People's Democratic Republic of Algeria

Ministry of Higher Education and Scientific Research

UNIVERSITY OF
ECHAHID HAMA LAKHDER EL OUED
FACULTY OF EXACT SCIENCES
Computer Science department

End of study memory

Presented for the Diploma of

ACADEMIC MASTER

Domain : **Mathematics and Computer Science**

Industry : **Computer Science**

Specialty: **Distributed Systems and Artificial Intelligence**

Presented by: TOUAOUA Elhabib
LACHRAF Iqbal

Them

Preventing MitM attack in IoT enviroment

.

Defended on *20-06-2021* before the jury:

Mr. Abdennacer Khelaifa	MAA	President
Mr. Abdelkader Laouid	MCA	Supervisor
Mr. Ismail kertiou	MAA	Reporter

Academic year 2020/2021

Made with LaTeX.

Dedicate

With the expression of my gratitude, I dedicate this modest work to those who, whatever the terms embraced, I would never manage to express my sincere love to them.

To the man, my precious gift from god, who owes my life, my success and all my respect: my dear father who raised me to be the person I am today.

To the woman who suffered without letting me suffer, who never said no to my demands and who spared no effort to make me happy: my adorable mother

To my dear sister and my fiancé who never stopped advising, encouraging and supporting me throughout my studies. May God protect them and give them luck and happiness.

To my brothers who always knows how to bring joy and happiness to the whole family.

To my grandmothers, uncles and aunts. May God give them a long and joyful life. To all the cousins, neighbors and friends that I have known until now. Thank to them for their love and their encouragement.

Without forgetting my partner Iqbal for his moral support, his patience and his understanding throughout this project

Touaoua elhabib

Dedicate

As I struggle to find the proper words to convey my genuine feelings of gratitude, I take this opportunity to express them nonetheless.

I dedicate this humble effort:

To my hardworking father: a quality for which I hold him in high regard.

To my attentive mother: an anchor of support and encouragement. Both in words and deeds.

To my dear siblings: for their good company and the fun we share.

May they live long and prosper.

And To those whom amongst, I felt at ease and welcomed. Thank you.

Likewise, I would like to extend my gratitude to my colleague El 'Habib, without whom this effort would have not been realized.

Lachraf Iqbal

Acknowledgments

First and foremost, thanks and glory to God, our lord, and the source of Inspiration, wisdom and understanding, the Almighty, for the blessings among all my research work to complete this research.

Our sincere gratitude goes to our supervisor Dr. LAOUID Abdelkader *for his professional guidance and academic support.*

We are also thankful to members of the jury for their willingness to discuss and enrich the material of this study.

Our special thanks go to all the people who have supported us, encouraged us and just give us any help even with a few words to stand up again and again all the time.

Abstract

The Internet of Things (IoT) is an emerging flow of the Internet that's attracted plenty of attention in the past couple of decades. It has dramatically interfered in our daily lives, where IoT devices can have a vast array of forms, from tiny to large appliances. The volatile setup of IoT is faced with privacy and security problems that could have significant threats to side the IoT's prospective advantages. Securing such systems raises many challenges, mainly in resource-constrained, heterogeneous, and large-scale surroundings. The most important goal with this thesis will be to overcome the IoT's security and privacy problems, particularly IoT attacks such as man-in-the-middle, brute force, and chosen plain/cipher-text attacks. In this context, we propose an efficient and robust security scheme for IoT systems to prevent these attacks. We evaluate our proposed solution's performance and security to known security schemes such as RSA. The obtained results show that our proposed technique are secure, efficient, and convenient for IoT systems than recent related methods.

Keywords: Man in the middle attack, internet of things (IoT), Lightweight encryption

خلاصة

إن إنترنت الأشياء (اية) هو تدفق ناشئ للإنترنت جذب الكثير من الاهتمام في العقدين الماضيين. لقد تداخلت بشكل كبير في حياتنا اليومية ، حيث يمكن أن تحتوي أجهزة إنترنت الأشياء على مجموعة واسعة من الأشكال ، من الأجهزة الصغيرة إلى الأجهزة الكبيرة. يواجه الإعداد المتقلب لإنترنت الأشياء مشكلات تتعلق بالخصوصية والأمان يمكن أن يكون لها تهديدات كبيرة إلى جانب المزايا المحتملة لإنترنت الأشياء. يثير تأمين مثل هذه الأنظمة العديد من التحديات ، لا سيما في بيئة محدودة الموارد وغير متجانسة وواسعة النطاق. سيكون الهدف الأكثر أهمية من هذه الأطروحة هو التغلب على مشكلات أمان وخصوصية إنترنت الأشياء ، لا سيما هجمات إنترنت الأشياء مثل الرجل في الوسط ، والقوة الغاشمة ، وهجمات النص العادي / المشفر المختار. في هذا السياق ، نقترح نظام أمان فعال وقوي لأنظمة إنترنت الأشياء لمنع هذه الهجمات. نقوم بتقييم أداء الحل المقترح وأمانه لمخططات الأمان المعروفة مثل غصا. تظهر النتائج التي تم الحصول عليها أن تقنيتنا المقترحة آمنة وفعالة وملائمة لأنظمة إنترنت الأشياء من الأساليب الحديثة ذات الصلة.

الكلمات المفتاحية: هجوم رجل في منتصف ، إنترنت الأشياء، تشفير خفيف الوزن

Résumé

L'Internet des objets (IoT) est un flux émergent d'Internet qui a attiré beaucoup d'attention au cours des deux dernières décennies. Il a considérablement interféré dans notre vie quotidienne, où les appareils IoT peuvent avoir une vaste gamme de formes, des petits aux gros appareils. La configuration volatile de l'IoT est confrontée à des problèmes de confidentialité et de sécurité qui pourraient constituer des menaces importantes pour les avantages potentiels de l'IoT. La sécurisation de tels systèmes soulève de nombreux défis, principalement dans des environnements aux ressources limitées, hétérogènes et à grande échelle. L'objectif le plus important de cette thèse sera de surmonter les problèmes de sécurité et de confidentialité de l'IoT, en particulier les attaques de l'IoT telles que l'homme du milieu, la force brute et les attaques choisies par texte brut/chiffré. Dans ce contexte, nous proposons un schéma de sécurité efficace et robuste pour les systèmes IoT afin de prévenir ces attaques. Nous évaluons les performances et la sécurité de notre solution proposée par rapport à des schémas de sécurité connus tels que RSA. Les résultats obtenus montrent que notre technique proposée est sécurisée, efficace et pratique pour les systèmes IoT que les méthodes connexes récentes. cryptage léger

Mots clés: L'homme au milieu attaque, Internet des objets, cryptage léger

CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ALGORITHMS

ABBREVIATIONS

6LoWPAN IPv6 over Low power Wireless Personal Area Networks

AES Advanced Encryption Standards

AODV Ad hoc On-demand Distance Vector

ATT attribute protocol

BLE Bluetooth Low Energy

CoAP Constrained Application Protocol

DAG Direct Acyclic Graph

DODAG Destination Oriented Direct Acyclic Graph

DoS Denial of Service

ECC Elliptic Curve Cryptography

IIoT Industrial Internet of Things

IoT Internet of Things

L2CAP Logical Link Control and Adaptation Protocol

LoRaWAN Long-Range Wide Area Network

MAC Medium Access Control

MIC Message Integrity Code

MiTM Man in The Middle

MQTT Message Queuing Telemetry Transport

NFC Near Field Communication

PBFT Practical Byzantine Fault Tolerance

PKC Public Key Cryptography

PoS Power of Stake

PoW Power of Work

REST Representational State Transfer

RFID Radio Frequency IDentification

RPL Routing Protocol for Low-power

RSA Rivest-Shamir-Adleman

SDR Software Defined Radio

SSL Secure Socket Layer

TDMA Time Division Multiple Access

UWB Ultra WideBand

WPANs Wireless Personal Area Networks

WSN Wireless Sensors Network

GENERAL INTRODUCTION

Internet of Things (IoT) is considered the third industrial revolution [1]. It is a group of interconnected computing devices embedded in everyday objects. Those devices are capable of interacting with each other via the internet by sending and receiving data. The IoT market is growing at a breathtaking pace, and it forecast to exceed 50 billion connected devices across all IoT markets by 2025 [2].

Therefore, IoT is used in almost all fields: domestic, education, entertainment, energy distribution, finances, healthcare, smart cities, tourism, and even transportation. Consequently, businesses, academia, and individuals are attempting to incorporate the flow of fast commercialization with seldom attention to the safety and the security of IoT devices and networks.

Nowadays, security breach and anomaly has become common phenomena In IoT devices, and the usual safety measures become vulnerable with the vulnerability of these devices. Exposing a single component affects the security of IoT systems and the complete ecosystem, including websites, applications, social networks, and servers which may lead to paralyzing part or complete Internet network.

This study proposes lightweight and efficient encryption technique directed to IoT networks to maintain data confidentiality, data integrity, authentication, availability, and freshness. We Consider the constraints of most of these devices regarding bandwidth, computation power, battery life, and communication capabilities.

This dissertation is organized as follows:

In Chapter 1, we defined the concept of IoT in general; then, we gave an overview of the various applications of this technology. after that, we presented some details about IoT architecture and elements along with the enabling technologies and protocols used in each layer of the environment.

Chapter 2 presents the IoT attacks and their definitions and the security requirements that must be performed to overcome those threats. We also introduced some emerging solutions to improve IoT security and discuss several related works to the proposed solutions.

Chapter 3 introduce and and explain our proposed scheme which is an efficient asymmetric lightweight security scheme. the scheme comprising a key generator algorithm and an encryption algorithm with its corresponding decryption algorithm.

In Chapter 4, we analyzed the proposed scheme in terms of execution time, storage space, factorization number problem,and robustness against different attacks like the Man-in-the-middle attack (MiTM), Brute-force attack, Plain-text Attack, and Chosen Cipher-text Attack

CHAPTER 1

INTERNET OF THINGS (IOT)

1.1 Introduction

During the last few years, the IoT has gained significant attention since it causes potentially tremendous benefits to the human. Kevin Ashton introduced the concept of the IoT in 1999. It aims to connect anything at any time in any place.

"Things" in IoT are embedded with sensing, processing, and actuating capabilities and cooperate in providing intelligent and innovative services autonomously. The IoT spans many diverse application domains such as home automation, environmental monitoring, healthcare, etc [3].

The IoT's primary objective is to unify these numerous diverse application domains under the same umbrella referred to as smart life [3]. The IoT architecture supports numerous heterogeneous devices and integrates various communication technologies that enable the connectivity of IoT devices to provide the required services to end-users.

This chapter presents an overview of the basic concepts of IoT. It introduces the IoT definition, potential applications, and architecture, including major elements and protocols used in IoT.

1.2 IoT definition

The Internet of things refers to a type of network to connect any such thing with the Internet based on designated protocols by information sensing tools to conduct information exchange and communications to achieve smart recognitions, positioning, tracking, monitoring, along with management [4].

The IoT devices involve various physical objects ranging from tiny to large machines that seamlessly exchange information autonomously via the Internet [6].

According to Cisco, 24 billion things are currently estimated to be connected to the Internet [2]. The IoT devices are equipped with sensors to smartly sense their surroundings and actuators to execute actions autonomously in the environment [7]. Figure 1.1 demonstrates the various integration of the internet of things in everyday use objects.

These things are natively resource-constrained. They have limited memory space, low processing capacity, and computation power. Different enabling technologies such as wireless sensor networks (WSNs), radio frequency identification (RFID), and cloud computing evolve as essential components for the development of the IoT paradigm [8]. Figure 1.2 illustrates some available technologies.

