Republic of Iraq
Ministry of Higher Education and Scientific Research
University of Babylon
College of Engineering
Department of Electrical Engineering

Efficient Implementation of Cloud-Based Smart Home Automation System

A Thesis

Submitted to the Council of The College of Engineering, the University of Babylon in Partial Fulfillment of the Requirements for the Degree of Master in Engineering\ Electrical Engineering\ Communication

By

Anwer Sattar Hamzah Hadi

Supervised by

Prof. Dr. Laith Ali Abdul-Rahaim

2022 A.D ***1444 A.H***

بِسۡمِ ٱللَّهِ ٱلرَّحۡمَٰنِ ٱلرَّحِيمِ

ٱقۡرَأۡ بِٱسۡمِ رَبِّكَ ٱلَّذِى خَلَقَ ﴿١﴾ خَلَقَ ٱلۡإِنسَٰنَ

مِنۡ عَلَقٍ ﴿٢﴾ ٱقۡرَأۡ وَرَبُّكَ ٱلۡأَكۡرَمُ ﴿٣﴾ ٱلَّذِى

عَلَّمَ بِٱلۡقَلَمِ ﴿٤﴾ عَلَّمَ ٱلۡإِنسَٰنَ مَا لَمۡ يَعۡلَمۡ

(صدق الله العلي العظيم)

سورة العلق : ألآيات (١- ٥)

Dedication

To the one who left us without me touching her forehead or me looking at her even for a moment.

My Dear Mother

To my father, endless Love, Support, and Encouragement

To my wife... the companion of the struggle and the difficult circumstances who did not hesitate to help me... Huda

To my beloved, my children, Yousif, Younis

To all researchers and students of knowledge

I dedicate this humble work

Anwer Sattar

Supervisor Certification

We certify that this thesis, entitled "**Efficient Implementation of Cloud-Based Smart Home Automation System**" was prepared by **Anwer Sattar Hamzah Hadi** under our supervision at the Department of Electrical Engineering, College of Engineering, University of Babylon, as partial fulfillment of the requirements for the degree of Master of Science in Engineering/ Electrical Engineering/ Communications.

Signature:

Name: Prof. Dr. Laith Ali Abdul Rahaim

(Supervisor)

Date: / / 2022

In view of the above recommendation, I forward this thesis for debate by the Examination Committee.

Head of Electrical Department

Signature:

Asst. Prof. Dr. Shamam Fadhil Alwash

Name:

Date: / / 2022

Examining Committee Certificate

We certify that we have read this thesis entitled" **Efficient Implementation of Cloud-Based Smart Home Automation System**" and, as the examination committee examined the student **Anwer Sattar Hamzah Hadi** in its contents and that in our opinion it meets the standard of a thesis for the degree of Master in Electronics and Communications Engineering.

Signature:
Name: Prof. Dr. Haider Jabbar Abd
Title: Professor
Date: / / 2022
(Chairman)

Signature:
Name: Dr. Mohammed Shakir Mahmood
Title: Assistant Professor
Date: / / 2022
(Member)

Signature:
Name: Dr. Hilal Abdul Hussein AL-Libawy
Title: Assistant Professor
Date: / / 2022
(Member)

Signature:
Name: Dr. Laith Ali Abdul Rahaim
Title: Professor
Date: / / 2022
(Member/ Supervisor)

Signature:
Name: Dr. Shamam Fadhil Alwash
Title: Asst. Prof.
Address: Head of Electrical Department
Date: / / 2022

Signature:
Name: Dr. Hatem Hadi Obeid
Title: Professor
Address: Dean of the College of Engineering
Date: / / 2022

Acknowledgments

First, I want to thank God for helping me and giving me the strength, willingness, and patience to finish what I have started.

I would like to express my gratitude, faithfulness, appreciation, and deep respect to my supervisor.

Prof. Dr. Laith Ali Abdul-Rahaim

For coming up with the idea for the project, supervising it, helping with it, giving me help, and giving me advice all the time.

My special thanks to all my friends who encouraged me to finish my studies. Also, thanks go to all the staff in the Department of Electrical Engineering, College of Engineering, University of Babylon.

I owe special thanks to my precious family, my father, and my brothers, who supported me and helped me throughout my life and during this study.

Finally, I want to thank my wife and my lovely children for being patient, understanding, and supportive through the toughest moments of my life. Thank God for enlightening my life with their presence.

Anwer Sattar

Abstract

Smart home automation is one of the main topics of the current era, which has attracted the attention of researchers for several years because smart home automation contributes to the realization of many capabilities. Specialists have begun to exploit the technological and scientific revolutions in this regard. When the age of automation, the Internet, and the Internet of Things started, smart homes were developing and growing to include many important features that helped a lot with things like saving energy, making a good environment, preventing fires and toxic gas leaks, and keeping your home safe.

The proposed system, which has been practically designed and implemented, includes several vital aspects of smart homes. The system focused first on home security, due to the increased rate of crime and theft and build a smart home that controls and monitors all the entrances to the house that are often vulnerable to intrusion by intruders based on personal identification using face detection and recognition technology, in addition to using the Radio Frequency Identification (RFID) technique as a mechanism to improve the performance of home security systems. The cloud server analyzes the identity of the receiving member to retrieve the home entry pass. The system was effective and responsive in transmitting live footage of any illegal intrusive activity at the door or windows of the house. Where the processing to open the door from the local computer took about 2 seconds, and the processing from cloud computing took about 3 seconds, which is a record time as compared with other systems. Many features have been added to achieve seamless monitoring and control in this field.

The second approach implemented in the proposed smart home automation system is to detect any leakage of gases, smoke, or fires with a warning via telegram app to the owner when any danger is detected and achieves

the right climate for the home, and reduces energy consumption. The proposed system is built using a sensor to detect fires, toxic gases, and smoke.

Another one that measures temperature and humidity and controls the cooling and heating systems operation based on the set value to turn each on/off, with a motion sensor that ensures none of these devices works when the house is empty. Two threshold values have been added to avoid continuously turning machines on and off when the temperature fluctuates at a certain value. These sensors are also connected to a small, open-source microcontroller that will transmit data and values via Wi-Fi to the cloud, and then display important results to the homeowner.

List of Contents

List of Abbreviations

API	Application Programming Interface
C#	C Sharp
CC	Cloud Computing
CD-RW	Compact Disc-Rewritable
CPU	Central Processing Unit
CSS	Cascading Style Sheets
DNA	Deoxyribonucleic Acid
FFD	Full Function Device
GHz	Giga Hertz
GUI	Graphical User Interface
H. W	Hardware
HDD	hard Disk Drive
HPC	High-Performance Computing
HTML	Hyper Text Markup Language
I2C	Inter-Integrated Circuit
IAAS	Infrastructure as a Service
IC	Integrated Circuits
ICSP	In-Circuit Serial Programming
IDE	Integrated Development Environment
IEEE	Institute Electrical and Electronics Engineers
IOT	Internet of Things
IP	Internet Protocol
IrDA	Infrared Data Association
ISO	International Organization for Standardization
JSON	JavaScript Object Notation
LAN	Local Area Network

LED	Light-Emitting Diode
LPG	Liquefied Petroleum Gas
MOS	Metal Oxide Semiconductor
MPI	Message Passing Interface
MSSQL	Microsoft-Structured Query Language
NIST	National Institute
NTC	Negative Temperature Coefficient
OS	Operating System
OSI	Open Systems Interconnection
PAAS	Platform as a Service
PAN	Personal Area Network
PC	Personal Computer
PDA	Personal Digital Assistant
PPM	Parts per million
RFD	Reduced Function Devices
RFID	Radio Frequency Identification
RSA	Rivest-Shamir-Adleman
S. W	Software
SAAS	Software as a Service
SSD	Solid-State Drive
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
UART	Universal Asynchronous Receiver/Transmitter
UIDs	Unique Identifiers
UHF	Ultra-High Frequency
USB	Universal Serial Bus
UWB	Ultra-Wide Band (UWB
WAN	Wireless Area Network
WI-FI	Wireless Fidelity

WiMAX	Worldwide Interoperability for Microwave Access
WLAN	Wireless-Local-Area-Networks
WMAN	Wireless Metropolitan-Area Networks
WPAN	Wireless -Personal-Area- Networks
WWANs	Wireless Wide Area Network
µW	Microwaves

List of Tables

List of Figures

Chapter One

General Introduction

Chapter One

General Introduction

1.1 Introduction

Smart home automation is a broad term to express any device that could eliminate the repetitive behavior of household tasks. More accurately, smart home automation refers to the fluent integration of all things connected, smart, and automatic devices that control the entire home environment to the user's desire.[1][2]. The mechanism of protecting houses with a lock and key has become a traditional mechanism, and relying on it is somewhat risky. Therefore, it was necessary to secure the home in more modern ways. The activation of home security equipment such as cameras, motion and sound detectors, etc., has several benefits. It also allows you to monitor children, People with special needs individuals, and the elderly [3]. Under worsening climatic and weather circumstances, it is now simple to construct pleasant and suitable smart home systems, therefore reducing fire catastrophes and poisoning by poisonous gases and smoke [4]. The reducing of electrical energy consumption has become one of the most important topics that smart home projects focus on due to the high costs consumed by air conditioners, heating systems, fans, and lighting[5]. With the increased popularity of smart homes, more connections are being established. As a consequence of this great improvement in connection, issues such as the expansion of Internet-uploaded data, information security, and irregular response times have emerged. To develop acceptable solutions to these challenges and to propose an appropriate concept of the situation, fog computing has been proposed to manage large and sensitive data related to security and latency. Fog computing acts as an intermediary between different IoT devices and cloud-based servers on the supply side (cloud layer) or the demand side (user device layer)[6].

1.2 Literature Review

This section of the introduction will discuss several pertinent works, which are listed below:

Kushank Sehgal and Richa Singh (2019)[7]. proposed a security system that relies on IoT and cloud computing and SMS messages. The cloud processes the data and sends it to the owner. A motion sensor was used. As a result, the system will close all doors and windows; then, it will send an alert message to the owner. Another system has been used, which is the correct key system; the system works when the wrong key is entered and pushed hard. All these sensors were connected to the Arduino MEGA ADK and the Amazon cloud server

Musaddak M. Abdul Zahra et al (2020) [8]. It showed a home security system using cloud computing with the ESP Arduino system. They improved the previous system by adding a wireless camera from Zmodo ZP-IBI13-WiF and using GSM to call a specific number when there is no internet connection. Three types of sensors were used (Gas, Temp, and Motion) connected to the ESP8266 Microcontroller as a Wi-Fi device to transfer data from these sensors to the cloud server and from there to the web server in Apache and MySQL format. The camera is directly connected to the web server. It can be opened directly through an application on a mobile phone.

Shaik Anwar and D. Kishore implement this (2016) [9]. It is based on the Raspberry Pi, PIR motion sensor, Raspberry Pi camera module, and an image storage feature received in the RAM in the Raspberry Pi, which sends a picture of the person via the user's e-mail. Other features were added to this system without depending on the cloud. The user can send a sound alert from his mobile phone if there is an intruder; the door lock can be controlled through the Android platform. The owner can open the camera directly at any time.

P.Amith Teja et al (2021). [10]. Use a Raspberry Pi, a camera, a PIR, an I.R., and a Piezo to find out who is there, temperature, and what sounds are around.

The system sends a message to the owner and then takes pictures and records a live video of the place when the event occurs, using the IoT cloud for GUI.

Shraddha Somani et al (2019) [11]. Introduced the same concept as the previous one with the addition of SMS via a phone in the event of an intruder. They used AES to encrypt the data to obtain security over the network. Other sensors have been connected to the Raspberry Pi, such as MQ2 and DHT22, to preserve the environment in the smart home.

M.Medhat et al (2020) [12]. It was based on the concept of fog computing. The system consists of three-layer sensors (open door, glass breaker, PIR, fi, re and water leakage sensors, and Arduino board) layer, a fog computing layer (Raspberry Pi and Camera Pi), and a cloud layer. This system can reduce the amount of data sent to the cloud. When this system was compared to the cloud system using the iFogsim Toolkit, the results showed that fog computing has made clear progress in terms of how long it takes to set up and how quickly it works.

T.Juhana, and V. Anggraini (2016) [13]. Based on a camera will detect an intruder by subtracting the current image from the background frame and activating the alarm to alert the homeowner when the intruder exists and sending the image to Dropbox to notify the owner aware at an early moment. The researcher treats the lack of detection accuracy that may be happened by using threshold value when making a comparison between the previous background and the current frame in terms of pixel count (white and black pixels) for the frame.

