F. BINGLAW

ATILIM UNIVERSITY 2021

SECURITY ISSUES IN THE INTERNET OF THINGS: REQUIREMENTS, ATTACKS AND COUNTERMEASURES

THE GRADUATE SCHOOL OF NATURAL AND APPLIED SCIENCES
OF
ATILIM UNIVERSITY

FTAYEM BINGLAW

A MASTER OF SCIENCE THESIS
IN
INFORMATION TECHNOLOGY

JANUARY 2021

SECURITY ISSUES IN THE INTERNET OF THINGS: REQUIREMENTS, ATTACKS AND COUNTERMEASURES

A THESIS SUBMITTED TO
THE GRADUATE SCHOOL OF NATURAL AND APPLIED SCIENCES
OF
ATILIM UNIVERSITY

BY

FTAYEM BINGLAW

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS
FOR
THE DEGREE OF MASTER
IN
INFORMATION TECHNOLOGY

JANUARY 2021

Approval of the Graduate School of Natural and Applied Sciences, Atilim University.

_____

Prof. Dr. Ali KARA
Director

I certify that this thesis satisfies all the requirements as a thesis for the degree of **Master of Science in Information Technology, Atilim University**.

_____

Assoc. Prof. Dr. Korhan Levent ERTÜRK
Head of Department

This is to certify that we have read the thesis SECURITY ISSUES IN THE INTERNET OF THINGS: REQUIREMENTS, ATTACKS AND COUNTERMEASURES submitted by FTAYEM BINGLAW and that in our opinion it is fully adequate, in scope and quality, as a thesis for the degree of Master of Science.

_____

Prof. Dr. Murat KOYUNCU
Supervisor

Assoc. Prof. Dr. Tolga PUSATLI
Mathematics Department, Çankaya University _____

Prof. Dr. Murat KOYUNCU
Information Sys. Eng. Department, Atilim University _____

Asst. Prof. Dr. Ziya KARAKAYA
Computer Eng. Department, Atilim University _____

Date: 13.01.2021

I hereby declare that all information in this document has been obtained and presented in accordance with academic rules and ethical conduct. I also declare that, as required by these rules and conduct, I have fully cited and referenced all material and results that are not original to this work.

Name, Last Name :

Signature :

ABSTRACT

SECURITY ISSUES IN THE INTERNET OF THINGS: REQUIREMENTS, ATTACKS AND COUNTERMEASURES

Binglaw, Ftayem

M.S., Information Technology

Supervisor: Prof. Dr. Murat Koyuncu

JANUARY 2021, 186 pages

The Internet of Things (IoT) is a development of the traditional Internet, as it not only connects people however also things. The IoT helps these things see, listen and take action by making them talk together with minimal human intervention to make people's lives easier. Due to the nature of IoT systems, which includes the exchange of personal information in most of its applications, it will be the target of attacks and security threats that will undermine consumer confidence in it. For this reason, defenses are required against these threats, which guarantee the availability of confidentiality and privacy in the IoT environment, among other things. In this thesis, we discussed the importance of security in IoT applications, while explaining the most important security requirements that the IoT must guarantee to judge it as a safe environment. Additionally, we covered the most common attacks targeting the IoT layers, namely the Perception, Network, and Application layer. Moreover, some countermeasures against these attacks have been mentioned. Finally, we talked about the smart home application as an example to identify the types of attack that may be exposed to it, and we prepared some recommendations and advice that stakeholders can benefit from to make the smart home more secure. We conclude from the study that security is one of the most important challenges standing in the way of adopting this important technology.

Keywords: Internet of Things, Security Requirements, Attacks, Countermeasures, Smart Home.

ÖZ

NESNELERİN İNTERNETİNDE GÜVENLİK KONULARI: GEREKSİNİMLER, SALDIRILAR VE KARŞI ÖNLEMLER

Binglaw, Ftayem

Y.L., Bilgi Teknolojileri

Tez Yöneticisi : Prof. Dr. Murat Koyuncu

OCAK 2021, 186 sayfa

Nesnelerin İnterneti (IoT), yalnızca insanları değil aynı zamanda nesneleri de birbirine bağladığı için geleneksel İnternet'in bir gelişmesidir. IoT, insanların hayatlarını kolaylaştırmak için minimum insan müdahalesiyle birlikte konuşmalarını sağlayarak bu nesnelerin görmesine, dinlemesine ve harekete geçmesine yardımcı olur. Uygulamalarının çoğunda kişisel bilgi alışverişini içeren IoT sistemlerinin doğası gereği, tüketicinin güvenini sarsacak saldırıların ve güvenlik tehditlerinin hedefi olacaktır. Bu nedenle, diğer hususların yanı sıra bu tehditlere karşı IoT ortamında gizlilik ve mahremiyetin mevcudiyetini garanti eden savunmalar gerekmektedir. Bu tezde, IoT'nin güvenli bir ortam olarak ele alınabilmesi için garanti edilmesi gereken en önemli güvenlik gereksinimlerini açıklarken, IoT uygulamalarında güvenliğin önemini tartıştık. Ek olarak, IoT katmanlarını Algılama, Ağ ve Uygulama katmanı bazında hedefleyen en yaygın saldırıları ele aldık. Ayrıca, bu saldırılara karşı bazı önlemlerden bahsedilmiştir. Son olarak, maruz kalabileceği saldırı türlerini belirlemek için örnek olarak akıllı ev uygulamasından bahsettik ve akıllı evi daha güvenli hale getirmek için paydaşların yararlanabileceği bazı öneriler ve tavsiyeler sunduk. Çalışma sonucunda, güvenliğin, bu önemli teknolojiyi benimseme yolunda duran en önemli zorluklardan biri olduğu sonucuna vardık.

Anahtar Kelimeler: Nesnelerin İnterneti, Güvenlik Gereksinimleri, Saldırılar, Karşı Tedbirler, Akıllı Ev

To my Family

ACKNOWLEDGMENTS

I thank everyone who helped me accomplish this work, especially my supervisor Prof. Dr. Murat Koyuncu and all the staff at Atilim University. I would also like to express my deepest thanks and gratitude to my family who supported me in achieving my goal of completing my postgraduate studies. Furthermore, I also find it my duty to thank the Center for Electronic Systems and Programming, the National Agency for Scientific Research and the Ministry of Higher Education that enabled me to study in Turkey. Finally, I am grateful to my country, Libya, which believed in my capabilities and the superiority of knowledge, and I hope that God will help me to serve, promote and advance it.

TABLE OF CONTENTS

LIST OF TABLES

TABLES

LIST OF FIGURES

FIGURES

LIST OF ABBREVIATIONS

ACK	Acknowledgment
2-ACKT	Two-way Acknowledgment-based Trust
ABAC	Attribute-Based Access Control
ACL	Access Control List
AES	Advanced encryption standard
AIDS	Anomaly-based Intrusion Detection System
AIS	Artificial Immune System
AP	Access Point
ARQ	Automatic Repeat Request
CapBAC	Capability-Based Access Control
CoT	Chain of Trust
CRC	Cyclic Redundancy Check
DAC	Discretionary Access Control
DDoS	Distributed Denial of Service
DNS	Domain Name Server
DNSBL	Domain Name System Black-Lists
DoS	Denial of Service
DSSS	Direct Sequence Spread Spectrum
DVR	Digital Video Recorders
ECC	Elliptic Curve Cryptography
ECC	Error Correction Code
ECG	Electrocardiography
ETSI	The European Telecommunications Standards Institute
FEC	Forward Error Correction
FHSS	Frequency Hopping Spread Spectrum

FTC	US Federal Trade Commission
GIS	Geographic Information System
GPS	Global Positioning System
HAN	Home Area Network
HIGHT	High security and lightweight
HMAC	Hash Message Authentication Code
HTTP	Hyper Text Transfer Protocol
HVAC	Heating, Ventilation and Airconditioning
ID	Identity
IDS	Intrusion Detection Systems
IoT	Internet of Things
IP	Internet Protocol
IPS	Intrusion Prevention System
ISP	Internet Service Provider
JTRG	Joint Test Action Group
LAN	Local Area Network
MAC	Message Authentication Code
MAC	Mandatory Access Control
MAC	Media Access Control
MCU	Micro-Controller Unit
MDT	Multi-Dataflow Topologies
MDS-VOW	Multi-Dimensional Scaling - Visualization Of Wormhole
MITM	Man-In-The-Middle
M2M	Machine-to-Machine
NAT	Network Address Translation
NIST	The National Institute of Standards and Technology
PCA	Principal Component Analysis
PDA	Personal Digital Assistant
PII	Personally Identifiable Information
PKI	Public Key Infrastructure

RAM	Random Access Memory
RBAC	Role-Based Access Control
RFID	Radio Frequency Identification
RM	Random Multicast
RSA	Rivest–Shamir–Adleman
RSS	Radio Signal Strength
RTT	Round-Trip Time
SHA	Secure Hash Algorithm
SIDS	Signature-based Intrusion Detection System
SSL	Secure Sockets Layer
SMRP	Secure Multi-hop Routing Protocol
SMS	Short Message Service
SNR	Signal to Noise Ratio
SSID	Service Set Identifier
TCP/IP	Transmission Control Protocol/Internet Protocol
UTM	Unified Threat Management
VLAN	Virtual Local Area Networks
VPN	Virtual Private Network
WPA	Wi-Fi Protected Access
WSN	Wireless Sensor Network
XSS	Cross-Site Scripting

CHAPTER 1

INTRODUCTION

Human interest and thought in connecting computers to each other appeared in the 1960s. With the development of this concept and the desire to use it to serve people, the Internet was born. Initially, Internet usage was limited, but over time, it became more ubiquitous and accessible to all people everywhere. With the great benefits that the Internet has given to mankind, everybody hastened to use it, and this has contributed to a huge rise in the number of devices connecting to the Internet. The Internet now includes millions of devices connected with the aim of exchanging information and acquiring knowledge in various fields; in industry, science, culture, education, entertainment and more [1].

The Internet we have all known has been focused largely on people for decision-making and execution. With the acceleration of the pace of life, the human mind has developed a new technology called the Internet of Things (IoT). The idea of this technology focuses on using the Internet as a universal way to allow the devices that people use in their daily lives to communicate with each other [2]. The first-time the term “Internet of Things” was used by Kevin Ashton in the late 1990s. The concept of the IoT has been defined as the system by which the Internet connects everyday physical objects in the world and makes them benefit from information gathered through sensors and Radio Frequency Identification (RFID) tags [3],[4].

The IoT contains a large variety of devices or things around us, for example from our homes, businesses, or cities, such as smartphones, personal computers, coffee machines, cars, cameras, etc. These devices include some of the built-in technologies that enable them to have the ability to sense, process and communicate anytime, anywhere and with any device or any one and by using any network with minimal human intervention. These devices collect and share data with each other to accomplish a specific goal in order to

make human life easier [5],[6],[7],[8]. IoT devices generate, share, and receive many different information. This information ranges from individual information such as usernames and phone numbers to information produced by monitoring soil moisture level and temperatures in a field [6]. Figure 1.1 illustrates the concept of the IoT with its capabilites.

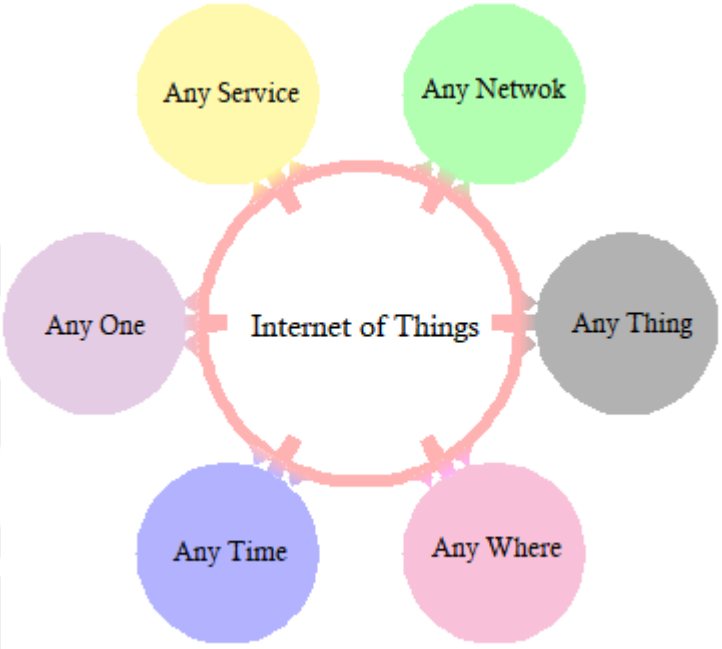


Figure 1.1 IoT Capabilities [5]

There are more and more things connecting to the IoT every day. This is due to IoT's positive influence on the lives of individuals and communities, and the wide variety of applications it offers, such as smart home, smart healthcare, smart cities, and so on. So in the future, the IoT is expected to gradually infiltrate our personal and practical lives and completely change our habits and the way we live [5].

IoT is a new era of technology and plays an important role in the lives of individuals, but unfortunately, the security issue makes it difficult to implement the IoT scenario as it is supposed to be. This is because this issue raises many people's fears, especially as this technology greatly affects their privacy and their secrets. The issue of poor security in the IoT may lead to its slow and reluctant adoption, especially in areas that deal with people's lives and their sensitive information. For the IoT to be widely adopted, these issues and

concerns need to be addressed to provide user confidence in terms of privacy and control of personal information [9]. These security issues could make the IoT, with its devices and information, vulnerable to several security attacks. These attacks may result in leakage, tampering, or destruction of information, and they may also affect the devices themselves, hoping to destroy or use them to launch dangerous attacks. The IoT security problem arises from several factors, including the fact that, to our knowledge, most devices used in the IoT are not designed to counter security and privacy attacks. Also, the use of the Internet as a basic infrastructure for communications made IoT suffer from the weakness of the Internet itself, which exacerbated the issue of security and privacy faced it [6]. These vulnerabilities in IoT security result in several security issues and challenges related to confidentiality, data integrity, authentication and access control [5],[9].

This thesis aims to shed light on the importance of security in the IoT since this issue may be the cause of the success or failure of any technology and its development in IoT domain. Our research also aims to clarify the dire consequences that IoT users may experience due to insecurity, which can lead to loss of life and property. In addition, among the goals of this work is to showcase the challenges that lie ahead for IoT technology that will affect everyone's lives in the future. Motivating and encouraging all IoT stakeholders to have a role in making this important and effective technology for all humanity safer is also among our goals. This is a key topic due to the importance of security on the life of people using IoT; because in the IoT:

- The information circulating between devices may be sensitive, and any tampering or leakage affecting it may result in significant losses of lives and money.
- Protecting the privacy of individuals from infringement is extremely important.
- The development and spread depend to a large extent on addressing security concerns, and as long as these concerns exist, the IoT will not have the full confidence of consumers.

Through our research, we will try to answer the following research questions:

- Why is it so important to secure the IoT?

- Why is it not possible to use known technologies to secure and protect information in order to protect the IoT?
- What are the basic security requirements that must be met in IoT to be a secure technology?
- What are the most common attacks against the IoT and how can they be prevented?
- What is the role of each stakeholder in the smart home application to make it a safer application or place?

Our main contributions in this study are as following:

- Providing basic information related to the most important aspects of the IoT that any researcher in the topic of IoT security needs to be familiar with before starting his research. In addition, this information may be of interest even to any ordinary person interested in the topic of the IoT, as we have provided information about it without going into complicated and technical details.
- Demonstrating the importance of providing security in the IoT by reviewing security attacks that have affected people and companies in real life
- Determining the minimum-security requirements that must be met in the IoT in order to consider it a secure technology, in addition to their definitions and how to implement them in the IoT environment.
- Systematically presenting the most important IoT attacks, using IoT architecture layers as a reference. In this way, we analyze IoT security issues using a bottom-up approach. In this approach, we mentioned security issues starting with the perception layer in the IoT, then moving to the network layer and ending at the application layer. This approach facilitates the presentation of the proposed solutions and helps understanding even for readers who do not have prior knowledge of the topic.
- Providing information about countermeasures against attacks in simple, uncomplicated, and easy-to-understand detail even to the casual readers interested

in this topic. We are gathering the most common attacks and some of the most effective countermeasures against them in one document. At the same time, we provide references that give more detailed information on these topics to help researchers who want to reach them easily.

- Providing a handbook for smart home application stakeholders including an explanation about their respective roles in making smart homes safer. This thesis has collected many important tips and recommendations that have not all been gathered in this way in one document before, to our knowledge.

We accomplished this work through a well-thought-out business plan that is primarily based on an understanding of IoT technology and identifying the importance of security in it. Then, we tried to understand the reasons that have made the IoT a target for cyber attacks and the reasons for its vulnerability in facing these attacks. After that, we looked at how to resist these attacks, and finally we used the smart home as an application of the IoT to clarify the types of attacks that a smart home application may be exposed to and the responsibilities of stakeholders for making it safer. In this range and in more detail:

- First, by reading scientific articles on this topic, we tried to understand what the IoT is. These articles provided us with basic and important information about the IoT such as its definition and objectives, as well as its components, architecture and applications.
- Then, we focused on the security requirements and issues of the IoT by studying a large number of scientific studies published in reliable scientific journals and extracting information related to the subject. This gave us an idea of how important security is in the IoT and what kind of security problems and attacks it might face.
- We analyzed the security attacks and their countermeasures in a systematic way considering the IoT architecture and its layers. In this point, we discussed some potential attacks for each layer and studied some proposed security solutions and measures that can be taken to defend against these attacks.

- In addition, we chose smart home, as an example of IoT applications, to show some of the potential attacks that it might be exposed to. Also, we have prepared a set of recommendations and advice for all smart home stakeholders that can help them to make the smart home safer.

Every day there are new devices connected to the IoT world and every day new IoT applications are developed for consumers. The development of the IoT, its circulation of sensitive and personal information and the growing market demand for it, makes it a target for new and ongoing security attacks and threats. Therefore, research on the protection of IoT is an active area of research and to this day this topic is still being studied and developed daily in order to meet the constant security challenges.

This thesis is organized as follows: Chapter 2 gives some information about IoT as a background while Chapter 3 discusses the differences between IoT security and traditional security followed by security requirements for the IoT technology. In Chapter 4, some of the security attacks that may be exposed to each layer of the IoT architecture are explained separately. Chapter 5 mentions general countermeasures that can be taken to limit attacks against the IoT as an integrated system, in addition to separately presenting some of the defensive means used against the attacks mentioned in Chapter 4. Chapter 6 presents examples of potential attacks against one of the most popular IoT applications, Smart Home, and provides tips and recommendations to overcome and prevent these attacks. Finally, Chapter 7 concludes the study.

CHAPTER 2

IOT BACKGROUND

2.1. Evolution

The origins of the Internet go back to the late 1960s after the first network was formed by connecting two computers together. When the number of connected devices began to increase little by little, the need arose to create a protocol that would regulate the exchange of data between these connected devices. In 1980s, Transmission Control Protocol/Internet Protocol (TCP / IP) was adopted as the primary Internet protocol that is used by the devices to understand each other. Over the past four or five decades, the Internet has grown rapidly and became the most widespread technology in people's lives, especially after the invention of smartphones and their ability to connect to the Internet. In fact, it can be said that the computer today is losing many of its benefits without an Internet connection [10].

According to the authors in [2], about two billion people around the world connect their devices (this number is increasing day by day) to the Internet to browse the web, exchange emails, play games, use social networks and many other tasks [2],[11]. Most of these connected devices contain resources that enable them to operate efficiently, such as sufficient storage space, high capability for data processing, operating systems, and advanced software. Personal computers, printers, smartphones, and tablets are examples of these devices.

With the passage of time and the development of sensor technology and wireless communication technologies, it became possible to connect any daily device in people's lives to the Internet. This was achieved through built-in sensors and wireless technology, for example, in the refrigerator, which makes it able to communicate with its surroundings. Once these things acquired the ability to collect information and communicate, they

became known as smart things. Among the things that could turn into smart things are home appliances, street surveillance cameras, cars, watches, and many more.

All this led to the development of another great new technology that uses the Internet as a global platform to allow smart things to communicate, sense, and coordinate with devices, infrastructures, or other environments to facilitate human life. The concept of this new area was firstly proposed by Kevin Ashton in 1990s [5], and it was called "Internet of Everything", "Internet of Smart Things" or "Smart Systems", or as it is today called "Internet of Things" (IoT) [2],[7],[8]. Ashton used these phrases to describe a system where the Internet connects to the 'real world' via a ubiquitous network of data sensors [10].

The emergence of the IoT and the increase in the possibility of converting things into smart devices, has led to a remarkable increase in the number of devices connected to the Internet [1]. The number of devices connected to the Internet is expected to exceed the world population, which, according to the United Nations, reached 7.7 billion in mid-2019 [12]. Figure 2.1 shows the number of devices connected to the Internet since 2015 and expected in 2025.

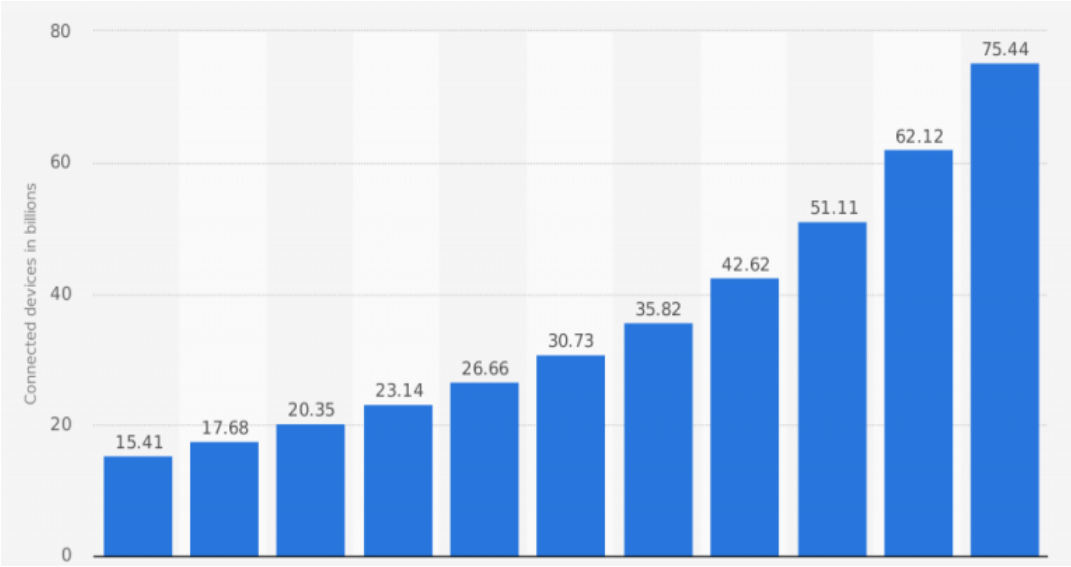


Figure 2.1 Number of the Internet-connected Devices since 2015 and Expected in 2025 [13]

This IoT technology became possible because the devices nature has changed; the world is shifting towards sensors which are based on machine-to-machine technology (M2M). These sensors became smaller and less expensive, which made it possible to include them in everyday things. Thus, these things will have the ability to sense their surroundings, capture data and share it with other devices, simply becoming smart things. Also, the availability and variation of wireless communication means facilitate the spread of this technology and its rapid adoption by consumers.

2.2. Definition of IoT

There are many definitions of the IoT, some are simple and others are more technical, however, they all give the same basic concept. According to Oxford dictionary's definition, the IoT is "The interconnection via the Internet of computing devices embedded in everyday objects, enabling them to send and receive data." [3]. Nevertheless, in simple words, the IoT can be described as an extension and development of the traditional Internet, whereby it not only connects people, but also things and the surrounding environment [14]. The IoT allows these things to see, hear, think and perform functions by having them "talk" together, and share information without much human intervention to make life easier and more efficient [15],[16].

The IoT is a technology that provides services at any time, anywhere and for anyone as it links real life to the virtual world. This technology includes a dynamic network of a large variety of heterogeneous things that will encompass every aspect of a human's life. Smart things in the IoT have a unique identifier (ID), built-in sensors to perceive their surroundings, a means of communication to send and receive data to / from decision-making places and actuators to do what is required. The Internet is used as a backbone to connect these things to each other anytime, anyplace, with anything and anyone using many different communication styles, such as human-to-human, human-to-thing, or thing-to-thing. Things are capable of communicate, collect and process information, share data and resources, making independent decisions with minimum human intervention by providing a range of services and applications [6],[11],[17],[18],[19],[20]. As a result, massive amounts of data are generated, and this data is processed and useful actions are

taken in light of it, enabling "command and control" of things to improve individuals' quality of life [8].

In IoT, the ordinary objects such as cups, tables, lamps, foods and cars are embedded with some technologies which help them to be smart things. These technologies include connectivity, sensing and computing technologies. Smartness enables things to provide services to people and provide for their needs automatically, which gets rid those people from their daily routine.

2.3. The Main Objectives of the IoT

The main purpose of the IoT is to change the way people live today and make it simpler, more relaxed and more effective. It does this by making objects around people like cars, microwave ovens, traffic lights, etc. do everyday tasks instead of people. For example, these things can be configured to run on a specific time basis without people asking them to, and it is also possible for these things to respond to people's voice commands without operating them manually. The IoT is making a better future for humanity. It provides things and devices that know what a person likes, wants, and needs, and behave accordingly without explicit instructions from him [18],[21]. When different things have the ability to understand people's needs and the ability to communicate with each other and with people, IoT applications can be found in almost all areas of life including homes, cities and hospitals. The IoT is also used to monitor and report environmental changes, prevent fires, reduce traffic accidents, monitor soil quality, and many other beneficial functions [6]. These functions optimize the use of resources, increase the quality of services offered to people. The basis for the IoT, which makes it possible to achieve all the above-mentioned goals, is the automatic exchange of information between two systems or two devices without any manual entry [7],[22].

2.4. Making Things Smart

The term Internet of Things contains two main words: The Internet and the things. Nowadays, the Internet is a technology that is well known for everybody. The simplest definition of it is that it is a network of devices that enables people to connect and share data and provide services. On the other hand, all objects of our everyday life such as

people, vehicles, computers, books, TVs, mobile phones, clothes, food, medicine, various home appliances, luggage, etc., can be considered as things.

All these objects are very different in terms of size, capability and functionality. However, the meaning of “things” in the IoT is a large variety of objects, such as the above-mentioned, that independently have the ability to interact with others. In addition, these objects must have the ability to sense the environment or / and to receive orders and carry out an action according to those orders [1],[5].

However, for these things to be part of the IoT and to meet the aforementioned conditions, they need to be smart. So what does it really mean something is smart, and what makes it smart? For example, how would a refrigerator or a toaster oven that has not been considered smart become a smart appliance? To make objects (or things) smart, they must have [2],[8],[16],[19]:

- micro-controller unit (MCU) which include:
  - memory,
  - A means of communication that enables the thing to be linked to a network and makes it capable of receiving and sending information,
  - the necessary programming ability and the necessary "command and control" functions,
  - process unit which is used to process data and make decisions,
- a unique identifier,
- sometimes the ability to sense the environment,
- the ability to be monitored and controlled remotely and
- the ability to respond to scenarios without human intervention.

2.5. IoT Elements

Identifying and understanding the IoT elements helps to gain a better insight into the real meaning and functionality of the IoT. These elements are the foundation upon which the IoT system is based as one integrated, reliable and effective framework that can work and

provide services. These elements are Identification, Sensing, Communication, Processing and Services [4],[14],[19].

2.5.1. Identification

Identification is crucial for the IoT that aims at providing a clear and unambiguous identity for each object within the system. This makes it easier to find and access objects when searching for them to extract information, give an order, or obtain a service, and it also makes it easier for objects to communicate with each other. Many methods are used for identifying the various things and they can be classified as: **Object Identifiers** and **Communication Identifiers.** The object identifiers are used to uniquely identify physical devices such as device's ID and device's serial number. On the other hand, communication identifiers are used to uniquely identify devices wittin a network such as Internet Protocol (IP) address and Bluetooth device address [4],[14]. Due to the interconnected nature of the IoT, one type of identification will not be sufficient for the purpose of obtaining a service. People, applications, or even other objects could be the consumers of the thing. It is therefore, necessary to specifically identify the objects and the users in order to establish the relationship between these users and those objects. For example, if the user wants to access an application, he needs several definitions such as the name of the target application (application ID or URL) and the ID and the IP address of the device or server that host the application that guarantee him access to the desired application. Reference [23] provides more information on the classification of identifiers used in the IoT environment.

2.5.2. Sensing

This component is responsible for collecting different types of data from surrounding areas and then sending this perceptible data to the relevant parties within the IoT environment to understand what is happening and act according it.

Data is acquired through many technologies, i.e. RFID, Wireless Sensor Network (WSN), Global Positioning System (GPS) terminals, cameras, etc. These collected data are analyzed to take specific actions based on required services [4],[3],[14],[24].

2.5.3. Communication

The role of communication technologies is to enable IoT devices to communicate with others. Of course, the more reliable, fast and secure this connection, the better in the IoT environment. This component enables devices to send data to processing system or storage locations, receive orders and interact with users and applications. Most IoT devices use wireless communication technologies to communicate with others, and the most popular wireless technologies are Wi-Fi and Bluetooth. These two technologies differ from each other in terms of speed, distance, security and the number of connected devices [4],[5],[14].

2.5.4. Processing

This important element represents the brain of the IoT, which is concerned with processing the data collected through the sensing element, and this process is performed by the processing units. All information collected by sensors is sent to processing units that make decisions in real time and resend them as commands and actions. The IoT processing unit can exist locally in the devices in the form of microcontrollers and software applications. On the other hand, the collected data can be sent to the cloud platforms. These platforms provide high computational capabilities, that IoT devices with limited resources often do not have, to process big data in real time, then return the result of that processing to IoT devices to take action [4],[14].

2.5.5. Services

The IoT provides a myriad of services to its customers, including but not limited to healthcare services, security services, disaster alert services, energy rationing, and much more. These services are provided within a large number of IoT applications. However, users need an interface to interact with IoT applications, which includes, for example, a mobile application or a web-based application. The interface will help the user to deal with IoT devices, for instance, to set them up, give them instructions or access the data. For example, in home automation, the user interface will help a homeowner to grant access to his home to specific people when he is away from home [4],[14],[25].

2.6. IoT Components

The IoT consists of several components that work seamlessly to enable the IoT system to perform its functions to the fullest. Figure 2.2 shows the components that represent the IoT. The following points explain these components:

- **Sensors:** They are small parts that can be placed in the outdoor environment or indoors, as well as on cars, bicycles and so on. Sensors measure some type of data from the surrounding environment and then send that data to some processors.
- **Local Processing and Local Storage:** In most cases, the sensors send data they collect directly to the cloud for processing, storage and decision-making purposes. However, now there is a trend to support what is known as local processing and storage. IoT should have some devices called IoT gateways that collect data from the sensors (basically computers). These devices have power necessary to process some data, make some decision locally and store some data in case of debugging, save or logs. It is also able to load some of the data to the cloud. Local processing is useful for services and applications that are time sensitive and cannot tolerate any delays. The advantage of this type of data processing is that it is not affected by problems that may be exposed to the Internet, such as the disconnection or congestion.

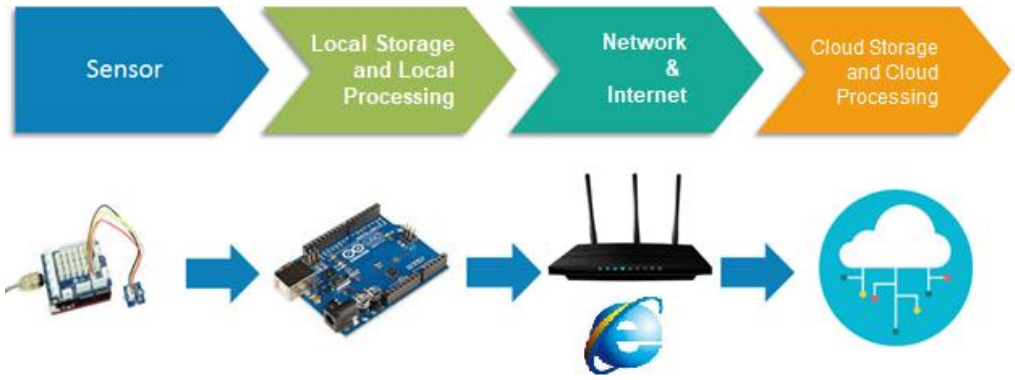


Figure 2.2 IoT Components [26]

- **Network and Internet:** They are used to provide connectivity to the IoT. A network is a method of linking things together while the Internet is used to connect

the IoT gateway to the cloud through an Internet gateway. The IoT gateway sends the data it collects from the sensors to the cloud via the Internet.

- **Cloud Processing and Storage:** Sensors send all the data they collect to the cloud and expect the cloud to process that data and gives them some answers back. Nowadays, this scenario is somewhat different. Now, the IoT gateways collect data from the sensors and then only send the data they have already processed to the cloud. The task of the cloud should be to collect this data, make conclusions, give some results, and store the data for the long term.

2.7. IoT Architecture

The IoT connects a variety of heterogeneous things. Most of these things exchange a huge amount of information over the Internet, which leads to an accelerated increase in network traffic [4],[19],[20]. Hence the need for a single framework that organizes, monitors and controls the flow of information between components of the IoT, this framework is known as IoT architecture. The responsibility of IoT architecture is to orgnaize and ensure consistency of the many technologies and components that enable the IoT, such as sensors, means of communication, user interface, cloud services, and the Internet.

The IoT architecture is developed as a multi-layer architecture. Each layer includes some of technologies to enable that layer to perform its function. There are different opinions about the number of layers in the IoT. This mainly depends on the capabilities of the IoT device, the function it is assigned to implement, the quantity and type of information it deals with, and the means of communication it uses. For example, the device’s function can be simple, such as sensor reading, alarm launching, LED illumination, motor control, etc.

Because IoT technologies cover a wide range of technologies, there is no single IoT architecture considered as a standard reference that can be used in all universally agreed IoT operations [15]. Today, although many projects and research have attempted to design a common IoT architecture, a reference model has not yet been reached [4]. However, according to most of the researcher's opinions on traditional IoT architecture, the IoT basically works on three layers. Nevertheless, this does not deny that there are other

architectures for the IoT that are more complex, some of them consist of four layers and some of them consisting of five layers, but we will depend in our study on the three- layer architecture [18]. The three-layer architecture is the most popular IoT architecture, which is divided into three important layers, namely, Perception, Network and Application [27],[28]. Figure 2.3 shows the basic three-layer architectural framework of IoT with respect to the devices and technologies that encompass each layer [16]. The functionalities and the features of each layer are presented below the figure.

2.7.1. The Perception Layer

The perception layer is the lowest/basic layer of the conventional IoT architecture and it is also called as Recognition layer, Sensor layer, Physical layer and Device layer [3],[22]. Perception layer includes data sensing technologies such as RFID, WSN, camera, GPS, etc. All of these technologies have different capabilities that are used to collect data and are used in different scenarios, according to the surrounding environment, and according to the type of information required to collect.

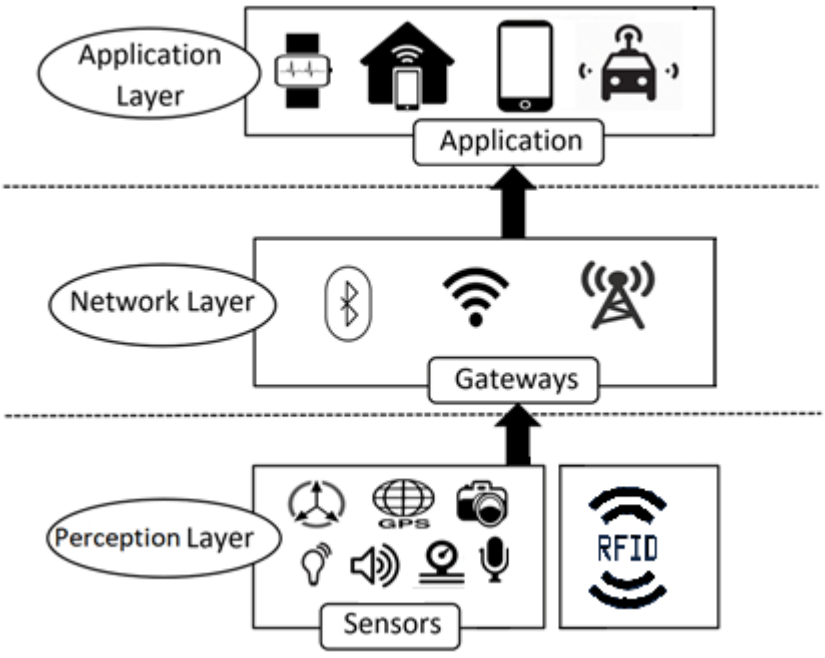


Figure 2.3 Three-layer IoT Architecture [18]

For example, RFID is used to discover and identify the objects to which it is attached. Whereas, WSNs provide readings from the environment in which they are installed. These readings vary according to the type of sensor, some are used to detect movement, others are used to detecting smoke, and there are other types which are used to measure the temperature. The perception layer technologies are small, with limited resources such as processing capability, storage space and power source. These resource-limited technologies are incorporated into the IoT devices that use them to interact with their surroundings through sensing and gathering data [1],[11].

The main tasks of this layer are to collect information from the surrounding environment or to uniquely identify objects by reading data about them and verifying the validity of this data by comparing it to a database [29]. In other words, it enables the IoT devices to sense, capture and collect information from the environment. Depending on the type of sensors, information collected or sensed can be about location, temperature, motion, vibration, accelerations, humidity, chemical changes in the air etc. [19],[30]. The collected information is then passed to Network layer for its transmission to the information processing system [19].

2.7.2. The Network Layer

The network layer is in the middle of the conventional IoT architecture and it is also called as Wireless Sensor, Middleware layer or Transmission layer [1],[19],[27]. This layer is simply a transmission layer that transfers the information collected through the perception layer to the processing system, by using communication technologies. This layer uses different communication technologies that may be wired or wireless such as Wi-Fi, Bluetooth and Ethernet. The primary objective of this layer is to connects all IoT components together as well as it works as a bridge between perception layer and application layer. However, the functions of this layer can be summarized in the following points [9],[31],[32]:

- Receive data from the perception layer, collect it and transfer it wirelessly to storage and decision-making centers often located in the cloud
- Return the result to IoT devices to act according to the decision made

- Deliver data to the end user (for example, a human or a device) through interfaces and across applications
- Exchange data among different IoT devices

Simply, the network layer connects IoT sensor nodes to the gateways, in addition to connecting the gateways to the Internet. Moreover, it connects IoT devices located in the same network with each other.

