VAASAN AMMATTIKORKEAKOULU
UNIVERSITY OF APPLIED SCIENCES

Md Farukul Islam

IOT SECURITY STUDY FOR DOMESTIC DEVICES

Bachelor of Technology Thesis

Technology and Communication
2020

VAASAN AMMATTIKORKEAKOULU
UNIVERSITY OF APPLIED SCIENCES
Information Technology

ABSTRACT

Author	Md Farukul Islam
Title	IoT Security Study for Domestic Devices
Year	2020
Language	English
Pages	52
Name of Supervisor	Jukka Matila

The internet is the most common, easy, and popular way of communication. IoT is one way of communication using this existing internet communication technology by following several protocols. Many IoT devices are using for domestic purposes, such as for home or office automation. These domestic IoT devices carry most of the private and sensitive information of a user. Moreover, all the IoT devices, actuators, and sensors are working through the public internet network. Thus, securing those domestic IoT devices from unauthorized access through this internet network and ensuring the user's privacy is difficult and challenging.

This thesis explains how to build a domestic IoT network, secure the system, analyze the security vulnerabilities of that secure network, and finally, provide possible security proposals for every domestic IoT user for better security practices. In the domestic IoT system, security is one of the major concerns because most domestic devices, including personal devices, mobiles, and laptops, are connected to the network. Thus, maintaining privacy is a crucial matter of concern and a challenging area to deal with. This thesis explains how to keep home IoT devices safe and secure and maintain security through the network.

There is nothing called perfect, so it is almost impossible to build an ideal security system for any IoT network. This thesis also explains the domestic IoT network's risk management system to maintain the security system's stability and durability.

Keywords IoT, Security, Domestic Devices

CONTENTS

LIST OF FIGURES

LIST OF TABLES

ABBREVIATION

AES	Advanced Encryption Standard
AI	Artificial Intelligence
API	Application Programming Interface
BPSK	Binary Phase-Shift Keying
CIA	Confidentiality, Integrity, Availability
DC	Data Centre
DDoS	Distributed Denial-of-Service
DMZ	Demilitarized Zone
DNS	Domain Name System
DoS	Denial-of-Service
FSK	Frequency-Shift Keying
FTP	File Transfer Protocol
GFSK	Gaussian Frequency-Shift Keying
HTTPS	Hypertext Transfer Protocol Secure
IAS	Information, Assurance, and Security
IDS	Intrusion Detection System
IoT	Internet of Things
IP	Internet protocol
IR	Incident Response
ISM	Industrial, Scientific, and Medical

LAN	Local Area network
M2M	Machine to Machine
MAC	Media Access Control
MITM	Man-in-the-middle
NAT	Network Access Control
OQPSK	Offset Quadrature Phase-Shift Keying
OSI	Open System Interconnection
PAN	Personal Area Network
PKI	Public-key Infrastructure
RFID	Radio Frequency Identification
RM	Reference Models
SDLC	Software Development Life Cycle
SHODAN	Sentient Hyper-Optimised Data Access Network
SSID	Service Set Identifier
SSL	Secure Socket Layer
TLS	Transport Layer Security
UI	User Interface
VPN	Virtual Private Network
WEP	Wired Equivalent Privacy
Wi-Fi	Wireless Fidelity

WLAN	Wireless Local Area Network
WPA	Wi-Fi Protected Access

1 INTRODUCTION

1.1 Internet of Things (IoT)

The term IoT is internet-based things, which are the smart devices integrated with sensors and actuators. These IoT devices are connected and sharing data worldwide through the internet using different IoT protocols. The main concept of IoT first came in early 1982 by connecting Coca-Cola vending machines to the internet. The phrase "Internet of Things" was given by Kevin Ashton in 1999 during the work at Procter and Gamble, which was regularly called by "embedded internet" or "pervasive computing" /1/. According to Ashton, "The IoT coordinates the interconnectedness of human culture - our 'things' – with the interconnectedness of our advanced data framework – 'the Internet.' That is known as the IoT" /2/. One of the first IoT applications was radio-frequency identification (RFID) tags to track expensive equipment locations. After adding IoT sensors to their product components, manufacturers introduce comprehensive, real-time data collection and analysis and improve their production system in a much responsive way. Now The utility industry, along with the manufacturing industry, is the largest segment using IoT endpoints. Building automation, automotive, and healthcare industries are the fastest-growing segments of using IoT endpoints /3/.

Table 1. IoT Endpoint Market by Segment, 2018-2020, worldwide /4/.

Segment	**2018**	**2019**	**2020**
Utilities	0.98	1.17	1.37
Government	0.40	0.53	0.70
Building Automation	0.23	0.31	0.44
Physical Security	0.83	0.95	1.09
Manufacturing & Natural Resources	0.33	0.40	0.49
Automotive	0.27	0.36	0.47
Healthcare Providers	0.21	0.28	0.36
Retail & Wholesale Trade	0.29	0.36	0.44
Information	0.37	0.37	0.37
Transportation	0.06	0.07	0.08
Total	**3.96**	**4.81**	**5.81**

Source: Gartner (August 2019)

1.2 IoT in Domestic Devices

Nowadays, IoT has become much popular for different automation purposes, mostly in-home and office automation industries. The system uses a mesh network topology, which can connect, control, and monitor every domestic IoT device. By using IoT, the users can control the appliances by giving accessible voice commands using Google Assistant, Alexa, Amazon Echo, or can control using remote mobile applications API or different IoT platform UI. For domestic purposes, there are many smart devices available that consume a small amount of power. Using the popular wireless IoT protocol, such as Zigbee or Z-wave, it becomes easy to control all the household devices altogether. However, there are every necessary domestic IoT devices which are connected through the network such as lite, fan, camera, security-lock, fridge, toaster, coffeemaker, tv, oven, cooker, car, watch, bed, switch bell, and including lots of sensors, actuators, and devices which are used for a different purpose in everyday life. Moreover, it is also easy to set up, control, and monitor the home automation system from everywhere /5/.

1.3 IoT Security Concerns

There are 7 billion IoT devices connected to the public internet, making lives easy and comfortable. Every day the number of connected IoT devices with the internet is

growing faster than thinking. The more popular IoT devices get, the more it is becoming the target for hackers. This risk of getting attacked by a hacker is also increasing every day, and it also raises security concerns and privacy issues. To avoid the attacks coming from the hacker's, users need protection against them. For ensuring this protection, users need to set up a proper security system and backup sensitive data. The more IoT devices are connected to the internet, and more opportunities are created for the hacker to breach the system. By using the internet, it opens many doors for cybercriminals to commit a cybercrime without being traced. These criminals can take the IoT devices control and can do more damage to the victims. They can spy on the users or blackmail them and claim a huge ransom. They can also control an industrial system, manipulate the production line, shut down the system, or even destroy it. For tackling those breaches, the system must be established with a better security system before the system got compromised. So, security is a major concern, issues, and threats for IoT device networks. The security failure can be an irrecoverable threat for the system owners /6, 7/. Some of the significant IoT device vulnerabilities are discussed below.

- IoT devices have a lack of security updates, which is a massive threat for users.
- Insecure communication through the network can compromise sensitive data breaches.
- Service authentication and web applications are insecure, which can cause significant damage to the user's data.
- Insecure internet-based services are exposed, which is a considerable threat for IoT device users /8/.

1.4 Objective

This thesis aims to establish a home IoT network, ensure network safety and security, analyze the system's security vulnerabilities, and finally suggest several security proposals for better security practice.

1.5 Research Methodology

This thesis is based on real-time experiments and literature analysis. The information presented throughout the thesis, most of them are obtained from the experiments. In this thesis experiment, a home IoT system was built with some IoT devices and sensors. All possible security steps were implemented, and finally, the security vulnerabilities of that system were analyzed. The secondary data were obtained from various archives, articles, tech web journals, distinctive tech reports, and books.

1.6 Thesis Structure

This thesis is separated into two principal parts: fabricating a protected home IoT network and a superior security proposition for that domestic IoT frameworks. Chapter 2 provides the security goals, IoT system architecture, security system threats, and possible cyber-attacks. Chapter 3 is about building the home IoT network, securing the network, and analyzing that secure home IoT network's vulnerabilities. The following chapter provides several better security practice suggestions for domestic IoT network users.

2 IOT SECURITY RISK

2.1 IoT Security Goals and Stakeholders

2.1.1 IoT Security Goals

The security goal for cyberspace security and IoT security are quite similar. The most traditional security goal is to ensure confidentiality, integrity, and availability, and these three together are called a CIA-triad. Although this CIA-triad is one of the most prevalent cybersecurity models, it has some limitations. To overcome these limitations of the security goals, information, assurance, and security (IAS) octave are utilized. The IAS octave comes with confidentiality, integrity, and availability of the existing three goals with additional five security goals, including Non-repudiation, privacy, audibility, accountability, and trustworthiness /11/.

