of memory and power usage is more optimal due to the tiny key size (64, 96, or 128) (Hajar et al., 2021).

Another essential element for the LWC algorithm is the block size. Processing times can be decreased while power consumption falls with smaller block sizes. Additionally, medical sensors usually send short messages that contain essential clinical data; thus the smaller block size is more productive. RECTANGLE, an LWC algorithm based on SPN, is presented in Zhang et al. (2015), to accomplish fast implementation, that uses a bit-slice mechanism with a 64-bit block.

LWC algorithms generally implement basic logic and mathematical calculations to adhere to resource limitations. The round number is raised as the outcome of performing simple procedures. As a result, when choosing an LWC algorithm for the IoT, the number of rounds is one of the important elements. PRINCE lightweight algorithm intends to accomplish encryption in one clock cycle by requiring a small round number, that requires rapid completion (Borghoff et al., 2012).

Energy consumption is the characteristic that defines the chance of implementing IoT devices in healthcare. This is the amount of battery power required during encryption or decryption. When creating real-time IoT-based healthcare monitoring, the main driving factor considered is improving energy efficiency (Ghosh et al., 2020). IoT in healthcare consists of active objects that are powered by batteries and are made to detect and respond to environmental changes (Uslu et al., 2020). For instance, the battery-operated Wireless Body Sensor Nodes (WBSNs) are generally energy-constrained, it is necessary to create energy-efficient data security mechanisms, such as LWC algorithms (Zang et al., 2018). Therefore, these algorithms should be simple and have low energy consumption. The lower the power consumption, the better for the algorithm. This metric is vital, especially for devices that gain power and energy from their surroundings, using a battery and storing a specific amount of energy. Also, many cases find it difficult to recharge or replace the batteries in the healthcare environment.

Because power consumption is affected by computational power due to processing time, the amount of calculations that define throughput becomes an indicator of lightness. The block length and secret key size are smaller than for conventional cryptography to support implementation, it is still essential to properly implement a reliable algorithm.

The IoT devices in healthcare must have a minimal demand for RAM, which the device needs to function to execute its operation, and ROM, which is where the procedure is recorded on the device. They help the real-time medical monitoring procedures properly. The main objective of LWC is to provide security mechanisms that could perform over resource-limited devices by utilizing less power and computing resources.

The throughput used for the number of plaintexts processed per second is one of the most important factors (bps). In this case, the algorithm prefers higher throughput. For devices that transfer a large amount of data, such as those used for remote patient monitoring, high throughput is required. The ability to perform parallel computing has a massive effect on throughput.

4.4 *Experimental Performance Testing Findings for RQ3*

This section provides the outcomes of performance testing on selected LWC algorithms. The Performance Testing results from the individual LWC algorithms are covered in Section 4.4.1. Subsection 4.4.2 describes the results for the individual performance experimental outcomes, and Subsection 4.4.3 provides a comprehensive summary of all research results.

4.4.1 Individual Findings

Eight LWC algorithms were tested in this experiment, including AES, PRESENT, SIMON, XTEA, PRINCE, MSEA, LEA, and RECTANGLE, for important elements such as execution time, memory usage (RAM and ROM), energy consumption, and throughput for encryption and decryption procedures. In experiments, the Raspberry Pi 3 is used as the main IoT device.

4.4.1.1 Encryption/Decryption Execution Times

The execution time is the time needed for the LWC algorithm to encrypt or decrypt. This section will include both the encryption and decryption execution times. Each of these will be recorded over the time required to encrypt or decrypt different files.

a. AES

Figure 4.2 illustrates the individual AES encryption testing results for various file sizes. As shown in the graph, the encryption execution times for most file sizes vary greatly; only the 16KB file encryption takes the shortest time.

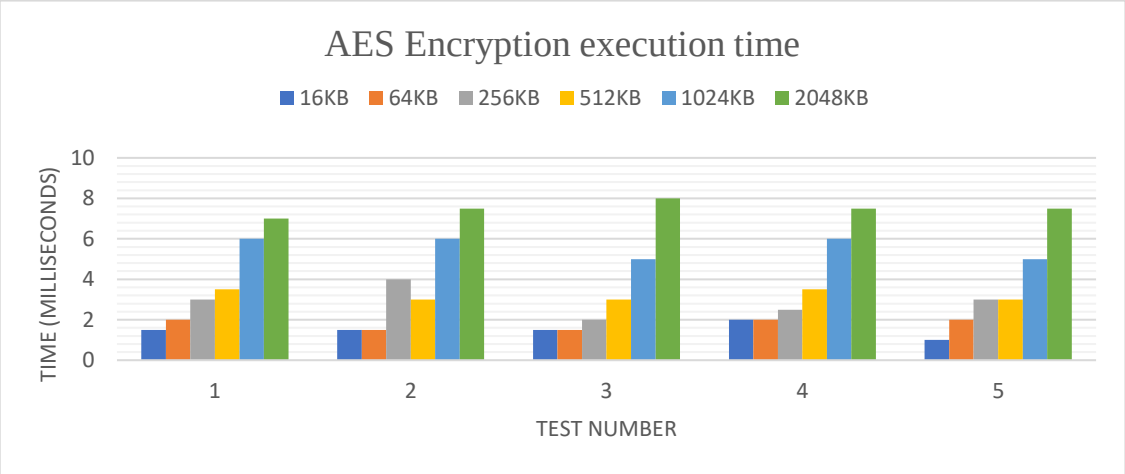


Figure 4.2 AES Encryption execution time

Figure 4.3 illustrates the AES decryption testing outcomes for the various file sizes. The 16KB file had the least amount of difference between encryption and decryption execution times. Overall, AES encryption and decryption appear to perform similarly and have comparable execution times.

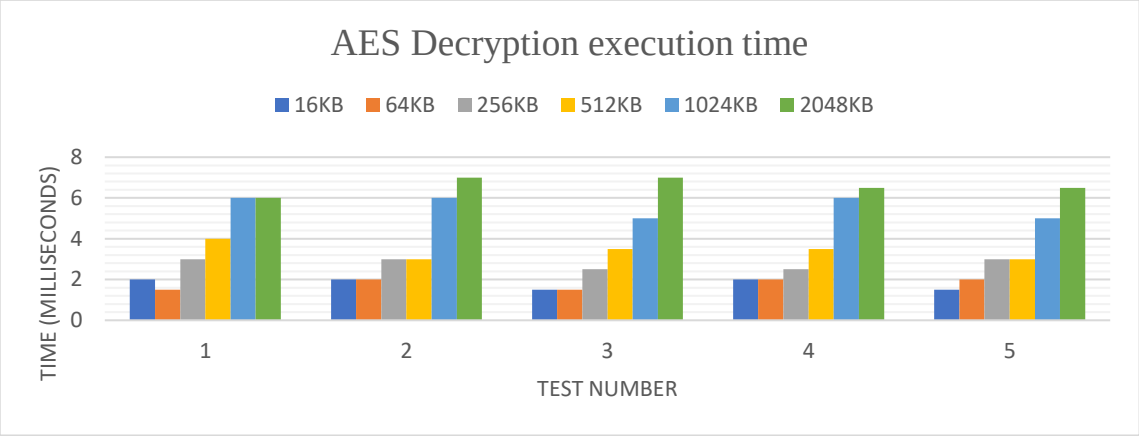


Figure 4.3 AES Decryption execution time

a. PRESENT

Figure 4.4 represents the PRESENT algorithm of individual encryption execution time for various file sizes. The stability of encryption execution times across most experiments is the first thing to notice about these findings. However, this is especially noticeable for a 16KB file because encryption took less than 0.005 seconds.

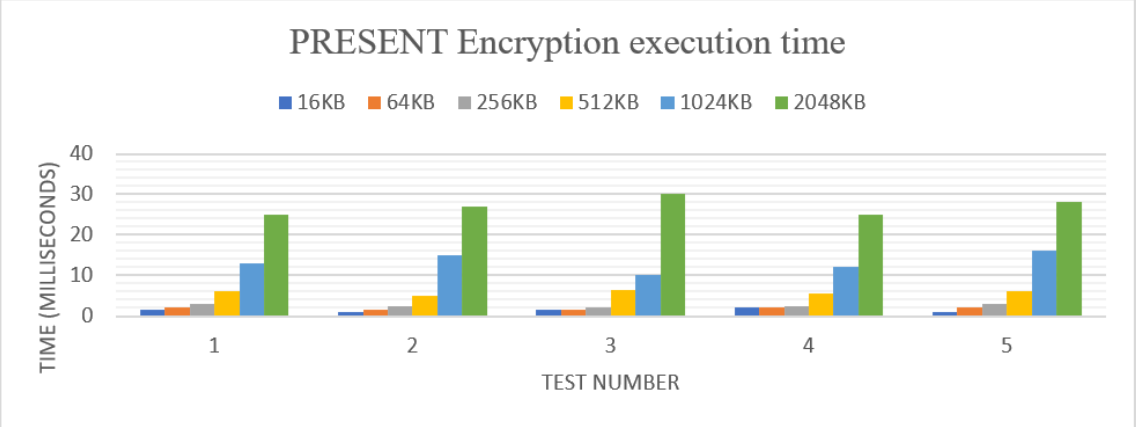


Figure 4.4 PRESENT Encryption execution time

Figure 4.5 represents the PRESENT decryption execution time for various file sizes.

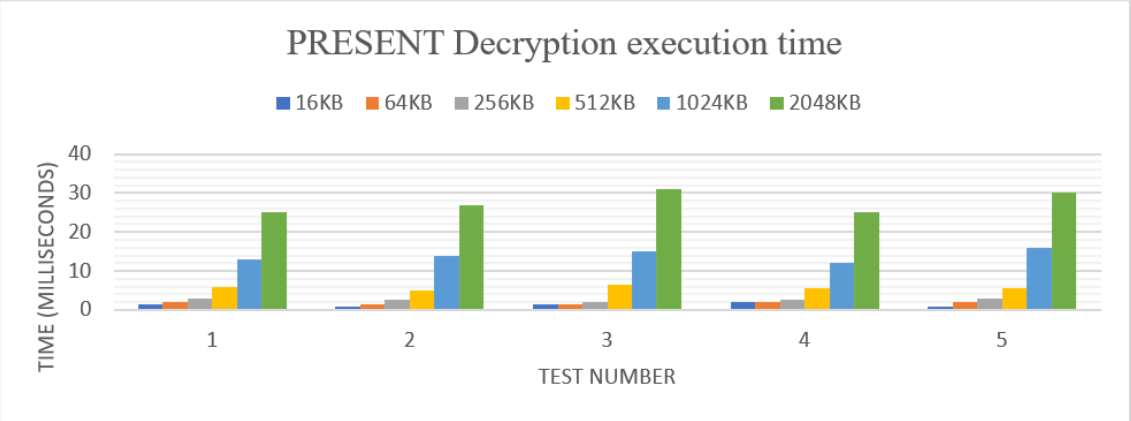


Figure 4.5 PRESENT Decryption execution time

b. MSEA

Figure 4.6 depicts the MSEA encryption execution time for various file sizes. According to the experiments, the main issue with MSEA encryption is that it requires a long encryption time. The only encryption that is feasible is for the 16KB file; all other files took too long to be considered usable.

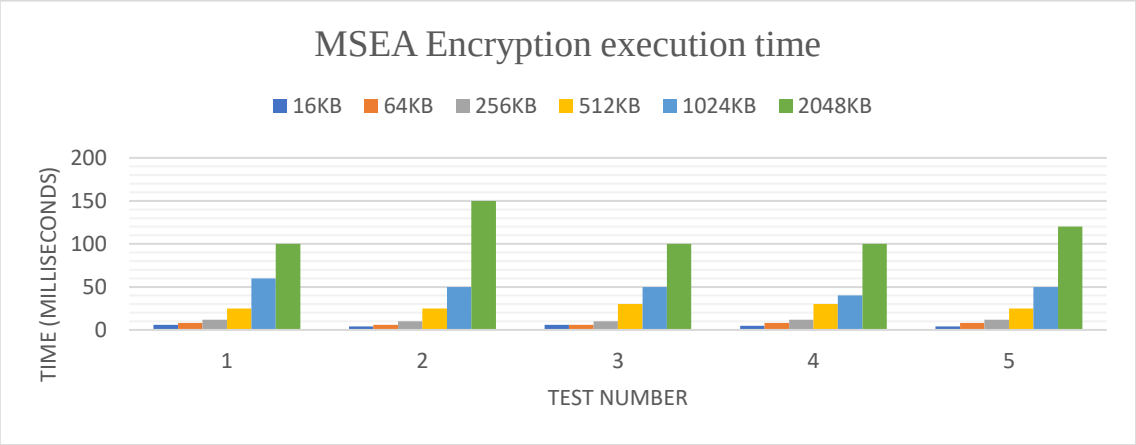


Figure. 4.6 MSEA Encryption execution time

Figure 4.7 illustrates the MSEA decryption execution times for various files. The decryption outcomes are comparable to the encryption findings.

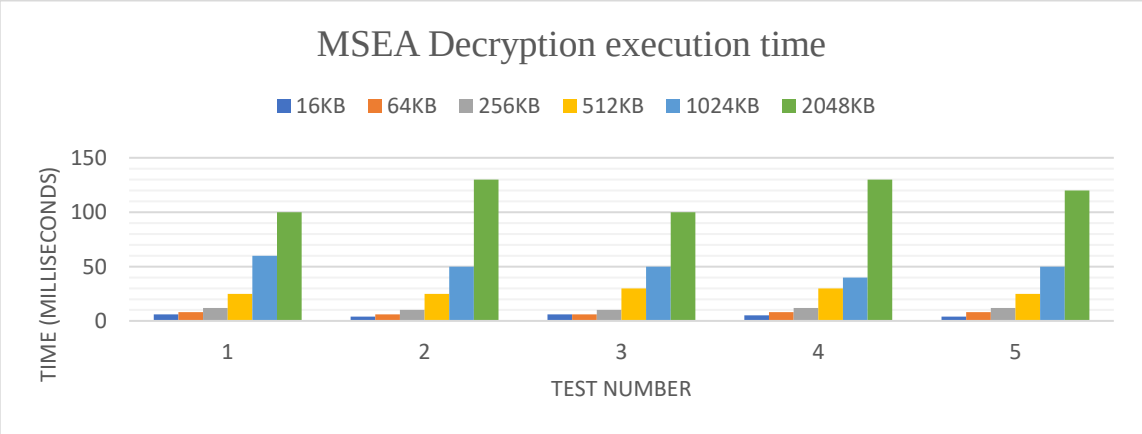


Figure 4.7 MSEA Decryption execution time

c. LEA

The individual outcomes for LEA encryption execution time across file sizes are shown in Figure 4.8. The majority of files' encryption execution times are stable.

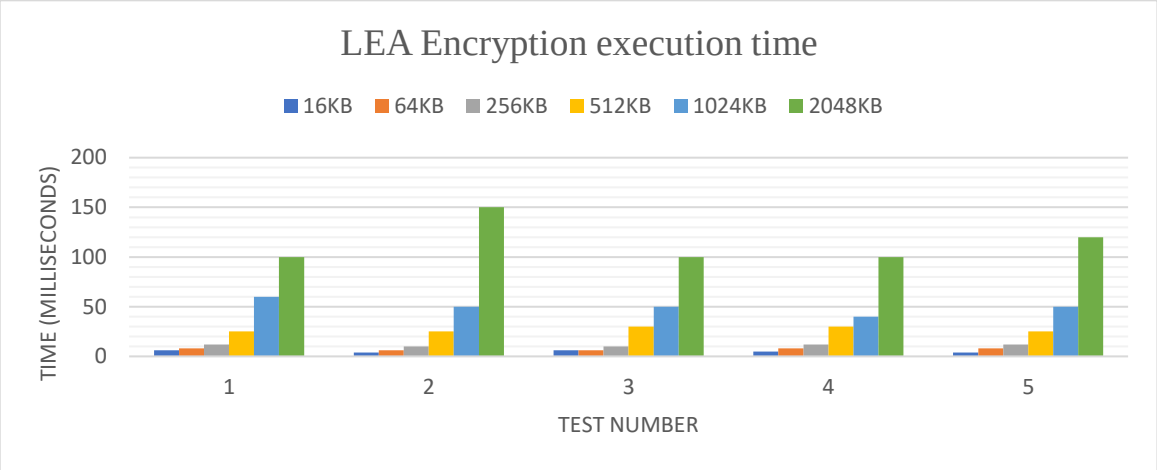


Figure 4.8 LEA Encryption execution time

Figure 4.9 shows the outcomes of individual LEA decryption execution times for several file sizes. Decryption execution times for most findings are stable, as they are for encryption.

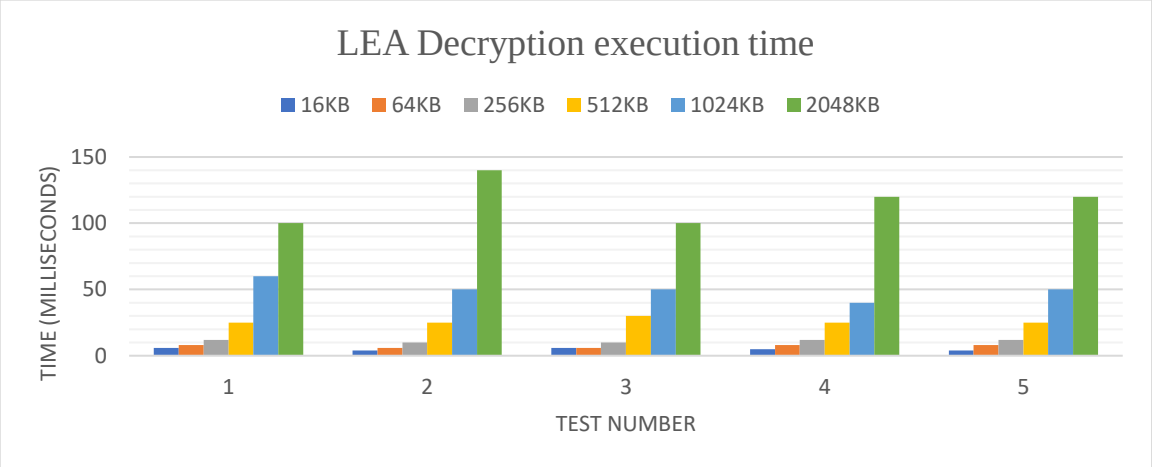


Figure 4.9 LEA Decryption execution time

d. XTEA

The constancy of the encryption timings is the first thing that stands out about these results. The times of XTEA encryption for the various file sizes are shown in Figure 4.10. There are a very small number of rounds with some variation, and they barely slightly alter the results. The encryption time for a 16KB file was less than 0.001 seconds.

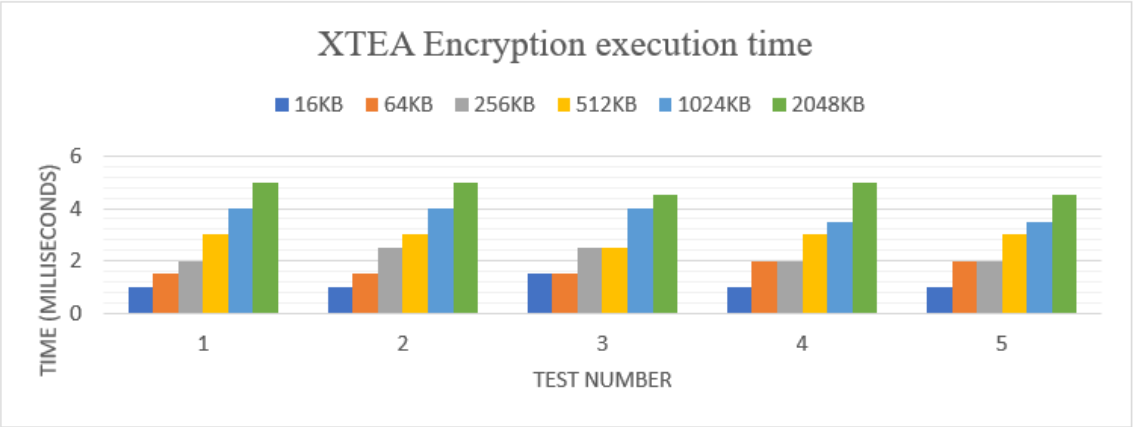


Figure 4.10 XTEA Encryption execution time

Figure 4.11 depicts the XTEA decryption execution time for various file sizes. The decryption time results demonstrate the same inferences as the encryption time results.

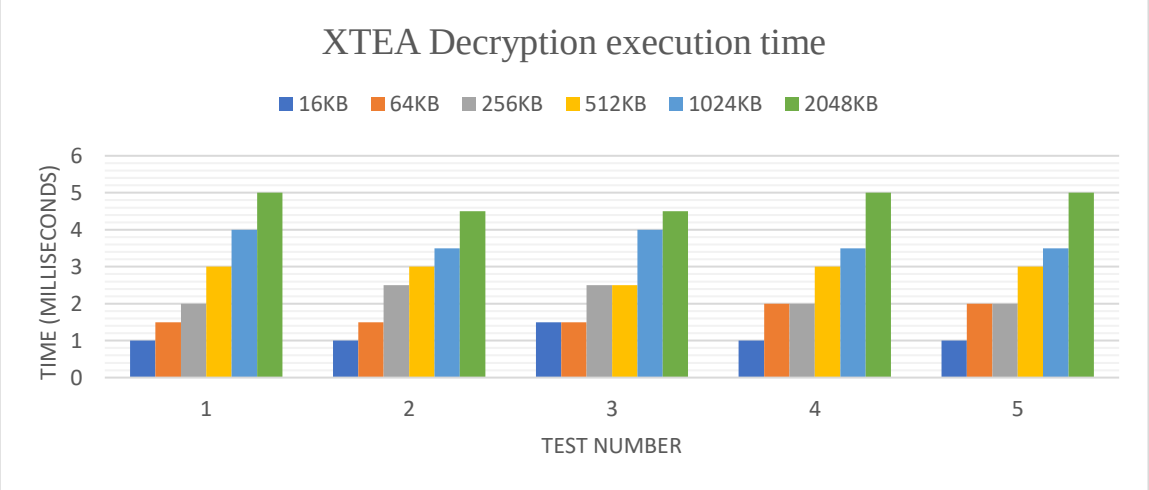


Figure. 4.11 XTEA Decryption execution time

e. SIMON

Figure 4.12 depicts the SIMON encryption execution times for various file sizes. The first thing to notice about these findings is the stability of the encryption times throughout the majority of them. This is less obvious for a 16KB file because encryption took less than 0.001 seconds.

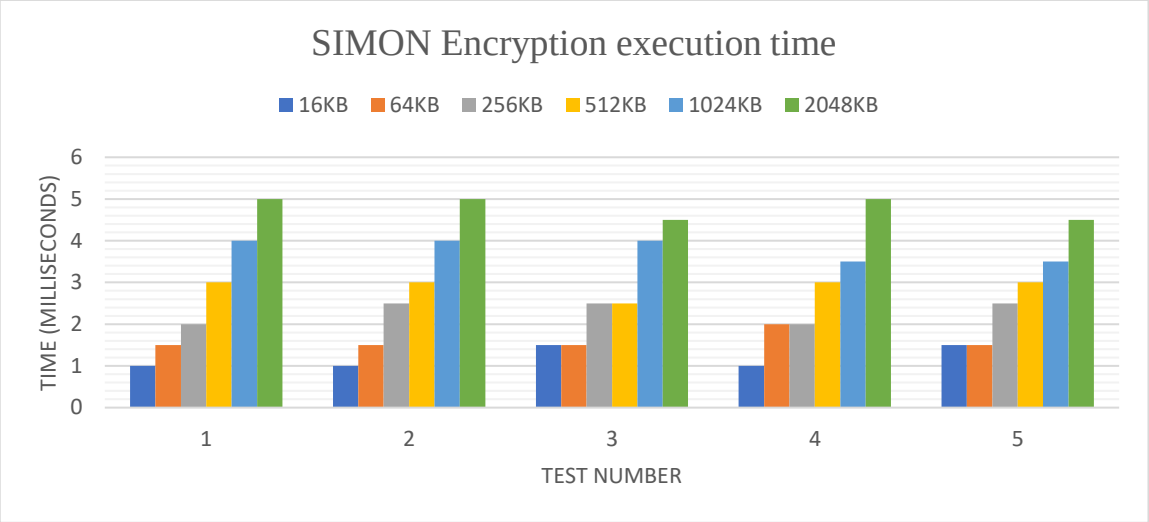


Figure 4.12 SIMON Encryption execution time

Figure 4.13 represents the SIMON decryption outcomes for various file sizes. The decryption time results show the same reflections as the encryption time results.

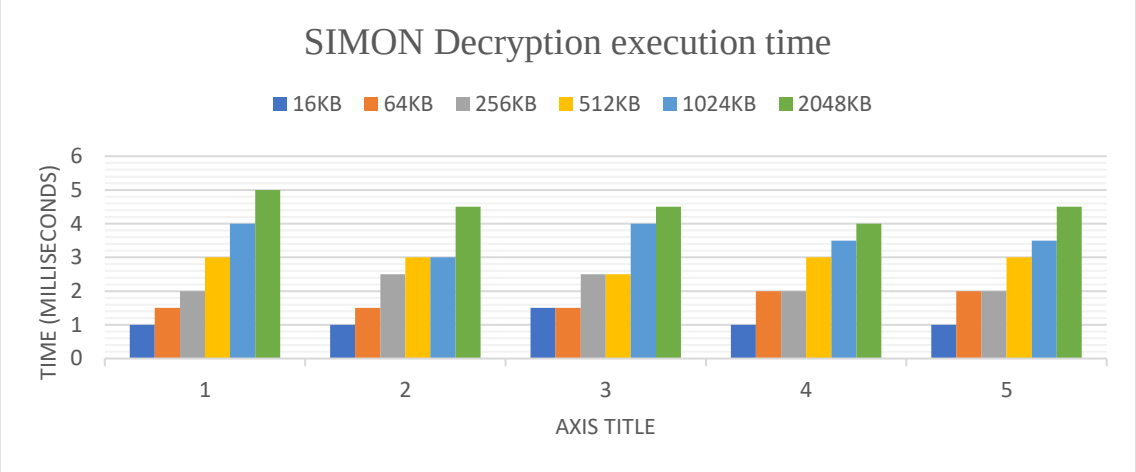


Figure 4.13 SIMON Decryption execution time

f. PRINCE

Figure. 4.14 shows the time the PRINCE encryption execution results for the different file sizes.

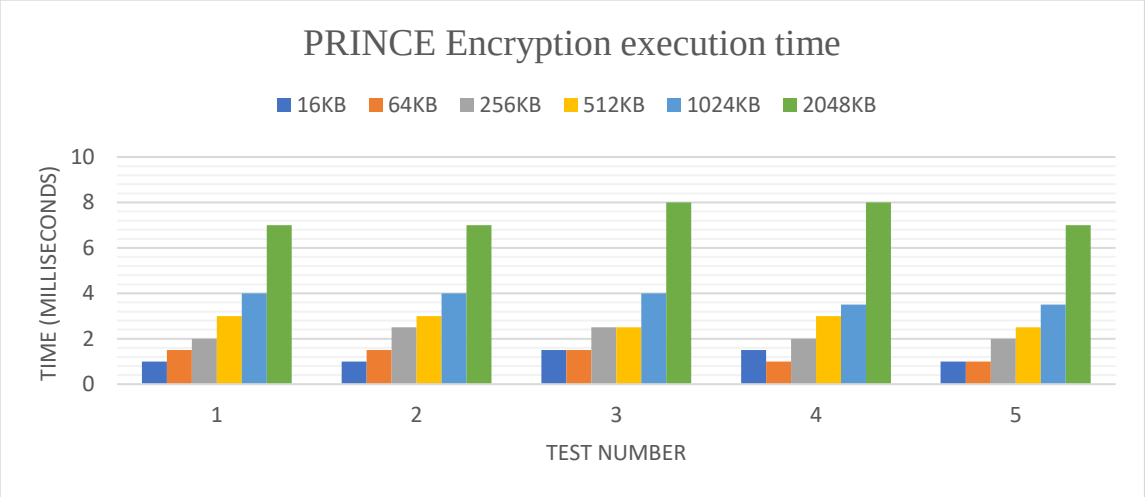


Figure 4.14 PRINCE Encryption execution time

Figure 4.15 represents the PRINCE decryption execution time findings for various file sizes.