The network layer collects and transfers data from various IoT nodes to, for example, decision making centers, switches, routers, gateways and vice versa. It does that by using various types of transmission technologies such as Wi-Fi, infrared, Bluetooth, 3G, Zigbee which are chosen to be used depending on the techniques adopted by the perception layer [3],[18],[19].

2.7.3. The Application Layer

Finally, the topmost or upper layer of conventional IoT architecture is known as the Application layer and it is the interface between the IoT applications and the end users. This layer uses the given data in order to provide, present and export all the system's functionalities and services to the final user according to his requirements [1],[9],[33],[34]. Moreover, in this layer, the system offers different interfaces to human users allowing them to manipulate things in the physical domain [35]. In addition, achieving a smart environment and providing global management of IoT application can be considered among the objectives of this layer. The application layer defines various high-level intelligent applications in which the IoT can be deployed, for example, disaster monitoring, health monitoring, smart grid, smart farming, smart home, smart city, intelligent transportation, etc. [17],[19],[28].

2.8. Some of the Technologies Used to Collect Data in the IoT

The main goal of the IoT is to provide services that aim to satisfy consumers' desires at anytime and anywhere. This can be achieved with the help of technologies built into IoT devices such as RFID and sensors. The function of these embedded technologies is to sense and read information from the surrounding environment such as temperature,

movement, and light intensity as well as identify and track objects [3],[33],[36]. Using this information and with the help of other IoT components, actions can be taken and services can be provided to the consumers that meet their requirements such as operating the heating, lock or unlock doors, and controlling the lighting level [15],[16],[36]. More information about the previous technologies are presented below.

2.8.1. RFID

The main technology used in the IoT is RFID and it is what made the IoT a reality. RFID system uses radio frequency signals to detect and identify uniquely an animal, person or object which they are attached with [37]. This technology is characterized by fast scanning, small size, reusability and low cost, etc. These features make the IoT perception layer take advantage of this technology to locate, monitor and track objects in real-time and exchange information over radio signals over a short distance [1],[32],[38]. In addition, the RFID system allows every object in the IoT to be distinguished from others using the identification mechanism [18]. RFID systems can be used in many applications such as personnel tracking, access control, books tracking in libraries, toll gate system,remote keyless unlocking, animal tracking and payment systems. The RFID system can be divided into three main components: back-end server, RFID reader and RFID tag.

- **Back-end Server**

The back-end server contains the database that contains all the identifying information for the tags and objects that are attached to it.

- **RFID Readers**

The RFID reader acts as the identity detector for each tag and obtains relevant information. It sends radio waves continuously, thus, when the RFID tag is within the reader range, it reacts to the reader by sending a feedback signal to the reader. Then these reflected signals in turn are passed to the backend server to identify and verify objects based on those reflected signals [14]. In other words, the reader plays the mediating role between the tags and the server. It reads the tag information and passes it to the server for comparison with what is kept in its database in order to confirm the identity of the object. In most cases,

the reader and the server communicate with each other using a wired connection which is considered secure.

- **RFID Tag**

An RFID tag is a simple chip or sticker which is located on the object (even persons or animals) we want to identify. It consists of two components: a chip to store the unique identity of the object and an antenna to allow the chip to communicate with RFID reader using radio waves [14]. This antenna is used for both receiving the reader signal and transmitting the tag ID [33].

RFID tags use radio frequency waves to communicate and exchange information with the reader without having to be contiguous, at one level of visibility, or even physically connected [38]. Tags can either be passive or active. Passive tags do not have an internal power source as they draw power to transmit data from the query signal sent by the RFID reader located near them. On the other hand, active tags house a battery internally [33],[38].

A tag can be attached to a product early in manufacture, allowing the product to be monitored during shipment, in store and finally after a consumer has purchased it.

2.8.2. WSN

WSN can play an important role in the IoT, especially when there is a need to implement remote sensing and information gathering as it occurs in a variety of applications, such as intrusion detection system, fire detection system and environmental monitoring systems [15].

WSN consists of a large number of geographically distributed sensor nodes with limited memory, limited processing power, and energy constrained. These nodes are collaborating and communicating wirelessly to execute a specific task [18],[33],[39]. This cooperation between sensor nodes is important, because many times, data from a single sensor is not useful in monitoring large areas and complex activities. The different sensor nodes need to collaborate with each other to provide enough information to rely on for correct decisions [28]. These wireless sensors nodes monitor, read and collect information about

physical environmental parameters such as temperature, pressure, sounds, chemical compositions, etc. [31],[39]. Nodes report the results of their sensing to special nodes called sinks. The sink receives the information gathered by the sensors network and delivers it to the end-user or to the decision-making center such as the cloud [38].

The sensor nodes of a typical WSN have several parts and these parts are a sensor (collecting data from the environment), microcontroller (processing the data), memory (used for programming the device and storing data), radio transceiver (communicating with other nodes by transmits and receives radio frequencies) and a battery (supporting the power) [9],[39].

2.9. IoT Applications

The main goal of the IoT is to create a smart environment and self-aware, autonomous devices. This smart environment makes humans life easier and improves its quality at home, while travelling, when sick, at work, when jogging and at the gym by implementing their desires without the need for explicit orders from them [33]. The potential applications of the IoT are many and varied, some of which are showed in figure 2.4, and are found in practically all areas of the daily life of individuals, organizations and society at large. For example, in the future, the IoT is expected to greatly improve the level of healthcare, especially for the elderly, and it can also be considered as one of the solutions to control traffic congestion [40],[41].

The use of the IoT for the Internet and the availability of a wide range of sensors and devices of different sizes and low costs helped the diversity of IoT applications and their presence in every aspect of our daily life [4]. The applications that can be provided by the IoT technology include but are not limited to:

- **Smart Homes**

The smart homes are becoming more popular today and their services are increasing day by day. They help in completing the daily tasks of residents automatically and without any participation from them, which saves their time and effort and makes them enjoy free time they spend, for example, for relax, study, or spend more time with family [5],[28]. In

this IoT application, home appliances meet their owners' wishes and offer services to them before they even ask for them. Connecting these devices to the home network allows them the ability to communicate with each other in order to provide these services.

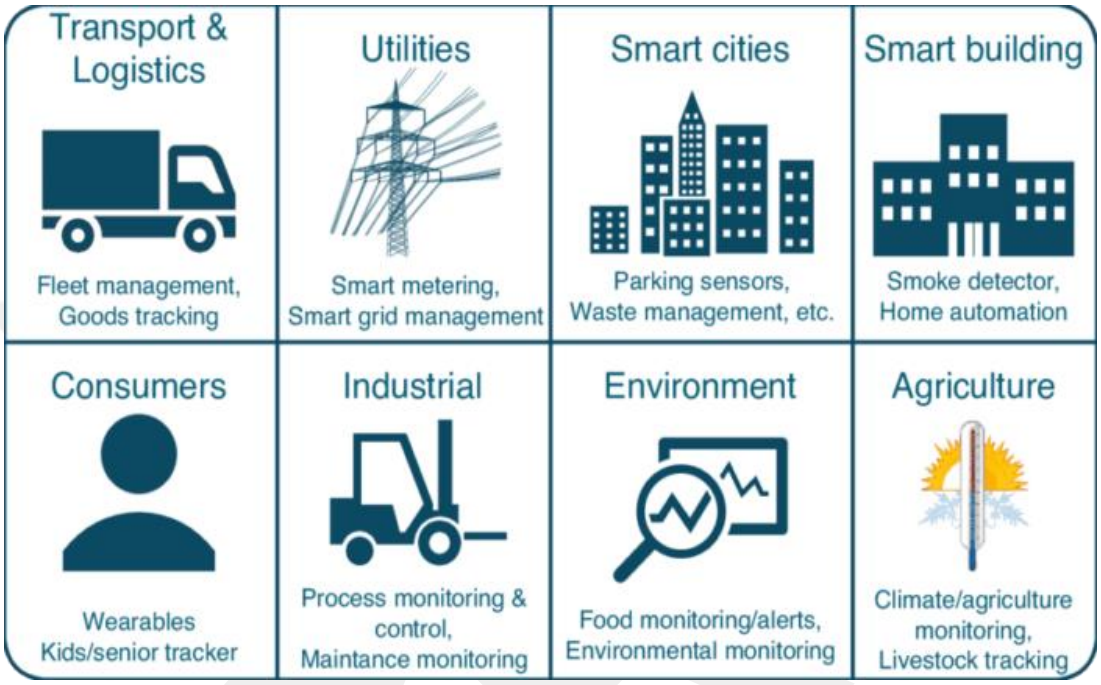


Figure 2.4 Some IoT Applications [42]

In addition, the owner of a smart home can remotely monitor and control his home and its contents through specific applications and after connecting them to the home's network or to the Internet [5],[27]. Some of the services that the smart home provides to its residents are:

- Sending the readings related with home electricity, telecommunications, gas and water automatically to their corresponding utility companies to enhance the efficiency of the work.
- Controlling windows, home ventilation, doors, lighting, air conditioning etc. remotely to avoid accidents and save energy and enhance security.
- Controlling electronic devices remotely and harness them to serve home residents, such as refrigerators, washing machines, oven, and others, through an application [27]

- Watering home garden when needed and according to the weather
- Giving the ability to remotely control who can enter the house by setting the time and date for visitors

- **Smart City**

In smart cities, sensors are deployed throughout roads, buildings, smart cars, etc. to allow city officials to interact directly with the city's infrastructure and monitor what is happening in the city as well as provide several services to citizens. A smart city uses information and communication technologies to [19],[43]:

- Provide real-time information about public transportations
- Provide real-time information about the available parking space
- Monitor and manage traffic and transport systems
- Monitor air quality, schools, libraries, hospitals
- Efficient light up of the city
- Water the gardens
- Manage the waste and many other services to the society

- **Smart Health Care**

The increasing financial cost of healthcare around the world requires a serious review of the traditional healthcare system, hence the value of IoT's smart healthcare application as a way of alleviating this issue [9]. Currently, healthcare-based IoT applications represent one of the promising technologies that greatly affect society, especially the elderly [43]. Smart healthcare offers a mechanism to improve the health care services by embedding sensors and actuators inside or outside the patient’s body for monitoring health parameters, activities, medicines intake, etc. [9],[19]. The built-in sensors have the ability to collect information directly from the patient's body area. This information is used to warn the patient of a nearby medical problem or it is sent to the nearest health center or doctor for help. For example, the ADAMM Smart Asthma Monitor is a wearable technology from Health Care Originals that can identify an upcoming asthma attack before a wearer notices symptoms. This technology monitors symptoms such as coughing, wheezing or shortness of breath, and warns the patient that he may have a seizure soon,

so he stops what he is doing or takes his medicine. This helped to obtain medical consultations without the frequent need to visit hospitals and medical clinics. When monitoring a patient's health parameters, doctors can get real-time information about patients, and they can take immediate action if patients are in a serious condition, especially if they live alone [43]. On the other hand, smart healthcare application can track the patients at the entrance of the hospital, and the hospital can use these data to control the number of people into the hospital.

These technologies can be also used to tracking of patients who stay in the hospital. Smart healthcare helps doctors obtain real-time information about patients, enabling them to take immediate action in the event that patients are exposed to danger due to, for example, a wrong drug dose or a harmful procedure [39].

In conclusion, it can be said that the IoT makes healthcare more efficient and effective by enhancing interaction between all healthcare parties. It also makes sure that patients get the services they need, and helps medical staff make correct medical decisions [31].

- **Smart Agriculture**

Smart agriculture includes a network of different sensors that are able to sense data from the environment such as air and soil and inform farmers, for example, through an application or text messages about a part of the land that needs special attention. For instance, intelligent farming system can measure the amount of moisture in the soil and, in light of the result, tell the farmer if this part of the land needs irrigation. In addition, smart agriculture system can also reduce resource consumption by extrapolating weather information and knowing the probability of precipitation, the system therefore decides not to irrigate the land because it will be irrigated anyway with rain.

Another important benefit of this application is its ability to help agricultural scientists better understand plant growth models by knowing ground conditions and climate variability. Moreover, livestock keepers can use this application to study air and food quality on farms, open pastures and in places where animals live to see how this affects the health of the animals and the quality of their products [19],[41].

- **Smart Transportation**

The smart transportation system will provide efficient transportation control and management that aims to link people, roads and smart vehicles as well as make the transportation safer, greener and more convenient. By connecting and distributing intelligent processors and sensors inside vehicles and also through transportation infrastructure, the smart transportation can provide many interesting services such as [19],[39],[43]:

  - Monitoring traffic rules violations
  - Avoiding traffic jams to minimize arrival delays
  - Controlling the length of traffic lights at intersections where traffic congestion occurs
  - Recording where and when the number of vehicles arrive at the peak
  - Tracking the vehicle in case it has been stolen, and it can help police find it quickly
  - Reporting traffic incidents
  - Providing smart parking
  - Monitoring public transportation

- **Smart Watches**

Smart watchs provide many services to its owner to make life easier and more convenient. Track the fitness activity, provide information about the weather, notes book, timer and display a detailed map of directions are some services offered by this IoT application.

Users can take advantage of this application while exercising, for example, to measure the number of calories burned, the level of heart rate, and the state of breathing. They are also used for public safety — for example, enhancing response times for first responders during emergencies by providing optimized routes to a location, or monitoring vital signs of construction workers or firefighters at life-threatening sites. Examples of this IoT app are the Apple smart watch, fitness band, and many more.

After presenting information about the IoT and understanding its components, about how it works, and its importance to humanity, it became necessary to know the factors that may stand in the way of its spread. Among these factors, the most important one is the security factor. In the next chapter, the security issue in IoT technology and its impact on the lives of IoT users will be presented. In addition, the security requirements that the IoT technology must meet in order to be considered a safe technology for its users will be discussed.

CHAPTER 3

SECURITY REQUIREMENTS FOR IOT ENVIRONMENT

IoT security can be defined as all the strategies and technologies that aim to protect any information collected, exchanged or stored in any IoT system from threats and malicious attacks [43]. This information may face many risks and threats such as theft, tampering and destruction. Also, the security of IoT components such as sensors, devices, applications and network falls under the heading of IoT security.

Security considerations are not new in the information technology context. Rather, they are a critical component of any technology's success, development, and adoptionSecurity has always been an issue since computers started communicating with each other, however, the effect has been limited, for example targeting money and intellectual property theft [34],[41]. The advent of the IoT with its complex environment added a whole new dimension to this problem and faced new and unique security challenges. This complexity is due to the large number of heterogeneous devices connected to the IoT, combined with the huge data generated and exchanged by these devices and the difference in the communication infrastructure used. As well as they are produced by different manufacturers, use different security policies, different communication stacks and various standards [5]. This has led to the failure to implement a robust security system for devices, especially since most of these devices are not equipped with an effective security mechanism and are not primarily designed to deal with security problems or even to connect to the Internet [17].

Because, the devices of IoT might not only handle and collect critical personal information such as users' names and telephone numbers, medical records and prescriptions, but can also monitor user activities (e.g., when users are in their houses) [6],[44]. Therefore, users must ensure that IoT devices and the services they provide are free from vulnerabilities and defects threaten user's security, especially as this technology is becoming more and

more common in daily life [36]. For this reason, ensuring security in IoT products should be a major stakeholder priority and goal to be achieved. Otherwise without IoT security and privacy guarantees, IoT solutions are unlikely to be widely adopted by stakeholders despite their benefits [2].

Attacks on IoT devices can sometimes be easy to implement, especially when they target devices with limited resources that represent the majority such as smart TVs and baby monitors. These resource limitations represent weaknesses and flaws that hackers can use to attack the IoT system as a whole, affect its overall safety, productivity, and more [16],[17],[45]. In addition, IoT devices may operate in harsh, irregular and even frightening environments without supervision, and thus are more vulnerable to various security breaches [21]. The common attack strategy on IoT devices is to hack one device that has vulnerabilities and take fraudulent actions against other connected devices, by impersonating the true identity of the hacked device [17]. As a result, it can be said that the interconnected nature of the IoT means that every insecure device connected to it has the potential to affect the security of the IoT system as a whole [36]. For example, attackers could compromise a home alarm system by intercepting the radio frequency signal used to lock and unlock home windows.

The IoT is the integration and collaboration of several technologies such as WSN, RFID, cloud computing, Internet, etc. Therefore, the IoT will suffer from all the vulnerabilities of these technologies, and it will be vulnerable to all the security threats that these technologies face [31].

3.1. The Importance of IoT Security

In the near future, the IoT is expected to enter various areas of our daily life such as our cities, homes, hospitals and schools. However, this prevalence depends on a very important factor, which is the degree of security that the IoT provides to consumers [46]. To find out the required level of security, confidence and privacy that must be available to consumers, IoT service providers must answer the following questions [4]:

- **Does the data need to be private?**

  The IoT largely deals with sensitive and private information whose leakage or disclosure can affect a person's life and money. Therefore, it is imperative that protecting this data appropriately at all times becomes a priority.

- **Does the data need to be trusted?**

  It must be verified that the source of the information is a reliable source. Also, it must be ensured that it is impossible to tamper with or alter this information by intruders during its circulation on the IoT.

- **Is the timely arrival of data important?**

  Data delays may have a serious impact on the service provided, especially in e-health applications.

- **Is it necessary to restrict access to or control the device only to the authorized user?**

  Preventing unauthorized access or controlling devices is essential if security is taken into account. If an intruder takes control of a device, he may be able to access sensitive data stored in it and can also access other devices in the IoT.

If IoT service providers want this technology to spread widely, they need to know that the typical answer to the previous questions is "yes". So they must take these questions into account when manufacturing or deploying IoT technology. This indicates that every potential IoT user wants to ensure that his private information is essentially protected from any kind of abuse before he thinks about using the IoT despite its multiple benefits. Also, the services and applications provided by the IoT must be available whenever the user needs them. In short, it can be said that the importance of security lies in the fact that it provides confidentiality, privacy, trust, reliability and availability.

3.2. Real-life IoT Security Incidents

Every day, IoT devices are targeted by attackers. It is worth noting that F-Secure published a report titled "Attack Landscape H1 2019: IoT, SMB Traffic", recording a 300% increase in the number of cyber-attacks on IoT devices in 2019. The attacks usually target IoT

devices that are found in homes and workplaces such as medical devices, smart TVs, and smart printers, which are considered weak and completely unsafe against these attacks. The scariest part is that attackers are using these easy to hack devices as access points to more critical and sensitive networks and systems. The importance of security in the IoT becomes more clear and important when dealing with some incidents that occurred to real people and through real events. This point clarifies the extent of the impact of this problem on consumers' lives, whether this effect is large or small. Here are few examples of real attacks that have led users of IoT applications to have some uncomfortable experiences [5],[47],[48]:

- **BMW's Connected Drive Vulnerable**

In January 2015, a security flaw appeared in BMW Connected Driving, a system that allows drivers whose cars have been accidentally locked to request a remote unlock of their vehicle from the BMW helpline. This flaw allowed the attacker to impersonate BMW's servers and send instructions to unlock locked vehicles remotely over the public cellular network even without any request from the owners. This attack allows anyone to enter the vehicle without any effort or draw attention to him and tamper with or steal its contents, whatever it is.

- **Hacking Web Sites**

On October 21, 2016, several websites including Twitter, Netflix, Spotify, Airbnb and The New York Times were reported to be inaccessible due to a Distributed Denial of Service (DDoS) attack. To launch this attack, the attacker hacked several IoT devices with limited resources and used them to send many useless requests to these sites. Huge requests made these sites unable to deal with their customers' requests, and thus these sites were considered out of service or unavailable. Therefore, this attack deprives consumers of the services provided by the IoT by consuming or completely disabling IoT resources.

- **Denial of Basic Services**

According to Simo Ronella, CEO of Valtia, the company responsible for managing the overall operations and maintenance of the damaged property, in 2016, two buildings in southeast Finland were attacked. This attack deprived residents of heating, which is an

essential service in a cold country like Finland. As it temporarily disrupted computer systems that were controlling central heating and hot water distribution to both buildings using a denial of service (DoS) attack. Local reports said they believed this cyber-attack lasted about a week, starting in late October and ending on November 3th.

- **Parents Nightmare: Hacked Baby Monitor**

According to NBC News, in 2018, a Texas couple experienced a cyber-attack targeting the cameras they used to monitor their four-month-old baby. They heard voices and insults coming from the child's room. Then they heard the voice of a man coming from the camera in their room telling them that their child had been kidnapped. However, when they got to their child's room, he was alone and was asleep as they left him.

- **Hackers can "Exploit" Connected Fax Machines**

In 2018, Yaniv Palmas and Eyal Atkin, two security researchers from Check Point, discovered that popular HP Officejet Pro All-in-One fax printers had security flaws. These flaws could allow hackers to steal data across the company's network using a phone line and fax number. They said that attackers could fax files loaded with malware that were specifically created to target networks. Fax vulnerabilities enable this malware to decrypt files and upload them to its memory, which could compromise sensitive information or cause disruption across connected networks.

- **Hacking Smart Bulbs**

The security experts from the University of Texas stated that the hackers can make use of Internet-connected light bulbs as a covert channel to exploit the user's private data. The researchers have taken the LIFX and Phillips Hue smart light systems for the study. The researchers stated that the hackers can launch an attack by manipulating the infrared light by creating a communication channel between the smart lights and a device that senses infrared light. And by installing a malicious agent on the phone the attackers can encode the private data and transfer them through the infrared covert channel.

These were simple examples of what attacks targeting the IoT can do. Of course, the attacks may be more dangerous than previously mentioned, especially if they target

applications that directly affect human life, such as e-health applications or smart transportation applications, which may cause accidents that threaten people's lives [3].

3.3. Factors that Restrict the Use of Traditional Security Methods to Protect IoT

It is well known that protecting the information stored and exchanged between devices and within the network is not a new problem. Since the Internet began, there have been concerns of cyber attacks targeting information. Through our study of this topic, we are absolutely certain that security will never be an old and stable issue with ready-made solutions. The IoT security requires the development and creation of new solutions designed to suit the nature of this technology or, at best, solutions modified from old solutions. This is because the regular Internet-connected devices differ from IoT devices in terms of functionality and device resources such as memory, power source, and data processing capability. For example, a laptop differs from a baby monitor and a smartphone differs from a smart door lock .

This difference makes it difficult to use traditional security that was originally designed to protect these systems, to protect the IoT. IoT security has to be stronger than traditional security because IoT devices are connected to the physical world and at the same time not designed to withstand the threats that this world faces. Here are some of the important features that distinguish the IoT from well-known information systems. It should be noted that these features were factors that contributed to making the use of known security technologies to secure the IoT difficult [17],[18],[20],[36],[49]:

3.3.1. Mobility

Most of the IoT devices are portable devices and they often connect to the Internet via a wide range of service providers. These devices are constantly moving, causing them to disconnect from a specific network, release its IP address, connect to another network, and get a new IP address, depending on their movement. Therefore, a stable network connection cannot be expected in such an environment.

This factor makes verifying the identity of everyone trying to connect to the network difficult and complicated. In addition to the difficulty of monitoring and tracking of the

device location that the user is trying to connect from, what resources he can access, and what risks this device may bring to the network.

3.3.2. Heterogeneity

The IoT is a heterogeneous and complex system that combines many products or things from different manufacturers based on different technologies. These products differ from each other in terms of resources (software and hardware), security policies, and functionality. Therefore, the interaction of these things together and their communication with each other is difficult due to the lack of a common language between them. Hence the problem of creating a common standard IoT infrastructure that builds on a single standard technology for all vendors and manufacturers. Creating this architecture would enhance the interoperability of the security functions of all components of the IoT system. The success of this will depend on collaboration between companies to create a global standard that greatly facilitates IoT network security [50].

3.3.3. Scalability

Scalability is related to the ability of the system, with all the software and hardware it contains, to meet the large increase in the number of devices and the vast amount of information circulating in addition to the increasing demand for services.

Things connected to the IoT are increasing daily, as their number is expected to reach about 28.5 billion devices by 2022. This significant increase in the number of devices is matched by an increase in the number of users and an increase in the services they demand. Also, the amount of information that these users share will increase by a huge amount. This increase in both information and devices will lead to other problems, including providing unique addresses for devices, where the information is stored, and how to control and monitor it. On the other hand, a lot of these devices will be deployed in areas where it may be impossible or impractical to provide physical security, which makes it easier for intruders to physically compromise devices on the network. So, the scalability feature makes it difficult to monitor, identify, and protect IoT devices.

3.3.4. Limited Resources

The implementation of a robust security mechanism in the IoT system depends on the availability of strong security in the IoT devices, separately. It is well known that the availability of robust security methods in any device depends to a large extent on having sufficient resources to support it, such as having an adequate power supply, sufficient memory space and high processing capability [50].

Most IoT devices are simple, limited resources things that often perform one function, such as turning the lights on / off or measuring the oxygen level in the blood. The lack of resources of these devices does not help them implement complex security solutions. Since traditional security solutions are designed to run on computers, smartphones, and other devices with sufficient resources, they will not be suitable for IoT devices with limited resources. Devices in the IoT have many limitations and restrictions that control the level of security they can provide. This is due to the manufacturers' desire to produce inexpensive and lightweight smart devices, which necessitated not providing them with sufficient resources to address security issues. The limitations on IoT devices include:

3.3.4.1. Limitations based on Hardware

The IoT devices are not being built with security in mind. They were also not designed be a smart and to exchange information with other devices. For example, the methods used to secure computers cannot be used to secure many IoT devices such as coffee machines, refrigerators, door locks, etc. This is due to the fact that these devices contain a limited amount of resources, unlike computers. These resources are as mentioned below:

- **Limited Computing Power**

IoT devices have limited or no computing power, so security methods that rely heavily on complex encryption techniques are not suitable for them.

- **Limited Energy Supply**

Power capacity is the amount of energy sufficient to operate a device over a specified period of time. In most cases, IoT devices are powered by batteries which are a limited source of power and must be replaced after a certain period of time. Conventional security technologies, which use algorithms to encrypt and authenticate data, are known to

consume a great deal of energy. This means the constant change of batteries, which is a problem in the IoT system due to the large number of devices, most of which are located in remote or difficult to reach places.

- **Memory Constraint**

Conventional security systems are highly efficient memory systems because they are designed for devices with high storage space such as PC, laptop, etc. However, for IoT devices, they have limited Random Access Memory (RAM) and flash memory compared to traditional digital devices, which makes it difficult to implement the same level of security. Therefore, designing complex and comprehensive security measures within a memory space ranging from 64 KB to 640 KB is a huge challenge for IoT device manufacturers and software developers. This memory space is small compared to the memory space in computers, for example, which might go up to 4GB or 8GB.

- **Low Processing Power**

A wide range of IoT devices, such as smart locks and light bulbs, contain processing and storage units that are very small. This makes them unable to install and run applications such as anti-malware or to use security protocols that require adequate resources.

- **The Possibility of being Tampered**

Current security solutions focus primarily on protection from remote attackers and are based on the fact that attackers cannot physically access the devices. This is mostly true for desktop computers and servers that are usually kept in closed buildings, or mobile devices that rarely leave their owners' pockets. However, this is not the case for IoT devices that may be located in many remote areas left unattended. In most cases, attackers or hackers can easily gain access to a device by capturing it and then they can extract secrets, modify programs, and add malicious data.

3.3.4.2. Limitations based on Software

- **Embedded Software Constraint**

IoT devices contain simple operating systems which are usually firmware whose mission is only to enable the device to perform its function such as capture, process and send

information, or respond to a command. These operating systems often lack the ability to provide adequate security technologies or support robust security protocols.

- **Dynamic Security Patch and Software Updates**

A patch is defined as a change or update that is applied to a software to correct a bug or remove a security vulnerability. This corrective action will prevent the attacker from exploiting any vulnerabilities in the system. However, applying updates, including patches, to the firmware or software running on IoT devices presents a number of challenges. For example, the constant search for available updates and apply them across distributed environments using heterogeneous devices that communicate over a range of different network protocols is one of the biggest challenges. On the other hand, updates may not be available for all devices, especially old devices or those devices that are no longer supported by their manufacturer but are still in use. Also, there are devices that do not support remote updating so physical access to the device is necessary in this case and this may require a temporary exit from work to apply the update. If there is an update available every week, for example, and given the number of devices that need to be updated, then applying the patches in this case is a huge challenge in the IoT.

3.3.4.3. Limitations based on Network

- **Scalability**

Monitoring and managing desktop and mobile computers within a network is not a difficult issue. The addition of a new tablet or laptop computer to the network does not affect this management or monitoring. However, when a smart home, for example, is filled with dozens of Internet-connected devices, and many of them operate without human intervention, management becomes a problem, especially since many devices are not monitored and therefore preferred targets for hackers.

- **The Diversity of Devices**

The IoT consists of many devices that use different communication methods, different protocols, and different security standards. Some of these devices can encrypt information before sending it over the network, and some cannot. This makes it difficult to find and

use one well-defined standard or rule for securing data as it is transmitted over the network.

- **Multiplicity of Communication Medium**

IoT devices connect to the local and public network via a wide range of links. For example, the home key connects to the smart lock via Bluetooth and at the same time it connects to the home owner's mobile via Wi-Fi. Additionally, many IoT devices, which do not support Wi-Fi, use, for example, Zigbee as the protocol to communicate with the gateway. This protocol does not consume much power, but at the same time it does not cover much distance and is slow compared to Wi-Fi. Therefore, it is difficult to find a comprehensive security protocol that takes into account the characteristics of all wired and wireless connectivity.

- **Multi-Protocol Networking**

IoT devices may use a non-IP network protocol to communicate in nearby networks. On the other hand, other device may connect to the IoT service provider via the IP network. The multi-protocol communication characteristics make traditional security systems unsuitable for IoT devices.

3.4. Security Requirements for the IoT

IoT is a multi-domain environment, with a large number of interconnected devices, whose goal is to provide its clients with diversified services. These IoT devices enter almost every aspect of a person's life and handle his personal and confidential information. To gain consumer confidence, breaches of privacy, threats, and information leakage, which affect them psychologically and safely, must be prevented. In addition, the presence of security problems makes companies fear that their reputation will be damaged when their data falls into the wrong hands, and governments are afraid of leakage of some of their sensitive information, which leads to many security risks [51].

Security is a major challenge standing in the way of the spread and adoption of the IoT technology. Therefore, it is necessary to win this challenge by enhancing the security capabilities of the devices [1],[52]. It is noted that some of the most prominent security problems in the IoT system arise from the security problems that exist in the technologies

that make the IoT achievable. These technologies include technologies for gathering information, technologies for transmitting information, and techniques for providing services, among others. This is in addition to the security problems present in the devices themselves due to the limited resources, and even their heterogeneous nature [18].

In order to ensure security in the IoT and to create readily available IoT devices and services, a set of security requirements must be taken into consideration. In order to create a reliable system that can be considered to be safe, an IoT system must fulfill these requirements. Failure to meet these requirements could mean failure to provide security, privacy and reliability, resulting in serious problems and dire consequences [16],[53].

There are several security requirements by which it is determined whether or not a system is safe. However, the minimum main security requirements to be met in any system are divided into three groups: Network Security, Privacy and Trust. The three main IoT security requirements along with their subcomponents are shown in figure 3.1 [49],[52].

3.4.1. Network Security Requirements

Since the IoT depends in its operation on a network of devices connected, the existence of specialized security requirements that ensure the security of information while it is moving in this network is essential. These network security requirements are confidentiality, integrity, and availability [4]. In order to meet these requirements, certain types of technologies must be used, such as encryption techniques and data integrity assurance techniques. However, before defining these technologies, one must take into account the heterogeneous nature of the IoT and the limited resources of most of its devices. Most of the techniques used before to provide confidentiality in the network are considered heavy on the IoT system and therefore cannot be implemented in this case. For example, some asymmetric encryption methods, which encode data through a complex calculation that require an adequate power source and high computational power, will not be suitable for use in IoT devices with limited resources. Next, each of these requirements will be explained [36].

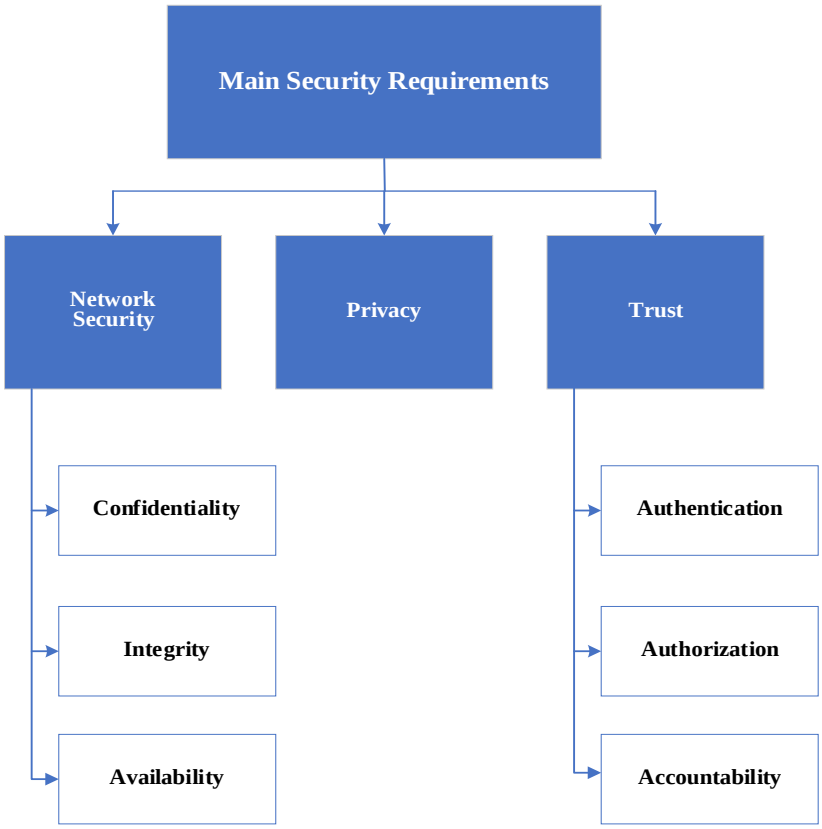


Figure 3.1 Main IoT Security Requirements and their Subcomponents [52],[53]

3.4.1.1. Confidentiality

IoT devices may deal with sensitive information important to individuals, institutions and governments, including medical records, banking transactions and military secrets. Therefore, the protection of this information is important and is closely related to the user's degree of confidence in the IoT technology and his willingness to use it and benefit from its services. For example, eavesdropping or tampering with information exchanged by health devices may lead to the disclosure of personal health information or even lead to life-threatening situations. As another example, the data related to the composition of any product that guarantees its quality and distinguishes it from other products should be

confidential because its spread can harm the company's reputation and competitive advantage [4],[45].

Confidentiality refers to granting only authorized users the right to access certain information in order to see and understand it, to ensure the security of that information and protect it from disclosure. Even if this information is stolen, the presence of this security requirement prevents the thieves from understanding the stolen data, which in turn prevents them from exploiting it for sinister purposes.

To achieve confidentiality, protect information and gain user confidence, specific technologies must be developed and used for this purpose. These technologies include, for example, encrypting data before it is transmitted and creating mechanisms for securely distributing cryptographic keys [22],[32],[49]. One of the well-known encryption methods is the symmetric key encryption method. In this method, the sender and receiver use the same secret key to encrypt and decrypt the data [54].

3.4.1.2. Integrity

This requirement is necessary to give users confidence in the reliability and integrity of the information provided by the IoT. The IoT is often based on the exchange of private, sensitive and valuable information between many different devices that greatly affect consumers. For this reason, it is important to ensure that accurate, original, legal, unaltered, timely and complete information reaches the consumer [18]. The incorrect information happens as a result of changing or tampering with the original information, and this change may be intentionally or unintentionally. In an intentional alteration, a malicious attacker picks up the information before it reaches its target, changes it, and then sends it back to its destination. Thus, the recipient receives information other than what was sent to him from the authorized sender. As a result, the attacker can modify, alter, or completely destroy the data, endangering the integrity of the IoT system, which entails great risks. As for the unintended change, it will sometimes result from a transmission error or unintended noise or as a result of weather factors, but in any case, it will also affect the reliability of the data [17],[55].

This security requirement is important to the IoT, and if not available, there may be serious consequences. For example, tampering with medical information and readings produced by medical devices, such as an insulin pump or pacemaker, may lead to life-threatening outcomes [44]. On the other hand, if the data is not reliable, then it cannot be used for the purposes for which it was designed, and therefore any service that relies on this data will be in doubt. However, the more dangerous thing is using this data without knowing that it has been tampered with, sometimes resulting in the patient being given the wrong drug or the wrong bank transfer. Hence the need to find and use technologies whose mission is to verify the integrity of the data provided by the IoT. One of the simplest techniques to verify data integrity is the Cyclic Redundancy Check (CRC). This technique is a way to ensure data integrity by adding a fixed-length value to detect network errors in the IoT. A request to resend the correct data is sent to the sender if this technology observes the arrival of incorrect data [21],[32],[37],[49].

3.4.1.3. Availability

The requirement of IoT availability is necessary to provide a fully functional Internet-connected environment. This ensures that services are available to consumers whenever they need them and without interruption [44]. In other words, availability ensures that authorized users can access all related devices, services and data provided by the IoT whenever they need it and without any delay. This availability must be achieved even in the event of attacks and crashes. It also guarantees the ability to provide minimum services in the event of a power outage and blackout [17],[18]. In IoT, most services are requested in real time, so if the request is not answered in time due to unavailability of the service, this request cannot be rescheduled sometimes [35]. For example, if information about an intruder in a home is sent to the police station the next day, that information loses its value. Likewise, if the blood glucose meter is given disturbing readings, and those readings are received late by the doctor, this can result in significant harm to the patient that may sometimes lead to the loss of his life.

DoS attack is one of the most dangerous attacks targeting availability on the IoT. This attack drains network resources, making it unable to serve ordinary consumers and

respond to their requests [22],[49]. Therefore, techniques should be studied and applied to ensure availability in IoT. For instance, IoT system needs to provide backup of vital information to prevent data loss and ensure data availability. On the other hand, firewalls can be installed on the network to prevent DoS attack [32].

3.4.2. Privacy Requirement

Privacy is the ability to protect data from eavesdropping and to control how it is shared and distributed. Privacy is also concerned with concealing the identity of the owner and recipient of the information, which is an important aspect, especially in the case of personal and sensitive information [53].

Since many people, devices and services are communicating and sharing everything online, such as photos, videos, health records, etc., it has become important to consider privacy as an important security requirement [32].