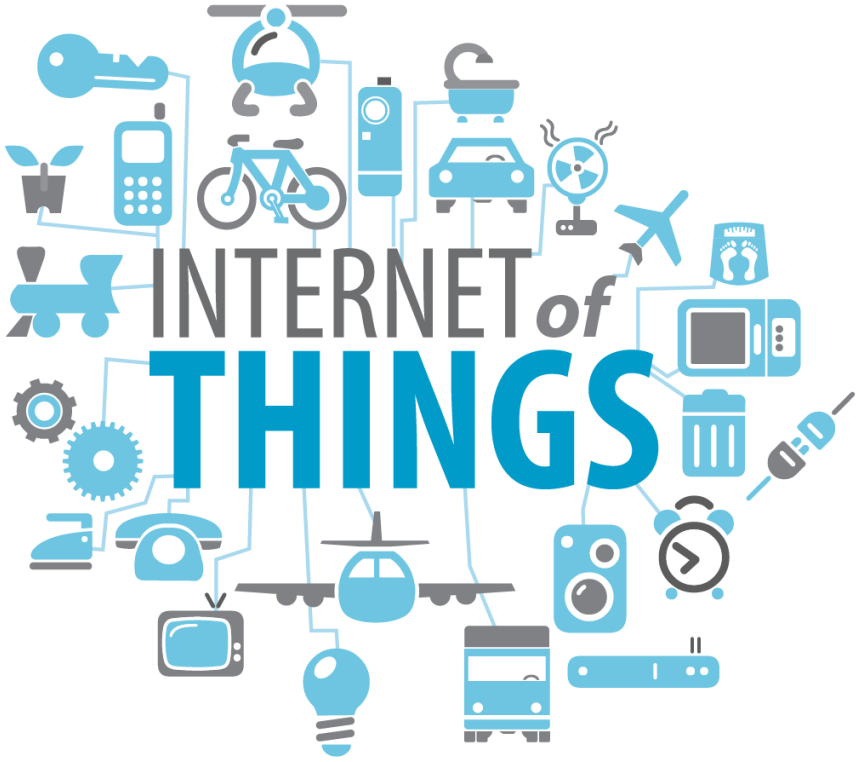

Figure 1.1: Internet of Things [5]

– **Wireless Sensor Network (WSN)** Includes a Lot of physical autonomous Detectors Set up in the environment in order to control the environmental conditions [10].

– **Radio Frequency IDentifiaction (RFID)** is utilized to identify and track IoT objects. It allows data exchange via radio signals over a short distance [10].

– **Cloud computing** performs a vital role in the IoT by granting unlimited storage resources and processing power [11].

– **Constrained Application Protocol (CoAP)** is an application layer protocol proposed for resource-constrained devices [12] [13].

– **IPv6 Low power Wireless Personal Area Network (6LoWPAN)** combines IPv6 and LoWPAN and allows transmission of IPv6 packets over IEEE 802.15.4 networks [12]. The 6LoWPAN is suitable for the IoT network with several advantages to offer.

– **Ultra WideBand (UWB)** is a viable technology for many IoT applications due to its low power consumption, higher precision, and security [14].

– **IEEE 802.15.4** is a protocol for the physical layer and the MAC (Medium Access Control) layer in Wireless Personal Area Networks (WPANs). It provides the connection of

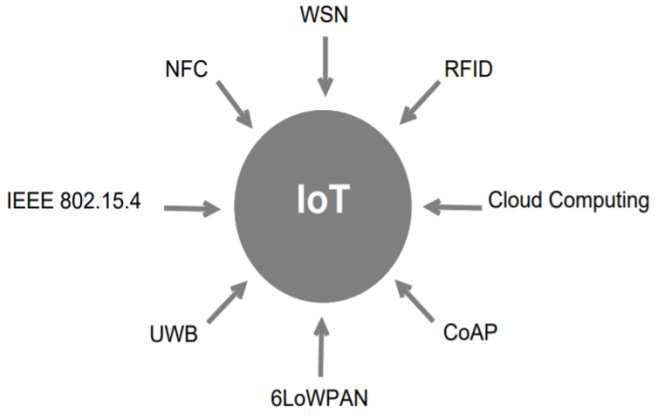

Figure 1.2: IoT enabling technologies [9]

things in the personal area with low energy consumption [12].

– **Near Field Communication (NFC)** is a short-range technology used in various IoT systems such as payments and authentication. The NFC provides easy network access and data exchange [15].

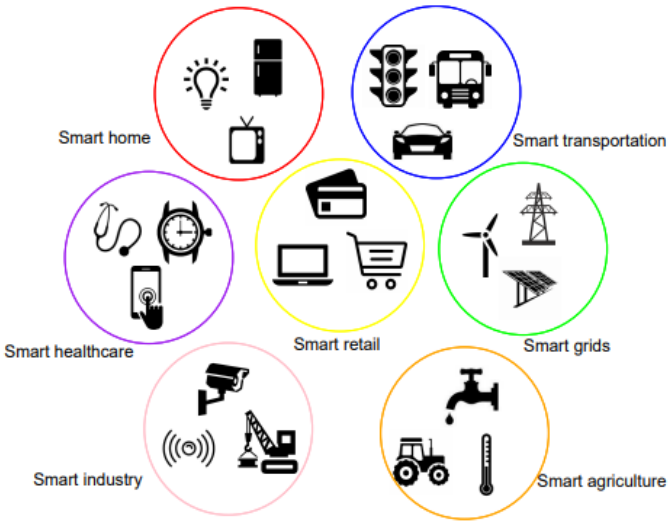

Figure 1.3: IoT applications [9]

1.3 IoT applications

The IoT enhances the development of numerous industry-oriented and user-specific IoT applications. Whereas devices and networks provide physical connectivity, IoT applications enable device-to-device and human-to-device interactions reliably and robustly. Figure 1.3 presents some examples of IoT application

Smart healthcare enables healthcare service providers to personalize patient care. New IoT technologies collect, transmit, and store patients' physiological information, creating opportunities for care providers to influence patients far more frequently and effectively. For example, Humana's Healthsense eNeighbor1 remote monitoring system reports changes in the member's typical movement patterns and activity to Humana care managers via in-home sensors. It measures daily activities routine with data analytics to help trigger interferences and help to prevent unpropitious events of escalating to the emergency room or hospital [16].

Smart home contains a set of smart devices (e.g., smart lock, baby monitor, fire detector) deployed at home for energy savings, family and property protection. Verizon Home Monitoring and Control network employs a wireless communications technology built specifically for handheld remote control applications. IoT-enabled home sensors and devices can be monitored and controlled outside the user's home through a computer, tablet, or smartphone. The Verizon Home Monitoring and Control network enables users to manage the security system, lock and unlock doors, receive automatic event notifications, control the climate and even adjust the lights [16].

Smart transportation covers a large number of smart vehicles that can communicate with each other (vehicle-to-vehicle), communicate with an outside station (vehicle-to-infrastructure), and to pedestrians (vehicle-to-pedestrian) over wireless networks. Using sensors embedded in these vehicles, mobile devices, and installed in the city, it is possible to offer optimized route suggestions, autonomous driving, easy parking reservations, economic street lighting, telematics for public means of transportation, more importantly, accident prevention [17].

Smart agriculture allows remote control of temperature, humidity, irrigation, soil moisture, and micro-climate conditions to provide high production/quality and prevent financial losses. In an intelligent farming system, sensors can be attached to animals to track livestock behaviors and health conditions.

Smart industry, known as industrial IoT (IIoT), uses machine-to-machine technology to automate manufacturing and energy management with trivial human intervention. The IIoT aims to manage the production process, data, and issues to provide efficient and reliable final products.

Smart retail permits retailers to gain deep insights into customer needs using IoT applications in beacons, smart shelves, digital signage, and sensors to deliver effective promotions and boost sales. Sensors can be attached to a retail item to track the product's traveling and status. For example, Kaa can help to implement applications for tracking inventory and delivery of goods using RFID tags, connecting Bluetooth beacons to provide customers with personalized

mobile shopping experiences, producing smart metering and smart lighting solutions, or managing digital signage displays and tracking visitors' interaction with them inside the store in order to maximize the effectiveness of retailers marketing efforts and improve customer service [18].

Smart grid is a typical application of IoT that can measure, monitor, and manage electricity consumption. It also enables early detection of things like power influxes resulting from earthquakes and extreme weather. It enables efficient and reliable electricity management, provides energy-saving, and reduces powers grids issues/failures.

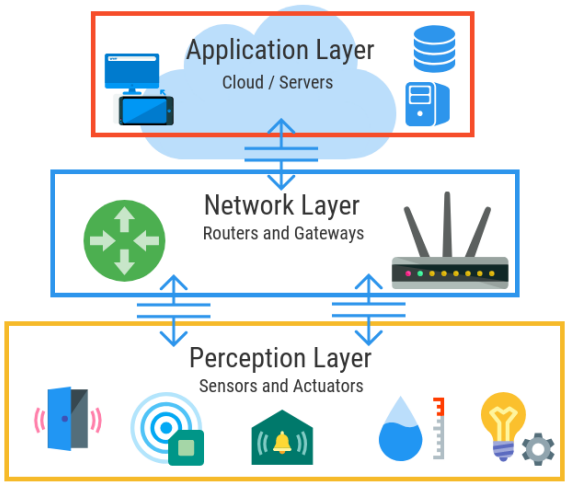

Figure 1.4: Three-layered IoT architecture [19]

1.4 IoT architecture, elements and protocols

The common basic architecture of IoT is a three-layer architecture as it was introduced in the early stages of research in this area. It has three layers, namely, the perception, network, and application layers, as shown in Figure 1.4.

1.4.1 Perception layer

The perception layer's role is recognizing IoT objects' physical properties; it is also responsible for interaction among devices and IoT data collection from the surrounding world. Data collection is performed using smart devices such as radio frequency identification (RFID) tags and sensors.

1.4.1.1 Wireless sensors

Wireless sensors perform an essential task in IoT by offering sense, and communicating services [20]. A Wireless sensor network (WSN) consists of many smart sensors stationed in remote environments to sense and gather data such as temperature, humidity, vibration, etc. Sensed data are transmitted through one or multi-hop to a gateway/base station, as depicted in Figure 1.5.

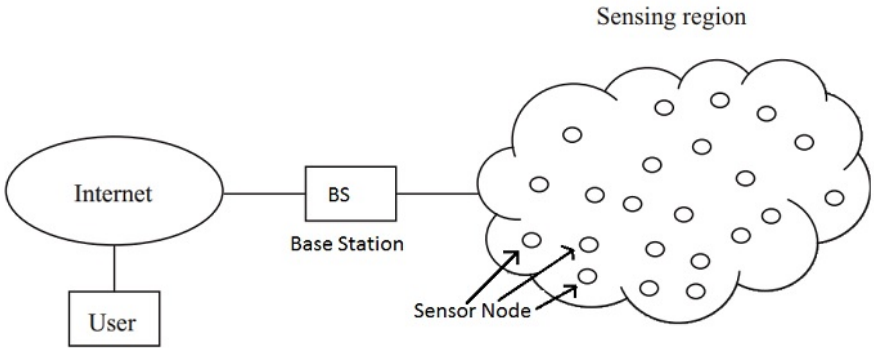

Figure 1.5: WSN architecture [21]

Figure 1.6: RFID system [9]

1.4.1.2 Radio frequency identification (RFID)

RFID technology is a major element of IoT due to its identification, tracking, and monitoring of objects [22]. An RFID system consists of a radio signal transponder (tag) that stores a unique identity of the object and a tag reader that identifies the object through radio waves. The tag reader transfers the identification number to a computer to track and monitor the object, as shown in Figure 1.6.