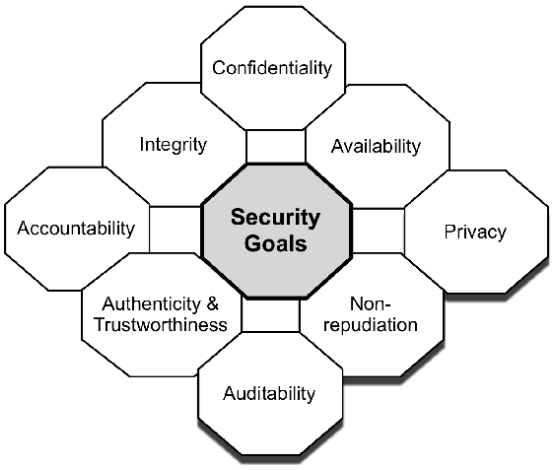

Figure 1. IoT security goals /9/.

Table 2. Internet of things (IoT) security goals /11/.

Security Requirements	Definition	Abbreviations
Confidentiality	Set of rules which ensure that the data can be accessed only by an authorized object.	C
Integrity	Set of rules which ensure that the data completeness and accuracy is preserved.	I

Availability	Set of rules which ensure that the data can be accessible every time demanded by the authorized object.	A
Non-repudiation	Set of rules which ensure that the system can validate the incident or non-incident of an event.	NR
Privacy	Set of rules which ensure that the system follows the privacy rules and allowing users to control their data.	P
Audibility	Set of rules which ensure that the system can perform firm monitoring on its actions.	AU
Accountability	Set of rules which ensure that the system users are responsible for their actions.	AC
Trustworthiness	Set of rules which ensure that the system can prove identity and confirm trust.	TW

2.1.2 IoT Stakeholders

In the IoT ecosystem, the stakeholder can be classified into four categories according to their roles. There are manufacturers, developers, consumers, and providers /11/.

Table 3. Internet of things (IoT) stakeholders /11/.

IoT Stakeholders	Roles	Abbreviations
Manufacturer	Producing IoT products and hardware.	M
Developer	Developing IoT solutions.	D
Consumer	Using IoT products, hardware.	C
Provider	Providing IoT services.	P

2.2 IoT Architecture

There is no single established consensus on the architecture of IoT. Different researchers have proposed different architecture for IoT. These IoT reference models (RM) include the three-level model, five-level model, and seven-level model. This reference model breaks into different level by simplifying the IoT ecosystem complexity. The most basic and common IoT architecture is a three-layer model, which includes the Application layer (cloud/server), Network-layer (router/gateways), and the Perception layer (sensors and actuators) /10, 11/.

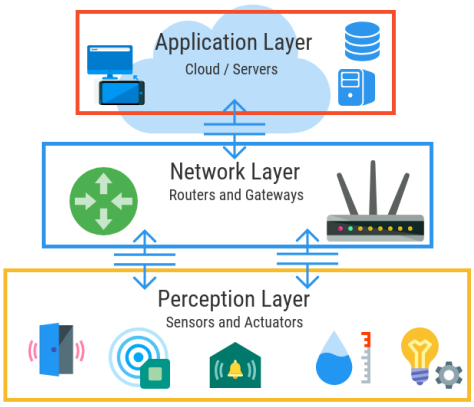

Figure 2. The most basic IoT three-layer architecture /10/.

2.2.1 IoT Seven-level Architecture

This discussion focuses only on seven-level reference models (RM). CISCO proposed the seven-level reference model (RM) in 2014 as an extension of five-level and three-layer models. These levels are level 1-Edge nodes, level 2-Communication, level 3-Edge computing, level 4-Data accumulation, level 5-Data abstraction, level 6-Application, level 7-Data centers (DC), and Users.

Figure 3. Seven-level model (CISCO's RM) /11/.

- Level 1-Edge nodes: This level consist of computing nodes such as devices, sensors, radio-frequency identification (RFID) readers, and controllers. The

security goals, such as confidentiality, integrity, and privacy, need to be considered at this level.

- Level 2-Communication: This level consists of protocols, communications, networks, machine to machine (M2M), Wi-Fi, telecom, and hardware (HW) kits.
- Level 3-Edge computing: This level has all the cloud infrastructure, such as public, private, hybrid, and managed.
- Level 4-Data accumulation: This level is responsible for processing, filtering, and storing such as Big data, harvest, and IoT data storage.
- Level 5-Data abstraction: This level is responsible for data manipulating, such as reporting, mining, and machine learning.
- Level 6-Application: This level is operating different IoT applications using the IoT data.
- Level 7-Datacenters (DC) and Users: At this level, only authorized users can communicate and make use of their data, which are getting from the applications /11, 12/.

2.3 IoT Threats and Possible Attacks

The more significant part of the web applications is facilitated on public internet servers. This makes them more vulnerable to attacks by hackers because of easy internet accessibility. The term hacking means exploring and exploiting different security breaches in a system or its associated network. There are several types of hackers in this society.

- White hat hacker: They are ethical hackers. They usually do their job by getting permission to hacking from the proper authority. They utilize their broad security knowledge for good instead of insidious purposes. They usually check the system vulnerabilities, find out the issues, and fix those security loopholes and issues.
- Gray hat hacker: They are neither good nor bad people. They usually look for different system vulnerabilities and access the system without the proper authority's permission. However, their intentions are not malicious; after getting any loopholes in a system, they usually report to the system authority and fix

those security issues by charging a small fee. Although their intentions are good, these activities are still illegal.

- Black hat hacker: They are cybercriminals. They use their extensive knowledge to bypass the security protocol and intercept the information that comes through the network. They also write malware to corrupt other systems and gaining access. Their primary motivations are financial gain, and some are addicted to the thrill of cyber-criminal activities /13/.

2.3.1 Different Types of Cyber-Attacks

There have various types of cyber-attacks that include the following:

- Denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks: A denial-of-service attack is overwhelming a system's capability. The system cannot respond to the requests made by the server. A DDoS attack is also a system's capacity overwhelming, but in this case, many host machines are infected by malicious software that has launched that attack. By using DoS or DDoS attacks, attackers do not want to access the system, but they want to take the system down. Several DoS and DDoS types of attacks, such as TCP SYN flood attack, teardrop attack, Smurf attack, ping-of-death attack, and botnets.
- Man-in-the-middle (MitM) attack: A man-in-the-middle attack is an attack when the attacker inserts itself into the system and interacts between the server and the client. There are several types of man-in-the-middle attacks, and the most common types are session hijacking, IP spoofing, and Replay.
- Phishing and spear-phishing attacks: Phishing attacks refer to tricking some-one into gaining access to all personal information. The hackers usually do it by sending a trusted e-mail with a malicious URL or attachment. The spear-phishing attacks are more specific and targeted, and it looks like the sending e-mail comes from the proper authority, such as management or a partner company. They can clone the websites and make users fool to get all the cre-dential information.

- Drive-by-download attack: A drive-by-download attack is an attack that can happen automatically by visiting websites, viewing an e-mail, or a pop-up window. The victims do not need to do anything to become infected. Hackers have already planted the malicious code to the specific site or e-mail message or pop-up window for this attack.
- Password attack: Using password attacks, hackers can gain system access by getting the password using different password gaining methods. They can get the password by only looking around the victim's desk, sniffing the network, and get an unencrypted password; a hacker can also get the password by doing social engineering, password guessing, or getting access to the password database. The most popular password attacks are brute-force attack and dictionary attack.
- SQL injection attack: SQL injection attacks attack SQL query executes by a malefactor via the input data. After an SQL injection, the attacker can exploit and read or modify any sensitive data information. The websites that use dynamic SQL are mostly get infected by this attack.
- Cross-site scripting (XSS) attack: In cross-site scripting (XSS) attacks, the attacker sends malicious JavaScript to the database, and when someone requests an HTML page, it comes with that malicious payload to the victim's browser and executes the script. By using this attack, attackers can insist on sending the victim's cookies to the attackers' server. After getting the cookies, then he/she will be able to capture screenshots, network information and take remote access control.
- Eavesdropping attack: In eavesdropping attacks, attackers can intercept the victim's network traffic and access all the credential information, including passwords and credit card information. In conclusion, this eavesdropping can be passive, listen to the transmitted message, or activate, grabbing the information actively sending queries.
- Birthday attack: Usually, a hash function generates a message digest (MD) for any unique message. In a birthday attack, the attackers can create the same message digest (MD) for another message and send it to the victim instead of the original one, and it is quite challenging to detect.

- Malware attack: Malware attacks are the attacks in which attackers install malicious software on the victim's system without consent. Some malware seems to come from a trusted source but eventually launched an attack and spread through the network. Several malware attacks such as macro viruses, file infectors, system or boot-record infectors, polymorphic viruses, stealth viruses, trojans, logic bombs, worms, droppers, ransomware /14/.