In an open environment like the IoT, a lot of personal information about individuals can be collected without them knowing if there are no security measures to prevent this. In an IoT environment, individuals will be able to take advantage of a large number of services that require personal information about the consumer. These services may require photos, emails, phone numbers or bank account information, etc. Moreover, the environment itself may be able to obtain this information automatically as a result of the interconnection between its services and devices. For example, some smart TV companies collect information about their customers in order to assess viewing behavior usually without the knowledge or desire of customers. So, privacy must provide protection to individuals by giving them full control over their personal data. Individuals must know who is responsible for collecting their data and where it is stored, and the owner of the data must be notified before it is shared through the system [1],[5],[11].

The privacy requirement should ensure that consumers' information and identities are in safe hands and completely protected from disclosure or leakage. The inability to access personal data except by the authorized person means that no other authenticated customer who has nothing to do with this information or any other type of individual can access it [5]. For example, hospital administration personnel need access to patient data for

administrative purposes (patient registration, billing, age ...) and are not allowed to know the patient's disease details. In this case, privacy concerns granting employees the right to access information related to their work only without disclosing sensitive medical information not related to their work [48].

IoT has become an integral part in various applications like remote patient monitoring, energy consumption control, traffic control, and smart parking system. In all of these applications, users require protection of personal information which is related to their movement, habits, and interactions with other people. Therefore, there is an urgent need to propose protocols and administrative frameworks for dealing with privacy and know where and who stores, manage and access information in IoT [56]. For example, people's information must be destroyed when they no longer need it. As another solution, all communication between IoT nodes can be encrypted using proper encryption algorithms. This solution ensures that this connection is confidential to the opponent who tries to eavesdrop on this connection and at the same time, privacy is guaranteed. Access control mechanisms are also among the steps that help protect individuals' privacy. This mechanism controls who has the right to access the data and what kind of action he can take on it [51].

3.4.3. Trust Requirements

To build trust between things, they must first verify each other's identities. In any system, trust is the foundation for communication between entities, which is strongly dependent on other domains like privacy and security. In fact, an entity should interact with another only if trust is established between them. The trust requirement means that IoT devices wanting to communicate with each other must be sure of each other’s identity, and that they have right to claim and build this connection. In simple words, the trust requirement answers this question: "Can the device sending the data be trusted and is it really the one who claims it?" [51],[57].

In the IoT, many devices are portable in nature as they can be physically transferred from one owner to another or from one location to another. In an environment like this involving ambiguity and doubts about the correctness of information and the identity of contacts,

trust is beneficial. Connected entities need this trust to ensure that the source of the data they receive is reliable and that the data can be trusted [57].

Trust-building mechanisms are needed to build trust between IoT devices to provide the interoperability between them. However, creating and maintaining the trust in a wide variety of objects in heterogeneous, mobility and scalability environments presents a major challenge for scientists and manufacturers [57].

Creating, updating and revoking credentials, keys, and certificates are methods used to achieve trust between communicating parties in the IoT [48]. Trust is often defined by many characteristics such as authentication, authorization and accountability. These characteristics are explained below:

3.4.3.1. Authentication

Authentication is a major requirement of the IoT because it provides confidence in the devices participating in the IoT network and this is critical to improving network performance. This security requirement is for everything that wants to connect to an IoT system. Typically, the authentication and identity management work together to manage and secure access to information, resources, and connect to the network. Identity Management uniquely identifies objects while authentication enables the IoT objects to confirm the identity of the peer it is communicating with. In other words, authentication enables the recipient to verify whether he has actually received the data from the sender who claims what he is. This means ensuring the legitimacy of the data presented in the networks, as well as the legitimacy of the objects sending and requesting that data. So, to provide security, no IoT entity should have the ability to directly access available resources unless its identity is authenticated first [16],[17],[32],[51],[55].

The process of authenticating and verifying the identity of an object is a prerequisite for allowing access to resources and requests any service in the IoT. This process ensures that no attacker can enter the network through a false ID and password and enter false messages. Hence the importance of having a mechanism that enables the recipient to ensure that the message received comes from a reliable source and at the same time enables the senders to ensure that the requester of information is reliable [37],[58].

The nature of scalability in the IoT is a major concern when authentication is taken into account. Identifying a large number of devices and authenticating each object directly in real time can be a huge challenge due to the vast number of objects connected to the IoT [38]. Because of all this, it is necessary to propose a mechanism that effectively deals with the scalability of devices in the IoT environment and at the same time enables entities to confirm each other's identity in every interaction in it. To work around this issue, different schemes and algorithms and pre-shared keys are proposed that are lightweight and do not adversely affect battery life within devices and their performance. For example, symmetric key encryption depends on both parties having the same encryption key to confirm their identity [15],[59]. Also, one of the methods used for authentication is what is known as the direct authentication methods for humans and machines. The user can open the office door using biometric identification (such as a fingerprint) or an object within a personal network, such as a passport, ID card, or smartphone. The combination of authentication methods can prevent any overall system security loss. These groups usually take the form of who I am, what I know or what I have + what I know [52].

3.4.3.2. Authorization

There is sometimes confusion between authentication and authorization requirements although these requirements differ completely in meaning. Authentication means confirmation of identity, while authorization means allowing access to the system. In simple terms, authentication is the process of self-verification, while authorization is the process of checking what the self has access to. Authorization enables determining if the person or object, after authenticate his identity, is permitted to, for example, access, use, or read the resource. These privileges or permissions are determined by the device or by the identity of the users. So, with proper identity, anyone can access IoT system while without permission, no one can access any resource in it [11],[17]. Therefore, it can be said that the authorization policy determine which specific resources can be accessed by any entity or user [60].

Authorization is typically implemented through the use of access control. Access control and authorization are important in establishing a secure connection between a number of

devices and resources. After determining whether this object has the right to access this resource, access control controls access to that resource either by allowing or denying 0. The main issue that must be addressed in access control is to make it easier to create and modify its rules, and to make these rules easy to understand and follow [16],[61].

3.4.3.3. Accountability

Accountability is essential to enhancing consumer confidence in the IoT. This security requirement provides accountability for those who build, deploy, manage, use, and interact with IoT systems. In the event of any error or leakage of information or its use for a purpose other than the purpose for which it was collected, the entity that requested, collected, processed and stored that information will be tracked. Accountability ensures that every action related to consumers or their information must be clearly and explicitly linked to the perpetrator of that action. It is essential that IoT users know how to handle their private information, where it is stored, and who has the right to access and process it. For example, if a business transaction fails due to IoT system errors, especially if it involves large amounts of money, companies need to know who is responsible [62].

This security requirement presents a particular challenge in IoT due to the scale of reuse of devices, services, and data for many purposes. For example, sometimes ownership of IoT devices changes from one person to another, the IoT service provider changes according to need, and so on. So, the administrator or owner today is not the same as tomorrow [52]. Given that IoT technology is widespread and complex, fulfilling this security requirement is a real problem, however, this has not prevented some attempts to implement it. The existence of a strong deterrent is the payment of fines or legal prosecution of those who betray trust and manipulate information is one of the most important means to achieve accountability requirement. On the other hand, the entities dealing with information must be transparent with consumers and explain to them how their information is processed, where it is stored, and who is responsible for accessing it. Also, signing an official document between the parties dealing with information preserves the rights of each of them and determines who bears legal responsibility in the event of an error or loss of data. Studies and research are now moving towards finding effective ways

to track data journey from end-to-end across the IoT and record it. These procedures identify the interactions that led to data leakage, physical harm, or other errors, helping to reveal the responsible by knowing who requested data, the manner in which it was received, how it was processed, and where it was stored. The reference [63] suggested using what is known as Databox, especially in smart homes. The Databox is an edge device that collects information from the sensors, processes it and sends the result only to whom it may concern. This helps not to publish personal information of homeowners for the purpose of processing and access it.

The information listed in this chapter provided an answer to some of the research questions raised in the first chapter. This chapter answered the first question, which asks about the importance of security in the IoT. For example, the presentation of security incidents that occurred in real life, largely shows what problems consumers of the IoT can encounter when there is no security. This chapter also explained the reasons that made it difficult to use known security methods and techniques to protect the IoT, which represents an answer to the second research question. In addition, the third question was answered regarding the basic security requirements that must be met in the IoT to be considered safe technology.

The previously mentioned security requirements are primarily targeted by cyber attacks. For example, there are cyber attacks such as the eavesdropping attack that targets the confidentiality of data exchanged between IoT nodes. On the other hand, a node capture attack undermines trust between the communication parties. The next chapter reviews these and other common attacks targeting the IoT.

CHAPTER 4

ATTACKS ON IOT ARCHITECTURE

In the IoT, billions of heterogeneous things perform different functions, and they communicate with each other through heterogeneous communication methods using different communication protocols. Given that this system often exchanges sensitive information, ensuring the confidentiality, integrity and availability of this information becomes a top priority. Therefore, robust and effective security technologies must be provided in the IoT, in order to ensure data protection and reliable services for all parties. Reducing the number of security accidents and attacks on the IoT system will increase customer confidence in this technology and the services it provides [1],[16],[17]. However, there are several factors affecting the ability of the IoT system to provide security for its consumers, among these factors:

- The location of the nodes or devices connected to the IoT
- Ease of physical or electronic access to the nodes
- The level of security available in the means of transferring information in the IoT

Providing IoT security is a complex topic for several reasons that were mentioned previously. Therefore, the best way to study the security issues of the IoT system may be to use the IoT architecture as a reference. Where the IoT layer-based architecture can be used to simplify the problem by studying the security issues of each layer separately. This idea was adopted because some of the most prominent security problems facing the IoT arise from security problems in the technologies used in each layer. These problems arise because every technology used in these layers contains vulnerabilities that attackers take advantage of to compromise the IoT system.

When the security of each layer is achieved in the IoT architecture, IoT security is achieved as a whole [37],[38]. It is important to note that to achieve the full security of

the IoT system, the security of each layer must be guaranteed and this security must be strong in and of itself. This is because poor security for one layer will affect the system as a whole, regardless of how strong the other layers are. Therefore, it becomes important to present the security problems that each layer is exposed to separately and try to find security mechanisms that enhance the protection of these layers [37].

The most basic architecture of IoT, as previously mentioned in Chapter 2, has divided into three layers: perception layer, network layer and application layer. Each of these layers is responsible for performing certain tasks, but at the same time it needs to collaborate with the other layers to enable the IoT to function. Each layer contains its own techniques that enable it to do its job. The functions of these layers are collection, transmission and presentation of information [64].

From security point of view, it can be said that the IoT architecture has some important vulnerabilities and issues related to security and privacy. Therefore, as more and more devices connect to the IoT, each layer will likely be exposed to a greater number of security threats and attacks. These attacks not only target information, but also the devices, the applications, the services and even the system as a whole. Each attack has a specific target or group of targets that differ from the targets of other attacks. These targets can be either eavesdropping, tampering, obstruction or destruction. For example, attacks can aim to steal sensitive information, such as credit card information, financial account passwords, and health-related information. Moreover, it may try to hack into IoT components, such as edge nodes, to launch attacks against a third party. For example, remote monitoring systems, and smart devices, such as smart TVs, can be used to spy on an important person. Because smart TVs have the ability to connect to the Internet in addition to providing other features, including enabling the user to use the TV's microphone to tell the TV to change the channel or turn up the volume. Some even have facial recognition features and can use the built-in camera to recognize the users and choose programming for them. All of these features can be used against the users. For example, an attacker can use the built-in microphones and camera to listen and watch the users. On the other hand, these cyber attacks can target companies and banks in order to

inflict financial losses, to paralyze their movement, or to destroy their reputation [29],[44],[55]. In this chapter, some of the potential attacks on each layer of the IoT architecture are presented. The attacks covered in this chapter are illustrated in figure 4.1. These attacks are presented generally without giving details of the attacks to which each technology is subjected in each layer separately. This is because giving these details will make this topic a rather big topic given the diversity of technologies in each layer in addition to the diversity of the attacks they target.

4.1. Perception Layer Attacks

The perception layer is especially found in IoT environments, unlike other layers that can be found in other information and communication environments [34]. This layer is the link between the physical world and the digital or electronic world [55]. The primary techniques used in perception layers are WSN, RFID and other types of sensor and identification techniques [29].

The perception layer may encounter many security threats and attacks. Firstly because, this layer contains a large number of nodes, which are distributed over large areas. This makes it difficult to monitor and provide protection for each node. Because of this, attackers may have easy access to these nodes or devices for the purpose of replacing, tampering with or even completely destroying them [65]. However, these nodes are not only attacked physically, but they can also be attacked electronically.

The second reason is that the nodes do not contain enough resources to enable them to use high-quality security technologies or to use known and effective security techniques [55],[65]. The third reason is the low quality of the node industry, because it is often made of low-cost materials. Finally, most IoT nodes use the air as a data transmission medium. This makes the attacker's task of intercepting data, often unencrypted, easier and simpler [34].

Security challenges lie in the perception layer on attacks targeting data collected by this layer, as well as attacks targeting devices that collect it [32]. Therefore, it must be ensured that the components that assist in obtaining information in the IoT (RFID reader and tag, and sensor network, etc.) have not been compromised, controlled or destroyed [37].

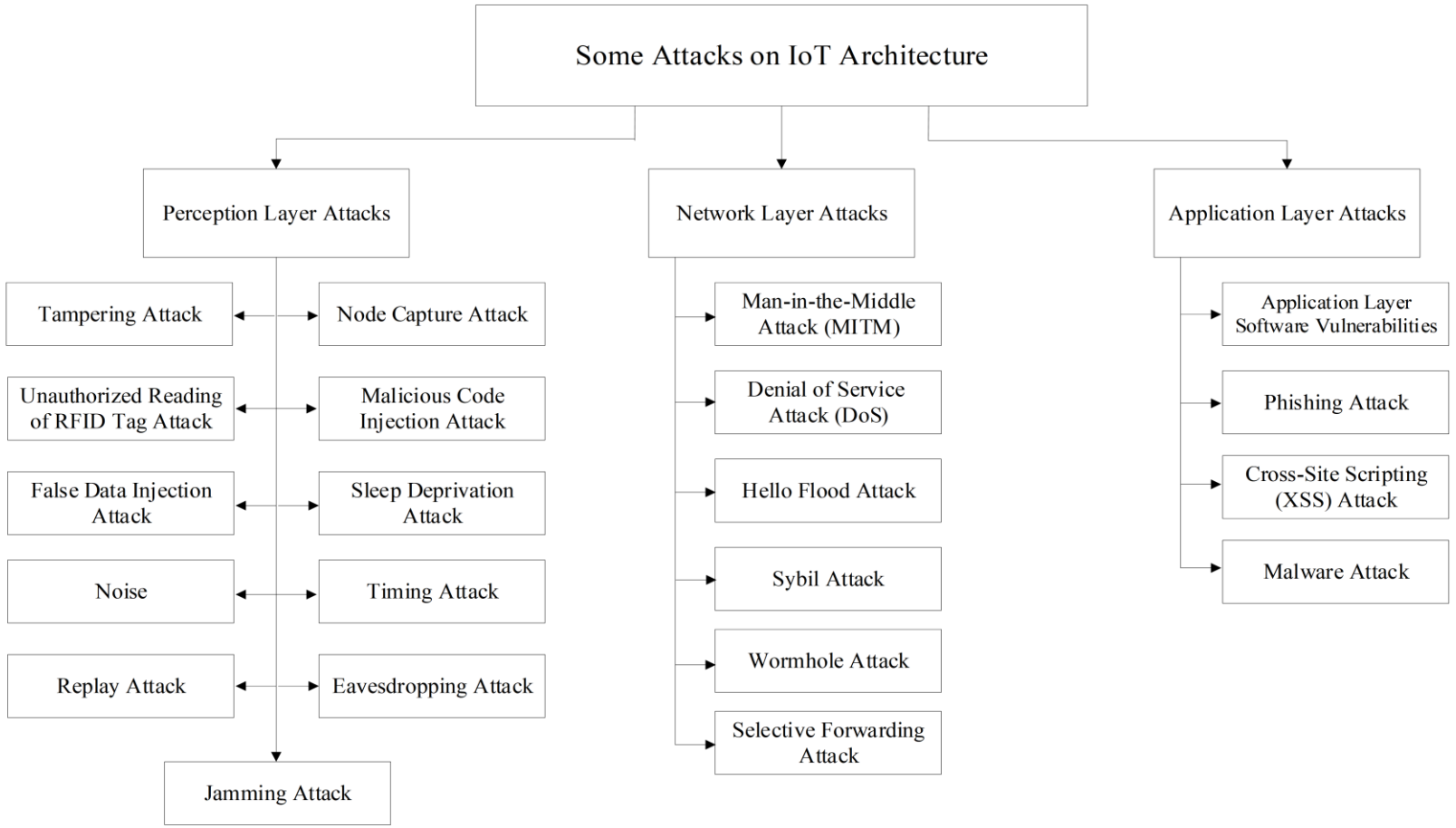


Figure 4.1 Some Attacks on IoT Architecture

These components can be attacked physically, or the programs inside them, or even the information that they exchange between them, can be attacked. Therefore, attacks on this layer can be classified into two types: physical attacks and network attacks (the network attackes here target the communcation between RFID reader and RFID tag) [22],[29],[32].

In the physical attacks, the node is targeted physically due to the attacker's ability to reach and touch it. Here the attacker targets the body of the node or the system inside it. Physical attacks enable an attacker to extract sensitive information stored in the node, tamper with its components or programs, or replace the entire node with a malicious one [16],[66]. On the other hand, network attacks target information when it is collected, for example information exchanged between an RFID tag and an RFID reader.

There are a large number of attacks targeting the perception layer. The number of these attacks is increasing day by day, as attackers try to create new types of them to carry out malicious purposes. Some of these attacks may target more than one layer of the IoT architecture. The most common attacks on the perception layer are explained below:

4.1.1. Tampering Attack

To reduce costs, most nodes are not manufactured from tamper-resistant materials, making them vulnerable to this attack. Tampering is the physical access to the node performed by an attacker. After the attacker accesses the node, he can manipulate, modify or stole it. For instance, the attacker can cause physical damage to the sensor node, by replacing the whole node or part of its components or even destroying it, which will affect the IoT system in one way or another. This attack also gives the attacker access to sensitive data stored in the node such as cryptographic keys [4],[22]. The success rate of this attack is high due to the fact that most IoT nodes are not monitored, protected, or placed in closed locations, making them accessible to attackers.

4.1.2. Node Capture Attack

This attack, which could lead to a serious impact on the IoT, is also called the node replication attack and the clone attack. This type of attack targets RFID tags as the attacker uses them to create fake copies of them. To do that, the attacker first captures or extracts

data from a valid tag by either eavesdropping the reader-tag communication or doing physical tampering. Then, the attacker enters this stolen data into a new tag so that this new tag becomes a replica of the original tag. In order to achieve the desired malicious action, this cloned tag is inserted into the system in a manner that the reader cannot recognize the cloned tag from the original one. The aim of the attack is to fool the reader for getting legal authentication to access to the system. Once the attacker is able to enter the system, he will carry out several more attacks. For example, the attacker can then send a large number of spoofed and useless messages just to create congestion in the network to slow or disable it. The danger of this attack is that it could target important applications such as electronic passports, credit cards and entry cards. For example, it is possible for an attacker to duplicate the tag into an electronic passport to make a forged passport which could lead to serious consequences [37],[67].

4.1.3. Unauthorized Reading of RFID Tag Attack

In this attack, the attacker exploits weak authentication procedures in RFID systems to obtain unauthorized access to the tags. The main objective of this attack is to violate sensitive data stored in the RFID system by reading it [21],[68]. Information obtained from the RFID tag can be used to track the owner of the tag, or it can be used to reproduce the tag so that the opponent can impersonate the owner of the tag.

The danger posed by this attack is reading the tags on passports and bank cards that contain sensitive information about the identity of the owner, his bank balance, etc. Also, there is a possibility that the attacker will track down the consumer depending on the tags in the items he carries, which makes it easier to know his location and use this to steal his home or office, for example [69].

4.1.4. Malicious Code Injection Attack

This attack is considered a type of physical attack in which an IoT device is hacked by injecting malicious code into the device by using a USB device or debug modules of the device. For example, the attacker uses this attack to break the normal boot process of a device by replacing the actual boot images with custom boot images. When the device starts the boot process, it boots from custom boot images.

Also, with this attack, an attacker can install malware such as virus on the device and use it to access the device remotely, and from it to the IoT system. Also, this injected malicious code can perform many functions such as help the attacker to move all information smoothly outside of the IoT network to a specific destination. The injected malicious code could give the attacker access to the IoT system, and even complete control over the IoT system [22],[32].

4.1.5. False Data Injection Attack

IoT applications depend to a large extent on data collected by the various and widely available sensors. Privacy and data integrity in applications dealing with sensitive data such as healthcare monitoring and home automation is a important requirement. The danger of this attack is that it destroys data integrity and privacy. Therefore, if an attacker breaks into a node and injects it with wrong data, this results in false reports and wrong decisions that lead to false events. The false data can be injected into the devices by accessing the device physically or remotely by using various communication media such as Bluetooth or Wi-Fi [22].

4.1.6. Sleep Deprivation Attack

This attack is a type of DoS attack where a specific node or group of nodes is targeted and killed by depleting their energy resources. In the IoT, most nodes have a limited power, which makes it important to program these nodes to work with a sleep routine. This routine is used to reduce energy consumption in order to extend the node battery's life cycle. When the node sleep, it is not busy capturing information from its surroundings or sending it or receiving it from others to conserve its energy. On the other hand, a node is in a waking state if it has a task to perform.

In a sleep deprivation attack, the malignant node sends requests and inquiries to the victim node to force it to respond in order to keep it awake, which increases the rate of energy consumption in the shortest possible time. This increase in power consumption speeds up the battery drain, which causes the node to exit from service. Unfortunately, this attack is difficult to detect because it is only carried out through the use of seemingly innocent messages [21],[54].

4.1.7. Noise

Noise in the perception layer means false positive readings. This means that the RFID reader reads RFID tags as well as other unexpected readings. This can be attributed to the many reasons such as:

- RFID tags are far from the reader beyond the reader's normal reading range so that the signal is weak or distorted
- Bring the tags close together. For example, while reading items from one tag, the reader may read items from neighboring tags.
- The presence of some devices that are sending wireless signals at the same frequency as the tag, which causes interference in the signals. For example, cities and industrial environments contain abundant electrical noise sources such as electric power lines, radio and television stations, and electronic equipment
- Reasons due to an error in the reader or reasons related to the surrounding environment

RFID systems generally operate in a noisy, unstable environment. Therefore, their communications are subject to possible interference and collision that distorts the information and affects its reliability and accuracy. Noise - whether intentional or unintended - can lead to incomplete or erroneous information and this is dangerous especially if this information deals with applications related to people's lives [54],[70].

4.1.8. Timing Attack

This attack relies on the fact that the attacker can identify the secret key, which is used to encrypt data, by tracking how long it takes the device to decrypt data. The timing attack is somewhat similar to someone noticing that the time it takes, for example, to dial the number three in analog phones than it takes to dial the number nine.

Due to the weak computing capabilities that most IoT devices possess, they cannot use cryptographic keys or sophisticated encryption algorithms to encrypt the information.

This attack is based on the fact that each letter in the alphabet takes a certain time to encode and a certain time to decode. Using this fact, the attacker can conclude and find the key

used to encrypt the information. As he uses some mathematical operations and logarithms to analyze and calculate the time taken to decode the information. Once the attacker has access to the key used for the encryption, he can simply expose the information encrypted with that key [22],[32]. This attack can occur at both the perception layer and the network layer. In the perception layer, it targets the information exchanged between the RFID reader and the tag. While at the network layer, it targets data sent between IoT nodes in the same network or over the Internet.

4.1.9. Replay Attack (or Freshness Attack)

In this attack, the attacker copies a message that he intercepted for the purpose of sending it back later. Initially, the attacker intercepts and stores a message sent from a legitimate node. This message contains legal identifying information for the node. After a while, the attacker uses a malicious node to send the same message to the destination node. This helps the malicious node impersonate the legitimate node, making it able to gain the confidence of the IoT. With this confidence, the attacker can modify or restart the node, causing other problems in the IoT system [32],[68]. An example of a replay attack is when an attacker registers the connection between the access card reader and the access card. So the attacker can use this registered information to gain access to a secure facility at a later time.

4.1.10. Eavesdropping Attack

The wireless nature of IoT system makes eavesdropping one of the most serious and widely deployed threats. This attack, as its name suggests, is the intentional listening of a conversation between the sender and the receiver. The eavesdropping attack targets the information transmitted wirelessly at both the perception layer and the network layer. The eavesdropping attack can be difficult to detect because the network transmissions will appear to be operating normally. The distance between the transmitter and the receiver is an important factor in the success and detection of this attack. The shorter the distance, the harder this attack is to execute and easier to detect, and vice versa [70].

This type of attack is divided into two types: passive and active. In a passive attack, the attacker captures and reads the information without tampering with it, then sends it back

to its destination. In an active attack, the attacker captures the information, reads it, manipulates it, and sends the modified information to its destination. Active eavesdropping attack is also called Man-In-The-Middle attack (MITM) [44],[64].

In the perception layer, the passive type of eavesdropping launches when an attacker captures data transmitted between RFID tag and reader. This is due to the limited resources of IoT devices, which makes it difficult to use any encryption technology during the transmission process at times [54]. In the network layer, the eavesdropper intentionally listens to private conversations via communication links, whether between nodes or between node and network. The eavesdropping attack can provide valuable information to an attacker when data like usernames and passwords is not encrypted. The attacker can then use this information to threaten the confidentiality of the information and the privacy of users in the system.

Confidentiality of information is threatened when an attacker reads, copies, or manipulates private information, thus violating the privacy of the owners. The information intercepted also enables the attackers to launch other dangerous attacks that may harm the system as a whole. For example, with the help of this information, an attacker could add a malicious node to the set of authorized nodes to damage the IoT system [4],[32].

4.1.11. Jamming Attack

We have already talked about the unintended noise that the transmitted signals are exposed to between the transmitter and the receiver. A jamming attack is a type of intentional noise that both the perception layer and the network layer can experience. Jamming is a deliberate attempt to disrupt the air interface between a sender (such as an RFID reader) and a receiver (such as an RFID tag) resulting in a limitation of communication capabilities. For example, jamming attack can be used to prevent send alarms within wireless security systems.

The attacker launches this attack by generating radio noise at the same frequency that the system is using, using several jamming sources. The target of the attacker is to cause interference between the noise signals and the radio frequency of the system.

This interference causes two things to happen. The first is the effect on the integrity of the data sent. The second is to make the wireless communication medium noisy, which sometimes prevents the communication parties from using it to send and receive data. For these reasons, this attack can be considered a type of DoS attack because this attack targets the availability of information and communication media by making the environment busy with noise, making the data transfer in it slow or even difficult or impossibl [71].

4.2. Network Layer Attacks

The network layer which might be both wired or wireless is exposed to numerous kinds of attacks. Achieving security in the network layer means that the network layer must maintain the integrity, confidentiality and availability of data whenever this data is transferred over the network and deal with everything that threatens it [64].

Network layer is the second layer in the architecture of IoT and it is not specific for the IoT environment, it is the backbone of every information and communication environment [34]. The main function of this layer is to send and direct the data collected from the perception layer to its destination via the communication media [72],[73].

The IoT uses of the Internet, with all its well-known and long-used routing and transmission technologies, as the primary method of transmitting information. The Internet is known as an ancient technology that has evolved over the years. This technology, in turn, suffered from problems and was subject to attacks that threatened its security. This required finding solutions and means to reduce these threats, thus ensuring the continuity and spread of the IoT. However, using these methods as they are in IoT technology may be useless as it is in the traditional Internet for many reasons such as [37],[59]:

- The traditional Internet security architecture design depends on the user playing an important role in it, and this does not necessarily apply to automatic communication between devices.

- The IoT contains a large number of devices. If the current authentication method is used to authenticate devices, this large amount of traffic is likely to be causing network congestion.
- The mutual authentication among a lot of equipment causes serious waste of the key resources.
- The heterogeneity of the IoT makes it difficult to use standardized network protocols.

The network layer in the IoT mainly consists of common technologies used in data transmission such as Worldwide Interoperability for Microwave Access (WiMAX), Wi-Fi, Bluetooth, 3G, 4G, etc. [55]. Because the IoT uses these technologies to transfer information, more attention must be paid to their security and remove vulnerabilities, which helps resist the attacks that target them. This means that network layer security includes access network security and core network security [37]. Although there are security concerns in this layer, there are many protection methods in use and are well defined, given that the technologies present in this layer have been known and used for a long time [34].

The most security challenges in this layer are related to wireless networks in IoT, because, most IoT devices are connected via wireless communication links. The two main reasons behind this challenge are that the wireless technology broadcasts the transmission so, communications may be monitored effortlessly by hackers. The second reason is that the node can join or leave the network at any time without any restrictions or little effort [32]. This poses a major threat to the network layer and makes it more vulnerable to security fears and attacks. The most common attacks against the network layer are presented in Sections 4.2.x.

4.2.1. Man-in-the-Middle Attack (MITM)

The MITM attack, also known as relay attack, is a real-time threat. This attack, a form of active eavesdropping, can target the perception layer and the network layer. In the perception layer, an adversarial device is surreptitiously placed between a legitimate RFID

tag and a reader. This device is capable of intercepting and modifying wireless signals exchanged between legitimate communication parties.

In the network layer, the attacker makes independent connections with the target nodes (sender node and the recipient node) without their knowledge by putting a physically malicious node between them. The nodes believe that they are talking directly to each other over a private connection. Then the attacker acts as a router between those nodes to control the entire conversation [54]. All information exchanged between the two nodes passes first to the attacker, and this gives him the ability to view, monitor and modify the information before they resend it to its original target. An attacker can also delete the information completely and send what he wants to the target nodes. Therefore, the MITM attack can violate the confidentiality, integrity and privacy of data circulating in the IoT by monitoring, eavesdropping, tampering and controlling communication between the two normal nodes. The danger of this attack is that the connected nodes often cannot detect the presence of a malicious node and recognize the attack even if the nodes find invalid data entry. Rather, the system may assume that the problem occurred due to network errors and that the nodes in it are still communicating directly with each other [22],[32],[37],[68].

4.2.2. Denial of Service Attack (DoS)

DoS attack is one of the most common attacks targeting the IoT system. DoS attacks that can be launched against the IoT are different and varied, but they all have one goal. This goal is to make the IoT system unavailable to consumers and thus to deprive them of the services and resources that the IoT provides to them. In other words, the DoS primary goal is to make nodes, data, services, applications and network not available to their legitimate users. This attack achieves that by trying to restrict access to those resources instead of sabotaging the resources themselves.

Although DoS attacks are not primarily aimed at stealing or losing important information, it is wrong to consider them as non-dangerous attacks because they may cost the victim a great deal of time and money.

In this attack, the attacker drains the resources available in the IoT in three ways [16],[32]:

- Target the network itself by flooding it with huge traffic
- Target the resources of IoT nodes like servers by sending too many requests at the same time. This causes the server to fail to respond to all requests, which either causes the server to crash or slow down.
- Physically destroying the sensing nodes, so that the nodes cannot perform their functions, which may lead to depriving consumers of some services or information

There are several types of attacks against the IoT system that fall under the category of DoS attack such as jamming attack and tampering attack in the perception layer and hello flood attack, selective forwarding attack in the network layer.

4.2.3. Hello Flood Attack

Some routing protocols in WSN require that nodes broadcast a hello message to inform their neighbors of its presence, join the network, and share channel and routing information with them. These hello messages let the nodes know their neighbors and they assume that they are within (normal) radio range of the hello message's sender. When each node receives a hello message, a node updates its routing table and registers the sender of the hello message in it. Then, it becomes possible for the nodes to use the node with the hello message to route messages to the base station or to other nodes [74].

A hello flood attack can affect the network in three ways. First, when a malicious node broadcasts a high-power hello packet to convince other nodes (near or far) that the malicious node is its neighbor. Therefore, the nodes may redirect their packets to that malicious node, causing them to be lost. If the nearby nodes direct their data through the malicious node, then this data can be read, modified, or destroyed so that it reaches its destination late or not at all. In the case of remote nodes, which think that the malicious node is their neighbor, two things happen to them if their data is routed through the malicious node. Either they experience a delay or loss of data, as happened to the nodes near the malicious node. Another thing is that they can drain their resources even more by sending data to a remote node [74].

Second, when this attack is considered a type of DoS attack. This attack can flood the network with a large number of hello messages, causing network congestion and thus reducing its efficiency and availability. Third, when the malicious node deludes the nodes far from it that it is their neighbor, this leads to confusion and falsification of routing information [74].

4.2.4. Sybil Attack

In a Sybil attack, the malicious node impersonates many fake identities in the same network and appears to the other nodes in that network as a group of nodes. The danger of this attack is that most Sybil nodes behave similarly to ordinary ones. This makes the distinction between a malignant node and a legitimate node difficult.

The aim of this attack is to extend control over the network, for example by interrupting the flow of information to other nodes on the network or trying to influence this information. Victims send messages to the malicious nodes, assuming that thay will forward it to other nodes, so the attacker manipulates this information before forwarding it or even never forwarding it. On the other hand, if the malicious nodes send wrong data to the neighboring legitimate nodes, they will accept this data without any doubt as to its source. This bogus data could be spam, advertisements, or other useless data that an attacker sends to fill the memory of neighboring nodes. In other cases, this fake information could be malicious software to steal other users' private information [4],[32],[64],[75].

4.2.5. Routing Information Attack

The routing information attack is the primary attack of this layer and affects how messages are routed. The main objective of this attack is to control the traffic of data packets as they pass through the network by targeting the routing information. The attacker uses this attack to redirect, mislead, or drop packets as they pass through the communication channel. The simplest way to do this is to make the packets move in circles (routing loops). This attack has two goals: one for delaying information, and the other for generating network congestion. Both of these goals affect the performance of the IoT especially in sensitive applications such as smart healthcare and security systems [4],[22],[32],[44].

The wormhole and selective forwarding attacks are examples of routing information attack.

4.2.5.1. Wormhole Attack

Wormhole attack is considered one of the most dangerous attacks that threaten the network layer because it does not require penetration of any sensor node in the network, obtaining a valid network identity, or even knowing the contents of the packets. Alternatively, it can be implemented even at the initial stage, when the sensors begin to detect surrounding information.

In this attack, two or more attackers colluded to make data packets circulating in the network pass through their own high-quality, low latency channel. The attackers do this by positioning themselves at different strategic points within the network and then connecting to each other, forming a tunnel called a wormhole.

As shown in figure 4.2, this attack begins when a source node A tries to find a path to deliver its data packets to a destination node B. First, the A sends a request to get a path. When one of the malicious nodes M1 receives this request, it transmits it to its partner M2 through their high-speed tunnel. After that, the M2 passes the packets to their destination B. This path is faster than any other path within the network because the attackers use a high-speed channel that causes the destination node to adopt this path and ignore any other path. This attack makes A and B think that they are neighbors and only move away from each other with one hop when in reality they are not neighbors. Node A spreads this misinformation into the network, so any node wanting to send data to B does so through A. Thus, the two complicit attackers M1 and M2 made sure that the nodes used their malicious channel, enabling them to control, delay or drop the packets that passed through them or launch other attacks.

It can also be mentioned that a wormhole attack confuses the routing tables within the network and manipulates the time when information arrives to its destinations inside the network [4],[32],[76]. It should be noted that if the attackers use this tunnel safely and reliably, they will provide a useful service to make the network more efficient, but unfortunately, they have malicious targets behind this attack.

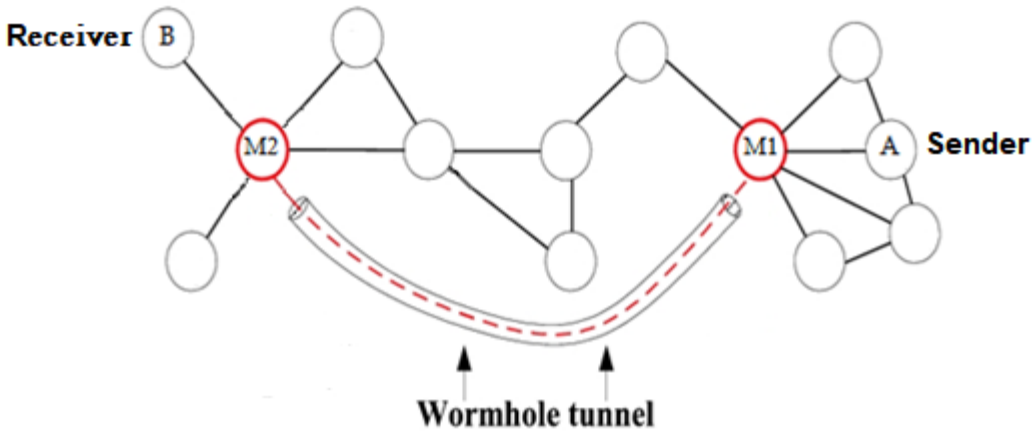


Figure 4.2 Wormhole Attack against WSN [77]

4.2.5.2. Selective Forwarding Attack

This attack is simple to implement but difficult to detect. In a selective forwarding attack, the malicious node functions as a normal node so that other nodes send information to it to forward over the network. When the malicious node receives this information, it forwards messages it did not care about, and forbids all those it does not want to publish. Besides, this node tries to stop the packets passing through it from a particular node or a group of nodes in the network by dropping these packets or refusing to forward them to their destinations. Also, a malicious node can choose a specific node to send information to instead of all nodes targeted. These nodes are determined based on the attacker's requirements to achieve his malicious aim [4],[38],[78].

As a result of the above, it can be said that the selective forwarding attack drops data packets based on two different methods. First, dropping packets based on their type and second, dropping packets on the basis of their source or destination. However, regardless of the target of the attacker, dropping data packets, especially those containing sensitive information, so that they do not reach their destination, can, for example, render entire surveillance systems useless. This attack is difficult to detect because it is targeted selectively. Sometimes a malicious node does the job of directing data through it without

any hostile action against it, which makes it just like any normal node. While at other times, it does not route that data.

4.3. Application Layer Attacks

The combination of the large number of connected devices, the large amount of data circulating, and the variety of applications provided by the IoT, leads to security problems at the application layer. These security issues vary according to the application and depend on the complexity or simplicity of that application. Data privacy, user privacy, access controls and data disclosure are important security issues for the application layer [3],[22],[79]. For instance, the different applications have different authentication mechanisms, which makes integration of all of them very difficult to ensure data privacy and identity authentication [22].