1.4.2 Network layer

The network layer is responsible for processing the collected data provided by the perception layer, storing or transmits the data to the application layer. It plays the most important

role in IoT architecture because it integrates various communication technologies that enable the connectivity of IoT devices. The widely used communication technologies include ZigBee, Bluetooth low energy (BLE), IPv6 over low power wireless personal area networks (6LoWPAN) and long-range wide area network (LoRaWAN).

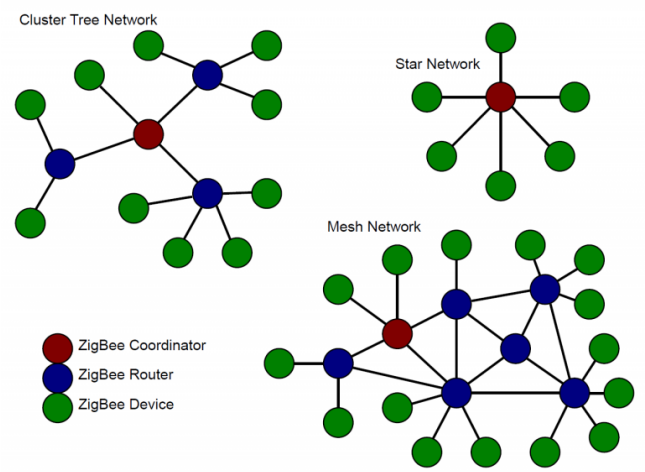

Figure 1.7: ZigBee topologies [23]

1.4.2.1 ZigBee

ZigBee is a wireless communication technology designed for short-range communications [24]. It can be deployed in smart agriculture, smart homes and smart healthcare. The ZigBee protocol stack includes physical layer (PHY) and medium access control (MAC) layers based on IEEE 802.15.4 standard [25], a network (NWK) layer and an application (APL) layer. A ZigBee network can have a star, tree or mesh topology, and each network has a coordinator node (trusted node) that manages the network and maintains security between devices. In the star network, end devices are directly connected to the coordinator, while tree or mesh networks use intermediate routers to extend the network, as shown in Figure 1.7. Data routing is offered by the NWK layer using cluster-tree and modified ad hoc on-demand distance vector (AODV) algorithms [26]. A ZigBee device can only interact and communicate with another ZigBee device.

1.4.2.2 BLE

BLE is a short-range communication technology designed to reduce energy consumption compared to classic Bluetooth [27]. It is widely used in IoT vehicular systems. BLE protocol stack includes PHY layer, MAC layer, logical link control and adaptation protocol (L2CAP) and

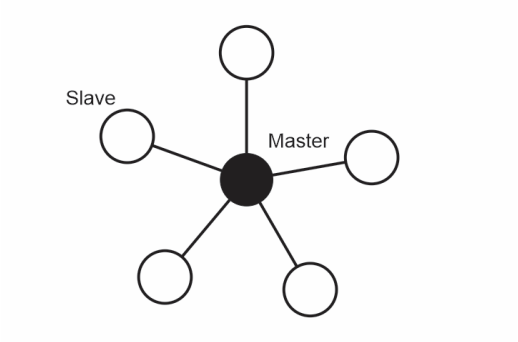

Figure 1.8: BLE topology [27]

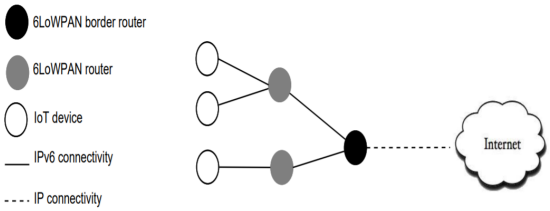

Figure 1.9: 6LoWPAN architecture [28]

attribute protocol (ATT). The BLE utilizes a star topology including master and slave devices, as demonstrated in Figure 1.8. Each slave node has a connection with a single master node. The master node is responsible for initiating the communication and providing a scheduling table according to time division multiple access (TDMA).

1.4.2.3 6LoWPAN

6LoWPAN is a coalition of the latest version of Internet protocol (IPv6), and low power wireless personal area network (LoWPAN) [29]. It allows IoT devices with limited capabilities to transmit data through wireless channels using IPv6. It is suitable for resource-constrained devices because it decreases transmission cost, supports mobility, etc. 6LoWPAN is mostly used in smart home, smart agriculture and industrial IoT. Unlike ZigBee, a 6LoWPAN device can communicate with another 6LoWPAN device or IEEE 802.15.4 device. It can also exchange information with an IP-based network such as Wi-Fi, as presented in Figure 1.9. The specification of 6LoWPAN defines a complete protocol stack that consists of PHY, and MAC layers based on IEEE 802.15.4 standard, the NWK layer, the transport layer and the APP layer [28]. The routing within the 6LoWPAN network uses routing protocol for low-power, and lossy networks (RPL) [30]. RPL supports point-to-point, point-to-multipoint and multipoint-to-point communications. It is based on a direct acyclic graph (DAG). From DAG, RPL forms a destination oriented direct acyclic graph (DODAG) tree that contains one root from the leaf

node to the root.

1.4.2.4 LoRaWAN

LoRaWAN is a long-range communication protocol designed for low power, and scalable IoT applications [31]. As depicted in Figure 1.10, a LoRaWAN network consists of end-devices, gateways and a single server in a star or star-of-star topology. The end devices can communicate and transmit data to one or more gateways using the ALOHA scheme through one-hop links. The transmitted data is received by multiple Gateways and then forward to a centralized network server.

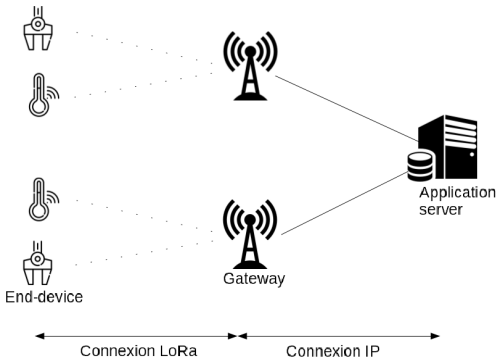

Figure 1.10: LoRaWAN architecture [31]

1.4.3 Application layer

The application layer role in IoT architecture is to receive the data from the network layer and respond with the required services to IoT users. It is deployed in various applications such as smart city, smart retail, smart grids, etc. Constrained application protocol (CoAP) and message queuing telemetry transport (MQTT) are The most common application protocols.

1.4.3.1 CoAP

IoT devices are constrained in resources; thus, HTTP protocol is inappropriate for low power devices due to its complexity. CoAP was designed to incorporate features of HTTP dedicated to IoT devices. As demonstrated in Figure 1.11, CoAP is a messaging protocol based on representational state transfer (REST) architecture [34]. It has four types of messages: confirmable, non-confirmable, reset (nack), and acknowledgement. Unlike HTTP, CoAP provides features like push notification (i.e., the server sends notifications to the device) and resource identification (i.e., the server can store the list of devices).

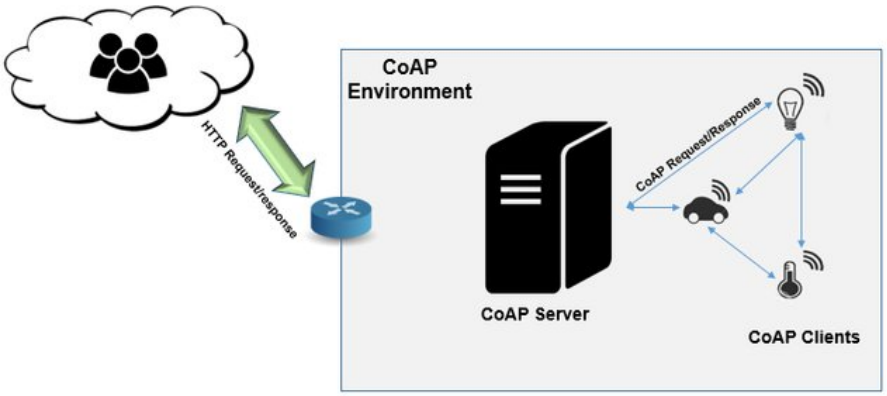

Figure 1.11: CoAP architecture [32]

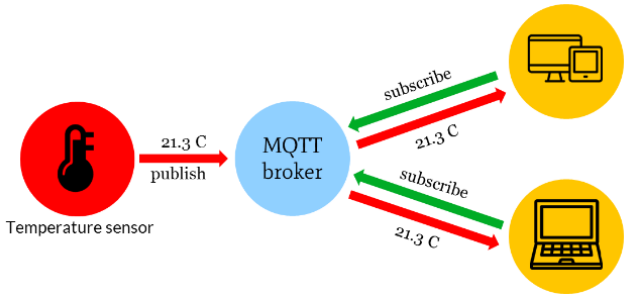

Figure 1.12: MQTT architecture [33]

1.4.3.2 MQTT

MQTT is a lightweight messaging protocol that provides the connectivity of networks and users with applications. It is a publish/subscribe architecture that runs over TCP. The system consists of three main components: publishers, subscribers, and brokers, as shown in Figure 1.12. Publishers are embedded things that send data to the broker, and subscribers are applications servers.

1.5 Conclusion

The IoT has drawn considerable attention in the past years since it has made revolutionary improvements in human life. The IoT enables the exchange of information in a large-scale variety of applications such as smart cities, smart healthcare, smart transportation, etc. This chapter introduced the definition of IoT network and presented enabling technologies that motivate the emergence of IoT. Moreover, we reviewed different applications provided by the IoT solution and discussed the principal elements and protocols integrated into the three-layered IoT architecture. In the next chapter, we focus on security vulnerabilities and requirements

of IoT. We present different security attacks that endanger the IoT environments. We provide a valuable taxonomy to highlight the security threats of IoT. To achieve the desired level of security in IoT, we propose a new taxonomy of security requirements, including data security, communication security and device security.

CHAPTER 2

STATE OF THE ART

2.1 Introduction

In spite of the extraordinary growth of IoT and the development of potential services to improve human lives, IoT faces several issues. As the IoT combines different existing technologies such as WSN and RFID, it inherits the security flaws of each technology [35]. Moreover, billions of devices are assumed to be connected to the Internet [36]. Therefore, an even more enormous amount of data will pass on the Internet [37]. This data might meet various security attacks like eavesdropping and altering. Consequently, the user's privacy will be endangered [38]. For instance, an adversary can intercept a baby monitor system using a Software Defined Radio (SDR) to endanger the user's privacy [39].

Security is a primary concern that inevitably affects IoT networks. It has attracted significant attention in the researchers' community [40,41]. Security vulnerabilities and attacks of IoT should be analyzed to develop a secure system. Several security requirements and properties such as authentication, confidentiality, integrity have to be guaranteed to secure IoT systems.

In this chapter, we present several security threats and vulnerabilities that endanger the IoT environment. We listed some known attacks with their definitions, including the level of the attack, the purposes, and the countermeasures to avoid such attacks. Moreover, we introduced a taxonomy of security requirements based on different attack purposes followed by emerging solutions that have been proposed to achieve a secure IoT environment.

2.2 IoT security attacks

The IoT is evolving very fast, and security attacks are advancing as well. It is first necessary to analyze the IoT vulnerabilities and attacks to include security requirements carefully into the IoT systems. The IoT devices are prone to various types of attacks since the IoT combines different already existed technologies like WSN, RFID, cloud computing, etc. Hence, it obtains the security stains of each technology. Different security attacks that threaten IoT networks are provided in Table 2.1 below.

Table 2.1: IoT security attacks.