3 IOT IN DOMESTIC DEVICES

3.1 IoT Based Smart Home System

The things connected through the internet and communicating in both ways are called the internet of things. In smart homes, almost all the home devices are connected through a wireless network hub connected to a home router or modem and controlled via some mobile applications, a dynamic network or remote controller, a static network. The home devices communicate with each other or network through an internet gateway called a smart hub, which uses low-power wireless communication protocols like Zigbee, Z-wave, or Wi-Fi. The smart hub usually integrates all the smart devices. Some third-party smart hubs, such as the Samsung smart hub, integrate all smart devices. This hub uses a ZigBee or Z-wave protocol to control a maximum of 250 smart IoT devices /15-24/.

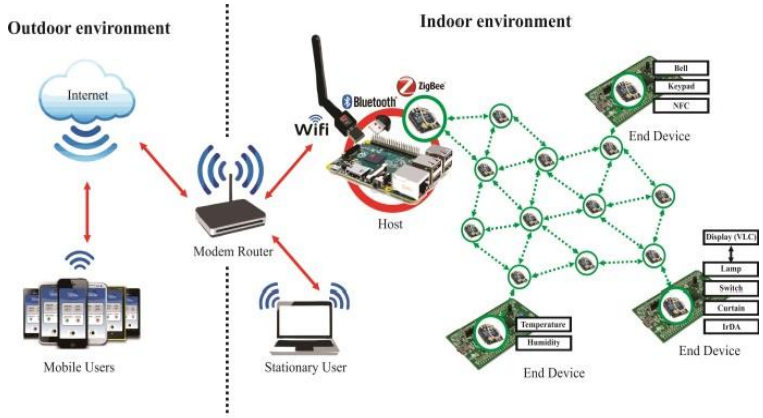

Figure 4. Smart Home System /25/.

One of the main things to control many IoT devices is a high-speed internet connection to handle many more devices smoothly. Fifth Generation bandwidth is best to use for controlling and monitoring a large scale of IoT devices together. A smart home system usually uses mesh network topology for connecting end-user devices to a network. The smart hub can also be controlled by the mobile application (Android, iOS) Application Programming Interface (API) from any outside network. It can also be controlled by a remote controller to control the Personal Area Network (PAN) from home as stationary users. The Mobile application has a dedicated cloud server, database, and web page to connect, monitor, and manage devices. This network can also be controlled by voice, such as Alexa, google assistant, Siri, and Echo

show. The smart devices related to the smart hub must be a specific supportive protocol such as ZigBee or Z-wave, Bluetooth, or Wi-Fi /26-36/.

3.1.1 IoT Wireless Protocols

A communications protocol maintains certain rules and allows two or more entities to communicate through a wired or wireless system. In smart home networks, there have several wireless communication protocols. The most popular and standard wireless protocols are which IoT devices communicate, such as ZigBee, Z-Wave, Wi-Fi, and Bluetooth.

- Zigbee: Zigbee is the most standard and well-known wireless protocols with low power capability; it is reliable to use, robust, and scalable. This protocol is also secure and uses the AES-128 encryption algorithm. It is a global standard that uses 2.4 GHz, 868 and 915 MHz bandwidths and uses OQPSK and BPSK modulation techniques. It covers up to 10 meters, and the data rate is 250 kbps, 40 kbps, and 20 kbps. It uses mash network topology for connecting wireless devices.
- Z-wave: Z-wave is another popular wireless protocol with low power capability; it is also reliable to use, robust, and scalable. This protocol is also secure and uses an AES-128 encryption algorithm. It is a global standard that uses ISM bands 868 and 989 MHz and uses FSK and GFSK modulation techniques. It covers up to 100 meters and supports 9.6 kbps, 40 kbps, and 100 Kbps data. Z-wave also uses mash network topology for connecting the devices.
- Wi-Fi: Wi-Fi is the most popular and common wireless protocol with low power capability and reliable and robust features. Wi-Fi uses several WEP, WPA, and WPA2 security protocols, but WPA is more secure than others because it uses an AES-128 encryption algorithm. It is a global standard that uses 2.4 GHz and 5 GHz bands. It covers up to 50 meters and supports the 150-200 Mbps data rate, which depends on the channel frequency and several

antennas, and it can also support the 600 Mbps maximum data rate. Wi-Fi uses star network topology for connecting devices.

- Bluetooth: Bluetooth is another popular and standard wireless communication protocols with low power capability, reliability, and robustness. Bluetooth uses a secure E0 algorithm, which is a 128-bit symmetric stream cipher. It is a global standard that uses the 2.4 GHz, frequency band. It covers up to 150 meters and supports the 1 Mbps data rate. It uses point to point topology for connecting devices, which are known as piconets /37/.

3.2 Smart Home System Setup

3.2.1 Home Assistant

Home Assistant is a smart platform for home automation where anyone can add and control all the domestic smart devices. It is an open-source platform that is continuously improving by a large Home Assistant community. A Home Assistant comes with built-in security and privacy, and unlike some other platforms, it is not cloud-based, and it is possible that everything can be done locally.

For installing a Home Assistant, a user needs to download the latest version of the Home Assistant image file according to the raspberry pi compatibility. Raspberry Pi is the most common platform for running the Home Assistant because they are reliable, small, and consumes a small amount of electricity. This system and network setup uses raspberry pi 4 B and downloads the 32-bit, the recommended version.

After that, the user needs one SD card where the downloaded image file can be installed, and for that, the user needs to download the balenaEtcher application to flash the image. For doing this, the user needs to insert the SD card to the PC, open the Etcher application, select the Home Assistant image by clicking the plus sign, locate the SD card, and then click on the flash button flash.

Now the user has to configure the network and connect the Raspberry Pi via the home Wi-Fi WLAN. The user must then create a folder CONFIG inside the SD card, which is already labeled Hassos-boot. Again, the user must create another folder named network inside that folder, and here the user needs to create a text file called my-

network. Finally, inside the my-network file, the network instruction must be provided. The network configuration instructions are given below. The user must then give a unique id, a 128-bit number generated from uuid.org, the user's Wi-Fi SSID, and a password in the SSID and PSK section (Figure.5).

After that, the user must insert the SD card into the Raspberry Pi and power up the Pi. It will take some moments, and finally, must check the Homeassistant.local:8123, and the Home Assistant server is up and running (Figure.6) /38/.

```
[connection]
id=my-network
uuid=YOUR_UUID_NUMBER
type=802-11-wireless

[802-11-wireless]
mode=infrastructure
ssid=YOUR_WIFI_NAME
#Uncomment below if your SSID is not broadcasted
#hidden=true

[802-11-wireless-security]
auth-alg=open
key-mgmt=wpa-psk
psk=YOUR_WIFI_PASSWORD

[ipv4]
method=auto

[ipv6]
addr-gen-mode=stable-privacy
method=auto
```

Figure 5. Network Configuration Code for Home Assistant /38/.

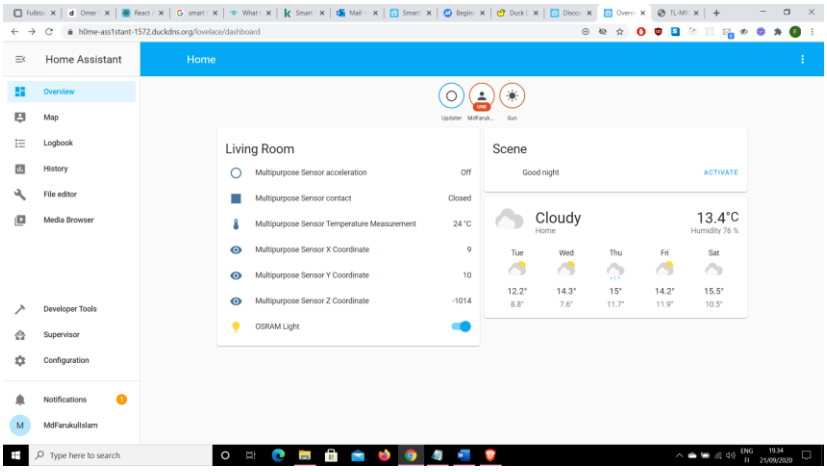

Figure 6. Home Assistant Interface /39/

3.2.2 Smart Hub

A smart hub is an IoT hub that controls all the smart devices of a home by using one mobile application. There are several IoT hubs in the market, but the most popular and common are Amazon Echo Plus, Google Home Hub, Securifi Smart Home Hub, Samsung SmartThings Hub, and Apple TV 4K. In this thesis, the Samsung Smart-Things hub is used for controlling the home's smart devices. A multipurpose sensor device is used to lock the door, one smart lite is used to control the room lite, and this hub sends the security alert to the user's mobile about the home's activity, for example, if someone opens the door. By using this smart hub, users can schedule the device to turn on and off automatically. If some devices are not working correctly, users can also monitor them using SmartThings. This Samsung SmartThings hub can also work with Amazon Alexa and Google Assistant for voice control. This hub supports Zigbee and Z-wave protocol for connecting to smart Home devices /40/.