S. Fattah and F. Mahmood (2019) [14]**.** The main goal of this system was to secure, monitor, automate, and control home appliances according to the powers assigned to each member of the home by using cloud services and biometric techniques. The system begins to recognize faces, takes a picture of the face, and uses the DWT and PCA methods to extract image features, reduce the image, and get the matching operation using Euclidean distance. Using the MATLAB

procedure, the user index can be sent to the cloud server; the cloud will analyze the member's identity to retrieve the member's profile and give permission.

M. Dhobale (2020) [15]. Based on facial recognition using a Pi camera type, motion sensor, and ultrasonics with the Raspberry Pi as the main controller. The system takes a picture of the person near the door. Then the LBP program in the Raspberry Pi compares the picture with the pictures previously stored in the SD RAM of the Raspberry. Once the face is recognized, the door will open directly. At the same time, if it is a stranger, the photo will be sent via Gmail.

N.Tkauc et al (2020) [16]. The programs used in facial recognition are often poorly performing, have low accuracy, and are prone to errors, so an online platform was adopted for face detection and recognition. Therefore, Amazon Web Services (AWS) were used in this regard. The mechanism of this project lies in the entry of employees and visitors to a company or factory building by recognizing the face. Then a special code is generated for the employee who intends to enter the building. As for the visitors, their speech will be converted into a text sent to the employee whose name is mentioned. The Google platform was used to convert speech into a speech-to-text API. The project was implemented using a Raspberry Pi, a camera, an LCD screen, a microphone, and a speaker.

Yulian Findawati et al (2020) [17]. The system is based on the use of the Node MCU Lua V3 microcontroller. A set of sensors (fire, motion, temperature, and humidity), in addition to the relay module that works like a key to turn on and off electrical appliances inside the house, is controlled by the Telegram chat app. Where the Node MCU is connected to the Telegram chat application server, there are advantages to using the Bot Telegram chat application, such as the ability to access it from any operating system. IOS, Android, Windows, or Linux.

Ridho Rahman Hariadi et al(2019) [18]. It has become necessary to reduce electricity consumption for air conditioners. Using IoT technology, this project was implemented to monitor the electrical energy consumption of the air conditioner and control it remotely and make it work automatically according to room temperature using temperature and humidity sensors. A device called Termo has been developed to monitor the use of electrical energy. The data will be transmitted to the server. All data will be saved to the database every 30 hours. There are two types of Termo devices installed in this first project that control the switching off of the air conditioner. Moreover, the other device was linked with the infrared LED to replace the remote control for the air conditioner. The proposed system reduced energy consumption by 81.8%.

Mohammad Miraj Shekh et al (2018) [19]. They designed a low-cost home or factory automation system to remotely control devices using a mobile or web application. Through a set of relays that have been linked with the Node MCU, which will be connected to the Wi-Fi network to receive commands via Wi-Fi. From the phone, instructions will be sent via Wi-Fi to the Blynk server.

Madhu B R et al. (2019) [20]. Control fan speed based on temperature and humidity readings using IoT and cloud computing. The electronic circuit has been connected using the Node MCU ESP8266, DHT11, LDR, and Relays; the potentiometer was used to control the speed of the D.C. motor depending on the value of temperature and humidity. The cloud is used to store and process data from sensors that come in over Wi-Fi,

Hikmat Yar et al. (2021) [21]. . The system consists of five layers. The first layer is the device layer, which consists of several sensors. The second layer is the broker (Raspberry Pi has been used as a broker) layer to transfer data from sensors to the service layer through the MQTT protocol. Layer 3 (service layer) receives data from the broker. This layer is designed using Node-red dashboard software. The fourth layer is the application layer. This layer is considered the front end for managing IoT devices.

Table 1.1 shows the comparison between previous systems In terms of strengths and weaknesses.

Table 1.1 Comparison of similar work

References	Capabilities	Controller	Strength	Weakness
Kushank[7]	Security	Arduino MEGA ADK	GSM SMS alert	Automatically only, low security
Musaddak et al [8],	Security, Environment	ESP8266	GSM SMS alert Sensor's value only	High Data uploaded, low security. Automatically only
Shaik Anwar [9]	Security	Raspberry Pi	Sound alert from mobile for security	delay in notifications Gmail, annoying system
P.Amith, et al. [10],	Security	Raspberry Pi	Alert on phone	multi-condition for achieving security
Shraddha [11]	Security, Environment	Raspberry Pi	Security and environment, SMS	AES Algorithm low security
T.Juhana, [13]	Securiy	Arduino Uno and Laptop	Artificial intelligent	Security only, Dropbox to notify
M.Medhat et al. [12]	Security, Environment	Arduino Uno, Raspberry Pi3	Low latency	costly
S. Fattah [14]	Security, Environment policy	Arduino Mega	powers assigned	Low security
M.Dhobale [15]	Security	Raspberry Pi	Face Detection and Recognition	Low accuracy
N.Tkauc et al	Security	Raspberry Pi	detection and recognition, Speech to text platform	Costly
Yulian et al[17]	Environment	Two E NodeMCU Lua V3	Telegam control	Environment only
Ridho et al [18]	Environment power consumption	ESP8266	power consumption	no security
Mohammad et al[19]	Home appliances	nodemcu esp8266	Low cost	Control appliances
Madhu [20]	Environment	Node MCU ESP8266	Low cost	Control fan only
Hikmet Yar et al. [21]	Security, Environment	Raspberry Pi	Low latency	High Data uploaded, No artificial intelligent

1.3 Aims of the project

In this project, a smart home automation system that focuses on boosting security and the environment has been planned and constructed as a functioning prototype with the following goals:

1- To design a smart home that is easy to use, improves home control management, and keeps an eye on all the entrances that are often used by burglars and thieves.

2- To ensure authorized people enter the home and send alerts if reliability is not achieved.

3- To detect any leakage of gases, smoke, and fires with a prior warning sent via Telegram app when any danger is detected and achieves a suitable climate for the home and reduces energy consumption

1.4 Outline Thesis

The thesis is organized as follows:

- Chapter 2, "Smart Home Automation System theory" covers some fundamental ideas on the usage of home sensors in the implemented system, as well as IoT topologies, Cloud and Fog computing, Wi-Fi technologies, protocols, and applications.
- Chapter 3, "Design and Implementation of Smart Homes Automation System," introduces the proposed system's hardware, software, and operation.
- Chapter 4, "Results and Discussion," demonstrates the results of the suggested system and their discussion
- Chapter 5, "Conclusions and Future Works," familiarizes conclusions and future works.

Chapter Two

Smart Home Automation Theory

Chapter Two

Smart Home Automation Theory

2.1 Introduction

Home automation or smart home is used interchangeably to describe one concept: to refer to a distinctive home emulating the latest technology. The latest innovations achieved by researchers are to create an environment suitable for a decent life that meets all the requirements of comfort and safety and to reduce electrical energy consumption at the lowest cost. and anyone can use an intelligent home system to adjust their sprinklers, adjust and monitor their home security system and cameras, or control devices such as air conditioning or heating [22].

Smart home devices are connected and can be accessed through one central point, such as a smartphone, tablet, or laptop. Through one home automation system, it can control door locks, windows, temperature, light intensity, and even appliances such as heating and cooling. the user can keep time schedules for detailed changes to take effect. Smart home devices are linked with machine learning skills to make it easier for the homeowner to make adjustments without human intervention. Some home automation systems alert the homeowner in case of a fire or gas leakage and detect any abnormal movement in the home. In turn, the authorities, the police, or the fire department, can be contacted in the event of danger. Services such as smart doorbells, smart security systems, and smart devices have become part of the Internet of Things (IoT), a network of physical and virtual objects that exchange electronic information between the home and its owner [23].

2.2 Computing Models

Cloud computing is a computing model, and to clearly understand cloud computing, it is necessary to look at the different types of computing [24].

1- High-Performance Computing (HPC): It is a general concept; other types of computing may have the same characteristics as this type. It is a collection of processors, machines, or central processing units (CPU) CPUs. There is software that controls them. These processors may be homogeneous or heterogeneous. It was formerly called a "supercomputer." The most important uses are in scientific experiments that require high data processing, such as nuclear and chemical.

2- Parallel Computing: Parallel computing can be considered HPC, but the difference here is that a set of processors work collaboratively, meaning that each processor will process a specific problem while the other processor will work on another problem simultaneously, and so on. To increase processing speed, all processors will be homogeneous; on a PC, the applications are executed as a series.

3- Distributed Computing: A set of computers, or the so-called processor machines, are connected through a network so that this group can solve complex operations. It can be homogeneous or heterogeneous. Its advantages include scalability and redundancy.

4- Cluster Computing It is smaller than distributed computing, which is a set of computers linked by LAN cables. Each computer has a message-passing interface (MPI) to communicate with them. It all works at the same time.

5- Grid Computing: Grid computing is the use of a set of clusters of computers in different geographical areas. When connected through a wide area network (WAN) and controlled by software like middleware, costs go down, processing power goes up, and it can work with other heterogeneous clusters.

6- Biocomputing: uses the biological mimicry concepts of molecules to perform computational processes to solve complex problems, instead of relying on chips and silicon. It becomes possible to manufacture by depending on other materials that mimic the molecules found in nature such as DNA

7- Mobile Computing: With the advent of cellular phones, processing elements are small. Cellular phone communication for voice applications proliferates worldwide. This technology is characterized by sending and receiving data through worldwide mobile phone networks such as voice calls, messaging, pictures, and video or group video calls.

8- Quantum Computing: manufacturing small integrated circuits (ICs) to obtain processing power. Quantum computers are more efficient and perform faster than the most powerful supercomputers.

9- Optic Computing: If we convert the computing system based on the electric circuit to the optical computing system, that is, the use of optical fibers in manufacturing computers, using photons in visible or infrared light to perform operations computationally Light is about ten times faster than an electric signal. It will be very expensive.

10- Nanocomputing: Parts of computers will be manufactured using nanotechnology. Transistors based on carbon nanotubes replace the silicon transistors in traditional computers. It is possible to put vast numbers of devices in a small area for computing operations and obtain enormous computing power.

11- Network Computing: Systems are designed using the latest technologies to support users with the best services possible, using a comprehensive and distributed network of computing resources to provide a valuable set of necessary services at a low cost appropriate to the user's needs.[24]**.**

12- Cloud Computing: The simplest form of cloud computing is accessing stored data and programs when the internet is available from any location instead of the local computer's internal storage. There is a fixed and formal definition of cloud computing defined by the National Institute, which sets definitions,

descriptions, and standards for each new technology (NIST). Cloud computing is a way to access a set of computing services, such as storage units, applications, communication networks, servers, and other features, on demand from anywhere on the network. These services can be set up and taken down whenever we want. be obtained. These services are provided by the service provider very quickly [24].

2.3 Need for Cloud Computing

There are several reasons for the need for cloud computing and its applications in our daily lives to achieve convenience and reliability:

1- Previously, if we needed a file, we would save it on a thumb drive, USB, HDD, SSD, CDRW, etc. Today we keep a file in the cloud by using a cloud application such as Dropbox, and we will be able to access it from any device on the internet.
2- It is possible to cooperate over the network to make it easier to exchange files with anyone.
3- The probability of losing the data is much lower. due to having many copies of our data.
4- Reduce the effort of administration, maintenance, and updating the system used by the customer[25].

2.3.1 Essential Characteristics of Cloud Computing

1- Service request as needed: no need to contact an expert to create a cloud subscription. There are accessible user interfaces to book any service as needed, and it is possible to cancel any unwanted service in the future.
2- It provides comprehensive network access, meaning a network to connect the different devices. Usually, the cloud is not homogeneous because there are different devices and software.

3- Flexible resource collection: Cloud computing providers can rent the resources to many consumers, depending on a multitenant concept
4- Flexibility in the rapid provision of resources and services for the customer, sometimes automatically, as well as the process of canceling it.
5- Measured service: There are reports sent to both the service provider and the consumer about the quantity of resource consumption and the type of services at the time and date [26].

2.3.2 Cloud Computing Deployment Models

1- Private Cloud: Cloud infrastructure provides for the specific use of a company or organization with a limited number of users (the cloud is usually managed, operated, and acquired by the owners of the organization or third party.
2- Public Cloud: It is more common than the other types. The infrastructure of this cloud is available to the general public. It may be managed and operated by an establishment, company, government-supported, or combination.
3- Community cloud: many organizations or institutions share a single cloud infrastructure that performs specific tasks in one common field between them, such as (tasks, protection requirements, guidelines, and observation). Organizations or a third party manage.
4- Hybrid Cloud: When a company or organization has a hybrid cloud infrastructure for two or all previous cloud infrastructures (private, community, or public) [26].