Attack	**Description**	**Purposes**
Replay attack	Eavesdrop the communication and re-transmit the packets to destination node [42]	Obtain the confidence and trust of the IoT system and launch additional attacks.
Sybil attack	Pretend the identities of many other nodes to be in more than one location [43]	Degrade the data security and resource utilization.
Sinkhole attack	Claim unconstrained capabilities to be selected for forwarding all traffic in WSN [44]	Breach the data confidentiality and launch additional attacks
Wormhole attack	Create a false one-hop transmission (tunnel) to deliver more data through this tunnel [45]	Breach the data confidentiality and launch additional attacks
Node injection	Deploy physically malicious nodes in the IoT network [35]	Control data flow, access to private information and launch additional attack
Man in the middle(MiTM)	Intercept and possibly alter the communication between two nodes [46]	Get private information and launch additional attacks
Eavesdropping attack	It is a subset of MiTM where an attacker intercepts secretly the communications [46]	Get private information
Brute force attack	Try many keys to guess the correct one [47]	Decrypt encrypted data
Denial of Service (DoS)	Send many packets to the IoT system [47]	Exhaust the service provider resources, disable the network and compromise data acquisition

Encryption attack	Use particular techniques like timing, power, fault and electromagnetic analysis on IoT devices to find the encryption key [35]	Break the encrypted system and get private data
Malicious software	Infect or cripple an IoT system with malicious software like virus, worms, trojan horse, etc [35]	Damage connected IoT devices and components, tamper and steal information.

2.3 IoT security threats

This section provides a classification of the security attacks based on their level, purposes, and countermeasures. We concentrated on the security vulnerabilities of IoT at the three layers: perception, network, and application layer.

Levels investigate the security issues of IoT at the three layers: Perception layer threats address the security attacks within major elements of IoT such as WSNs and RFID. Network layer threats analyze vulnerabilities of the communication protocols mentioned above. Application layer threats include attacks related to IoT software and end-user devices.

Purposes estimate the effect of security attacks on IoT systems. The main purposes of IoT attacks are communication access, data capturing or alter data, damage services, and drain device resources.

Security requirement involves data security, communication security, and device security. IoT communications can be secured by providing authentication, access control, and non-repudiation. In order To protect data, relevant security requirements such as confidentiality, privacy, and integrity must be considered. Other fundamental requirements, including trust and availability of IoT devices, are needed in different environments.

2.3.1 Perception layer threats

The constraints in terms of resources and the heterogeneous nature of IoT devices make them vulnerable to various security attacks.

WSN used a Multi-hop transmission mode to transmit data from one node to another with the cooperation of an intermediate node. However, this Multi-hop routing technique has several

Protocol	**Security attacks**
ZigBee	Encryption key, sinkhole, DoS, code injection
BLE	Eavesdropping, MiTM, DoS, brute force
6LoWPAN	Fragment injection, sinkhole, blackhole, sybil, DoS
LoRaWAN	Encryption key, DoS, MiTM

Table 2.2: Security threats of IoT network layer protocols

issues regarding security and privacy, which lead to attacks like a sinkhole, blackhole, wormhole, Sybil, denial of service (DoS) [9]. Brief information on these security attacks are provided in Table 2.1.

Like WSN, the RFID networks are susceptive to different types of attacks, including spoofing, cloning, and sniffing attacks.

2.3.2 Network layer threats

ZigBee protocol adopted security mechanisms, including advanced encryption standards with cipher block chaining message (AES-CCM) and message integrity code (MIC) to provide authentication, integrity, and confidentiality. The ZigBee security is based on three keys:

– A master key that is installed in the device during the manufacturing process.

– A link key that is generated using key transport or establishment method.

– The network key is acquired using the key transport method.

An attacker can read the master key stored on the device memory after performing a successful node capturing attack. ZigBee network is vulnerable also gainst sinkhole attack, DoS, and Encryption key attack. The IoT acquires the security threats of WSNs and RFID because they are essential elements of IoT networks.

BLE protocol offers authentication and confidentiality employing the 128-bits AES-CCM algorithm as ZigBee. The symmetric key is generated using the pairing procedure. However, The pairing methods have several security issues, including eavesdropping, man-in-the-middle (MiTM), DoS, and brute force attacks.

6LoWPAN protocol enables resource-constrained devices to connect to the Internet via IPv6 addresses. It utilizes IPv6 header compression and packet fragmentation to decrease transmission overhead. Nevertheless, it does not provide authentication, integrity, or confidentiality

preservation. An adversary can inject fake fragments with the header of a legitimate fragment. The security of 6LoWPAN also relies on securing communications at the MAC layer or APP layer. The security of the MAC layer is provided using AES-CCM and MIC. However, the specification of IEEE 802.15.4 does not define the key management procedure. 6LoWPAN is vulnerable to several attacks, including sinkhole attack, Sybil, DoS, and MiTM attack.

loRaWAN protocol utilizes a 128-bits AES algorithm and MIC to ensure data confidentiality and integrity. The authorized devices in loRaWAN use two keys assigned by the network server to encryption/decryption data: network session key and application session key. An intruder can access session keys using a side channels attack since they are stored on the end-device. The authors in [48] demonstrated that the LoRaWAN network is vulnerable to DoS and MiTM attacks.

Security threats of IoT communication protocols are summarized in Table 2.2

2.3.3 Application layer threats

CoAP is an application layer protocol built on the UDP transport protocol. It enables resource-constrained devices to achieve RESTful interactions. Datagram TLS (DTLS) has been suggested to provide authentication, integrity, and confidentiality preservation in CoAP protocol [40]. On the other hand, the constraints of DTLS could be considered as security threats of CoAP protocol.

A secure socket layer (SSL) was introduced to secure data transfer using the MQTT protocol. It uses an asymmetric cryptographic technique to encrypt/decrypt the data and still vulnerable to MiTM attacks. An adversary can imitate or manipulate legitimate users to access an IoT system by injecting malicious software. The lack of user authentication has led to various IoT attacks, such as Bashlite and Mirai attacks [49].

2.4 IoT security Requirements

IoT security requirements are classified into three categories: data security, communication security, and device security, as presented in Figure 2.1.

2.4.1 Data Security

The IoT devices capture and transmit data collected from the physical environment through wireless channels. Nevertheless, this transmitted data is vulnerable to different security threats

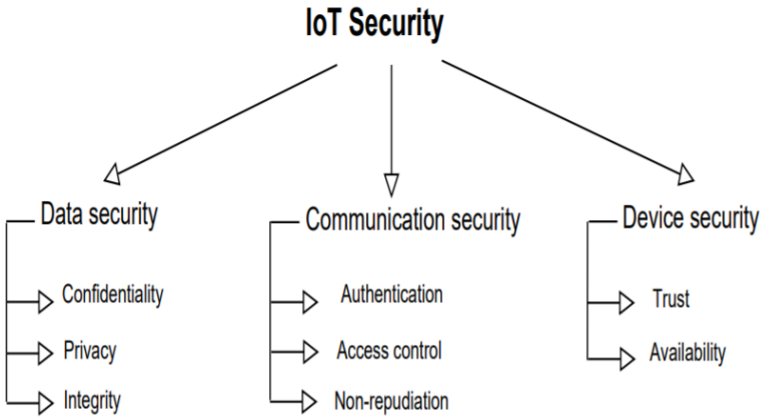

Figure 2.1: IoT security requirements [9]

like eavesdropping and altering. To ensure the security of data in the context of IoT, we should retain its confidentiality, privacy, and integrity.

Data confidentiality is defined as the procedure of concealing private information from unauthorized IoT devices. Standard encryption mechanisms can not be carried out immediately for the IoT system since IoT devices have constrained resources. Consequently, The usage of lightweight cryptography algorithms is needed In order to provide data protection and confidentiality.

Data integrity is the fact that the information received has not been changed or modified during transmission [50]. Integrity requires preserving the consistency, precision, and trustworthiness of this information. Cryptographic hash algorithms such as MD5 and SHA1 cannot be implemented since the IoT devices are inherently resource-constrained [51], so various Light Weight hash acts were suggested to address this issue.

2.4.2 Communication security

Before establishing any connection between IoT devices, an authentication procedure is necessary. So, only licensed devices can reach information or systems.

Authentication is the process of authenticating an identity using login and other data like digital certificates, PINs, or passwords. Every new connected device to the internet should authenticate itself before exchanging data. This authentication can be checked using lightweight cryptographic algorithms, physical primitives, or biometric identification.

Access control is a security feature that verifies the permission granted to users and systems to perform operations on other systems and resources [52]. The authors in [53] divided access control algorithms into five distinct types: role-based, organization-based, capability-

based, attribute-based, and trust-based algorithms.

non-repudiation is also an essential element of network security. It is defined as the ability to ensure that an IoT node cannot repudiate having sent a message and that the receiver cannot deny having received the message [50]. It could be achieved utilizing Public Key Cryptography (PKC) [54].

2.4.3 Device Security

To provide security in a critical ecosystem, ensuring trust and confidence between interacting nodes is the main task. Moreover, access to these IoT appliances is exceptionally demanded.

Trust management process is making a decision concern establishing communication with unknown entities. Interaction with trusted IoT devices only is necessary to prevent unwanted actions conducted by malicious nodes. The trust management techniques are split into two principal categories: deterministic and non-deterministic trust. The deterministic trust encompasses policy-based and certificate-based mechanisms, while the non-deterministic trust includes recommendation-based, reputation-based, prediction-based, and social network-based systems [53].

Device availability is an essential factor in IoT systems since they can be utilized in crucial areas, including economy, industry, healthcare, etc. [55]. According to [12], the availability of IoT networks should be performed in hardware and software. Hardware availability of the IoT application means the existence of all devices all the time, while software availability is the ability to provide services anywhere and anytime.

2.5 IoT security Solutions

The number of IoT devices and the variety of IoT applications have rapidly increased in the last few years. IoT applications are now used in various industries such as health, military, education, insurance, airlines, logistics, and even homes. Attackers target these devices in order to capture sensitive information and compromise the system. This growth faces several security issues that must be addressed. The IoT networks are deployed on a large scale and support heterogeneous devices. Most IoT devices are resource-constrained; thus, security-enhancing solutions must be computationally efficient. The emerging security solutions cannot be fully integrated into IoT systems because of the dynamic and heterogeneous nature and limited capabilities of IoT devices. Consequently, these solutions impose different security challenges

that need to be adequately solved. It is a very challenging position choosing between security and efficiency in IoT networks [9]. This section provides some recent solutions that have been proposed for securing the IoT in different application domains.

2.5.1 Lightweight cryptography solutions

Cryptography is an effective tool to guarantee confidentiality, integrity, and authentication. However, most IoT devices have challenging characteristics such as processing, memory, and battery power; traditional cryptographic algorithms are not suitable for such devices. Recently, lightweight cryptographic primitives were proposed to secure IoT systems. There are mainly four types of lightweight cryptographic primitives that are available for use. As presented in Figure 2.2 the lightweight cryptography primitives can be classified as Block Cipher, Stream Ciphers, Hash Functions, and Elliptic Curve Cryptography (ECC) [56].

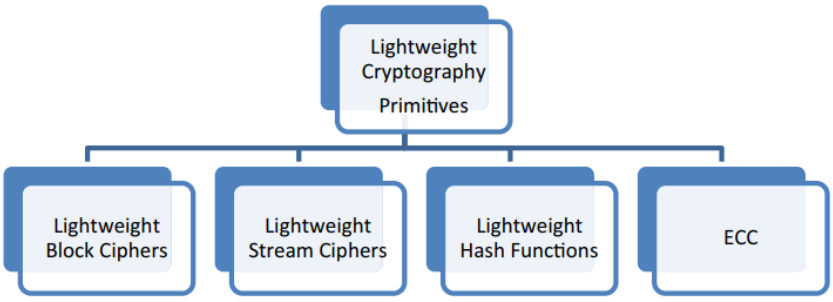

Figure 2.2: Lightweight cryptography for IoT [9]

A Block cipher is a type of symmetric cipher where a complete block is processed at once. A practical, lightweight block cipher takes into consideration the reduction in the block and key size, creating easier rounds, and designing simple key schedules. However, stream cipher encrypts and decrypts 1 byte at a time. Lightweight hash functions are a different way to provide security. They generate a fixed-length 'message digest' from an arbitrary-length message to ensure the integrity of the transmitted data.