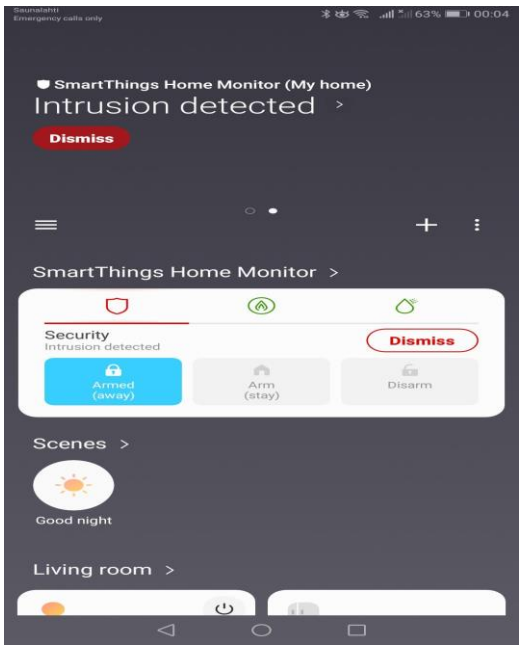

Figure 7. Mobile app detecting intrusion and activated alarm (Samsung Smart App).

3.2.3 Smart Devices and Sensors

Smart devices and Sensors are those IoT devices in which devices are connected to Home Assistant by using Smart Hub for making the home system smart. These devices and sensors are low cost, physically small, wireless, self-validation, robust, self-diagnostic, self-calibrating, and data pre-processing. There are a vast number of

IoT devices and sensors produced by different manufacturers for making home control smart and comfortable. This thesis uses smart light, a smart camera, and a smart multipurpose sensor supported by Samsung SmartThings and Zigbee, Z-wave wireless protocols /40/.

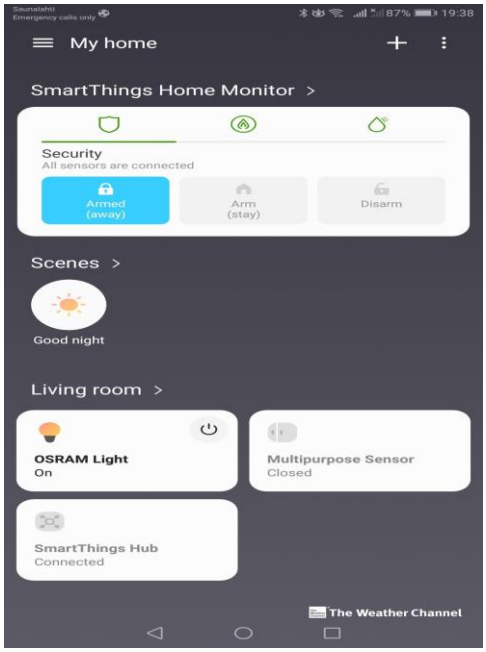

Figure 8. Controlling IoT Devices (Samsung Smart App).

3.3 Samsung SmartThings Hub:

The Samsung SmartThings can directly connect to the home broadband router network. It provides communications among all the connected IoT devices, SmartThings cloud servers, and SmartThings mobile applications. It can simply plug it into the router to provide power, connect any SmartThings device to the user's SmartThings account, and support a third-party SmartThings kit. It uses a connectivity management layer to connect SmartThings Hub to the cloud server and client as a mobile phone to the cloud server /41/.

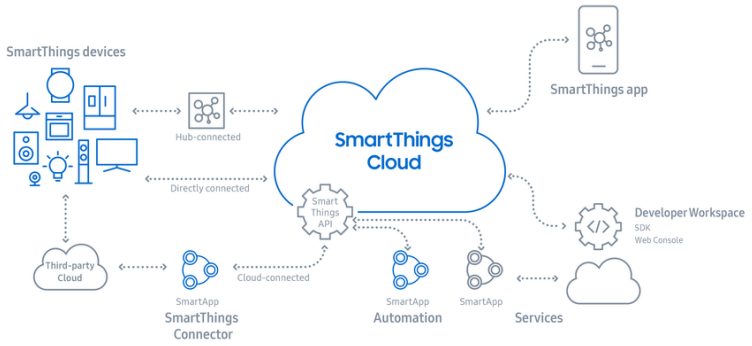

Figure 9. Samsung SmartThings Architecture /42/.

3.3.1 Security Vulnerabilities of Samsung SmartThings Hub

IoT comes with enormous benefits for users and challenges along with it. In IoT devices, maintaining security and privacy are more challenging for users. To discuss the security vulnerabilities of Samsung SmartThings Hub, the user must know what user information they collect and how long they keep those data. The service company, in this case, Samsung, collects user account information, including name, account ID, e-mail, mailing address, phone number, username and password, and third-party service partner's information through the cloud server. They collect different application data using app logs, groups, rules, location names, and other configurations. They receive device usage information such as sensors, SmartThings hubs, smart bulbs, home monitoring cameras and also collect usage information about home IoT devices, such as device model, name, group name, locations name, network information, surrounding network environment information, mobile country code, mobile network operator, OS version, IP address, and IMEI, sensors, error and malfunction logs. The company also obtains detailed information about the whole process and data of application usage information, and different technical error logs. The service company also collects the video, audio clips, images, and different smart devices' detailed information. That means they have access and control over the user's every bit of information. So, by using the SmartThings hubs, users have already compromised their own privacy to that organization. Moreover, if a hacker gets this information access, one's security and privacy are in danger. /43/.

One security research has proven that using smart hub vulnerabilities, and hackers can access the product's server and unveil their customers /44/.

Table 4. How long the Samsung SmartThings hub keeps user information /43/.

Data type	*Retention period*
Account Information	(i) Until you ask us to delete it, or (ii) Until you delete your Samsung account, whichever comes first
App, Appliance and Device Usage Information	(i) Until you ask us to delete it, or (ii) Until you delete your Samsung account, whichever comes first
Voice Information and Smart TV Information	(i) Until you ask us to delete it, or (ii) Until you delete your Samsung account, whichever comes first
Video and Audio Clips	Automatically delated after 30 days (unless you ask us to delete it/ you delete your Samsung Account) before that point.
Location Information	(i) Until you ask us to delete it, (ii) Until you delete your Samsung account, whichever comes first

3.3.2 Samsung SmartThings Hub Security

There are two default options to make the Samsung SmartThings hub secure: secure mode ON or OFF. Another security option is to allow or not to allow device firmware updates automatically. The hub's secure mode allows or blocks insecure ZigBee devices depending on toggle secure mode ON or OFF. Secure mode ON means Zigbee insecure network connection becomes disabled and insecure devices may drop off from the network. Furthermore, by allowing the device firmware automatic updates, any future firmware will update automatically /45/.

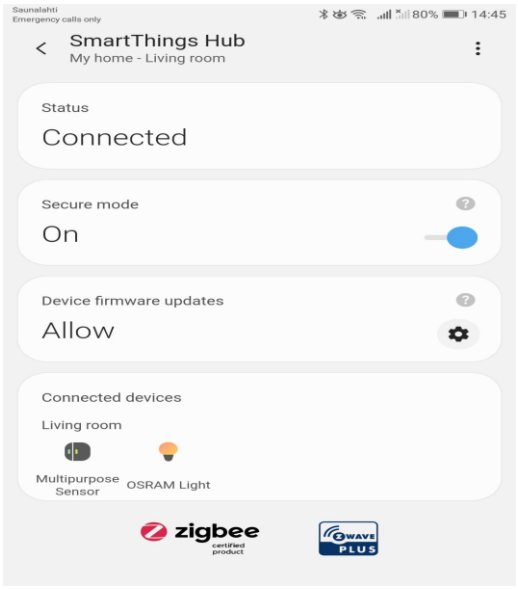

Figure 10. Samsung SmartThings hub security options (Mobile App).

3.4 Security Vulnerabilities of the Smart Home System

After implementing the smart home IoT system, the security vulnerabilities' default security system analysis is as follows.