2.3.3 Cloud Computing Service Models

1- SAAS: Software as a service. The highest levels of cloud services are provided. The end customer only needs simple access to the web via the

internet and the use of ready-made applications. The customer does not care about upgrading, data protection, or ensuring service continuity.

2- PAAS: platform as a service, programmers, and developers often use this cloud-provided service to take advantage of this platform to develop their software and applications. There are specialized companies that provide this type of service. To accommodate the customer's working environment, the consumer must consult the software license agreement (SLA)

3- IAAS: infrastructure as a service, the client rents a complete virtual device and starts installing his platform (OS), applications, and programs. Start-up companies often benefit from this type of device[26].

2.4 Fog Computing

Fog computing is sometimes called edge computing. A local server is any device with computing, storage, and network connectivity that can be a fog node. It will be an intermediate between end devices or sensor groups and cloud computing, used to transfer the data after processing to cloud computing [27]. The idea of fog computing is to extend the cloud nearer to the IoT device and use decentralized servers between the network core and a network edge for data processing and immediate requirements of the end systems. The Fog Computing market was valued at 22.3 million dollars in 2018; it is anticipated to increase to 205 million dollars in approximately 2023. Given the excellent performance of intelligent devices, it will have considerable significance for the Internet of Things vision [28]. Many reasons make using fog computing valuable. The most important ones will be mentioned:

1- Processing and storing of data between the cloud and an end device. It is a way of providing requirements more instantly and near ground devices.

2- There is no need to send every piece of information to the cloud channels, which reduces the amount of bandwidth required.

3- The ability of the current cloud model to handle some of the requirements is insufficient, such as volume, latency, and bandwidth.
4- There are an unlimited number of sensors and devices that can be connected to the fog with the possibility of adding other devices in the future.
5- Users can select the data they want to upload to the cloud according to the sensitivity, size, and importance of this data from a security point of view. Some data may be confidential, which we do not want to share online [29].

2.5 Wireless networks

Wireless networks transfer data and information between two or more devices by radio waves. The necessary reason this technology is so widely used is the ability to connect to remote devices for a few feet or several kilometers without thinking about cables and connections and the difficulty of installing them. Each wireless technology has its frequency, transmission speed, and range. The waves are transferred from one place to another with the possibility and presence of interference between them. Therefore, it was necessary to set standards to specify the spectral range and transmission permittivity for each technique in all countries. It is a set of various rules for wireless local zone networks by the Institute of Electrical and Electronics Engineers (IEEE). As it is known, it is difficult to confine electromagnetic waves to a specific geographical area, which facilitates penetration and infiltration of wireless networks if the data is not encrypted. So, the information must be secure and encrypted before being sent. Wireless networks are categorized into four specific groups. Figure (2.1) describes the classifications for these networks [30].

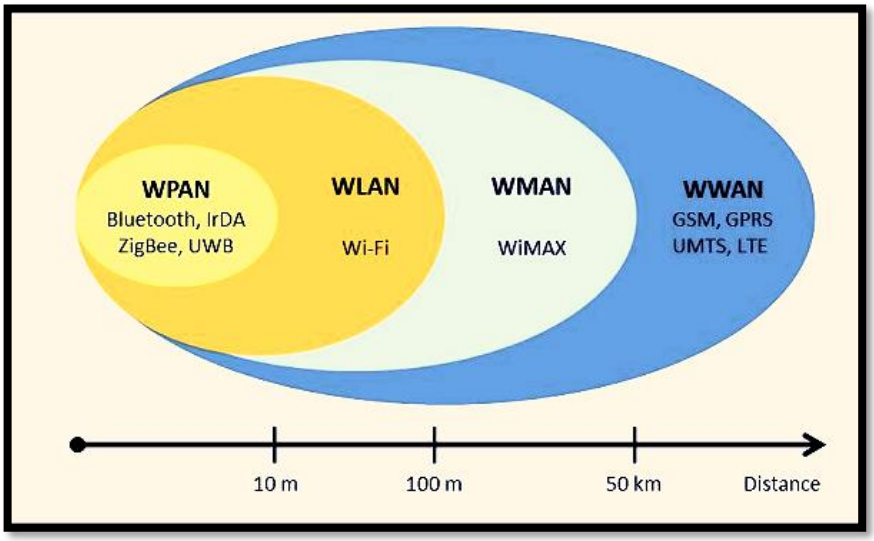

Figure 2.1 Wireless network classification

2.6 WI-FI

Wi-Fi is a set of wireless networking technologies founded on the 802.11 standards. The Wi-Fi Alliance is a brand of non-profit worldwide network established in 1999, which consists of a group of companies evolving and implementing Wi-Fi to ensure compatibility for Wi-Fi devices. The Wi-Fi Alliance vigorously participates in developing the IEEE 802.11 standard by submitting suggestions for technical features, beginning with presenting the basic version of IEEE 802.11, with a maximum range of 2 Mbit/s since 1997, and improving the bandwidth reliability and accessibility with each new development step. Every five years, a new IEEE 802.11 standard generation is introduced, while three recent versions have often been called the fourth, fifth, and sixth Wi-Fi standards [31]. The evolution of the Wi-Fi standard is represented in Figure 2.2[32].

STANDARD		DATE	FREQUENCY (GHZ)	MAXIMUM DATA RATE
WiFi 1	802.11b	1999	2.4	11 Mbps
WiFi 2	802.11a	1999	5.0	54 Mbps
WiFi 3	802.11g	2003	2.4	54 Mbps
WiFi 4	802.11n	2009	2.4 / 5.0	600 Mbps
WiFi 5	802.11ac (Wave 1) 802.11ac (Wave 2)	2013 2015	5.0 5.0	1.73 Gbps 3.46 Gbps
WiFi 6	802.11ax	2020	2.4 / 5.0/ 6.0	9.60 Gbps

Figure 2.2 **The evolution of Wi-Fi standard**

2.7 Internet of things

Generally mentioned worldwide, the Internet of Things (IoT) consists of two main words: Internet and things. The broad expression of the IoT is constructing things capable of connecting to the internet and generating useful information. More than that, it makes the interaction between the virtual and physical worlds very easy. The Internet of Things has become the most vital topic that has occupied people and has loomed large on the horizon due to its excellent ability to connect millions of objects with intelligent sensing capabilities and embedded machines connected via Internet Protocol (IP), innovative entities, and or just (things) or everything for ordinary life, supplemented by microcontrollers, wire, or wireless transceivers, followed by sensors, actuators, and protocol accumulations proper for contact in different environments where intended devices have specified resources, permitting them to collect data and represent it in the physical world [33].

2.7.1 Internet of Things Architectures

Managing millions of non-homogeneous interconnected devices via the networks demands a flexible, multi-layer architecture. There is more than one IoT architectural model. Nevertheless, no standard reference architecture has

been embraced. To methodically discuss the IoT technologies to obtain an overview of public IoT, there is an architecture of IoT technologies that describes the thorough, public, and uncomplicated architecture; the IoT Model consists of the five-layer shown in Figure 2.3. This model is compatible with many of the meanings of further models and simplifies and sums it up. Consequently, architecture has been used broadly in contemporary studies; each layer contains examples of technologies classified depending on the functionalities provided. The layers can be compared with the Transmission Control Protocol TCP/IP layers. However, considerable IoT technologies can conform to the TCP/IP or Open Systems Interconnection (OSI), and classifying all IoT technologies based on the TCP/IP model does not enclose whole layers. Thus, their classification based on the five-layer model is highly suitable [34].

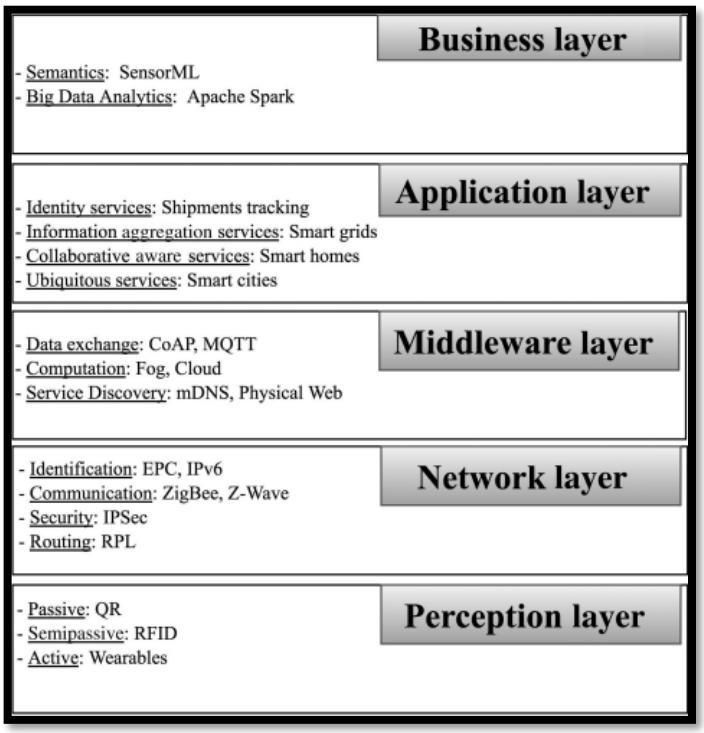

Figure 2.3 Five-layer IoT architecture model

2.7.2 IoT Architecture Based on Fog Computing

Despite the numerous benefits of cloud computing in IoT, there has been some concern about unloading entire data sets and analyzing and processing

them in the cloud [35], [36]. In many cases, the service user is near the data producer, such as sensors, which are transmitted to the cloud. One of the most important problems is the unnecessary uploading of data on the internet and the time wasted in transferring this data to the cloud. Excessive traffic may make the network expensive where no broadband connection is available. Fog computing is a paradigm coined by Cisco for a concept similar to cloud computing that presents a highly virtualized resource pool near users and provides computing, storage, and processing services to consumers. While the cloud naturally exists at the boundary of the network, Consequently, the fog will have an adequate distribution and a more comprehensive range with considerable hardware heterogeneity. The fog vision can represent a cloud near the user's environment. The overall architecture for the IoT, including cloud and fog, is illustrated in Figure 2.4 [34].

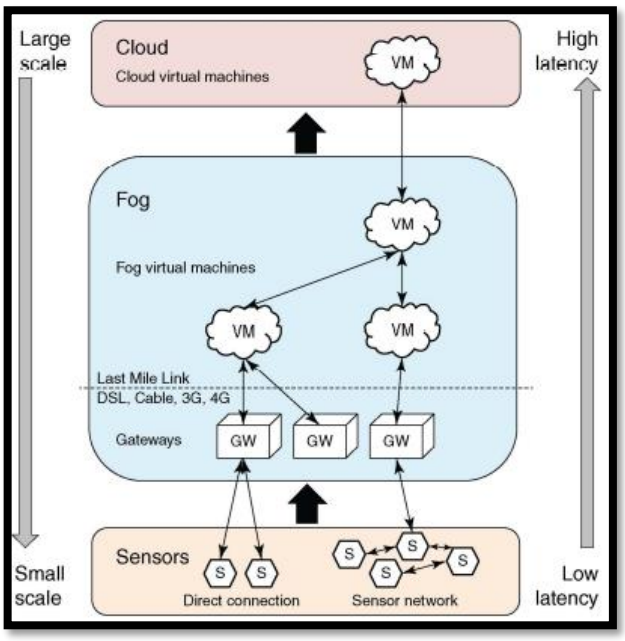

Figure 2.4 Architecture combining fog and cloud-based IoT

2.8 Sensors

It is a device whose principle is to convert a physical quantity into an electrical signal, which may be either an electric current or voltage, a change in the value of resistance, or capacitive, or inductive impedance [37]. In other words, it is a device that reacts to a material stimulus (such as temperature, rays, sound, pressure, gas magnetism, displacement, speed, or acceleration) and supplies an output for either measurement of that physical amount or operating control [38]. Home automation has many sensors that help build an intelligent home capable of providing comfort and safety, improving energy sources, and reducing them. Figure 2.5 represented Common sensor categories in IoT applications.