ECC is a lightweight asymmetric cryptographic technique that provides the same level of security as the rivest-Shamir-Adleman (RSA) algorithm with a smaller key size.

There has been a growing demand for efficient, lightweight encryption mechanisms that combine all the features of lightweight symmetric and asymmetric algorithms. These cryptographic techniques can be adopted to achieve essential security requirements, including confidentiality, integrity, and authentication.

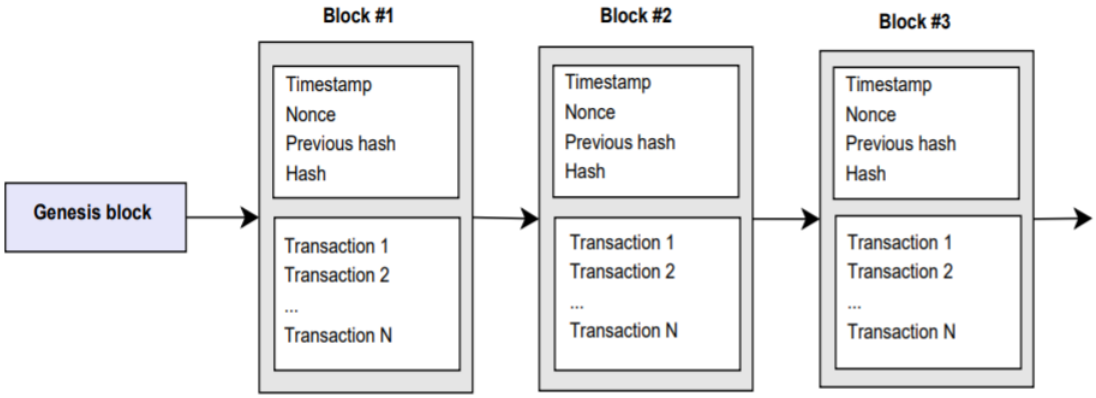

Figure 2.3: Blockchain structure [9]

2.5.2 Blockchain solutions

Blockchain is a disruptive technology that has revolutionized the world of cryptocurrency. A distributed database/ledger includes transactions of nodes in a peer-to-peer (P2P) network [57]. A set of transactions are grouped into a single block and validated in a distributed way using a consensus algorithm. These blocks are linked to form a chain of blocks or blockchain, as demonstrated in Figure 2.3. Each block consists of two parts, the first part represents the validated transactions, and the second part contains block timestamp, nonce value, a hash of the block, and the hash of the previous block. The consensus process is performed via some nodes in the network named miners. Standard consensus algorithms include power of work (PoW), power of stake (PoS), and practical byzantine fault tolerance (PBFT) [57]. These algorithms can be utilized to allow miners nodes to agree on adding a new block to the blockchain. There are two main types of blockchain, namely public and private blockchain [57]. A public blockchain has no access restrictions. Any node can join the network and send transactions, while only defined nodes can access the network in a private blockchain. The common public blockchains are Bitcoin and Ethereum. The selection of blockchain type and consensus algorithm depends on the nature and requirements of the IoT application. Blockchain technology can provide authentication, access control, and trust management to IoT applications.

2.5.3 Machine learning solutions

Machine learning (ML) is a promising technology that offers embedded intelligence to IoT devices to cope with different security issues. It is a subset of artificial intelligence (AI) that can be used to develop intelligent security systems for IoT networks. Various types of attacks launched on IoT systems, such as DoS attacks, can be detected and mitigated using ML

techniques. The ML algorithms can also be used to detect anomalies and intrusions in IoT networks [58].

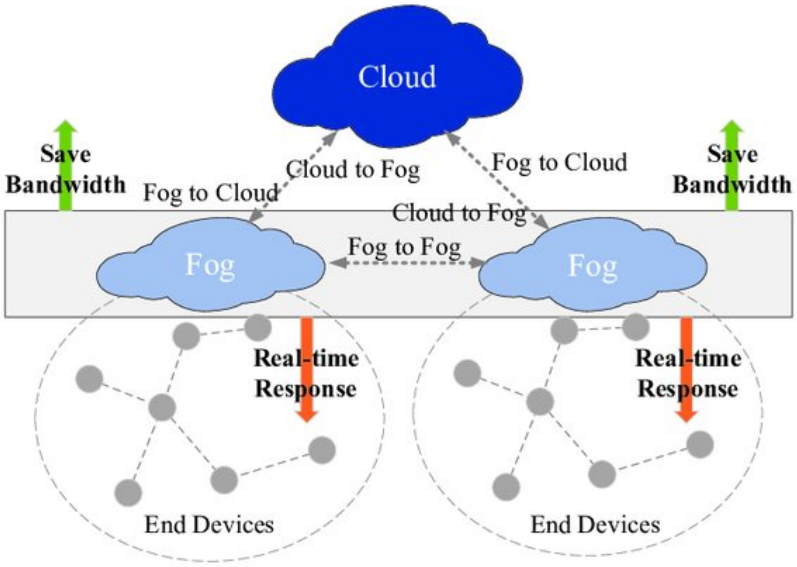

Figure 2.4: Fog Computing architecture [59]

2.5.4 Fog computing solution

Fog computing has been introduced as a new paradigm to extend the computational resources of Cloud computing. It offers computation, storage, and networking/communication at the network side [59]. Fog computing architecture consists of fog nodes deployed near IoT devices and connected to the cloud server, as shown in Figure 2.4.

The fog architecture decreases the volume of data transferred between the IoT devices and the cloud infrastructure. Fog computing supports mobility, location awareness, low latency, heterogeneity, scalability and can be ideally adapted into real-time or latency-sensitive IoT applications. Since IoT devices are limited in terms of resources, fog nodes can provide several security requirements such as authentication , privacy-preserving, and encryption to secure IoT environments [60, 61].

2.6 Related Works

Researches address the inherent resource limitations of IoT devices that make it challenging to apply conventional encryption algorithms that require a significant amount of resources for

their operation. They cope with these challenges by proposing lightweight encryption techniques to provide efficient and secure communication and reasonable resource utilization.

Singh et al. [62] have elaborated on several features of lightweight cryptography. They proposed a lightweight hybrid algorithm designed for IoT devices. It can determine which LWC algorithm is suitable for a specific device. This decision is made based on memory storage and power of the device besides the computational power needed to perform the LWC algorithm.

In the study by Ammar et al. [63], eight different IoT frameworks have been presented, along with the requirements to develop third-party applications for IoT systems. The primary security need in every IoT application and framework is Authentication and access control. This study helps the developers to enhance the security and design of systems and applications they produce.

Since learning algorithms have a success rate in security and privacy, Hasan et al. [64] presented a comparative study of the performance of several machine learning models to detect and predict attacks and anomalies on the IoT systems accurately. The study found that the random forest model can accurately predict attacks in the IoT environment than other approaches.

In Medileh et al. [65], authors proposed a flexible encryption technique to secure data while transmitting and storing this data. The flexibility of this technique comes with the ability to choose the number of rounds used to cipher information and a smaller key overhead size, which leads to an improvement in encryption time without reducing security levels.

2.7 Conclusion

In this chapter, we presented several security attacks and threats that endanger the security of the IoT environment, along with the requirements and solutions proposed to overcome these issues. We also reviewed recent related works that were proposed to achieve IoT security.

In the next chapter, we present our proposed encryption technique that considers the advantages and limitations of related work to enhance the security of IoT systems.

CHAPTER 3

THE PROPOSED CONTRIBUTION

3.1 Introduction

The Internet of Things (IoT) is an evolving paradigm that has been known as a revolutionary technology of this century. It enables devices to communicate seamlessly with each other to provide services without human interference [66]. The primary aim of the IoT is to improve human life continuously through its smartness and intelligence.

These devices can gather and share sensible data through the network, allowing attackers to reveal private information. Hence, it is compulsory to ensure privacy-preserving in IoT environments [67].

Cryptography is a powerful method for protecting the transmitted data in wireless channels [68]. It involves encryption and decryption processes and has two main types: symmetric and asymmetric techniques. Symmetric cryptography uses one key to encrypt and decrypt the data, while asymmetric cryptography requires two keys, a public key for encryption and a private key for decryption. Traditional cryptographic algorithms are inadequate for resource-constrained IoT devices because they demand extensive resources (i.e., processing and memory). Consequently, attaining a good level of security with lightweight procedures is challenging [69].

Lightweight cryptography has attracted significant attention lately. It aims to optimize conventional cryptographic algorithms and provide lightweight security solutions for resource-constrained devices [70].

In this chapter, we propose an improved asymmetric lightweight security scheme to achieve privacy-preserving in the IoT.

3.2 Global scheme

In this section, we will present the overall scheme of our proposal, as the following figure illustrates all the steps from the generation and calculation of keys to the encryption and decryption of the messages.

We concentrate on how to provide a linear, cyclic asymmetric encryption that will lightweight and boost the encryption time and maintain effective and secure encryption against attacks.

Our proposal encryption scheme consists of three processes: key generation, encryption, and decryption.

- **Key generation:** that returns a secret Sk and public key Pk, (Sk, Pk) = (k, k + r × p).

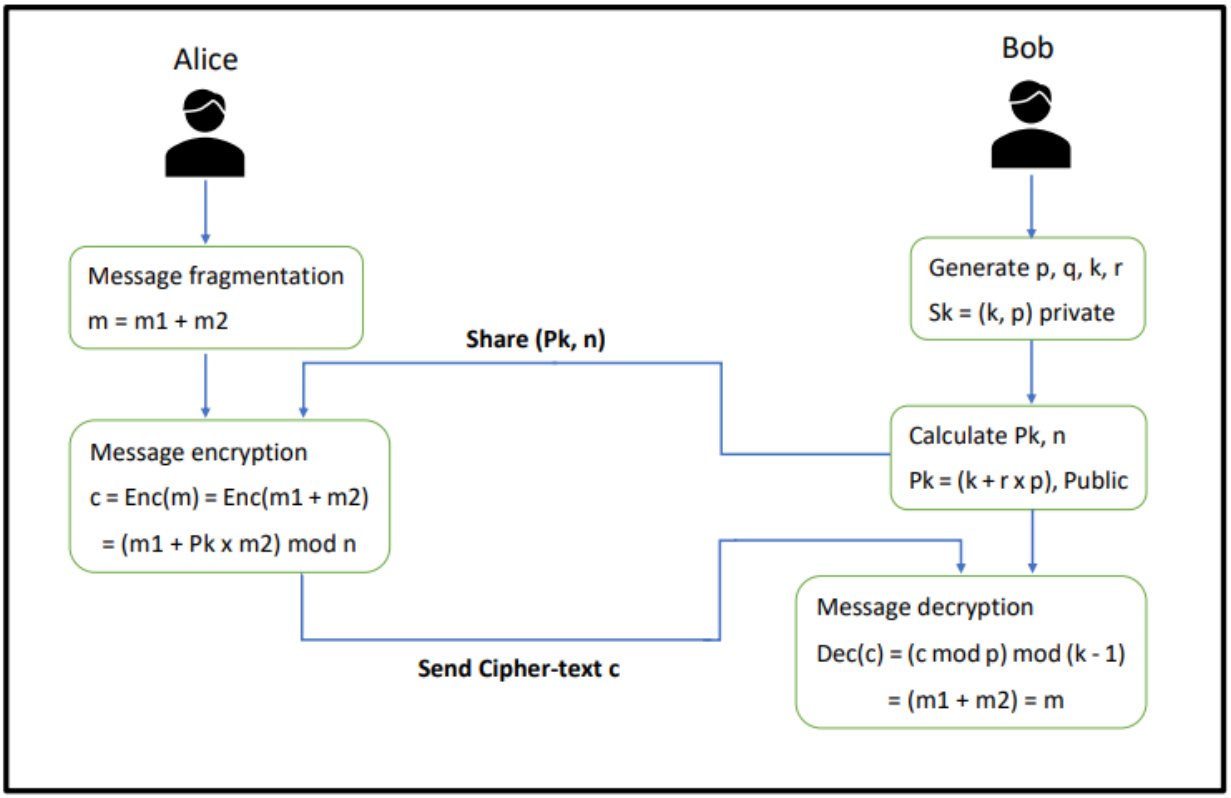

Figure 3.1: The proposal global scheme

- **Encryption Enc(m):** which encrypt a plain text m using the public key Pk, c = (m' + m" × pk) mod n.
- **Decryption Dec(c):** which decrypt a ciphered text using the secret key Sk, m = (c mod p) mod (k - 1)

3.3 Encryption and decryption process

3.3.1 Key generation process

Bob will generate p and q, which are two large prime numbers where p != q. Then, he will general a random number r and a secrete key Sk = k which is used later to decrypt the received cipher-text from Alice.