- No default SSL or TLS protocol for the home assistant domain system establishes a secure connection between the browser and the server. By using these vulnerabilities, hackers can launch different cyber-attacks, such as Man in the Middle (MITM) attacks, SQL injection, Cross-site request forgery, Denial of Service Attacks, Code Injection, Defacement, Drive-by downloads, and take control of the system.
- For any browser to send the server's request, the network uses service port 80, which maintain HTTP protocol is not secure. In Hassio, the default service port is 8321, which is not secure, either. Using these vulnerabilities, hackers can launch a Man-in-the-Middle attack, Broken Authentication, SQL injection, Cross-site request forgery, Cross-site request forgery, Denial of Service Attacks, Code Injection, Defacement, and gaining access to the system.
- If hackers can somehow identify the router brand, then using the foot-printing or reconnaissance method, they could get the default router username and password for the TP-Link router username: admin and password: admin. So, it is easy to get control anyone's router by getting this default information.
- Some routers have their default network SSID and password, and anyone can quickly get this information tag from the router's body. If anyone knows the router name or model, it is easy to find out the SSID and password information. For getting this information, hackers can launch several attacks such as Credential Stuffing, Phishing, Brute Force**,** Rogue Wireless Devices, Peer-to-peer Attacks, Eavesdropping, Encryption Cracking, Authentication Attacks, MAC Spoofing, Wireless Hijacking, and take the system control.
- If the router's default firmware gets backdated, the hacker can modify the firmware and control the router's instruction. Finally, the router gets compromised and the system as well. To get the firmware control, hackers launch

different attacks, which are Malware and UEFI rootkits, Exploit firmware remotely, Physical tempering, Management backdoors, and supply chain attacks**.**

- By default, the router has no established access control over IP address or mac address. So hackers can launch attacks such as network sniffing attacks, spoofing a MAC address, Phishing, physical attack, social engineering, Credential Stuffing, and gaining access to the network.
- Usually, every network broadcasts its network SSID to the client. After getting an SSID, a hacker can quickly get the password by launching these attacks Credential Stuffing, Phishing, Brute Force**,** Rogue Wireless Devices, Peer-to-peer Attacks, Eavesdropping, Encryption Cracking, Authentication Attacks, MAC Spoofing, Wireless Hijacking and gets full control over the system.
- Users usually do not use any password manager; they usually set an easy password for their system and use the same password for every system they log in. They do this because it is an easy way to remember the password and ID. If any system is hacked, then every system will be vulnerable. Although some users set a different and strong password, they usually write these passwords somewhere in a plain format. This method is also risky because if the file is hacked, everything could be unveiled.
- In most routers, WPS is usually enabled along with WPA or WPA2 security protocol. The WPS protocol is easy to break because it needs only pressing buttons or entering a short pin to configure the network. Hackers can easily brute-force WPS using tools like Reaver.
- The firewalls, VPN, ALG in the router are not default enabled; hackers can take control of the system using attacks such as malware, worms, virus, rogue software, Malvertising, Man-in-the-middle (MitM) attack, Man-in-the-browser (MitB) attack, and Social engineering.

- The DoS protection and packet filtering in the router are not default enabled; the hackers can be launched attacks such as Syn flooding, Fragmentation attacks, TCP-State exhaustion attack, Application Layer Attacks, Plashing, and make the system fail.
- By default, a router uses the ISP provided DNS server, so it is easy for a hacker to down the server by launching different denial of service attacks such as DNS blocking and hijacking, DNS spoofing attack, DNS flood attack, Cache Poisoning, DNS tunneling, Distributed Denial of Service (DDoS).
- Without using any secure antivirus in a mobile phone or PC, secure browser, secure search engine, secure mailing system, VPN, anyone can be traceable and become a victim of cybercriminals. There also have Adware, Ransomware, Bot, Rogue Software, Trojan Horse, Phishing, Rootkit, Spyware, Virus, which are caring threats to everyday life /46- 53/.

3.5 Securing Home IoT System:

Based on the analysis of the IoT system vulnerabilities, it seems that there are several security loopholes, and the default security is almost none. To overcome this situation and secure the system, the users must implement security systems for the smart home IoT system.

- To implement a secure domain system for entering the home assistant interface by implementing a DuckDns secure SSL certificate. Now the connections are encrypted between the browser and server, and it is using a secure socket layer protocol.
- Using port forwarding to secure the browser service port, port 443, which is secure and maintains HTTPS protocol instead of Hassio default port 8321, uses the HTTP protocol. The connection will now get a secured communication through port 443 to deliver the data instead of other ports like 80, using the HTTP protocol or Hassio port 8123.
- Instead of default ID and password, the user needs to set a unique username and strong password for the router. S strong password is a minimum of 15 letters long, mixing with uppercase, lowercase, spatial char, and number. The user must change the password regularly and never use the same password to other accounts.

- The user needs to set up a new SSID and password for accessing the network. Instead of using the default SSID and password, users must set his/her own unique SSID and strong password. The password character must be a minimum of 15 letters long, mixing with uppercase, lowercase, spatial char, and number. Furthermore, these passwords must have to change regularly.
- The updated firmware must always be used for the IoT devices, including WLAN. The updated firmware version solved the vulnerabilities of the previous version.
- With MAC filtering created access control, which uses the MAC address of all my home devices connected to my router mobile, laptop, Hassio, hub, and the internet will only work for those devices after matching the mac address. Using this access control over the internet on devices will be restricted to connect with other unauthorized devices.
- The user's internet network SSID must be hidden. Broadcasting the network SSID must not be allowed. If someone wants to access the system, the hacker must find out the SSID.
- By using a password manager (last pass), which can store and encrypted all the passwords using SHA-256 hashing algorithms. It is easy to save, monitor, use, generate, and encrypt a long and strong password. Besides, the password manager supports two-factor authentication, which is hard to crack.
- Disabled WPS, which is lass secured, and Enabled WPA2-PSK, which uses AES encryption. WPS allows users to configure networks, only pressing buttons or entering a short pin. By disabling WPS, the user can reduce this risk.
- Enabling all the firewalls, VPN, ALG inside the WLAN. The firewall will protect us from some unauthorized, malicious activities and packet filtering. The VPN will hide the user IP, and the ALG will augment the firewall or NAT.
- Enabling DoS protection and setup packet filtering to the router. It will protect the system from different denial of service and distribution of denial of service attacks by filtering the packet.

- Choosing a different Domain Name System (DNS) server, the Google's Public DNS server on 8.8.8.8 and 8.8.4.4 for the IPv4 service instead of the ISP default DNS servers. If the user's default ISP DNS is attacked, the user will have a backup and switch to another DNS. Furthermore, using google's public DNS server is much more safe, fast, and secure for the user.
- Users can use antivirus software for his/her pc or mobile devices, can use a secure (Brave) browser for web browsing, using a secure (DuckDuckGo) search engine, use (proton mail) a secure mail, and use VPN for internet security. Antivirus software can protect the user from malicious software and different malware, even help intrusion detection /54/.

3.6 Security Analysis and Attack Vectors

In the previous section (section 3.4), the security system was built for the home IoT system. This discussion follows a security analysis for the home IoT system, the possible threats, and the attack vectors.

- Every operating system has "traceroute," a build-in function. By putting this command to the command prompt, users can see the connection routes, which traveled to the destination and shows up to 30 different gateways with IP addresses. When the user sends a DNS request through the browser, the server shows the IP address related to the given URL.

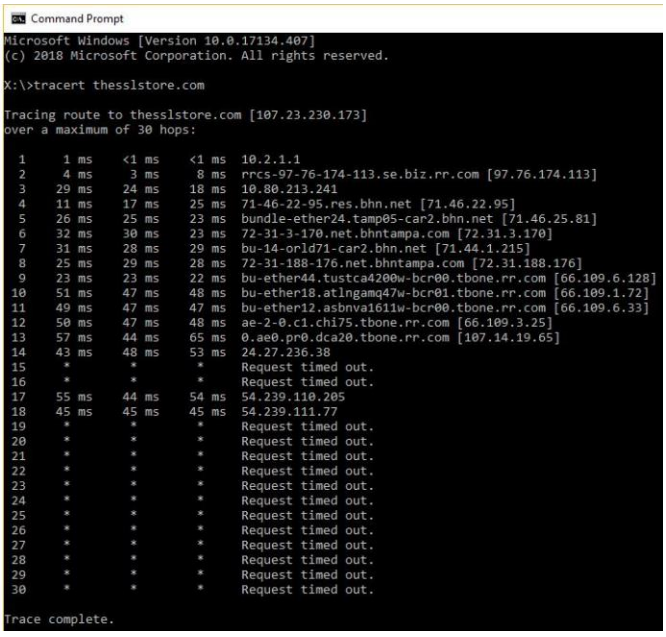

Figure 11. The "tracert" command shows the network hops /55/.

Every internet connection passes dozens of gateways to the destination and takes the different quickest path each time. Among all these hopes or gateways, not all are secure. In fact, most of these routers do not ever change the default ID and Password.

SHODAN is a search engine that can locate every device connected to the internet and returns information, such as IP address, device names, manufacturers, and firmware versions, especially in which devices are insecure. By using this, it is possible to use the IP address and search for specific devices. Moreover, the devices which are not secure and using default setting are targeted for MITM attacks. It is also possible to find the default admin ID and password by using a simple google search. Finally, using this information, anyone can gain unauthorized access to that device and perform a MITM attack.