In the application layer, an attacker can easily hack into secret data such as passwords, and it is easy to inject malicious data into this layer. Therefore, it becomes important for access privileges to be limited to ensure that unauthorized access to and use of data does not occur [21]. In addition, IoT users must control the data they want to disclose and must be aware of who has used their data and when [18]. It is also important to say that this layer must have the ability to identify valid data, spam data, and harmful data and filter them in order for applications to be considered secure for the user and maintain the privacy of his data [79].

This layer is a link between the IoT system and its users. Consequently, its main purpose is to provide the services and applications that the IoT provides and that users want. Users access these services and applications through an application layer interface, for example, using mobile devices, computers, and others. Thus, the other challenges in the application layer is how different users will interact with the applications, the amount of data that will be revealed, and who will be responsible for managing these applications [22]. Some of the potential attacks and threats to the IoT application layer are presented below [32],[55]:

4.3.1. Application Layer Software Vulnerabilities

This point is not an attack in and of itself on this layer, but rather a safety factor or security vulnerability that helps these attacks to occur.

Software vulnerabilities are security holes or flaws discovered in an operating system or application. Hackers might benefit from this weakness by writing code that detects these vulnerabilities and exploits them to insert malicious software into a device.

As a result of the manufacturers' lack of interest in the aspect of secrecy when designing or producing IoT devices, several unintended security vulnerabilities appeared in the application layer of the IoT. These vulnerabilities can exist, for example, as a result of using pre-existing software to run a device or provide a service that is not specifically designed for use in an IoT environment. The use of weak code written by programmers also creates security vulnerabilities in the system. Also, developers and programmers may leave design flaws and software bugs that can lead to security holes in the system.

Attackers are looking for these vulnerabilities in IoT software to exploit them to launch various dangerous attacks on the IoT environment [17],[55]. Therefore, getting rid of security vulnerabilities and defects in the application layer is important, and any negligence or lack of interest in this topic may lead to:

- Weaknesses in authentication, authorization, or encryption practices
- Access control problems
- Buffer overflow

Buffer overflow is an example of the most common application layer security vulnerabilities. Buffer overflow is an anomaly that occurs when the program writes data into the buffer so that the amount of data is larger than the buffer capacity, which leads to the buffer overflow. Attackers can exploit buffer overflows with the goal of altering computer memory to prevent or control program execution. Unfortunately, many mobile apps are written by programming languages such as C / C ++. These languages are known to be prone to buffer overflow and incorrect calculation of buffer size.

4.3.2. Phishing Attack

Phishing attack can be referred to as automatic identity theft. The concept of "phishing" came from the traditional "fishing", whereby a fisherman roams the river and throws bait to the fish to deceive and catch it. Likewise, the “phisher” roams the Internet, trolling his victims using bait to deceive them and steal their credentials [80],[71].

In this attack, the attacker sends fraudulent communications that appear to be from a trusted source. The goal of this attack is to steal sensitive data such as credit card and login information, or to install malware on the victim's machine that the attacker uses to launch more dangerous attacks.

The attacker captures sensitive information either by using phishing emails or using fake websites. There are methods called technical phishing that the phisher uses to carry out this attack in order to obtain personal information, including the use of malicious code, key logging programs, and screenshots. These phishing techniques can be embedded in websites or in emails and are often installed on victims' devices without their knowledge. Sometimes a victim can be tricked into downloading a program on the grounds that it is against viruses, but it is in fact a virus or malware. With phishing via email, the phishing scammer sends out a phishing emails that appear innocent to the victim. Phishers usually send an email to users that contains a link or URL. Once a user clicks on this link, he will be forwarded to a malicious "phishing" website whose purpose is to collect the user information such as name, phone number, password, and credit card number. When the user enters this information, this deceptive website collects it for the benefit of the cyber criminals who use it to enter the user account or cause other damages such as extortion, theft of sensitive information, damage to reputation, etc. As for website phishing, an attacker creates a phishing website that is a replica of some legitimate website. Of course, its main goal is to defraud people in order to obtain their personal and financial data [82].

4.3.3. Cross-Site Scripting (XSS) Attack

This attack is a type of malicious script attack. Malicious scripts are pieces of code that an attacker often hides on legitimate websites that IoT users use to obtain services and

applications. These malicious scripts are the perfect bait for any victim, because the victim will never suspect their danger due to their presence on a trusted website.

Cyber criminals can execute this attack on users' systems by exploiting various security weaknesses in it, for example in browsers or in the operating system, or others. Once a malicious script (JavaScript for example) is run on the victim's system, it will download and execute what is known as a payload. This payload is a piece of malicious code that has the ability to exploit vulnerabilities in the victim's system, allowing the attacker to attack that system. This malicious script has been programmed by the attacker to attack the IoT node software by adding, modifying, or deleting it. This can sometimes lead to IoT node corruption, data tampering, and denial of services [73]. In addition, malicious scripts are used to install malware, conduct phishing attacks, and redirect users to another sites.

Sometimes, the scripts are executed automatically and without user intervention. The reason behind this is due to the permissions granted during the user's system configuration.

In XSS attack, the malicious scripts are injected into benign and trusted websites. An attacker can use XSS to send malicious script to an unsuspecting user. The end-user browser has no way of knowing that this script should not be trusted, and will execute it. XSS can access and steal any sensitive session cookie information that the browser maintains and is used with this website. Therefore, this attack is considered one of the most dangerous attacks on the application layer because, as is known, cookies help users to log in automatically. So, by using the stolen cookies, the attacker can log in with the identities of others.

XSS attacks occur in two ways: reflected–XSS or stored–XSS. In reflected- XSS attacks, the injected script is executed in the victim's browser instantly and only once, as the text is included in the response to the HyperText Transfer Protocol **(**HTTP) request. On the other hand, the goal of stored-XSS attacks is to execute script in a continuous manner. The injected malicious script will be executed multiple times whenever the victim visits the webpage containing that malicious script [83].

4.3.4. Malware Attack

Malware is also a dangerous attack targeting application layer in IoT devices, as it has the potential to disrupt the device or, in some cases, put the IoT system under the control of the attacker. The most well-known malware according to cyber attack statistics are rootkits, ransomware, bots, financial malware, logic bomb, virus, worms and trojans. These malwares are explained below [84]:

- **Rootkits:** It is a type of malware that is designed to remain hidden on the device so that it goes unnoticed, but remains active on that device. A rootkit gives cyber criminals the ability to remotely control an infected device. Rootkits can also contain a number of tools such as those that help hackers steal a device owner's passwords by tracking the keys that the owner presses to enter his password.
- **Ransomware:** This malware encrypts important files and folders, and prevents their owners from accessing them to extort money from the owners in exchange for giving them a decryption key.
- **Bots:** After infecting devices with this malware, it communicates with a server known as "bot master", which acts as a central control server for the affected devices. The bot master with its infected devices create what is known as botnets. The botnets allow attackers to take control of all connected devices for the purpose of using them to carry out various larger attacks. For example, in late 2016, the network of bots called Mirai, made up mainly of IoT devices, ranging from Digital Video Recorders (DVR), IP cameras, routers, and printers, took over the Internet. Mirai used these IoT devices to launch a large-scale DDoS attack on several prominent targets and in many different countries [84],[85].
- **Financial Malware:** As is clear from its name, the goal of this program is to try to collect bank account information from the devices that it targets. It is designed to search a computer or an entire network for financial transaction-related details.
- **Logic Bombs:** This type of malware only works after a certain event, time, or date. Logic bombs are harmless and invisible until they are activated to unload their malicious instructions. Its danger is that it stays for days, months or longer without

the user's knowledge, which makes it difficult to determine who sent it, how to stop it, and the extent of the damage it caused. Once a logic bomb is triggered, various malicious things can happen depending on the target of the hacker such as delete files, steal passwords, wipe an entire hard drive and etc.

- **Virus**: A virus is a specific type of malware that self-replicates from device to device based on its spread on a file or document. In other words, viruses spread by attaching themselves to legitimate files and programs. These infected files are placed or attached to websites, flash drives, and emails. The victim activates the virus by opening the infected file. Once the file containing the virus is opened, the virus attacks either by deleting or encrypting files, modifying applications or disrupting system functions.
- **Worms:** Worms are programs that work independently, that is, they have the ability to spread itself without user intervention and it does not need to attach itself to a software program in order to cause damage.
- **Trojans:** A Trojan horse is a type of malware that often disguises itself as legitimate software. It differs from a virus in that it cannot execute itself by itself, rather it depends on the user who is running it, thinking that it is a reliable file or program. Once the Trojan is executed or opened, it will do a lot of harmful things. such as damage, disable or steal on data or network.

These malicious programs pose many threats to IoT devices that consumers use to access services and applications, among which are mobile phones, laptops and personal computers. For example, Uapush.A, Kasandra.B, and Short Message Service **(**SMS) Tracker are mobile threats. Uapush.A is a Trojan horse that can steal data from a mobile device as well as send useless SMS text messages for the purpose of wasting money. Kasandra.B is another Trojan horse that can access sensitive data contained in the mobile phone like logs, credentials, history, etc. SMS Tracker is an android app that allows attackers to monitor SMS, phone calls, etc. of a mobile device [84].

The fourth research question, which was asking about the types of attacks that may be exposed to the IoT, was answered through this chapter. This chapter also contributed to

deepening our understanding of the importance of security in the IoT, which clarified the answer to the first research question, presented in Chapter 1, which raised this topic.

All of the attacks mentioned in this chapter need to use countermeasures against them to either detect them, prevent them, or reduce their negative effects on the IoT system. Some of these countermeasures will be presented in the next chapter. This presentation will be in two ways: a general way intended to provide protection from attacks to the IoT system in general, and a specific way aimed at providing countermeasures for each attack separately.

CHAPTER 5

COUNTERMEASURES AGAINST ATTACKS ON IOT ARCHITECTURE

As explained in Chapter 4, the IoT architecture is vulnerable to many attacks. These attacks not only target data, but also target networks, applications and devices. Due to the great diversity and severity of the attacks, there is no single technology or single solution that can address all of these attacks.

Because there are so many factors that distinguish the IoT from other well-known information systems such as limited resources, mobility and scalability, conventional security measures cannot be applied directly to IoT scenarios. On the other hand, the heterogeneous IoT environment (different applications, different devices, different protocols and different means of communication), is another factor in the inability to use a unified security solution for the IoT as a whole. Therefore, IoT requires modified and improved security measures that are applicable across all three layers of IoT; In the perception layer, in the network layer, and in the application layer. These measures should emerge from the ongoing and up-to-date understanding of the security vulnerabilities of IoT systems. These effective measures must achieve security, privacy and trust within the IoT, which has become an urgent and important requirements for successful adoption of the IoT and the deployment of its applications [18].

In this chapter, some solutions and countermeasures to confront attacks on IoT layers, mentioned in the previous chapter, prevent their occurrence and minimize their effects will be discussed. However, before we start talking about these countermeasures, it is worth noting that there are some documents and reports that have been written and submitted by some governments and organizations, which define the security standards that must be provided in IoT technology. These documents and reports are directed to the manufacturers and distributors of IoT products and in some cases to their users, so that

these standards, when taken into account, ensure an acceptable level of security for IoT users.

5.1. IoT Security Standards

Many IoT manufacturers and developers want to provide security in their products. However, they do not make considerable efforts and spend money to achieve that, even though consumers of IoT technologies are willing to pay additional amounts in exchange for security in the products they buy. From this standpoint, some countries have begun to develop regulations and standards that define IoT security. For example, in the United States, "reasonable security features" in IoT devices are now mandated by the states of California and Oregon. Also, the UK Government has created a code of practice that includes 13 recommendations aimed at ensuring customer privacy and protection.

These standards, despite their importance, still do not regulate the IoT market or force any company to do anything, as companies can continue to sell IoT devices in any inferior security method they want. However, it is hoped that in the near future providing security will become a legal and mandatory requirement for any company or manufacturers in the IoT space. There are many standards that have been set by many organizations. These standards define the security standards that must be provided (or recommended) in IoT products that manufacturers and consumers must follow to make IoT technology more secure. These orgnizations and their studies can be summarized as follows [86][87][88]:

- **The National Institute of Standards and Technology (NIST)**

The NIST released a document entitled "IoT Device Manufacturers' Foundational Cybersecurity Activities," which advises manufacturers of IoT devices on how to properly protect IoT devices. Six technologies that manufacturers may use to add protection features to IoT devices are recommended in this document. Four of them refer to how, before producing the unit, the manufacturer thinks about protection. To support the devices sold, the other two methods are planned. For example, the document advises manufacturers to identify potential customers and users, and to define expected use cases early in the design process to make decisions about which security tools to use and how to incorporate them. This document recommends that manufacturers should define

approaches for communicating with customers about device security risks. This step must be available as soon as the customer purchases a product, and this contact should be directly with the customer or through sales centers.

In addition, NIST has developed Federal Information Processing Standards (FIPS), that the United States Government applies to regulate information technology and computer security. These standards define requirements for cryptographic modules that all government technologies must comply with in order to protect valuable data.

- **The European Union Agency for Cybersecurity (ENISA)**

The European Union has made continuous efforts to improve information security as it published the Cyber Security Act on 27 June 2019 and put it into practice. In accordance with this law, the ENISA is given a permanent mandate, and the strengthening of its financial and human resources to achieve a common level of cybersecurity standards among the countries of the Union. Also, what is known as the European Union Cybersecurity Certificate has been established, ensuring that digital products and services (such as the IoT) follow this security standard.

The role of ENISA is mainly to provide expertise and advice as it issued a publication in November 2017 that includes "Fundamental Security Recommendations for the IoT in the Context of Critical Information Infrastructures", which contains three overarching topics for security measures:

- Technical measures: For example, the emphasis on using unique, hard-to-crack default passwords for every device
- Policies: For example, focus on integrating security by design into the IoT system rather than adding both at the end of development.
- Organizational, people, and process measures: For example, advice to manufacturers on how to make devices more secure as well as a recommendation on training employees in privacy and security practices.

- **US Federal Trade Commission (FTC)**

The US Federal Trade Commission is one of the main regulators in the United States that bears responsibility and accountability for the world of "things" and the extent of their impact on public safety. The FTC has provided several documents and reports in this regard that contain recommendations and instructions on how to deal with the issue of IoT security, and among these documents and reports:

- The Internet of Things: Privacy & Security in a Connected World (2015)
- What's the security shelf-life of IoT? (2015)
- What you need to know to secure your IoT devices (2016)
- FTC Charges D-Link Put Consumers' Privacy at Risk Due to the Inadequate Security of Its Computer Routers and Cameras (2017)

- **The European Telecommunications Standards Institute (ETSI)**

The ETSI TS 103 645 standard for the cybersecurity of consumer IoT products was published in February 2019 by ETSI which includes, for example, secure communications, regular software updates and minimization of exposed attack surfaces. This standard primarily governs the safety of Internet-connected electronic equipment and related utilities, including toys, baby monitors and items related to Internet safety, such as smoke alarms, other home appliances and wearable devices.

- **UK Government**

The UK government has published a proposed code of security practices in the IoT for the consumer. This code aims to improve the security of consumers' IoT products and associated services. This code contains 13 instructions, including:

- no default passwords
- ensure software integrity
- simple consumer deletion of personal data

After mentioning some security standards for the IoT, it is now necessary to present the countermeasures that must be taken to protect the IoT from cyber attacks and reduce their effects.

We presented this topic in two ways, both of which are concerned with how to make the IoT a stronger system against attacks that threaten it. In the first section, general countermeasures whose function is to protect the IoT system as a whole is discussed. The second section explains some of the potential defenses that could be adopted against each attack mentioned in the previous chapter.

5.2. The General Countermeasures

The mission of general countermeasures is to make the IoT environment generally safer because it has the potential to reduce the risk of threats and attacks to it. These countermeasures are implemented across the system as a whole and across all layers, from the perception layer through the network layer to the application layer. If only these general countermeasures are provided without resorting to the measures mentioned in the next section, then IoT security will be largely achieved.

The manufacturers, consumers and Internet service providers all share the responsibility for implementing these countermeasures so as to realize a suitable level of protection. Some of these countermeasures must be available during the production and manufacturing process as encryption technologies and others are used by Internet service provider such as the firewall, and others are entirely dependent on the consumer such as increasing the level of security sense.

General countermeasures include many security mechanisms and technologies that have specific functions, and these functions are as follows:

- **Prevention:** The goal of this function is to prevent attacks before they happen. This is done by deducing vulnerabilities that attackers might exploit and eliminating them.
- **Detection:** The need to implement this function means that the prevention function has failed. There must be security solutions designed to detect the attack and

identify the nodes that have been compromised and the data that has been tampered with. For example, the use of intrusion detection systems (IDS) is an effective method in this case.

- **Mitigation:** This function aims to mitigate the effects of attacks and minimize losses and consequences, which were detected by the second function. For example, to secure the network, security measures must be taken, such as excluding affected nodes in the network or disabling computer ports that were used during the attack.

It can be said that if these three functions are fully implemented, a strong security of the IoT system has been achieved. However, for IoT to be fully secure, these functions must be provided by the technologies available to defend against different types of attacks.

There are many security measures that can be adopted to overcome security problems in the IoT system and mitigate their effects. Most of these measures are still under study and development. So far, there are no standard steps to protect the security of the IoT, due to the evolving attacks and their attempt to overcome any measures taken against them. New countermeasures are evolved and improved every day to counter the attacks that target the IoT. It should be noted that the general countermeasures must be implemented simultaneously to protect against attacks. Some of the general countermeasures are listed below:

5.2.1. Risk Assessment

Risk assessment is an effective security process whose task is to identify, analyze, evaluate risks and the factors behind them. Manufacturers use the risk assessment process to provide a comprehensive product overview to identify things and situations that may create a risk or threat. This process is done by defining the product's working scenarios and the extent to which it meets the required standards. After that, the risk assessment process identifies the sources of risks that threaten the product and evaluates the likelihood and severity of these risks on the product and their impact on the applications and services it provides. Then, the manufacturer or consumer can decide what measures should be taken to prevent these risks or reduce their effects should they occur [22],[54],[73],[89].

Risk assessment is important to achieve a secure IoT and enhance the security plans as whole and it is considered the first step and the basic building block to achieve that. The importance of the risk assessment process is that it performs the following procedures:

- create awareness of risks
- identify products at risk
- determine the risks that may occur to the product
- determine appropriate countermeasures for each potential risk to the product
- deciding whether the current countermeasures are sufficient or more should be done

These procedures are performed at certain times to give the best result, and among these times:

- before a new product is launched to the market
- when making changes or developments to an existing active product
- when new hazards arise, the product may be exposed to them

5.2.2. Safeguard Physical Infrastructures

IoT systems are spread in different places, some of which can be easily reached such as buildings, and some are not easily accessible, such as roads outside cities. The protection of buildings containing IoT systems, with all their devices, networks, antennas and others they contain, is a basic security countermeasure. This countermeasure protects these systems from unauthorized access, tampering, and intentional and unintentional physical destruction. For example, the use of alarms, locked doors, fences, guards and cameras against unauthorized access is an important step in achieving this [22],[70].

Care must also be taken when designing and manufacturing the node itself so that it must be well designed and made of the highest quality materials. This will give the node the ability to resist threats. In other words, the design must meet requirements such as stability and tamper resistance. For example, the design of the node includes the design of the

antenna, the design of the internal components of the node and its external structure. This can be a huge challenge for manufacturers whose biggest goal is to manufacture affordable smart devices, because the more quality the materials they use, the higher the price of the device [80].

On the other hand, nodes must be hidden in strategic or hard-to-reach locations which also helps protect them from being attacked. In addition, monitoring and guarding these contracts, if possible, is an important countermeasure that effectively protects them from violations [4], [22].

5.2.3. Authentication

Traditional authentication techniques cannot be applied to an IoT environment due to the resource-limited nature of its devices. This is because traditional authentication systems are designed for devices with sufficient resources such as power and high processing capabilities. This led to the emergence of what are known as lightweight authentication systems. In IoT, if a device wants to interact with another device or access the network, it must first and foremost identify itself and prove its identity. In the same way, if a user wants to request a service or access an application, he must first prove his identity and eligibility to obtain that service or access this application. This process is known as authentication. The authentication in IoT can be defined as the process of determining which users and devices are authorized to access IoT system and benefit from the services it provides and the data stored therein.

The availability of a technology performing the authentication process is a very important countermeasure as it protects the IoT system from being violated by unauthorized nodes or illegal people. This countermeasure prevents unauthorized access to IoT nodes and networks that could result in information theft and system disruption.

There are two types of authentication in IoT environment: device-based and user-based:

5.2.3.1. Device-Based Authentication

This type of authentication is performed by devices without interference from operators or users. The IoT relies on device-based authentication in the perception layer and network

layer because most of its devices rely on themselves to perform their functions without user intervention. In other words, the IoT depends to a large extent on M2M communication.

To ensure security and privacy, any node that wants to interact with each other over the same network or over the Internet with the goal of exchanging data must first verify each other's identities. This type of authentication is required to ensure that the devices that want to connect to the IoT are authorized and trusted devices.

Device based authentication relies on the use of some techniques to verify the identity of the parties. One of these technologies is by distribution a shared secret key between the parties before they begin to interact with one another. If a party receives a request to exchange information, it can verify the identity of the sender via the request message. If the request message contains the correct shared secret key, the recipient verifies the identity of the sender and agrees to interact with him. The second authentication technique is digital signature. This technique is based on asymmetric cryptographic schema. In digital signature method, the sender sends a signed request using its private key. If the recipient is able to open the request message using the sender's public key, this is proof of its identity.

Therefore, it is important that the nodes include techniques that enable them to authenticate themselves with other nodes. For example, RFID readers and tags must authenticate one another in order to be considered a reliable source of information. The use of authentication techniques is an important countermeasure to many attacks that focus on counterfeiting and identity theft such as cloning attack and DoS attack [22],[59],[73],[80].

Different authentication protocols have been proposed, researched, and evaluated in the literature. These protocols take care of and regulate the ways in which secret keys are generated, managed, and distributed between the parties. These protocols are adopted based on the resources available in the nodes. If a node has enough resources, it can use a rather complex protocol for authentication; if its resources are limited, it uses a simple authentication protocol. However, most of these protocols are based on the fact that a

secret number is exchanged between the nodes before any conversation begins between them in order to verify their identity. There are several protocols proposed that can be used for authentication in the IoT environment. These protocols cannot be enumerated or all talked about in this thesis, so only some examples are provided as an illustration. For instance, authors in [90] proposed some Lightweight Authentication Protocols for Low-Cost RFID Tags. In addition, the references [91],[92],[93],[94] provide detailed information on the different authentication protocols that have been proposed for use by RFID systems.

5.2.3.2. User-Based Authentication

User-based authentication focuses on the user rather than the device which is important in the IoT environment to prevent any attackers from impersonating legitimate users. Users who want to access or request data from any device in the IoT must be approved, it must be a legitimate customer. In other words, when the user wants to use the applications and services provided by the IoT, he must first prove his identity to the system by authentication process.

Usually, authentication is done by a node that acts as an intermediary between the user and the terminal nodes and this node is called the gateway node. When a user wants to access a sensor node, for example, his request is directed first to the gateway node, which checks the identity of the user first. Then the gateway node sends the user's request to the sensor node along with proof of his identity.

There are many authentication models used for user authentication. One of these forms is simply based on a password and a username. There is also a two-factor user authentication technique which typically combines a password with a second layer of protection. This technology consists of two stages, (1) the registration stage, and (2) the authentication stage. In the registration step, the user registers his credential information in the gateway node. As for the authentication stage itself, it is divided into login and verification. In the login stage, the user enters his credential information, then the authentication step verifies their validity [95].

Biometric authentication (such as face or fingerprint) can also be used to verify a user's identity. This method of authentication is considered more secure than the previous method, as it is difficult for fraud to occur. Biometric authentication is a logical and critical method for identifying an individual. As is known, there is a possibility that the enemy will reveal someone's password, but he cannot in any way impersonate him using his fingerprint, for example. The latest mobile phones from Apple and Samsung, as well as many new desktop and laptop computers, have built-in biometric sensors. Therefore, it is expected that this method of authentication will spread widely in the IoT environment.

5.2.4. Data Encryption

The IoT produces massive amounts of data about things, the physical environment, and most importantly, people. In order to obtain effective and efficient services from the IoT, this data must be exchanged between IoT components. Here comes the importance of protecting data exchanged over the IoT, which is the biggest factor affecting the future of this technology [21]. Therefore, device manufacturers should produce devices that support data encryption technologies to better protect sensitive users' data. This is because data encryption prevents disclosure of this data to anyone who has no right to see it.

The primary goal of encryption is to secure information and maintain its privacy so that only the intended sender and receiver can read the information and understand it. This protects the data from any tampering or eavesdropping by any hacker intercepting or stealing it. The data encryption process must be applied to the data present or stored in the node or the data that is transferring in the network between the nodes

IoT smart system have resource limitations and low-resource devices in terms of low computing power, limited battery life, small size, small memory, and low bandwidth. In addition, these devices are heterogeneous devices that are manufactured by different companies with different security standards. Consequently, traditional cryptographic algorithms requiring complex mathematical operations are not well suited for an IoT scenario that contains devices with such characteristics. The traditional encryption algorithm will work very well with computers, servers and some mobile devices. However, it does not work in devices such as RFID tags, sensors, and the embedded

system effectively. For all of the reasons mentioned above, it was necessary to develop a new encryption technology that would act as a countermeasure against illegal disclosure of data. This technology must be compatible with IoT resource features so, that using it does not deplete IoT resources. These devices require lightweight cryptography platforms. The requirements of these lightweight encryption techniques are smaller size (key and data block), lower power consumption, simpler computation operations, and faster processing (throughput, delay).

The cryptography used in the IoT can be divided into two types, symmetric key and asymmetric key cryptographies. In symmetric key cryptography, the same secret key is used for encryption by the sender and decryption by the recipient. In this type, the secret distribution of the cryptographic key between the parties to the communication is a matter that needs to be taken into consideration. This type of cryptography is considered lightweight, because the calculations in it are not very complicated. On the other hand, in asymmetric encryption, a secret key is used for encryption called the public key and another key for decryption called the private key. Thus, it appears that this type of encryption uses two mismatched keys in the cryptographic process, which eliminates the need to distribute secret keys before the information transfer process. The sender encrypts the data it wants to send to a specific recipient using the public key of that recipient, which in turn decrypts the data sent to it using its private key. The private key is produced from the public key through a complex mathematical process. It is complex enough that it becomes very difficult to guess the private key when knowing the public key. This type of cryptography is much more complex than the symmetric type because it relies on complex mathematical operations, both in private key production, encryption or decryption.

Many encryption techniques have been proposed and used in IoT environment, but this field continues to evolve every day. Table 5.1 shows some lightweight encryption algorithms used by IoT systems [96],[97]. The references [96],[97],[98] provide more information about lightweight encryption algorithms used by IoT system.

Table 5.1 Some Lightweight Encryption Algorithms used by IoT System

Symmetric Lightweight Algorithm	Asymmetric Lightweight Algorithms
Advanced Encryption Standard (AES)	Rivest–Shamir–Adleman (RSA)
TWINE	
HIGh Security and LightweigHT (HIGHT)	
PRESENT	

5.2.5. Key Management

Establishing an end-to-end secure channel between remote entities is one of the biggest challenges facing the IoT. To create such a channel, it is necessary to provide key management mechanisms that allow two devices to negotiate and choose specific security credentials (secret keys). These secret keys are used to ensure the secure flow of information between the communication parties. This mechanism deals with generating, exchanging, storing, using and replacing keys as needed.

Key management is the core of security, and it is an important way to ensure data confidentiality in the IoT. This is because the success of other security technologies, such as encryption and authentication, depends on how securely the keys are distributed between the communication parties. These secret keys are used by communication parties to authenticate each other and to encrypt the data before transmit it to each other. So, if an intruder can obtain those keys, the data will not be secure and the network will also be vulnerable to violate.

Typically, IoT nodes are restricted devices with limited computing power, and the key management mechanisms used to negotiate a session key with other entities may be too heavy for them. Therefore, it is important to choose a management mechanism appropriate for the resources of these nodes.

A key management mechanism is needed when a node wants to connect to the Internet or when a node wants to connect to another neighboring node. In the first case there will be an intermediary between the node and the Internet, such as Access Point (AP). Typically,

this AP has enough resources to create keys that IoT nodes use to authenticate or encrypt data. So, when a node wants to communicate with its neighbor, it can use pre-shared key approaches.

Eschenauer and Gligor proposed in [99] a random key pre-distribution scheme. In this method, contiguous nodes in the same local network receive a random subset of keys from a large key pool. When any two nodes want to communicate between them, they choose a single shared key from their subset and use this key as a shared secret key between them.

There are several proposed key management mechanisms that depend on available resources. The references [100],[101] provide information on some of the mechanisms that may be adopted to perform the key management function.

5.2.6. Error Control Techniques

Data integrity in the IoT system is a priority and a type of security due to the impacts and risks resulting from the arrival of wrong data on the system's performance. Therefore, it has become important to design a mechanism for error detection and correction in wireless sensor networks. Data alteration can occur when it travels through the system, intentionally or unintentionally. Among the reasons that lead to an unintended error that affects the integrity of the information:

- Signal Strength
- The Distance between the Transmitter and the Receiver
- Signal to Noise Ratio (SNR)

There are several methods used to detect data errors. These methods take into account the limited resources of the techniques used in the perception layer. RFID and WSN use error detection and correction schemes to detect errors that may be caused by noise or other defects during transmission from transmitter to receiver and to reconstruct the original data free of these errors. These schemes add some redundancy (i.e, some additional data) to the message, which recipients can use to verify the integrity of the delivered message, and recover the original data if anything goes wrong. Error detection is most commonly achieved by using a suitable hash function such as parity bit, checksum, CRC, or

cryptographic hash function. The hash function adds a fixed-length tag to the message, which enables recipients to verify the delivered message by recalculating the tag and comparing it to the tag provided.

Moreover, among the methods that WSN uses to recover defective packets are: Automatic Repeat Request (ARQ) and Forward Error Correction (FEC). ARQ is an error-control method for transmitting data that uses acknowledgments and timeout to achieve reliable data transmission over an untrusted communication channel. If the sender does not receive an acknowledgment before the time-out expires, it usually retransmits the packet until the sender receives an acknowledgment or exceeds a predetermined number of retransmissions. The simplest form of the FEC is that the sender sends each character twice as redundant data. The receiver checks each letter to make sure it was transmitted correctly. If compatibility occurs in either case, the letter is accepted. If in either case the compatibility does not occur, the character is rejected. FEC provides the receiver with the ability to correct errors without sending a request to resend the data on the communication channel [102].

In RFID, CRC is used. However, this technique is an error detection technology, but it is not for correcting errors when errors are discovered. So, the whole package is re-sent in case of an error. Unfortunately, this technique takes time to confirm that the data has gone wrong, so it makes the RFID system very ineffective due to the time delay [103]. In [103], the researchers proposed a technique known as the split periodic repeat assay. It is a simple, efficient and reliable algorithm used by an RFID reader to quickly read tag memory for the purpose of error detection and correction. In this algorithm, the required data is split into multiple segments with a predefined segment length. After that, each part is checked separately with CRC technology to see if there is an error. If there is an error in this segment, then only re-transmission of that segment is required, not all data. This technology reduces connection cost and increases network efficiency.

5.2.7. Data Integrity

Data integrity is an extension of Section 5.2.6 that talks about error control techniques as they can be viewed as two sides of the same coin. Data manipulation in the IoT may lead

to system malfunctions, incorrect decisions and incorrect actions. This, in turn, could lead to dangerous repercussions such as economic loss, infrastructure damage and human injuries.

Ensuring data integrity is critical in the IoT. It means making sure that the data is complete, original, accurate and not tampered with or altered, thus making this data more reliable. There are two common things that can affect data integrity. The first is an attack that aims to tamper with the data stored in a node or when it travels over the network. Second, the data-loaded signal is subject to interference or noise, for example, from close equipment or unfavorable radio channel conditions.

Data must be protected at all stages of its lifecycle, when it is in transit or at rest. Otherwise, there is no assurance that the integrity of current data is maintained [104].

Data-in-motion requires that data be protected from modification while on its journey from sender to destination. In this case, data integrity can be verified using several techniques, which depend on their compatibility with node resources. One of these techniques is the Message Authentication Code (MAC) which is calculated with each packet. MAC is a short piece of information used to authenticate a message and to ensure that this message came from the specified sender and has not been tampered with. The transmitter enters messages to the MAC algorithm using the shared secret key to produce the MAC data tag. Then the message and MAC tag are sent to the receiver. The receiver, in turn, enters the received message through the same MAC algorithm using the same key, which results in a second MAC data tag. Then the receiver compares the MAC tag received from the transmitter with the MAC tag it calculated. If they are identical, the recipient can assume that the message has not been altered or tampered with during transmission [105].

It takes time to create a MAC for each data packet, as it is based on performing calculations in both the sender and the receiver. This may result in delayed response and decisions making. However, using this method in IoT devices that do not handle a large data flow, for example, devices that send data at low rates, such as 1 packet per second or less, may be a solution to the problem of ensuring data integrity. On the other hand, due

to the resource-limited nature of the IoT nodes, computing and sending MAC with each packet may be impractical for high data rate IoT systems. This is because calculating the MAC tag for each packet sent or received, and the comparison process between them is too burdensome for limited-power nodes.

Another method that can be used to verify data integrity is to use Public Key Infrastructure (PKI). In PKI, the sender of the data digitally signs the sent message using his private key. So, the message can only be opened using the sender's public key, and thus the receiver guarantees that the data is in fact sent from a reliable source. However, this method has its drawbacks as well. This is due to the fact that this method is computationally complex for many IoT devices. The reference [105] suggested using the Hash Message Authentication Code (HMAC) with Secure Hash Algorithm (SHA) 256 to ensure data integrity in the smart home system.

In the event that data has been tampered with when sending data from the sender to the receiver, the recipient requests that the data be resent as mentioned in Section 5.2.6.

Encrypting stored data, verifying the identity of everyone or anything that wants to enter the node, and defining their privileges are all important factors to prevent any attempt to unauthorized tamper with and modify data.

5.2.8. Firewall

It is a robust network security technology that creates a barrier between a reliable internal network and an unreliable external network, such as the Internet, and monitors the ports that connect them. The firewall can be a software. This software can be located on the endpoints. Also, the firewall can be a hardware device in itself (such as a router) [21],[22]. In this case, the router performs two functions together: directing the data traffic in and out of the associated network and also protecting the network from unauthorized data entry and exit.

The main function of the firewall is packet filtering. It scans every incoming and outgoing packet of data based on predefined security rules and determines whether to pass or reject this data packet [106].

The firewall predetermines the IP addresses allowed to send or receive data (source and destination IP address), and it also defines which applications are allowed to do so (source and destination ports). When data is transferred to or from the network, the firewall checks the IP address and port numbers before deciding whether or not that data is allowed in. This type of firewall is known as a traditional firewall and it is the first line of defense in cybersecurity. However, it does have a weakness. Traditional firewalls only scan IP addresses and ports, but they don't deeply investigate packets entering the network. Thus, any attacker who was able to obtain information about the addresses allowed to access can simply attack the network.

Some devices have been developed based on the idea of a traditional firewall but they perform more in-depth checks on the data that travels through them. These devices are known as Unified Threat Management (UTM). UTM is a security device that performs the same functions as a traditional firewall in addition to having other features such as Intrusion Prevention System (IPS), Virtual Private Network (VPN), anti-spam, anti-virus and URL filtering.

5.2.9. Intrusion Detection System (IDS)

If the firewalls are security guards, intrusion detection systems are security cameras. IDS is a traffic data monitoring tool that works mainly in the network layer of an IoT system. It is used to identify intrusive data and prevent it from threatening the confidentiality, integrity, and availability of the information system [50],[55].

IDS provides uninterrupted monitoring network traffic. Then, it uses this monitoring process to detect any suspicious activity in the network, which sometimes indicates that the network is under attack and then alerts the system about this activity. Where the IDS captures a copy of the traffic in an information system and then analyzes that copy to detect potentially harmful activities [50],[55].

So, it can be said that IDS operations are divided into three stages. The first stage is the monitoring stage, that its function is to monitor the traffic of information in the network to look for signs of known attacks or deviations from normal activity. The second stage is

the analysis stage, which is based on comparing the information with the usual data pattern stored in the IDS database. And finally, the detection stage is responsible for detecting intrusion or misuse.

There are several types of IDS that use different intrusion detection techniques. One of them is a **Signature-based Intrusion Detection System (SIDS)** which uses a database of known signatures and patterns of malicious codes and intrusions to detect well-known attacks. The other technique is a **Anomaly-based Intrusion Detection System (AIDS).** In this technique, a normal data pattern is created based on data from regular users, and then it is compared with the current data patterns circulating over the the network to discover anomalies. Such anomalies arise accidentally, for example due to noise, or deliberately through hacking tools [50].

IDS used in information systems relies on specific types of algorithms that aid in monitoring, comparison, and discovery. These functions require the availability of resources such as storage capacity and processing capability. Therefore, due to the limited computing and storage capabilities of IoT devices and the specific protocols used, traditional IDS systems may not be an appropriate option for IoT environments. Therefore, many IDS systems and lightweight algorithms are designed to be compatible with IoT based smart environments. For example, Principal Component Analysis (PCA) is one of the lightweight algorithms that can be used for various detection techniques in intrusion detection systems. In addition, Liu et al. in [107] proposed an Artificial Immune System (AIS) based IDS for IoT environment. This system mimics the human immune system, which protects the body from various harmful, disease-causing infections, such as bacteria, viruses, and parasites. It does so largely without prior knowledge of the structure of these harmful creatures. This suggested system attempts to figure out the unknown vulnerabilities and take advantage of them to build up an adaptive system that instantly organizes itself as these vulnerabilities eventually arise. AIS is a robust, adaptive, self-organizing information processing system that has the advantage of self-learning for new attacks. For more information, [50] reviews many of the lightweight algorithms it uses as well as several proposed IDS systems.

IDS technology can be placed in various ways in the IoT: in a distributed manner, in a centralized manner, or in a mixed manner. In the distributed method, IDS is placed in every IoT node but the IDS in this case must be lightweight due to the restricted resources in the IoT nodes. Distributed IDS monitors node power consumption to detect intrusions. By focusing only on monitoring single-node parameters, the resource consumption of the computations needed to detect intrusion is minimal [108]. In centralized IDS placement, IDS is placed in the border router. All data collected by the IoT nodes is transferred to the Internet via the border router along with the requests that the Internet clients send to the IoT nodes. So, IDS placed in border router can analyze all traffic exchanged between IoT nodes and Internet. But in this type, the traffic between nodes in the same network cannot be monitored by IDS. Hybrid IDS combines central and distributed placement concepts to capitalize on their strengths and avoid their drawbacks. In this type, the network is organized into groups or regions, and only the master node hosts IDS. However, this node must contain the most available resource in the group of nodes it represents. After that, the responsibility for monitoring other nodes in the group rests with this node [108].