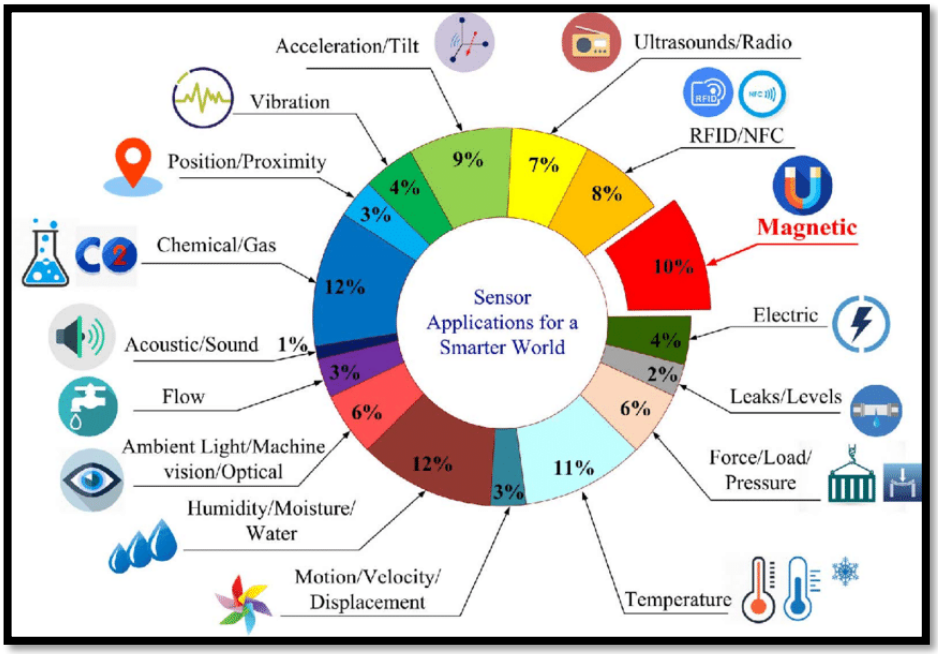

figure 2.5 Common sensor categories in IoT applications

2.8.1 Smart Home Environment System Sensors

What makes a house smart are the interactive technologies that are included inside it, not the fact that it is environmentally friendly, uses solar electricity, and recycles its wastewater. The term "intelligent" is used to describe

a smart home since its computer systems can monitor several areas of everyday living[39]. Some types of sensors used in smart home automation:

2.8.1.1 Temperature and Humidity Sensors

Monitoring the values of the temperature and humidity inside the home is needed to ensure comfortable weather living. There are several types of sensors for measuring temperature and humidity. There is a difference between these sensors in terms of their ability to measure high or low temperatures and the percentage of measurement error, as well as in terms of cost and response time. which must be balanced with something that suits the user's needs. The DHT11 sensor will be chosen as a model to describe the idea of this type of sensor. This sensor model can measure temperature and humidity and produce a built-in digital value for sensing humidity and temperature. It has a very accurate value of humidity and temperature, high reliability, and is long-term. It is easy to use with any microcontroller like Arduino, Raspberry Pi, etc. It consists of resistive-type humidity measurement and a Negative Temperature Coefficient (NTC) temperature measurement and has an 8-bit microcontroller; Therefore, it has the best quality, elevated response, and low cost. The DHT11 module works in communication consecutively by sending data in a train of pulses at a time-specific duration; the process duration time is 4 ms approximately. Its small size, low power consumption, and sense of up to 20 meters make it the best choice for many applications. The component is a 4-pin single-row pin package [40]**.** The DHT11 temperature range is from 0°C to 50°C with (+-2) degrees of accuracy, and the humidity range is from (20 to 80%) with (5%) accuracy. DHT11 is depicted in Figure (2.5)[41].

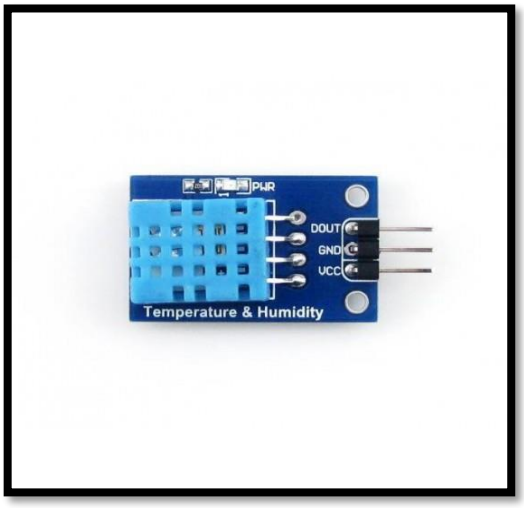

Figure 2.6 Temperature and Humidity Sensor DHT11

2.8.1.2 Gas Sensor

The MQ2 is the most widely used gas sensor in the MQ series. It is a Metal Oxide Semiconductor (MOS) type Gas Sensor. It detects the new reading of the resistance of the sensor material when gases approach the material. A simple voltage divider can detect quantities of different gases. The MQ2 Gas sensor needs 5V DC and consumes roughly 800 milliwatts. It can detect gases such as liquefied petroleum gas (LPG), smoke, alcohol, propane, hydrogen, methane, and carbon monoxide (CO) with various condensations from 200 to 10,000 ppm. The sensor is usually covered with a double layer of anti-explosion stainless steel [42]. The output voltage provided by the sensor is directly proportional to the smoke or gas concentration [43]. As shown in figure 2.6.

Figure 2.7 MQ2 Gas Sensor

2.8.2 Smart Home Security System Sensors

In the short term, more than 25 billion IoT devices are expected to be used by businesses and consumers by 2021. Depending on the latest technology available to improve home security and comfort and reduce energy consumption [44]. Figure (2.7) [45]. It represents innovative home architecture consisting of three-node sensors: node, internet, and users.

Figure 2.8 Smart home architecture

One of the most important that resonated on the horizon is the home security system, which has developed rapidly in recent years[46]. [3]. Security systems have become significantly advanced by integrating them with innovative home technologies, including real-time sending and receiving of data via the internet [47]. Some types of sensors used in smart home security systems:

2.8.2.1 Radio Frequency Identification (RFID)

RFID is a widely used technology for preserving and retrieving data based on radio frequency. RFID techniques usually include RF tags, an RF reader, and a database. RFID is used to automatically determine the identity of somebody or thing from several millimeters to hundreds of meters. It is used in several areas, including marketing and security, and is widely used in systems for opening and closing doors and giving authorized access to specific users. The RFID tags have unique identifiers (UIDs) that pass identification by the reader based on the database [48]. A combination of RFID technology and computing technology is called an RFID system. An RFID system consists of the following components:

1- RFID Reader

The reader, or an interrogator or scanner, exchanges RF data to and from the tag through antennas. A reader may have multiple antennas that send and receive radio waves. A reader informs the data processing system about the existence of a tagged object. It consists of three main parts: control, high-frequency interface, and antenna. Reading across a range of readers is affected by several factors. Antenna gain, the frequency range, and the direction of the antenna. Readers have four types: Read, read/write, fixed, and mobile.[49]. Figure (2.8) shows the internal electronic circuit of the RFID.

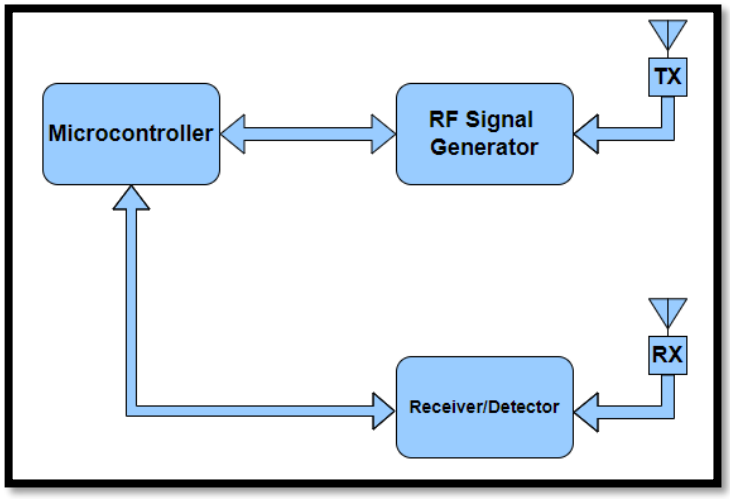

Figure 2.9 RFID Reader electronic circuit

2- Transponder (Tags)

RFID Tags or Transponders It contains a microchip and an antenna (the chip and the antenna are called TAG). The antenna allows the chip to transmit the information to a reader after being powered by an RFID reader via radio waves. The reader converts the radio waves mirrored from the RFID tag into digital data. Figure (2.9) shows the internal electronic circuit of the RFID tag.

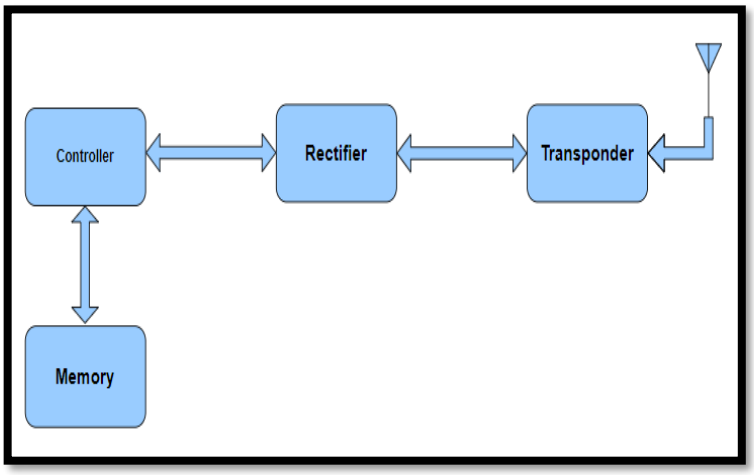

Figure 2.10 RFID tag electronic Circuit

There are many types of tags: active tags, passive tags, and semi-passive tags; The passive tag's antenna will receive a signal when the reader sends electromagnetic waves. The tag reflects the RF signal sent after adding the information to the chip by modifying the reflected signal. Passive RFID tags are

most commonly used for safety access, stock monitoring, and good tracking. The active tag has a battery built-in. Generally, it ensures a more extended read range than passive tags and is more costly compared to passive tags. The batteries need to be replaced. Active tags are used for road tolls and asset tracking in larger areas. but Semi-Passive Tags use a battery to keep memory inside the tag and operate it in the same way as passive tags [50].

RFID technology is a sufficiently-prominent wireless application for tracing and access management. RFID has become a unique product. It is used in wide fields such as ticketing, passports, key systems, fees, etc. RFID benefits a as low-cost tag system. The frequency range of RFID is represented in Table 2.1[51][52].

Table 2.1 The frequency range of RFID

Type	Range	Frequency	Reading Range	Application
LF	30-300 K Hz	125 kHz	less than 10 cm	Access control, tracking
HF	3-30 MHz	13.56 MHz	10 cm-1.0 m	Ticketing, Payment, Data transfer
UHF	860-960 MHz	900, 915MHz	1.0-12.0 m	Rain RFID
µW	2.4– 6.8 GHz	2.45, 3.0 GHz	Up to 100 m	Industrial, Scientific, Medical

There are many types and models of RFID technology. The most important one in the field of security for homes and other buildings is RC522 RFID 13.56MHz radio frequency reader module is designed to communicate with RFID tags according to ISO 14443A standard tags). The reader can connect to a microcontroller over a 4-pin with a maximum data rate of 10 Mbps. It also establishes communication over I2C and UART protocols. The method of communication between the transmitter and the receiver is based on the radio wave [53]. As shown in Figure (2.10).

Figure 2.11 RFID-RC5

2.8.2.2 Ultra-Sonic Sensor

The ultrasonic sensor (HC-SR04) measures the distance between an object and a sensor using a radio or sound wave. It is also called a transceiver. It works like radar or sonar. The object's distance can be determined by calculating the wave's actual time returned or reflected from this object, suitable for use indoors and outdoors. The applications and their forms can be seen in Figure (2.11).

Figure 2.12 Ultra-Sonic HC-SR04

The ultrasonic sensor detects distances ranging from 2 cm to 500 cm with a 0.3 cm resolution. The voltage supply required by the sensor is 5V and littler than the 2mA standby current. The ultrasonic sensor consists of ultrasonic transmitters, a receiver, and a control circuit. This sensor measures distance by sending an ultrasonic signal, receiving its echo, and then measuring the time

between the two events, generating a waveform where the high time peak is proportional to the distance. The transmitter of the ultrasonic sensor emits an ultrasonic wave in one direction by launching the waves, and it starts timing. If it meets a hitch on the way, the ultrasonic spreads in the air and returns immediately [54]. The formula for distance measurement is expressed as seen in the following equation (2.1):

$D = v * t$ ... ... (2.1)

Where D: is the measurement of distance

V: the velocity of ultrasonic spread in the air is 340 m/s.

t: time delay between wave emission and echo reception (s)

$D = 340\ t\ /\ 2$ ... ... (2.2) [55].