After that, Bob calculates the public key Pk and n that will be shared with Alice over the network to encrypt the data.

$$Pk = k + r * p \tag{3.1}$$

$$n = p * q \tag{3.2}$$

Algorithm 1 Key-Pair Generation

1: **Require Private**: p,q:Two large prime numbers, k:large random number, r(Nonce), Sk.
2: **Require Public**: n, Pk.
3: **Ensure:** p > r > q , k.
4: Sk ← k
5: Pk ← k + r * p
6: n ← p * q
7: **Return** (Sk,(Pk,n))

This phase will return the private key Sk and the public key Pk along with n.

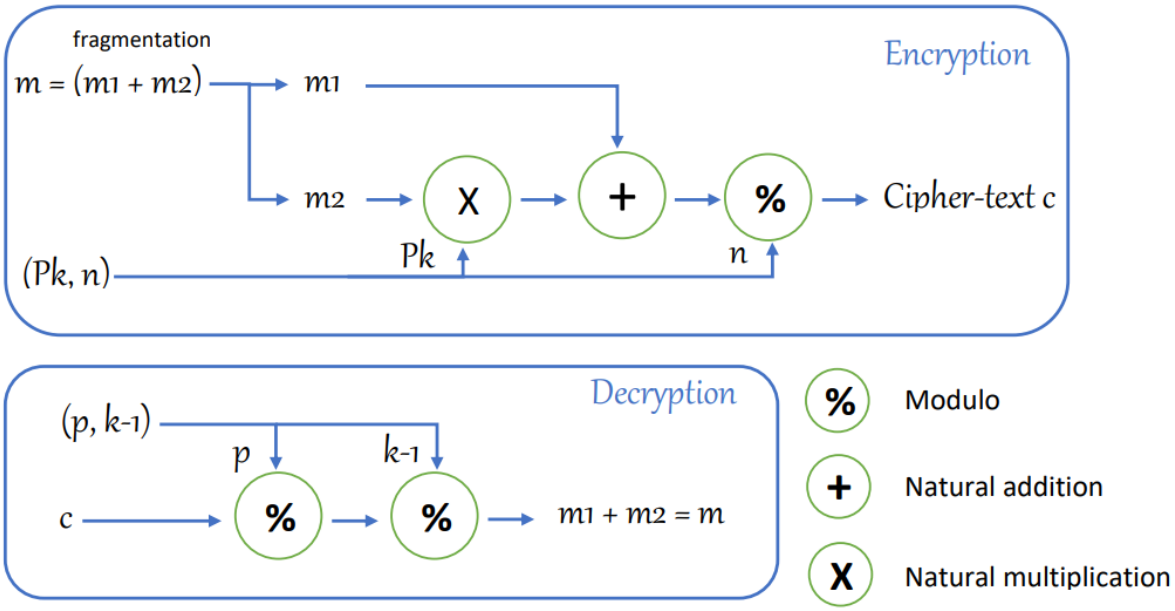

Figure 3.2: Encryption and decryption illustration

3.3.2 Encryption process

Asymmetric encryption of the proposed scheme enables Alice to send Bob a ciphered-text utilizing the shared public key, which works as illustrated in Figure 3.2.

Alice randomly fragments the message m into m1 and m2 in which m = m1 + m2. The reason behind the fragmentation of the message is to make it more difficult for the attacker to find the used m1 and m2 in order to extract p.

After that, Alice encrypt the message using Bob's public key and the message fragments as illustrated in Figure 3.2 using the formula:

$$c = (m1 + Pk * m2) \bmod n \tag{3.3}$$

Algorithm 2 Encryption

1: **Required Public**: n, Pk

2: **Ensure:** m = m1 + m2

3: c ← (m1+ m2 * Pk) mod n

4: **Return** c

This equation returns the cipher-text c, which is then sent to Bob for decryption .

3.3.3 Decryption process

Bob receive the ciphered-text and lunch the decryption process as shown in Figure 3.2.

Algorithm 3 Decryption

1: **Required Private**: p,k

2: **Required Public**: c (Cipher data)

3: **Ensure:** c

4: m ← (c mod p)mod (k-1)

5: **Return** m

- We have $c = m1 + m2 * Pk$, and $Pk = k + r * p$ so we get $c = m1 + m2 * (k + r * p)$.
- $c = m1 + k * m2 + r * p * m2$ then $c \bmod p = m1 + k * m2$ because m2 x r × p mod p = 0.
- the last step is $(c \bmod p) \bmod (k - 1) = m1 + m2 = m$

After the last step, Bob can fully reveal the message content sent by Alice.

3.4 Conclusion

In conclusion, we observe the benefits of public-key encryption(asymmetric encryption). We chose to introduce a global encryption scheme comprising a key generator algorithm and an encryption algorithm with its corresponding decryption algorithm to reap those benefits. The encryption algorithm is an affine encryption algorithm of the form F(x) = (ax+b) mod m, but that does not make it limited to monoalphabetic substitution. This type of function was chosen for the ease of computation, and other advantages, chief among them is the added benefit of randomness using the parameter m (plaintext), which elevates the level of entropy in the system and mitigates the shortcomings of this kind of encryption through fragmentation to achieve the desired effect and negate any predictable pattern that an adversary might try to exploit. All these benefits and more will be explored in the next chapter.

CHAPTER 4

EXPERIMENTS AND EVALUATION

4.1 Introduction

In the previous chapter, we presented our proposed lightweight encryption technique to encrypt/decrypt data in the IoT environment. In this chapter, we will implement our proposal; then, we will analyze it in terms of execution time, storage space, factorization number problem, and robustness against different attacks like the Man-in-the-middle attack (MiTM), Brute-force attack, Plaintext Attack, and Chosen-Ciphertext Attack.

4.2 Development environment

In this section, we will mention the software and hardware used to implement and analyze our proposal.

4.2.1 Software environment

We used Python environment to implement our lightweight cryptography algorithm.

Python is an interpreted high-level programming language with an object-oriented paradigm and dynamic semantics. It is high-level built-in data structures, combined with dynamic typing and dynamic binding, make it very attractive for Rapid Application Development and for use as a scripting or glue language to connect existing components [71].

We used Python for our proposed lightweight encryption technique project because it is rich with ready-to-use libraries that make the programming process easier for us, which allowed us to focus more on the idea for the project.

4.2.2 Hardware environment

The application was developed on a Desktop PC (Generic) that have the following characteristics:

- **processor :** AMD Ryzen 5 3400G with Radeon Vega Graphics, 3700 Mhz, 4 Core(s), 8 Logical Processor(s)
- **Installed Physical Memory (RAM) :** 14.00 GB.
- **Disk drive :** ADATA SU630 240GB.
- **Graphic card :** AMD Radeon RX Vega 11
- **Operating system (OS) :** Microsoft Windows 10 Pro x64-based.

4.3 RSA Algorithm

Public key Cryptography, also known as asymmetric encryption, is a cryptosystem that uses two keys, public and private keys, for encryption and decryption. This type of cryptosystem helps in achieving confidentiality, authentication, or both. Public key cryptography includes key exchange, digital signatures, and encryption of blocks of data. Among the public key cryptosystem algorithms, RSA is the most widely used. It is a secure method for transmitting data. It is a block cipher system, which is based on number theory. RSA includes Key generation, encryption, and decryption steps. The security of RSA depends on the factorization of numbers.

In the next section, we are going to compare our proposal encryption algorithm with the RSA algorithm in terms of encryption and decryption execution time along with storage space of the ciphered-text