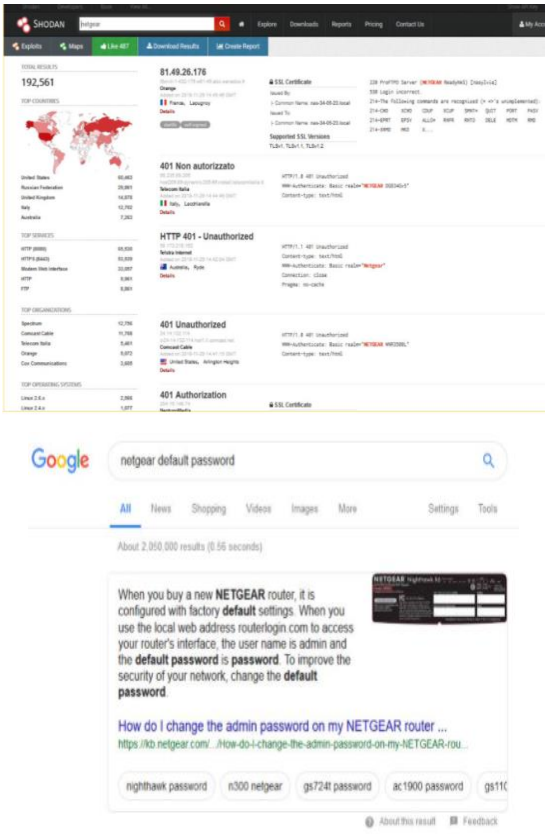

Figure 12. SODEN interface and searching NETGEAR password /55/.

The information which is transmitted through the network is encoded and broken into packets of data. Those packets of data can be inspected by using a packet sniffer, which is readily available on GitHub, and by Google search, hackers can make it more effective. Using this packet sniffer, the attacker can read every packet of data and any sensitive information passing via the HTTP protocol.

The only way to prevent these MITM attacks is to using SSL/TLS encryption and HTTPS protocol, which encrypts the transferred data on the way to the destination. The encrypted data can also be intercepted from the network, but it is unreadable and useless /55/.

- The SSL protected website using HTTPS can also be hacked. The SSL certificates can be breakable by using SSLScan and Kali Linux /56/.
- By using the commands below, the Wi-Fi network password or security key can be recovered. However, this method only works if that password was used previously to attach to the Wi-Fi.

  netsh wlan show profile

  windowsOS:netsh wlan show profile name="XXXXXXXX" key=clear

  MacOS: security find-generic-password -wa XXXXX

  By resetting the router is another option to recover the router username/password. From RouterPassword.com, it is possible to found the router default username/password.

  Another way to crack the network password using one Linux distribution is called Kali Linux, and it has all the necessary tools to crack a network integrated. By using Aircrack-ng, Airgeddon, KisMAC can crack the much stronger password and passphrases using WPA/WPA2 algorithms. Reaver-WPS is another tool used to break WPS and reveal a password, but this must have a strong router signal, and WPS turned on. In WPS, it can push a button on a Wi-Fi and another button on the router, and both find each other and automatically create an encrypted connection. Even if WPS is turned off still has the possibility to establish a connection /57/.

- Any firmware on the devices can be hacked. The firmware can be found from the vendor's website, OTA update sniffing, support groups, mobile applications, or dumping from the device. After getting the firmware by analyzing, emulating, and reverse engineering, it is possible to decrypt the firmware /58/.
- MAC filtering can be bypassed using different tools by Airman-ng, Wireshark, Airodump-ng, and macchanger tool /59/.
- The hidden network SSID can be revealed using Kali Linux tools Airmon-ng for network monitoring, Airdum-ng for discovering broadcasting network access points, and Airplay-ng for the de-authentication attack. After network monitoring, the hidden SSID shows as <length:0> and some other information, including the channel number. By listening to that channel and applying a de-authentication attack, it can get the network SSID /60/.
- A password manager is created to increase the user's security by generating, encrypting, and storing a strong password. However, unfortunately, researchers have found security vulnerabilities by researching five top password managers. So, using these vulnerabilities, hackers can steal a user's password from that password manager /61/.
- Hackers can bypass the firewall using Malicious use of authorized devices, Application vulnerabilities, Bypassing the perimeter, IP address Spoofing, Source Routing Attacks, Tiny Fragment Attacks.
- Hackers can bypass DoS protection using different attacks such as Syn flooding, Fragmentation attacks, TCP-State exhaustion attack, Application Layer Attacks, Plashing, DDoS.
- Hackers can occupy and stop the DNS server by using attacks like DNS blocking and hijacking, DNS spoofing attack, DNS flood attack, Cache Poisoning, DNS tunneling, Distributed Denial of Service (DDoS).
- Whatever security antivirus, search engine, browser, mail service a user is using, hackers can still catch up using different methods such as Adware, Ransomware, Bot, rogue software, Trojan Horse, phishing, Rootkit, Spyware, Virus /62/.

4 SECURITY PROPOSALS FOR DOMESTIC IOT SYSTEM

This part of the thesis explains the best security practices for the network (IoT network), software (applications), hardware (IoT devices), and data security (IoT data). The security instructions discussed here can be a bit complicated for the common home IoT users. According to the cybersecurity definition, security is a practice defending against different malicious activities /63/. The more knowledge anyone has about the network system, application system, hardware system, and data storage system, the more the user can defend themselves against malicious activities. That is why this part discusses the possible best security practice, and although this practice is not mandatory but recommended. Besides, cybersecurity is not only for IT professionals, and directly or indirectly, most people are dealing with cyberspace, so it is important to gain some security knowledge and practice those securities for their own safety /63/.

4.1 Public Awareness

Most people do not have any basic security knowledge, a strong password for logging their system. Some people still think they do not have any security threat, so they do not need to practice any security. Others really do not understand why they need to practice security. Some people know the importance and consequences of cybersecurity practice but are still carefree about security issues, and some of them use phone number or birthday for their password. Public awareness is essential for practicing at least basic security. Nowadays, anyone without security is also harmful to others. Without understanding, any malicious Trojan link or phishing e-mail can come from trusted friends, and both can be victims. Especially in a family, if a hacker tries to attack someone, it is too easy to target who has the weakest security knowledge. By using them, the hacker can get access to the family's common WLAN network. Anyone without knowing and without concern about cybersecurity can be a major threat to others. Overall, cybersecurity practices are not for some specific person who maintains cybersecurity; everyone must be aware of cyber threats and practice at least basic security. There is some proposal for taking steps of security awareness.

- Develop an effective security strategy for security awareness.
- Keep defensive practice up to date and always monitor the system.

- Security awareness training educates common system users on cyber threats, raises awareness about the sensitivity of data, how to avoid common attacks such as phishing e-mail or other scams, how to reduce data breaches, how to minimize the damages if the system got affected, and overall build a security compliance culture which will ensure the cyber safety /64/.

4.2 Risk Management

No system is perfectly secured. No matter how hard anyone tries or how complicated the security system anyone can build, the system can be hackable. Any stronger system with proper security can prevent the system from being hacked instantly. The strong layers of security a system has, the more days it could hold against the hacker. The user must always prepare for all kinds of situations. By analyzing the risk and prepare for the situation can save time, money, and possible damages. For better risk management practices, users can follow the below steps.

- First, the user must build a strong intrusion detection system. It is possible to reduce the damage or even prevent the attack if it can detect the attack earlier.
- The system user must prepare for the worst-case scenario and build up at least two backup systems.
- Besides, all the data must have more than two backup storage and store the data in different data centers of different global locations and a physical hard disc.
- The system user must measure the risk level and act according to the risk level.
- For cybersecurity purposes, the user must consider every possible threat and find out the reason and solution for that reason. Never underestimate any security vulnerability and threat. In cybersecurity, one small wrong step can ruin the entire system.
- Focus on internal threats.
- Continuous Monitoring and Recordkeeping.
- Cyber risk visualization by identifying patterns and mapping out networks.

- There is no fool-proof strategy for the system so that cybersecurity insurance can be beneficial /65/.

4.3 Network Security

It is better to use two network routers for practicing better network security, one without VPN support and another is with VPN support. This because some websites do not support VPN access, and anyone can hide true network identification using a VPN embedded router. Some best network security practices are described below.

To build a strong network, troubleshoot problems, evaluate third-party products, and develop effective applications, it is important to understand the basic OSI Model /66/.

Table 5. Internet OSI model and its functions /66/.

Layer	Function	Protocols
Application	E-mail, file servers, and file transfers.	HTTP, FTP, TFTP, DNS, SMTP, SFTP, SNMP, Rlogin, BootP, MIME.
Presentation	Encryption, data formatting, and code conversion.	MPEG, JPEG, TIFF.
Session	Establishing a connection between computer and negotiations.	SQL, X-Window, ASP, DNA, SCP, NFS, RPC.
Transport	Supporting end-to-end data delivery.	TCP, UDP, SPX.
Network	Packet routing.	IP, OSPF, ICMP, ARP, RARP.
Datalink	Error checking and message frame transfer.	Ethernet, Token Ring, 802.11.
Physical	Data sending over the network using physical interfaces.	EIA RS-232, EIA RS-449, IEEE, 802.

Another important thing to understand is network devices' building a strong network and defending the network /66/.

Table 6. Network devices and their functions /66/.