2.9 Face detection and recognition

Face detection and recognition are essential in today's biometric authentication techniques. Facial recognition involves using the characteristics of a face in biometric systems. Face recognition has two main steps: confirmation and identification. Face identification denotes a 1: N problem that compares a query face image with all the image templates in a face database.

The general term "face recognition" can be described in multiple scenarios. The first is recognition or identification, and the second is authentication or confirmation. People will initially be registered in the database. Then, images are used as tests to match them with the photos in the gallery. In the recognition process, the match is 1: N. This means that one image is investigated against all previously-stored images to find the best approximation with a value above a certain threshold. As for the authentication process, the match will be 1:1. When entering the gallery, the image is matched to the identity, and the required identity is taken for authentication if the matching quality exceeds the threshold value.

The recognition procedure is technically more complex than the authentication scenario. One reason is that the probability of error is relatively high. Another reason is that you have to scan and scrutinize the entire gallery in every recognition process. Generally, two procedures associated with image processing are face detection and face recognition, as shown in Figure 2.12. Face detection is an essential initial step to selecting the boundary and extracting the face part from the backdrop. The solution to the problem involves the division and extraction of faces and perhaps facial features from an uncontrolled environment. A face recognition operation involves achieving verification and identification; this stage takes the investigation image extracted from the background during the face detection step and compares it with an earlier registered face database. Exploring for the closest matching images is then executed to specify the most likely matched face. The final step of face recognition is identification and verification. Identification compares a face with more than one face to determine the most likely probability. Face verification compares the test face with another known face in the database, resulting in either being accepted as a known person or rejecting the face as a deception. [56].

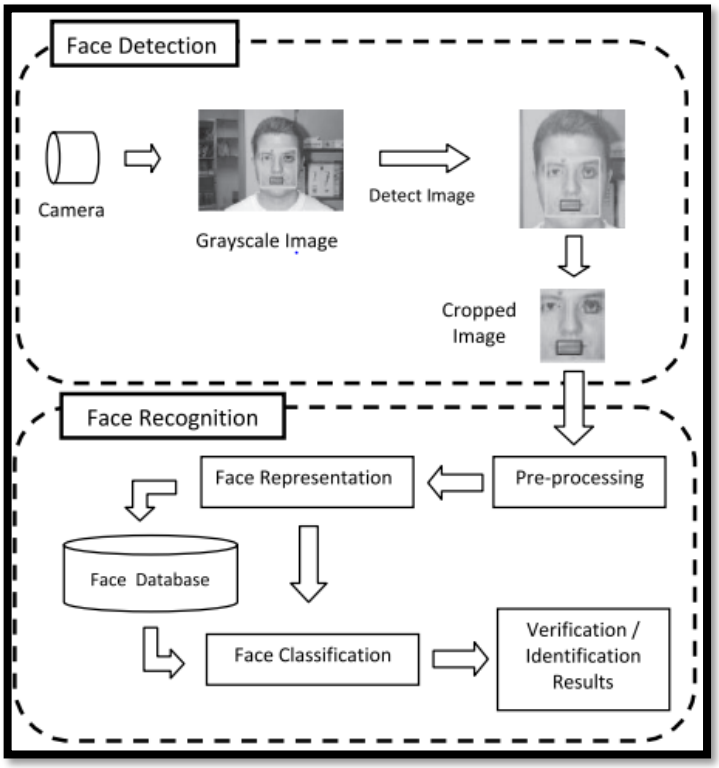

Figure 2.13 Face detection and face recognition

2.10 Microcontroller

Programming embedded computers is a difficult task that should only be undertaken by experienced individuals. Then, many institutions tried to make this challenge effortless and available to all. The Arduino is one of the latest innovations to make technology less complicated and more creative. Arduino is a microcontroller platform that is based on simple software and hardware and has an open source. Arduino Boards can read analog or digital inputs from sensors or any data source and perform some actions after turning the data to the output, like switching on an LED, starting an actuator, or broadcasting something online. By uploading a group of commands to the microcontroller, you can tell your board what to do. A programing language like C/C++ writes the instructions of the Arduino language and uploads them by using an "Integrated development environment (IDE)"[57].

2.10.1 Arduino Uno

The Arduino Uno is a favorite and most used among other Arduino models; it contains an ATmega328p microcontroller with 14 digital input/output pins (analog pins are also possible to use as digital pins in some cases). Six pins from 14 digital pins can operate as PWM outputs, six as analog inputs, a 16 MHz crystal oscillator, a power port, a reset button, an ICSP header, and a USB connection. This board contains all the components needed to support the microcontroller; it's ready to connect to a computer and program. This board can be powered with an external battery or an AC-to-DC adapter [58] See figure (2.13) [59].

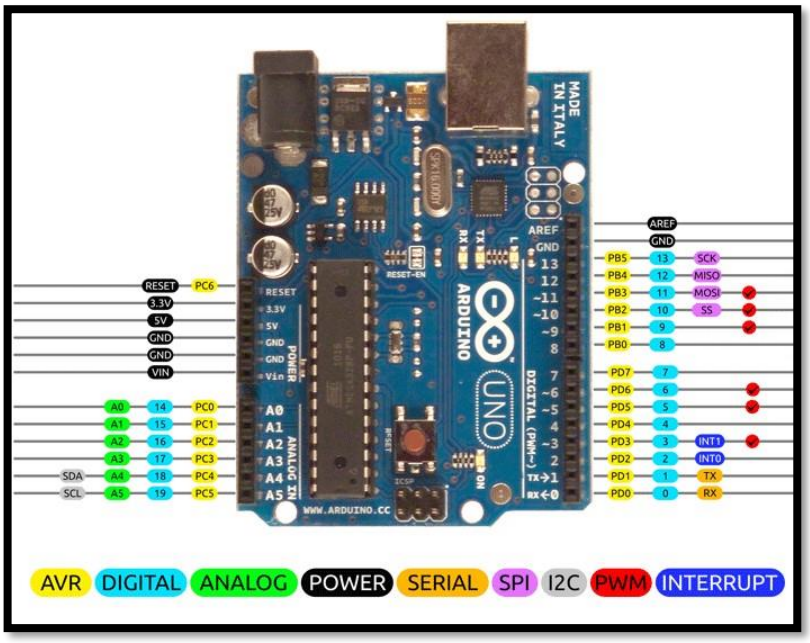

Figure 2.14 Arduino Uno

2.10.2 Uno R3-Atmega328p-Node MCU ESP8266 -USB-TTL CH340G

The Arduino Uno Wi-Fi R3 AtMega328p+NodeMCU ESP8266 capacity 8 Megabyte Memory USB-TTL CH340G is a collection on a single electronic chip that is the same as the Arduino UNO. The modules can work concurrently or individually. Furthermore, each one has pins. It is the correct key for a new

project needing Uno and Wi-Fi. You can modify sketches and firmware for ATmega328 and ESP8266 through USB. For this purpose, there is a USB-serial converter CH340G. It is a recent release of the traditional Arduino UNO R3 model. Modules can function together or separately, making the microcontrollers the facility to connect sensors and actuators with high efficiency. The new microcontroller compatible with Arduino UNO is a suitable solution for designing the latest practical projects that demand Uno and Wi-Fi in their design. For more details, see appendix A.

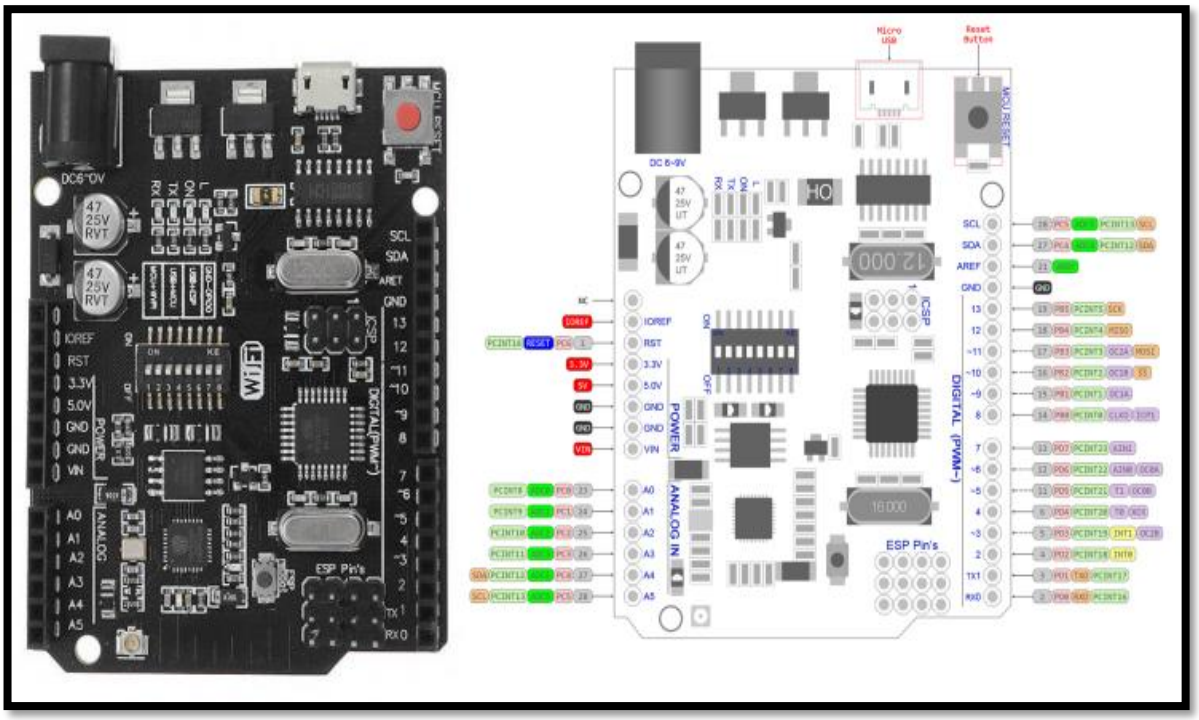

Figure 2.15 Uno R3-Atmega328p-Node MCU ESP8266 -USB-TTL CH340G

Chapter Three

Design and Implementation of Smart Home Automation System

Chapter Three

Design and Implementation of Smart Home Automation System

3.1 Introduction

This chapter discusses the design and implementation of the smart home automation system, which consists of several essential parts that reflect the benefits they provide to homeowners' comfort. The first part is concerned with the security of the home and ways to protect it from intruders and strangers. In contrast, the second part maintains a suitable environment for living by providing appropriate temperatures and humidity to fit the desires of persons in the house and reduces energy consumption, and the third part ensures the safety of everyone from the leakage of gases and smoke with a previous alert. These parts have different methods and programming languages that help this system integrate and work as a single system environment.

3.2 Proposed System Smart Home Automation

The proposed work aims to design and practically implement a smart home automation system based on IoT and cloud computing. Fog computing technology has been added as a new idea because of its many advantages. The home is monitored and controlled through a Web application and text message alerts. The programming languages used in this project are C, C Sharp (C#), JSON, HTML, ASP.NET, React, Cascading Style Sheets (CSS), and MSSQL.

The proposed system can read sensor data such as temperature and humidity and control the operation of heating or cooling devices according to the climate inside the house based on the presence of persons only to reduce power consumption, as well as measure the proportion of gas, fire, and smoke by specific sensors distributed inside the house. The system is also able to monitor

the security aspect of the house by opening the door for those authorized to enter only and detecting intruders, whether from the door or window, and controlling it manually or automatically at anytime from anywhere using the web application. The block diagram for the overall system is shown in Figure (3.1).