4.4 Evaluation criteria and discussion

4.4.1 Execution time

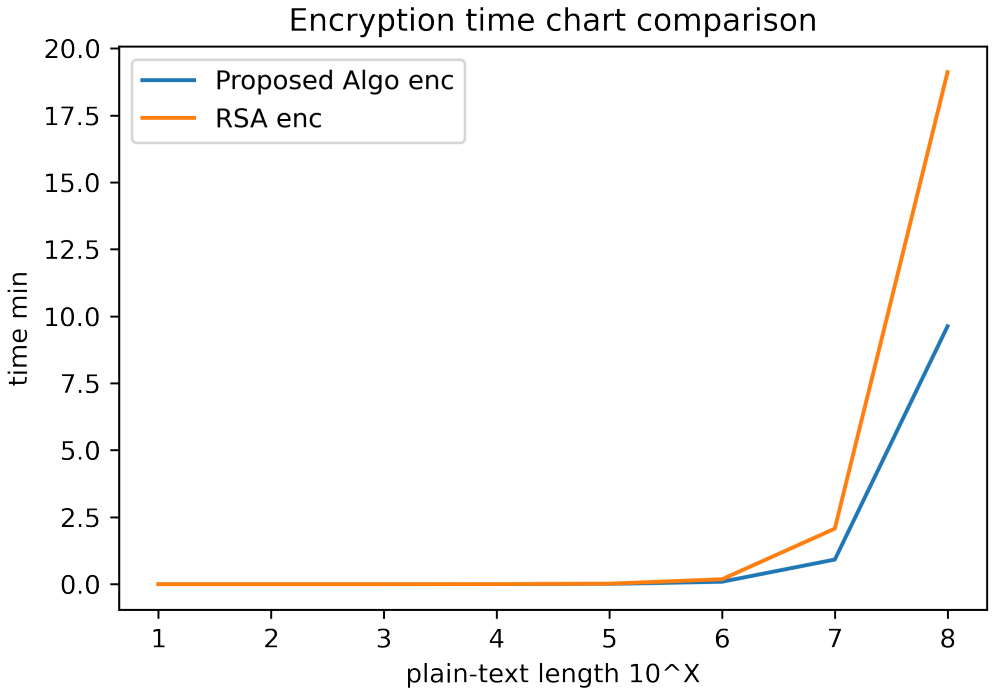

Figure 4.1: Encryption time comparison

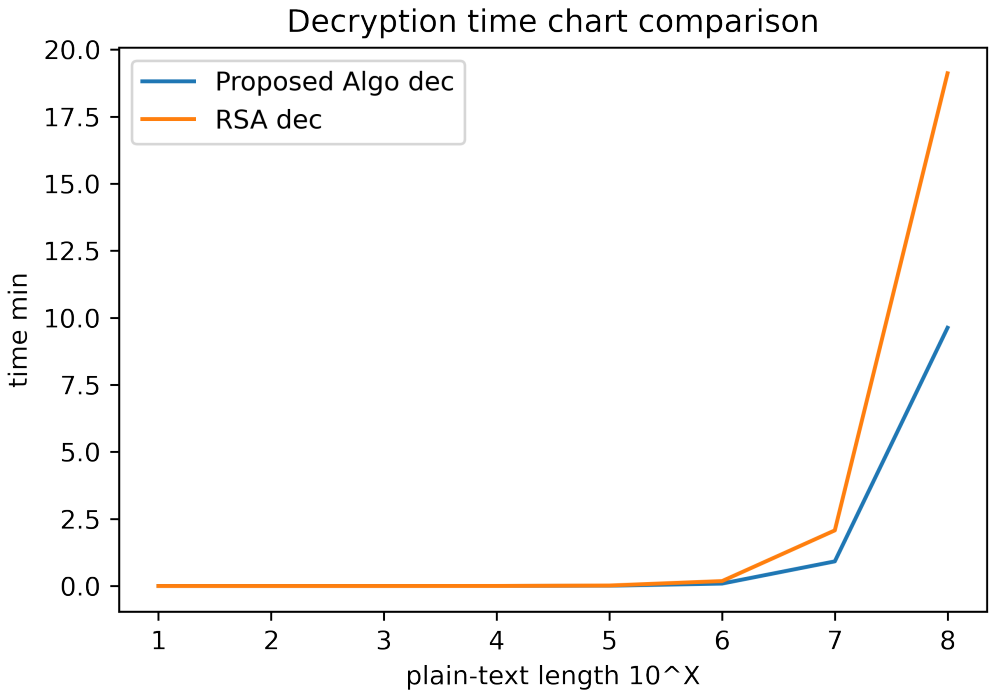

Figure 4.2: Decryption time comparison

Figure 4.1, 4.2 represents the results produced by the aggregation of multiple test results of the execution time of both the encryption and decryption of the proposed algorithm and RSA.

In that group of tests, we tested for the encryption time with a plain-text of varying lengths from 10^1 to 10^8 (multiple iterations through the same test) and with different keys in each test.

We found that the proposed algo is more efficient encryption-wise, as it takes 50% less time to execute than the RSA, decryption wise the proposed algo takes 97% less time to execute.

In each test, the same parameters (p,q) are used to generate keys for the Proposed algo and the RSA Algo, thus saving more power and increasing process speed, especially on resource-limited and constrained devices.

4.4.2 Storage space

Figure 4.3 shows the results pertaining to storage space criteria, with the same conditions as the previous series of tests. These tests demonstrate that the proposed algo produces cipher-texts that save 40% storage space when compared to the ciphers produced by RSA.

4.4.3 Factorization number and Brute-force attack

The integer Factorization problem in an np-hard problem revolves around the decomposition of integers into a product of small integers. If these composing factors are prime numbers, the

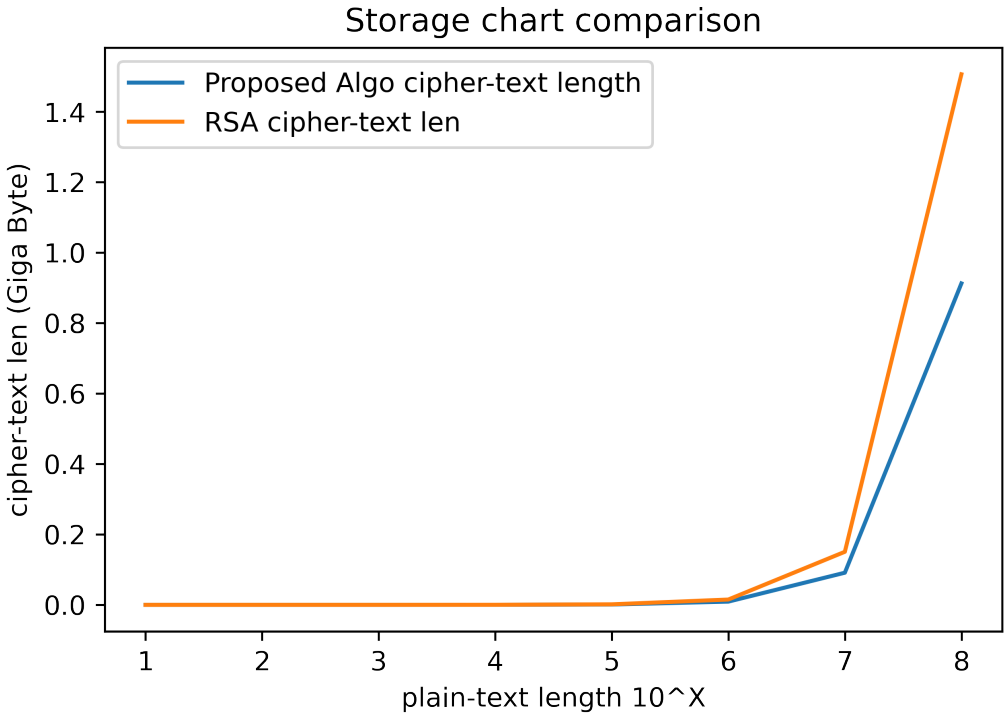

Figure 4.3: Storage space comparison

problem Is known as Prime factorization.

Prime factorization is a hard and difficult problem to solve, especially when semi-primes are involved, which are the product of two prime numbers. The difficulty stems from both the randomness and the size of those numbers. This property made it so that it is beneficial in the field of asymmetric cryptography as the adversary can use the numbers for key generation and encryption/decryption.

One of the useful use cases of integer factorization is securing against Brute force attacks, which attempts to guess the correct password or key by calculating all possible combinations.

In our scenario for example : it would be to calculate all possible values of k to try to factorize a number greater than n (a semi prime) because :$Pk - k = k + r * p = r * p$ where $r > q => r * p > p * q => r * p > n$, which is extremely difficult to achieve on a classical computer.

4.4.4 Chosen Plain/Cipher-text and MiTM Attacks

Chosen plain-text attack and chosen cipher-text attack can be used in tandem with MiTM attack to try to obtain the secret key.

In the case of the chosen cipher-text attack, the attacker can intercept cipher-text c and

replace it with cipher-text c', and then tries to gather information through obtaining the full or partial decryption of the chosen cipher-text c' (m'). Consequently, he can use that info to recover the hidden secret key (Sk) used for decryption.

In the scenario of chosen cipher-text attack, which is applied to the encryption function as opposed to the CCTA that targets the decryption function. The attacker chooses a plain text p' and views their corresponding encryption; this kind of attack is always available to the adversary in a scenario of public-key cryptography due to the availability of the public key (Pk).

Both these attacks try to exploit the malleability property of some cryptographic algorithms, which is defined as the ability to produce a cipher-text c' by modifying a cipher-text c which produces upon decryption a plain-text m' that is related to m the plain-text of c.

In the proposed scheme, we exploit the randomness of the fragmentation, making the algorithm non-deterministic in hopes of guarantying semantic security or cipher-text indistinguishability, which leads to the extraction of minor information at best, resulting in immunity against chosen plain text attacks.

4.5 Conclusion

In conclusion, we find that the exploitation of the mathematical properties of semi primes and the randomness property of fragmentation yields beneficial results in increasing the robustness of the proposed algorithm against brute force attacks and the MiTM by mitigating some of its correlated attacks such as Chosen cipher-text attack and Chosen Plain text attacks.

4.6 General Conclusion

Nowadays, the IoT serves a significant part of our daily life. Billions of smart and independent things across the world are connected and communicate with each other. These objects can generate, collect, analyze, process, and exchange data to provide high-level services. With the enormous number of new devices expected to be connected to the Internet in the upcoming years, there is a wide variety of potential privacy and security dangers encountered by this expanding network. Hence, secure architectures and frameworks are required, enabling the IoT system to identify whether it is under attack and enhance the protection mechanisms. Nevertheless, such approaches cannot use traditional security protocols (RSA, TLS, etc..) because they do not guarantee good performance and are not proper for resource-constrained IoT devices.

In this thesis, we investigated the security and privacy concerns and proposed lightweight and robust mechanisms to improve IoT security without affecting the performance requirements. Initially, we analyzed the IoT security vulnerabilities and attacks of each layer. Then, we presented a taxonomy of IoT security attacks based on levels, purposes, and countermeasures. We also introduced a classification of IoT security requirements based on the attacks' objectives. This analysis can help developers and researchers design new projects to address the security concerns of IoT systems.

Furthermore, we gave a comparative analysis with standard methods regarding computation cost, storage cost, and security requirements. The evaluation outcomes illustrated that our proposed scheme is more lightweight and robust.

4.7 Future works

Regardless of the proposed security mechanism for IoT is very promising and provides a good level of security with very acceptable performance. There are other related topics that should be carried out to strengthen IoT security. Some of the future perspectives are listed as follows:

- Enhance the proposed schemes in terms of efficiency without affecting the security provisions.
- Identify user anomalies in IoT ecosystems using blockchain technology and machine learning algorithms.

BIBLIOGRAPHY

[1] J. Rifkin, *The zero marginal cost society: The internet of things, the collaborative commons, and the eclipse of capitalism.* St. Martin's Press, 2014.

[2] D. Evans, "The internet of things: How the next evolution of the internet is changing everything," *CISCO white paper*, vol. 1, no. 2011, pp. 1–11, 2011.

[3] O. Vermesan and P. Friess, *Internet of things: converging technologies for smart environments and integrated ecosystems.* River publishers, 2013.

[4] K. K. Patel, S. M. Patel *et al.*, "Internet of things-iot: definition, characteristics, architecture, enabling technologies, application & future challenges," *International journal of engineering science and computing*, vol. 6, no. 5, 2016.

[5] "Internet of things," https://www.azinovatechnologies.com/blog/the-internet-of-things-technological-bliss-or-dystopia/, accessed: 2021-05-25.

[6] Z. Yan, P. Zhang, and A. V. Vasilakos, "A survey on trust management for internet of things," *Journal of network and computer applications*, vol. 42, pp. 120–134, 2014.

[7] I. Saif, S. Peasley, and A. Perinkolam, "Safeguarding the internet of things: Being secure, vigilant, and resilient in the connected age," *Deloitte Review*, vol. 17, 2015.

[8] R. Roman, J. Zhou, and J. Lopez, "On the features and challenges of security and privacy in distributed internet of things," *Computer Networks*, vol. 57, no. 10, pp. 2266–2279, 2013.

[9] Y. Harbi, Z. Aliouat, S. Harous, A. Bentaleb, and A. Refoufi, "A review of security in internet of things," *Wireless Personal Communications*, vol. 108, no. 1, pp. 325–344, 2019.

[10] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of things (iot): A vision, architectural elements, and future directions," *Future generation computer systems*, vol. 29, no. 7, pp. 1645–1660, 2013.

[11] A. Botta, W. De Donato, V. Persico, and A. Pescapé, "Integration of cloud computing and internet of things: a survey," *Future generation computer systems*, vol. 56, pp. 684–700, 2016.

[12] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of things: A survey on enabling technologies, protocols, and applications," *IEEE communications surveys & tutorials*, vol. 17, no. 4, pp. 2347–2376, 2015.

[13] C. Bormann, A. P. Castellani, and Z. Shelby, "Coap: An application protocol for billions of tiny internet nodes," *IEEE Internet Computing*, vol. 16, no. 2, pp. 62–67, 2012.