5.2.10. Routing Security

Routing information is the information that network devices (routers) use to determine the path through which packets can travel from source to destination. This information is stored in the router inside a table called the routing table. When a device sends a data packet to another device, it attaches the destination address to the packet to determine its destination. If the destination address is in the same network, the local switch will perform the routing task using its own table. In case the destination address is outside the local network, the router uses this address to determine which path this packet should take to reach its destination with the help of its routing table.

In the case of using router, the packet path can be determined either on an end-to-end or hop-by-hop basis. End-to-end means that the path of a packet from its source until it reaches its destination is well known and defined. For the hop-by-hop base, the packet path is known to the next hop only and then the path is specified for the next hop and so

on until the packet reaches its destination. When data packets are intercepted, an attacker can see the routing information contained in them that he can exploit to carry out a variety of attacks.

The use of encryption mechanisms is the first line of defense to ensure that routing information is protected because they prevent attackers who intend to disclose this information from achieving their goal. In addition, the use of secure routing protocols is important as a means of protecting against attacks occurring within the network by compromised nodes.

After much research has been done, various secure routing protocols that can be used in IoT to ensure secure data routing have been proposed. These protocols ensure that the information path is not exposed or tampered with by attackers for the purpose of carrying out attacks such as wormhole attacks.

The Secure Multi-hop Routing Protocol (SMRP) and Two-way acknowledgment-based trust (2-ACKT) are examples of these protocols. SMRP allows IoT devices to communicate in a secure manner by ensuring that IoT devices are authenticated while joining or creating a network. In this protocol, the path formation and authentication process takes place simultaneously, providing a secure IoT connection. This happens based on recorded information such as the owner of the IoT devices, the network address, and the Media Access Control (MAC) address of each device. As for 2-ACKT, it is based on a dual acknowledgment system in developing trust among neighboring nodes. With 2-ACKT, the sender can confirm that the neighboring node has successfully received the packet and that this node has forwarded the packet to the destination faithfully by following the routing protocol. In doing so, they make sure that nodes are not compromised and that they do not pose a threat to the network. The references [109],[110] give more information about secure routing protocol for IoT.

5.2.11. Security Awareness

Notably, a large number of users do not take the process of changing default passwords for IoT products seriously. It is also common for people to frequently disclose their

personal information and whereabouts to the general public online through social media such as Facebook and Twitter.

Security awareness is a important non-technical countermeasure related to information security. It is about raising awareness of the seriousness of the risks and security threats that IoT users are exposed to. In addition, knowledge of the steps and measures by which to prevent the occurrence of these risks or limit their effects should be the focus of attention of IoT users and their priorities.

IoT users should increase their sense of security and know how to use IoT services correctly. In addition, education on handling and managing sensitive data such as password management, physical security management, and resource management should be of interest to users. Also, users should ensure that they install, use and periodically update the tools that detect threats targeting IoT devices.

IoT users should not hesitate to seek the help of experts and companies specialized in the field of information security to help them in configure their devices to be more resistant to threats. Users can also seek the help of some companies that provide services such as attack detection, disposal services, or periodic monitoring of IoT products to ensure that they are not exposed to any threat.

5.2.12. Access Control Mechanisms

In a typical IoT system, a node provides the resources it owns such as data, services, storage units, computing units, etc., to others that need these resources. However, there is a possibility that adversaries could snoop on IoT systems, to gain illegal access to these provided resources. Therefore, finding a way to protect resources from unauthorized use and control access to them is becoming an increasingly important issue in the IoT. Thus, access control must be implemented in IoT system to prevent and deny unauthorized request, access or use of the resources [111].

An access control mechanism can be defined as a set of rules and permissions related to an object that are implemented to control requests to access the resources of that object. Also, these rules specify the operations allowed on those resources. That means who or

what can access to the resource and what can he do to it (read, write, execute, delete, etc.) [21],[22].

Nowadays, there are many access-control models that are applied to various IoT scenarios to provide more security. Here, the most popular models will be covered with a brief summary of each:

- **Mandatory Access Control (MAC) Model:** In this model, only the system administrator is allowed to grant permission to access the resource and the subjects of that access. Only an administrator can modify these permissions. MAC model's usage is usually limited to military applications [112].
- **Discretionary Access Control (DAC) Model:** In this model, the users who own the resources determine and grant permissions to access their resources to whomever they want by including them in Access Control Lists (ACLs). Permissions are usually stored within resources. Unlike MAC, where the administrator grants permissions, in the DAC the permissions are granted by the users who decide the rights to access the resources to which they belong [112].
- **Role-Based Access Control (RBAC) Model:** As the name suggests, this model manages resource access based on a hierarchy of permissions and rights assigned to specific roles. In this model, multiple users are grouped into roles (e.g., administer and guest) that need access to the same resources and then the security policies grant rights to roles rather than to users [111].
- **Attribute-Based Access Control (ABAC) Model:** In this model, access control is not assigned solely based on identity and roles. ABAC is evaluated against a set of attributes that define user, resource, procedure and environment. It enables administrators to choose the best combination of a range of variables to build a robust and comprehensive set of access rules and policies [111],[112].
- **Capability-Based Access Control (CapBAC) Model:** In the model, access rights are granted to subjects (entities want to access a resource) based on the concept of capability. The capability is a token, ticket, or key that gives its possessor

permission to access an entity or object in a system. Each token indicates the objects and resources that its owner can access and the privileges granted to him for each object and resource [113]. Any request submitted with the correct token gives its owner the ability to interact with the object indicated in the token in accordance with the specified access rights. In other words, when a subject wants to access a specific resource for an object, it sends the token along with the request. The object that receives the token depends on the permissions that this token contains when processing this request [112].

It should also be noted that access control is implemented through two approaches: the centralized approach and the distributed approach.

- **Centralized Approach:** In a centralized approach, a central entity is responsible for filtering and managing access requests based on their authorization policies. In this approach, IoT end devices play only a limited role as information providers. This central approach does not take into account resource limitations, because the access control logic is located in a central entity that does not suffer from these limitations. MAC, DAC, RBAC, and ABAC models use a centralized approach for access control. However, this approach has serious problems, as it does not take into account the end devices when determining and making access control decisions. Also, the access control mechanism is implemented by a single entity, so any vulnerability that this entity suffers from could breach the entire system. Moreover, this entity can be considered a single point of failure, because if that entity ceases to function, the access control mechanism will not be able to do its job [112]. Furthermore, achieving end-to-end security using a centralized architecture on a distributed system such as the IoT can be challenging. Because the centralized approach does not meet the requirements of IoT scenarios, which demand flexibility, scalability, and ease of use in environments containing billions of devices.
- **Distributed Approach:** This approach may provide the solution to problems in the centralized policy and is more suited to IoT scenarios and architectures [112].

In this approach, the end device is a smart thing that can be totally relied upon in making access control decisions without having to delegate this process to central entities. CapBAC model use the distributed approach for access control. However, although this approach is best suited to the IoT environment, it is affected by the low resources of IoT devices, making them easily vulnerable to penetration. As a result, access control decisions made based on this approach cannot be fully trusted, especially in insecure IoT environments [111].

5.2.13. Data Backup and Recovery Mechanisms

Backup and restore mechanisms are another type of countermeasure that can be taken to ensure that data is not lost, whether by deleting or replacing it in an intended or unintended manner. This would increase the user's confidence in the efficiency of the IoT in dealing with potential risks [21].

Backup data can be stored locally, for example, in hard disks or it can be stored in the cloud. So, if the data is protected locally, it should be saved in a fireproof safe and in safe and guarded places, whether with guards or cameras, depending on the importance of the stored information. The stored information must be encrypted in order to add another level of security to it. In the case of storing the information in the cloud, the cloud service providers must be responsible for data protection in accordance with a contract signed between them and the consumer.

It is also important to make sure that the backup process is done frequently and on schedule to ensure that no important information is lost.

5.2.14. Anti-Malware

In general, malware can be defined as any program designed to intentionally inflict damage on a device or network. Malware is the most dangerous threat to IoT devices, which can destroy data or disrupt devices. The most common malware, as mentioned in Chapter 4 are: Rootkits, Ransomware, Bots, Financial Malware, Logic Bombs, Virus, Worms and Trojans [84].

To protect the IoT system from these malicious programs, which have become increasingly prevalent in recent years, the need to use effective detection and protection methods such as Anti-malware has increase. These Anti-Malware software is installed in the devices that the user use to interact with IoT application such as personal computers, tabs, laptops and smart phones.

The use of anti-malware software is essential for the confidentiality, reliability and integrity of the IoT system because it does an important job to identify and get rid of all kinds of malicious codes [22],[114]. The malware detection methods used today are divided into two categories:

- **Static Detection:** Static detection method is performed by analyzing the malicious codes and its characteristic as well as extract its features without executing it on a device. This method is most suitable for the IoT due to its light weight, less resource consumption and less time as it does not involve the execution of the malicious code in order to identify it [115]. One method that falls under this category is Signature-Based Detection. Signature-Based Detection is the most popular method and relies on detecting the presence of malware according to its signature. Signature means the usual effect or pattern associated with a malicious program. This method relies on the existence of a prior repository of malware signatures in order to compare any program against it. This repository should be updated frequently as new threats are detected [84]. The disadvantages of this detection method are, first, the malware must first be analyzed for its pattern. Second, only malware in its repository can be detected, and malware that is not present cannot be detected. Therefore, it is important to update this detection method frequently to add signature of the new malware to its database. Third, it is not suitable for devices with insufficient memory like most IoT devices. Heuristic detection is another method for static detection of malware. This method searches for commands and instructions whose presence in a program or application is considered unnatural or logical - instead of searching for a specific, well-known signature.

- **Dynamic Detection:** This method analyzes malware by executing the suspected program, then studying its behavior and intentions, and on the basis of this study, this program is classified as malicious or reliable. Dynamic detection monitors the suspected program during runtime to detect abnormal behaviors such as network behavior, power consumption, CPU load, virtual memory, etc. Suspicious programs are usually tested, run, and monitored in a virtual environment, so they don't affect the actual system. However, this method, despite its ability to detect malware at run-time, is considered unsuitable for the IoT environment because monitoring implementation processes requires many resources [84],[115].

The references [84],[116] provide more information about the malicious detection methods.

5.3. Defense against Attacks

In the previous chapter, a collection of attacks against the IoT environment was introduced. These attacks have been broken down based on the layers that make up the IoT architecture. In this section, some defend measures that can be taken or used to prevent these attacks or to limit their effects on the functioning of each layer will be identified. These defensive measures, if provided, can work side by side with general countermeasures to create a highly reliable and secure IoT system.

The defensive measures mentioned in this section are not all that can be done to defend against these attacks, but rather are examples of what can be used. There is always new research to improve IoT security against attacks. The need for this continuous research is due to two reasons. The first is the continuous development of technology, which allows finding more successful solutions. Second, the attackers continually attempt to develop attacks, rendering ancient defenses ineffective.

5.3.1. Defenses against Attacks on the Perception Layer

Perception layer security issues include information acquisition security issues, and physical security issues of devices such as sensors and RFID nodes. In addition, the

security of the information exchanged between an RFID reader and an RFID tag falls under this heading.

There are several factors that affect the security of the IoT perception layer. First, most of the nodes are spread in places that are difficult to monitor and protect, either because of the nature of the place itself or the large number of these nodes. Second, the majority of this nodes is manufactured at the lowest possible cost, which affects its security quality. Finally, most IoT devices use wireless networks to communicate and transmit data. Due to all the aforementioned reasons, the attacker can easily steal, change or destroy the data stored in the smart device or intercept it while it is being transmitted [59].

In general, it can be said that the security requirements that are an absolute necessity for this layer are lightweight encryption technology, node authentication, physical protection, and key management [3],[55]. There are many security measures that can be adopted to overcome security attacks in the perception layer and mitigate their effects. Most of these measures are still under study and development. Here are some of the defensive measures against the attacks mentioned in the previous chapter regarding this layer:

5.3.1.1. Defend against Tampering Attack

A tamper attack might aim to damage the device or reprogram it with a malicious system capable of carrying out attacks from inside the IoT system. Safeguard physical infrastructure is important defense against this attack.

To be able to carry out this attack, the attacker would need unattended access to the system for a period of time. This often requires removing nodes from the deployment area and moving them to the laboratory or bringing equipment to the nodes, this, of course, causes the node to stop working in both cases.

Given that regular communication with neighboring nodes is part of normal network operation in WSN, the constant absence of a node is an unusual condition and can be noticed by its neighbors. This enables the system to detect and respond to a tamper attack in real time.

A tamper attack requires physical contact with the node and this can be done via a Joint Test Action Group (JTAG) interface. The JTAG interface is a special interface that provides a way to communicate directly with the chips on the product board. It is used by electronics engineers to assist them in testing, debugging and programming node components during the development stage. Therefore, it is necessary to disable access to the microcontroller's internals via JTAG before launching the final product. If JTAG access is left enabled, an attacker equipped with an appropriate adapter cable and a portable computer is capable of taking complete control over the node. Another defensive measure that can protect a node from tampering even after it is stolen is to protect the bootloader with a password. A bootloader is a small code and its goal is to bring the system to a state in which it can perform its main function and to download the fireware. It offers the ability to update or modify the systems' firmware (to fix bugs, or just to update with new features) [117].

If the purpose of the physical attack on the node is to steal the sensitive information stored in it, then it is recommended to store the least amount of information in it. It is also possible to delete the key used for encryption after it has been used for certain times and to use a new key using pre-distribution technology. Also, storing information in an encrypted manner represents another level of security and makes it difficult for an attacker, who aims to extract the information, to achieve his goal.

5.3.1.2. Defend against Node Capture Attack

The first step that can be taken to protect nodes from this attack is to make it difficult to physically access them. This is done by applying the same procedures mentioned in section 5.2.2. If the attacker can somehow access the node, it will be difficult to extract the information stored in it and copy them if this information is encrypted. Therefore, encrypting the information is important to prevent this attack.

If the attacker can launch this attack and propagate the cloned nodes in the network, then techniques must be in place to detect the presence of these cloned nodes. This reduces the impact that the IoT can suffer. Once detected, these nodes can be isolated and prevented

from harming the network. Many types of detection schemes are proposed for detecting cloned nodes. All of them are categorized based on Centralized or Distributed approaches.

- **Centralized Approaches:** In the central approach, the base station is primarily responsible for monitoring all nodes. One of the detection schemes proposed in this approach is the use of random key pre-distribution. This node replication detection technique is proposed by Brooks et al. in [118]. The nodes use this pre-distributed key to communicate with each other. The base station calculates the total number of usages of a given key. This number reveals if multiple nodes are using the same key for communication because they are clones of each other.
- **Distributed Approaches:** In distributed technologies, there is no central authority to monitor. But the information is sent to a randomly selected node called the witness node. An example of this approach is Random Multicast (RM). RM technique is proposed by Parno et al in [119]. In this technique, when a node broadcasts its location, all neighboring nodes respond by sending a signed copy of their sites. If a node detects that there is more than one node with the same definition, but is present in more than one place at the same time, it will give a warning that something is wrong and that this node may be cloned. The node that triggers the alarm is called the witness node.

The references [119],[120] present more information about the other detecting schemas.

5.3.1.3. Defend against Unauthorized Reading of RFID Tag

One of the most important ways to prevent this attack is to lock the tag so that the attacker cannot access to read it. There are several ways to make the tag locked and among these methods [69],[121]:

- **The Kill Command Method:** is a straightforward way to make the tag not work. The reader sends the kill command to the tag after reading it to lock the tag. When the tag receives the "kill" command, its status changes to inactive. This command is tasked with restricting the use of the tag by removing its identity. When using this method, the tag cannot function again, as it is permanently suspended from

work. This often happens with goods purchased at checkout employee. As a result, goods or products no longer contains any active RFID tags, so consumer privacy is now protected.

- **The Sleeping Command Method:** In this method, the reader sends a "sleep" command to the tag, and the tag will be temporarily inactive. The sleeping tag can be then awakened by receiving a PIN code from the reader. Another method used to unlock or wake the tag is the secret handshake. The user unlocks the RFID tag using the secret handshake by moving or shaking the tag (or its container) in a specific pattern.

Blocker tag is another way to prevent unauthorized reading of tags. Blocker tag is a device that controls the tag reading process by broadcasting radio signals to prevent or allow nearby RFID readers to read the tag. The blocker tag adds a bit of privacy to the tag. While in store, the tag privacy bit is usually set to 0, indicating that all customers can access the tag identification. In this case, the blocker tag allows for unrestricted reading of the tag. During checkout, this privacy bit changes to 1, indicating that access to this tag is now restricted to one customer. In this case, the blocker tag knows that the tag has become private and restricts access to it [69],[121].

Encryption technologies, authentication protocols, or access control mechanism may provide an alternative solution. However, these techniques should be lightweight due to the limited resources of the tag. A Faraday cage can also be used as a solution. It is a cover made of a material that takes the form of a metal plate or an opaque mesh. Its mission is to isolate the tag on any radio waves and thus inaccessible to it. Today consumers can purchase Faraday cages in the form of wallets and sliding cases to protect their RFID-enabled cards from unwanted scans [69],[121].

5.3.1.4. Defend against Malicious Code Injection Attack

First of all, the nodes must be protected from unauthorized physical access. This is done through the security measures mentioned in Section 5.2.2, as well as the points mentioned in the defend against tampering attacks.

Installing anti-spyware and virus programs on IoT devices is one of the most important ways to resist this attack, as described in the general countermeasures in Section 5.2.14. Additionally, to mitigate this attack, a Chain of Trust (CoT) based secure boot can be created. When a device's CPU starts up, it just executes some very specific instructions on a specific address. There are simply not enough resources to start any code. At this point, all the system can do is search for, validate, install, and run a small piece of the firmware. CoT is used to verify "signatures" on this initial piece of firmware to ensure it has not been illegally modified or replaced. It is intended to ensure that only trusted software and hardware can be used. Regular code review is another potential solution to this attack. It is an activity used to ensure software quality and to find bugs, performance issues, vulnerabilities, and injected malware [70].

5.3.1.5. Defend against False Data Injection Attack

The same security measures to protect against the previously mentioned physical attacks are also required to reduce the occurrence of this attack. Moreover, there are several countermeasures that researchers have proposed over the years against this attack. For example, in [122] the authors suggested an approach that relied on attaching keys to nodes based on their geographic location. Whereas, nodes located close to each other must contain the same key. Their method of uncovering false reports relied that adjacent nodes should behave similarly when an event occurs, resulting in them producing converging reports. Therefore, if a node submits a report that is significantly different from that of nodes in the same region, it will be considered a false report.

Using the same idea of previous approach, researchers in [122],[123] proposed a scheme for filtering data and identifying false reporting, namely the Geographic Information System (GIS). GIS is a system that analyzes and displays information, so that it links this information to specific geographical areas. For example, if fires were started in three different places, then a GIS analysis might show that all of these fires occurred in places where camping is more frequent and suffers some form of drought. So, GIS maps can then display all sites in the area that have similar conditions, so that firefighters expect new

fires to break out in these sites. The references [122],[123] gives more proposed countermeasures against this attack.

5.3.1.6. Defend against Sleep Deprivation Attack

In sensor networks, clustering is used to organize sensor nodes into clusters that depend in part on their physical proximity. One of the nodes in the group is delegated the task of being the head of the cluster. The cluster head collects the information from the group and sends it as a single message to the gateway or to the processing center.

To launch this attack, the malicious node must become the head of the cluster, because the sensor nodes deal with the cluster head only and receive orders from it and send information to it. For this reason, preventing a malicious node from becoming the head of the cluster is a way to prevent this attack. The reference [124] proposed many algorithms that make it hard for an adversary to become a cluster head, thereby greatly reducing the effect of a sleep deprivation attack such as Random Vote Cluster Head Selection.

Also, Firewall can be used to prevent this attack because it allows only trusted data to access the network. On the other hand, IDS can help detect the occurrence of this attack by monitoring the network for anomalies such as sending unnecessary and redundant requests to a node in short periods of time.

5.3.1.7. Defend against Noise

To reduce noise, the data must be filtered. The data filter has the function of separating the real data from the noise. Many data filtering techniques are proposed. For example, researchers in [125] have developed effective RFID data filtering techniques to generate clean RFID data, which can be incorporated into RFID-based applications. They studied two types of filtering, one that removes noise from the RFID data (noise reduction or smoothing), and the other combines repeated readings to form one correct reading.

5.3.1.8. Defend against Timing Attack

There are simple countermeasures that can be used to defend against this attack, including the following:

- **Random Delay:** A random delay can be added to the time required to decode an element, making it difficult for an attacker to guess its true value. This random delay varies from one element to another or even for the same element from time to time.
- **Blinding:** For example, performing a calculation on the encrypted text to generate another encrypted text before sending it (i.e, the encrypted text is doubled). The more the number is multiplied (e.g., doubling it four times is more complicated than doubling it twice), the harder the attacker can deduce the real text.

5.3.1.9. Defend against Replay Attack

There are some countermeasures that can be used to defend against this attack such as [70]:

- **Sequence Number:** Each message is attached to a serial number before sending, so that this number is used to indicate the order of the message in relation to the rest of the messages in a single conversation. The recipient does not accept the message and acknowledge its authenticity, unless the serial number is in the proper order.
- **Timestamps:** The timestamp records the time and date the message was sent to the recipient. The sender sends the message with its timestamp to the recipient. The recipient checks the timestamp to see how fresh the message is. However, for this method to work efficiently, the timing at both ends of the communication must be identical.
- **Challenge/ Response:** The sender (A) first sends a number (nonce) to the recipient (B) in encrypted format (challenge). Then A asks B to send the number back to it (Response). Therefore, (B) decrypts the number with the shared secret key and then re-encrypts it and sends the number back to A in plain text and in encrypted form. In this way, A and B verify each other's identities.

5.3.1.10. Defend against Eavesdropping Attack

Using strong and lightweight cryptographic techniques for encryption is a important countermeasure against this attack. Before data can be sent through the transmission medium, it must be encrypted first, making it impossible for the attacker to take advantage of the information even if he could eavesdrop on it. It is also important to use an efficient key distribution mechanism to securely distribute cryptographic keys between nodes. This will ensure that these keys do not fall into the hands of attackers, rendering information encryption ineffective.

5.3.1.11. Defend against Jamming Attack

There are several countermeasures that have been suggested to overcome jamming attacks such as [126]:

- **Appropriate Power Transmission:** For a successful jamming attack, the strength of the jamming signal must be higher than the strength of the original signal so that the jammer can defeat the original signal. So, the higher the transmitted signal strength, the greater the jamming resistance.
- **Frequency Hopping Spread Spectrum (FHSS):** FHSS is a method used to avoid interference. By using this method, the sender and receiver change the frequency that is used to carry the transmitting radio signals. In FHSS, the available frequency band is divided into smaller sub-bands. The frequencies that carry the transmitted signals change (hop) rapidly from sub-band to another in a pre-determined order. These changes are controlled by a code known to both the sender and the recipient. This method is effective method against jamming attack if the frequency hopping pattern is unknown.
- **Direct Sequence Spread Spectrum (DSSS):** Direct sequence modulation is a spread spectrum modulation that helps reduce interference to the original signal. DSSS makes the transmitted signal wider in bandwidth than information bandwidth. In this technique, the data signal and spurious noise are multiplied to produce a wider bandwidth output signal that replaces the original signal.

At the receiver, noise is filtered in order to recover the original data. DSSS is more secure than FHSS because it is difficult for an attacker to retrieve the signal sent from DSSS.

- **Polarization of Antenna:** Antenna polarization can be defined as the direction of the antenna and the radiant energy produced by it. To communicate with different antennas, it is necessary to have the same polarization between them.

  The antennas on the nodes must maintain a single line of sight to establish reliable communication with each other in a jamming environment. If the nodes sense any interference in the environment, they can change their polarization and save the network from interference.

- **Directional Antenna:** Directional antennas are antennas used in IoT nodes that send and receive data in only a specific direction. With directional antennas, a jamming attack can be avoided because this type of antenna has the ability to focus the beam making the signal with some energy travel to a wider distance. This ability improves transmitter performance and can make the network more resistant to interference.

  The advantage of these antennas to resist jamming attack appears when compared to the omnidirectional transmitter antennas used these days. As the antennas of the omnidirectional transmitter have the ability to transmit and receive waves from every possible direction at the same time, this leads to security problems and reduces the reliability of these antennas.

Table 5.2 summarizes the attacks on the perception layer mentioned in Chapter 4 and some countermeasures that can be taken against them.

Table 5.2 Some Attacks on the Perception Layer and Some Countermeasures against them

Attack	Countermeasures
Tampering Attack	• install IoT node in hidden and monitored locations • routinely physical checking of the nodes • make the IoT node from strong and safe materials • disabling JTAG interface of the sensors • use of good password protection for the bootstrap loader of the sensor boards
Node Capture Attack	• countermeasures against a physical attack • encryption • centralized approaches detection schema • distributed approaches detection schema
Unauthorized Reading of RFID Tag	• the kill command method • the sleeping command method • blocker tag • encryption • authentication • faraday cage
Malicious Code Injection Attack	• countermeasures against a physical attack • anti-malware programs • CoT • regular code review
False Data Injection Attack	• countermeasures against a physical attack • attaching keys to nodes based on their geographic location • GIS

Table 5.2 (continued)

Attack	Countermeasures
Sleep Deprivation Attack	• random vote cluster head selection • firewall • IDS
Noise in Data	• data filtering techniques
Timing Attack	• random delay • blinding
Replay Attack	• sequence number • timestamps • challenge/ response
Eavesdropping	• encryption • securely key distribution mechanism
Jamming Attack	• appropriate power transmission • FHSS • DSSS • polarization of antenna • directional antenna

5.3.2. Defenses against Attacks on the Network Layer

The network layer of IoT architecture depends on the Internet and existing networks to perform its function. Therefore, it is not specific to the IoT environment, but rather the backbone of all information and communication environments. For this reason, this layer suffers from traditional network vulnerabilities and threats present in these environments. These security problems have been under constant research for a period of time, and have resulted in many well-defined protection methods that can also be used in the IoT environment. For example, in IoT environment, the solutions of some known attacks such as MITM attack, eavesdropping, routing attacks are already known [34],[59],[127].

However, with the development of IoT, this does not preclude trying to find a more effective security strategies for protecting the network layer. The goal of these strategies is to maintain the confidentiality, integrity and availability of data while it is transmitted over the network. Lack of these strategies, makes it easy for attackers to steal, alter, or block information as it travels across the network. This leads to disclosure or loss of information, or even knowing the address of the sender and the recipient [128]. To achieve these strategies, many countermeasures are needed that can help overcome many attacks and threats targeting this layer [3],[21]. There are several measures that have been suggested by many researchers to increase the security at the network layer and resist the attacks it faces. Among these measures are:

5.3.2.1. Defend against MITM Attack

Detection and defense of such attack is critical for the wireless networks to ensure data integrity and secure connection. There are several methods suggested for detecting the MITM attack such as:

- **Round-Trip Time (RTT):** The authors mentioned in [129] that when a MITM attack occurs, a time delay occurs. This delay is due to the attacker's need to impersonate the intended sender and receiver, plus the attacker needs time to hack the message, buffer it, tamper with it, and then send it back to its destination. So, they suggested that it is possible to detect a MITM attack by carefully measuring Round-Trip Time (RTT) during the data transfer between the sender and the receiver. RTT is the time in milliseconds that it takes for a request message to travel from the sender node to the destination node and back again to the sender node.
- **Media Access Control Layer (MAC) protocol:** Another detection method was proposed in [130] that used a modification of the MAC protocol for this. This method is based on the fact that a successful attack must guarantee the receipt of an acknowledgment (ACK) within the ACK timeout period. That is why, in this detection method, the sender and receiver secretly agreed on number of packets

that will be transmitted without acknowledgement. Hence, an intruder is detected when it sends acknowledgement after receiving each packet.

- **Radio Signal Strength (RSS):** The recipient senses the RSS of the received message, which enables it to notice whether there was an attack or not. This is due to the fact that the attacker has different computing hardware from the victims', and his physical location may be near or far from the receiver, and these are all factors that affect RSS [129].
- **Integrated Intrusion Detection System (IDS) and Intrusion Prevention System (IPS):** MITM attack detection relies solely on monitoring the behavior of nodes in the network. Therefore, the Integrated IDS and IPS can help deal with a MITM attack at the network layer. This is based on three main points that occur when this attack occurs and these points are used by IDS and IPS to detect the MITM attack [131]:
  1) A change in the content of the sent packets
  2) Delay in the arrival time of the sent packets
  3) A change in the destination of the packets

When talking about ways to prevent this attack and limit its effects, it is worth noting that the following two points can work together to achieve this:

- Encrypting the transmitted data can be very helpful in reducing the effects of this attack. If the attacker can intercept the transmitted data, then he will not have the ability to detect or tamper with it because it is encrypted. Encryption also prevents the enemy from knowing the destination and source of the information and thus cannot launch this attack that relies on this information to succeed. However, for data encryption to be effective, it must be preceded by the use of an appropriate mechanism to distribute the keys so that it does not fall into the hands of the attacker, thus enabling him to decrypt the data.
- In a MITM attack, both ends of the communication believe that they are communicating directly without an intruder between them. For this reason, there must be an effective mechanism for authentication between the two

communication parties, in order to verify the identity of each, before starting to transmit data between them.

5.3.2.2. Defend against DoS Attack

Both the firewall and IDS do an important job in protecting against this attack. The firewall limits the data packets that are allowed to enter and exit the network, which prevents suspicious request packets from entering the network and creating congestion in it. The IDS monitors any suspicious activity in the network such as abnormally repeated requests sent to the server.

Authentication is also effective against a DoS attack. Before accepting any connection request from any party, it must be verified that it is allowed to request the service or enter the network. If it is not allowed to request or join, its request will simply be ignored or rejected which limits the possibility of this attack.

It has also been indicated before that there are several types of attacks that fall under the category of DoS attack, such as jamming, tampering, hello flood attack, etc. In addition to the above countermeasures, the countermeasures against these attacks are also measures against a DoS attack, depending on its type.

5.3.2.3. Defend against Hello Flood Attack

This attack is considered a type of DoS attack, so IDS and firewalls are two important measures against this attack. Additionally, there are also some technologies that can be used to detect and mitigate Hello Flood attacks such as [132],[133]:

- **Signal Strength Based Scheme:** It is known that the enemy in this attack uses high transmission power to ensure that the hello message he sent reaches all the targeted nodes. Therefore, it becomes possible to detect the hello attack by checking the received signal strength. This is because as some researchers have suggested, each node has the same signal strength in a certain range. When a node receives a hello message, it compares the strength of this received message against the known strength of the signal in the radio range. If the two results are the same,

the node is considered a friend (normal node). Otherwise, the node is considered - strange (malignant node)

- **Client Puzzle Schema:** As mentioned in the previous point, the received message signal strength is compared with the fixed signal strength of the radio range. In light of the result, the sending node of the message is determined as either "friend" or "stranger". To distinguish between friend and stranger, client puzzle technique is used. The idea of this technique is to require all clients connected to a server to properly solve a puzzle before establishing a connection. After solving this puzzle, the client has to return the solution to the server, which the server will quickly verify, either accepting or rejecting the client's connection.

  The client puzzle technique is used here when a strange node is asked to solve a puzzle and reply within a specified period of time. If the reply is correct within the time, it is considered as a friend. The puzzle difficulty level increases by counting the number of hello messages sent by the node. Therefore, whenever a node sends a large number of hello messages to initiate an attack, the puzzle it must solve to prove its legitimacy is extremely difficult.
- **Cryptographic Solution:** First, two nodes share same secret key for communication between them in a secret way. Then the node uses this key to encrypt each request message (even hello message) sent to the other node. In this way, the neighboring node can decode, verify, and then respond to the request message while the attacker will not know the key and will be prevented from launching the attack.

5.3.2.4. Defend against Sybil Attack

To defend against Sybil attacks, the identities of every node should be verified. This attack relies on hacking a legitimate node and using it to launch the attack, so protecting the legitimate nodes from a physical attack might be the first line of defense against this attack. Encrypting information within nodes is also important against a sybil attack, so that the attacker cannot use this information to join the network. To verify nodes identities before beginning the exchange of information, an effective authentication technique must

be adopted that enables the nodes to confirm the identity of the node requesting the exchange of information with it. However, if this attack does occur, there are several methods proposed to detect sybil nodes within the network such as [134],[135]:

- **Random Key Pre-Distribution:** This technology allows nodes to create secure links to other nodes. In random key pre-distribution, each node shares a unique symmetric key with a trusted base station.

  When two nodes need to communicate to each other, they use Needham-Schroeder as a protocol to verify each other's identity and create a shared key. In this protocol, the access point is responsible for creating a shared secret key to be used by the nodes that want to communicate with each other. Then these neighboring nodes can use the resulting key to implement an authenticated, encrypted link between them. To prevent an intruder from roaming within the network and creating shared keys with every node in the network, the base station can limit the number of neighbors a single node is allowed to have. If the node exceeds the allowed number, an error message will be sent to the base station.
- **Registration:** In wireless sensor networks, there may be a trusted central authority managing the network. One of the functions of this authority is to record the identities of the nodes spread in the network, and it also distributes this information secretly to those nodes. To prevent a Sybil attack, any node can check the list of "known" identities to verify the legality of any node trying to communicate with it.
- **Position Verification:** In this approach, the network verifies the physical location of each node. Sybil nodes can be detected using this method because they will all appear in exactly the same location as the malignant node that generates them.

  This approach may not be useful in the case of a mobile attacker. This is because he may be able to present a certain identity in one place and then move to another place and provide another identity. To get around this, all nodes location can be verified simultaneously.
- **Code Attestation:** The basic idea behind this method is to exploit the fact that the code running on a malicious node must be different from that on a legitimate node.

Therefore, the legitimacy of a node can be verified by checking its memory content. This method is still being developed and studied to make it verifiable in wireless sensor networks.

5.3.2.5. Defend against Wormhole Attack

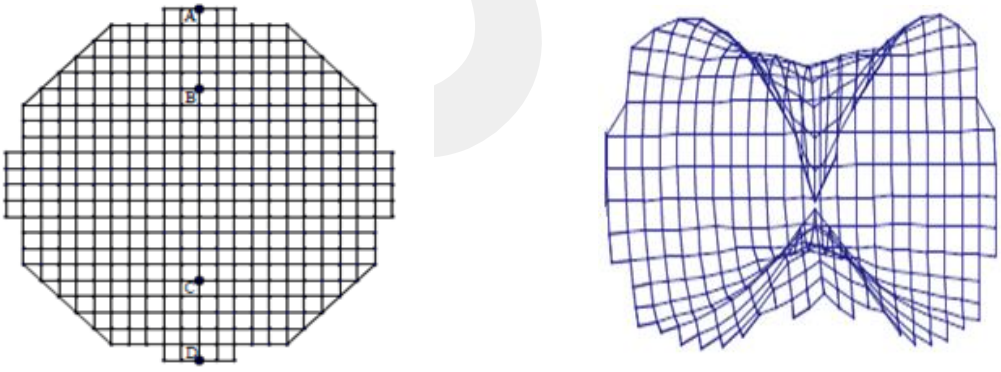
Because wormholes use a special channel that is invisible to the sensor network, so they are often difficult to detect. Nevertheless, the researchers suggested several methods that could be used to detect wormholes in sensor networks. For example, the authors in [136] proposed an approach to wormhole attack detection using Statistical Analysis of Multi-Path. First, all paths in the network are explored. Then the relative frequency of each path used to link nodes in the network is calculated. Then it is determined that the path with the highest relative frequency is a wormhole. Hu, Perrig and Johnson proposed to use packet leashes to detect the wormhole attack [137]. In packet leashes, location or timing information is included in packets, which is used to discover whether the packet has traveled further than it's allowed. Two types of packet leashes are proposed, Geographical Leashes and Temporal Leashes.

- **Geographical Leashes:** A geographical leash ensures that the recipient of the packet is within a certain distance from the sender. Therefore, to use the geographical leash, two conditions must be met, the first is that each node must know its own location, and the second is that all nodes must have loosely synchronized clock.

  To use the geographical leash, the sending node includes its own location in the packet when it was sent, as well as the time it was sent. When the receiving node receives the packet, it compares the included information with its location and the time it received the packet. If the sender and receiver clocks are synchronized, and the speed limit for any node is known, the receiver can calculate the upper limit of the distance between the sender and the receiver itself. Thus, the recipient can determine whether the sender is its neighbor or not [137],[138],[139].
- **Temporal Leashes:** For a temporal leash to run efficiently, all nodes must have tightly synchronized clocks. To use temporal leashes, when the sending node

wants to send any packet, it includes the transmission time in the packet. Upon receiving the packet, the receiving node compares the transmission time to the time the packet was received. Thus, the receiver is able to detect if the packet has moved too far, based on the transmission time and the speed of light which is the speed of the packet while traveling. Also, a temporal leash can be created by including the packet expiration time instead of the transmission time. If the packet has expired, the recipient must refrain from accepting and ignore it. The lifetime of the packet is determined based on the maximum permissible packet distance and based on the speed of light and it is used to prevent the packet from traveling further than a specific distance [137],[138],[139].

Multi-Dimensional Scaling - Visualization Of Wormhole (MDS-VOW) was one of the techniques proposed to detect the wormhole attack. This technique was suggested by Wang and Bhargava in [140]. MDS-VOW first reconstructs the network using multi-dimensional scaling as shown in figure 5.1 (a). Then MDS-VOW detects the wormhole by visualizing the anomaly caused by the attack that significantly changes the original layout. Deflections caused by phantom connections across the wormhole make the surface shown in the drawing curved due to the sensors being pulled away from each other as shown in figure 5.1 (b).



(a) (b)

Figure 5.1 (a) Reconstruct Original Sensor Network using MDS [140]
(b) The rebuilt network when a wormhole exists between sensor A and C.

Suspicious nodes can also be detected by measuring the signal strength. This is because the nodes involved in creating the wormhole are distant from each other. This makes it need to increase the signal strength in order to reach its destination. In addition, nodes must use effective authentication technology to verify each other's identity before sending data for the purpose of routing it.