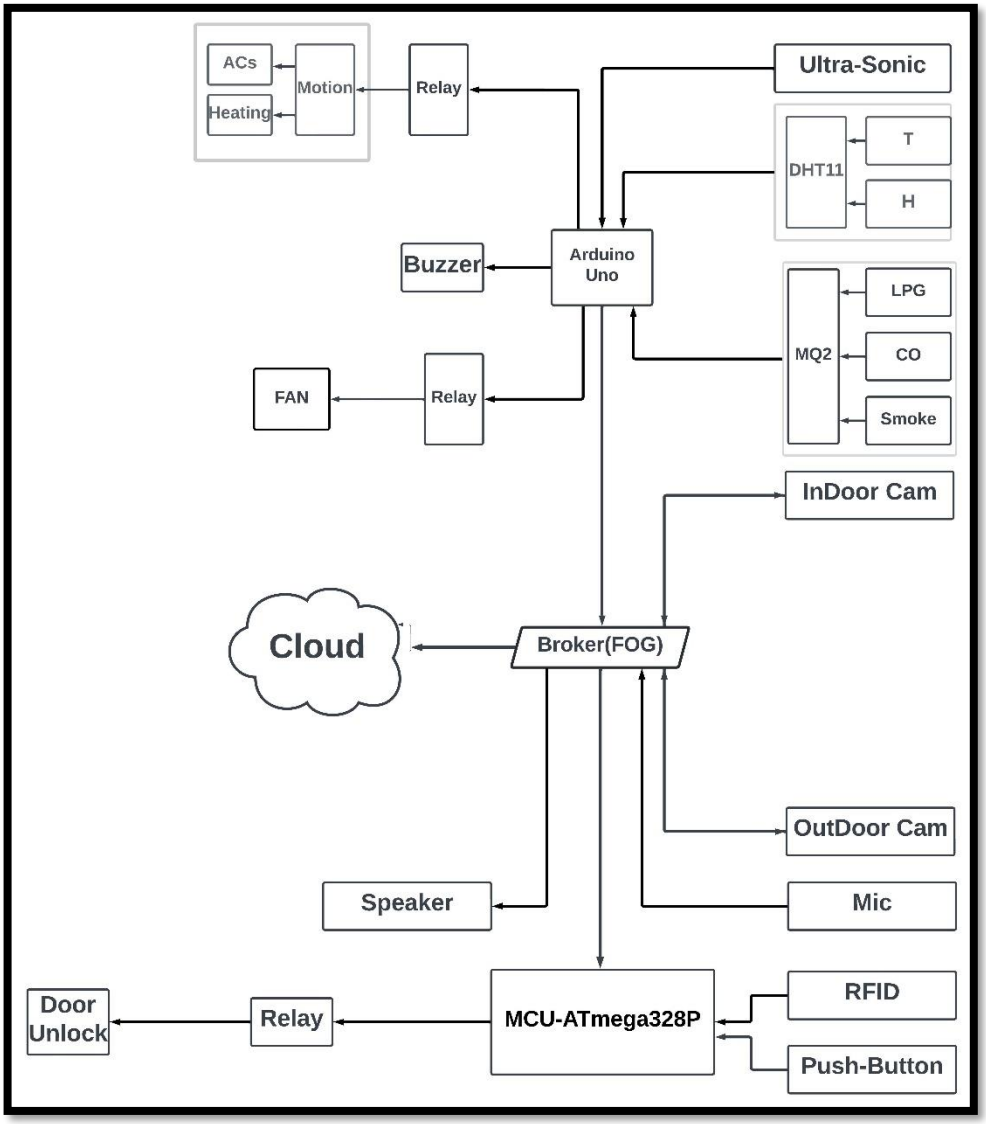

Figure 3.1 Schematic of smart home automation system

The proposed system design can also be applied to a group of homes, where they are directly linked to one cloud and a web application for more than one user. As shown in Figure (3.2).

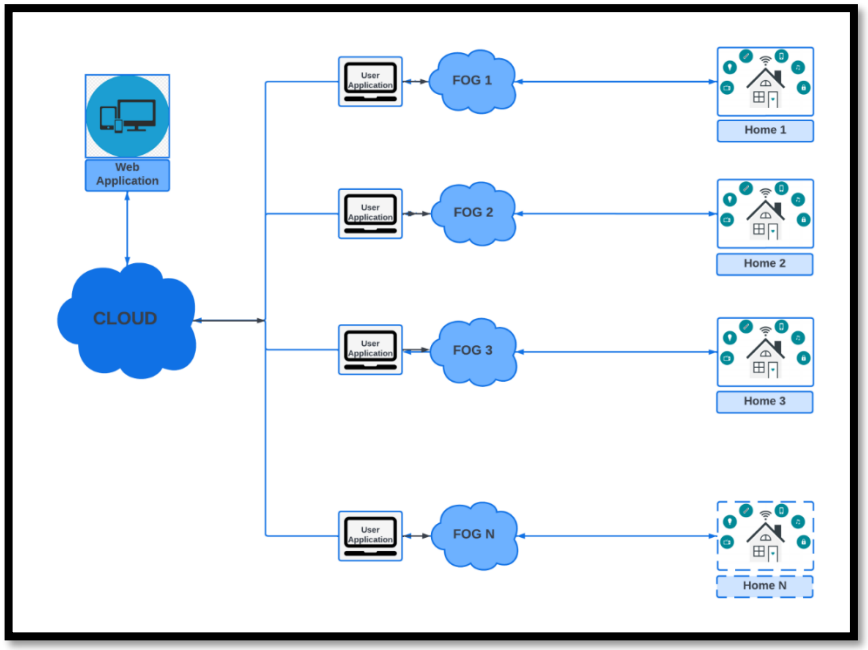

Figure 3.2 Schematic For a group of smart homes

3.3 Overall System Description

Since Wi-Fi is so widely used, there is no need to complicate things by using additional devices, thus Wi-Fi technology has been used to link smart home gadgets. Wi-Fi takes matters into its own hands regarding simplicity. Four parts make up the proposed system: an interior unit, an outdoor unit, a broker unit (fog computing), and a cloud computing unit. A web application is used to monitor and manage the system.

The indoor unit consists of sensors such as (DHT11, MQ2, Ultra-Sonic_, relays, actuators such as (Cooling LED, Heating LED, and Fan) and Arduino UNO to collect the data and then send it to the broker node, and the indoor camera is connected directly to the broker node.

The outdoor units consist of RFID, push-button, relays, door locks, and MCU-ATmega328P to collect the data and send it to the broker node, and an outdoor camera connected directly to the broker node. The broker collects data from all sensors after analyzing, processing, storing it, displaying it on the computer screen, and then sending the information to the cloud for display on the

Graphical User Interface (GUI) via Wi-Fi. The GUI is used to monitor and control the system manually or automatically. The user receives data during the observation period. The system will be described according to the characteristics common to the units. Figure (3.3) shows the smart home system components. Figure (3.4) depicts the completed demo Smart Home system.

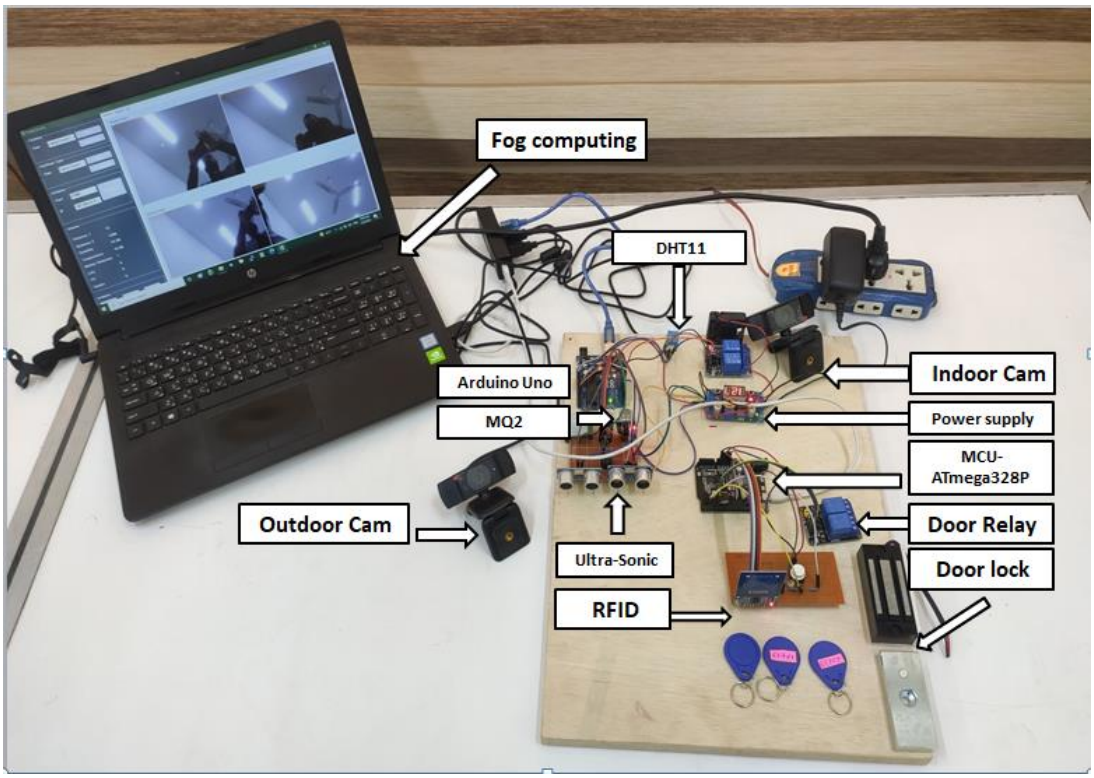

Figure 3.3 Smart Home system components

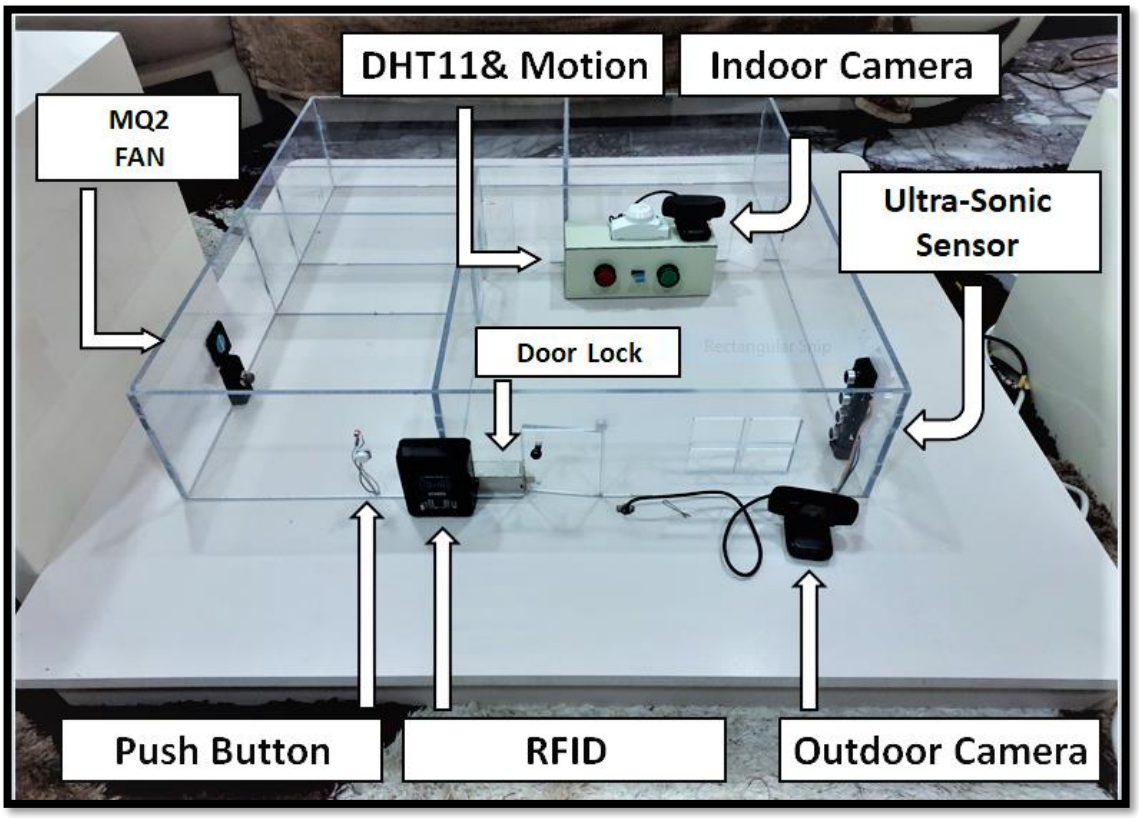

Figure 3.4 Constructed demo of Smart home

3.3.1 Sensors

This unit is an integral part of smart home automation systems such as temperature and humidity sensors, microwave motion sensor, Ultra-Sonic sensor, gas ssensors and RFID. Their purpose is to provide as much detail as possible about home conditions.

1- DHT11 Sensor

DHT11 Is used to measure the temperature and humidity inside the house. This data helps control heating and cooling systems, save energy, and create a suitable living environment inside the home. As shown in Figures (3.5) and (3.6).