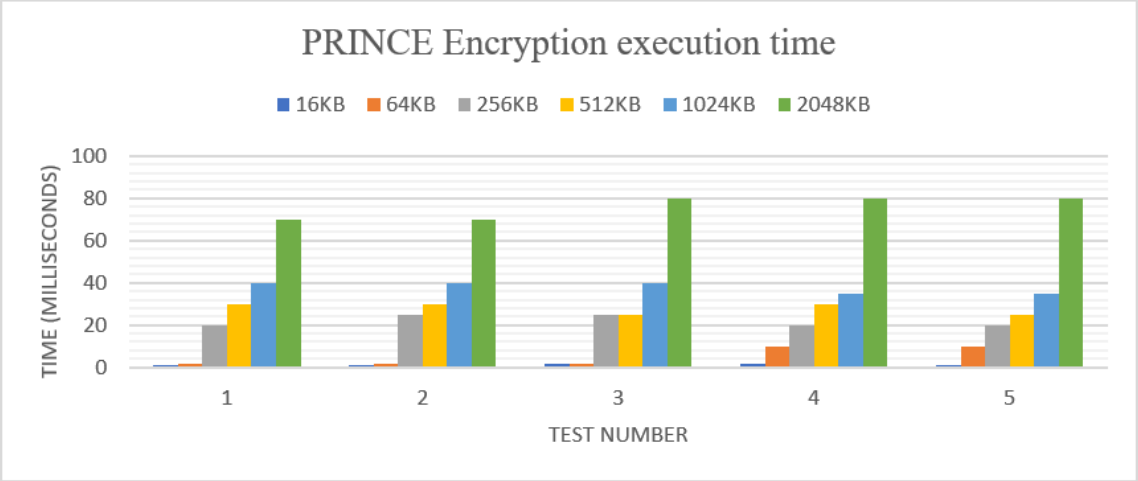


Figure 4.15 PRINCE Decryption execution time

g. RECTANGLE

Figure 4.16 represents the RECTANGLE encryption execution time for various file sizes. A few numbers confirmed some differences, but they are few and only have a minor difference.

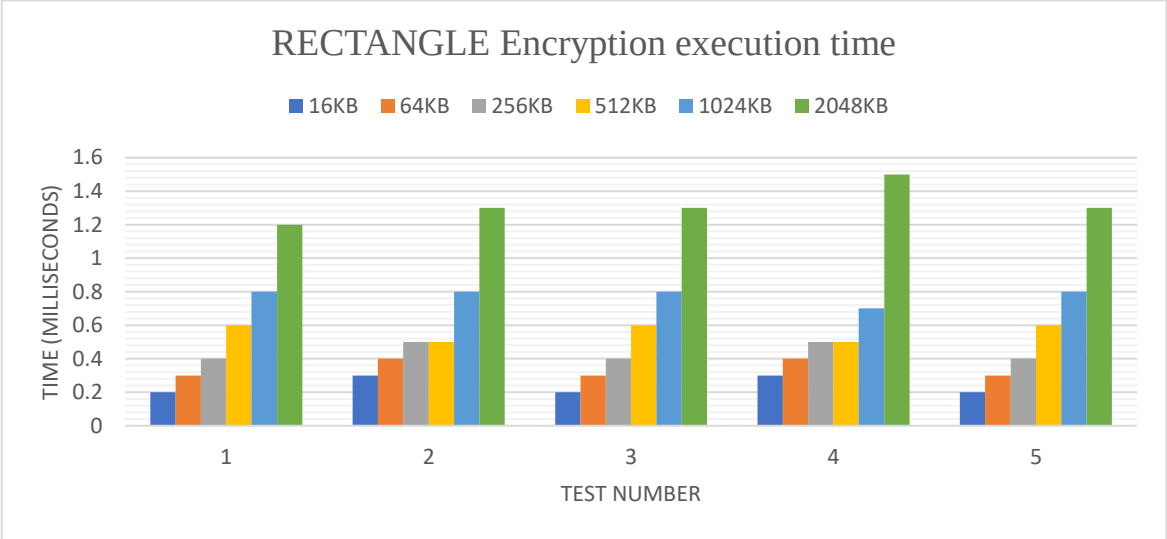


Figure 4.16 RECTANGLE Encryption execution time

Figure 4.17 displays the RECTANGLE decryption execution time outcomes for various file sizes. The decryption time results show the same findings as the encryption time outcomes.

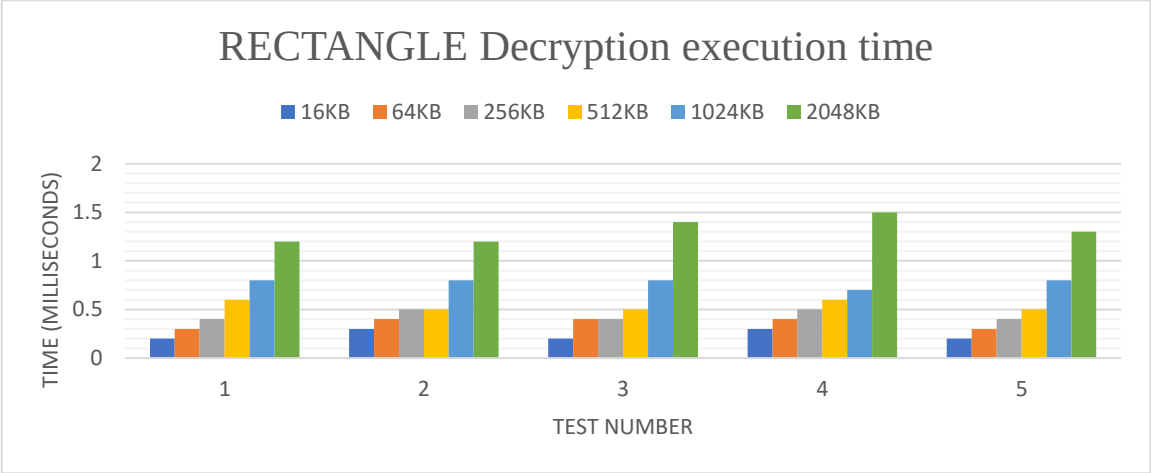


Figure 4.17 RECTANGLE Decryption execution time

4.4.1.2 Power Consumption

The following formulas were used to calculate the volume of power spent by an algorithm:

$$\text{Charge (C)} = \text{Current Stream (A)} * \text{Time (Seconds)}$$

$$\text{Energy (J)} = \text{Charge (C)} * \text{Voltage (V)}$$

a. AES

Figures 4.18 and 4.19 display the power consumption of the AES algorithm utilised to encrypt and decrypt the various size files. The data sets are calculated from the average power consumption of file encryption or decryption.

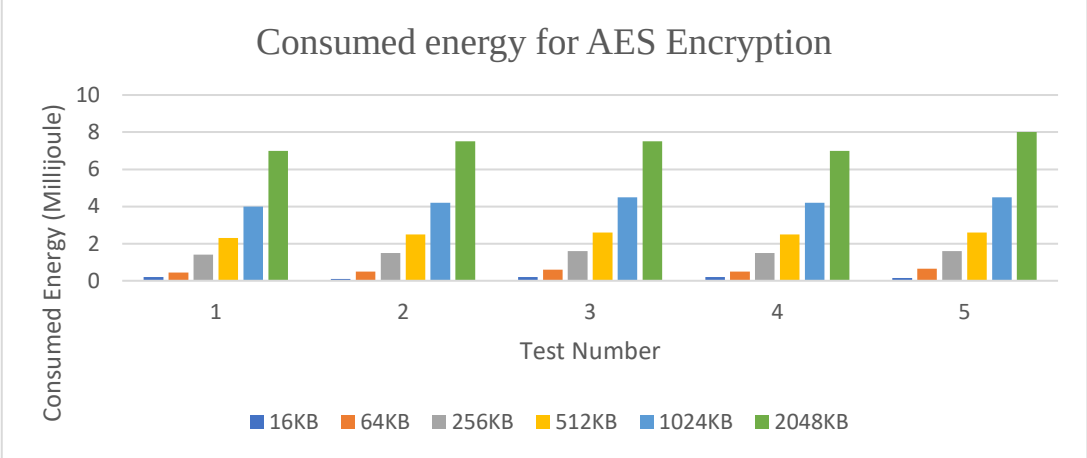


Figure 4.18 Consumed energy for AES Encryption across file sizes

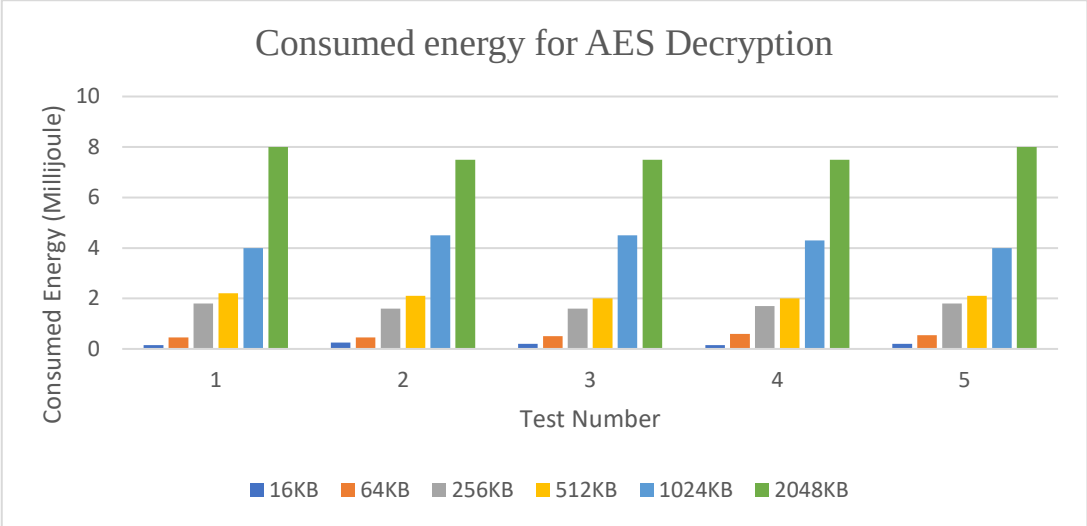


Figure 4.19 Consumed energy for AES Decryption across file sizes

b. PRESENT

Figures 4.20 and 4.21 display the energy utilization performance for PRESENT encryption and decryption. These operations consume more battery charge because the encryption and decryption execution times are longer.

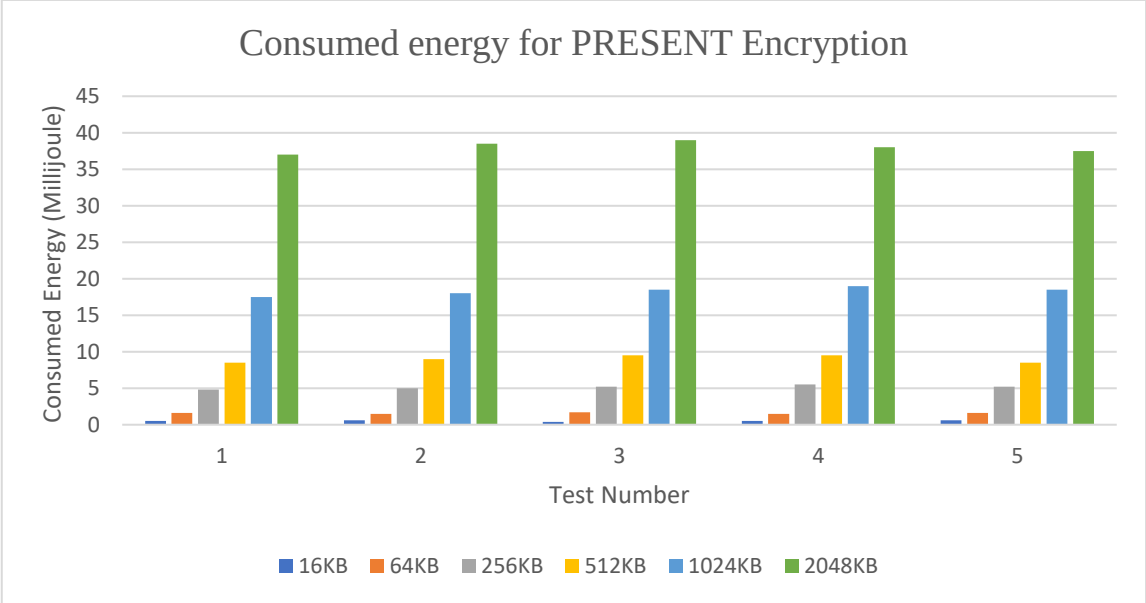


Figure 4.20 Consumed energy for PRESENT Encryption across file sizes

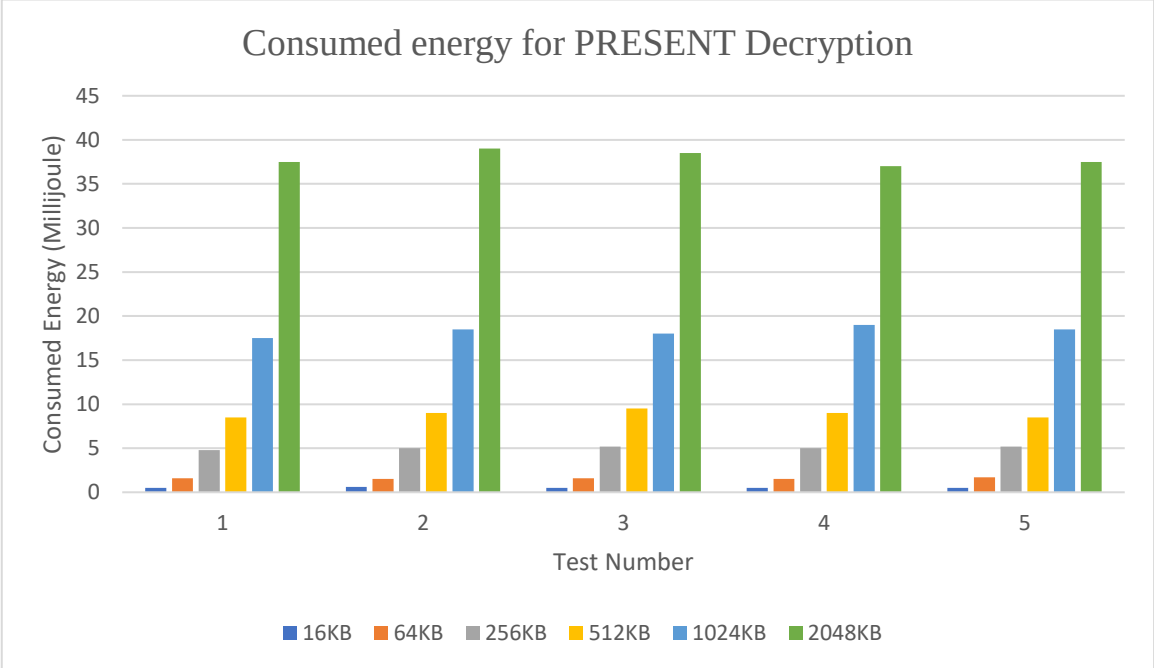


Figure 4.21 Consumed energy for PRESENT Decryption across file sizes

c. MSEA

Figures 4.22 and 4.23 illustrate the power used by MSEA encryption and decryption. As estimated, when the file size grows, so does the charge for encryption or decryption. Because of the long encryption and decryption times, these operations impose high power usage.

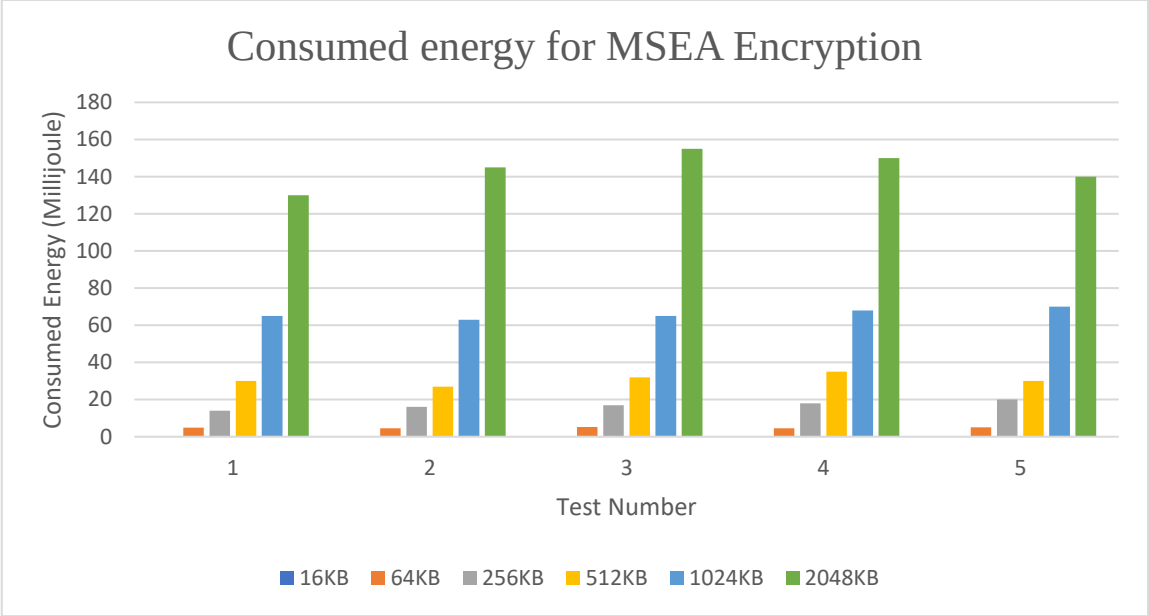


Figure 4.22 Consumed energy for MSEA Encryption across file sizes

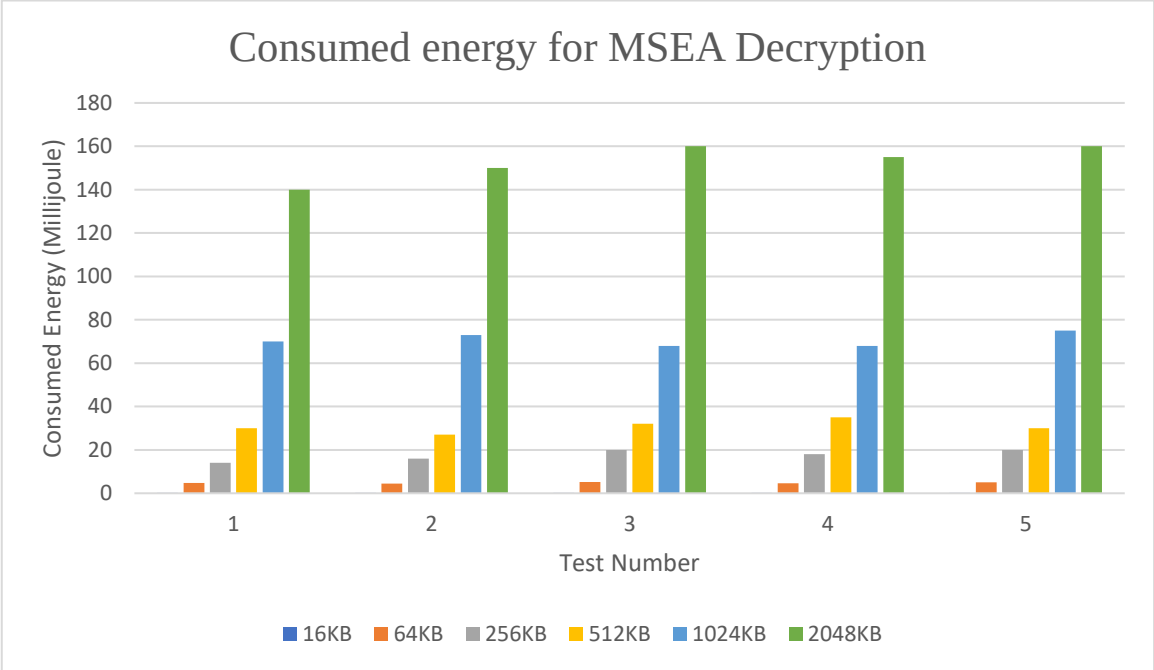


Figure 4.23 Consumed energy for MSEA Decryption across file sizes

d. LEA

Figures 4.24 and 4.25 display the energy utilization outcomes for LEA encryption and decryption. The growth in file sizes, as estimated, appears to increase battery consumption.

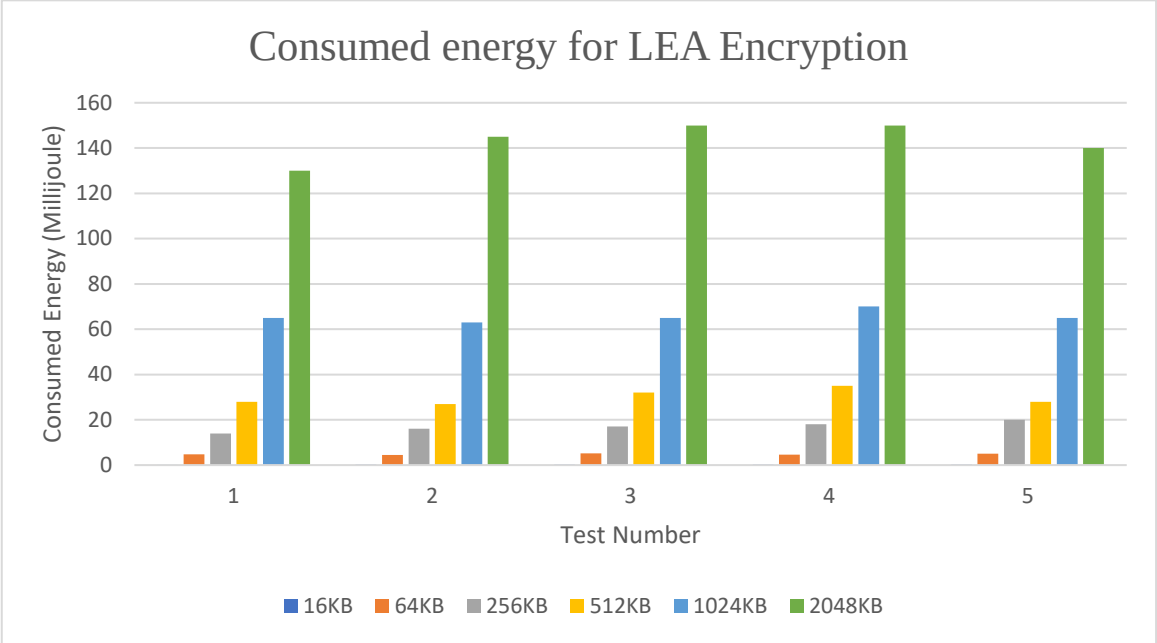


Figure 4.24 Consumed energy for LEA Encryption across file sizes

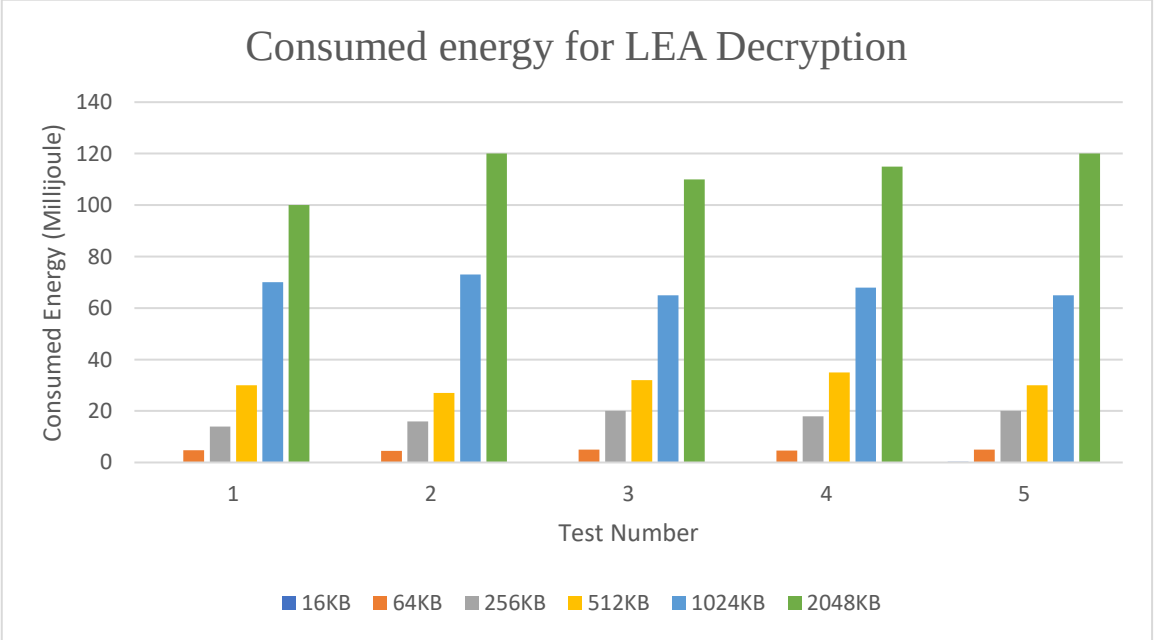


Figure 4.25 Consumed energy for LEA Decryption across file sizes

e. XTEA

Figures 4.26 and 4.27 reveal the electricity usage findings for XTEA encryption and decryption.