[14] S. Ullah, M. Ali, A. Hussain, and K. S. Kwak, "Applications of uwb technology," *arXiv preprint arXiv:0911.1681*, 2009.

[15] K. Curran, A. Millar, and C. Mc Garvey, "Near field communication," *International Journal of Electrical and Computer Engineering*, vol. 2, no. 3, p. 371, 2012.

[16] I. Lee and K. Lee, "The internet of things (iot): Applications, investments, and challenges for enterprises," *Business Horizons*, vol. 58, no. 4, pp. 431–440, 2015.

[17] F. Zantalis, G. Koulouras, S. Karabetsos, and D. Kandris, "A review of machine learning and iot in smart transportation," *Future Internet*, vol. 11, no. 4, p. 94, 2019.

[18] "Smart retail," https://www.kaaproject.org/retail, accessed: 2021-05-25.

[19] "Iot architecture layer," https://waziup.org/courses/iotfundamentals/, accessed: 2021-05-25.

[20] M. Kocakulak and I. Butun, "An overview of wireless sensor networks towards internet of things," in *2017 IEEE 7th annual computing and communication workshop and conference (CCWC)*. IEEE, 2017, pp. 1–6.

[21] "Wireless sensors network architecture," https://www.electronicshub.org/wireless-sensor-networks-wsn/, accessed: 2021-05-25.

[22] X. Jia, Q. Feng, T. Fan, and Q. Lei, "Rfid technology and its applications in internet of things (iot)," in *2012 2nd international conference on consumer electronics, communications and networks (CECNet)*. IEEE, 2012, pp. 1282–1285.

[23] "Network topologies of zigbee," https://www.electricaltechnology.org/2017/09/zigbee-technology-wireless-networking-system.html, accessed: 2021-05-26.

[24] A. Zigbee, "Zigbee specification," *ZigBee document 053474r13*, 2006.

[25] I. W. Group *et al.*, "Wireless medium access control and physical layer specifications for low-rate wireless personal area networks," *IEEE Standard*, vol. 802, no. 4, p. 2003, 2003.

[26] J. Li, X. Zhu, N. Tang, and J. Sui, "Study on zigbee network architecture and routing algorithm," in *2010 2nd International Conference on Signal Processing Systems*, vol. 2. IEEE, 2010, pp. V2–389.

[27] M. Woolley, "Bluetooth core specification v5." Bluetooth, 2019.

[28] G. Mulligan, "The 6lowpan architecture," in *Proceedings of the 4th workshop on Embedded networked sensors*, 2007, pp. 78–82.

[29] G. Montenegro, N. Kushalnagar, J. Hui, D. Culler *et al.*, "Transmission of ipv6 packets over ieee 802.15. 4 networks," *Internet proposed standard RFC*, vol. 4944, p. 130, 2007.

[30] T. Winter, P. Thubert, A. Brandt, J. W. Hui, R. Kelsey, P. Levis, K. Pister, R. Struik, J.-P. Vasseur, R. K. Alexander *et al.*, "Rpl: Ipv6 routing protocol for low-power and lossy networks." *rfc*, vol. 6550, pp. 1–157, 2012.

[31] N. Sornin, M. Luis, T. Eirich, T. Kramp, and O. Hersent, "Lorawan specification," *LoRa alliance*, 2015.

[32] J. d. C. Silva, J. J. Rodrigues, J. Al-Muhtadi, R. A. Rabêlo, and V. Furtado, "Management platforms and protocols for internet of things: A survey," *Sensors*, vol. 19, no. 3, p. 676, 2019.

[33] "Mqtt architecture," http://istsos.org/en/trunk/doc/ws_mqtt.html, accessed: 2021-05-26.

[34] Z. Shelby, K. Hartke, and C. Bormann, "The constrained application protocol (coap)," 2014.

[35] I. Andrea, C. Chrysostomou, and G. Hadjichristofi, "Internet of things: Security vulnerabilities and challenges," in *2015 IEEE symposium on computers and communication (ISCC)*. IEEE, 2015, pp. 180–187.

[36] S. Singh and N. Singh, "Internet of things (iot): Security challenges, business opportunities & reference architecture for e-commerce," in *2015 International Conference on Green Computing and Internet of Things (ICGCIoT)*. Ieee, 2015, pp. 1577–1581.

[37] T. Borgohain, U. Kumar, and S. Sanyal, "Survey of security and privacy issues of internet of things," *arXiv preprint arXiv:1501.02211*, 2015.

[38] Q. Jing, A. V. Vasilakos, J. Wan, J. Lu, and D. Qiu, "Security of the internet of things: perspectives and challenges," *Wireless Networks*, vol. 20, no. 8, pp. 2481–2501, 2014.

[39] S. Cesare, "Breaking the security of physical devices," *Presentation at Blackhat*, vol. 14, 2014.

[40] J. Granjal, E. Monteiro, and J. S. Silva, "Security for the internet of things: a survey of existing protocols and open research issues," *IEEE Communications Surveys & Tutorials*, vol. 17, no. 3, pp. 1294–1312, 2015.

[41] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, "Security, privacy and trust in internet of things: The road ahead," *Computer networks*, vol. 76, pp. 146–164, 2015.

[42] K. Zhao and L. Ge, "A survey on the internet of things security," in *2013 Ninth international conference on computational intelligence and security*. IEEE, 2013, pp. 663–667.

[43] K. Zhang, X. Liang, R. Lu, and X. Shen, "Sybil attacks and their defenses in the internet of things," *IEEE Internet of Things Journal*, vol. 1, no. 5, pp. 372–383, 2014.

[44] V. Soni, P. Modi, and V. Chaudhri, "Detecting sinkhole attack in wireless sensor network," *International Journal of Application or Innovation in Engineering & Management*, vol. 2, no. 2, pp. 29–32, 2013.

[45] P. Lee, A. Clark, L. Bushnell, and R. Poovendran, "A passivity framework for modeling and mitigating wormhole attacks on networked control systems," *IEEE Transactions on Automatic Control*, vol. 59, no. 12, pp. 3224–3237, 2014.

[46] M. Nawir, A. Amir, N. Yaakob, and O. B. Lynn, "Internet of things (iot): Taxonomy of security attacks," in *2016 3rd International Conference on Electronic Design (ICED)*. IEEE, 2016, pp. 321–326.

[47] E. Alsaadi and A. Tubaishat, "Internet of things: features, challenges, and vulnerabilities," *International Journal of Advanced Computer Science and Information Technology*, vol. 4, no. 1, pp. 1–13, 2015.

[48] X. Yang, E. Karampatzakis, C. Doerr, and F. Kuipers, "Security vulnerabilities in lorawan," in *2018 IEEE/ACM Third International Conference on Internet-of-Things Design and Implementation (IoTDI)*. IEEE, 2018, pp. 129–140.

[49] A. Marzano, D. Alexander, O. Fonseca, E. Fazzion, C. Hoepers, K. Steding-Jessen, M. H. Chaves, Í. Cunha, D. Guedes, and W. Meira, "The evolution of bashlite and mirai iot botnets," in *2018 IEEE Symposium on Computers and Communications (ISCC)*. IEEE, 2018, pp. 00 813–00 818.

[50] M. M. Hossain, M. Fotouhi, and R. Hasan, "Towards an analysis of security issues, challenges, and open problems in the internet of things," in *2015 ieee world congress on services*. IEEE, 2015, pp. 21–28.

[51] L. Atzori, A. Iera, and G. Morabito, "The internet of things: A survey," *Computer networks*, vol. 54, no. 15, pp. 2787–2805, 2010.

[52] J. Liu, Y. Xiao, and C. P. Chen, "Internet of things' authentication and access control," *International Journal of Security and Networks*, vol. 7, no. 4, pp. 228–241, 2012.

[53] A. R. Sfar, E. Natalizio, Y. Challal, and Z. Chtourou, "A roadmap for security challenges in the internet of things," *Digital Communications and Networks*, vol. 4, no. 2, pp. 118–137, 2018.

[54] E. Oriwoh, H. al Khateeb, and M. Conrad, "Responsibility and non-repudiation in resource-constrained internet of things scenarios." International Conference on Computing and Technology Innovation (CTI 2015), 2016.

[55] P. Kasinathan, C. Pastrone, M. A. Spirito, and M. Vinkovits, "Denial-of-service detection in 6lowpan based internet of things," in *2013 IEEE 9th international conference on wireless and mobile computing, networking and communications (WiMob)*. IEEE, 2013, pp. 600–607.

[56] S. S. Dhanda, B. Singh, and P. Jindal, "Lightweight cryptography: A solution to secure iot," *Wireless Personal Communications*, vol. 112, no. 3, pp. 1947–1980, 2020.

[57] Y. Maleh, M. Shojafar, M. Alazab, and I. Romdhani, *Blockchain for cybersecurity and privacy: architectures, challenges, and applications*. CRC Press, 2020.

[58] M. A. Al-Garadi, A. Mohamed, A. K. Al-Ali, X. Du, I. Ali, and M. Guizani, "A survey of machine and deep learning methods for internet of things (iot) security," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 3, pp. 1646–1685, 2020.

[59] F. Bonomi, R. Milito, J. Zhu, and S. Addepalli, "Fog computing and its role in the internet of things," in *Proceedings of the first edition of the MCC workshop on Mobile cloud computing*, 2012, pp. 13–16.

[60] H. Li and T. Jing, "A ciphertext-policy attribute-based encryption scheme with public verification for an iot-fog-cloud architecture," *Procedia Computer Science*, vol. 174, pp. 243–251, 2020.

[61] A. Alrawais, A. Alhothaily, C. Hu, X. Xing, and X. Cheng, "An attribute-based encryption scheme to secure fog communications," *IEEE access*, vol. 5, pp. 9131–9138, 2017.

[62] S. Singh, P. K. Sharma, S. Y. Moon, and J. H. Park, "Advanced lightweight encryption algorithms for iot devices: survey, challenges and solutions," *Journal of Ambient Intelligence and Humanized Computing*, pp. 1–18, 2017.

[63] M. Ammar, G. Russello, and B. Crispo, "Internet of things: A survey on the security of iot frameworks," *Journal of Information Security and Applications*, vol. 38, pp. 8–27, 2018.

[64] M. Hasan, M. M. Islam, M. I. I. Zarif, and M. Hashem, "Attack and anomaly detection in iot sensors in iot sites using machine learning approaches," *Internet of Things*, vol. 7, p. 100059, 2019.

[65] S. Medileh, A. Laouid, R. Euler, A. Bounceur, M. Hammoudeh, M. AlShaikh, A. Eleyan, O. A. Khashan *et al.*, "A flexible encryption technique for the internet of things environment," *Ad Hoc Networks*, vol. 106, p. 102240, 2020.

[66] A. Whitmore, A. Agarwal, and L. Da Xu, "The internet of things—a survey of topics and trends," *Information systems frontiers*, vol. 17, no. 2, pp. 261–274, 2015.

[67] Y. Harbi, Z. Aliouat, A. Refoufi, and S. Harous, "Efficient end-to-end security scheme for privacy-preserving in iot," in *2019 International Conference on Networking and Advanced Systems (ICNAS)*. IEEE, 2019, pp. 1–6.

[68] S. Vaudenay, *A classical introduction to cryptography: Applications for communications security*. Springer Science & Business Media, 2006.

[69] H. Hellaoui, M. Koudil, and A. Bouabdallah, "Energy-efficient mechanisms in security of the internet of things: A survey," *Computer Networks*, vol. 127, pp. 173–189, 2017.

[70] K. McKay, L. Bassham, M. Sönmez Turan, and N. Mouha, "Report on lightweight cryptography," National Institute of Standards and Technology, Tech. Rep., 2016.

[71] G. van Rossum, "What is python? executive summary," 1998.