Network Devices	Functions
Hubs	Connect multiple Local Area Network (LAN), use as a repeater, which can amplify signals.
Switches	Connecting multiple LAN, more intelligent than a hub, working on the data link layer, can read hardware addresses.
Routers	Transmit packets and works on network layers.
Bridges	They use hardware media access control (MAC) to transfer frames to two or more hosts, working on physical and data link layers.
Gateways	Work on transport and session layers; they deal with vendors from different protocols.

The IoT users must know network defenses for using proper devices and defend the network /66/.

Table 7. Network defense solutions and its functions /66/.

Network Defences	Functions
Firewall	Isolate one network from another can be both hardware and software firewall solutions.
An intrusion detection system (IDS)	Spotting malicious activities on the network and use data logged events to defend the future similar intrusion.

Network Access Control (NAT)	Restricting endpoint devices from network resources according to security policy.
Web Filters	Preventing the browser from loading specific web pages.
Proxy servers	Traffic filtering and performance-enhancing.
Load balancers	Minimize the server overwhelming and optimize the bandwidth.

Segmenting networks into different zones based on logical or functional units is called network segmentation, which is important to defend the network /66/.

Table 8. Network segment and its functions /66/.

Network Segment	Functions
Public network	Everyone can get access to the internet.
Semi-private network	In between public and private networks, under some regulation, it can carry confidential information.
Private network	Handle confidential and proprietary data.
A demilitarized zone (DMZ)	A firewall separates the secure region of a private network.

- Every secure device must be placed at a critical point, such as a firewall that can be placed in every network zone junction.
- Network Address Translation (NAT) can be used to translate private addresses into public addresses.
- It is recommended not to disable Personal Firewalls.
- Try to use centralized logging and immediate log analysis for tracing suspicious login.
- Use proxy servers for routing direct internet access from workstations.

- Use Honeypots and Honeynets for the attackers.
- Secure the network equipment physically.
- Use an intrusion detection system (IDS) properly to monitor suspicious activity.
- Use VPN for accessing the public internet and always need to monitor and baseline network protocols /66/.

4.4 Software Security

The software must be updated, and pirated software should never be used because of all the trap hackers set through this pirated software. For software security, users can practice these steps, as described below.

- Patch the software and system regularly to ensure that all the systems are up-to-date software.
- Educate and train all the system users to follow some basic security practices.
- Automate routine tasks such as device security configurations and analyzing firewall changes to automate day-to-day security tasks.
- Enforce the least privilege to access the system, and it also eliminates the rights of unnecessary access.
- Create a robust incident response (IR) plan to minimize the damages, even if the system got attacked.
- Segment the network and limit the traffic controls on those network segments.
- Monitor user activities to ensure that users are following the best security practices /67/.

4.5 Hardware Security

It is impossible to ensure the user's hardware security because most of the IoT devices are embedded, and only manufacturers can change it or update it. Wt Users can buy the product from a reputed brand because it always tries to give the best security product. They will never want to lose their reputation because of some security scam. The possible hardware security a user can provide is discussed below.

- Provide physical security to avoid the stealing of the device.
- After using, the user must destroy the device. Otherwise, hackers can collect potential information from those devices.
- If possible, lock the hardware device using a strong password to avoid unauthorized access /68/.

4.6 Data Privacy and Security

We can use several data back-ups in several places for data security, such as a local hard drive, personal computer, and more than one cloud server. For better data security practice, the system owners can follow the steps described below.

- Lockdown data Access and it also depends on the data sensitivity.
- Use basic security authentication login using a strong password for accessing the data.
- The user's data can be stored using decentralized cloud storage services such as Storj, Sia Network, Filecoin, and MaidSafe, for better data privacy and security. /69/.
- The backup can be stored in a secured and private physical hard disk.
- Embrace multi-factor authentication for getting access to the system /70/.

5 FINDINGS

In this thesis, the home IoT system developed has one home WLAN connected to the public internet. Under this home router, the system has a mobile/laptop, Samsung SmartThings Hub, Home Assistant, using the Wi-Fi protocol. Again, under the Samsung SmartThings Hub, there are some IoT devices, such as multipurpose sensors and smart light, which are using Zigbee protocol. The Samsung SmartThings Hub sends all the data from IoT devices and sensors to the Samsung Cloud Server, and by using a Samsung smart mobile app, users can control and monitor home IoT devices. This system is also integrated with the IoT platform Hassio, which can also access the data server. Using the Hassio UI, the user can also control and monitor IoT devices locally.

Figure 13. Samsung SmartThings Cloud /71/.

By analyzing the implemented home IoT system, the user has less scope for implementing security over the home IoT system.

- The user can ensure network security by securing a home router (WLAN/LAN).
- Thus, inside the network, the user can only update the device firmware; some default security features trigger ON/OFF (Samsung SmartThings Hub), use password authentication, and encrypt the browser server communication (Home Assistant) using an SSL certificate.
- The user cannot implement or change or modify or update anything over IoT devices, but it depends on product default security and the next security patch's arrival.

- The most important thing is data privacy. In every security system, the goal and aim for that security are to protect the system data. While using different manufacturer's products, they collect user's data and keep them to some remote cloud servers. The user can use this data (using mobile apps or some IoT platform like Hassio). The users or the data owners cannot control their private data, but the manufacturers do. Because here, the data are owned by the organizations, not the data owner. Even after deleting a user account, the user is not sure about his or her data being deleted from the server or not.
- Using different decentralized cloud storage services that are using blockchain technology, these issues can be solved because these service providers claim that the organizations do not own the data. Instead, the owner himself owns the data and can access it securely and quickly /69/.

6 CONCLUSIONS AND LIMITATIONS

With the proliferation of modern technological improvement and tremendous internet revolution, IoT has become a great advantage for automating our home, production, and manufacturing process. Our everyday daily life is getting much easier and better by using these Internet of Things devices. This IoT technology aids not only us but also criminals. It is much easier for a criminal to spy on internet users, blackmail theme from anywhere in the world, destroy production, and even kill anyone by simply giving a command through the technology. Using a public Wi-Fi network is the most effective threat for users because hackers always target public Wi-Fi and use the network as a lure for people.

Nowadays, IoT devices are connected almost everywhere. Everybody is directly or indirectly encountering this technology in their everyday life. There is no skipping from this technology but face it to establishing and maintaining some proper and strong security protocols. The internet was invented to make people's lives convenient, but it also gave criminals an online platform to expand their criminal activities. All technology has its advantages and disadvantages depending on the positive and negative use of that technology.

This thesis's prime objective was to study domestic IoT devices' security, develop one IoT network, and secure that home IoT network. Some strong security recommendations and proposals for the domestic IoT device users' best security practices were also made by analyzing the vulnerabilities. The users' best security practices search's outcome is that no system is perfectly secure and safe, and it is impossible to build such a system. No one can totally avoid a hacker's access to their system. Still, hackers' efforts can be made difficult and time-consuming by implementing multiple security layers and preparing for any situation. The user must ensure maximum security for their system and always monitor the system and upgrade the security patch. To ensure IoT security is not a simple thing. Network security, software security, hardware security, and data security, all possible routes that must be checked and secured.

The limitations of this thesis emerge from the aforementioned findings. This thesis provides security guidelines for IoT device users, but the devices that come with the manufacturer's security vulnerabilities are still a great thread. In fact, in this case, the user must wait for certain security patches or firmware updates, which are time-consuming and increase the risk. The users also have no idea about the data server security, and this also depends on the service provider companies.

REFERENCES

/1/ IOT Analytics. Accessed 15.08.2020. https://iot-analytics.com/internet-of-things-definition/

/2/ ZDNet. Accessed 15.08.2020. https://www.zdnet.com/article/what-is-the-internet-of-things-everything-you-need-to-know-about-the-iot-right-now/

/3/ SECURITY Today. Accessed 15.08.2020. https://securitytoday.com/articles/2020/01/13/the-iot-rundown-for 2020.aspx#:~:text=How%20many%20IoT%20devices%20are,are%20connected%20to%20the%20web

/4/ I-SCOOP. Accessed 15.08.2020. https://www.i-scoop.eu/internet-of-things-guide/iot-endpoints-2020/#:~:text=With%20an%20impressive%2042%25%2C%20building,and%200.44%20billion%20IoT%20endpoints.