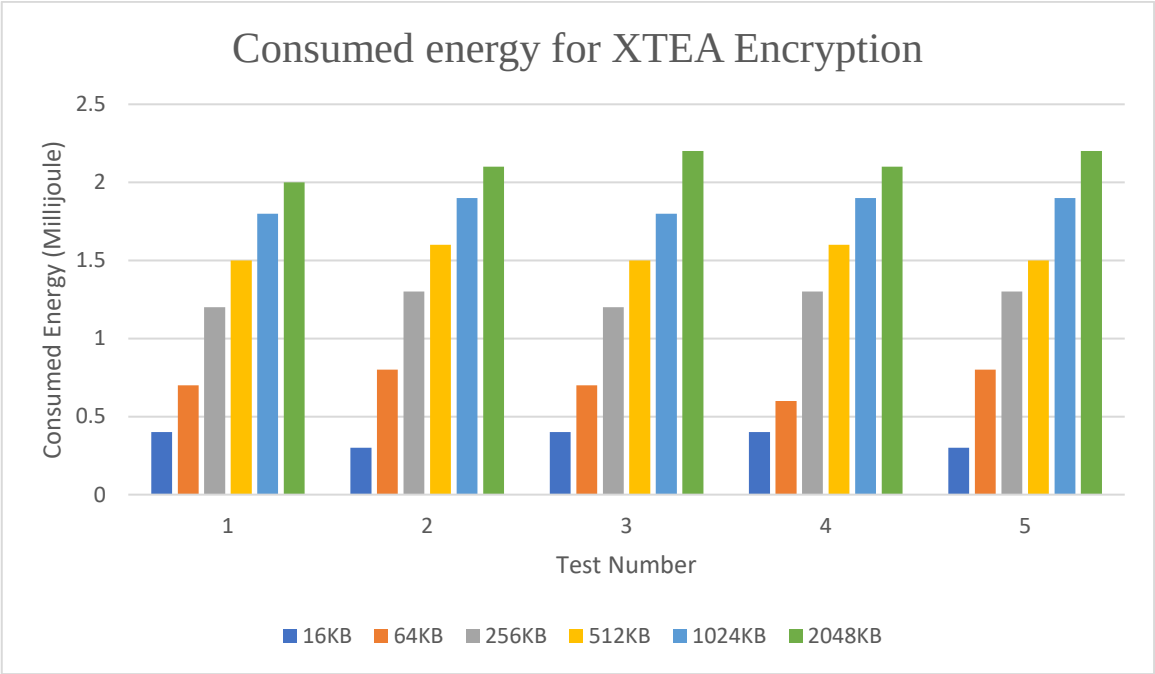


Figure 4.26 Consumed energy for XTEA Encryption across file sizes

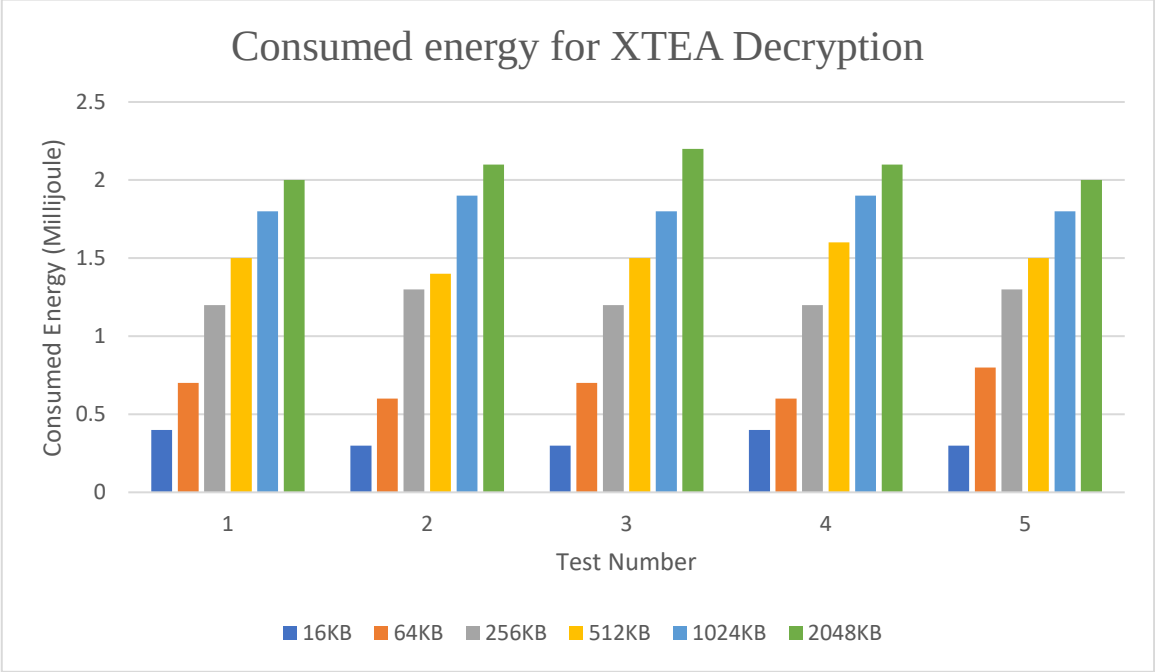


Figure 4.27 Consumed energy for XTEA Decryption across file sizes

f. SIMON

Figures 4.28 and 4.29 display the power consumption outcomes for SIMON encryption and decryption.

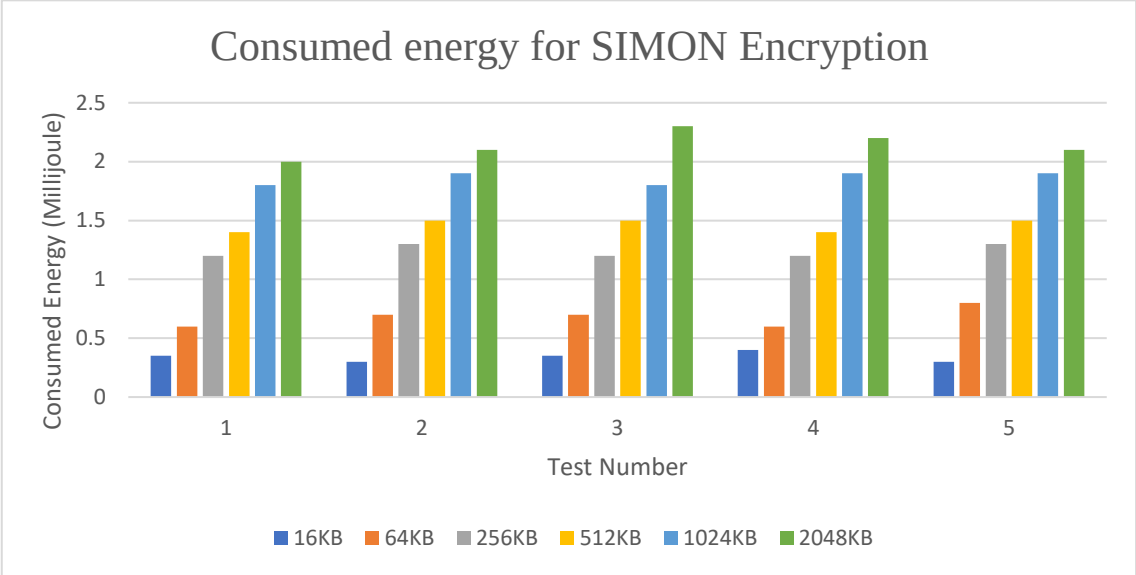


Figure 4.28 Consumed energy for SIMON Encryption across file sizes

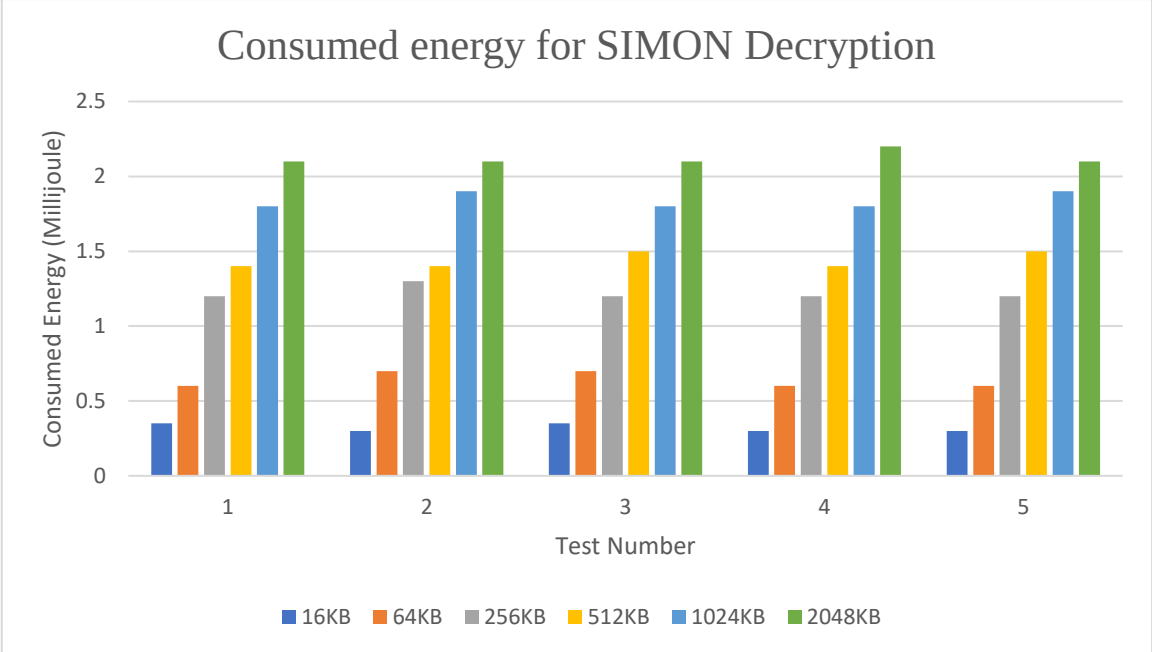


Figure. 4.29 Consumed energy for SIMON Decryption across file sizes

g. PRINCE

Figures 4.30 and 4.31 illustrate the power utilisation outcomes for PRINCE encryption and decryption.

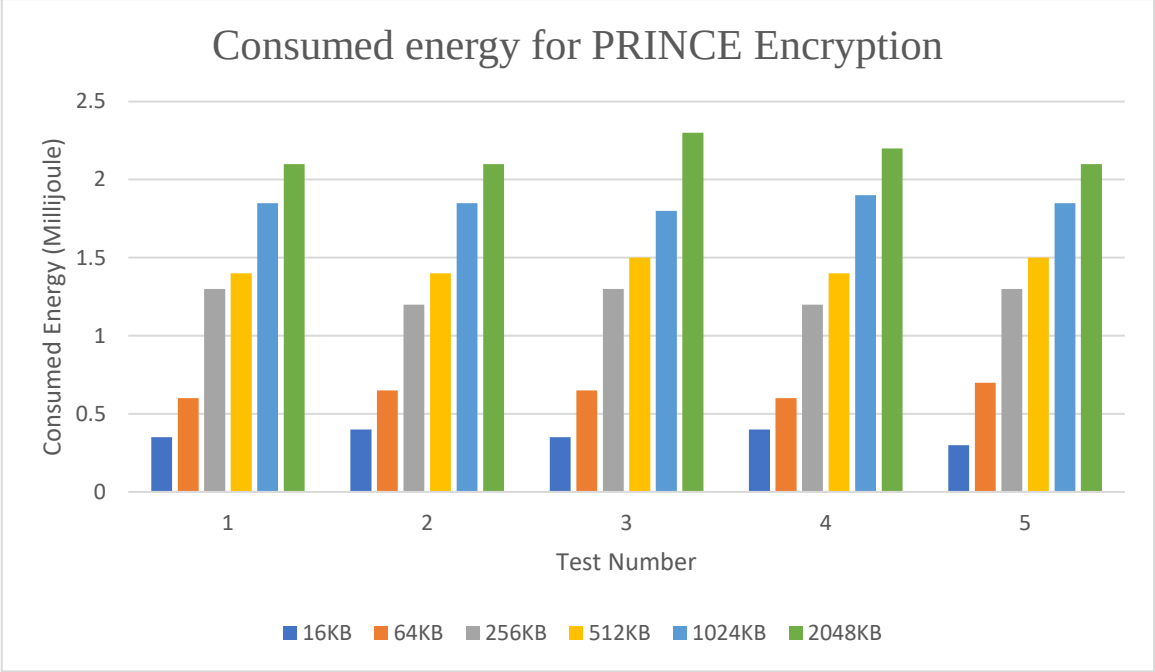


Figure 4.30 Consumed energy for PRINCE Encryption across file sizes

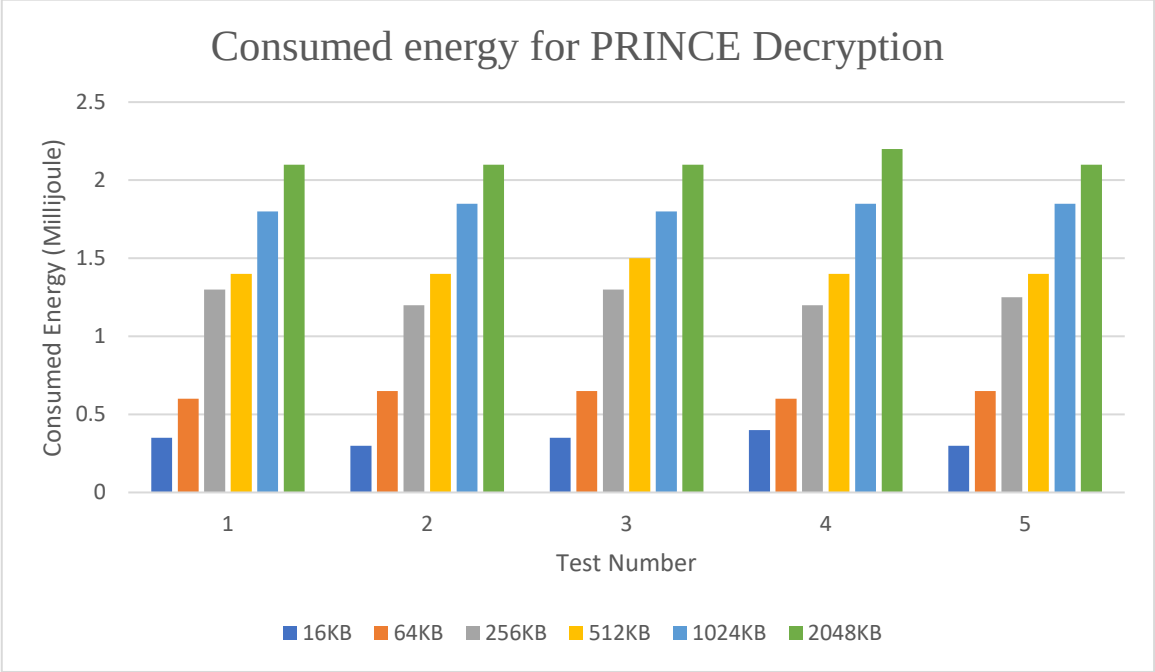


Figure 4.31 Consumed energy for PRINCE Decryption across file sizes

h. RECTANGLE

Figures 4.32 and 4.33 depict the outcomes of the energy consumption for RECTANGLE encryption and decryption.

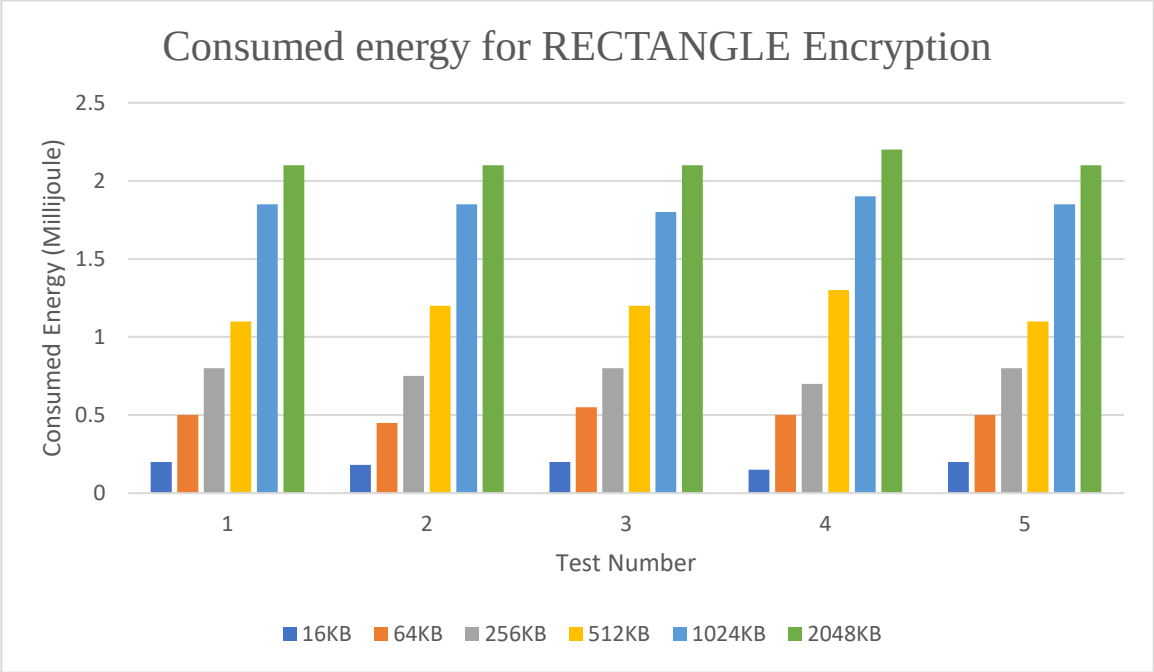


Figure 4.32 Consumed energy for RECTANGLE Encryption across file sizes

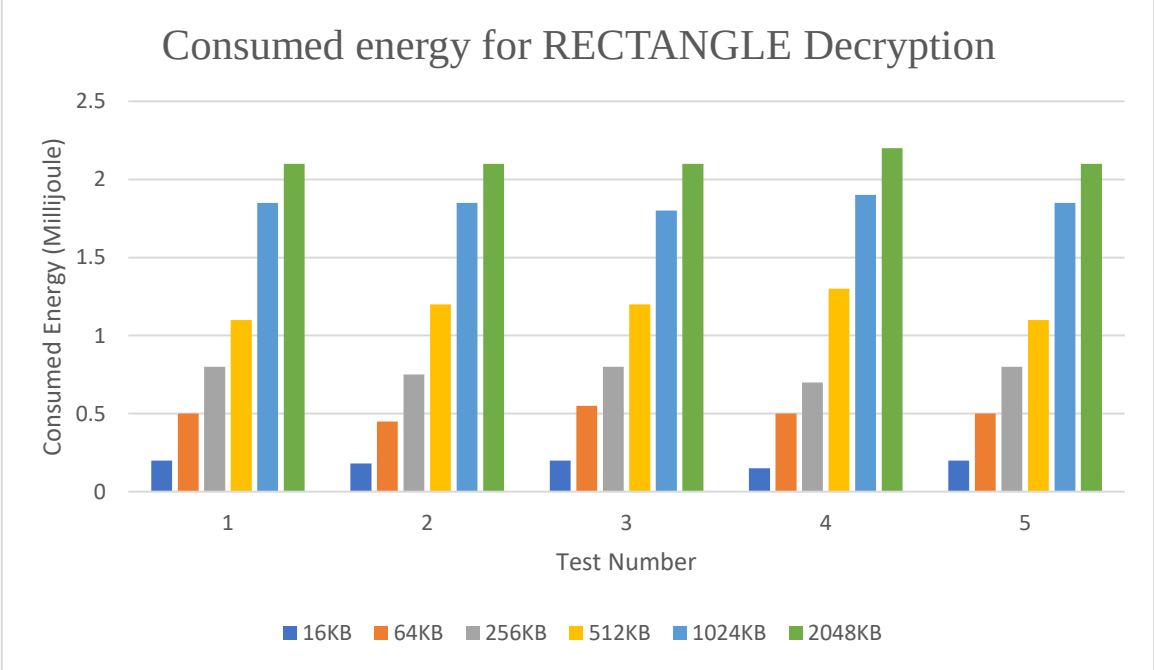


Figure 4.33 Consumed energy for RECTANGLE Decryption across file sizes

4.4.1.3 Memory Usage

This section presents the memory used throughout the encryption and decryption operations of the LWC algorithms.

a. AES

Figures 4.34 and 4.35 display the RAM utilised by AES encryption and decryption for all file sizes. The highest recorded amount of memory that an algorithm consumes during the largest file size procedure.

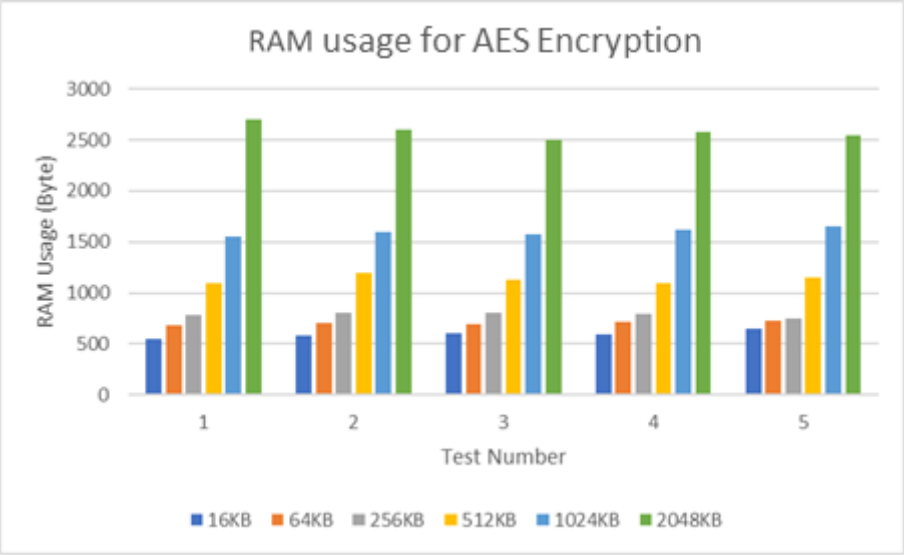


Figure 4.34 RAM usage for AES Encryption across file sizes

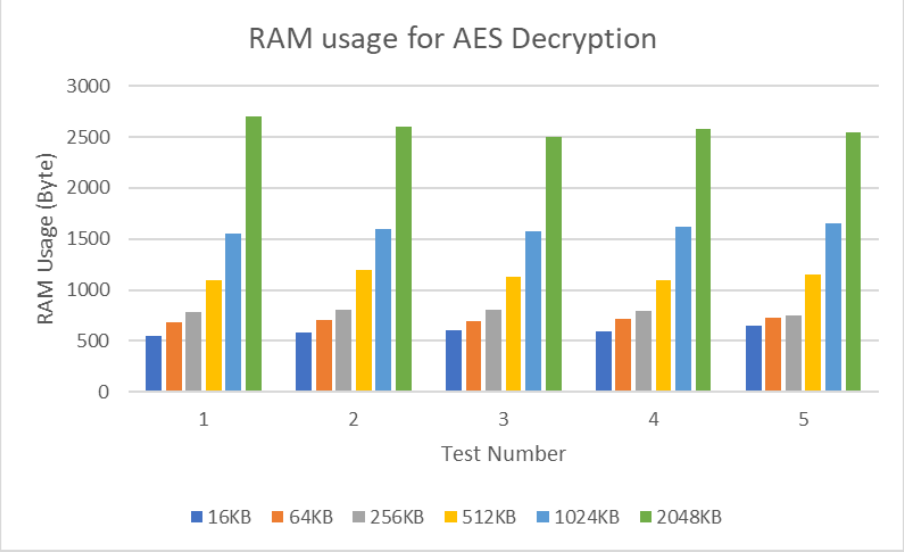


Figure 4.35 RAM usage for AES Decryption across file sizes

For all file sizes, Figures 4.36 and 4.37 illustrate the ROM utilised by AES encryption and decryption.

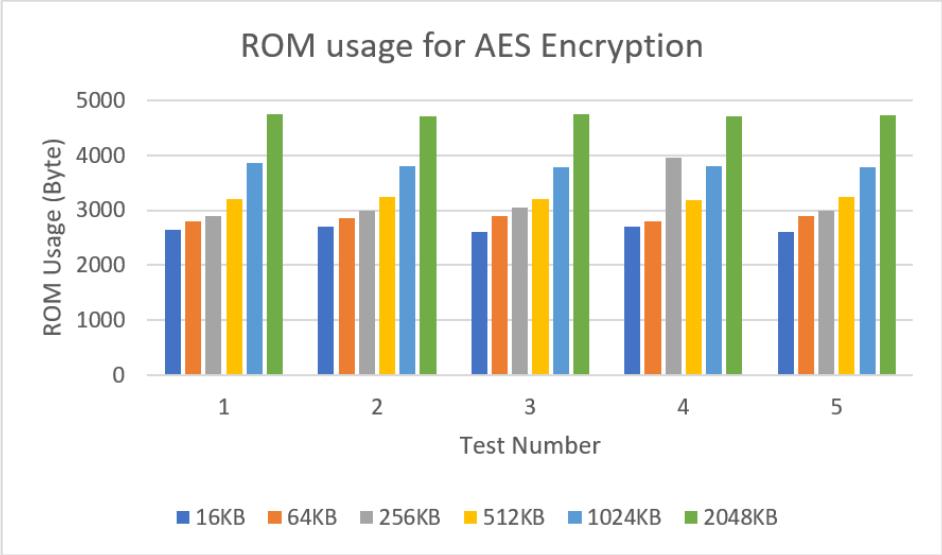


Figure 4.36 ROM usage for AES Encryption across file sizes

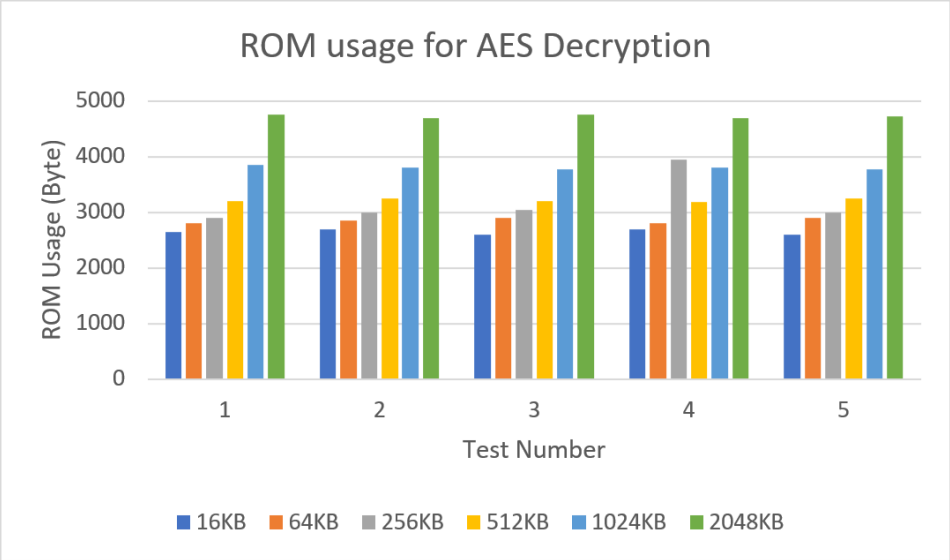


Figure 4.37 ROM usage for AES Decryption across file sizes

b. PRESENT

Figures 4.38 and 4.39 display the RAM usage for PRESENT encryption and decryption with all files.

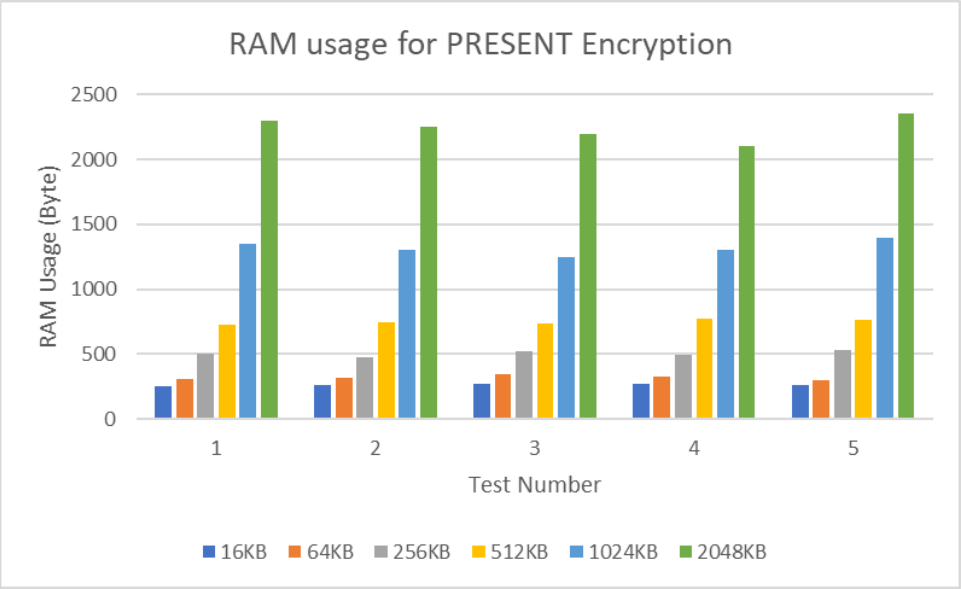


Figure 4.38 RAM usage for PRESENT Encryption across file sizes

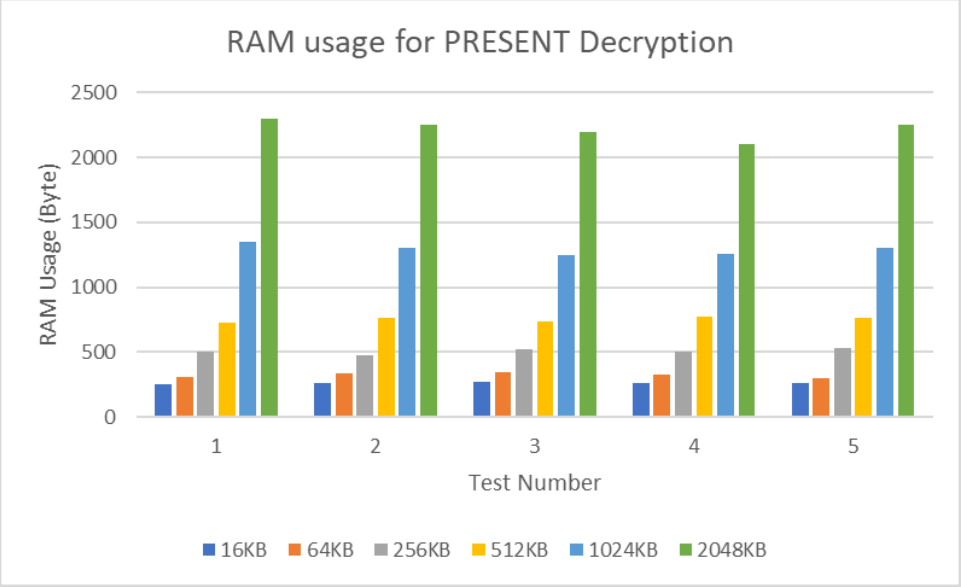


Figure 4.39 RAM usage for PRESENT Decryption across file sizes

The ROM utilised by PRESENT encryption and decryption in all file sizes is pictured in Figures 4.40 and 4.41.