5.3.2.6. Defend against Selective Forwarding Attack

As we mentioned in the previous chapter, this attack is easy to implement, but difficult to detect, because the malicious nodes selectively pass some data packets, like any normal node, and drops others. In an effort to overcome the selective forwarding attack, various countermeasures and detection schemes have been proposed to counter it. Some of these countermeasures are listed below:

- **Detection Using Acknowledgments:** Yu and Xaio in [141] introduced a multi-hop acknowledgement scheme that relied on intermediate nodes in the path between the sender and the receiver to detect the presence of malicious nodes and launch an alarm. To launch the alarm, these intermediate nodes generate alarm packet and deliver it to the sender node through multiple hops.

  The idea of this scheme is that, after an intermediate node forwards a packet of data to its neighboring node, it waits for ACK packets to be returned by that neighboring node within a certain period of time. If not, the intermediate node suspects the previous data packet was dropped by a malicious node.
- **Multi Data Flow Detection Scheme:** The Multi-Dataflow Topologies (MDT)'s primary task is to mitigate the damage caused by a selective forwarding attack. It has the ability to make the base station receive information from sensor nodes continuously even in the presence of a selective forwarding attack. In addition, when using this scheme, there is no need to retransmit packets that were dropped by malicious nodes [142]. The main idea in the MDT is that before deploying the sensor nodes, the base station divides the sensor nodes into different groups. So that each sensor belongs to only one group and can only communicate with sensor nodes belonging to the same group. Each group will belong to one data flow

topology. After building multiple data flow topologies, each sensor node will begin to sense itself and send information back to the base station. More than one data flow topology may overlap and cover the same area, so that two sensors from two different topology can collect the same information and send it to the base station. Therefore, the base station only requires one of the reports from one topology to control the entire network. If a selective forwarding attack does occur and drops some sensitive data packets to prevent the base station from receiving it, however, the base station still can receive the same lost information but by the other dataflow topology. This is because the sensor area of the dataflow topology is overlapping.

- **Distributed Cooperative Failure Detection Technique:** The basis of this technique is that the nodes around the suspected node collaborate with each other to reach agreement on whether the suspect is malfunctioning or malicious. This technique has three major components [143]:
  1. **Failure Detection without Coordination:** Used to detect bad routing behavior, a node listens to the transport activities of its neighbors. If the number of packets a neighbor failed to redirect exceeds a certain limit, the matter becomes suspicious.
  2. **Collect Results from Distributed Detection:** When a node suspects a defect in one of its neighbors, it sends messages to request opinions on the suspected neighbor's behavior from other neighbors of the suspect. All neighbors submit their opinions in response to its request.
  3. **Diagnosis and Reporting of Diagnostic Result:** After gathering the opinions of neighbor nodes, the requesting node arrives at a decision on whether the suspected node is a malicious node or not.

As we mentioned in the Section 5.2.3, authentication between nodes before sharing information is important to prevent this attack. If the node cannot prove that it is a legitimate and harmless node, then the other nodes will not send any information to it, so there will be no data loss. Also, IDS use plays a vital role in detecting the presence of a selective forwarding attack. It has the ability to detect errors in the process of routing

information within the network causing it to trigger an alarm. In addition to the foregoing, the reference [144] provides information on other countermeasures used to defend against a selective forwarding attack. Table 5.3 summarizes the attacks on the network layer mentioned in Chapter 4 and some countermeasures that can be taken against them.

Table 5.3 Some Attacks on the Network Layer and Some Countermeasures against them

Attack	Countermeasures
Man-in-the-Middle Attack (MITM)	• measure RTT • MAC protocol • sense RSS • integrated IDS and IPS • encryption and authentication
Denial of Service Attack (DoS)	• IDS • firewall • authentication
Hello Flood Attack	• IDS • firewall • signal strength-based scheme • client puzzle schemes • cryptographic solution
Sybil Attack	• physical attacks countermeasures • encryption • authentication • random key pre-distribution • registration • position verification • code attestation

Table 5.3 (continued)

Attack	Countermeasures
Wormhole Attack	• statistical analysis of multi-path • geographical leashes • temporal leashes • MDS-VOW • suspicious node detection by signal strength • authentication
Selective Forwarding Attack	• detection using acknowledgments • MDT • distributed cooperative failure detection technique • authentication • IDS

5.3.3. Defenses against Attacks on the Application Layer

The IoT provides its users with many applications in various fields, from smart healthcare to smart homes. The user deals with these applications through the application layer in the IoT architecture, so it is worth saying that the application layer, is the real service provider for the end user. This layer processes data collected by perception layer and transmitted by network layer. This information is mostly sensitive and private, and any penetration of this layer means a violation of user privacy. So, the challenge in this layer, after taking into account the different security needs in different applications, is how to protect the privacy of users in addition to ensuring the safety of IoT applications, which makes the information it provides reliable [59].

In addition to protecting privacy, which is the primary goal of securing this layer, there are other security requirements that must be fulfilled to say that this layer is safe. Confidentiality, data integrity, authentication, availability, privacy protection, security

education and management, especially password management, are essential security requirements at the application layer [3],[21],[59].

The following subsections represent some of the important countermeasures and defenses against attacks mentioned in Chapter 4 that this layer faces. The mission of these security measures is to achieve protection for the IoT application layer from attacks and reduce their impact.

5.3.3.1. Reducing Application Layer Software Vulnerabilities

In order to reduce the security holes that may exist in the programs of this layer, manufacturers and developers of IoT devices and programs should pay more attention to the security aspect. Applications, services, and software appropriate to the IoT environment must be designed, written, or developed, taking into account all security weaknesses that this layer may suffer from.

Moreover, to prevent vulnerabilities, programming languages should be used that does not allow these vulnerabilities to exist. For example, using programming languages such as Java, Python and .NET can alleviate the buffer overflow problem.

Another step that can be used to reduce the presence of security vulnerabilities, is to carry out the process of developing software, applications, and operating systems in IoT devices whenever this is available. Using proper patching is also important. Because a patch is a collection of changes to a device's software or supporting data designed to update, fix, or improve it [22].

Correcting code errors from time to time is helpful in correcting the gaps detected in the code. This can happen by using debug code, which is code introduced to the device software for error checking or to help decide the source of the error [22].

5.3.3.2. Defend against Phishing Attack

Several methods have been suggested against phishing attacks, including:

- **Network Level Protection:** This attack can be prevented or protected from at the network level by allowing a specific group of IP addresses or a group of domains

to enter the network. This is done by using a firewall or IDS that helps monitor network behavior and notify administrators if something is suspected.

Domain Name System Blacklists (DNSBL) is a service that enables mail servers with the help of Domain Name Server (DNS) to check whether a sending IP address is blacklisted for common IP addresses for sending spam. DNSBLs create and update its blacklist regularly by monitoring network traffic.

- **Authentication:** This method is used to confirm whether the message was sent with a valid path and domain name. The authentication method can be done, for example, by digitally signing the document before sending.
- **Anti-Phishing Toolbars:** These tools are available in some browsers and their most important functions are:
  - Check email content and web page fields like username, password, suspicious links, images, etc.
  - Report and block suspected fraud and phishing sites
  - Validate the content of web pages.
  - Filter phishing emails from the mailbox of the customer
  - Provide comprehensive site reviews, including content, risk analyses, etc.

  PhishGuard is an example of these toolbars. It starts working when it detects that the authentication process has started by sending the user ID and password (or equivalent). PhishGuard redirects the real user ID to the page but some incorrect (random) passwords instead of the real password repeatedly, for a certain number of times. If the page responds negatively, it is most likely a legitimate site. On the other hand, if the page responds positively, then the site can be considered as a phishing site [82].
- **User Education:** The user must have a background on this attack and how it works because this will help him to be careful when dealing with suspicious websites and emails. Information about this attack and how to prevent it must be made available to all users, and this information must be easily accessible, for example, by publishing it online. Additionally, training users and providing them with testing tools would greatly improve their ability to identify phishing sites and emails [81].

5.3.3.3. Defend against XSS Attack

This type of attack primarily exploits vulnerabilities found in applications and websites. Therefore, attention to security risks and vulnerabilities in the applications has an important role in preventing XSS attack. Also, web application developers should study the causes that put applications at risk such as poor design, configuration errors, flaws, etc.

This attack is one of the most common attacks against the application layer. That is why, when researching the means used against this attack, we found a large number of countermeasures proposed to prevent this attack. Since it is not possible to talk about all of them, so only some of them are mentioned as examples.

Some authors have proposed the use of static analysis techniques or tools in the Web server-side to discover XSS attack in a web application. These static analysis security tools attempt to find security vulnerabilities without executing the software by scanning the source code for known potentially security-compromising functions [145]. There are many proposed static security analysis tools such as Flaw Finder which use a vulnerability database to find malicious scripts. Additionally, BOON tool performs static analysis focusing primarily on the detection of the buffer overflow security vulnerability [145]. Moreover, those static analysis schemas are usually complemented by the use of dynamic analysis techniques. Dynamic analysis is used to confirm potential vulnerabilities discovered during static analysis by monitoring application behavior at runtime. One of the dynamic techniques, used is to detect XSS, is an anomaly-based intrusion detection system. This technology analyzes web server logs by taking these logs as input and then comparing them with incoming user requests. The web server logs contain information about host IP address and user authentication data. So, requests with atypical parameter profiles can be classified as potential attacks [146].

Disabling JavaScript by users before they visit a suspected website is also a good strategy to keep users safe. Also, a client-side web firewall can be used to protect against an XSS attack. For example, the authors [147] suggested a technology called Noxes that acts as a web proxy. Noxes uses both manual and auto-generated rules to mitigate potential cross-

site scripting attempts. With limited user involvement, Noxes efficiently defends against data leakage from the user environment.

Since this attack primarily targets cookies, it is important to protect these cookies. One of the methods used to do this is secure cookies. Secure cookies mean that cookies exchanged between the client and the server must be encrypted. This can be achieved if cookies can be sent over Secure Sockets Layer (SSL) connections. Cookies can also be rendered useless for XSS attacks through the technique proposed by Putthacharoen and Bunyatnoparat [148]. This technique is called Dynamic Cookie Rewriting. With this technology implemented, the web proxy will automatically rewrite the value in the cookie with a random value before sending the cookie to the user's browser, so the browser will keep the random value in its database instead of the original value sent from the web application. The cookie returned from the browser will also be rewritten to the original value in the web proxy before being redirected to the web application. So even if the attacker managed to steal these cookies, the information they contain would be of no value [148].

5.3.3.4. Defend against Malware Attack

Due to the marked increase in malware attacks on IoT devices, there is an urgent need for stable and effective detection and protection methods against them. There are several measures that can be taken to prevent malware attacks or reduce their effects, should they occur, including:

- Apply the latest updates to operating systems and applications.
- Educate users to be wary of suspicious websites and emails and not to open any suspicious links.
- Back up important files regularly to prevent them from being lost if they are erased by a malicious program.
- Use access control to important files and folders to protect them from illegal access. This prevents, for example, ransomware programs from accessing and encrypting files.

- Use Anti-malware programs (as mentioned in Section 5.2.14) that can be installed on devices that the consumer uses to interact with IoT applications.

Table 5.4 summarizes the attacks on the application layer mentioned in Chapter 4 and some countermeasures that can be taken against them.

Table 5.4 Some Attacks on the Application Layer and Some Countermeasures against them

Attack	Countermeasures
Application Layer Software Vulnerabilities	• use safe programming language • developing software, applications, and operating systems • code debugging
Phishing Attack	• DNSBL, firewall, IDS • authentication • anti-phishing toolbars • user education
Cross-Site Scripting (XSS) Attack	• static analysis tools • anomaly-based intrusion detection system • web proxy • disabling JavaScript by users • Noxes • secure cookies • dynamic cookie rewriting
Malware Attack	• updates operating systems and applications whenever it is available • educate users • back up important files regularly • access Control mechanism • anti-malware programs

Among the research questions presented in Chapter 1, there was a question related to cyber attacks against the IoT and how to prevent them, which is the fourth question. This chapter answered the part in the fourth question related to how to prevent and protect against cyber attacks.

After listing countermeasures against attacks targeting IoT, we considered using one of the most popular IoT applications, which is smart home, as an example or a case study. Through this study, we will explain some real attacks targeting the smart home, their purpose, and the extent of the damage they may cause. The next chapter will be devoted to this study. In addition, the next chapter will identify who is really responsible for providing smart home security and discuss measures they can take by him to make the smart home immune to cyber attacks targeting sensitive information for homeowners that may target their lives and properties.

CHAPTER 6

SMART HOME SECURITY

6.1. Smart Home Background

Nowadays, two new terms emerge describing homes: traditional homes and smart homes. The traditional home can be defined as a home with manually operated devices, usually by flipping the switch or pressing a button. In addition, managing the power consumption of these devices is difficult and they do not have the ability to communicate with other devices or with the outside. On the other hand, smart homes are completely different, they allow their owners to control and manage smart home appliances electronically and remotely (refrigerators, air conditioners, washing machines, etc.).

Also, smart home devices have the ability to interact with one another and communicate with the outside world in order to provide services to their owners [149],[150]. It can be said that one of the most important differences between traditional homes and smart homes is that the latter can be monitored, accessed and controlled remotely. For example, a homeowner can lock / unlock his home doors from miles away, smoke alarms can warn his mobile phone when a fire is detected and he can control lighting systems remotely [54].

As a promising application of the IoT, smart homes have provided a large number of benefits to consumers, making them gained great popularity among people. As a result, many consumers are converting their traditional homes into smart homes, especially with the continuous advancement and low cost in communications technology, information technology and electronic devices. In addition, many home appliances have been provided, that have the ability to connect to the Internet, and many IoT devices have been produced with sensors (cameras, motion detectors, etc.) and actuators (lamps, locks, etc.). These are all important factors that have contributed to the acceleration of smart home adoption [54].

The production of a large variety of smart devices over the past years has helped a lot to make the smart home application workable. Companies like Philips, Amazon, and others have produced many smart devices. For example, Philips makes smart light bulbs called Philips Hue. Philips Hue allows the user to wirelessly control the lighting system in the home. The user, through an application on his smartphone or on his computer, sends commands to them, which in turn sends them to the lights.

As for Amazon, they produce a smart speaker called Amazon Echo. This smart speaker provides consumers the ability to control their smart homes via voice commands. The Amazon Echo features microphones that are programmed to listen for 'wake-up' commands and input voice to complete tasks such as dimming the lights and playing music [112].

Furthermore, Samsung and Apple companies produce smart home platforms such as Samsung SmartThings and Apple Homekit. They are systems that allow a homeowner to control all their smart home appliances made by different manufacturers, all from one place [149]. Figure 6.1 shows an example what is SmartThings platform can really do in smart home environment as a daily scenario.

- At smart home, when homeowner wakes up in the morning, SmartThings can turn on lights, turn up the climate devices, turn on the radio and turn on the coffee machine.
- When he leaves home, SmartThings locks all the doors, turns off all lights, turns down the thermostat, and turns on the security camera.
- While homeowner is away from home, SmartThings can send him video alerts if there is unexpected activity, warns him if there is a water leak, gas leak and much more.
- When he arrives home in the evening, SmartThings can open his garage door automatically, adjust the lights for him, turn on his favorite music, and control his home appliances.
- When homeowner goes to sleep, SmartThings can warn him if doors or windows have been left open. Then it turns off all the lights and turns down the thermostat.

Figure 6.1 A Daily Smart Home Scenario [151]

6.1.1. Smart Home Definition

Smart Home is a building that supports an automated system and is equipped with a set of interconnected components that work together automatically and in harmony to serve the residents of the home. These components include (sensors, networks, actuators, and home appliances). They are made by different manufacturers; they support different communication technologies and are distributed in different places inside and outside the house. Despite this, they have the ability to coexist, interact and cooperate with each other, with the outside world and with the homeowner [149]. Consumer can control and monitor his smart devices by voice, physical gestures, remote control device, as well as smart home applications on his smartphone, tablet and computer. The consumer can use the smart

home application to control his home, whether he is inside or outside the house, close to it or far away [152]. Figure 6.2 illustrates the smart home system and shows some of the smart devices and systems that can be found in many smart homes.

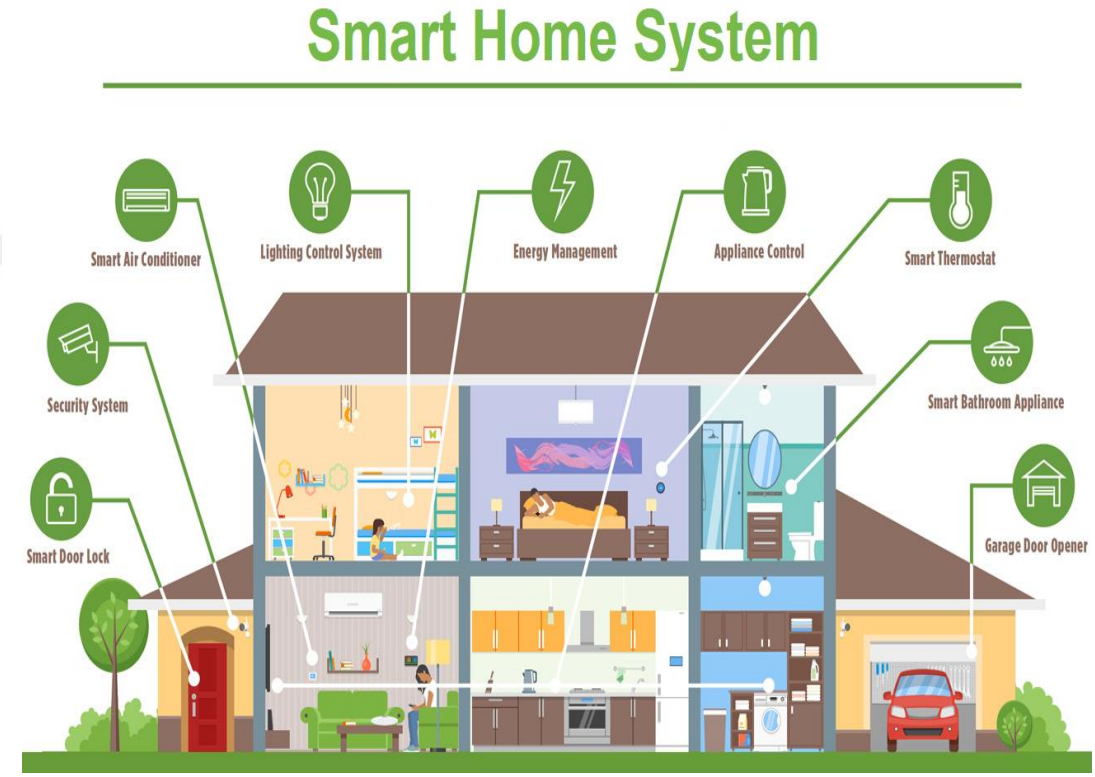


Figure 6.2 Smart Home System [153]

6.1.2. Smart Home Benefits

Smart homes have demonstrated their ability to make their residents' lives easier and more comfortabile by accomplishing household tasks in an automated manner, fulfilling demands, and delivering a range of services [28]. In general, a smart home provides peace of mind to its residents because it is able to know what they prefer, what they need and their daily routine, and act and adapt accordingly [152].

A smart home provides its residents with continuous information about the state of the home and gives them broad access to many parts of it even from a distance. Whether the owner of the house is at home, work or on vacation, the smart home informs him about

the current affairs in it, which helps a lot in emergency situations. For example, in the event of a fire in the house, the smart home will wake the residents by turn on the fire alarm and at the same time it will open the doors and communicate with the fire department. It also allows its residents to control and monitor connected home appliances. This monitoring feature helps residents deal with emerging risks, for example forgetting to turn off a home appliance or leaving the home door open [152].

There is also a so-called smart irrigation system, which irrigates the garden only when needed and only with as much water as it needs. Smart home also reduces energy consumption which leads to lower bills. It does this by turning off the lights automatically when the person leaves the room, and controlling the rooms heating or cooling as needed. As a result, energy, water and other resources are used more efficiently, which helps to save both natural and money resources for the consumer. In the field of helping the elderly to stay alone for a long time, smart homes are a promising technology in this field, providing many important services. This type of homes reminds residents when it's time to take the medicine, and alert the hospital in the event of an accident. It also helps the elderly's families to monitor and care for them remotely.

6.1.3. Smart Home Components

The smart home consists of a group of different components that work together in harmony and interdependence so that the smart home can provide services to its residents. These components usually include sensors, actuators, networks, and smart appliances as shown in figure 6.3 which shows the smart home structure as well [154],[155],[156]. The components of a smart home and a brief overview of each is presented below

- **Sensors:** There are many types of sensors used in smart home such as (light, temperature, motion, smoke) sensors. These sensors perform specific functions to measure characteristics of the surrounding environment, such as temperature and the amount of light, or characteristics of surrounding objects, such as movement or heart rate. Sensors can range from wearable devices (such as wrist straps) to non-wearable sensors (such as security cameras). These cameras, along with microphones, are the most sensitive to homeowner's privacy. In general, smart

home sensors generate a large amount of highly personal data about activities within the home [154].

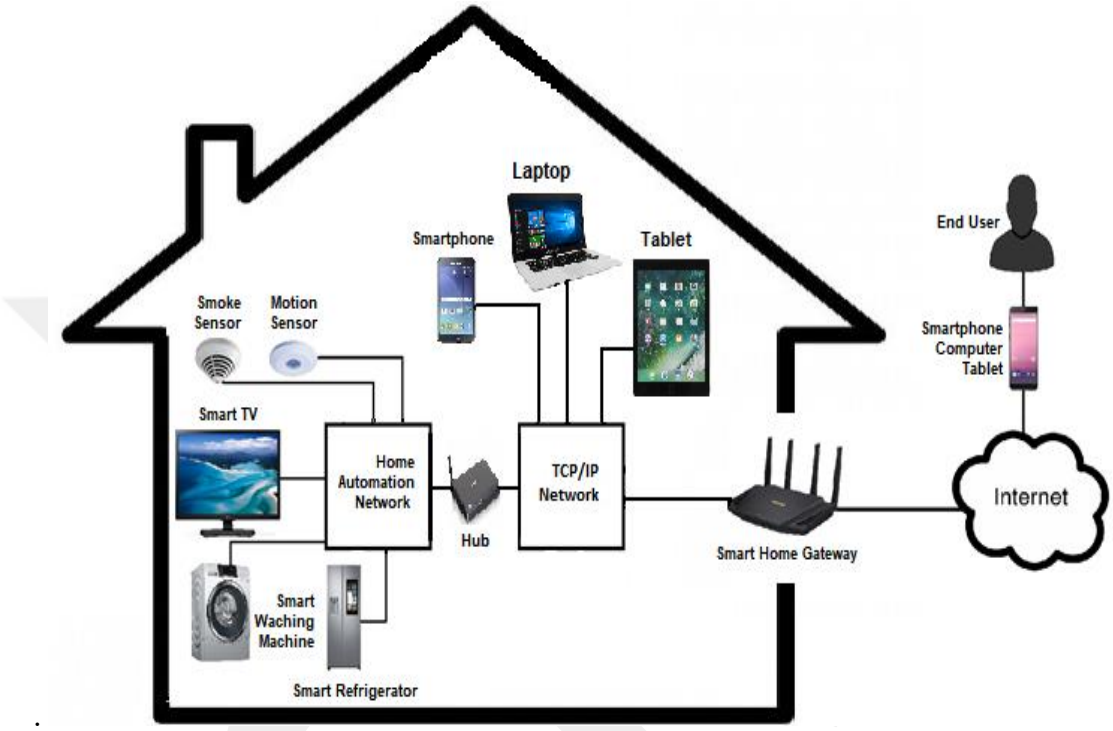


Figure 6.3 the Smart Home Structure

- **Actuators:** Their job is to carry out actions such as improving or controlling lighting, locking the door, closing windows, closing blinds, launching an alarm, etc. [154].
- **Home Area Network (HAN):** The smart home has two types of networks:
  - **TCP/IP Network:** This network usually consists of a combination of Ethernet and Wi-Fi wireless networking technology and uses the TCP / IP networking protocol. It enables multiple devices e.g, PCs, smart phones, tablets, etc. to connect to each other, and also to connect to the Internet. This network connects the devices with the Internet via a smart home's gateway. This network helps the homeowner to access, control and monitor his home from remote places.

- **Home Automation Network:** Most smart home devices have wireless connectivity, but at the same time they are considered low-power devices, which means that the Wi-Fi wireless technology used in networks based on TCP / IP is not suitable for them. So, the first generations of home automation devices developed to use Z-Wave or Zigbee wireless technologies. The key benefits of these technologies are that they are low in energy and less affected by building design, which makes their coverage greater. Because these technologies do not use IP addresses, the devices that do use them cannot directly connect to a TCP / IP network. This prevents the consumer from using his phone or computer to communicate with the devices and control them. To solve this problem, many home automation networks will require some form of hub or gateway. The function of this hub is to connect an IP-network to a non-IP network which enables the homeowner to control smart devices via his mobile phone internally or remotely.

- **Smart Objects:** They may include any device that uses electricity or batteries and provides services and has the ability to connect to a HAN. Smart devices can range from a coffee machine to a door lock. The next section mentions more types of smart home devices that may be present in a smart home.
- **Services:** Services are software applications located in the cloud or in a home environment. Responsibility for implementing automation, device management, decision making, etc. rests with these services. Consumers interact locally or remotely with the devices using these applications through their smartphones or tablets.

6.1.4. Smart Home Devices

Usually, a smart home includes several connected devices belonging to a variety of applications areas. However, the majority of connected devices that homes use are still computers and smartphones, which communicate via Wi-Fi through the home router. In addition to these types of devices, smart TVs are the second most popular IoT devices in

smart homes around the world, followed by printers, media boxes, and security cameras [157].

Any home device can be part of the smart home if it has at least one transducer (sensor or actuator) for interacting directly with the physical world and at least one network interface (wire or wireless) for interfacing with the digital world. Many smart home devices now provide functions that did not exist before, such as processing capability, data storage and network connectivity. These functions enable the smart device to possess new technological competencies and capabilities. Remote access, the ability to extract and transmit information, interact with the external environment, make decisions are examples of these technological capabilities [158]. The numbers and types of smart home appliances increase every day to keep pace with the needs of consumers. There are dozens of different smart home devices and some of the most popular smart home devices are known to be found in most smart homes are [159]:

- **Security Devices:** These products are used to protect the home from external risks such as intrusion and theft. These devices include surveillance cameras and lock systems (door, windows, garage).
- **Sensors**: They are used to detect and avoid threats to life or property, for example gas, water leak and smoke detectors.
- **eHealth Devices:** These devices have the function of medical examination as well as providing medical assistance when needed such as smart wristbands, portable Electrocardiography (ECG), pulse oximeters.
- **Measurement Devices:** Water meter, electric meter and gas meter
- **Heating, Ventilation and Airconditioning (HVAC) Devices:** They are used to regulate room temperature (cooling, heating) and air ventilation such as thermostats, climate control units or the ventilation device.
- **Light and Shadow Devices:** These devices are used to control the amount of light, such as light bulbs, awnings, and curtains.
- **Household Appliance:** cooker, coffee maker, dishwasher, washing machine, refrigerators and ovens.

- **Entertainment Devices**: smart-TVs, audio systems, gaming consoles, media players and wireless speakers.
- **Network Devices:** gateways, routers, network storage devices, mobile phones and printers

6.1.5. Smart Home Applications

Smart home provides consumers with multiple applications belonging to different fields. The primary goal of these applications is to make life at home more comfortable and to save effort, time and money by providing various important services, and among these applications [149],[150],[154]:

- **Lighting Control**

Smart home lighting systems consist of smart lights, controllers and sensors. When these systems detect the surrounding conditions such as the presence of residents or the amount of sunlight available, they automatically control the lighting according to these conditions. This automatic control includes turning on and off lights and controlling their brightness according to residents' preferences and activities or energy saving rules. Another benefit of this application is that it aims to save energy consumption and manage it in an efficient manner.

- **Appliance Control**

In the past, household appliances such as refrigerators, ovens and washing machines were stand-alone systems that were manually controlled with their own control system. However, with the significant decline in the prices of the transceiver chips, it made it possible to include those chips in many home appliances. This step gave the home appliances the ability to communicate and cooperate with others. As a result, many smart home devices have become available for use, for example smart coffee makers that can prepare a fresh cup for the homeowner as soon as the alarm goes off. Furthermore, smart refrigerators that keep track of expiration dates, make shopping lists or even create recipes based on ingredients currently on hand. The appliances control system also has the ability to control energy consumption, which reduces costs. For example, high-energy consuming

appliances such as washing machines and ovens could schedule operations during off-peak energy rates.

- **Entertainment**

Entertainment system include, for example, smart TV, a DVD player, with multimedia players such as tablets, smartphones, and MP3 players. Entertainment systems in smart homes provide connectivity, access to shared resources and distribution of content according to users' preferences.

One of the most important benefits that this system provides to families is what is known as monitoring. The system allows parents, for example, to easily monitor the type of entertainment their kids are having. All the parents need to do, is check their phone and they will be able to know the channels kids are watching, the websites they are visiting and the video games they are playing. Additionally, smart TVs connect to the Internet to access content, such as on-demand video and music, via application. Some smart TVs have the ability to understand sounds or gestures.

- **Safety and Security**

The security and safety system for a smart home is one of the most important applications provided by these smart homes as it provides services designed to monitor, detect and control security and safety threats. The importance of this system lies in saving the lives of the residents of the house from external dangers such as thieves and intruders and internal dangers such as fire and gas leakage.

Some components of the smart home safety and security system include smoke detectors, zone intrusion detectors, burglar alarms, surveillance cameras and smart door lock. For example, using smart locks and garage-door openers, residents can grant or deny access to anybody. These locks can also detect when residents are near and unlock the doors for them. As for smart security cameras, alarms and smart motion sensors, they enable homeowners to monitor their home when they are far away. Additionally, the safety and security system has the ability to notify the authorities when they have detected suspicious behavior.

- **Climate Control**

HVAC system can be controlled automatically in smart homes by using smart thermostat in order to provide a climate suitable for residents and at the same time saves energy. Smart thermostats allow users to schedule, monitor and remotely control home temperatures, for example by their phones. For instance, rooms temperatures can be regulated based on the presence of a resident in them. When residents are ready to go to sleep, the smart thermostat turns on climate controls devices in bedrooms and reduces or turn them off in the rest of the house. In addition, it turns climate control devices off when the house is empty and activates them before residents return to home. Smart thermostats can also report energy use and remind users to change filters, among other things. These procedures help reduce household energy consumption and reduce bills.

- **Assisted Living**

This application primarily aims to provide remote assistance and care to elderly, sick and disabled homeowners to help them live independently, comfortably and safely in their homes.

Wearables, other healthcare technologies and sensors monitor the elderly, recognize their activities and act accordingly. For example, when the system detects a person's wake up, it turns the lights on automatically. Moreover, when any unusual activity of the elderly such as his fall or injury occurs, the smart home notifies the emergency units immediately [150]. This system also provides medical monitoring for the elderly by wearing a smart bracelet. This smart bracelet monitors the vital signs of the elderly like heart rate, blood oxygen level, among others. If these vital signs are suspected of deteriorating, the bracelet sends an alarm to the emergency or the doctor to take what is necessary.

6.1.6. The Risks Facing the Smart Home

A smart home may be exposed to many risks that affect the services it offers to its residents, either by affecting their quality, using them against residents, or permanently stopping them. These risks may form as a result of an intentional attack with the aim of causing damage, or it may be an unplanned problem that occurs by chance. However, in

both cases, the smart home is affected in one way or another by these risks. Below are examples of some of these risks:

- **Physical Attacks**

Most appliances in smart homes can be physically damaged, or be attacked and stolen because of their financial value. These physical attacks may either weaken the functionality of smart devices or prevent them from fully functioning.

Smart devices such as smartphones, tablets, removable storage media, and computers that move in and out of the home are more vulnerable to physical attack, especially when they are outside the home. Smart homes may also have sensors or actuators distributed outside the home that are more likely to be vandalized or stolen than those indoors. An example is those located near doors and windows, inside a garden, or near the outside gate to a house.

When these devices were manufactured, they were manufactured on the basis that only their owner can access them, which ensures their security. However, this does not really happen. In reality, there are others who can gain unauthorized access to the home devices. This unauthorized access may result in downloading new programs on them that may be malicious, adding components to them that help spy, change their settings, or even extract cipher keys [152].

- **Disasters**

Among the dangers that fall under this heading are fires, floods, pollution, dust, erosion by time, lightning, water, violent physical movement, and unfavorable weather conditions. These disasters can seriously reduce efficiency or prevent the functionality of smart devices, reduce their age, or even completely destroy them.

- **Threats to Sensitive Information**

Smart home devices collect and store a large amount of sensitive information related to their owner and this increases the likelihood of them becoming a target for intruders. The devices' lack of systems that enhance security, such as the ability to encrypt data while storing or sending it, is an important contributing factor in the occurrence of these risks.

Sensitive information can be stored in both physical and digital media. For example, if the information is stored in a smartphone, this information may be lost or leaked if this phone is damaged or stolen. On the other hand, this information may be subject to eavesdropping, interception and kidnapping. Home appliances do not have as good resources as the processing capability and power (if they are on batteries) to use an effective security technology to protect the information. These limited resources do not enable the devices to use technologies to encrypt information and thus protect them from several attacks such as eavesdropping attacks, reply attacks, and MITM attack.

- **Failures/Malfunctions**

Like any device in life, smart devices may also malfunction for many reasons such as the end of their life or a sudden increase in electrical energy. In many cases, this malfunction will result in unavailability of smart home service. This unavailability may either cause slight annoyance, for example the inability to access the media, or it may lead to expensive damage, for example, damage to a refrigerator or doors that cannot be opened without repair.

- **Outages**

Power outages, Internet outages, or a malfunction in the home network leads to a breakdown of services that a smart home provides to its residents.

6.2. Smart Home Security

Over time, smart homes have become an attractive application for consumers, and it is expected that these homes will increase in popularity and become part of normal life within a few years [159]. This seems to be expected due to the many benefits and advantages of this application on people's lives. However, an important question must be asked: Is using the smart home application safe for us? The security and safety of smart homes has always been and remains the biggest concern for consumers. This topic is important, because it relates to consumer privacy directly more than any other application of the IoT. The privacy of people, their behavior, habits, contacts, data, pictures, and locations are all related to smart home security. For instance, hackers may spy on family activities using the integrated cameras and microphones in the surveillance system.

Many smart home apps handle owners' sensitive data related to their privacy and secrets such as photos, personal videos, health, financial information, and physical access information to the home. Therefore, providing protection for this information is what determines whether a smart home is safe or not [157].

Smart home security is related to the security of every technology used in it (devices, networks, software, hardware, operating systems, Internet, cloud services, etc.). Any weakness in any technology may affect the security of the smart home as a whole [152]. Avast, which is one of the largest security companies in the world, has examined more than 16 million smart home networks around the world and found that two out of five (40.8%) of smart homes contain at least one device that is vulnerable to cyber attacks, which may put the entire house at risk [157].

Smart homes contain devices such as security cameras and microphones that can, for example, be activated remotely by an attacker to monitor the homeowners' movements and activities as well as listen to private conversations [154]. Therefore, the disclosure and use of this information leads to severe consequences for their owners such as stealing their homes or even publishing their personal lives and photos for the purpose of defamation.

The biggest security threat a smart home faces comes from poor security in IoT devices. Unfortunately, many of these non-computer, non-smartphone devices — from door lock to refrigerators to alarm systems — weren't built with security in mind. Many smart devices can be compromised, including thermostats, ovens, locks, security cameras, and Personal Digital Assistents (PDAs). Whether people are using their smart alarm to wake up and send a request to a coffee maker to start preparing it, the truth is that cybercriminals can use this smart alarm to extract valuable personal data about family habits [157].

6.2.1. Security Vulnerabilities in the Smart Home

There are several factors that have contributed to making the smart home more vulnerable to attacks and security threats such as [155],[156],[160],[161]:

- high total cost of the system

- complexity of the system
- complexity of the user interfaces
- different communication protocols used such as Wi-Fi, Bluetooth, ZigBee and others [152]
- integration of many heterogeneous devices into the home automation system
- fixed firmware for many home devices
- constrained resources of home devices such as processing capability and low memory space [152]
- lack of reliable devices in the smart home
- lack of consumer awareness of how to configure and deal with smart home and enhance security in it
- poor configuration
- most smart home devices have little or no built-in security techniques
- easy access to smart home devices from the Internet

6.2.2. Smart Home Threat Types

Threats to smart homes can be one of two types; internal threat or external threat. The source of the internal threat is malicious attackers located near or inside the smart home buildings, while in an external threat, an attacker can attack only through an Internet connection. In both cases, attackers target either the smart home's infrastructure, or the information stored locally or in the related cloud services [156],[162].

Each threat includes a malicious attack in a passive or active manner depending on the aim of the attackers. In a passive attack, the attacker will attempt to eavesdrop on the available connections in order to obtain information without wanting to change this information. This type of attack is difficult to detect because it does not change data, but only learns something from that data. The information gathered through this attack can either be used to harm the user morally, physically, or financially, or it can be used to assist in carrying out an active attack. On the other hand, the attacker in an active attack will not only eavesdrop on the connection to steal information, but will attempt to impersonate a legitimate user in order to access smart home devices. Then he can control,

use, or even extract sensitive information from it. The danger of this attack is that it affects the user's privacy, the confidentiality of the service provided, and the integrity of the data [156],[162]. Also, an active attack is able to tamper with the information on smart devices in order to confuse their work and push them to make wrong decisions that result in wrong actions. An attacker can also combine two types of attacks together (passive and active) to get more effect. For example, by eavesdropping, an attacker could obtain the password to access the home network. Once an attacker gains access, he can simply perform a DoS attack. This attack will have serious consequences that may be related to someone's life, especially if it targets smart healthcare devices such as blood glucose meter [156],[162]. An attacker can also eavesdrop to obtain a home unlock / lock code, and the least he can do with this information is to change that code to prevent homeowners from entering their homes.