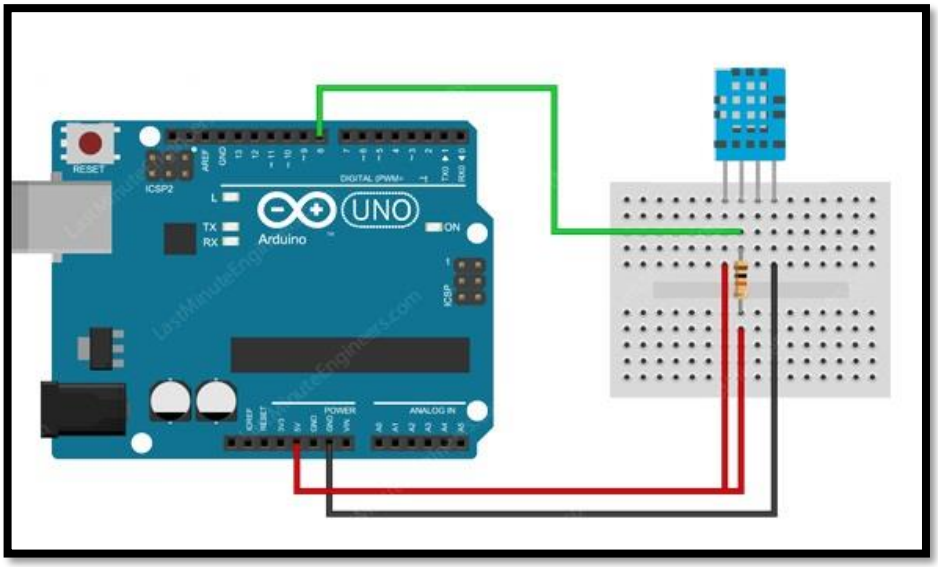

Figure 3.5 DHT11 connection with Arduino Uno

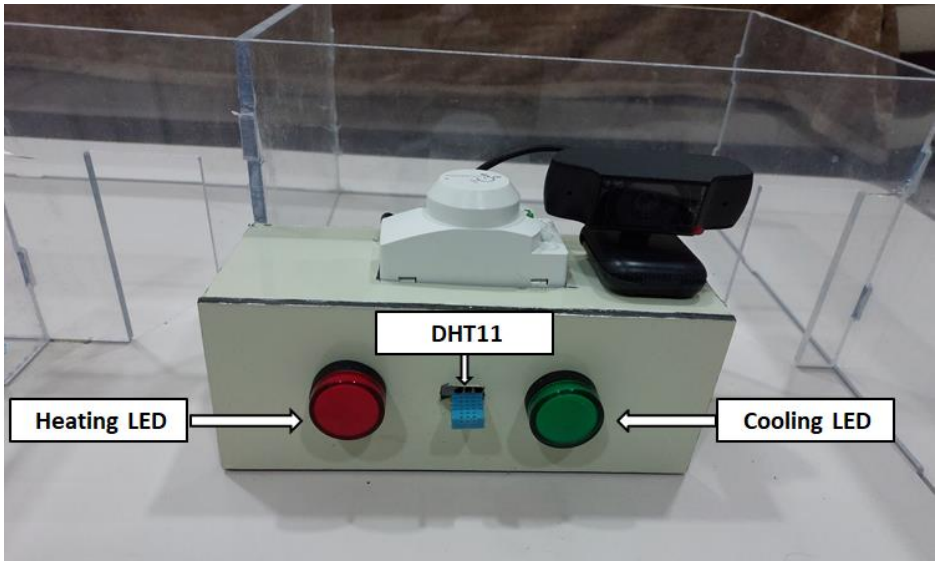

Figure 3.6 Temperature and Humidity Sensor DHT11

2- Microwave Motion Sensor

This type of motion detector can detect an area with a diameter of 360 and a distance of 1-8 meters, ranging from 2 seconds to 12 minutes. It is suitable for the living room and can control heating and cooling devices. The motion detection system works with DHT11 to measure temperatures, and accordingly, the fog decides whether to turn on the air conditioning or not. As shown in Figure 3.7

Figure 3.7 Microwave motion sensor

3- MQ2 Sensor

It is necessary to monitor the gas leakage, the amount of smoke in case of a fire, carbon dioxide, and other toxic gases. The system makes use of a gas sensor (MQ2) that can detect smoke and flammable gases at concentrations ranging from 300 to 10,000 ppm. Figure (3.8) shows how to practically connect with the Arduino UNO microcontroller and Figure (3.9) shows how to connect it to the proposed system.

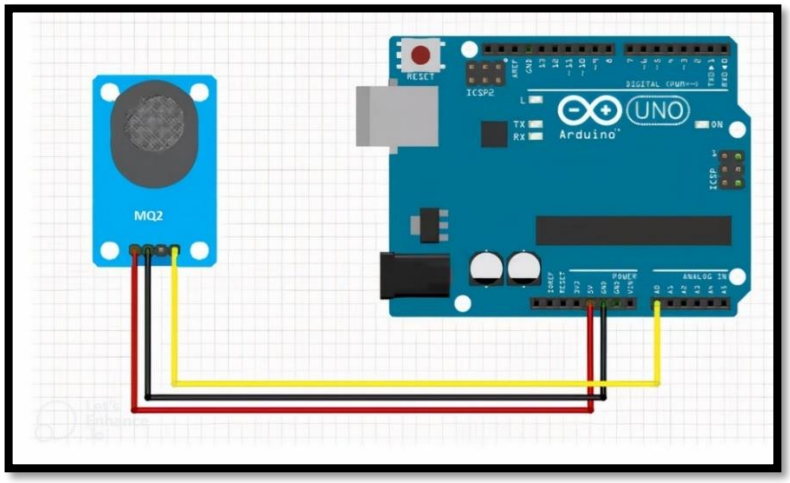

Figure 3.8 MQ2 connection with Arduino UNO

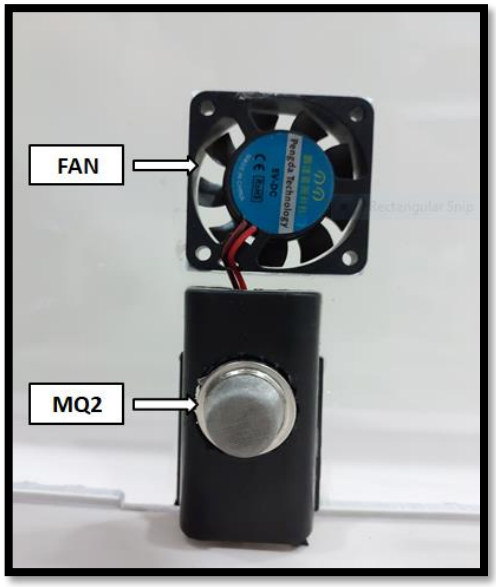

Figure 3.9 Gas sensor MQ2

4- Ultra-Sonic Sensor (HC-SR04)

An ultrasonic sensor (HC-SR04) has been used to measure the real distance between the sensor and objects, to secure the home from thieves and robbers, and keep the doors and windows under continual observation. As a result, it keeps track of any instances when this distance changes as a result of opening a door or window. It is attached to the house's camera. to alert the homeowner in case of a security breach. Figure (3.10) below shows the electronic circuit for the Ultra-Sonic sensors and buzzer alert connected with the Arduino Uno. Figure (3.11) represents the design of the sensor.

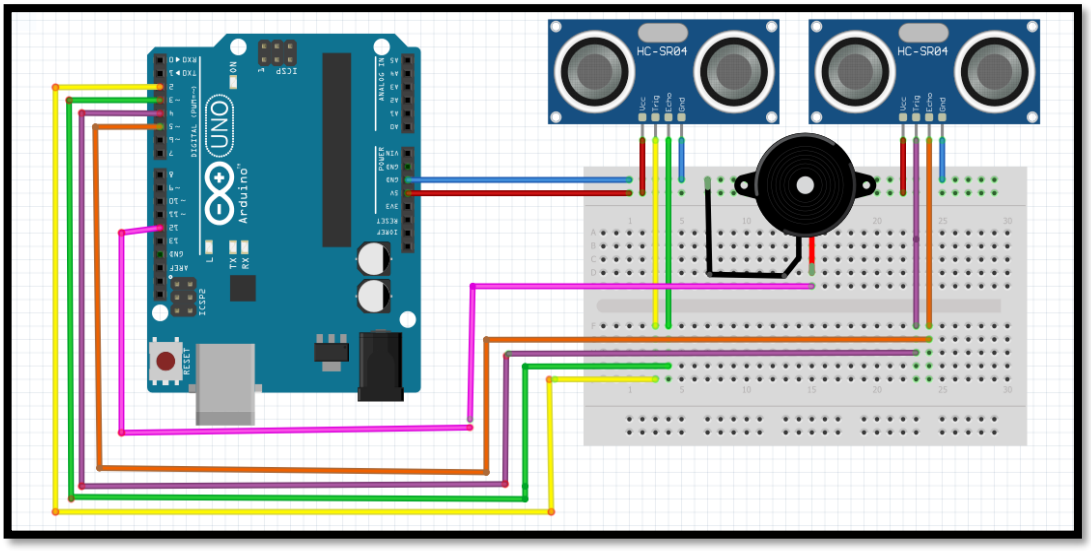

Figure 3.10 Circuit of Ultra-Sonic sensors and buzzer connected with Arduino UNO

Figure 3.11 Ultra-Sonic Sensor

5- RFID-RC522

This technology was used as part of the outdoor unit, which allows tag holders in the system to enter the house. The door will be opened automatically when the card is known, and its data is registered in the system. As shown in Figures (3.12) and (3.13)