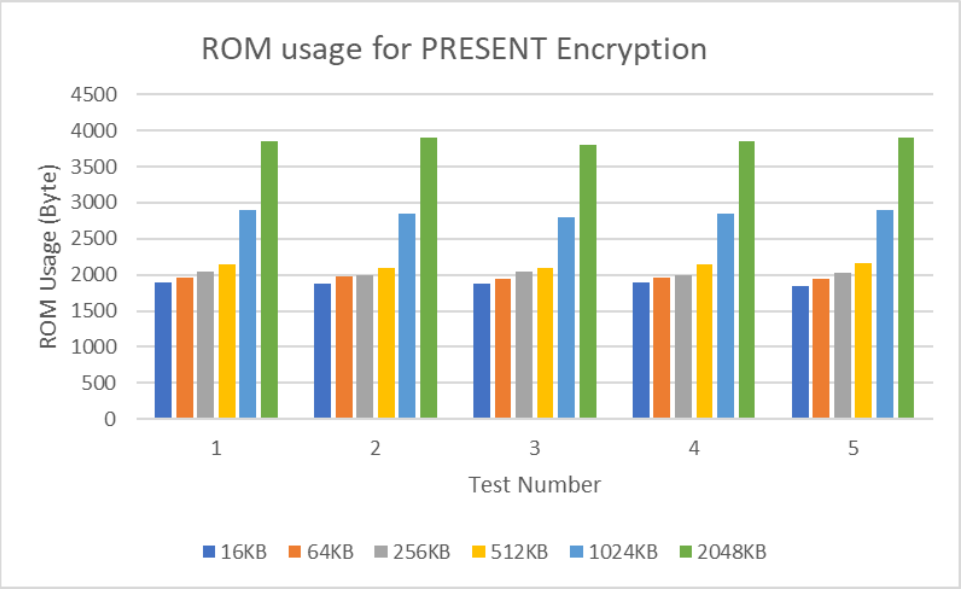


Figure 4.40 ROM usage for PRESENT Encryption across file sizes

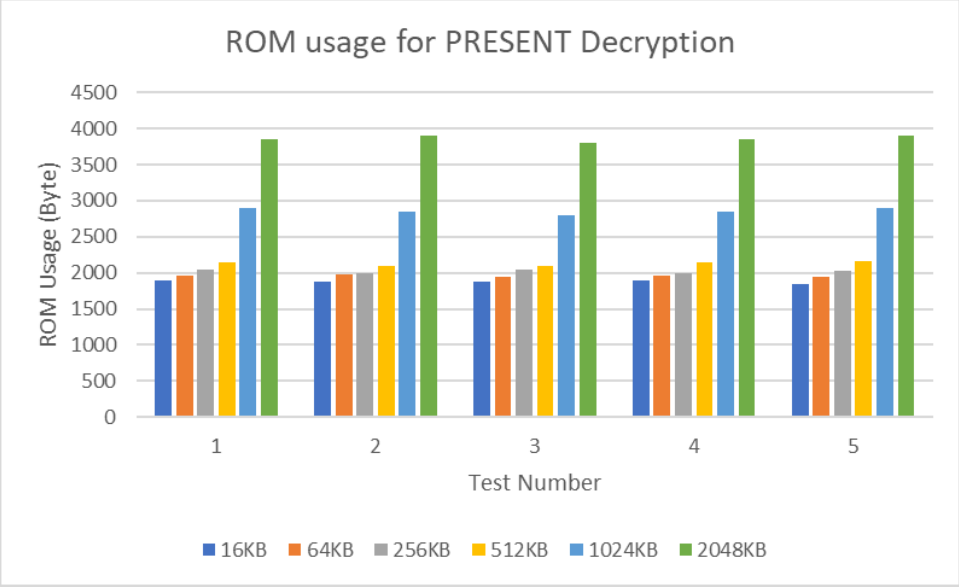


Figure 4.41 ROM usage for PRESENT Decryption across file sizes

c. MSEA

The RAM consumption for encryption and decryption of various size files is illustrated in Figures 4.42 and 4.43.

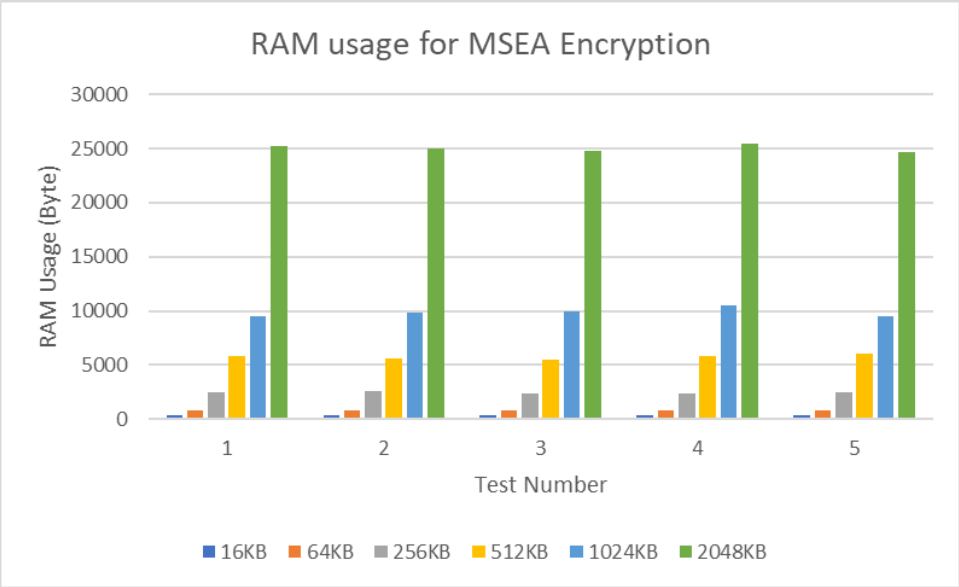


Figure 4.42 RAM usage for MSEA Encryption across file sizes

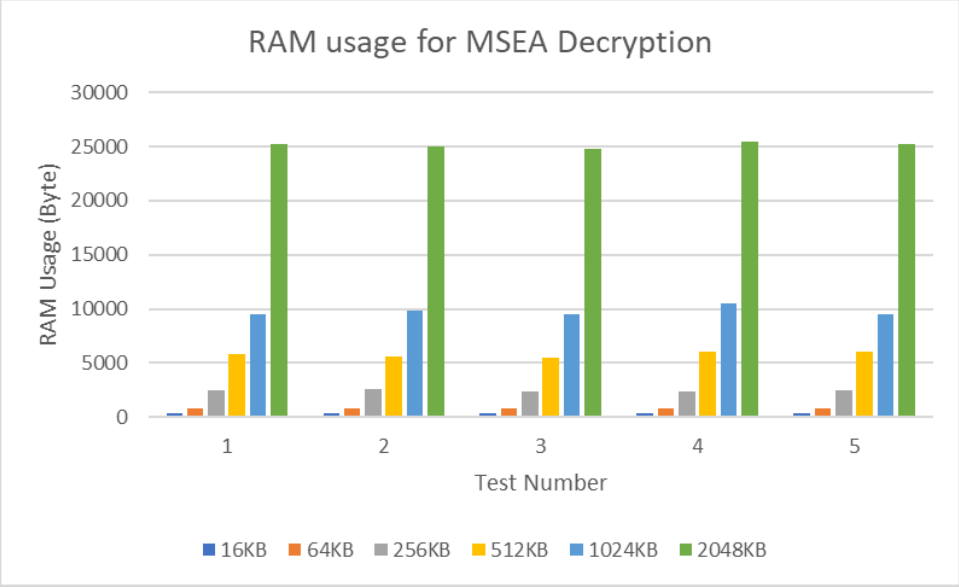


Figure 4.43 RAM usage for MSEA Decryption across file sizes

Figures 4.44 and 4.45 show the ROM used by MSEA for encryption and decryption across all file sizes.

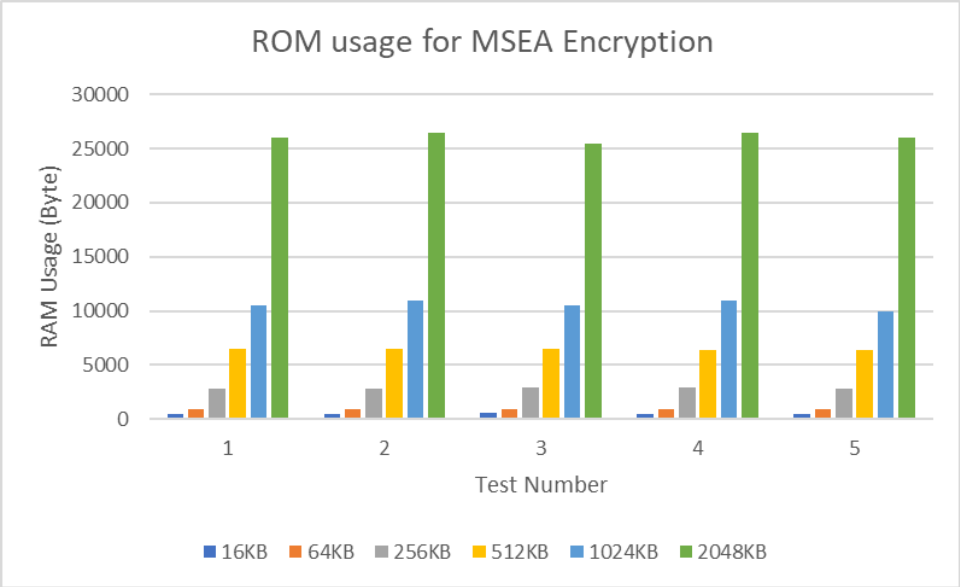


Figure 4.44 ROM usage for MSEA Encryption across file sizes

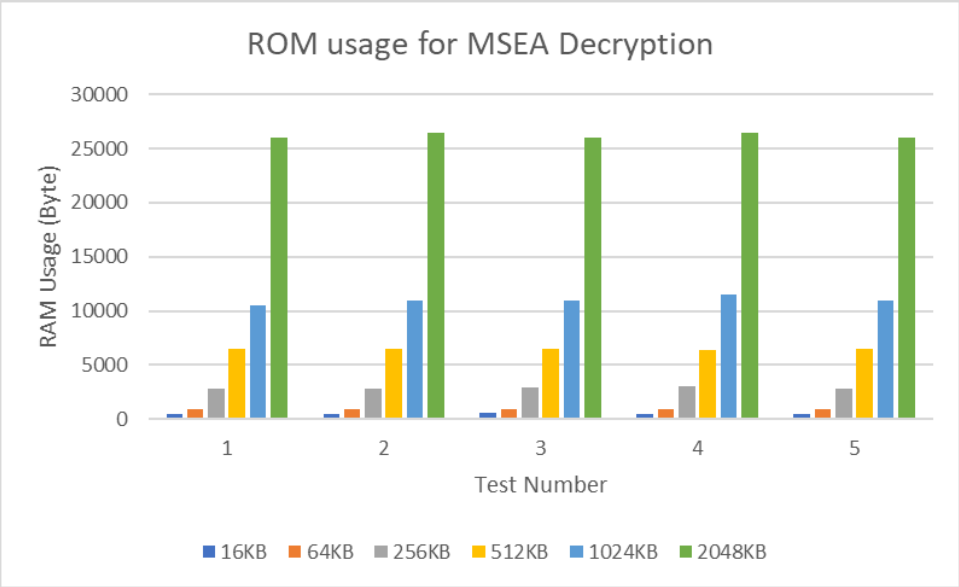


Figure 4.45 ROM usage for MSEA Decryption across file sizes

d. LEA

Figures 4.46 and 4.47 show the RAM utilisation for LEA encryption and decryption among all files, respectively.

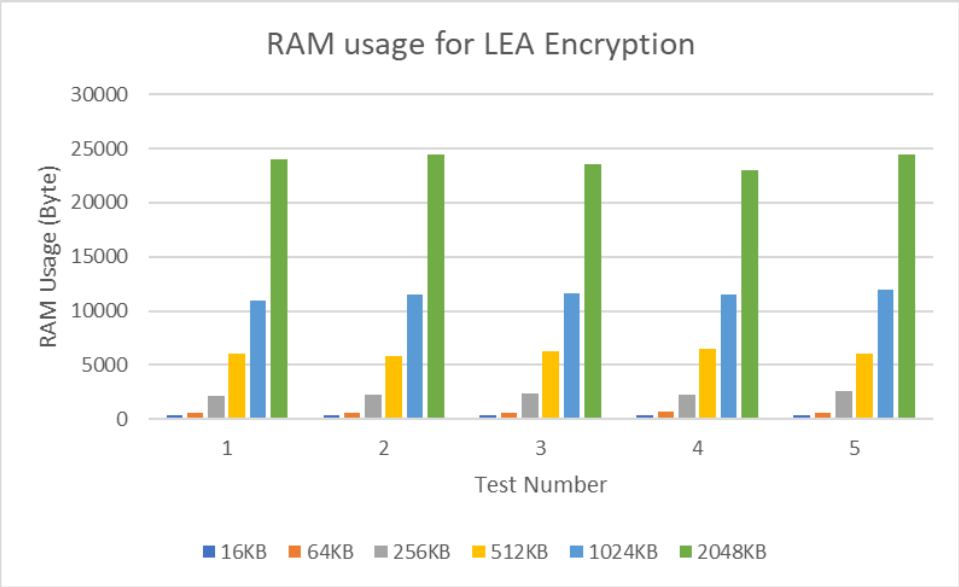


Figure 4.46 RAM usage for LEA Encryption across file sizes

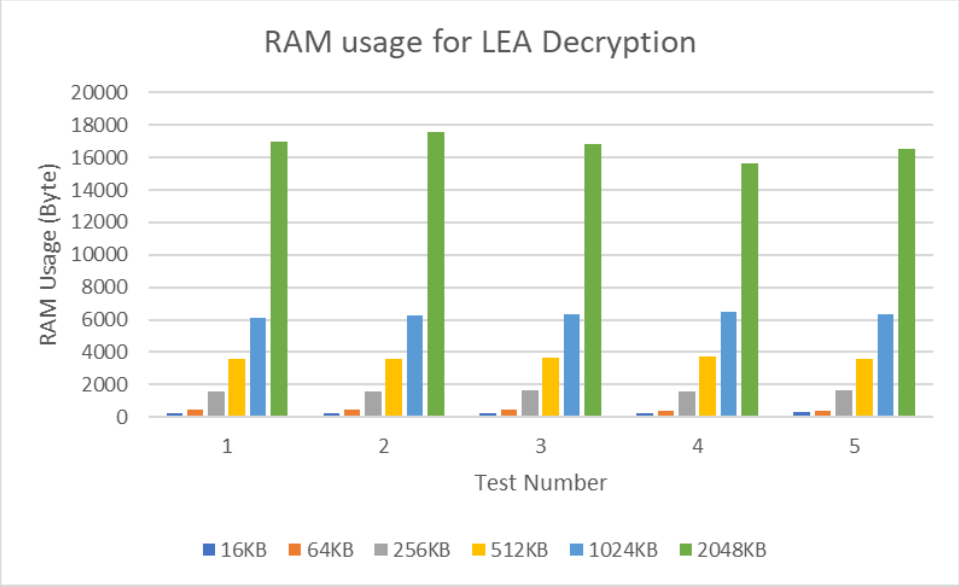


Figure 4.47 RAM usage for LEA Decryption across file sizes

Figures 4.48 and 4.49 display what ROM is used for LEA encryption and decryption over all files.

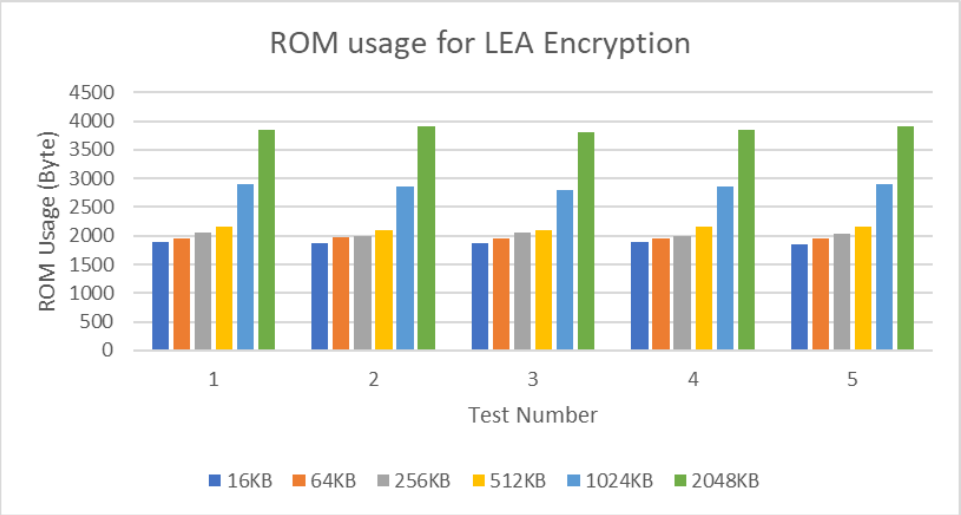


Figure 4.48 ROM usage for LEA Encryption across file sizes

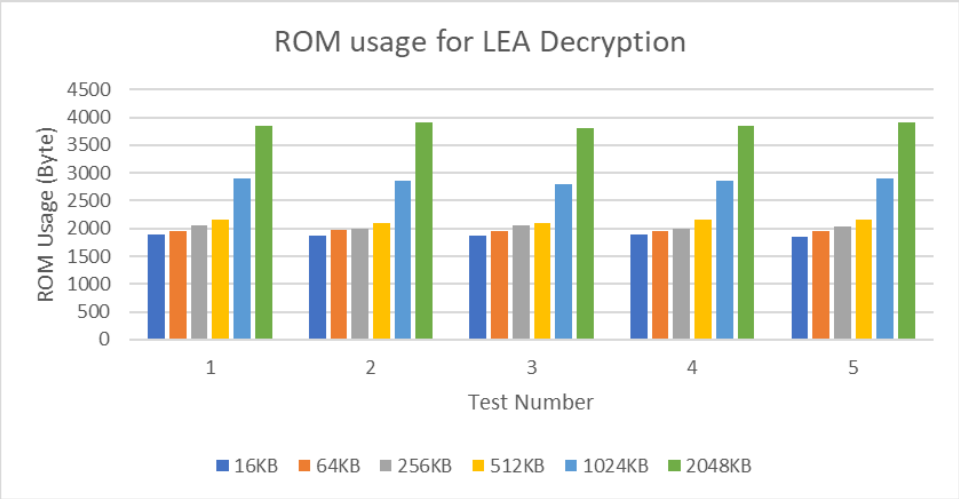


Figure 4.49 ROM usage for LEA Decryption across file sizes

e. XTEA

Figures 4.50 and 4.51 illustrate how much RAM is consumed by all files during the XTEA encryption and decryption processes. According to XTEA, the maximum RAM usage for operations across all file sizes is around 2000KB.

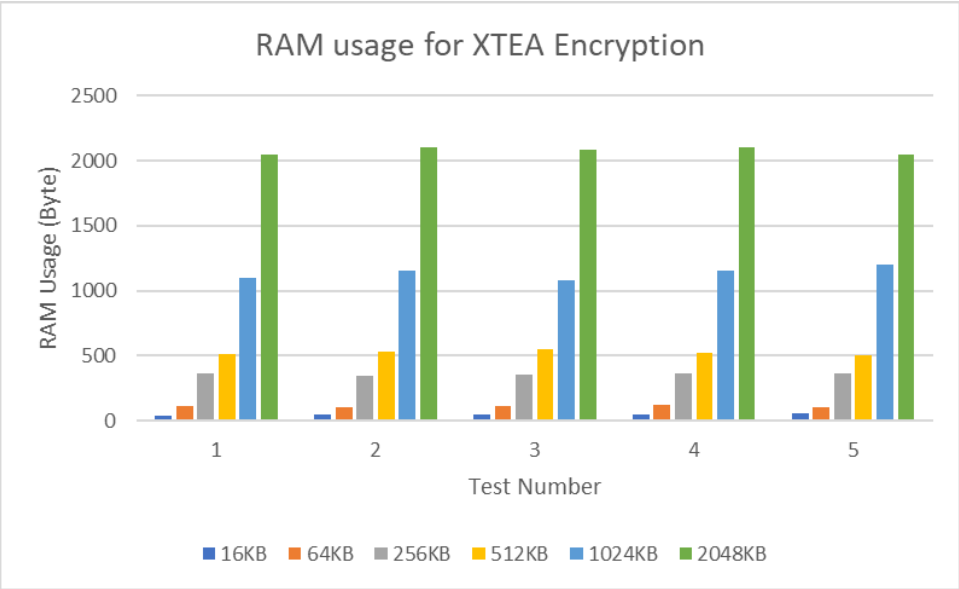


Figure 4.50 RAM usage for XTEA Encryption across file sizes

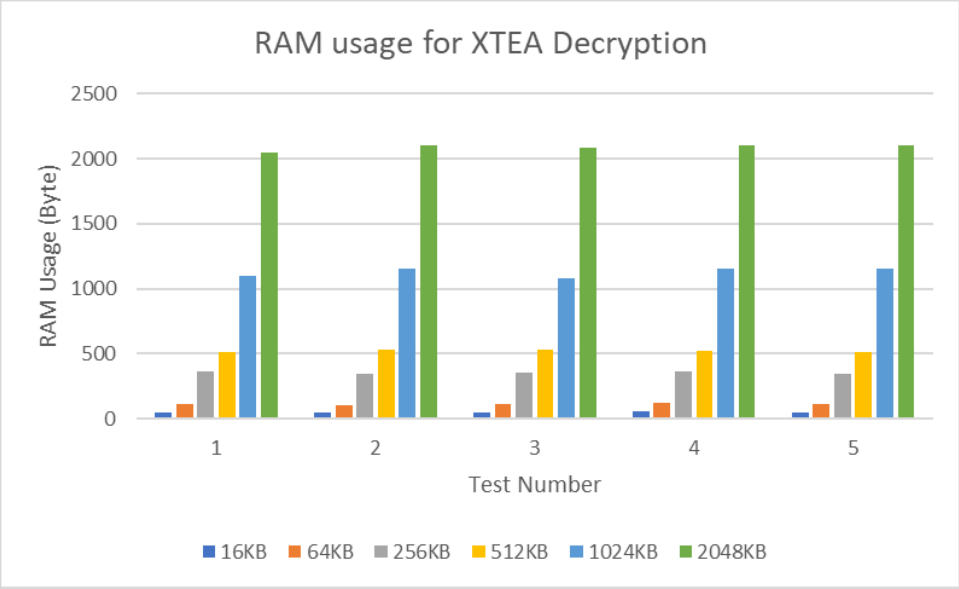


Figure 4.51 RAM usage for XTEA Decryption across file sizes

Figures 4.52 and 4.53 illustrate what ROM is used for XTEA encryption and decryption of all files.

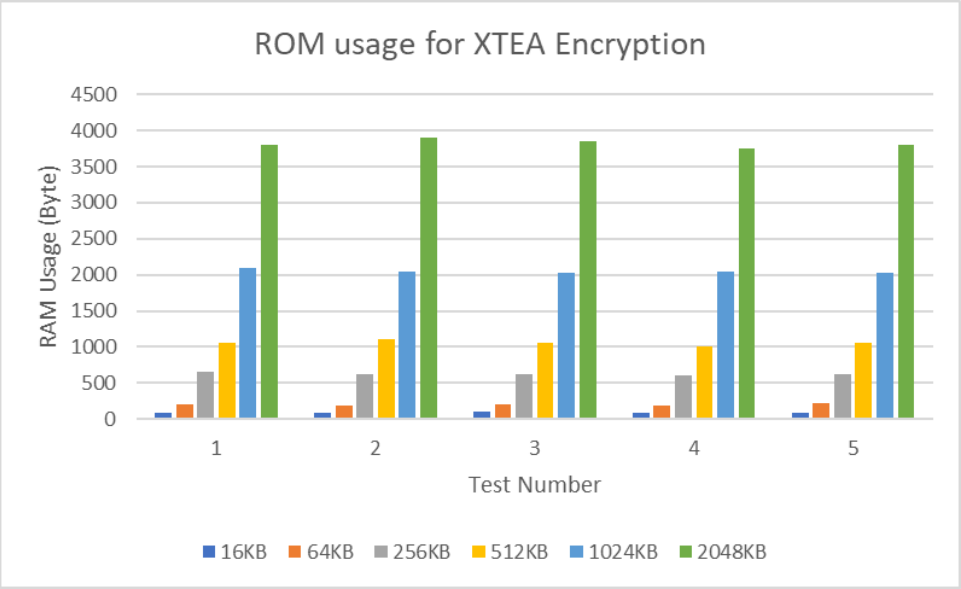


Figure 4.52 ROM usage for XTEA Encryption across file sizes

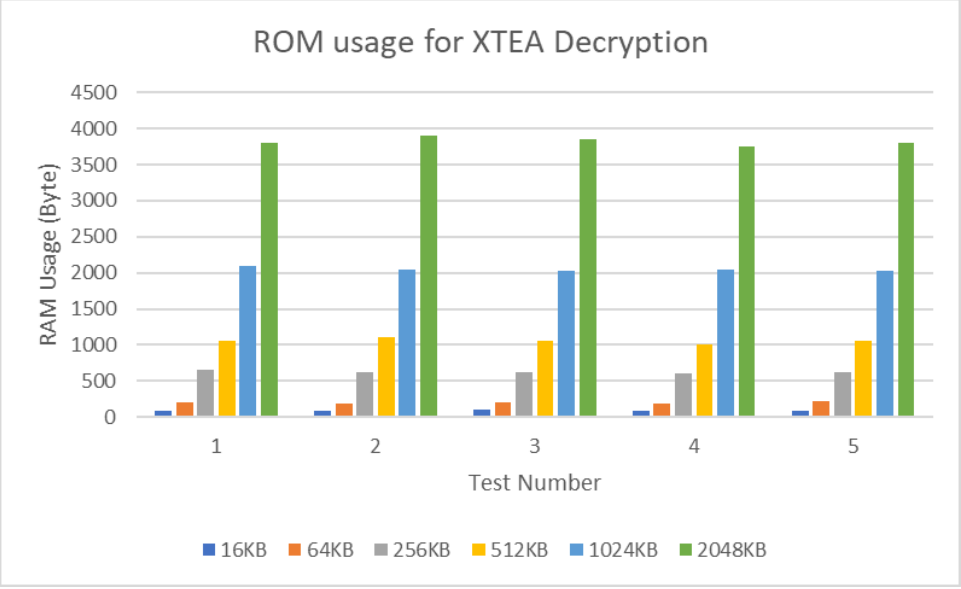


Figure 4.53 ROM usage for XTEA Decryption across file sizes

f. SIMON

Figures 4.54 and 4.55 display the RAM consumption of SIMON encryption and decryption for various files. SIMON's RAM utilisation is consistent for both encryption and decryption.