/5/ eeNews ANALOG. Accessed 17.08.2020. https://www.eenewsanalog.com/news/automotive-enterprise-iot-endpoints-reach-58-billion-2020

/6/ iotforall. Accessed 19.08.2020. https://www.iotforall.com/7-most-common-iot-security-threats-2019/

/7/ UBUNTU PIT. Accessed 19.08.2020. https://www.ubuntupit.com/25-most-common-iot-security-threats-in-an-increasingly-connected-world/

/8/ Vulnerabilities in IoT Devices for Smart Home Environment. Accessed 20.08.2020. file:///C:/Users/mfisl/Downloads/ICISSP_2019_100_CR.pdf

/9/ SEMENTIC SCHOLAR. Accessed 21.08.2020. https://www.semanticscholar.org/thesis/Secure*BPMN-%3A-a-graphical-extension-for-BPMN-2.0-on-Cherdantseva/4887dbc62514f7a9e47ad360901be96e9ebdb293/figure/21

/10/ NetBurner. Accessed 21.02.2020. https://www.netburner.com/learn/architectural-frameworks-in-the-iot-civilization/

/11/ Journal of Sensor and Actuator network. Accessed 21.08.2020. file:///C:/Users/mfisl/Downloads/jsan-08-00022-v3.pdf

/12/ RESEARCHGATE. Accessed 21.08.2020. https://www.researchgate.net/figure/oT-represented-by-a-seven-layer-architecture-Source_fig3_329520432

/13/ Norton. Accessed 26.08.2020. https://us.norton.com/internetsecurity-emerging-threats-what-is-the-difference-between-black-white-and-grey-hat-hackers.html

/14/ Netwrix Blog. Accessed 07.09.2020. https://blog.netwrix.com/2018/05/15/top-10-most-common-types-of-cyber-attacks/

/15/ ubidots. Accessed 07.09.2020. https://ubidots.com/blog/open-source-home-automation/

/16/ the ambient. Accessed 07.09.2020. https://www.the-ambient.com/guides/smart-home-sensors-essential-guide-896

/17/ THIS IS WHY IM BROKE. Accessed 07.09.2020. https://www.thisiswhyimbroke.com/smart-home-devices/

/18/ HOME Stratosphere. Accessed 07.09.2020. https://www.homestratosphere.com/smart-home-sensors/

/19/ safewise. Accessed 07.09.2020. https://www.safewise.com/resources/home-security-cameras/

/20/ PC. Accessed 07.09.2020. https://uk.pcmag.com/home-security-cameras/121565/the-best-uk-smart-home-security-systems

/21/ T3. Accessed 07.09.2020. https://www.t3.com/features/best-smart-plugs

/22/ Wave. Accessed 07.09.2020. http://waveav.solutions/home-climate-control-eco-home-automation-control.html

/23/ PC. Accessed 07.09.2020. https://uk.pcmag.com/smart-locks/77460/the-best-smart-locks

/24/ Clas ohlson. Accessed 07.09.2020. https://www.clasohlson.com/fi/WiFi-Smart-Bulb-Clas-OhlsonHome/p/Pr388774000

/25/ SEMANTIC SCHOLAR. Accessed 28.08.2020. https://www.semanticscholar.org/thesis/Wireless-protocol-design-for-smart-home-on-mesh-Fathany-Adiono/6f4e05683fe41be1af1bc492705a2fdd6ce251ba/figure/0

/26/ PHILIPS hue. Accessed 08.09.2020. https://www2.meethue.com/fi-fi/support/security-advisory

/27/ IKEA. Accessed 15.09.2020. https://www.ikea.com/fi/fi/product-guides/ikea-home-smart-system/

/28/ Clas ohlson. Accessed 15.09.2020. https://www.clasohlson.com/fi/Elektroniikka/%C3%84lykoti/c/2633

/29/ Electro maker. Accessed 15.09.2020. https://www.electromaker.io/blog/article/9-best-raspberry-pi-smart-home-software-options

/30/ The Magpi. Accessed 15.09.2020. https://magpi.raspberrypi.org/articles/home-automation-add-ons-for-raspberry-pi

/31/ Software Testing Help. Accessed 15.09.2020. https://www.softwaretestinghelp.com/iot-devices/

/32/ iotforall. Accessed 15.09.2020. https://medium.com/iotforall/smart-home-protocols-thread-zigbee-z-wave-knx-and-more-71efa4b410e1

/33/ ALARM NEW ENGLAND. Accessed 15.09.2020. https://www.alarmnewengland.com/blog/home-automation-protocols

/34/ Zwave. Accessed 15.09.2020. https://www.z-wave.com/

/35/ RANDOM NERD TUTORIALS. Accessed 16.09.2020. https://randomnerdtutorials.com/what-is-mqtt-and-how-it-works/

/36/ IFTT. Accessed 15.09.2020. https://ifttt.com/

/37/ DESIGNSPARK. Accessed 17.09.2020. https://www.rs-online.com/designspark/eleven-internet-of-things-iot-protocols-you-need-to-know-about

/38/ JUANMTECH. Accessed 18.09.2020. https://www.juanmtech.com/guide-to-home-assistant

/39/ Home Assistant. Accessed 21.09.2020. https://h0me-ass1stant-1572.duckdns.org/lovelace/default_view

/40/ Safety.com. Accessed 21.09.2020. https://www.safety.com/best-smart-home-hubs/

/41/ SmartThings Classic Documentation. Accessed 21.09.2020. https://docs.smartthings.com/en/latest/architecture/

/42/ RESEARCHGATE. Accessed 21.09.2020. https://www.researchgate.net/figure/Samsung-SmartThings-architecture-23_fig4_332532551

/43/ SmartThings Privacy Notice. Accessed 22.09.2020. https://eula.samsungiotcloud.com/legal/europe/en/pps.html

/44/ kaspersky. Accessed 22.09.2020. https://www.kaspersky.com/about/press-releases/2018_smart-hack-kl-discovers-smart-home-hub-vulnerable-to-remote-attacks

/45/ SAMSUNG. Accessed 22.09.2020. https://www.samsung.com/sg/support/mobile-devices/overview-of-samsung-smartthings-secure-mode/

/46/ TECH BRIEFS. Accessed 24.09.2020. https://www.techbriefs.com/component/content/article/tb/pub/features/articles/33212

/47/ Quora. Accessed 24.09.2020. https://www.quora.com/If-a-professional-hacker-can-hack-https-websites-then-why-are-the-websites-moving-for-https-instead-of-http-for-security

/48/ SOLID STATE SYSTEM LLC. Accessed 24.09.2020. http://solidsystemsllc.com/firmware-security/

/49/ SentinelOne.blog. Accessed 24.09.2020. https://www.sentinelone.com/blog/7-ways-hackers-steal-your-passwords/

/50/ hashedout. Accessed 24.09.2020. https://www.thesslstore.com/blog/firmware-attacks-what-they-are-how-i-can-protect-myself/

/51/ HELP DESK GEEK. Accessed 24.09.2020. https://helpdeskgeek.com/networking/mac-address-filtering/

/52/ ACCESSAGILITY. Accessed 24.09.2020. https://www.accessagility.com/blog/why-ssid-hiding-is-not-secure

/53/ GURU99. Accessed 24.09.2020. https://www.guru99.com/how-to-hack-website.html

/54/ ITPro. Accessed 25.09.2020. https://www.itpro.co.uk/general-data-protection-regulation-gdpr/secure-your-wi-fi-against-hackers-in-10-steps

/55/ hashedout. Accessed 28.09.2020. https://www.thesslstore.com/blog/man-in-the-middle-attack-2/

/56/ HackeRoyale. Accessed 28.09.2020. https://www.hackeroyale.com/hack-ssl-sites-using-sslscan/

/57/ PCMag. Accessed 28.09.2020. https://uk.pcmag.com/how-to/40259/how-to-hack-wi-fi-passwords

/58/ IOT Pentesting Guide. Accessed 28.09.2020. https://www.iotpentestingguide.com/firmware-hacking.html

/59/ InfoSec Adventures. Accessed 28.09.2020. https://medium.com/infosec-adventures/bypass-mac-filtering-6036235699c8

/60/ Hackernoon. Accessed 28.09.2020. https://hackernoon.com/uncovering-hidden-ssids-8hons3x5i

/61/ Laptop. Accessed 28.09.2020. https://www.laptopmag.com/news/popular-password-managers-can-get-hacked-should-you-keep-using-them

/62/ Insights For Professionals. Accessed 28.09.2020. https://www.insightsforprofessionals.com/it/security/hacks-sure-to-defeat-your-firewall

/63/ kaspersky. Accessed 30.09.2020. https://www.kaspersky.com/resource-center/definitions/what-is-cyber-security

/64/ MetaCompliance. Accessed 30.09.2020. https://www.metacompliance.com/blog/how-to-promote-cyber-security-awareness-in-your-organisation/

/65/ University of San Diego. Accessed 30.09.2020. https://onlinedegrees.sandiego.edu/cyber-security-risk-management/

/66/ netwrix. Accessed 01.10.2020. https://www.netwrix.com/network_security_best_practices.html

/67/ SYNOPSYS. Accessed 01.10.2020. https://www.synopsys.com/blogs/software-security/top-10-software-security-best-practices/

/68/ Embedded.Accessed 01.10.2010. https://www.embedded.com/iot-security-physical-and-hardware-security/

/69/ DevTeam.Space. Accessed 01.10.2020. https://www.devteam.space/blog/how-to-build-a-decentralized-cloud-storage-solution-like-storj-io/

/70/ FormAssembly. Accessed 01.10.2020. https://www.formassembly.com/blog/data-security-best-practices/

/71/ Craftroom. Accessed 05.10.2020. https://craftroom.tizen.org/smart-motion-light-smartthings/