6.2.3. The Targets of Attacks on the Smart Home

A smart home can be vulnerable to many of the attacks discussed in Chapter 4, such as: eavesdropping, jamming, tampering, malicious code injection, replay attack, DoS attack, MITM attack, wormhole attack, sybil attack and many other attacks. The purpose of these attacks is to infiltrate the smart home network and compromise its devices. This, in addition to more dangerous targets that can sometimes lead to loss of life and property. This can happen when the attacker deprives the residents of the service provided by home medical devices, or prevents smoke detectors from working to warn of a potential fire or even tampering with electrical systems at home [150],[161]. Sometimes, cybercriminals hack thousands of IoT devices into unexpected smart homes such as refrigerators to create networks of infected devices known as bots to carry out attacks on other sites. This type of attack is common because of the ease of penetration of home appliances compared to the penetration of computers and smartphones [157]. The main targets of smart home attacks are listed below [5]:

- **Harm:** It causes damage to life, property, or both. For example, if the attacker hacked a smart door lock with an eavesdropping attack, the smart home could be broken into without needing to physically destroy the door itself. This may cause

the contents of the house to be stolen or the life of its residents threatened. Also, if the attacker can control a smart home device such as a thermostat, he will be able to manipulate the home's temperature. He can either raise or lower it, which affects the health and psyche of the residents.

- **Monitoring and Leaking of Personal Information:** The safety devices used in the smart home may be exploited to work against the homeowners if it is compromised. For example, an intruder may use sensors used to monitor children and resist intrusion, such as security cameras, to monitor the residents themselves and collect personal information about them. Then, the attacker can use this information to blackmail or discredit the homeowners. Also, the information that the attacker extracts from the surveillance devices enables him to know when the residents of the house are in it. This makes it easier for the attacker to schedule a home theft when the residents are outside.
- **Denial of Services:** Attackers can access the smart home network and use the DoS attack to prevent devices from performing their function and providing services due to the depletion of their resources through this attack.
- **Counterfeiting:** By MITM attack, an attacker can tamper with the data he obtains and make devices perform unwanted services from them, give false results or take wrong actions.

6.2.4. Potential Compromised Devices in the Smart Home

The factors mentioned in Section 6.2.1 can help an attacker to compromise at least one device in the smart home system, which will likely be the most vulnerable and the easiest to compromise. Once this device is compromised, an attacker can take a number of actions depending on the device's capabilities and functions. According to Cytelligence, a cyber-security firm, top five smart devices that made an impact on cyber security in 2019 are smart TVs, voice-controlled assistants, connected cars, connected baby monitors and cell phones. On the other hand, table 6.1 shows some of the most common and most vulnerable smart devices as well as some of their functions, and provides examples of the consequences of attacking them [41],[163].

Table 6.1 Hacked Devices, their Normal Functions, and the Targets of the Attacks

Device	Some of its Functions	Some Targets of the Attack
Smart Lock	• lock and unlock doors, windows, and garages even without a physical key, instead using a smart card, mobile device or web interface • record permanent and temporary users who are entitled to enter the home and sometimes define their own access schedules, represented in days and times • turn on alarms when breaking into the house to warn residents • lock automatically after unlocking for a specified period of time. This happens in cases where residents forget to lock the house.	• opening the door for strangers to enter the house • control the lock and deny home residents entry or exit from the home • change the lock password remotely • disturb the residents by operating the intrusion alarm when no intrusion occurs
Smart Refrigerator	• send an order to the online grocery store when there is a shortage of items in the refrigerator • record the expiration dates for the items in the refrigerator and alert residents the item's expiration date, so that they can consume them as long as they are still valid • prepare and send grocery lists to mobile devices for resident while they are near a grocery center.	• order a large amount of groceries online beyond the needs of home residents • destroy food in the refrigerator by manipulating the temperature by either raising it or lowering it to the highest possible level

Table 6.1 (continued)

Device	Some of its Functions	Some Targets of the Attack
Smart Coffee Maker	• prepare coffee based on the timer or make an order remotely • allowing residents to participate in the preparation of high-quality coffee by giving them the option to add a component or cancel a component as they like	• stop the coffee preparation process completely • make coffee without ordering it incessantly throughout the day • manipulate the coffee ingredients either by adding too much sugar or milk or not at all
Smart Game	• interact with its players in an educational way • owning a feature that enables it to receive game-controlled orders from parents remotely • provide remote video and audio access for parents	• record game players' voices and conversations with each other and leak these recordings online • connect with the game players for a purpose • scare game players by controlling or destroying the game, or even raising the game sound volume a lot to make it noisy • hacking the smart home network through the smart game to carry out other attacks

Table 6.1 (continued)

Device	Some of its Functions	Some Targets of the Attack
Smart Bulb	• it can be controlled by mobile app or a website • control the amount of light brightness according to the amount of daylight available • turn on or off as scheduled or according to the presence of the residents in the room	• turn the light on or off at inappropriate times • turn on all lights in the house to overload the power system, increase energy consumption, and raise bills • turn the lights on and off frequently, until the lamps are damaged
Home Gateway	• connect the smart home to the Internet • provide gateway functions like WAN to-LAN bridging, Network Address Translation (NAT), firewall	• disable firewall • steal credentials or personally identifiable information (PII) through the gateway • prevent data routing • redirect data toward hidden malicious paths

Most of the attacks listed in the table do not pose a serious threat to homeowners. However, once the attacker breaks into any of these devices, he will be able to infiltrate the system as a whole and this will help him carry out more dangerous attacks. For example, an attacker can remotely hack certain devices, such as a refrigerator, over the Internet and use them to access other devices in the home. It's easy for an attacker to do this because home appliances are usually connected to a single local network. For example, an attacker can now access security cameras distributed around the house and find out where the residents are. After that, he penetrates the smart lock and allows the

hackers to enter the house and at the same time disable any alarms that can alert the residents to what is happening. Another event that can be added to this scenario is that the attacker can use the post-hacking fitness tracker to monitor its owner, finds out about his daily routine and then gives this information to the hackers. This information allows hackers to determine when a house was broken into, for example as the owner goes out for a run. Another possible scenario is that the attacker takes control of many home devices such as surveillance cameras, speakers and microphones and uses them to monitor the residents. The attacker then uses what he gets from this surveillance to blackmail the residents in order to get money.

6.2.5. Securing Smart Homes

As much as homeowners care to protect their homes physically by buying locks and installing alarms, they should pay attention to protecting their smart home system. The importance of this is due to the observed increase in the number of attacks on smart homes over the past few years. For example, parents are very interested in installing stairs doors and safety locks indoors to protect their children from accidents. However, they do not pay the same attention when purchasing toys with the possibility of Internet connection for their children and ask whether these toys are hackable or not. Therefore, protecting and securing smart homes from potential attacks should become an important priority for consumers and manufacturers.

Home appliances are not strong enough in terms of security, such as computers, tablets and smartphones. Since home devices became connectable to the Internet, they have become an easy target for attackers. The smart home, as an application of the IoT, is vulnerable to the attacks mentioned in Chapter 4. Attackers compromise these devices to gain access to the other devices on the same network. When this happens, electronic thieves can access sensitive information such as identity, bank credentials, credit card numbers and other personal information .

However, who is responsible for protecting the smart home? Are they the manufacturers of smart home devices, homeowners, or Internet service providers? It seems to be a shared responsibility of all parties, because all the stakeholders of the smart home app will win

one way or the other if this app is safe. When the manufacturer makes its products safer, this increases the confidence of the consumer, which results in an increase in sales, spread and good reputation. On the other hand, when a homeowner contributes to making his smart home safer, he thus protects his privacy, secrets, and even his life from any danger his smart home might pose. If the ISP can help in this regard, it will lead to new customer acquisition and boost the confidence of previous customers.

The countermeasures mentioned in Chapter 5 will also be effective in the smart home app. However, in this section we will not repeat what was mentioned before about how to defend against attacks, but rather, we will try to make a smart home safer in another way. Our approach is to present more practical and more specific steps to be taken by smart home stakeholders (consumers, manufacturers, and service providers).

During our research on what role homeowners, manufacturers and service providers might play in making a smart home safer, we came up with a set of tips and recommendations that these parties could implement and they take it into account to reach the desired result. The next three sections are suggestions about the role the manufacturer, consumer, and Internet Service Provider (ISP) might play in making the smart home a safer place.

6.2.5.1. The Manufacturer Role

During companies competing with each other to produce the first generation of smart devices and put them on the market quickly and at a reasonable price, the provision of security for these devices was neglected. These companies did not pay attention to the topic of making smart devices more resistant to hacking, electronic or physical attacks, but rather made it their last concern [157]. The pressure on smart device manufacturers has increased by several governments to make their products more secure. Some governments around the world have emphasized the importance of protecting the people who use smart devices and their information. As some of these governments have already issued laws and regulations to determine the level of security that should be available in smart devices. Of course, some companies were quick to pay attention to this issue, while some have slowed. The growing demand for smart devices has also created a pressure. For these reasons, it has become a priority for manufacturers to ensure that their products

have appropriate security measures to protect the people who use them. If some companies do not pay attention to this problem, they will lose the confidence of consumers, who will turn to other companies that have made consumer safety a top priority. In addition to the foregoing reasons, it is the company's reputation and consumer requirements that have prompted manufacturers to devote extra effort for ensuring that the product has adequate levels of safety [164].

Any step that manufacturers take to improve the security of their smart devices will surely help their customers maintain their security and privacy while using these devices. However, what are the measures and procedures that might help manufacturers make their smart products safer? During our research on this topic we found some useful information in this regard and extracted from it some voluntary recommendations and advice. This information is included in some international IoT security standards reports and documents such as those mentioned in Section 5.1. Smart device developers can also take these recommendations and tips into consideration when designing and manufacturing their products for consumers. Some of these recommendations that may help mitigate cybersecurity risks and improve product quality overall are listed below [158]:

- **Create an Effective Team**

The smart device design and manufacturing team should include information security experts in addition to traditional engineers. These experts will take care of the security aspect from the design stage through to the manufacturing stage. While designing any smart device, this team must answer some questions such as:

- Who is the expected user?
- How will the device be used? For one or multiple purposes?
- What physical environments will the device be used in? (For example, indoors or outdoors)
- How will the IoT device interact with the physical world?
- What will the nature of the IoT device’s data be?
- What are the security requirements for the IoT device?

- What are the possible ways in which an attacker could misuse or endanger the device?
- What are the means that may assist the device in defending against the attacks that it may be exposed to?
- What are the resources needed to make these means effective, and can these resources be included in the device?

Having answers to these questions greatly helps the design team to determine the security risks that smart devices may be exposed and their countermeasures. After identifying the risks and their countermeasures, the team should try to integrate these measures into the smart device as it is being designed and from the start. These countermeasures are defined as security capabilities, features, or functions that devices provide through their own technical means [158].

In addition, it is very important that the team maintains an updated and accurate inventory of all IoT devices and their related characteristics throughout the device's life cycles. The team will use this information for risk management, research and development.

- **Taking Security Requirements into Consideration**

The design team must consider security requirements when designing and developing any smart device such as secure authentication, availability and confidentiality. It is important to manufacture a smart device that meets these requirements even if it increases its cost, since security is more important than cost. Among the most important security requirements:

- **Authentication:** A smart device that supports the authentication process, such as two-factor authentication, must be designed and manufactured [150].
- **Confidentiality:** The smart device must have the ability to maintain the confidentiality of the information stored in it such as access credentials and security-sensitive data. Embedding a fairly good encryption technology is an important requirement that every smart device should have.

- **Secure Communication**: In the past years, many secure communication protocols were introduced like IPsec, SSL and HTTPS so, it would be a good idea for smart devices to use these secure protocols.
- **Physical Protection:** Most of the time electronic devices are left unattended, subject to tampering attacks. Thus, physical protection is an important requirement for smart devices. These devices must be made strong against tamper attacks [150].

Some companies, such as Develco Products company, have begun to take these requirements into consideration and have designed smart devices according to them. For example, the devices from this company use of installation codes, certificates and pre-defined keys to authenticate the connection when they attempt to join a network. Furthermore, after the devices have connected to the network, the gateway transports the information across the different secure wireless protocols [165].

- **Security Level Analysis According to Some Standards**

To address security risks, many government agencies around the world have set the levels of security required to adequately protect the product and the end users. Some documents have been written and published that outline high-level security requirements for consumer devices connected to a network infrastructure, such as the Internet or a home network. These documents provide basic guidance for companies involved in developing and manufacturing consumer IoT devices. They contain a set of provisions that must be met when designing and manufacturing smart devices to achieve the required level of security. Among these documents are ETSI TS 106445 V1.1.1 (2019-02) (CYBER; Cyber Security for the Internet of Things for Consumers) and GDPR - General Data Protection Regulation [164],[166]. Smart home devices manufacturers can look at these documents and use them as a reference for safe smart home design.

- **Providing New Features**

Providing smart devices with some special features that were not previously present in them may help enhance the security of these devices. These include: remote connection authentication, VPNs between end users and the homes they are connected to, and protection against malware.

- **Using Unique Default Passwords**

Companies usually use the same default password for all devices of the same type and version. They then document this password in the device's operating manual. Most people who are interested in technology know this, making it easier for hackers to obtain passwords for smart devices.

If the consumer does not change the default password for his smart device, which is what happens more often, the hacker can use this password to hack the device. To make hackers job more difficult, manufacturers must use a unique default password for each smart device. At first glance, this seems like a difficult task, due to the large number of smart devices being produced. However, implementing this step will result in a huge benefit that will overwhelm any difficulty. Encouraging users by manufacturers and marketing companies and reminding them of the need to change the default passwords to another, is one of the steps that may help secure more smart devices.

- **Providing a Point of Contact between the Manufacture and the Consumer**

The manufacturer or smart device marketing companies must stay in contact with the consumer. It should provide an easy means of communication that a consumer can use to send any notes or reports about weaknesses that a consumer may discover while using the smart device. Using these reports, the manufacturer can fix these vulnerabilities and send solutions to other consumers. In addition, the consumer may seek advice from the manufacture through this communication channel when something goes wrong with the smart device. In this case, the manufacturer must provide the information to the consumer in simple language that does not go into technical details that the consumer may not understand. It is also important for the manufacturer to ensure the integrity and correctness of the information exchanged through the communication channels so that it is not tampered with.

- **Providing Information to Consumers**

The manufacturer or smart device marketing companies should also provide information to consumers about the smart devices that they sold to them, and this information should cover:

- The period of time during which the manufacturer is expected to provide support, advice and maintenance to the consumer
- Cybersecurity services that a manufacturer can provide by a related device, service, or system
- Information that the consumer should know about the device configuration and capabilities, such as information about device software, firmware, hardware, services, functions, and data types in the device
- Notifications that should be sent to the consumer about software and firmware updates as soon as they become available
- The steps that the consumer must follow to dispose of the device when it is no longer needed, so that this does not expose any information that was in the device

- **Keeping Software Updated**

When the manufacture updates the software of any smart device for any reason, for example to correct some defects, he must notify his customers of this without waiting for the customer to request it. The manufacturer may use the previously mentioned communication channels as a means of informing the customer of these updates. Another step is to make these updates easy to access and implement on the regular customer. The manufacturer can also encourage customers to implement these updates by providing a simple explanation of the importance of these updates and their benefit.

Since some smart devices may stop working during the update process even for a short period, which may cause a problem for consumers, the manufacturer must take into account that the smart device must continue to perform its work during the update process.

- **Minimizing Exposed Attack Surfaces**

After producing any smart device, manufacturers must reduce the ports that attackers can use to attack these smart devices. For example, unused programs, network ports, and hardware access methods (such as open serial access, ports, or test points) should be closed. Also, the code in the device should be limited to only what helps it do its job. In addition, the smart device must have the necessary minimum privileges that help it provide

the service intended for it. All of these are important to prevent the hacker from finding any port that he can use to hack a smart device.

- **Making it Easy for Consumers to Delete Personal Data**

When ownership of the device is transferred or when the consumer wants to dispose of the device, the manufacturer must provide clear instructions to consumers on how to permanently delete their personal data from the device.

- **Making Installation and Maintenance of Devices Easy**

The manufacturer must provide advices to consumers on how to safely set up, install and maintain their devices, for example through clear, easy-to-follow steps written in a manual accompanying the product or through the company's website.

6.2.5.2. The Consumer Role

There is also an important role for consumers in protecting and securing their smart homes even if most of the vulnerabilities are due to security flaws during design and manufacturing.

All security measures taken by manufacturers will help consumers secure their homes. However, the need to maintain the security of smart home devices is not the responsibility of manufacturers alone. Consumers also have a responsibility to protect, secure, and make their smart homes safe from attacks and threats.

Due to the increasing popularity of IoT devices, such as Smart Lock or Smart Thermostat, there needs to be greater awareness among consumers of how to use and protect these devices. This will help consumers contribute effectively to securing their smart homes and help mitigate the risks that they would be exposed to if not properly secured [157].

Some countermeasures aimed at preventing or mitigating these attacks are helpful in this case [149],[150]. In the previous chapter, several countermeasures were generally discussed that protect IoT system from attacks they may be exposed to. This section will explain the actions the consumer must follow to protect his smart home from attacks. In other words, this section will be an answer to the question: What should the consumer do to protect his smart home [163]? The following points or tips are written to serve as an

easy-to-follow guide for ordinary people who care about the safety of their smart homes. Therefore, they can use this guide as a first step towards a safe smart home.

- **Buy the Best Smart Home Appliances**

Before purchasing any smart device, the consumer must do some research and review feedbacks. He should try to find the best types of smart devices, especially with regard to the security aspect and features that help to update and enhance that aspect. The consumer must know what kind of information these smart devices collect and store, and the protection measures related to protecting this information.

There are several companies that provide a variety of smart home devices from which the consumer can choose such as Amazon, Apple, Philips, Samsung and many others. These companies offer their products on their websites, explaining the features, properties and prices of these smart devices. Sometimes delivery and installation services are also offered depending on the location of the consumer's home. The consumer can simply search the Internet with any browser to find different products and compare between them to choose the best one. It should be noted that there are many sites that assist the consumer in this confusing selection task such as saftey.com and pcmag.com and many others. These sites offer the best and most recent smart home products from various companies. An important rule that can be followed by the consumer is that it is not necessary for him to buy all his smart home appliances from one company, but rather he chooses according to his security needs, money and others.

In addition to all of the above, before purchasing any smart device, the consumer must take into account customers' feedback. This helps him to check if the devices have any safety faults or if they have experienced security incidents before. Because unfortunately, many IoT devices are produced regardless of security protection, so consumers have to wait before purchasing and choose home appliances for their home.

- **Map All Connected Devices**

The consumer has to keep a list of the devices that connect to the home network. This will make it easier for him to discover vulnerabilities in his smart home and assess the security

measures that need to be taken to enhance security. Also, this evaluation helps the consumer in taking the decision to replace or upgrade the devices.

Another action that a consumer can take is to keep their smart devices at a minimum by disconnecting the devices they do not use or need because the more devices the consumer adds to his home, the more vulnerable it becomes. Any device connected to the router could be a potential entry point for attackers that they could use to access other devices on the same network. For example, if the use of a smart refrigerator or smart light bulbs is not necessary for the consumer, then he should continue to use the traditional ones. Because if attackers gain access to the smart refrigerator using its default login credentials, they can use it to control more devices connected to the same network, such as smart home speakers or a smart TV [157]. These procedures will keep the level of threat exposure low at home. In addition, they will reduce the points that an attacker can use to break into a smart home and make it easier for the consumer to locate the breach.

- **Disable Features and Functionalities that may not be Necessary**

After the consumer chooses only the smart devices he needs, he should check the features and functionalities that are enabled in those devices by default. IoT devices come with a variety of services such as remote access, which are often enabled by default. If the consumer does not need this service, he should disable it so that the attacker cannot exploit it to access the device remotely. More functionality simply makes a device more vulnerable to a cyber attack.

- **Change the Default Username, Password and Settings of the Smart Devices**

Many smart devices are controlled through a connected mobile application, and the customer will need to set up an account for each of these devices. He interacts with his home devices first by entering a password and username as a form of security.

For example, the SmartHQ app is an application used to control devices such as smart refrigerator. This application can be used on iOS or Android smart phones, and is available to download for free from the Apple App Store or Google Play. Once downloaded, consumer can open the SmartHQ app on his smart phone and sign in or create a Wi-Fi account for the refrigerator. The consumer uses the default password in his refrigerator

instruction booklet to enter its welcome screen. This password is the same in all refrigerators of the same type and the same brand.

Many consumers do not change the default settings of the device such as password, username and device name, despite widespread warnings for them to do so and advise them to choose strong and unique passwords. Over 69% of vulnerable devices remain at risk due to default or weak access credentials, which provide hackers with easy access and an opportunity to take control of these devices [164].

Any attacker can simply obtain the instruction manual of the smart devices and use the default passwords in them to penetrate these devices and carry out a widespread attack. Hence the importance of changing default passwords and choosing strong alternative to them that are difficult to guess is appear. Moreover, the consumer should not use the same password for all of his home devices. Because if one of these accounts is compromised and the password is exposed, the hackers have passwords for all the other accounts belonging to the other devices.

- **Update Firmware Regularly**

Firmware is low-level software that runs on hardware and is included in read-only memory (ROM) which is critical to device operation [158]. For example, a printer firmware is the program stored inside of a printer that allows it to receive information from the computer and turn it into a printed image. Hackers target the firmware of home devices, especially the old ones, as they are weaker and easier to penetrate. Old software in smart devices lacks the latest security measures and patches, which makes them riddled with security holes. This leaves owners of these devices vulnerable to hackers who know how to exploit vulnerabilities. The attackers use old software as a place to include malware and hide other malicious code that could endanger the system. For this reason, the customer should update firmware. Regular firmware updates are fundamental to keeping the devices in home secure [157]. These updates are useful for fixing security vulnerabilities and other errors as well as adding new features to the device that improve its functionality or performance. Firmware updates are expected for everything from car stereos to smart light bulbs. Most companies put these updates over the Internet, and many

devices regularly check for new firmware and automatically download and install it. If the device does not have the automatic update feature, the consumer should visit the manufacturer's website to download firmware updates and install them manually or uses an application on his smartphone. For example, consumer can update the smart TV by using its remote control then he moves to Settings, Support, Software Update, and then selects Update Now. New updates will be downloaded and installed on his TV.

Update firmware is important, so it should be a priority for the consumer and he should not ignore or postpone it. Because releasing a new update by the company often means discovering a new security vulnerability in the device that has been exploited by hackers to launch an attack on the device. Therefore, the consumer must update the firmware immediately if he does not wish to expose the device to penetration by exploiting the errors that have not been fixed. Unfortunately, 59.1% of users worldwide have never updated the firmware despite the importance of this procedure [157].

- **Use Authentication Mechanism**

Strong passwords and two-factor authentication are a vital part of the security steps that homeowners need to take when protecting their smart homes [157]. Authentication is important because it enables consumer to keep their home networks secure by permitting only authenticated entities to access home devices and resources.

The consumer can use two-factor or biometric authentication, which have some reliable options that provide extra layers of security, when his devices allow these options.
For two-factor authentication, the consumer usually uses a strong password as the first factor and, for example, a one-time six-digit code as the second factor on the services that support it. This code can be got via text message or a specialized smartphone app called an "authenticator". Therefore, even if the hacker managed to steal the password, it is unlikely that the hacker would hack the consumer's phone as well in order to obtain the code. On the other hand, some methods of biometric authentication can be used in smart home environment. This type of authentication includes fingerprint, eye scanning, voice and facial recognition. The biometric authentication methods are used by people to obtain

access to a wide range of their smart devices. It is also difficult for any hacker to forge this type of authentication as it is impossible to match two pieces of vital data.

- **Secure the Home Wi-Fi Network**

Although the era of the manufacture of smart devices is still in its infancy, many of these devices were produced, which differ greatly from each other in terms of style, programs and design. Therefore, trying to secure each device separately will be a very complicated work. The only reasonable solution is to protect them as a group, by protecting the network that connects them and which is considered an infiltration point for attackers. For example, there are not many smart TV antivirus programs that can be used to protect against the malware, but the home Wi-Fi network can be protected so that malware cannot attack the TV.

The home Wi-Fi network connects the home network to the home gateway and from there to the Internet. This network must be protected because it is the way or the route that hackers use to access smart devices in the home. There are several methods that a consumer can use to protect this network which include:

- Use a strong password to protect the router. That is because, the router usually is either unsafe or uses a generic password like "admin", which makes it easier for hackers to hack into it and access the devices connected to it.
- Disable the access to the router from the Internet by router administration screen. Most home consumers do not need to change router settings when they are outside.
- Use a strong Wi-Fi encryption method to protect data from being detected even after it has been captured by attackers. Therefore, the consumer should use the encryption methods in the settings of the home router. The most common methods are the Wi-Fi Protected Access (WPA) and WPA2.
- Change the router's Service Set Identifier (SSID) from the model-specific name to any other name to make the home network finding process somewhat difficult for hackers. For example, the consumer should not stick to the name the company gave to the home router, which often contains the brand or model. Instead, he should give it an unusual name that has nothing to do with its title.

– Use a network firewall, either inside the router or software that can be installed in peripheral devices. Most routers at home act as a firewall to constantly monitor traffic and prevent unexpected or unwanted traffic specifically. In addition, the consumer can install VPN in his router. In this case, the consumer ensures that all data is encrypted when it leaves LAN.

Recently, specialized devices or technologies that protect the smart home network have appeared on the market. Therefore, the consumer can buy these technologies and use them in his smart homes because of their effective role in protecting the network. These devices are connected to the home router and act as gatekeepers for the home network [154]. Examples of these devices are:

CUJO: It is a smart device that provides a firewall combined with antivirus and anti-malware protection, protecting the home network from phishing, scammers, and hackers. Once connected to a home router, the CUJO monitors everything that comes in and out of the home network. It also prevents the home devices from sending out information that should be private. This device also scans all data entering home network for viruses and malware, and the detected threats are automatically eliminated. Furthermore, CUJO is automatically updated to keep itself current with the thousands of new security holes that appear every month.

Dojo: Like CUJO, Dojo also connects to the home router. Once connected to a home network, the Dojo can automatically detect the connected devices, monitor and analysis their traffic and how connected devices behave. If Dojo detect any suspicious activities in the network, it stops them and send notifications on these activities to the homeowner by the Dojo smartphone app. This device uses lights to indicate network safety status. Green light means that everything is OK, yellow light means that a risk has been detected and taken care of automatically. A red light indicates that action must be taken by the owner against this risk.

Keezel: It also connects to the home router but it is different from the mentioned devices previously. Once connected, Keezel becomes a Wi-Fi repeater as well as it uses VPN technology to protect data from threats. VPN technology create a

secure tunnel between the home devices and the router. The data sent through this tunnel will be encrypted and protected and most of the time it will be invisible to any potential threat.

- **Replace Outdated Routers**

The home router is the front door of the smart home and is like any front door, it must be solid and equipped with strong locks to stand up to any attack. This router is the primary component in any smart home and act as a gateway that connects most smart home devices and makes them connectable to the world outside the home. However, routers are the weak entry point to many smart homes. So, if the home router, for example, is hacked or badly configured this allows attackers to access the network and gain control over most of the devices connected to it [157]. Therefore, building a more secure smart home starts with the router.

Most homeowners use the router provided by their ISP, but many independent companies also sell routers that may provide more protection than a regular router. Good for the consumer to find the safest router on the market. Even if the consumer uses a safer router, this does not prevent changing the router after a while and replacing it with a newer version, just as it does with all other electronic devices such as computers and smartphones. The emergence of a new version of the router means the emergence of newer protocols, technologies, components, and features that may help protect the router and its connected network from threats.

- **Split Up the Home Network**

In December 2019, the FBI warned that "your fridge and your laptop should not be on the same network. Keep your most private, sensitive data on a separate system from your other IoT devices."

The consumer must create more than one local network in his home and connect devices to these networks according to the importance and sensitivity of these devices. For example, he can assign a network to computers, tablets, printers and smartphones used in Internet banking, shopping, and general web activity; The other can be for the smart

devices. Partitioning can also be according to how vulnerable these devices are against attack, so that devices with more vulnerability are isolated from other devices [149].

To separate home networks, consumer can use, for example, Virtual Local Area Networks (VLAN) and assign different IP addresses to them. Also, separation can be done physically using more than one router. Therefore, if one network is compromised, the malware that infected that network is unlikely to jump and penetrate devices on other networks. This method helps limit the spread of any attack and prevents it from hitting the entire smart home system.

- **Set up a Guest Network**

Most home routers support guest networks, which use a different password than the main home network. This network often provides limited access to smart home resources and services. The consumer must have a private network for visitors, friends and relatives so that this network is separate from the main home network connected to their IoT devices. By doing this, the consumer can clearly determine who has access to the network and what resources he can use. Among the advantages of this network is that it allows guests to connect to the home network without the ability to access the personal devices of the homeowner.

- **Avoid Public Wi-Fi Networks**

A consumer sometimes needs to access and manage his home network when he is away from home. However, he should reduce as much as possible the use of public networks for this purpose, such as those in airports, hotels, cafes and shopping malls. If the consumer is forced to do so, he should use a VPN. For example, Norton Secure VPN offers a number of privacy and security features for public and home Wi-Fi. The VPN can hide the IP address of the user and block its location, allowing him to send and receive information more privately on public Internet networks [167].

- **Keep the Smartphone under Sight all the Time**

The consumer must be careful not to leave his smartphone unattended, especially if he uses it in a public place. Besides containing the consumer's private information, the smartphone contains smart home management software and passwords for that. Also, the

consumer, especially in crowded places, should turn off Wi-Fi or Bluetooth if he does not need it, because some smartphone brands allow automatic sharing with other users in close proximity.

- **Install Malware Protection**

Smart home devices are controlled by applications that are installed in smartphones, computers, and tablets. If these devices are hacked, the hackers will have the ability to control smart home devices. For this reason, it has become important for consumers to protect their computers and phones with the latest anti-malware programs.

- **Use LAN if Possible**

Despite the spread of wireless networks, they suffer from problems in terms of noise, interference and the ease of interception of the information that is exchanged through them. For these reasons, it is better for the consumer to use wired networks if possible, to connect the largest number of devices to the central hub. This reduces the chances of hackers to capture information. In addition, the wired connection prevents signals interference from high-bandwidth devices such as video streams or security cameras.

Although this solution is very useful, it is difficult to implement, as most smart homes use wireless or hybrid networks of both wired and wireless types, which makes securing home networks more urgent.

- **Prevent Smart Devices from accessing the Internet**

One of the most important services that the smart home provides is to access smart devices inside the home, via the Internet. However, this feature makes these devices vulnerable to attacks by remote intruders. If the consumer is not interested in this feature, disabling it will improve security significantly. Even if the homeowner has the advantage of controlling his smart devices only from inside the house, this house is still considered a smart home.

- **Seek Professional Aid**

There are some smart home system vendors that offer smart home system installation and remote monitoring as part of the package. Often this is done by security experts or experts

in smart home systems. The consumer should take advantage of this feature if it is offered to him or even look for sellers who offer it to buy their products. This feature provides an additional level of protection, as it provides active monitoring of the smart home system for any signs of unusual behavior. It is also used to identify problems when they arise and notify the homeowner to deal with them himself or by a specialized team.

- **Check IoT Devices already on the Home Network**

The consumer should check their smart home devices, and take some time to check if there are new releases on these devices. New releases often contain new functions and features that may help enhance the security of these devices. Therefore, consumers should replace old devices with new ones whenever possible.

- **Clear Personal Information**

Sometimes, the consumer decides to discard the smart device, either because it is not for him, because it is defective, or because he wants to replace it with a newer version. In this case, the consumer should erase his personal information stored in the device by performing a factory reset of the device. By returning the device to its original settings, consumers will delete all their personal data from it, which means that no one can exploit this information to use it in a malicious way.

- **Use the Factory Reset Procedure**

A consumer should use the factory reset procedure when he suspects or believes that a strange person is controlling a device inside his home. This prevents the hacker from obtaining the information stored in the device or using it to infiltrate other devices or use it to launch an extended attack on other targets.

- **Ask for advice**

If the consumer becomes aware of a security incident of a smart device of the same brand of his device, whether through the news or the Internet, he should contact the manufacturer for advice.

6.2.5.3. The ISP Role

ISPs are companies that provide a homeowner with Internet access services. Although the biggest responsibility rests with the manufacturer and the consumer in protecting the smart home, there may be a role that an ISP can play in this regard.

The ISP can apply a number of controls to its infrastructure such as firewalls and IDS in order to maintain availability of the service, which can be considered, indirectly, as "protection" for its customers. On the other hand, it can provide customers with a router that includes similar functions to enhance security in the smart home. These routers may also contain anti-virus / malware protection services which is important in regards to protecting IoT devices that cannot really defend themselves. Network Address Translation (NAT) service provided by the router can also play a role in monitoring traffic to and from the network, which allows to a large extent in detecting some abnormal behavior in the network. Additionally, NAT allows for stricter control of access to resources on both sides of the router.

In fact, the ISP does very little in the matter of providing security for smart homes, and it is often nothing more than built-in antivirus, and some basic port blockers, and that is it. There are several reasons the ISP takes as an excuse not to play a major role in providing security. From an ISP's perspective, these reasons can affect their credibility and reputation and undermine customer confidence in them. The most important reasons can be summarized as follows:

- **The Impact of Security on Privacy:** Some of the methods used to provide security are to monitor user surfing on the Internet. They also analyze the traffic content in depth and record all activities for later analysis. This could open up a discussion about whether ISPs can use this data for other reasons which is a concern to Internet privacy advocates.
- **A Difference between Censorship and Providing Security:** Some users may feel that censorship by the ISP limits their choices and steals their freedom.
- **Everyone is Responsible for his Mistakes:** ISP cannot be held responsible for users' mistakes because they cannot control their user's actions. Even if ISP have

the best security controls in the world, their users can still do wrong things that make them get into trouble.

- **Define Boundaries:** What are the limitations of the ISP in the context of providing security? Should they monitor their customers' traffic? Should they make a firewall? Should they enable IPS to prevent exploits? Should they scan client networks for vulnerabilities and block suspicious devices? Creating regulations to prevent ISPs from overstepping their limits and powers will be a huge challenge.

This chapter provided a comprehensive answer to the fifth research question related to the role of every stakeholder in the smart home application to make this application more secure. This chapter defines the role of the manufacturer, the consumer, and the service provider, and what measures can be taken by them to increase the security of the smart home.

At the end of this chapter and throughout all of the previous chapters, we have raised security issues in IoT technology: their causes, consequences, attacks targeting, and how to resist these attacks. Finally, we provided a realistic example using the smart home app and explained what these security attacks are and what practical steps can be taken to resist them. In the end, we have to write some kind of conclusion for this topic, which is represented in the next chapter.

CHAPTER 7

CONCLUSION

The emergence of the Internet of Things (IoT) is the beginning of a new era of using technology for the benefit of people. The IoT collects information from the environment around people and translates this information into services that it provides to them. The main goal of these services is to make human life more comfortable, efficient and effective.

The IoT can be defined as a system consisting of a group of things that have the ability to collect and transfer data over a network at anytime and anywhere with anything and anyone without the need for human intervention. Each of these things should be smart and have their own unique identifiers. Computers, machines, home appliances, animals, and people can be among these things.

In the past decade, IoT technology has spread predictably in modern society due to the various and useful applications it has provided. Among these applications are smart healthcare, smart cities, smart transportation, smart home and many more. In addition to all the applications and benefits it provided and continues to provide, the IoT has proven its effectiveness during the COVID 19 pandemic. It played an important role in limiting the spread of this epidemic as it provided many services to its users from their homes, thus reducing the need to go out. During COVID-19, the IoT has played an important role in aiding the healthcare system in several ways. For example, the IoT has been used to obtain remote medical consultations, digital diagnostics, and remote patient monitoring. In addition, The IoT has been used to track and monitor people infected with COVID 19 through networks and connected devices such as their phones or smart bracelets. Smart bracelets were also used of to monitor users' vital readings, such as temperature and blood

oxygen levels. In the event that there is any suspicion of the existence of symptoms of Covid 19 disease, these smart bracelets send these readings to the emergency center to follow up on the matter.

The spread of the IoT and its handling of information that is often considered sensitive and personal has made it a target for cyber attacks. These attacks aim to steal information, tamper with it, or deny people access to it. This targeting of the IoT, if it continues without solutions, will undermine people's confidence in this technology and limit its spread. Especially since some of these attacks are considered very dangerous as they may harm people's lives or money.

From this standpoint and the importance of this technology in people's lives, we chose the topic of this thesis. The main focus of our thesis was to highlight the importance of security issues of the IoT, with an emphasis on some security attacks and their countermeasures.

In this thesis, we have provided, first of all, an overview of the IoT that includes many of its aspects, from its definition to the applications it provides. This part was important as an introduction to the thesis, making it easy for us to understand what the IoT is, its benefits, components, and how it works. Then we shed light on the importance of security in the IoT and what will happen if this aspect is neglected. We provided some examples of situations that occurred in real life where insecurity in the IoT caused various threats. We also discussed the reasons that made it impossible to use known and adopted security technologies in information security to secure the IoT. In addition, security requirements such as confidentiality, integrity, authentication, etc., which must be available on the IoT in order to say that the IoT is a safe system are discussed.

We have further discussed the most common security attacks against various IoT layers including the perception layer, network layer, and application layer. Then we highlighted some of the proposed countermeasures that have been taken to resist the attacks and limit their effects. We first reviewed what is known as general countermeasures, which are the least that can be done to ensure a reasonable level of security. We have followed this by presenting some effective methods and means proposed to defend against each attack separately in an attempt to provide as much information as possible in this regard.

The final part of our work focused on examining the security risks of one of the most popular IoT applications, the smart home. We have identified some malicious targets that a smart home may be exposed to. We also provided some recommendations and advice that IoT stakeholders can use to build a more secure and robust system.

Our thesis contains some limitations that must be mentioned. Firstly, some of the topics could not be covered with all details since we intended not to give to much technical details, and also, this will increase the length of the thesis. Even now, it can be considered quite long in terms of number of pages, due to the fact that this topic is a huge topic. However, interested readers can access detailed information through the given references. Second, our work is limited to information collected from published documents. It does not include any practical experiences or data collected from users, manufacturers or experts. Third, we cannot claim that the given countermeasures can be implemented practically on any IoT applications and can protect any kind of IoT attacks. Notice that this is a hot topic which needs more research and experiences to become more mature. However, we believe that this study provides valuable information to secure IoT applications.

In our study of this topic, we attempted with great interest to answer the research questions we asked in Chapter 1. This study allowed us to analyze these questions, understand them and find answers to them, which then helped us to conclude several points, which we explain below:

- Our first research question was “Why is it so important to secure the IoT?”. This research question is discussed in Chapter 3 and 4 in detail. Considering the explanation given in the given chapters, we conclude:
  - Security is one of the biggest challenges facing IoT technology, which greatly affects consumers' confidence in and use of it.
  - IoT security is an important research topic that needs continuous research and development.