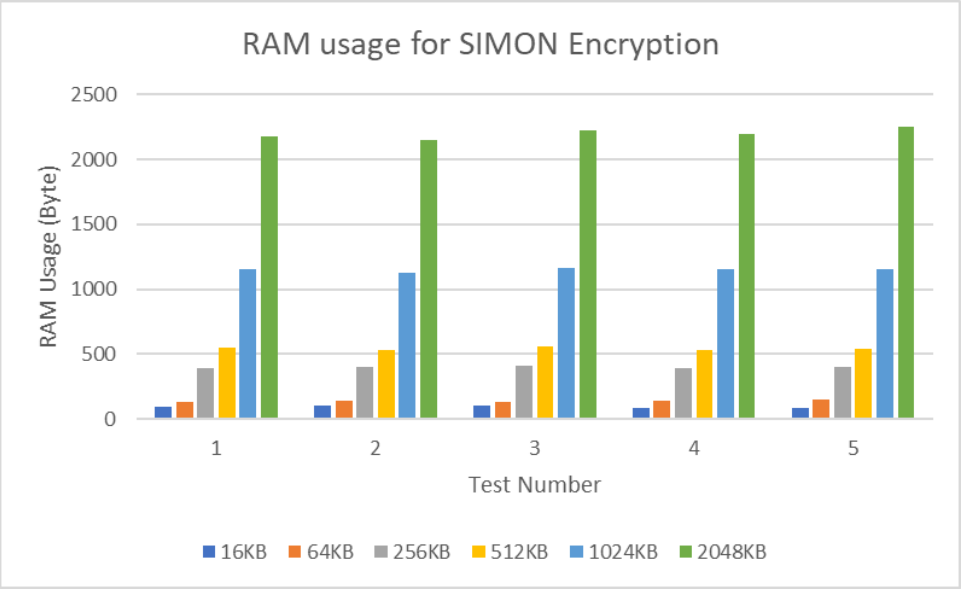


Figure 4.54 RAM usage for SIMON Encryption across file sizes

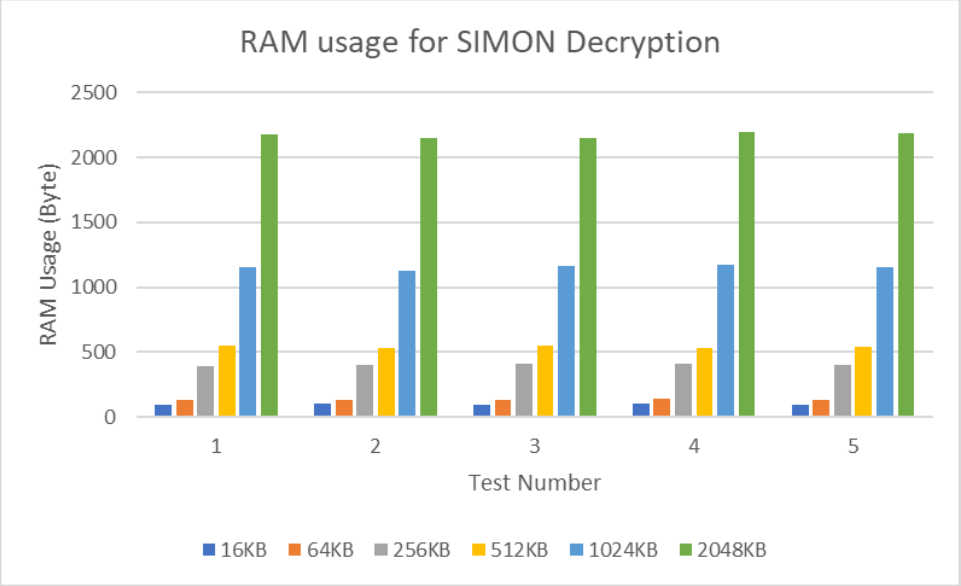


Figure 4.55 RAM usage for SIMON Decryption across file sizes

Figures 4.56 and 4.57 depict the ROM utilisation for SIMON encryption and decryption over all files.

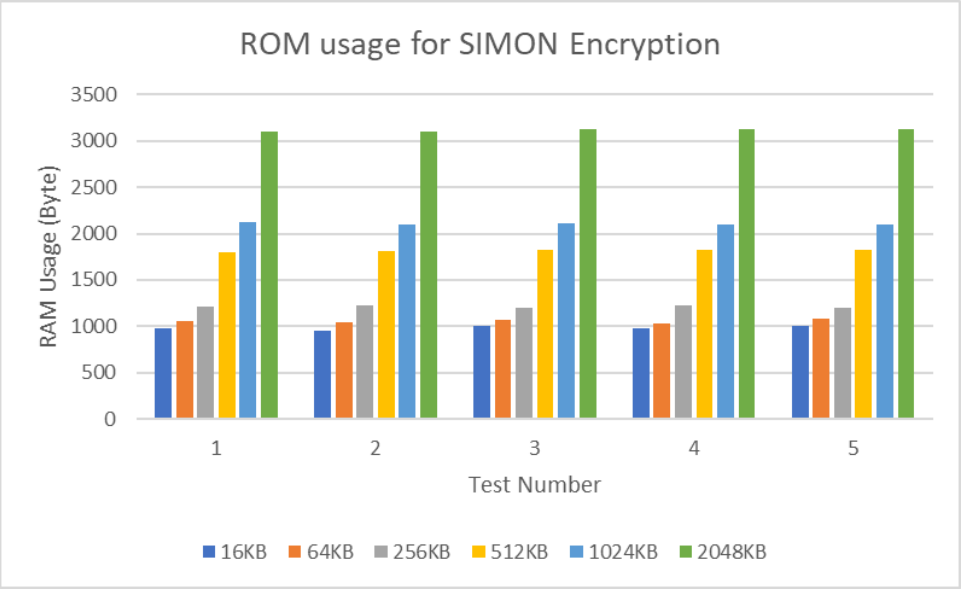


Figure 4.56 ROM usage for SIMON Encryption across file sizes

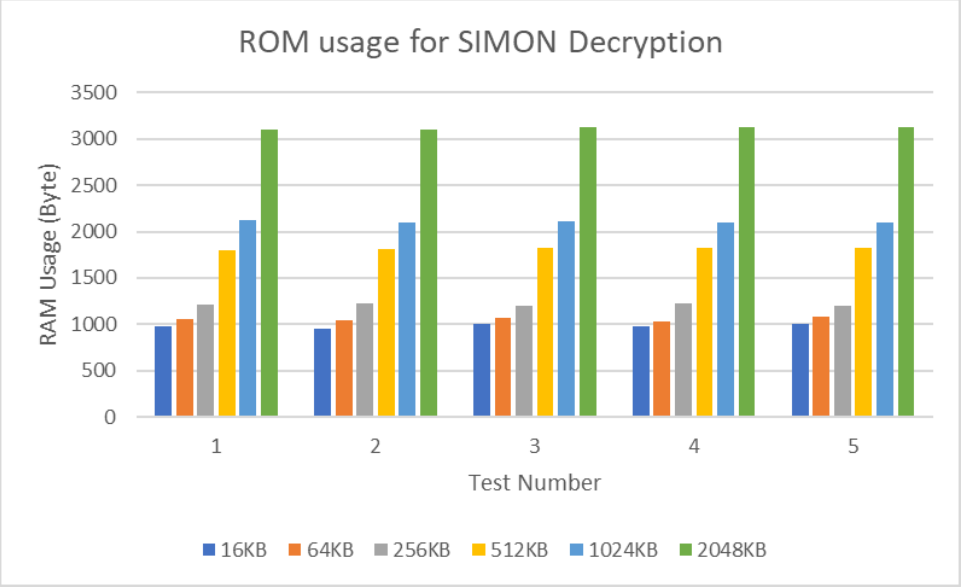


Figure 4.57 ROM usage for SIMON Decryption across file sizes

g. PRINCE

Figures 4.58 and 4.59 depict how much RAM is consumed by PRINCE encryption and decryption across all files.

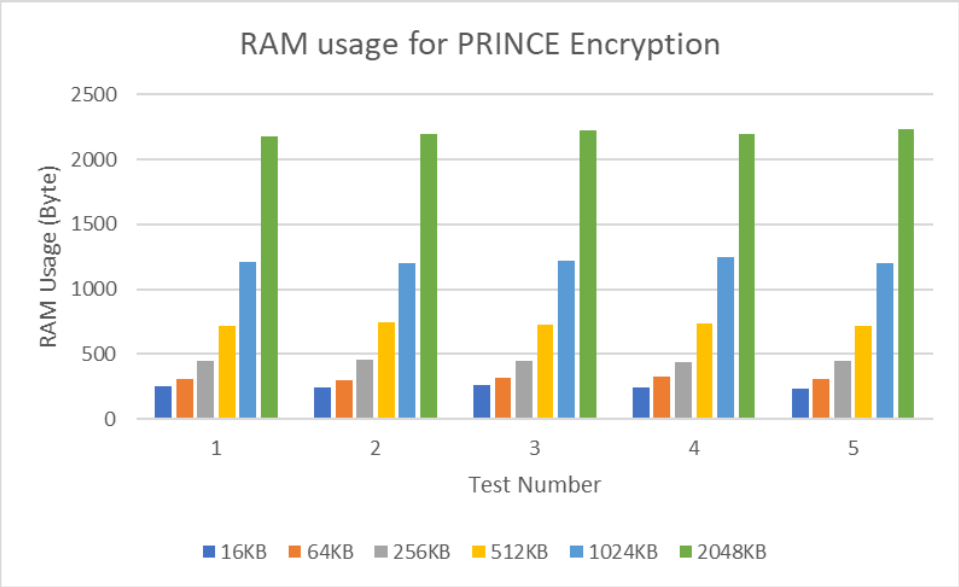


Figure 4.58 RAM usage for PRINCE Encryption across file sizes

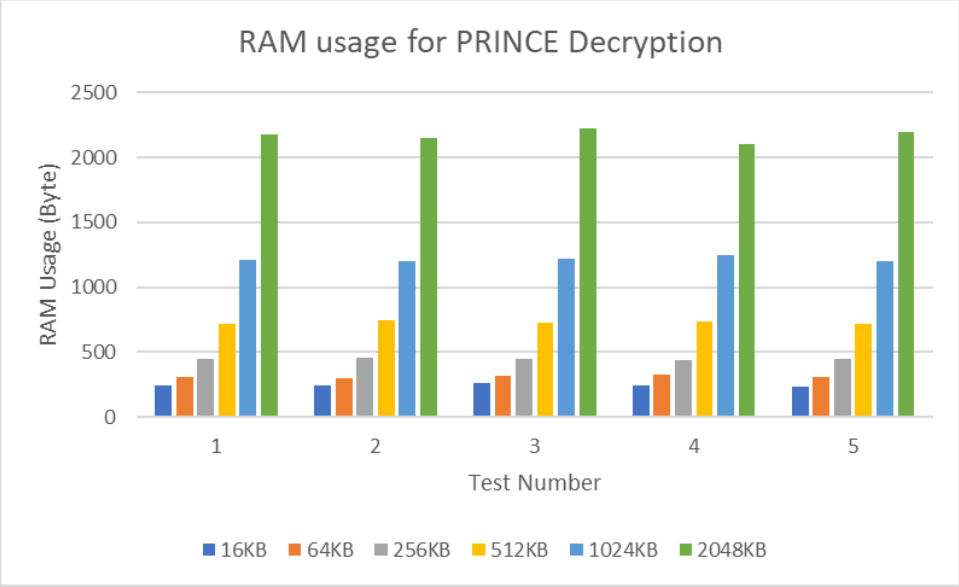


Figure 4.59 RAM usage for PRINCE Decryption across file sizes

Figures 4.60 and 4.61 show how much ROM is utilised for PRINCE encryption and decryption processes of all files.

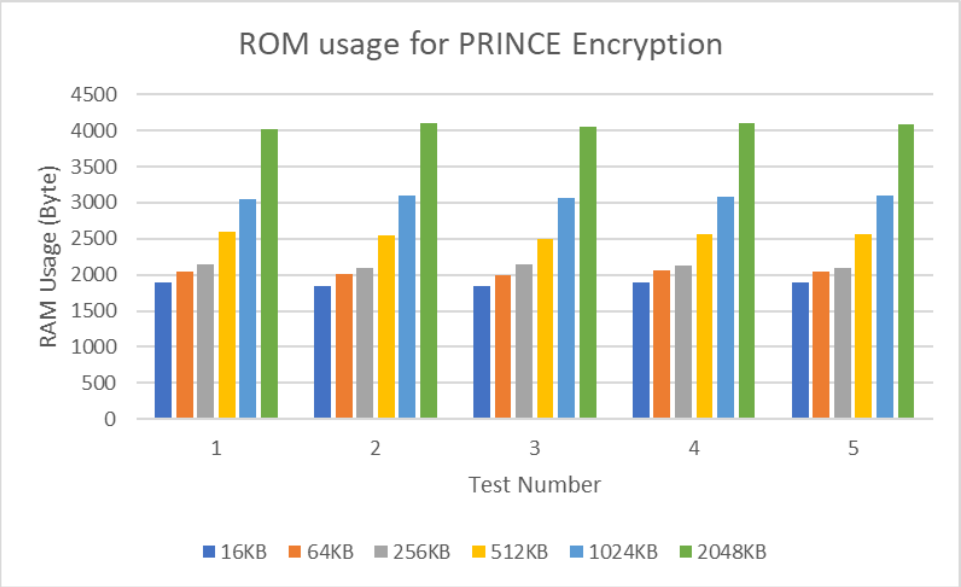


Figure 4.60 ROM usage for PRINCE Encryption across file sizes

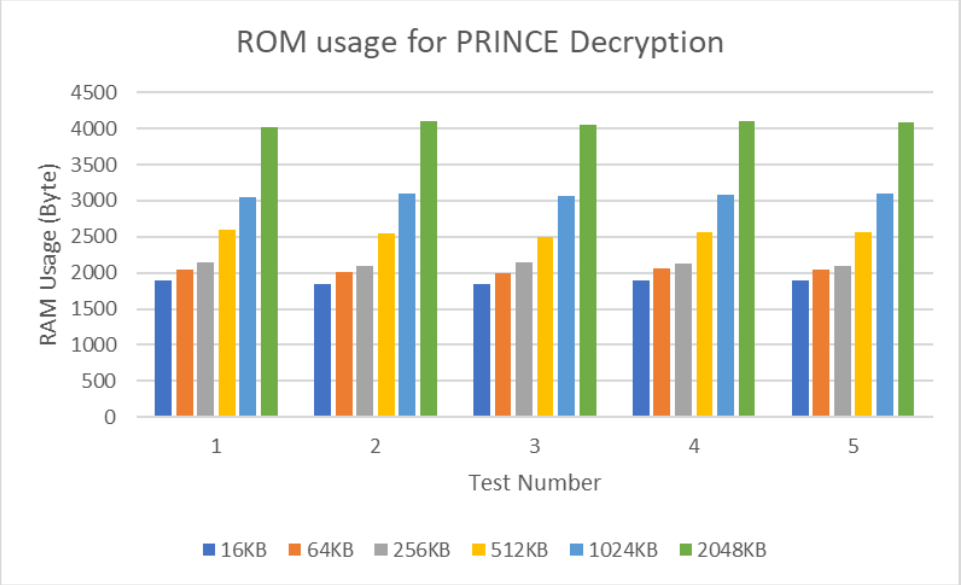


Figure 4.61 ROM usage for PRINCE Decryption across file sizes

h. RECTANGLE

Figures 4.62 and 4.63 illustrate the RAM utilisation for RECTANGLE encryption and decryption for all files. RECTANGLE consumes a similar amount of RAM for encryption and decryption processes.

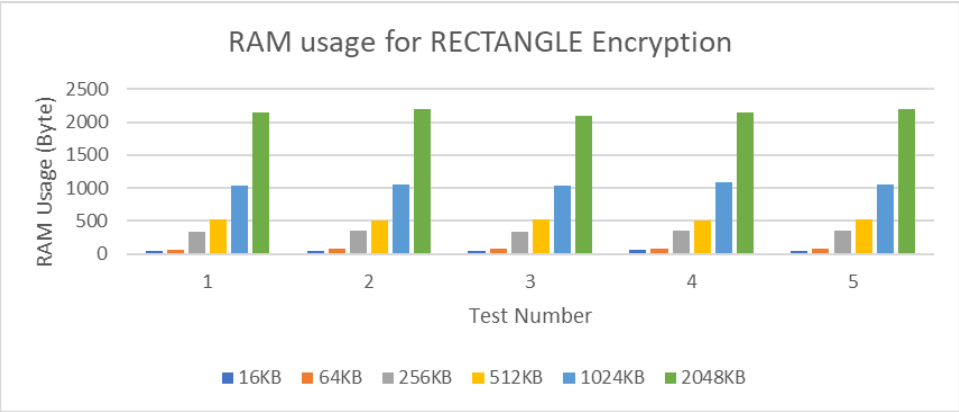


Figure 4.62 RAM usage for RECTANGLE Encryption across file sizes

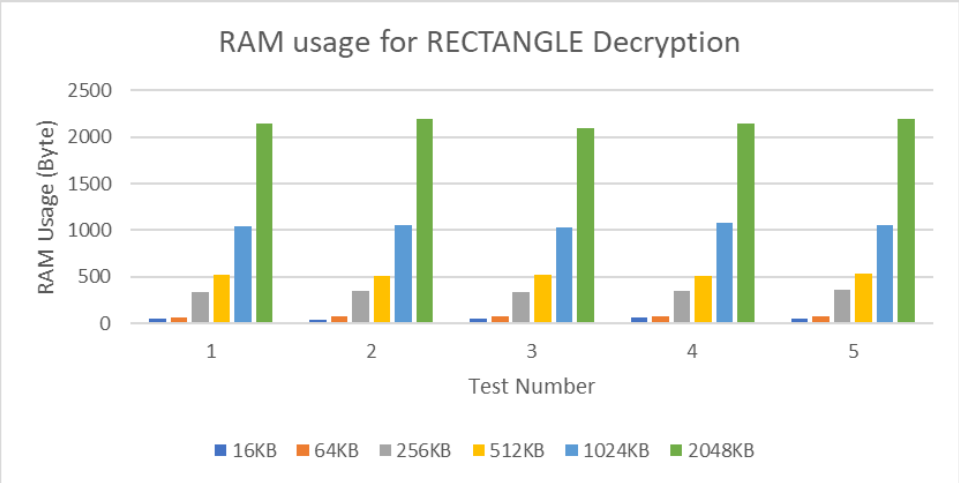


Figure 4.63 RAM usage for RECTANGLE Decryption across file sizes

Figures 4.64 and 4.65 represent the ROM utilisation for RECTANGLE encryption and decryption processes with all files.

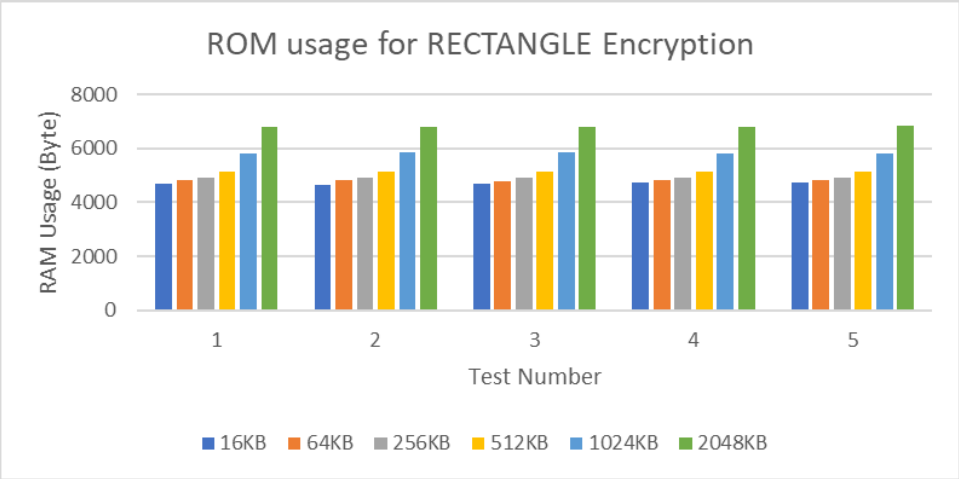


Figure 4.64 ROM usage for RECTANGLE Encryption across file sizes

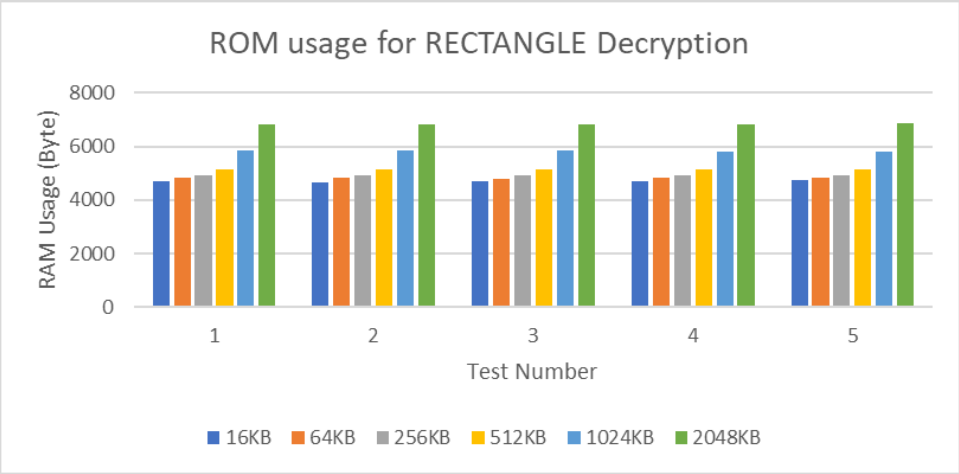


Figure 4.65 ROM usage for RECTANGLE Decryption across file sizes

4.4.2 LWC Algorithms Performance Evaluation

The outcomes of each LWC algorithm will be evaluated in this section due to experiment classifications.

a. Encryption and Decryption Times

The following figures (Figures 4.66 and 4.67) and tables (Tables 4.6 and 4.7) evaluate the LWC algorithms. The tables comprise the values utilised to evaluate each LWC algorithm. The encryption and decryption execution times for the 16KB file is subject to competition among the algorithms. RECTANGLE is the fastest of the chosen LWC algorithms, performing the majority of procedures on 512KB and bigger files. MSEA and LEA algorithms do not compete with the other LWC algorithms at any other file size.

LEA and MSEA algorithms have the longest execution times, starting at 64 bytes. RECTANGLE and XTEA, however, have the shortest operation time of the other algorithms. Table 4.7 summarises the LWC algorithm's order for decryption operations of execution time.

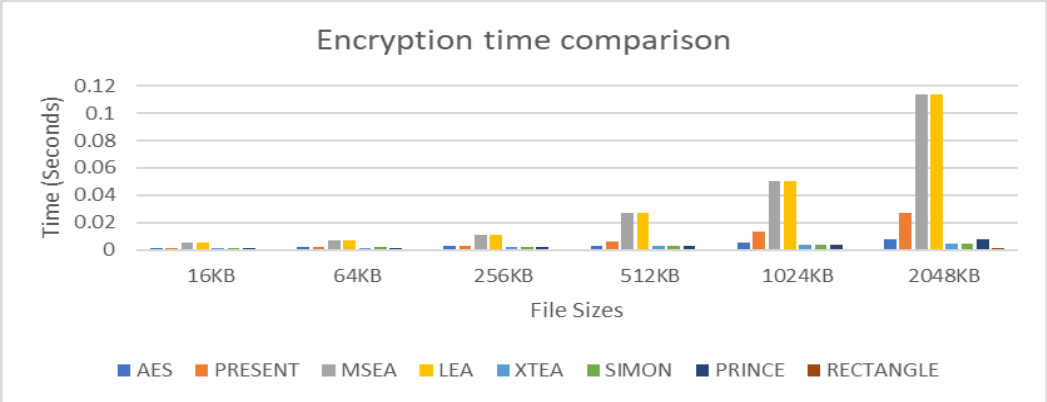


Figure 4.66 Encryption time comparison

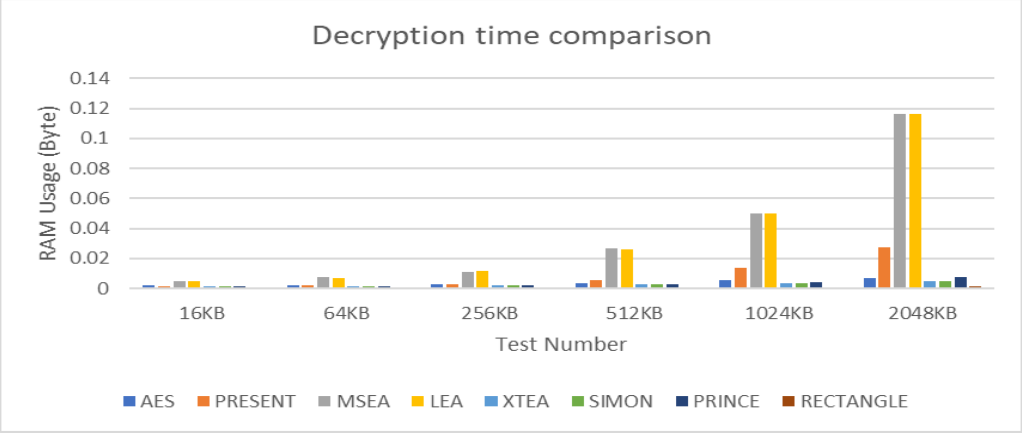


Figure 4.67 Decryption time comparison

Table 4.6 Encryption time comparison (Seconds)

	AES	PRESENT	MSEA	LEA	XTEA	SIMON	PRINCE	RECTANGLE
16KB	0.0016	0.0014	0.005	0.005	0.0012	0.0011	0.0012	0.00024
64KB	0.0018	0.0018	0.0072	0.0072	0.0016	0.0017	0.0013	0.00034
256KB	0.0029	0.0026	0.0112	0.0112	0.0023	0.0022	0.0022	0.00044
512KB	0.0032	0.0058	0.027	0.027	0.0029	0.0029	0.0028	0.00056
1024KB	0.0056	0.0132	0.05	0.05	0.0038	0.0036	0.0038	0.00078
2048KB	0.0073	0.027	0.114	0.114	0.0048	0.0046	0.0074	0.00132

Table 4.7 Decryption time comparison (Seconds)

	AES	PRESENT	MSEA	LEA	XTEA	SIMON	PRINCE	RECTANGLE
16KB	0.0018	0.0014	0.005	0.005	0.0011	0.0011	0.0012	0.00024
64KB	0.0018	0.0018	0.0072	0.007	0.0017	0.0017	0.0013	0.00036
256KB	0.0028	0.0026	0.0112	0.0116	0.0022	0.0022	0.0022	0.00044
512KB	0.0034	0.0057	0.027	0.026	0.0029	0.0029	0.0028	0.00054
1024KB	0.0056	0.014	0.05	0.05	0.0037	0.0036	0.0038	0.00078
2048KB	0.0066	0.0276	0.116	0.116	0.0048	0.0045	0.0076	0.00132

b. Power Consumption

Because energy consumption is proportional to encryption or decryption execution times, the power usage for LWC algorithms pursues a similar trend to encryption and decryption. Figures 4.68, 4.69, Table 4.8, and Table 4.9 all illustrate a comparable illustration of encryption and decryption for the results, even though they are indicating charge utilisation. As a result, MSEA and LEA consume significantly more energy than the other six LWC algorithms. MSEA gives some challenges at smaller file sizes, but it is slower than other LWC algorithms at larger files. When compared to the other LWC algorithms, RECTANGLE has the lowest charge usage, but this difference could be viewed as insignificant.

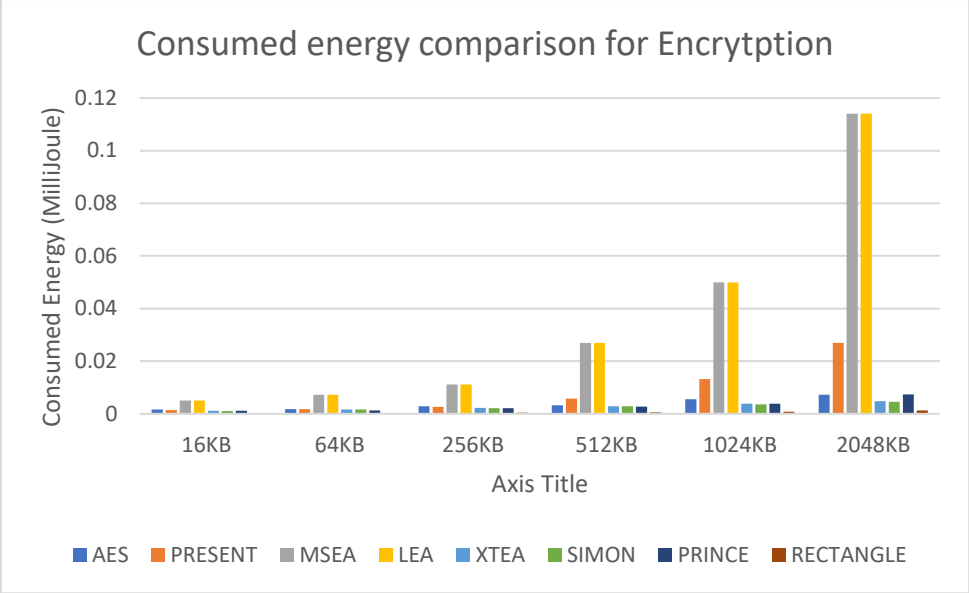


Figure. 4.68 Consumed energy comparison for Encryption across file sizes

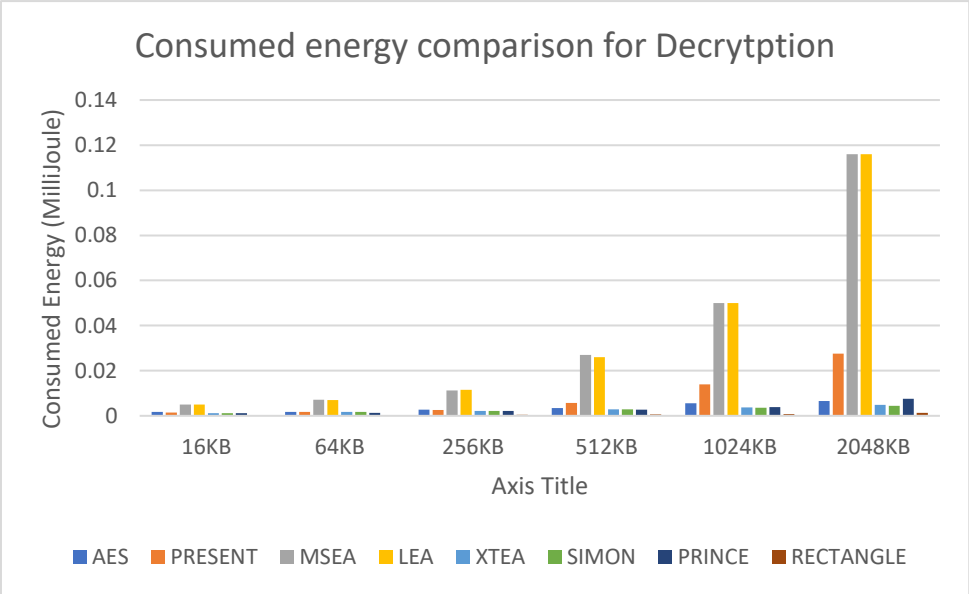


Figure 4.69 Consumed energy comparison for Decryption across file sizes

Table 4.8 Consumed energy comparison for Encryption (Millijoule)

	AES	PRESENT	MSEA	LEA	XTEA	SIMON	PRINCE	RECTANGLE
16KB	0.0016	0.0014	0.005	0.005	0.0012	0.0011	0.0012	0.00024
64KB	0.0018	0.0018	0.0072	0.0072	0.0016	0.0017	0.0013	0.00034
256KB	0.0029	0.0026	0.0112	0.0112	0.0023	0.0022	0.0022	0.00044
512KB	0.0032	0.0058	0.027	0.027	0.0029	0.0029	0.0028	0.00056
1024KB	0.0056	0.0132	0.05	0.05	0.0038	0.0036	0.0038	0.00078
2048KB	0.0073	0.027	0.114	0.114	0.0048	0.0046	0.0074	0.00132

Table 4.9 Consumed energy comparison for Decryption (Millijoule)

	AES	PRESENT	MSEA	LEA	XTEA	SIMON	PRINCE	RECTANGLE
16KB	0.0018	0.0014	0.005	0.005	0.0011	0.0011	0.0012	0.00024
64KB	0.0018	0.0018	0.0072	0.007	0.0017	0.0017	0.0013	0.00036
256KB	0.0028	0.0026	0.0112	0.0116	0.0022	0.0022	0.0022	0.00044
512KB	0.0034	0.0057	0.027	0.026	0.0029	0.0029	0.0028	0.00054
1024KB	0.0056	0.014	0.05	0.05	0.0037	0.0036	0.0038	0.00078
2048KB	0.0066	0.0276	0.116	0.116	0.0048	0.0045	0.0076	0.00132

c. Memory Usage

Because memory consumption is proportional to encryption or decryption execution times, LWC algorithm memory usage follows a similar pattern to encryption and decryption. Figures 4.70, 4.71, Table 4.8, and Table 4.9 all show a comparable illustration of encryption and decryption for the results, in terms of memory consumption. As a result, MSEA and LEA use significantly more memory than the other six LWC algorithms. MSEA presents some challenges at smaller file sizes, but it is still larger than other LWC algorithms at bigger file sizes. When compared to the other LWC algorithms, RECTANGLE uses the least amount of memory.

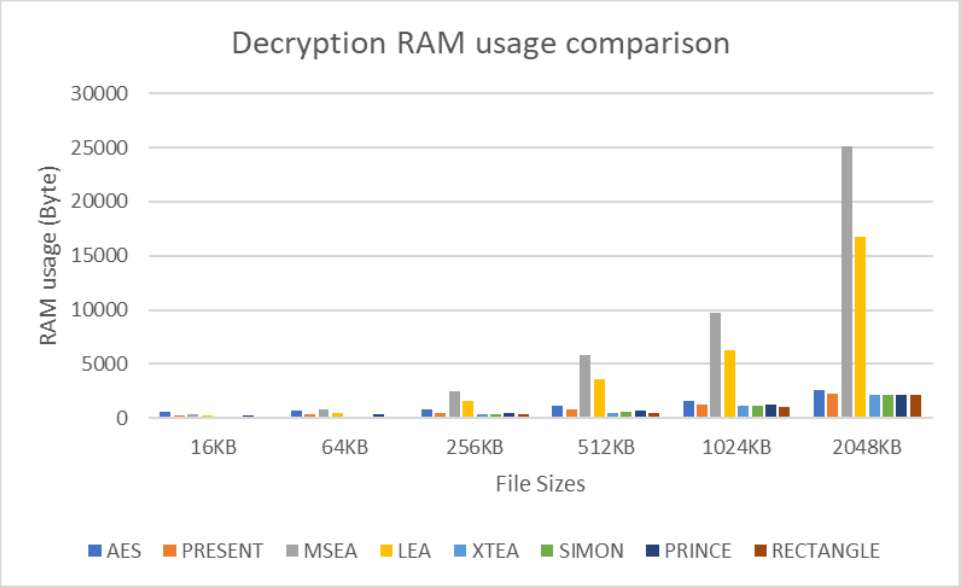


Figure 4.70 Encryption RAM usage comparison

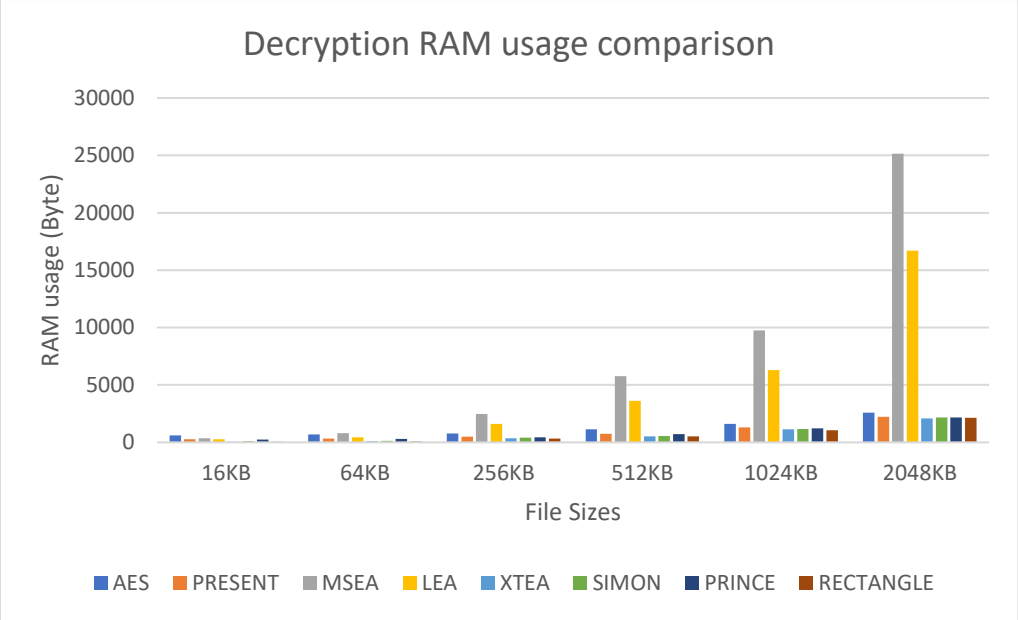


Figure 4.71 Decryption RAM usage comparison

Table 4.10 Encryption RAM usage (Bytes)

	AES	PRESENT	MSEA	LEA	XTEA	SIMON	PRINCE	RECTANGLE
16KB	393	263	360	334	49	95	244	51
64KB	452	322	810	592	109	139	314	76
256KB	519	504	2470	2320	358	398	450	348
512KB	822	750	5780	6140	522	542	732	518
1024KB	1498	1320	9860	11520	1136	1148	1216	1052
2048KB	2500	2240	25040	23920	2076	2200	2206	2160

Table 4.11 Decryption RAM usage (Bytes)

	AES	PRESENT	MSEA	LEA	XTEA	SIMON	PRINCE	RECTANGLE
16KB	594	261	358	260	49	97	242	49
64KB	704	326	804	440	112	134	314	76
256KB	786	506	2470	1614	355	402	450	342
512KB	1134	752	5780	3622	520	540	732	512
1024KB	1600	1292	9760	6290	1126	1152	1216	1058
2048KB	2586	2220	25140	16700	2086	2174	2170	2150

d. Encryption/Decryption Throughput

The following formula is utilised to measure throughput:

$$\text{Throughput} = \text{Number of Bytes} / (\text{End Time} - \text{Start Time})$$

Figure 4.72 represents the median encryption throughputs.

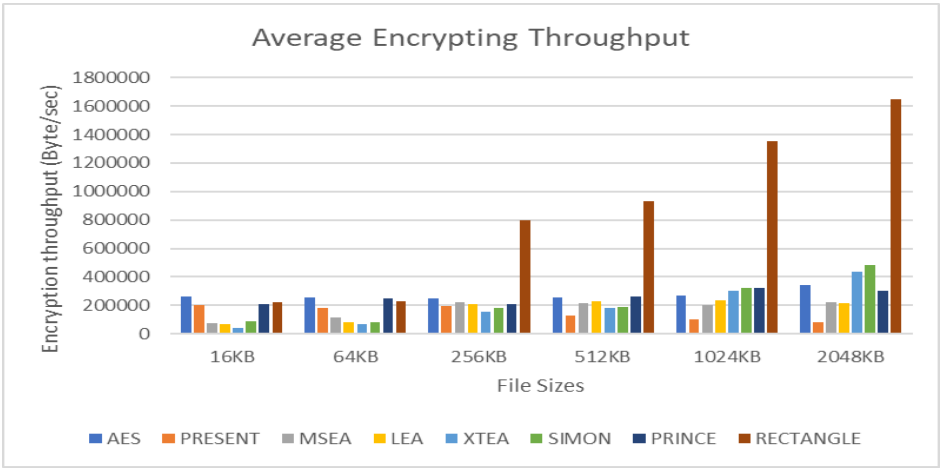


Figure 4.72 Average Encrypting Throughput across file sizes

RECTANGLE has the highest throughput from 256KB file. AES achieves the peak value for encryption for 16KB, among others. Figure 4.73 illustrates the typical decrypting throughputs.

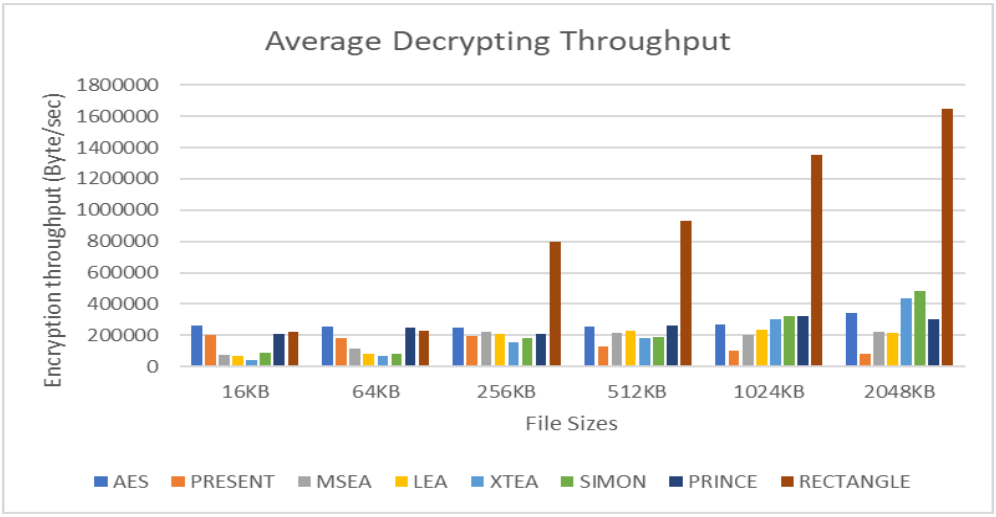


Figure 4.73 Average Decrypting Throughput across file sizes

Throughputs for RECTANGLE, SIMON, and XTEA are considerably greater than other LWC algorithms. PRESENT encryption throughput results are the smallest among other LWC algorithms.

4.5 Conclusion

The outcomes of a Systematic Literature Review (SLR) and Experimental Performance Testing of a group of LWC algorithms determining their performance were reported in Chapter 4.

The SLR has identified the critical security and privacy problems regarding IoT as well as the key factors of IoT LWC algorithms in the medical industry. The results of the experimental performance testing have demonstrated to evaluate the efficiency of selected IoT lightweight cryptography algorithms in a healthcare environment.

The findings will be addressed in Chapter 5, compared to the literature review, and applied to answer the research questions.

Chapter 5: Discussion

5.1 Introduction

The outcomes of the Systematic Literature Review and the Experimental Performance Testing evaluation of eight LWC algorithms were reported in Chapter 4. These results were collected through research methodologies obtained from an overview of previous studies, which are outlined in Chapter 3.

The purpose of Chapter 5 is to analyse the outcomes provided in Chapter 4 and explore their relevance to the challenges of IoT security and privacy in healthcare highlighted in the existing literature. These research results provide the answers to the research questions presented in Chapter 3.

This chapter is divided into the following sections. Section 5.2 responds to the research questions and analyses whether the outcomes indicate, progress, or confirm prior related studies provided in the literature review, thereby accomplishing the thesis's main objective. Section 5.3 contains a more in-depth discussion of the research's main findings. Finally, Section 5.4 offers recommendations for improving IoT privacy and security in the Healthcare sector based on the research outcomes.

5.2 Review of the Research Questions

The purpose of this thesis was to answer three research questions:

***Research Question 1 (RQ1):* What are the main IoT security and privacy issues in healthcare?**

According to the research findings, the main IoT security and privacy issues in healthcare were measured across three IoT layers: the Network Layer, the Perception Layer, and the Application Layer.

Research Question 2 (RQ2): What are the most important performance factors of IoT lightweight cryptographic algorithms in healthcare?

The research findings of this thesis revealed that the most significant factors of IoT LWC algorithms in healthcare are block size, key size, number of rounds, memory usage (RAM and ROM), energy consumption, and throughput.

Research Question 3 (RQ3): Which lightweight cryptographic algorithm would produce the best performance results?

The performance evaluation of LWC algorithms' experimental testing results indicate that RECTANGLE outperforms other LWC algorithms in terms of encryption and decryption operations performance for various payloads due to execution time, energy consumption, memory usage (RAM and ROM), and throughput.

5.3 Main IoT Security and Privacy Issues in Healthcare

There are two types of IoT security and privacy threats, which can be either passive or active. Attackers can acquire data without affecting network behaviour in passive threats; however, inactive threats intruders can block or slow down service administration (Alraja et al., 2021). Findings of this study show that the primary IoT security and privacy problems in healthcare were measured in three layers of IoT as follows:

1. Perception Layer security and privacy threats were found, including Denial of Service, Timing attack, Routing attack, Node capture, Fake node, Side channel attack, Insufficient cryptographic algorithms, Security parameters extraction, and Privacy Threats.
2. Network Layer security and privacy threats were found, including Man-in-the-Middle attacks, Denial of Service attacks, Congestion attacks, Eavesdropping, Replay attacks, and Routing attacks.
3. Application Layer Main security attacks and privacy issues including Firmware Replacement Attack, SQL injection, Phishing attack, Sniffing attack, Buffer overflow Data accessibility and authentication issues, data privacy, and identity issues were found.

The findings of this thesis support the literature review discussed in Chapter 2 that stated IoT security and privacy challenges were increasing in the healthcare sector (Alraja et al., 2021). This high level of consideration assumes that industries of IoT devices could also give more attention to this sector, as well as acknowledge individuals' security and privacy vulnerabilities. According to the research results, the following IoT security and privacy issues in healthcare were measured in three layers of IoT:

5.3.1 Perception Layer Issues

The literature review found that the IoT perception layer has convergence problems, which affect various security threats frequently, and providing sufficient security and privacy in this layer is challenging (Nasiri et al., 2019). Findings from the SLR of this research also show similar results.

Different types of data are captured in the perception layer via perception nodes and IoT devices. Perception nodes or sensors of various IoT devices collect data, including

characteristics and data linked to situations and surroundings, and regulate them in the data to generate commands to deliver to the perception layer.

If appropriate security countermeasures are not implemented, the data could be tracked, duplicated, and altered. LWC algorithms should be used in IoT devices due to their characteristics, which have limited memory capabilities and electrical power. Network threats could be recognised, and sensor data could be secured to ensure confidentiality, authentication, and accessibility.

The SLR findings indicate that the IoT perception layer is made up of sensors and sensor gates that could be impacted by a wide range of threats.

5.3.2 Network Layer Issues

According to the literature review, it is difficult to provide adequate security and privacy in this layer while maintaining the flexibility and expandability of the IoT network (Ren et al., 2017). This thesis' SLR outcomes reveal comparable results.

The potential of IoT tends to raise authentication security problems. Even though the network's core is comparatively protected, it could not be overloaded with invalid network connectivity, eavesdropping, harm to confidentiality and integrity, cyber theft, hacking, unauthorised access, malicious code, and malware. This layer could pay special attention to data confidentiality. DDOS attacks could be assumed, and security solutions should be applied to deal with them.

5.3.3 Application Layer Issues

Firmware Replacement Attacks, Phishing attacks, SQL Injection, Sniffing attacks, and Buffer Overflow are some of the most typical security and privacy vulnerabilities at the application layer. Issues with data privacy and identification, data accessibility, and authentication were discovered.
The study's findings suggest that the following application layer attacks are frequent:

Attack using a firmware replacement: An object's firmware, software, and operating system may all be updated to take advantage of novel functions while it is functioning or during maintenance. By substituting malicious objects, the attacker could interfere with the IoT device’s normal operation.

5.4 Important Performance Factors of Lightweight Cryptographic Algorithms for IoT in Healthcare

The findings of this study show that block size, key length, number of rounds, memory consumption (RAM and ROM), energy usage, and throughput are the most important factors of LWC algorithms for IoT in healthcare as follows:

The key size is important because medical IoT devices, such as node sensors, have very little storage. It is recommended to use the LWC algorithm that has a shorter key size and gives the identical degree of protection. The performance in terms of memory and power usage is more optimal due to the tiny key size (64, 96, or 128).

Another essential element for the LWC algorithm is the block size. Processing times can be decreased while power consumption falls with smaller block sizes. Additionally, medical sensors usually send short messages that contain essential clinical data; thus the smaller block size is more productive. An algorithm that is focused on hardware is SIMON (Beaulieu et al., 2015). RECTANGLE, an LWC algorithm based on SPN, is presented in Zhang et al. (2015). To accomplish fast implementation, it utilise a bit-slice mechanism with 64-bit block size.

LWC algorithms generally implement basic logic and mathematical calculations to adhere to resource limitations. As the outcome of performing simple procedures, the amount of rounds is accelerated. As a result, when choosing an LWC algorithm for the IoT, the number of rounds is one of the important factors. The PRINCE lightweight algorithm (Borghoff et al., 2012) is an LWC algorithm which attempts to enable encryption in a single cycle by utilising a few rounds, that requires quick completion.

Energy consumption is the performance element defining the viability of implementing IoT devices in healthcare. This is the amount of battery power required during the encryption or decryption procedures. When developing a real-time IoT-based healthcare monitoring system, the main driving factor considered is improving energy efficiency (Gosh et al., 2020). IoT in healthcare contains active devices which are powered by batteries and are made to detect and respond to environmental changes (Uslu et al., 2020). For instance, the battery-operated Wireless Body Sensor Nodes (WBSNs) are generally energy-constrained, it is necessary to create energy-efficient data security mechanisms, such as LWC algorithms (Zang et al., 2018).

Therefore, these LWC algorithms should be simple and have low energy consumption. The lower the power consumption, the better for the LWC algorithm. This metric is vital, especially for devices that gain power and energy from their surroundings, using a battery and storing a specific amount of energy. Also, many cases find it difficult to recharge or replace the batteries in the healthcare environment.

One of the important performance factors of IoT LWC algorithms in healthcare is memory usage (ROM/RAM). The IoT devices in healthcare should have minimal usage for RAM, which is employed by the IoT device to function its process, and ROM, which is utilised to store data on the IoT device. It helps the real-time medical monitoring procedures properly. The purpose of LWC algorithms is to provide security countermeasures that could perform with resource limited IoT medical devices by consuming less memory, computing resources, and power source.

The performance factor throughput is used for the number of plaintexts processed per second (bps). Here the higher it is, the better for the algorithm. Higher throughput is necessary for encryption/decryption in IoT devices with limited resources in healthcare, with large data transmissions, while low latency is essential for real-time monitoring of medical systems.

Because the power consumption is significantly reliant on the hardware, such as the circuit size and the processor, the size could become one of the main factors of the LWC algorithms. The parallel computing capability has a massive impact on throughput. The quick output of LWC algorithms could reduce energy consumption and increase battery life.

In terms of security, encryption is the technical basis of entire system security, LWC must employ a procedure that has been examined as providing a sufficient degree of security in cryptography. Even when the block and secret key lengths are placed to be shorter than in conventional cryptography to enable execution, using a reliable technique is still needed.

5.5 Discussion of Performance Evaluation Testing Results

It should be noted that most of the available studies focused on the challenges associated with optimising a specific platform. It is essential to recognize that if the LWC algorithm achieves the best performance on a dedicated platform, it could be superior on most other platforms. Furthermore, it may reach the usability limit of the platform's life cycle, which constantly changes at a rapid pace. In this study, the RECTANGLE algorithm was found to be the best. It is intended to improve security in constrained environments, such as IoT medical applications. It is currently being developed as a general LWC algorithm that is predicted to perform a key position in many future IoT applications. Furthermore, RECTANGLE is practically flexible, working well on a variety of platforms and being adaptable for innovative future use. This

research found that the RECTANGLE algorithm performs better than other LWC algorithms procedures in software implementation.

Performance evaluation of LWC algorithms was measured by this study in four areas, as follows:

Encryption/Decryption execution time

The encryption and decryption execution times are the one of the critical performance factors to consider in the innovation of the LWC algorithms for IoT in healthcare, and it is identified as the total time required to encrypt and decrypt particular file (Thabit et al., 2021).

According to the research findings of this thesis, RECTANGLE is the fastest with the most encryption operations on various file sizes. RECTANGLE and XTEA have the fastest decryption execution times when compared to other LWC algorithms.

For example, in the findings seen in Figure 4.66 and 4.67, the encryption and decryption times for the 16KB file, where all LWC algorithms compete in some way. In the remaining file sizes, MSEA and LEA have no challenges. PRESENT is the slowest of the rest of the LWC algorithms, performing the majority of procedures on 512KB and bigger files.

Energy consumption

MSEA and LEA algorithms had quite bad results considering the encryption and decryption processes. The findings in Section 4.3.1.b presented that RECTANGLE have the lowest power utilisation when compared to the others. RECTANGLE utilises the lowest electricity, 128-bit key, and 64-bit block length to encrypt. While the RECTANGLE algorithm was the most power-efficient, other algorithms produced more comparable results.

When this study's findings are analysed, it is possible to conclude that the algorithm's block size affects power usage. This is extremely significant for IoT devices that have limited resources. Encrypting small blocks is more effective. AES, MSEA, and LEA algorithms have the longest block length of 128 bits, whereas other LWC algorithms have a block length of 64 bits.

Furthermore, the larger increased key size, which could reduce energy efficiency. Obviously, the larger the key, the greater the security. However, in IoT applications, keys with lengths ranging from 80 to 128 bits are ideal. Choosing design in LWC algorithms in a simple and energy-efficient manner increases performance. This is demonstrated by energy-consuming formations like reduced mechanisms used in MSEA and LEA algorithms. It could be indicated that the RECTANGLE algorithm ranks first in these metrics because it contains simple functions like XOR and S-boxes.

Memory usage (RAM and ROM)

The findings in Section 4.4.2.c presented XTEA and RECTANGLE algorithms have the least amount of memory usage when compared to other algorithms in encryption/decryption processes.