  - The development and spread of the IoT is closely related to the security issue. Therefore, security should be viewed as a top priority and no effort should be spared in the search for new means and technologies to achieve it.
  - Any complacency in the matter of IoT security can have dire consequences that may affect the lives of individuals and societies.

- Our second research question was "Why is it not possible to use known technologies to secure and protect information in order to protect the IoT?". This research question is discussed in Chapter 3 in details. Considering the explanation given in the given chapter, we conclude:
  - Due to the huge number of heterogeneous things related to IoT technology, it makes it difficult to use known information security methods to ensure the security of the IoT. This heterogeneous nature of IoT components has resulted in no single security standard or policy that can be applied to the IoT environment as a whole to provide security in it.
  - The lack of adequate resources in IoT devices, such as storage capacity, power source, and computing capability, has made it impossible to use traditional security technologies to protect them.
  - All the security measures and technologies proposed to protect IoT should not consume its resources, but rather be lightweight to fit IoT technology and at the same time be effective against attacks.

- Our third research question was "What are the basic security requirements that must be met in IoT to be a secure technology?". This research question is discussed in Chapter 3 in detail. Considering the explanation given in the given chapter, we conclude:
  - IoT security is related to information security, devices security and network security.
  - Confidentiality, privacy and trust are among the most basic security requirements that must be met in the IoT.

- Any security solutions and technologies designed or used in the IoT environment must be able to ensure the confidentiality and privacy of users and objects.

- Our fourth research question was “What are the most common attacks against the IoT and how can they be prevented?”. This research question is discussed in Chapter 4 and 5 in detail. Considering the explanation given in the given chapters, we conclude:
  - The development of IoT is accompanied by the development and invention of many attacks of different types and objectives.
  - The lack of security technologies in IoT devices has made them easy targets for many attacks targeting the devices themselves or the information they contain.
  - Most of the vulnerabilities that make the IoT vulnerable to attacks stem from vulnerabilities in the technologies that make the IoT achievable such as RFID, WSN and the Internet.
  - Research and studies are still nailed and in constant development in order to find countermeasures against cyber attacks against IoT.
  - The general countermeasures presented in this thesis could achieve, if implemented alone, an acceptable level of security in the IoT.

- Our fifth research question was “What is the role of each stakeholder in the smart home application to make it a safer application or place?”. This research question is discussed in Chapter 6 in detail. Considering the explanation given in the given chapter, we conclude:
  - Providing security in IoT is not the responsibility of one party in and of itself, rather it is a collaborative process whereby each stakeholder can contribute on his part to make the IoT more secure.

- To protect against any hacker or security threat, users should change the devices' default passwords and search more for the steps they need to take to make their devices more secure.
- Most IoT devices are designed and built by many companies without regard to security. This is due to the desire of these companies to provide consumers with inexpensive and lightweight smart devices as quickly as possible.
- Manufacturers should pay more attention to making the devices they manufacture safer, and they should start that from the design stage.
- It must be ensured that appropriate security technologies are available before deploying the technology and it becomes a part of our daily life rather than trying to find solutions too late.

Over the course of a year, we invested our effort and time to produce a thesis that would benefit readers interested in the issue of IoT security. In our search for information, we rely on more than 160 references, most of them from international scholarly journals. Among these journals are: *International Journal of Scientific Research in Science, Engineering and Technology, Journal of Network and Computer Applications, International Journal of Information Technology and Mechanical Engineering* and many other journals.

Finally, we hope this thesis has highlighted the importance of reaching radical solutions to secure the IoT and its users. In our thesis, we tried to provide a basic introduction to this important topic that draw the future path of information technology along with the future of our lives. This introduction can act as a catalyst for researchers interested in developing new schemas in the context of IoT security, as we have provided them with the necessary information that helps them examine this topic in a more detailed and expanded way.

REFERENCES

[1] B. O. Vikas, (2015), "Internet of Things (IoT): A Survey on Privacy Issues and Security". *International Journal of Scientific Research in Science, Engineering and Technology*, *1*(3), 168-173.

[2] D. Miorandi, S. Sicari, F. De Pellegrini & I. Chlamtac, (2012), "Internet of things: Vision, applications and research challenges". *Ad hoc networks*, *10*(7), 1497-1516.

[3] M. Bilal, (2017), "A review of internet of things architecture, technologies and analysis smartphone-based attacks against 3D printers". *arXiv preprint arXiv:1708.04560*.

[4] G. Cerullo, G. Mazzeo, G. Papale, B. Ragucci & L. Sgaglione, (2018), "Iot and sensor networks security" .In *Security and Resilience in Intelligent Data-Centric Systems and Communication Networks* (pp. 77-101). Academic Press.

[5] M. A. Razzaq, S. H. Gill, M. A. Qureshi & S. Ullah, (2017), "Security issues in the Internet of Things (IoT): a comprehensive study". *International Journal of Advanced Computer Science and Applications*, *8*(6), 383.

[6] Y. Yang, L. Wu, G. Yin, L. Li & H. Zhao, (2017), "A survey on security and privacy issues in Internet-of-Things". *IEEE Internet of Things Journal*, *4*(5), 1250-1258.

[7] A. Balte, A. Kashid & B. Patil, (2015), "Security issues in Internet of things (IoT): A survey". *International Journal of Advanced Research in Computer Science and Software Engineering*, *5*(4).

[8] K. Karimi & G. Atkinson, (2013), "What the Internet of Things (IoT) needs to become a reality". *White Paper, FreeScale and ARM*, 1-16.

[9] F. A. Alaba, M. Othman, I. A. T. Hashem, & F. Alotaibi, (2017), "Internet of Things security: A survey". *Journal of Network and Computer Applications*, *88*, 10-28.

[10] P. Corcoran, (2015), "The Internet of Things: why now, and what's next?". *IEEE consumer electronics magazine*, *5*(1), 63-68.

[11] R. S. M. Joshitta & L. Arockiam, (2016), "Security in IoT environment: a survey". *International Journal of Information Technology and Mechanical Engineering*, *2*(7), 1-8.

[12] G. Pison, "How many humans tomorrow? The United Nations revises its projections". Internet: https://phys.org/news/2019-06-humans-tomorrow-nations.html June 18, 2019 [Oct. 11, 2020].

[13] Number of IoT devices 2015 - 2025. (n.d.). Internet from Statista.com: https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/ [Dec. 20, 2020]

[14] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari & M. Ayyash, (2015), "Internet of things: A survey on enabling technologies, protocols, and applications". *IEEE communications surveys & tutorials*, *17*(4), 2347-2376.

[15] S. U. Rehman, I. U. Khan, M. Moiz & S. Hasan, (2016), "Security and privacy issues in IoT". *International journal of communication networks and information security*, *8*(3), 147.

[16] M. Abomhara & G. M. Køien, (2014, May), "Security and privacy in the Internet of Things: Current status and open issues". In *2014 international conference on privacy and security in mobile systems (PRISMS)* (pp. 1-8). IEEE.

[17] M. M. Hossain, M. Fotouhi & R. Hasan, (2015, June), "Towards an analysis of security issues, challenges, and open problems in the internet of things". In *2015 IEEE World Congress on Services* (pp. 21-28). IEEE.

[18] R. Mahmoud, T. Yousuf, F. Aloul & I. Zualkernan, (2015, December), "Internet of things (IoT) security: Current status, challenges and prospective measures". In *2015 10th International Conference for Internet Technology and Secured Transactions (ICITST)* (pp. 336-341). IEEE.

[19] R. Khan, S. U. Khan, R. Zaheer & S. Khan, (2012, December), "Future internet: the internet of things architecture, possible applications and key challenges". In *2012 10th international conference on frontiers of information technology* (pp. 257-260). IEEE.

[20] A. Haroon, M. A. Shah, Y. Asim, W. Naeem, M. Kamran & Q. Javaid, (2016), "Constraints in the IoT: the world in 2020 and beyond". *Constraints*, *7*(11), 252-271.

[21] B. S. Krishna & T. Gnanasekaran, (2017, February), "A systematic study of security issues in Internet-of-Things (IoT)". In *2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC)* (pp. 107-111). IEEE.

[22] U. E. Chinanu, O. E. Oche & J. O. Okah-Edemoh, (2018), "Architectural Layers of Internet of Things: Analysis of Security Threats and Their Countermeasures". *Scientific Review*, *4*(10), 80-89.

[23] Alliance for Internet of Things Innovation (AIOTI). (2018). "Identifiers in Internet of Things (IoT)", Internet: http:// aioti.eu/ wp-content/uploads/2018/03/AIOTI-Identifiers_in_IoT-1_0.pdf.pdf, Version 1.0, Feb. 2018

[24] B. N. Silva, M. Khan & K. Han, (2018), "Internet of things: A comprehensive review of enabling technologies, architecture, and challenges". *IETE Technical review*, *35*(2), 205-220.

[25] C. P. Mayer, (2009), "Security and privacy challenges in the internet of things". *Electronic Communications of the EASST*, *17*.

[26] "IoT Solution Architecture Models – Javatpoint" (n.d.). from Javatpoint.com Internet: https://www.javatpoint.com/iot-architecture-models, (Dec. 8, 2020).

[27] J. S. Kumar & D. R. Patel, (2014), "A survey on internet of things: Security and privacy issues". *International Journal of Computer Applications*, *90*(11).

[28] P. Sethi & S. R. Sarangi, (2017), "Internet of things: architectures, protocols, and applications". *Journal of Electrical and Computer Engineering*, *2017*.

[29] A. Tewari & B. B. Gupta, (2020), "Security, privacy and trust of different layers in Internet-of-Things (IoTs) framework". *Future generation computer systems*, *108*, 909-920.

[30] B. Zhang, X. X. Ma & Z. G. Qin, (2011), "Security architecture on the trusting internet of things". *Journal of Electronic Science and Technology*, *9*(4), 364-367.

[31] I. Andrea, C. Chrysostomou & G. Hadjichristofi, (2015, July), "Internet of Things: Security vulnerabilities and challenges". In *2015 IEEE Symposium on Computers and Communication (ISCC)* (pp. 180-187). IEEE.

[32] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang & W. Zhao, (2017), "A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications". *IEEE Internet of Things Journal*, *4*(5), 1125-1142.

[33] L. Atzori, A. Iera & G. Morabito, (2010), "The internet of things: A survey". *Computer networks*, *54*(15), 2787-2805.

[34] I. Cvitić & M. Vujić, (2015), "CLASSIFICATION OF SECURITY RISKS IN THE IOT ENVIRONMENT". *Annals of DAAAM & Proceedings*, *26*(1).

[35] D. Kozlov, J. Veijalainen & Y. Ali, (2012, February), "Security and privacy threats in IoT architectures". In *BODYNETS* (pp. 256-262).

[36] M. A. Iqbal, O. G. Olaleye & M. A. Bayoumi, (2017), "A review on internet of things (IoT): security and privacy requirements and the solution approaches". *Global Journal of Computer Science and Technology*.

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

[38] H. A. Khattak, M. A. Shah, S. Khan, I. Ali & M. Imran, (2019), "Perception layer security in Internet of Things". *Future Generation Computer Systems*, *100*, 144-164.

[39] G. Shen & B. Liu, (2011, May), "The visions, technologies, applications and security issues of Internet of Things". In *2011 International Conference on E-Business and E-Government (ICEE)* (pp. 1-4). IEEE.

[40] S. Li, L. Da Xu & S. Zhao, (2015), "The internet of things: a survey". *Information Systems Frontiers*, *17*(2), 243-259.

[41] K. K. Patel & S. M. Patel, (2016), "Internet of things-IOT: definition, characteristics, architecture, enabling technologies, application & future challenges". *International journal of engineering science and computing*, *6*(5).

[42] A. A. A. Boulogeorgos, P. D. Diamantoulakis & G. K. Karagiannidis, (2016), "Low power wide area networks (lpwans) for internet of things (iot) applications: Research challenges and future trends". *arXiv preprint arXiv:1611.07449*.

[43] D. E. Kouicem, A. Bouabdallah & H. Lakhlef, (2018), "Internet of things security: A top-down survey". *Computer Networks*, *141*, 199-221.

[44] A. Mosenia & N. K. Jha, (2016), "A comprehensive study of security of internet-of-things". *IEEE Transactions on Emerging Topics in Computing*, *5*(4), 586-602.

[45] A. Jha & M. C. Sunil, (2014), "Security considerations for Internet of Things". *L&T Technology Services*.

[46] K. Shamsi & Dr. A. Mazhar (2017), "IoT implementation using secure communication protocols". *International Journal of Computational Engineering Research (IJCER)*, (2250 – 3005)

[47] M. Ross, T. Hannes & A. Jara, (2019), "Baseline security recommendations for IoT in the context of Critical Information Infrastructures, 2017".

[48] A. R. Sfar, E. Natalizio, Y. Challal & Z. Chtourou, (2018), "A roadmap for security challenges in the Internet of Things". *Digital Communications and Networks*, *4*(2), 118-137.

[49] S. I. Al-Sharekh & K. H. A. Al-Shqeerat, (2019), "Security challenges and limitations in IoT environments". *Int. J. Comput. Sci. Netw. Secur.*, *19*(2), 193-199.

[50] M. F. Elrawy, A. I. Awad & H. F. Hamed, (2018), "Intrusion detection systems for IoT-based smart environments: a survey". *Journal of Cloud Computing*, *7*(1), 21.

[51] A. Kanuparthi, R. Karri & S. Addepalli, (2013, November), "Hardware and embedded security in the context of internet of things". In *Proceedings of the 2013 ACM workshop on Security, privacy & dependability for cyber vehicles* (pp. 61-64).

[52] E. Vasilomanolakis, J. Daubert, M. Luthra, V. Gazis, A. Wiesmaier & P. Kikiras, (2015, September), "On the security and privacy of Internet of Things architectures and

systems". In *2015 International Workshop on Secure Internet of Things (SIoT)* (pp. 49-57). IEEE.

[53] A. H. Ngu, M. Gutierrez, V. Metsis, S. Nepal & Q. Z. Sheng, (2016), "IoT middleware: A survey on issues and enabling technologies". *IEEE Internet of Things Journal*, *4*(1), 1-20.

[54] Q. M. Ashraf & M. H. Habaebi, (2015), "Autonomic schemes for threat mitigation in Internet of Things". *Journal of Network and Computer Applications*, *49*, 112-127.

[55] K. Laeeq & J. A. Shamsi, (2015), "A study of security issues, vulnerabilities and challenges in internet of things". *Securing Cyber-Physical Systems, 10*.

[56] S. Hameed, F. I. Khan & B. Hameed, (2019), "Understanding security requirements and challenges in Internet of Things (IoT): A review". *Journal of Computer Networks and Communications, 2019*.

[57] D. Ferraris & C. Fernandez-Gago, (2020), "TrUStAPIS: a trust requirements elicitation method for IoT". *International Journal of Information Security*, *19*(1), 111-127.

[58] F. I. P. S. Pub, (2006), "Minimum Security Requirements for Federal Information and Information Systems".

[59] K. Zhao & L. Ge, (2013, December), "A survey on the internet of things security". In *2013 Ninth international conference on computational intelligence and security* (pp. 663-667). IEEE.

[60] Antara de & H S. Guruprasad, (2015), "A Survey on Securing IOT Systems". *Journal of Emerging Technologies and Innovative Research*. 2. 34-41.

[61] R. Roman, P. Najera & J. Lopez, (2011), "Securing the internet of things". *Computer*, *44*(9), 51-58.

[62] R. H. Weber, (2011), "Accountability in the Internet of Things". *Computer Law & Security Review*, *27*(2), 133-138.

[63] A. Crabtree, T. Lodge, , J. Colley, C. Greenhalgh, K. Glover, H. Haddadi, ... & L. Wang, (2018), "Building accountability into the Internet of Things: the IoT Databox model". *Journal of Reliable Intelligent Environments*, *4*(1), 39-55.

[64] L. Li, (2012, May), "Study on security architecture in the Internet of Things". In *Proceedings of 2012 international conference on measurement, information and control* (Vol. 1, pp. 374-377). IEEE.

[65] X. Xiaohui, (2013, June), "Study on security problems and key technologies of the internet of things". In *2013 International conference on computational and information sciences* (pp. 407-410). IEEE.

[66] A. Wahid & P. Kumar, (2015), "A survey on attacks, challenges and security mechanisms in wireless sensor network". *International Journal for Innovative Research in Science and Technology*, *1*(8), 189-196.

[67] X. Chen, J. Liu, X. Wang, X. Zhang, Y. Wang & L. Chen, (2018, June), "Combating Tag Cloning with COTS RFID Devices". In *2018 15th Annual IEEE International Conference on Sensing, Communication, and Networking (SECON)* (pp. 1-9). IEEE.

[68] H. A. Abdul-Ghani, D. Konstantas & M. Mahyoub, (2018), "A comprehensive IoT attacks survey based on a building-blocked reference model". *IJACSA) International Journal of Advanced Computer Science and Applications*, *9*(3), 355-373.

[69] T. S. Heydt-Benjamin, D. V. Bailey, K. Fu, A. Juels & T. O'hare, (2007, February), "Vulnerabilities in first-generation RFID-enabled credit cards". In *International Conference on Financial Cryptography and Data Security* (pp. 2-14). Springer, Berlin, Heidelberg.

[70] A. Mitrokotsa, M. R. Rieback & A. S. Tanenbaum, (2010), "Classifying RFID attacks and defenses". *Information Systems Frontiers*, *12*(5), 491-505.

[71] S. Jaitly, H. Malhotra & B. Bhushan, (2017, July), "Security vulnerabilities and countermeasures against jamming attacks in Wireless Sensor Networks: A survey". In *2017 International Conference on Computer, Communications and Electronics (Comptelix)* (pp. 559-564). IEEE.

[72] J. Deogirikar & A. Vidhate, (2017, February), "Security attacks in IoT: A survey". In *2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)* (pp. 32-37). IEEE.

[73] S. N. Swamy, D. Jadhav & N. Kulkarni, (2017, February), "Security threats in the application layer in IOT applications". In *2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)* (pp. 477-480). IEEE.

[74] M. Bouabdellah, N. Kaabouch, F. El Bouanani & H. Ben-Azza, (2018), "Network layer attacks and countermeasures in cognitive radio networks: A survey". *Journal of information security and applications*, *38*, 40-49.

[75] I. Andrea, C. Chrysostomou & G. Hadjichristofi, (2015, July), "Internet of Things: Security vulnerabilities and challenges". In *2015 IEEE Symposium on Computers and Communication (ISCC)* (pp. 180-187). IEEE.

[76] R. A. J. Shree & R. A. Khan, (2014), "Wormhole attack in wireless sensor network". *International Journal of Computer Networks and Communications Security*, *2*(1), 22-26.

[77] M. Patel, A. Aggarwal & N. Chaubey, (2017), "Wormhole attacks and countermeasures in wireless sensor networks: a survey". *International Journal of Engineering and Technology (IJET), ISSN*, 0975-4024.

[78] W. Z. Khan, Y. Xiang, M. Y. Aalsalem & Q. Arshad, (2012), "The selective forwarding attack in sensor networks: Detections and countermeasures". *International Journal of Wireless and Microwave Technologies (IJWMT)*, *2*(2), 33.

[79] H. Verma & K. Chahal, (2017, June), "A review on security problems and measures of Internet of Things". In *2017 International Conference on Intelligent Computing and Control Systems (ICICCS)* (pp. 71-76). IEEE.

[80] A. Kamble & S. Bhutad, (2018, January), "Survey on Internet of Things (IoT) security issues & solutions". In *2018 2nd International Conference on Inventive Systems and Control (ICISC)* (pp. 307-312). IEEE.

[81] B. B. Gupta, N. A. Arachchilage & K. E. Psannis, (2018), "Defending against phishing attacks: taxonomy of methods, current issues and future directions". *Telecommunication Systems*, *67*(2), 247-267.

[82] B. B. Gupta, A. Tewari, A. K. Jain & D. P. Agrawal, (2017), "Fighting against phishing attacks: state of the art and future challenges". *Neural Computing and Applications*, *28*(12), 3629-3654.

[83] E. Galán, A. Alcaide, A. Orfila & J. Blasco, (2010, November), "A multi-agent scanner to detect stored-XSS vulnerabilities". In *2010 International Conference for Internet Technology and Secured Transactions* (pp. 1-6). IEEE.

[84] J. Milosevic, N. Sklavos & K. Koutsikou, (2016), "Malware in iot software and hardware".

[85] M. Antonakakis, T. April, M. Bailey, M. Bernhard, E. Bursztein, J. Cochran, ... & Kumar, D. (2017), "Understanding the mirai botnet". In *26th {USENIX} security symposium ({USENIX} Security 17)* (pp. 1093-1110).

[86] "A quick guide to IoT security regulations and standards". (n.d.), from Pufsecurity.com website, Internet: https://www.pufsecurity.com/standards, [Jan. 23, 2021].

[87] "IoT security standards & frameworks – SENKI", from Senki.org website, Internet: https://www.senki.org/operators-security-toolkit/sp-security/iot-security-standards, April 3, 2017 [Jan 24, 2021].

[88] "What Are the IoT Security Standards?". (n.d.). from Sdxcentral.com website, Internet: https://www.sdxcentral.com/5g/iot/definitions/what-are-iot-security-standards/ June 17, 2020 [Jan 24, 2021].

[89] J. R. Nurse, S. Creese & D. De Roure, (2017), "Security risk assessment in Internet of Things systems". *IT professional*, *19*(5), 20-26.

[90] I. Vajda & L. Buttyán, (2003, October), "Lightweight authentication protocols for low-cost RFID tags". In *Second Workshop on Security in Ubiquitous Computing–Ubicomp* (Vol. 2003).

[91] P. Alexander, R. Baashirah & A. Abuzneid, (2018), "Comparison and Feasibility of Various RFID Authentication Methods Using ECC". *Sensors*, *18*(9), 2902.

[92] R. Baashirah & A. Abuzneid, (2018), "Survey on prominent RFID authentication protocols for passive tags". *Sensors*, *18*(10), 3584.

[93] Y. Y. Chen & M. L. Tsai, (2011), "The Study on Secure RFID Authentication and Access Control". *Current Trends and Challenges in RFID*, 393.

[94] A. Maarof, M. Senhadji, Z. Labbi, & M. Belkasmi, (2014, November), "Security analysis of low cost RFID systems". In *2014 5th Workshop on Codes, Cryptography and Communication Systems (WCCCS)* (pp. 11-16). IEEE.

[95] M. L. Das, (2009), "Two-factor user authentication in wireless sensor networks". *IEEE transactions on wireless communications*, *8*(3), 1086-1090.

[96] S. Singh, P. K. Sharma, S. Y. Moon & J. H. Park, (2017), "Advanced lightweight encryption algorithms for IoT devices: survey, challenges and solutions". *Journal of Ambient Intelligence and Humanized Computing*, 1-18.

[97] A. Shah & M. Engineer, (2019), "A survey of lightweight cryptographic algorithms for iot-based applications". In *Smart Innovations in Communication and Computational Sciences* (pp. 283-293). Springer, Singapore.

[98] I. Bhardwaj, A. Kumar & M. Bansal, (2017, September), "A review on lightweight cryptography algorithms for data security and authentication in IoTs". In *2017 4th International Conference on Signal Processing, Computing and Control (ISPCC)* (pp. 504-509). IEEE.

[99] L. Eschenauer & V. D. Gligor, (2002, November), "A key-management scheme for distributed sensor networks". In *Proceedings of the 9th ACM conference on Computer and communications security* (pp. 41-47).

[100] R. Roman, C. Alcaraz, J. Lopez & N. Sklavos, (2011), "Key management systems for sensor networks in the context of the Internet of Things". *Computers & Electrical Engineering*, *37*(2), 147-159.

[101] W. Du, J. Deng, Y. S. Han, S. Chen & P. K. Varshney, (2004, March), "A key management scheme for wireless sensor networks using deployment knowledge". In *IEEE INFOCOM 2004* (Vol. 1). IEEE.

[102] R. Logapriya & J. Preethi, (2016), "Efficient Methods in wireless sensor network for error detection, correction and recovery of data". *International Journal of Novel Research in Computer Science and Software Engineering*, *3*(2), 47-54.

[103] X. Deng, M. Rong, T. Liu, Y. Yuan & D. Yu, (2008, March), "Segmented Cyclic Redundancy Check: A Data Protection Scheme for Fast Reading RFID Tag's Memory". In *2008 IEEE Wireless Communications and Networking Conference* (pp. 1576-1581). IEEE.

[104] M. N. Aman, B. Sikdar, K. C. Chua & A. Ali, (2018), "Low power data integrity in IoT systems". *IEEE Internet of Things Journal*, *5*(4), 3102-3113.

[105] I. Shah, F. Lone, S. Ahmad, F. Malik & H. Haqani, (2018, January), "HMACSHA256 With RSA For Ensuring Secure Communication In IoT Based Smart Home System". *International Journal of Advance Engineering and Research Development* (Vol. 5).

[106] B. Soewito & C. E. Andhika, (2019, August), "Next Generation Firewall for Improving Security in Company and IoT Network". In *2019 International Seminar on Intelligent Technology and Its Applications (ISITIA)* (pp. 205-209). IEEE.

[107] C. Liu, J. Yang, R. Chen, Y. Zhang & J. Zeng, (2011, July), "Research on immunity-based intrusion detection technology for the internet of things". In *2011 Seventh International Conference on Natural Computation* (Vol. 1, pp. 212-216). IEEE.

[108] B. B. Zarpelão, R. S. Miani, C. T. Kawakani & S. C. de Alvarenga, (2017), "A survey of intrusion detection in Internet of Things". *Journal of Network and Computer Applications*, *84*, 25-37.

[109] A. Kamble, V. S. Malemath & D. Patil, (2017, February), "Security attacks and secure routing protocols in RPL-based Internet of Things: Survey". In *2017 International Conference on Emerging Trends & Innovation in ICT (ICEI)* (pp. 33-39). IEEE.

[110] D. Airehrour, J. Gutierrez & S. K. Ray, (2016), "Secure routing for internet of things: A survey". *Journal of Network and Computer Applications*, *66*, 198-213.

[111] Y. Zhang, S. Kasahara, Y. Shen, X. Jiang & J. Wan, (2018), "Smart contract-based access control for the internet of things". *IEEE Internet of Things Journal*, *6*(2), 1594-1605.

[112] Y. Andaloussi, M. D. El Ouadghiri, Y. Maurel, J. M. Bonnin & H. Chaoui, (2018), "Access control in IoT environments: Feasible scenarios". *Procedia computer science*, *130*, 1031-1036.

[113] A. Ouaddah, H. Mousannif, A. Abou Elkalam & A. A. Ouahman, (2017), "Access control in the Internet of Things: Big challenges and new opportunities". *Computer Networks*, *112*, 237-262.

[114] S. N. Swamy, D. Jadhav & N. Kulkarni, (2017, February), "Security threats in the application layer in IOT applications". In *2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC)* (pp. 477-480). IEEE.

[115] Q. D. Ngo, H. T. Nguyen, L. C. Nguyen & D. H. Nguyen, (2020), "A survey of IoT malware and detection methods based on static features". *ICT Express*.

[116] A. Damodaran, F. Di Troia, C. A. Visaggio, T. H. Austin & M. Stamp, (2017), "A comparison of static, dynamic, and hybrid analysis for malware detection". *Journal of Computer Virology and Hacking Techniques*, *13*(1), 1-12.

[117] Z. Benenson, P. M. Cholewinski & F. C. Freiling, (2008), "Vulnerabilities and attacks in wireless sensor networks". *Wireless Sensors Networks Security*, 22-43.

[118] R. Brooks, P. Y. Govindaraju, M. Pirretti, N. Vijaykrishnan & M. T. Kandemir, (2007), "On the detection of clones in sensor networks using random key predistribution". *IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews)*, *37*(6), 1246-1258.

[119] B. Parno, A. Perrig & V. Gligor, (2005, May), "Distributed detection of node replication attacks in sensor networks". In *2005 IEEE Symposium on Security and Privacy (S&P'05)* (pp. 49-63). IEEE.

[120] L. Sujihelen, C. Jayakumar & C. Senthil Singh, (2015), "Detecting node replication attacks in wireless sensor networks: Survey". *Indian Journal of Science and Technology*, *8*(16).

[121] D. Ma & N. Saxena, (2014), "A context-aware approach to defend against unauthorized reading and relay attacks in RFID systems". *Security and Communication Networks*, *7*(12), 2684-2695.

[122] J. Wang, Z. Liu, S. Zhang & X. Zhang, (2014), "Defending collaborative false data injection attacks in wireless sensor networks". *Information Sciences*, *254*, 39-53.

[123] B. Bostami, M. Ahmed & S. Choudhury, (2019), "False data injection attacks in internet of things". In *Performability in Internet of Things* (pp. 47-58). Springer, Cham.

[124] M. Pirretti, S. Zhu, N. Vijaykrishnan, P. McDaniel, M. Kandemir & R. Brooks, (2006), "The sleep deprivation attack in sensor networks: Analysis and methods of defense". *International Journal of Distributed Sensor Networks*, *2*(3), 267-287.

[125] Y. Bai, F. Wang & P. Liu, (2006, September), "Efficiently Filtering RFID Data Streams". In *CleanDB*.

[126] S. Jaitly, H. Malhotra & B. Bhushan, (2017, July), "Security vulnerabilities and countermeasures against jamming attacks in Wireless Sensor Networks: A survey". In *2017 International Conference on Computer, Communications and Electronics (Comptelix)* (pp. 559-564). IEEE.

[127] T. Bhattasali, R. Chaki & N. Chaki, (2013, September), "Study of security issues in pervasive environment of next generation internet of things". In *IFIP International Conference on Computer Information Systems and Industrial Management* (pp. 206-217). Springer, Berlin, Heidelberg.

[128] Y. Peng, U. He & J. Choi, (2012), "Internet of Things: International Workshop, IOT" 2012, Changsha, China, August 17-19, 2012. Proceedings.

[129] Z. C. Dong, R. Espejo, Y. Wan & W. Zhuang, (2015), "Detecting and locating man-in-the-middle attacks in fixed wireless networks". *Journal of computing and information technology*, *23*(4), 283-293.

[130] S. M. Glass, V. Muthukkumarasamy & M. Portmann, (2009, May), "Detecting man-in-the-middle and wormhole attacks in wireless mesh networks". In *2009 International Conference on Advanced Information Networking and Applications* (pp. 530-538). IEEE.

[131] F. Aliyu, T. Sheltami & E. M. Shakshuki, (2018), "A detection and prevention technique for man in the middle attack in fog computing". *Procedia Computer Science*, *141*, 24-31.

[132] V. P. Singh, S. Jain & J. Singhai, (2010), "Hello flood attack and its countermeasures in wireless sensor networks". *International Journal of Computer Science Issues (IJCSI)*, *7*(3), 23.

[133] V. P. Singh, A. S. A. Ukey & S. Jain, (2013), "Signal strength based hello flood attack detection and prevention in wireless sensor networks". *International Journal of Computer Applications*, *62*(15).

[134] I. Butun, P. Österberg & H. Song, (2019), "Security of the Internet of Things: Vulnerabilities, attacks, and countermeasures". *IEEE Communications Surveys & Tutorials*, *22*(1), 616-644.

[135] J. Newsome, E. Shi, D. Song & A. Perrig, (2004, April), "The sybil attack in sensor networks: analysis & defenses". In *Third international symposium on information processing in sensor networks, 2004. IPSN 2004* (pp. 259-268). IEEE.

[136] L. Qian, N. Song & X. Li, (2005, March), "Detecting and locating wormhole attacks in wireless ad hoc networks through statistical analysis of multi-path". In *IEEE Wireless Communications and Networking Conference, 2005* (Vol. 4, pp. 2106-2111). IEEE.

[137] R. H. Khokhar, M. A. Ngadi & S. Mandala, (2008), "A review of current routing attacks in mobile ad hoc networks". *International journal of computer science and security*, *2*(3), 18-29.

[138] Y. C. Hu, A. Perrig & D. B. Johnson, (2006), "Wormhole attacks in wireless networks". *IEEE journal on selected areas in communications*, *24*(2), 370-380.

[139] Y. C. Hu, A. Perrig & D. B. Johnson, (2003, March), "Packet leashes: a defense against wormhole attacks in wireless networks". In *IEEE INFOCOM 2003. Twenty-second Annual Joint Conference of the IEEE Computer and Communications Societies (IEEE Cat. No. 03CH37428)* (Vol. 3, pp. 1976-1986). IEEE.

[140] W. Wang & B. Bhargava, (2004, October), "Visualization of wormholes in sensor networks". In *Proceedings of the 3rd ACM workshop on Wireless security* (pp. 51-60).

[141] B. Yu & B. Xiao, (2006, April), "Detecting selective forwarding attacks in wireless sensor networks". In *Proceedings 20th IEEE international parallel & distributed processing symposium* (pp. 8-pp). IEEE.

[142] H. M. Sun, C. M. Chen & Y. C. Hsiao, (2007, October), "An efficient countermeasure to the selective forwarding attack in wireless sensor networks". In *TENCON 2007-2007 IEEE Region 10 Conference* (pp. 1-4). IEEE.

[143] G. Wang, W. Zhang, G. Cao & T. La Porta, (2003, October), "On supporting distributed collaboration in sensor networks". In *IEEE Military Communications Conference, 2003. MILCOM 2003.* (Vol. 2, pp. 752-757). IEEE.

[144] P. Sharma, M. Saluja & K. K. Saluja, (2012), "Detection techniques of selective forwarding attacks in wireless sensor networks: a survey". *arXiv preprint arXiv:1205.4905*.

[145] V. Satyanarayana & M. V. B. C. Sekhar, (2011), "Static analysis tool for detecting web application vulnerabilities". *Int. Journal of Modern Engineering Research (IJMER)*, *1*(1), 127-133.

[146] P. Vogt, F. Nentwich, N. Jovanovic, E. Kirda, C. Kruegel & G. Vigna, (2007, February), "Cross Site Scripting Prevention with Dynamic Data Tainting and Static Analysis". In *NDSS* (Vol. 2007, p. 12).

[147] E. Kirda, C. Kruegel, G. Vigna & N. Jovanovic, (2006, April), "Noxes: a client-side solution for mitigating cross-site scripting attacks". In *Proceedings of the 2006 ACM symposium on Applied computing* (pp. 330-337).

[148] R. Putthacharoen & P. Bunyatnoparat, (2011, February), "Protecting cookies from cross site script attacks using dynamic cookies rewriting technique". In *13th International*

Conference on Advanced Communication Technology (ICACT2011) (pp. 1090-1094). IEEE.

[149] E. Zeng, S. Mare & F. Roesner, (2017), "End user security and privacy concerns with smart homes". In *Thirteenth Symposium on Usable Privacy and Security ({SOUPS} 2017)* (pp. 65-80).

[150] C. Lee, L. Zappaterra, K. Choi & H. A. Choi, (2014, October), "Securing smart home: Technologies, security challenges, and security requirements". In *2014 IEEE Conference on Communications and Network Security* (pp. 67-72). IEEE.

[151] "SmartThings Hub". from Samsung.com website, Internet: https://www.samsung.com/tr/smartthings/hub/smartthings-hub-gp-u999sjvlgeb/, Sep 24, 2020 [Dec. 9, 2020].

[152] D. Barnard-Wills, L. Marinos & S. Portesi, (2014), "Threat landscape and good practice guide for smart home and converged media". *European Union Agency for Network and Information Security (ENISA)*.

[153] "Smart Home", Smart Home ecosystem - Home automation tech. from Homeautotechs.com website, Internet: https://homeautotechs.com/, May 27, 2018 [Dec. 9, 2020].

[154] J. Bugeja, A. Jacobsson & P. Davidsson, (2016, August), "On privacy and security challenges in smart connected homes". In *2016 European Intelligence and Security Informatics Conference (EISIC)* (pp. 172-175). IEEE.

[155] J. M. Batalla, A. Vasilakos & M. Gajewski, (2017), "Secure smart homes: Opportunities and challenges". *ACM Computing Surveys (CSUR), 50*(5), 1-32.

[156] D. Geneiatakis, I. Kounelis, R. Neisse, I. Nai-Fovino, G. Steri & G. Baldini, (2017, May), "Security and privacy issues for an IoT based smart home". In *2017 40th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)* (pp. 1292-1297). IEEE.

[157] "Avast Smart Home Report 2019". (n.d.). from Avast.com website, Internet: https://press.avast.com/press-kits/avast-smart-home-report-2019, [Dec. 9, 2020].

[158] M. Fagan, K. N. Megas, K. Scarfone & M. Smith, (2020), "Foundational Cybersecurity Activities for IoT Device Manufacturers" (*No. NIST Internal or Interagency Report (NISTIR) 8259). National Institute of Standards and Technology*.

[159] M. Schiefer, (2015, May), "Smart home definition and security threats". In *2015 ninth international conference on IT security incident management & IT forensics* (pp. 114-118). IEEE.

[160] H. Lin & N. W. Bergmann, (2016), "IoT privacy and security challenges for smart home environments". *Information*, *7*(3), 44.

[161] U. Saxena, J. S. Sodhi & Y. Singh, (2017, January), "Analysis of security attacks in a smart home networks". In *2017 7th International Conference on Cloud Computing, Data Science & Engineering-Confluence* (pp. 431-436). IEEE.

[162] W. Ali, G. Dustgeer, M. Awais & M. A. Shah, (2017, September), "IoT based smart home: Security challenges, security requirements and solutions". In *2017 23rd International Conference on Automation and Computing (ICAC)* (pp. 1-6). IEEE.

[163] "Inside the smart home: IoT device threats and attack scenarios". (n.d.). from Trendmicro.com website, Internet: https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/inside-the-smart-home-iot-device-threats-and-attack-scenarios, [Dec. 9, 2020]

[164] "Internet of things (IoT): Industrial controls – riscure". from Riscure.com website, Internet: https://www.riscure.com/market/iot-industrial-controls/, May 31, 2018 [Dec. 9, 2020].

[165] "Security and Privacy - data privacy in IoT". (n.d.). from Develcoproducts.com website, Internet: https://www.develcoproducts.com/gateway/security-and-privacy/, [Dec. 9, 2020].

[166] "TECHNICAL SPECIFICATION". (n.d.). ETSI TS 102 941 V1.3.1 (2019-02). from Etsi.org website, Internet: https://www.etsi.org/deliver/etsi_ts/102900_102999/102941/01.03.01_60/ts_102941v010301p.pdf, [Dec. 9, 2020].

[167] Norton™ VPN. (n.d.), from Norton.com website, Internet: https://us.norton.com/products/norton-secure-vpn, [Dec. 9, 2020].