The XTEA algorithm employs the smallest amount of memory for the 16KB file, followed by RECTANGLE and SIMON. RECTANGLE utilises only 2KB more than XTEA, while the other utilises nearly 40KB more for its procedures. All LWC algorithms have a rise in memory consumption for the remaining files, but as previously stated, this could be caused by the lack of the encryption. LEA and MSEA both use a similar size of memory; PRESENT decryption utileses the less memory; however, the findings are for the total LWC algorithms, the higher memory consumption could be recognised as the LWC algorithms' actual memory consumption. MSEA has not been mentioned because of its extremely high memory usage, which makes it incomparable to the other LWC algorithms.

The findings of this study, which are similar to Tasmine et al., (2018) show that the variation of key lengths could not affect the performance findings of XTEA and RECTANGLE.

Throughput

The average quantity of plain text is divided by the average encryption execution time when calculating the throughput of the encryption procedure, and the average quantity of cypher text is divided by the average decryption execution time when calculating the throughput of the decryption (Singh & Singla, 2018).

The comparison of encryption throughput results shows that RECTANGLE has the highest outcome in this study, followed by SIMON, XTEA, and PRINCE, in that order. The result indicates that the RECTANGLE algorithm outperforms the other techniques in encryption process throughput. Because the algorithm will run faster and use less energy, the throughput would increase.

Figure 4.74 illustrates the experiment's decryption output. In terms of decryption process throughput, the findings demonstrate that the RECTANGLE algorithm is superior to the other LWC algorithms. Except for RECTANGLE, it is clear that SIMON outperforms the other methods in terms of decryption throughput. PRESENT has a minor performance, as is evident.

It has been determined that RECTANGLE is faster than others and that this could be further enhanced by optimisation. This also applies to charge utilisation, as encryption and decryption times are correlated with the charge. RECTANGLE's memory utilisation is the only expensive component, but this aspect could potentially be optimised. RECTANGLE is the best lightweight

algorithm for IoT devices overall.

This research chooses to focus on eight LWC algorithms that have been implemented in software for constrained medical applications. The encryption/decryption execution time, energy consumption, memory usage, and throughput of all eight LWC algorithms were examined and analysed. Table 5.1 presents what scenarios each of the LWC algorithms could find their relevance. This can help the decision makers to choose which LWC algorithm could be suitable in different healthcare IoT devices.

Table 5.1 Performance Scenarios of the LWC algorithms ((+) acceptable, (-) unacceptable)

LWC Algorithms	Execution Time	Memory Usage (RAM and ROM)	Energy Consumption	Throughput
AES	(+ +)	(+ +)	(+)	(-)
PRESENT	(-)	(-)	(-)	(-)
MSEA	(- - -)	(- - -)	(- - -)	(-)
LEA	(- - -)	(- -)	(- - -)	(-)
XTEA	(+ +)	(+ + +)	(+ +)	(+)
SIMON	(+ +)	(+ + +)	(+ +)	(+ +)
PRINCE	(+ +)	(+ + +)	(+ +)	(-)
RECTANGLE	(+ + +)	(+ + +)	(+ + +)	(+ + +)

Focused on the evaluation, RECTANGLE was found to be efficient and suitable. It is predicted to play a significant position in many potential IoT devices in healthcare. According to the findings of this study, the RECTANGLE algorithm is the best LWC algorithm for IoT in healthcare, because it is fast, small, simple, and flexible.

5.6 Further Discussion

The following further discusses the difficulties of implementing IoT technologies in the healthcare environment.

Resource constraints: The key challenge in establishing a robust security mechanism for this technology is the medical IoT devices have restricted resources, such as power, processing, and storage capabilities. Due to the necessity for lightweight procedures, it is necessary to rethink the available protocols while enhancing simple calculation-free energy extraction methods (NIST, 2018).

Interoperability: All protocols deployed at different layers must offer straightforward, interoperable processes to standardise the global security mechanism that will be utilised on the

IoT. The architecture limitations could be used to describe how a mix of practical security requirements at each layer works with global procedures.

Breakpoints: The IoT design becomes more sensitive despite heterogeneous networks, topologies, and protocols (Haddadpajouh et al., 2019). Due to the current market between infrastructure and service quality and expenses, particularly for critical areas, hardware or firmware risks, processes, and requirements that carry redundancy into account should be developed. The concept of the IoT is getting more sensitive with the introduction of low-cost, low-power devices. It also refers to the use of security protocols, in addition to the actual operation of IoT. Therefore, it is rather essential to check the security of IoT devices, and the accuracy of monitoring and upgrades. The focus of current research should be on IoT security and data privacy challenges to manage, update, and provide reliable, resilient, and flexible software to large numbers of IoT devices.

Blockchain vulnerabilities: Blockchain technology is a valuable solution for the security of IoT. Blockchain technology, on the other hand, faces research problems in the areas of optimisation and effectiveness (Hassan et al., 2019). Private keys with a random limit cloud also are employed to access blockchain accounts.

5.7 Recommendations for Improving IoT Privacy and Security in Healthcare

Firstly, several techniques should be used to secure these IoT devices in healthcare. Perception layer protection of IoT medical devices is highly vital. The best way to accomplish this is to:

- Disable the usage of external devices like flash drives but only enable them to be used after authorisation.
- Restrict straightforward the Internet connectivity for critical equipment.
- Deactivate or isolate unused services, such as unprotected protocols and open ports.
- Keep updating the operating system of equipment on a regular schedule.
- Prevent unrelated nodes from gaining access
- Protecting data security and privacy transfer among nodes in security key exchange
- Utilization of LWC algorithms

Secondly, at the IoT network layer in the medical sector, reflective security recommendations and options can be focused on and addressed in 3 groups:

The wired networks of IoT in healthcare:

- Implement wired network security measures such as surveillance cameras, access control systems to track who enters the network, and protected zones to stop unauthorised connections.
- Using security methods such as firewalls and Intrusion Prevention System (IPS).

Remote connections:

- To authenticate authorised account holders' access to the remote network, utilise powerful authentication methods like Multi Factor Authentication (MFA).
- Allowing workers to connect to the company's network through protected channels.

Wireless networks:

- When connecting to a wireless network, utilise protected equipment and entry point setups.
- The implementation of cryptographic algorithms for authentication

Finally, the following should be considered when securing the IoT application layer in healthcare:

- Check the accuracy of the input data
- To reduce security breaches, write applications with reliable standard code
- Evaluating applications to discover weaknesses and develop appropriate action to mitigate harm
- Consumers must be authenticated
- Encrypt data during transmission
- Deactivate application ports that aren't needed for the normal procedure
- Isolation or rank of vulnerable software applications, such as cryptographic procedures, from other application modules

5.8 Conclusion

The findings of the SLR and the Experimental Performance Testing provided in Chapter 4, were discussed in Chapter 5, and the Research Questions raised by this thesis were addressed. The findings revealed severe issues regarding IoT security and privacy in healthcare. These problems were also discovered in the healthcare environment studied in this thesis, supporting the fact that IoT devices present a risk to consumers in healthcare.

This chapter presented steps that the broader sector may accept to improve IoT security and privacy in healthcare and reduce vulnerabilities, such as incorporating more practical security mechanisms of IoT, enacting tougher data regulatory requirements, and studying comprehensive data transmission techniques for presenting security and privacy. Finally, the chapter recommends effective measures that healthcare organisations and patients can take to effectively protect their sensitive data in medical IoT field.

Chapter 6: Conclusion

The first chapter of the thesis presented the research subject of IoT security and privacy in healthcare, highlighted the thesis structure, and explained why this research was conducted. The IoT, IoT security, Cryptography and IoT, and Lightweight Cryptography are covered in Chapter 2.

The main problems of IoT security and privacy in the healthcare sector mentioned in Chapter 2, motivated the development of research questions, which focuses on IoT vulnerabilities in healthcare and the LWC algorithms. Related research works and research methodologies were employed to develop the appropriate research methodologies to explore the research questions. The SLR research methodology and the Experimental Performance Testing research methodology utilised in this thesis is described in Chapter 3.

The results of utilising these research methodologies were provided in Chapter 4. These outcomes revealed IoT problems in healthcare, the important performance factors of LWC algorithms, and the best IoT algorithm with the best performance results. Additionally, several suggestions for how developers and users could strength security and privacy in the IoT in the medical system were addressed. The findings were further presented and analysed in Chapter 5 to connect to the literature review and to reply to the research questions presented by this thesis.

Chapter 6 summarises the thesis, recognising its contributions to the wider scope for IoT security and privacy in healthcare, LWC algorithms for IoT, and making recommendations for future studies.

6.1 Summary of Research

The main purpose of this thesis is to determine whether IoT devices in healthcare pose any privacy or security risks to patients and to find the best LWC algorithm to secure these devices. It investigated the main security and privacy problems of IoT and identified the most important performance factors of LWC algorithms for IoT in healthcare utilising the SLR research methodology. Furthermore, LWC algorithms currently offered for use in IoT devices were tested to determine which algorithm provides the best performance results for IoT privacy and security in healthcare.

The analysis for IoT device security and privacy threats in healthcare revealed weaknesses in three layers: perception, network, and application. Denial of Service, Timing attack, Routing attack, Node capture, Fake node, Side-channel attack, Insufficient cryptographic algorithms, Security parameters extraction, and Privacy Threats was discovered in the Perception Layer. The network layer’s security and privacy threats were DoS attacks, MitM attacks, Congestion

attacks, Eavesdropping, Replay attacks, and Routing attacks. Firmware Replacement Attacks, SQL Injection, Phishing attacks, Sniffing attacks, and Buffer Overflow are examples of application layer security and privacy issues. There were issues with data accessibility and authentication, as well as data privacy and identity.

The IoT vulnerabilities discovered in this thesis help to improve understanding of the possible consequences of weak IoT design. The same IoT devices designed with the user's privacy and security are more vulnerable to popular attacks, eavesdropping, unauthorised access, and device manipulation.

The findings of SLR show that block size, key size, rounds, memory consumption (RAM and ROM), energy usage, and throughput are the most important factors of LWC algorithms for IoT in the medical sector.

The findings of the evaluation of experimental performance testing indicate that the RECTANGLE algorithm outperforms other LWC algorithms in the performance of execution time, energy consumption, memory usage (RAM and ROM), and throughput of multiple payloads.

6.2 Research Limitations

Although numerous experiments and data collection were conducted, several limitations were noticed during the completion of this thesis. Some of the limitations were:

- This thesis could have used more microcontroller devices like the Arduino UNO. It would have been informative to work with two or more microcontroller devices and compare their output to others.

- Some significant factors, such as code size and cycle count, caused the use of specialised hardware not included in the scope.

- The budget for the study was limited, which reduced the scope of the research. It became clear during the completion of this work that other physical equipment could have facilitated the experiment.

6.3 Recommendations and Contributions

This thesis has highlighted the present situation of IoT security and privacy in the healthcare sector. It has confirmed the issues discovered and listed IoT medical devices. Recognizing that deploying IoT in healthcare could adversely affect security and privacy shows the significance of raising awareness of these challenges. It is crucial to push for better regulations to protect patients and more tools to inform users. Additionally, this research shows that focusing educational initiatives on patients and those with less formal education can significantly improve public knowledge of these issues in the healthcare industry.

Implementing more modern standards to lessen the level of risk that IoT devices currently face. IoT devices should include fundamental security measures. It may be possible to secure the protection of patients' data by placing more emphasis on implementing and advertising security and privacy measures than on offering cheaper IoT devices.

Consider taking preventative measures that do not require additional components, such as choosing secure login credentials, and protecting the household Wi-Fi with the most recent protocols, as they will all lessen the potential of any security and privacy issues.

6.4 Future Research

There will need to be more than a comprehensive LWC algorithm due to the increase of IoT devices. It covered even though specific lightweight algorithms in this work might only apply in specified contexts. There might never be a unique, efficient, lightweight algorithm that can be used for all IoT device applications in healthcare. Every application will have different needs, which must be considered while choosing a suitable algorithm. Other lightweight algorithms will need to correspond to these boundaries regarding tasks.

Many of these applications have already been the research subject, but as IoT spreads into new fields, potential innovations keep emerging. These applications, or a generic variant of them, must first be recognised. Following their evaluation, simple algorithms appropriate for the application can be implemented. Since they can be more appropriate for particular lightweight environments/applications, these additional design patterns must also be considered.

6.5 Conclusion

The IoT is the technology that can lessen or even eliminate these problems. However, despite its enormous potential and capabilities, IoT still has privacy and security concerns that could affect the healthcare system. Through automated data gathering and analysis, IoT in healthcare collects private information, which raises security and privacy concerns. These challenges provide significant obstacles to the full development and application of IoT and present many vulnerabilities.

Recognising security and privacy issues in healthcare is essential for dealing with its complexity and assisting the industry in taking advantage of its potential. Because consumers provide personal information about their health, privacy and safety risks are severe issues in the healthcare industry. The design of the IoT system should have an effective security architecture that considers every layer of the IoT system, from the devices to the applications.

This study aims to draw attention to potential IoT privacy and security problems in the healthcare environment. The three primary layers of IoT security and privacy challenges in healthcare were examined in this thesis. The SLR research methodology is used to find block size, key size, number of rounds, memory consumption (RAM and ROM), power usage, and throughput are the most important factors of LWC algorithms for IoT in healthcare.

The LWC algorithms are utilised to verify complete security for resource-limited devices. Eight lightweight encryption algorithms were selected for this thesis, and the Raspberry Pi 3 device was used to test each one's performance. The execution time, energy consumption, memory utilisation (RAM and ROM), and throughput of encryption and decryption procedures were all evaluated for various payloads.

This study examined IoT security and privacy vulnerabilities and their underlying causes, which could significantly affect how widely they are implemented in the healthcare sector. This paper's contents will help technology developers and healthcare service providers identify many security and privacy problems and develop secure solutions taking them into account. In addition, the large proportion of the safety concerns described above is addressed, protecting patient information regarding privacy and confidentiality. Thus, most IoT healthcare issues can be managed with the necessary actions. Also, the RECTANGLE algorithm, one of the LWC algorithms tested, is the best choice for IoT software implementation in medical applications, promising exciting future research.

References

Aarika, K., Meriem, B., Rachida, A. A., Elfilali, S., & Habib, B. (2020). Perception layer security in the Internet of things. *Procedia Computer Science*. 175. 591-596. https://doi.org/10.1016/j.procs.2020.07.085

Abdullah, A., Hamad, R., Abdulrahman, M., Moala, H., & Elkhediri, S. (2019). CyberSecurity: A Review of Internet of Things (IoT) Security Issues, Challenges and Techniques. *2nd International Conference on Computer Applications & Information Security (ICCAIS).* pp. 1-6. https://doi.org/10.1109/CAIS.2019.8769560

Abed, S., Jaffal, R., Mohd, B. J., & Al-Shayeji, M. (2021). An analysis and evaluation of lightweight hash functions for blockchain-based IoT devices. *Cluster Computing*. 24. 4. 3065–3084. https://doi.org/10.1007/s10586-021-03324-1

Aboshosha, B., Dessouky, M., Ramadan, R., & El-Sayed, A. (2020). Evaluation of Lightweight Block Ciphers Based on General Feistel Structure (GFS). 2. 39-47

Abouelmehdi, K., Beni-Hessane, A. & Khaloufi, H. (2018). Big healthcare data: preserving security and privacy. *J Big Data* **5**, 1. https://doi.org/10.1186/s40537-017-0110-7

Ajami, S., & Rajabzadeh, A., (2013). Radio Frequency Identification (RFID) technology and patient safety. *J Res Med Sci*. 18(9):809-13.

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/10.1016/j.jnca.2017.04.002

Alagar, V., Alsaig, A., Ormandjiva, O., & Wan, K. (2018). Context-Based Security and Privacy for Healthcare IoT. *IEEE International Conference on Smart Internet of Things (SmartIoT).* pp. 122-128. https://doi.org/10.1109/SmartIoT.2018.00-14

Alassaf, N., Gutub, A., Parah, S.A., Ghamdi, M. A. (2019). Enhancing speed of SIMON: A light-weight-cryptographic algorithm for IoT applications. *Multimed Tools Appl*. 78. 32633–32657. https://doi.org/10.1007/s11042-018-6801-z

Alem, Č., Adisa, H., & Karahodza, B. (2021). Wireless communication technologies for the Internet of Things. 1. 1-14. https://doi.org/10.54327/set2021/v1.i1.3

Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2015) Internet

of things: A survey on enabling technologies, protocols, and applications. *IEEE Communications Surveys & Tutorials*. vol. 17 no. 4. pp. 2347–2376. https://doi.org/10.1109/COMST.2015.2444095

Ali, S., Khan, M.A., Ahmad, J., Malik, A.W., & Rahman, A.U. (2018). Detection and prevention of Black Hole Attacks in IOT & WSN. *2018 Third International Conference on Fog and Mobile Edge Computing (FMEC).* 217-226. https://doi.org/10.1109/FMEC.2018.8364068

Alkhatib, S., Waycott, J., Buchanan, G., & Bosua, R. (2018). Privacy and the Internet of Things (IoT) Monitoring Solutions for Older Adults: A Review. *Connecting the System to Enhance the Practitioner and Consumer Experience in Healthcare: Selected Papers from the 26th Australian National Health Informatics Conference (HIC 2018).* Vol. 252, pp. 8-14). https://doi.org/10.3233/978-1-61499-890-7-8

Almheiri, A., & Maamar, Z. (2021). IoT Protocols – MQTT versus CoAP. *In Proceedings of the 4th International Conference on Networking, Information Systems & Security*. Association for Computing Machinery. 19. 1–5. https://doi.org/10.1145/3454127.3456594

Alraja, M., Barhamgi, H., Rattrout, A., & Barhamgi, M. (2021). An integrated framework for privacy protection in IoT - Applied to smart healthcare. Computers & Electrical Engineering. 91. 107060. https://doi.org/10.1016/j.compeleceng.2021.107060

Alsubaei, F., Abuhussein, A., & Shiva, S. (2017). Security and Privacy in the Internet of Medical Things: Taxonomy and Risk Assessment. *Proceedings - 2017 IEEE 42nd Conference on Local Computer Networks Workshops, LCN Workshops 2017*, 112-120. https://doi.org/10.1109/LCN.Workshops.2017.72

Alsubaei, M. (2019). Smart Home Systems Based on Internet of Things. *Internet of Things (IoT) for Automated and Smart Applications.* IntechOpen. https://doi.org/10.5772/intechopen.84894

Amaraweera, S., & Halgamuge, M. (2019). Internet of Things in the Healthcare Sector: Overview of Security and Privacy Issues. https://doi.org/10.1007/978-3-030-18075-1_8

Anca, J., Pasika, R., & Lina, X. (2019). *Introduction to IoT Security*. https://doi.org/10.1002/9781119471509.w5GRef260

Anil, C., & Thaier, H. (2018). Security and Privacy Issues with IoT in Healthcare. EAI Endorsed Transactions on Pervasive Health and Technology. 4. 155079. https://doi.org/10.4108/eai.13-

7-2018.155079

Anwar, A., Mahmood, A. N., & Tari, Z. (2015). Identification of vulnerable node clusters against false data injection attack in an AMI based Smart Grid. *Information Systems.* Volume 53. 201-212. https://doi.org/10.1016/j.is.2014.12.001

Argaw, S. T., Troncoso-Pastoriza, J. R., Lacey, D. Florin, M., Calcavecchia, F., Anderson, D., Burleson, W., Vogel, J., O'Leary, C., Eshaya-Chauvin, B., & Flahault, A. (2020). Cybersecurity of Hospitals: discussing the challenges and working towards mitigating the risks. *BMC Med Inform Decis Mak* 20, 146. https://doi.org/10.1186/s12911-020-01161-7

Arora, S., Yttri, J., & Nilse, W. (2014). Privacy and Security in Mobile Health (mHealth) Research. *Alcohol research: current reviews*, *36*(1), 143–151

Austin, Z., & Sutton, J. (2014). Qualitative research: getting started. *Can J Hosp Pharm.* 67(6):436-40. https://doi.org/10.4212/cjhp.v67i6.1406

Bajrić, S. (2020). Data Security and Privacy Issues in Healthcare. *Applied Medical Informatics*. *42*(1). 19-27. Retrieved from https://ami.info.umfcluj.ro/index.php/AMI/article/view/702

Beaulieu, R., Douglas, S., Jason S., Stefan T., Bryan W., & Louis W. (2014). The SIMON and SPECK block ciphers on AVR 8-bit microcontrollers. In International Workshop on Lightweight Cryptography for Security and Privacy. pp. 3–20.

Bhatt, D. P., Raja, L., Sharma, S. (2020). Light-weighted cryptographic algorithms for energy efficient applications. *Journal of Discrete Mathematical Sciences and Cryptography*. 23:2, pages 643-650.

Bouayad, L., Ialynytchev, A., & Padmanabhan, B. (2017). Patient Health Record Systems Scope and Functionalities: Literature Review and Future Directions. *J Med Internet Res.* 19(11):e388. https://doi.org/10.2196/jmir.8073

Bogdanov, A., Knudsen, L., Leander, G., Paar, C., Poschmann, A., Robshaw, M., & Seurin, Y., & Vikkelsoe, C. (2007). PRESENT: an ultra-lightweight block cipher. Lect Note. *Comput. Sci.* 4727. 450-466. https://doi.org/10.1007/978-3-540-74735-2_31

Booth, A. (2016). Searching for qualitative research for inclusion in systematic reviews: a structured methodological review. *Syst Rev* 5. 74. https://doi.org/10.1186/s13643-016-0249-x

Borghoff, J. Canteaut, A., Güneysu, T., Kavun, E. B., Knezevic, M., Knudsen, L. R., Leander,

G., Nikov, V., Paar, C., Rechberger, C., Rombouts, P., Thomsen, S. S., & Yalçın, T. (2012). PRINCE – A Low-Latency Block Cipher for Pervasive Computing Applications. *Lecture Notes in Computer Science.* vol 7658. https://doi.org/10.1007/978-3-642-34961-4_14

Botta, M., Simek, M., & Mitton, N. (2013). Comparison of hardware and software based encryption for secure communication in wireless sensor networks. *36th International Conference on Telecommunications and Signal Processing (TSP).* pp. 6-10. https://doi.org/10.1109/TSP.2013.6613880

Bouayad, L., Ialynytchev, A., & Padmanabhan, B. (2017). Patient Health Record Systems Scope and Functionalities: Literature Review and Future Directions. *J Med Internet Res.* 19(11):e388. https://doi.org/10.2196/jmir.8073

Bui, D. H., Puschini, D., Bacles-Min, S., Beigné E., & Tran, X. T. (2017). AES Datapath Optimization Strategies for Low-Power Low-Energy Multisecurity-Level Internet-of-Things Applications. *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 25. no. 12. pp. 3281-3290. https://doi.org/10.1109/TVLSI.2017.2716386

Burhan, M., Rehman, R. A., Khan, B., & Kim, B, S. (2018). IoT Elements, Layered Architectures and Security Issues: A Comprehensive Survey. *Sensors (Basel).* 18(9):2796. https://doi.org/10.3390/s18092796

Calihman, A. (2019, January 30). *Architectures in the IoT Civilization.* Retrieved from: https://www.netburner.com/learn/architectural-frameworks-in-the-iot-civilization/

Chacko, A., & Hayajneh, T. (2018). Security and Privacy Issues with IoT in Healthcare. PHAT. EAI. https://doi.org/10.4108/eai.13-7-2018.155079

Cilliers, L. (2020). Wearable devices in healthcare: Privacy and information security issues. *Health Inf Manag.* 49(2-3):150-156. https://doi.org/10.1177/1833358319851684

Claeys, T., Vučinić, M., Watteyne, T., Rousseau, F., Tourancheau, B., (2021) Performance of the Transport Layer Security Handshake Over 6TiSCH. *Sensors (Basel).* 21(6):2192. https://doi.org/10.3390/s21062192

Devibala, A. (2019). A Survey on Security Issues in Iot for Blockchain Healthcare. (2019). *IEEE International Conference on Electrical, Computer and Communication Technologies (ICECCT)*. pp. 1-7. https://doi.org/10.1109/ICECCT.2019.8869253.

Djenna, A., & Saïdouni, D. E. (2018). Cyber Attacks Classification in IoT-Based-Healthcare

Infrastructure. *2nd Cyber Security in Networking Conference (CSNet).* pp. 1-4, doi: https://doi.org/10.1109/CSNET.2018.8602974

Dutta, N. S., & Chakraborty, S. (2020). A survey on implementation of lightweight block ciphers for resource constraints devices. *Journal of Discrete Mathematical Sciences and Cryptography*. https://doi.org/10.1080/09720502.2020.1766764

Dworkin, M., Barker, E., Nechvatal, J., Foti, J., Bassham, L., Roback, E., & Dray, J. (2001). Advanced Encryption Standard (AES), *Federal Inf. Process. Stds.* (NIST FIPS). https://doi.org/10.6028/NIST.FIPS.197

Elhoseny, M., Thilakarathne, N. N., Alghamdi, M. I., Mahendran, R.K., Gardezi, A.A., Weerasinghe, H., & Welhenge, A. (2021). Security and Privacy Issues in Medical Internet of Things: Overview, Countermeasures, Challenges and Future Directions. Sustainability 13, 11645. https://doi.org/10.3390/ su132111645

Ertaul, L. (2017). Performance Analysis of CLEFIA , PICCOLO , TWINE Lightweight Block Ciphers in IoT Environment. *International Conference on Security and Management (SAM).* (WorldComp). pp. 25–31.

Fazeldehkordi, E., Owe, O., & Noll, J. (2019). Security and Privacy in IoT Systems: A Case Study of Healthcare Products. *13th International Symposium on Medical Information and Communication Technology (ISMICT).* pp. 1-8, https://doi.org/10.1109/ISMICT.2019.8743971.

Federal Trade Commission (FTC). (2015). Internet of Things: Privacy and security in a connectedworld. *Journal of Current Issues in Media & Telecommunications*. 7(2). 155–188.

Fips, N. (2001). 197: Announcing the advanced encryption standard (AES). *Technol. Lab. Natl. Inst. Stand.* pp. 8–12.

Gafurov, K., & Chung, T. M. (2019). Comprehensive survey on Internet of Things, architecture, security aspects, applications, related technologies, economic perspective, and future directions. *Journal of Information Processing Systems.* vol. 15, no. 4. pp. 797-819. https://doi.org/10.3745/JIPS.03.0125

Ghosh, A., Raha, A., & Mukherjee, A. (2020). Energy-Efficient IoT-Health Monitoring System using Approximate Computing. Internet of Things. 9. https://doi.org/10.1016/j.iot.2020.100166.

Gibson, D. (2014). *CompTIA Security+ get certified get ahead SYO-401 study guide.* Virgina Beach. YCDA, LLC.

Gill, S. S., Tuli, S., Xu, M., Singh, I., Singh, K.V., Lindsay, D., Tuli, S., Smirnova, D., Singh, M., Jain, U., Pervaiz, H., Sehgal, B., Kaila, S. S., Misra, S., Aslanpour, M. S., Mehta, H., Stankovski, V., & Garraghan, P. (2019). Transformative effects of IoT, Blockchain and Artificial Intelligence on cloud computing: Evolution, vision, trends and open challenges. *Internet of Things*, Volume 8, 100118. https://doi.org/10.1016/j.iot.2019.100118

Greenberg, A. (Sept 2020). *Kids' Smartwatches Are a Security Nightmare Despite Years of Warnings.* Wired. https://www.wired.com/story/kid-smartwatch-security-vulnerabilities/

Großschädl, J., Tillich, S., Rechberger, C., Hofmann, M., & Medwed. M. (2007). Energy evaluation of software implementations of block ciphers under memory constraints. *In Proceedings of the conference on Design, automation and test in Europe*. EDA Consortium.

Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of things (IoT): A vision, architectural elements, and future directions. *Future generation computer systems*. 29(7):1645-1660. https://doi.org/10.1016/j.future.2013.01.010

Gurpreet, S., & Supriya, K. (2013). A Study of Encryption Algorithms (RSA, DES, 3DES and AES) for Information Security. *International Journal of Computer Applications*. 67. 33-38. https://doi.org/10.5120/11507-7224

Hajar, M. S., Omar, M., & Kalutarage, H. K. (2021). A survey on wireless body area networks: architecture, security challenges and research opportunities. Computers & Security. Volume 104. https://doi.org/10.1016/j.cose.2021.102211

Hosseinzadeh, J., & Bafghi, A.G. (2017). Software Implementation And Evaluation Of Lightweight Symmetric Block Ciphers Of The Energy Perspectives And Memory.

Hong, D., Lee, J. K., Kim, D. C., Kwon, D., Ryu, K. H., & Lee, D. G. (2014). LEA: A128-bit block cipher for fast encryption on common processors. *Lect. Notes Comput. Sci.* vol. 8267 LNCS. pp. 3–27.

Heron, S. (2009). Advanced Encryption Standard (AES). *Network Security*. Volume 2009. Issue 12. Pages 8-12. https://doi.org/10.1016/S1353-4858(10)70006-4

Hurrah, N. N., Parah, S. A., Sheikh, J. A., Al-Turjman, F., Muhammad, K. (2019). Secure data transmission framework for confidentiality in IoTs. *Ad Hoc Networks*. Volume 95. 101989. https://doi.org/10.1016/j.adhoc.2019.101989

Ianculescu, M., Coardoș, D., Bica, O., & Vevera, V. (2020). Security and Privacy Risks for Remote Healthcare Monitoring Systems. *International Conference on e-Health and Bioengineering (EHB).* pp. 1-4. https://doi.org/10.1109/EHB50910.2020.9280103

Imran, M.A., Zoha, A., Zhang, L., & Abbasi, Q. H. (2020). Grand Challenges in IoT and Sensor Networks. *Front. Comms. Net.* 1:619452. https://doi.org/10.3389/frcmn.2020.619452

Internet of Things. (2022). In English Cambridge Dictionary. Retrieved from https://dictionary.cambridge.org/dictionary/english/internet-of-things

Jap, D., & Breier, J. (2015). Differential Fault Attack on LEA. *Information and Communication Technology. Lecture Notes in Computer Science.* vol 9357. https://doi.org/10.1007/978-3-319-24315-3_27

Jia, X., Feng, Q., Fan, T., & Lei, Q. (2012). RFID technology and its applications in Internet of things (IoT). *2nd international conference on consumer electronics, communications and networks (CECNet)*. 1282-1285. https://doi.org/10.1109/CECNet.2012.6201508

Karunarathne, S. M., Saxena, N. & Khan, M. K. (2021). Security and Privacy in IoT Smart Healthcare. IEEE Internet Computing. vol. 25, no. 4, pp. 37-48. https://doi.org/10.1109/MIC.2021.3051675.

Kelly, J.T., Campbell, K. L., Gong, E., & Scuffham, P. (2020). The Internet of Things: Impact and Implications for Health Care Delivery. *J Med Internet Res.* 22(11):e20135. https://doi.org/10.2196/20135

Kevin, C., Amanda, M., & Conor, G. (2012). Near Field Communication. *International Journal of Electrical and Computer Engineering (IJECE).* 2. https://doi.org/10.11591/ijece.v2i3.234

Kiran, D. R. (2019). Chapter 35 - Internet of Things. *In Production Planning and Control*. 495–513. Butterworth-Heinemann. https://doi.org/10.1016/B978-0-12-818364-9.00035-4

Kliarsky, A. (2017). *Detecting attacks against the Internet of Things.* Retrieved from: https://www.sans.org/reading-room/whitepapers/internet/detecting-attacks-039-internet-things-039-37712

Kocakulak, M., & Butun, I. (2017). An overview of Wireless Sensor Networks towards internet of things. *IEEE 7th Annual Computing and Communication Workshop and Conference (CCWC).* 2017, pp. 1-6. https://doi.org/10.1109/CCWC.2017.7868374

Kuan, Z., Xiaohui, L., Rongxing, L., & Xuemin, S. (2014). Sybil Attacks and Their

Defenses in the Internet of Things. *Internet of Things Journal*. IEEE. 1. 372-383. https://doi.org/10.1109/JIOT.2014.2344013

Kumar, R., Mishra, K. K., Tripathi, A., Tomar, A., & Singh, S. (2014). MSEA: Modified Symmetric Encryption Algorithm. pp. 1–14.

Kumar, P., Rawat, S., Choudhury, T., & Pradhan, S. (2016). A performance based comparison of various symmetric cryptographic algorithms in run-time scenario. *International Conference System Modeling & Advancement in Research Trends (SMART).* pp. 37-41. https://doi.org/10.1109/SYSMART.2016.7894485

Kumar, G. (2016). Denial of service attacks – an updated perspective. Systems Science & Control Engineering. 4:1. 285-294. https://doi.org 10.1080/21642583.2016.1241193

Kumar, N., Madhuri, J., & ChanneGowda, M. (2017). Review on security and privacy concerns in internet of things. *International Conference on IoT and Application (ICIOT)* (pp. 1-5). IEEE.

Kuznetsov, A., Gorbenko, Y., Andrushkevych, A., & Belozersev, I. (2017). Analysis of block symmetric algorithms from international standard of lightweight cryptography ISO/IEC 29192-2. *4th International Scientific-Practical Conference Problems of Infocommunications.* pp. 203-206. https://doi.org/10.1109/INFOCOMMST.2017.8246380

Landaluce, H., Arjona, L., Perallos, A., Falcone, F., Angulo, I., & Muralter, F. (2020). A Review of IoT Sensing Applications and Challenges Using RFID and Wireless Sensor Networks. Sensors. *Basel*. 20(9):2495. https://doi.org/10.3390/s20092495

Lee, P., Clark, A., Bushnell, L., & Poovendran, R. (2014). A passivity framework for modeling and mitigating wormhole attacks on networked control systems. IEEE Transactions on Automatic Control. 59 (12). 3224–3237. https://doi.org/10.48550/arXiv.1312.1397

Li, J., Zhu, X., Tang, N., & Sui, J. (2010). Study on ZigBee network architecture and routing algorithm. *2nd International Conference on Signal Processing Systems, 2*, V2-389-V2-393

Li, S., Xu, L.D., & Zhao, S. (2015). The internet of things: a survey. *Inf Syst Front* 17, 243–259. https://doi.org/10.1007/s10796-014-9492-7

Li, X., Dai, H. N., Wang, Q., Imran, M., Li, D., & Imran, M. A., (2020). Securing Internet of Medical Things with Friendly-jamming schemes. *Comput Commun.* 160:431-442. https://doi.org/10.1016/j.comcom.2020.06.026

Lin, J., Yu, W., Nan, Z., Xinyu, Y., Hanlin, Z., & Wei, Z., (2017). A survey on Internet of Things: Architecture, enabling technologies, security and privacy, and applications, IEEE Internet of Things Journal, 4(5). 1125–1142. https://doi.org/10.1109/JIOT.2017.26832

Lindqvist, U., & Neumann, P. G. (2017). The future of the Internet of Things. *Communications of the ACM*, 60(2), 26–30. https://doi.org/10.1145/3029589

LoRa Alliance. (2017). *Lorawan 1.1 specification*. Technical specification.

Luhach, A.K., & Kumar, S. (2016). Layer Based Security in Internet of Things: Current Mechanisms, Prospective Attacks, and Future Orientation. *Communications in Computer and Information Science.* vol 628. https://doi.org/10.1007/978-981-10-3433-6_107

Mahanty, A., Singh, G., Som, S., & Khatri, S. K. (2018). Security Issues and Challenges in Perception Layer of Smart Healthcare. *7th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO).* pp. 639-644, https://doi.org/10.1109/ICRITO.2018.8748684

Mary, S., Zayaraz, G., Kaniappan, V., & Vijayalakshmi, V. (2021). Lightweight Cryptography Algorithms for Internet of Things enabled Networks: An Overview. *Journal of Physics: Conference Series.* 1717. 012072. https://doi.org/10.1088/1742-6596/1717/1/012072

Maple, C. (2017). Security and privacy in the Internet of things. *Journal of Cyber Policy*. 2:2. 155-184. https://doi.org/10.1080/23738871.2017.1366536

McGraw, D., & Mandl, K.D. (2021). Privacy protections to encourage use of health-relevant digital data in a learning health system. *npj Digit. Med.* **4.** 2. https://doi.org/10.1038/s41746-020-00362-8

McKay, K.., Bassham, L.., Sonmez T. M., & Mouha, N. (2017). Report on Lightweight Cryptography. *NIST Interagency/Internal Report (NISTIR).* National Institute of Standards and Technology. https://doi.org/10.6028/NIST.IR.8114

Mohammad, S. M. (2020). Security and Privacy Concerns of the Internet of Things (IoT) in IT and its Help in the Various Sectors across the World. *International Journal of Computer Trends and Technology*. 68(4). 263-272.

Montenegro, G., Kushalnagar, N., Hui, J., & Culler, D. (2007). Transmission of ipv6 packets over IEEE 802.15. 4 networks. *Internet proposed standard RFC*. 4944:130.

Moradi, A., Poschmann, A., Ling, S., Paar, C., Wang, H. (2011). Pushing the Limits: A Very

Compact and a Threshold Implementation of AES. *Lecture Notes in Computer Science.* vol 6632. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-20465-4_6

Moriai, S. (2015). Japan CRYPTREC Activity on Lightweight Cryptography. *Cryptography Research and Evaluation Commitees.* pp. 1–23.

Munn, Z., Peters, M.D.J., Stern, C., Tufanaru, C., McArthur, A., & Aromataris, E. (2018). Systematic review or scoping review? Guidance for authors when choosing between a systematic or scoping review approach. *BMC Med Res Methodol* **18**, 143 https://doi.org/10.1186/s12874-018-0611-x

Nasiri, S., Sadoughi, F., Tadayon, M. H., & Dehnad, A. (2019). Security Requirements of Internet of Things-Based Healthcare System: a Survey Study. *Acta Informatica Medica.* 27. 253-258. https://doi.org/10.5455/aim.2019.27.253-258

National Institute for Standards and Technology (NIST). (d.n.). Lightweight Cryptography Project. Available online: https://csrc.nist.gov/Projects/lightweight-cryptography (accessed on 8 September 2021).

Nausheen, F., & Begum, S. H. (2018). Healthcare IoT: Benefits, vulnerabilities and solutions. *2nd International Conference on Inventive Systems and Control (ICISC).* pp. 517-522, https://doi.org/10.1109/ICISC.2018.8399126

Nishant, K., Madhuri, J., & Manjunath, C. (2017). Review on security and privacy concerns in Internet of Things. 1-5. https://doi.org/10.1109/ICIOTA.2017.8073640

Nguyen, K. T., Laurent, M., & Oualha, N. (2015). Survey on secure communication protocols for the Internet of Things. *Ad Hoc Networks*. 32. 17–31. https://doi.org/10.1016/j.adhoc.2015.01.006

Norah, A., Basem, A., & Adnan, G. (2017). Applicable Light-Weight Cryptography to Secure Medical Data in IoT Systems. *Journal of Research in Engineering and Applied Sciences (JREAS)*. 2. 50-58. https://doi.org/10.46565/jreas.2017.v02i02.002

Okello, W. J., Liu, Q., Ali Siddiqui, F., & Zhang, C. (2017). A survey of the current state of lightweight cryptography for the Internet of things. International Conference on Computer, *Information and Telecommunication Systems (CITS).* pp. 292-296. https://doi.org/10.1109/CITS.2017.8035317

Obogo, J. (2020). Security and Privacy Challenges in Healthcare IoT Devices For Patient Treatment and Monitoring. https://doi.org/10.13140/RG.2.2.13613.31206

Omrani, T., Rhouma, R., & Layth, S. (2018). Lightweight Cryptography for Resource-Constrained Devices: A Comparative Study and Rectangle Cryptanalysis: *Third International Conference.* https://doi.org/10.1007/978-3-319-97749-2_8

Pal P., Sambhakar, S., Dave, V., Paliwal, S. K., Paliwal, S., Sharma, M., Kumar, A., Dhama, N. (2021). A review on emerging smart technological innovations in healthcare sector for increasing patient's medication adherence. *Global Health Journal*. Volume 5. Issue 4. Pages 183-189. https://doi.org/10.1016/j.glohj.2021.11.006

Palmer, D. (2017, July). *175,000 IoT cameras can be remotely hacked thanks to flaw, says security researcher*. ZDNet. Retrieved from: https://www.zdnet.com/article/175000-iot-cameras-can-be-remotely-hacked-thanks-to-flaw-says-security-researcher/

Panagiotis, I., Grammatikis, R., Panagiotis, G., & Moscholios, I, D. (2019). Securing the Internet of Things: Challenges, threats and solutions. Internet of Things. Volume 5. 41-70. https://doi.org/10.1016/j.iot.2018.11.003

Paré, G., & Kitsiou, S. (2017 Feb 27). Chapter 9: Methods for Literature Reviews. *Handbook of eHealth Evaluation: An Evidence-based Approach*. University of Victoria. Available from: https://www.ncbi.nlm.nih.gov/books/NBK481583/

Patil, H. K., & Chen, T. M. (2017). Wireless Sensor Network Security: The Internet of Things, *Computer and Information Security Handbook*. (Third Edition). Pages 317-337. https://doi.org/10.1016/B978-0-12-803843-7.00018-1

Patil, P., Narayankar, P., Narayan D.G., & Meena S. M. (2016). A Comprehensive Evaluation of Cryptographic Algorithms: DES, 3DES, AES, RSA and Blowfish, *Procedia Computer Science*. 78. 617-624. https://doi.org/10.1016/j.procs.2016.02.108

Paulsen, C., & Byers, R. (2019). Glossary of Key Information Security Terms. *NIST Interagency/Internal Report (NISTIR)*, National Institute of Standards and Technology, Gaithersburg. MD. https://doi.org/10.6028/NIST.IR.7298r3

Peterson, L. L., & Davie, B. S. (2012). *Computer networks: a systems approach*. Amsterdam. Morgan Kaufmann.

Pradhan, B., Bhattacharyya, S., & Pal, K. (2021). IoT-Based Applications in Healthcare Devices. *Journal of Healthcare Engineering*. vol. 2021. Article ID 6632599. https://doi.org/10.1155/2021/6632599

Radovan, M., Golub, B., & Daimler, A. (2017). Trends in IoT security. *40th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*. 1302. https://doi.org/10.23919/MIPRO.2017.7973624

Raspberry Pi. (n.d.). Raspberry Pi 3 Model B - Raspberry Pi. Available: https://www.raspberrypi.org/products/raspberry-pi-3-model-b/

Raza, S., Seitz, L., Sitenkov, D., & Selander, G. (2016). S3K: Scalable Security with Symmetric Keys—DTLS key establishment for the Internet of Things. *IEEE Transactions on Automation Science and Engineering, Automation Science and Engineering*. 3. 1270. https://doi.org/10.1109/TASE.2015.2511301

Ren, Z., Liu, X., Ye, R., & Zhang, T. (2017). Security and privacy on internet of things. 7th IEEE International Conference on Electronics Information and Emergency Communication (ICEIEC). pp. 140-144. https://doi.org/1109/ICEIEC.2017.8076530

Rivas, M.L. (2017). *Securing the home IoT network.* Retrieved from: https://www.sans.org/reading-room/whitepapers/internet/securing-home-iot-network-37717

Rizvi, S., Pipetti, R., McIntyre, N., Todd, J., & Williams, I. (2020). Threat model for securing internet of things (IoT) network at device-level. *Internet of Things (Netherlands)*. *11*. 100240. https://doi.org/10.1016/j.iot.2020.100240

Rughoobur, P., & Nagowah, L. (2017). A lightweight replay attack detection framework for battery depended IoT devices designed for healthcare. *International Conference on Infocom Technologies and Unmanned Systems (Trends and Future Directions) (ICTUS).* pp. 811-817. https://doi.org/10.1109/ICTUS.2017.8286118

Saba, T., Haseeb, K., Ahmed, I., Rehman, A. (2020). Secure and energy-efficient framework using Internet of Medical Things for e-healthcare. *J Infect Public Health.* 13(10):1567-1575. https://doi.org/10.1016/j.jiph.2020.06.027

Sadek, I., Rehman, S. U., Codjo, J., & Abdulrazak, B. (2019). Privacy and Security of IoT Based Healthcare Systems: Concerns, Solutions, and Recommendations. *How AI Impacts Urban Living and Public Health. Lecture Notes in Computer Science*. vol 11862. https://doi.org/10.1007/978-3-030-32785-9_1

Salunke, R., Bansod, G., Naidu, P. (2019). Design and implementation of a lightweight encryption scheme for wireless sensor nodes. *Advances in Intelligent Systems and Computing,* vol. 998. https://doi.org/10.1007/978-3- 030-22868-2_41

Sameena, N. (2021). Detection of Phishing in Internet of Things Using Machine Learning Approach. International Journal of Digital Crime and Forensics. 13. 1-15. https://doi.org/10.4018/IJDCF.2021030101

Seh, A. H., Zarour, M., Alenezi, M., Sarkar, A. K., Agrawal, A., Kumar, R., & Khan, R. A. (2020). Healthcare Data Breaches: Insights and Implications. *Healthcare (Basel)*. 8(2):133. https:/doi.org/10.3390/healthcare8020133

Selvaraj, S., & Sundaravaradhan, S. (2020). Challenges and opportunities in IoT healthcare systems: a systematic review. *SN Appl. Sci.* 2, 139. https://doi.org/10.1007/s42452-019-1925-y

Sethi, P., & Sarangi, S. R. (2017). Internet of Things: Architectures, Protocols, and Applications. *Journal of Electrical & Computer Engineering.* 1. 25. https://doi.org/10.1155/2017/9324035

Schukat, M., McCaldin, D., Wang, K., Schreier, G., Lovell, N. H., Marschollek, M., & Redmond, S. J. (2016). Unintended Consequences of Wearable Sensor Use in Healthcare. Contribution of the IMIA Wearable Sensors in Healthcare WG. *Yearb Med Inform*. (1):73-86. https://doi.org/10.15265/IY-2016-025

Sharma, G., Bala, S., & Verma, A. K. (2012). Security Frameworks for Wireless Sensor Networks-Review. *Procedia Technology*. 6, 978. https:/doi.org/10.1016/j.protcy.2012.10.119

Sharma, S., Chen, K., & Sheth, A. (2018). Toward Practical Privacy-Preserving Analytics for IoT and Cloud-Based Healthcare Systems. IEEE Internet Computing. vol. 22. no. 2, pp. 42-51. https://doi.org/10.1109/MIC.2018.112102519

Shelby, Z., Hartke, K. & Bormann, C. (2014). The Constrained Application Protocol (CoAP). *Internet Engineering Task Force (IETF)*. RFC-7252. http://dx.doi.org/10.17487/RFC7252

Shi, S., He, D., Li, L., Kumar, N., Khan, M. K., & Choo, K. R. (2020). Applications of blockchain in ensuring the security and privacy of electronic health record systems: A survey. *Comput Secur*. https://doi.org/10.1016/j.cose.2020.101966

Shrivastava, V., & Namdev, M. (2019). A Review on Security and Privacy Issues in Wireless Body Area Networks for Healthcare Applications. *SMART MOVES JOURNAL IJOSCIENCE*, *5*(11). 22–28. https://doi.org/10.24113/ijoscience.v5i11.246

SIG Bluetooth. (2015). Bluetooth core specication. *Specication of the Bluetooth System*. 1:7.

Singh, A., & Chatterjee, K. (2019). Security and privacy issues of electronic healthcare system:

A survey. *Journal of Information and Optimization Sciences.* 40. 1709-1729. https://doi.org/10.1080/02522667.2019.1703265

Singh, P., & Kedar, D. (2018). Performance evaluation of cryptographic ciphers on IoT devices. https://doi.org/10.48550/arXiv.1812.02220

Snyder, H. (2019). Literature review as a research methodology: An overview and guidelines. *Journal of Business Research.* Volume 104. Pages 333-339. https://doi.org/10.1016/j.jbusres.2019.07.039.

Soni, V. K., Modi, P. P., & Chaudhri, V. (2013). Detecting sinkhole attack in wireless sensor network. *International Journal of Application or Innovation in Engineering & Management*. 2(2):29–32.

Stout, W., & Urias, V. (2016). Challenges to securing the Internet of Things. *IEEE International Carnahan Conference on Security Technology (ICCST),* 1-8. https://doi.org/10.1109/CCST.2016.7815675

Sultania, A.K., Delgado, C., & Famaey, J. (2020). Enabling Low-Latency Bluetooth Low Energy on Energy Harvesting Batteryless Devices Using Wake-Up Radios. *Sensors (Basel).* 20(18):5196. https://doi.org/10.3390/s20185196

Suo, H., Wan, J., Zou, C., & Liu, J. (2012). Security in the Internet of Things: A Review. *IEEE International Conference on Computer Science and Electronics Engineering.* 23-25. 648-651. https://doi.org/10.1109/ICCSEE.2012.373

Taiwo, O., & Ezugwu, A. E. (2020). Smart healthcare support for remote patient monitoring during covid-19 quarantine. *Inform Med Unlocked.* 20:100428. https://doi.org/10.1016/j.imu.2020.100428

Taleb, H., Andrieux, G., & Cruz, E. M. (2021). Wireless technologies, medical applications and future challenges in WBAN: a survey. *Wireless Netw* **27**, 5271–5295 https://doi.org/10.1007/s11276-021-02780-2

Tankard, C. (2015). Feature: The security issues of the Internet of Things. *Computer Fraud & Security*. 9. 11–14. https://doi.org/10.1016/S1361-3723(15)30084-1

Tara, S., & Raj, J. (2017). A Survey of Protocols and Standards for Internet of Things. *Advanced Computing and Communications*. 1. https://doi.org/10.34048/2017.1.F3.

Thomas, C. (2020). Introductory Chapter: Computer Security Threats. *Computer Security*

Threats. IntechOpen. https://doi.org/10.5772/intechopen.93041

Thakor, V. A., Razzaque, M. A., & Khandaker, M. R. A. (2021). Lightweight Cryptography Algorithms for Resource-Constrained IoT Devices: A Review, Comparison and Research Opportunities. *IEEE Access*. vol. 9. pp. 28177-28193. https://doi.org/10.1109/ACCESS.2021.3052867

Tim, G. (2016). The Internet of Things; Epic Change to Follow. *National Institute of Standards and Technology.*

Touati F, Mnaouer A, Erdene-Ochir O, Menhood W, Hassan A, and Gaabab B. (2016). Feasibility and Performance Evaluation of a LoWPAN-Enabled platform for Ubiquitous Healthcare Monitoring. *Wirel. Commun. Mob. Comput.* 1271-1281. https://doi.org/101002/wcm.2601

Townsend, K., Akiba, C., & Davidson, R. (2014). Getting started with Bluetooth Low Energy. Sebastopol, CA: O'Reilly.

Unit 42 research team. 2020. Key findings on how to reduce IoT risks. *Unit 42 IoT Threat Report.* Palo Alto Networks. Retrieved from: https://start.paloaltonetworks.com/unit-42-iot-threat-report

Unit 42 research team. (2020). *Unit 42 IoT Threat Report.* Retrieved from: https://unit42.paloaltonetworks.com/iot-threat-report-2020/

Uslu B. Ç., Okay, E., & Dursun, E. (2020). Analysis of factors affecting IoT-based smart hospital design. *J Cloud Comput (Heidelb).* 9(1):67. https://doi.org/10.1186/s13677-020-00215-5

Vaniotis, G. (2018, June 21). *Everything you need to know about RFID technology.* Labtag. Retrieved from: https://blog.labtag.com/everything-you-need-to-know-about-rfid-technology/

Verri, L. A., Augusto, S. L., Luchtenberg, R., Garcez, L., Mao, X., García, O, R., Miguel, P. I., Luis V. J., Reis, Q. L. V. (2020). A Case Study on the Development of a Data Privacy Management Solution Based on Patient Information. *Sensors (Basel).* 20(21):6030. https://doi.org/10.3390/s20216030

Virtual Mentor. (2012). 14(9). 712-719. https://doi.org/10.1001/virtualmentor.2012.14.9.stas1-1209.

Wei, Z., Yu, S., & Ma, W. (2021). Defending against Internal Attacks in Healthcare-Based

WSNs. *J Healthc Eng.* 2081246. https://doi.org/10.1155/2021/2081246

Whitmore, A., Agarwal, A., & Da Xu, L. (2015). The Internet of Things - A survey of topics and trends. *Inf. Syst. Front.* vol. 17. no. 2, pp. 261–274. https://doi.org/10.1007/s10796-014-9489-2

Wright, R.W., Brand, R. A., Dunn, W., & Spindler, K.P. (2007). How to write a systematic review. *Clin Orthop Relat Res*. https://doi.org/10.1097/BLO.0b013e31802c9098

Xiao, Y., & Watson, M. (2019). Guidance on Conducting a Systematic Literature Review. *Journal of Planning Education and Research.* 39(1). 93–112. https://doi.org/10.1177/0739456X17723971

Xu, L. D., He, W., & Li, S. (2014). Internet of Things in Industries: A Survey. *IEEE Transactions on Industrial Informatics.* vol. 10. no. 4, pp. 2233-2243. https://doi.org/ https://doi.org/10.1109/TII.2014.2300753

Yang, J., & Johansson, T. (2020). An overview of cryptographic primitives for possible use in 5G and beyond. *Sci. China Inf. Sci.* 63, 220301. https://doi.org/10.1007/s11432-019-2907-4

Yao, X., Farha, F., Li, R., Psychoula, I., Chen, L., & Ning, H. (2021). Security and privacy issues of physical objects in the IoT: Challenges and opportunities. *Digital Communications and Networks.* Volume 7. Issue 3. Pages 373-384. https://doi.org/10.1016/j.dcan.2020.09.001

Yasmine, H., Zibouda, A., Allaoua, R., & Harous, S. (2021). Recent Security Trends in Internet of Things: A Comprehensive Survey. *IEEE Access*. PP. 1-1. https://doi.org/10.1109/ACCESS.2021.3103725

Yeole, A., & Kalbande, D. R. (2021). Ensuring Security and Privacy in IoT for Healthcare Applications. *Cognitive Engineering for Next Generation Computing: A Practical Analytical Approach*. 299. https://doi.org/10.1002/9781119711308.ch11

Yick, J., Mukherjee, B., & Ghosal, D. (2008). Wireless sensor network survey. *Comput. Networks.* vol. 52, no. 12, pp. 2292–2330. https://doi.org/10.1016/j.comnet.2008.04.002

Zeadally, S., Siddiqui, F., Baig, Z. & Ibrahim, A. (2020). Smart healthcare: Challenges and potential solutions using internet of things (IoT) and big data analytics. *PSU Research Review*, Vol. 4 No. 2, pp. 149-168. https://doi.org/10.1108/PRR-08-2019-0027

Zhang, W.; Bao, Z.; Lin, D.; Rijmen, V.; Yang, B.; Verbauwhede, I. (2015). RECTANGLE: a bit-slice lightweight block cipher suitable formultiple platforms. *Sci. China Inf.* 58(12), 1–15.

https://doi.org/10.1007/s11432-015-5459-7

Zhao, K., & Ge, L. (2013). A survey on the Internet of things security. In Computational Intelligence and Security (CIS). *9th International Conference*. pages 663–667. IEEE. https://doi.org/10.1109/CIS.2013.145

ZigBee Standards Organization (ZSO). (2006). ZigBee Specication. *Zigbee document*.