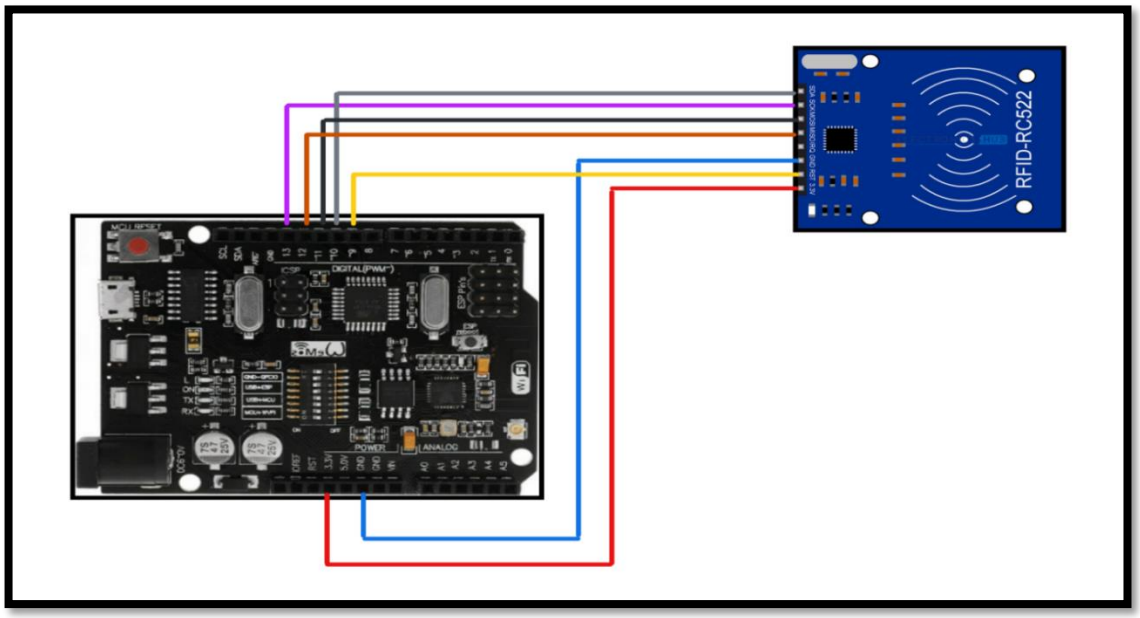

Figure 3.12 RFID connected with MCU-ATmega328P

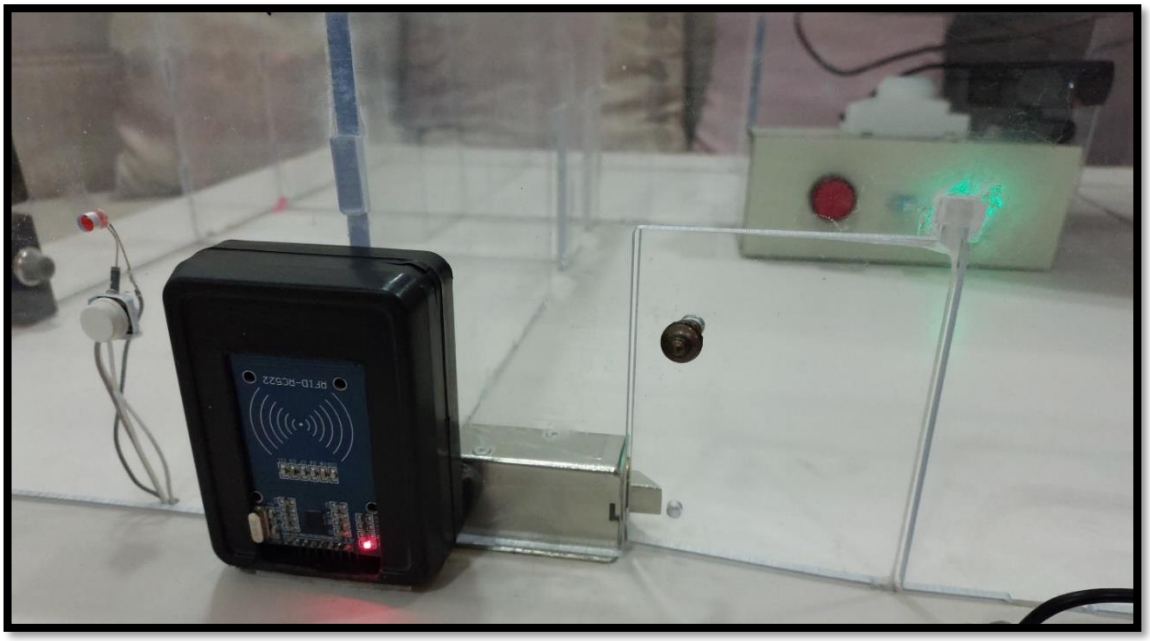

Figure 3.13 RFID Reader

3.3.2 Power Supply

DC-DC Buck Converter Step-down, 12V to 5V, 2A power, A voltage source was used to feed the devices in this system due to the significant need for a 5-volt voltage source for many sensors and relays and a 12-volt source for other purposes. As shown in Figure (3.14)

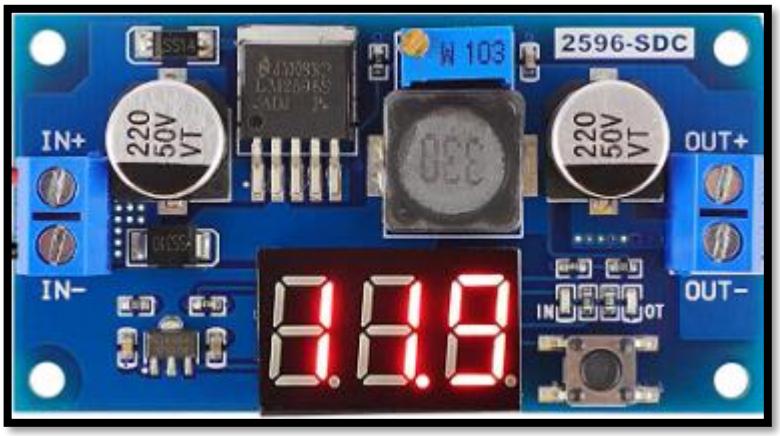

Figure 3.14 Buck Converter DC-DC Step-down

If an auxiliary power supply is needed in the proposed system, there are many ways to supply this, such as a DC battery, an AC adapter, a rechargeable battery, etc.

3.3.3 Control unit

The microcontroller is the main element to which almost all sensors and relays are connected. On the other hand, it transmits the sensor's readings and the status of different devices to the broker node. This system makes use of the following microcontrollers:

- **Arduino UNO**

This part connects all the sensors in the indoor unit for the house. such as DHT11, MQ2, Ultra-Sonic motion sensors, and relays. On the other hand, it transmits sensor readings and other devices to the broker node to be displayed in the fog node and then, via Wi-Fi, transmitted to the cloud and from there to the

web application. Arduino Uno is programmed using an integrated development environment (IDE), which is based on the C/C++ coding language. Appendix (d-1) refers to the Environment System's running software.

- **Uno R3-Atmega328p-MCU ESP8266 -USB-TTL CH340G**

The main components of this part are RFIDs and relays connected to them. On the other hand, it transmits the readings of the sensor and other devices to the fog node to control the opening and closing of the door based on the permission of the person to enter. (IDE) is used to program (Uno R3-Atmega328p-MCU ESP8266-USB-TTL CH340G), which is based on the C/C++ language. The operating program for door access based on RFID is referred to in Appendix (d.2).

3.3.4 Relays

The 2-line relay shield connects with the Arduino Uno and waits for the activation signal from the controller to operate devices connected to it; each relay is responsible for one task. These tasks and the Arduino pins are shown in Table 3.1. The shield is 5 volts powered by the Arduino or by an external source. Figure 3.15 shows another 2-line connected to an Uno R3-Atmega328p to operate the solenoid door lock for the outdoor unit.

Table 3.1 Relay Shield pins and Microcontroller pins

Board Type	Pin No.	Relay No.	Description
MCU-ATmega328P	4	1	Main Door Lock
MCU-ATmega328P	5	2	Garage Door (Future Work)
Arduino Uno	9	3	Ventilation Fan ON
Arduino Uno	10	4	Cooling LED ON
Arduino Uno	6	5	Heating LED ON

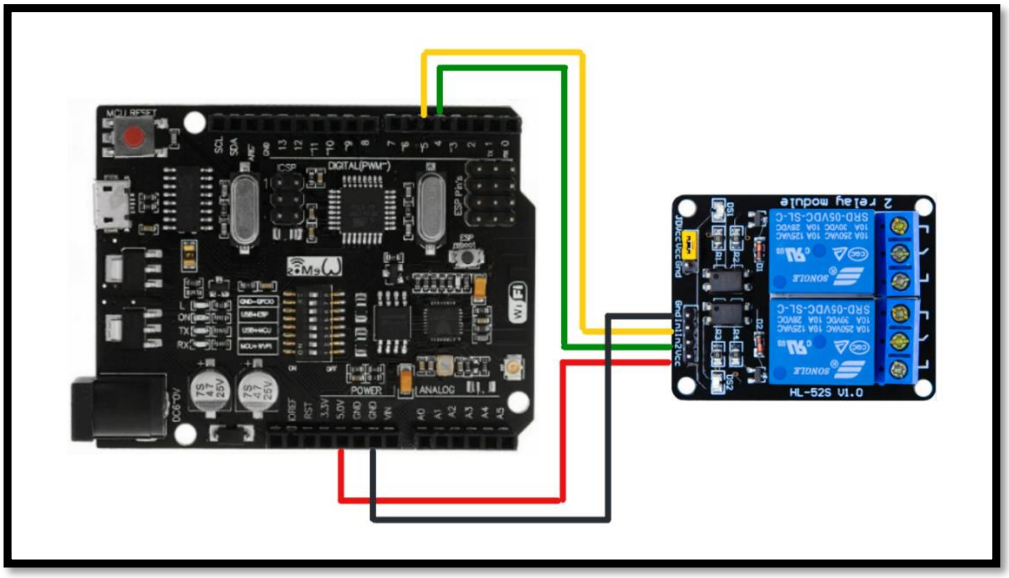

Figure 3.15 Door lock Relay connection

3.3.5 Actuators

This part represents the practical and applied side of the system, which means the output of the sensors and other mechanisms. For example, when temperatures rise above a threshold value, the cooling system will work, and so on.

3.3.5.1 Bush Button

Typically, push buttons are used in electrical circuits to switch on a component or transfer signals to a microcontroller when depressed., as shown in figure (3.16). The pins on the same side are connected when the button is pressed. Push buttons can act as switches. This switch is combined with an LED light; the LED can only be on while the button is pressed. Through this button, you can log in via the camera, and it also has another use, it activates a mic to record the voices of people at the door.

Figure 3.16 Bush Button

3.3.5.2 Solenoid Door Lock

This lock will operate based on the instructions from the microcontroller, which allows the door to be opened by authorized persons or manually by the owner. This lock works well. It works with 12 volts, is fast in response, and is tight. As shown in Figure (3.17)

Figure 3.17 Solenoid Door Lock

3.3.5.3 Buzzer

A small device that serves as a warning siren is used in the event of an intrusion into the house through a window or door. It has been practically linked with the ultrasonic sensor system.

3.3.5.4 Ventilation Fan

The indoor unit of the house is hooked up to a ventilation fan that works based on a gas sensor to let the air out if toxic or flammable gases start to leak.

3.3.6 Surveillance and Security

This part is for the security side of the house, which consists of surveillance cameras, consisting of two external and internal cameras. (USB-Webcam RAPOO C200) has been used inside and outside the home. To monitor the house from the inside and take photos if an intrusion happens into the place through the door or window. In contrast, the external camera will enable authorized persons to enter the house after recognizing them and verifying their identities using face detection and recognition technology. Also send photos for persons, whether they are trusted or not, to be displayed in the user interface. As shown in figure (3.18), appendix B for more details.

Figure 3.18 USB-Webcam RAPOO C200

3.3.5 Broker (Fog Computing)

It is correct to call it the local processing unit, which will work like the cloud but close to the peripherals. The application that connects all peripheral devices, actuators, sensors, microcontrollers, and cameras with cloud computing is designed in the C # language.

The tasks performed by this part of the system are as follows:

1- analyze, process, store, and present all the readings from the sensors, and send the readings to the cloud and from the cloud to the graphical user interface (GUI) to be monitored and controlled, such as (Temperature, Humidity, Gases, Distance).
2- The cameras are connected directly to the local server, so live photos are sent to the cloud and the homeowner right away.
3- Through it, persons authorized to enter are added or deleted with ease by saving a previous image of the person authorized to enter.
4- Receive the voice recording of the owner if there is a person at the door asking for permission to enter through the microphone and vice versa
5- The previous conditions can be changed programmatically via the C# language
6- The main entrance door can be opened manually through the Fog node

3.3.6 System Cloud Design

The goal of the cloud design is to collect data from different sensors such as temperature, humidity, gas, and smoke quantity and access it from anywhere and at any time through a web application. The devices can be controlled and home monitored through surveillance cameras and data storage The cloud consists of three main parts that are important in the design of a cloud system: client-side, server-side, and database-side. The client side displays data through a graphic user interface (GUI) consisting of two parts: the back end and the front

end. ASP.net Core and HTML5 have designed the back end, while the front end was created using many languages such as HTML5, React, and CSS. The server side provides information to the client side by collecting it from the database side or vice versa. The ASP Smarter.net server was used for this task. On the database side, MSSQL stores information from sensors and devices and displays it to the user on demand.

An SSL layer certificate protects the web application. The user can enter the site securely via HTTPS protocol and log in with a password to maintain the security of the transmitted information using the RSA algorithm. The RSA algorithm is one of the asymmetric cryptography techniques that have two keys the public key used for encryption and the private key techniques to make the process decryption [60]. One design feature is its high flexibility because the process of control provides the user with manual or automatic control using the website.

3.4 System operation

The suggested system is comprised of two components: the environmental system and the security system. Each area has its unique scenario:

3.4.1 Environment System

The temperature, humidity, and other factors like the amount of gas leaks, smoke, fires, etc., the system will create the ideal atmosphere for those within the home in this section.

i. Starting with the endpoint's sensors, the endpoint gathers sensor data and compares it to threshold values previously set in the Arduino Uno's memory to make decisions on how to operate the devices connected to each reading.
ii. Once all tasks have been completed, the data may be transferred to the broker via a USB cord. to use the application to show the data on the

computer's screen (local server). The C# language is the primary tool used to display and modify data

iii. The broker node uses Wi-Fi to transmit packet data from sensing nodes to the cloud. Keeping data safe across internet connections using the HTTPS Protocol

iv. There are alerts sent directly from Fog Computing to the homeowner in case of abnormal readings, such as the sensor that detects harmful gases, which may cause disasters. Alerts are sent through the Telegram application by using the Bot API platform to send text messages to the owner through a Wi-Fi that is connected to the internet immediately when a gas leak or fire occurs.

v. All readings will be stored in the cloud through the database MSSQL, then displayed over the GUI.

vi. When the user opens the web page with a secure username and password, they can see how the house is doing in terms of temperature, humidity, different gases, and previous readings. This is done through a simple and easy-to-use user interface.

vii. The following flow chart describes the entire environment system in Figure (3.19) for the end node part and Figure (3.20) for the broker and cloud part.

.

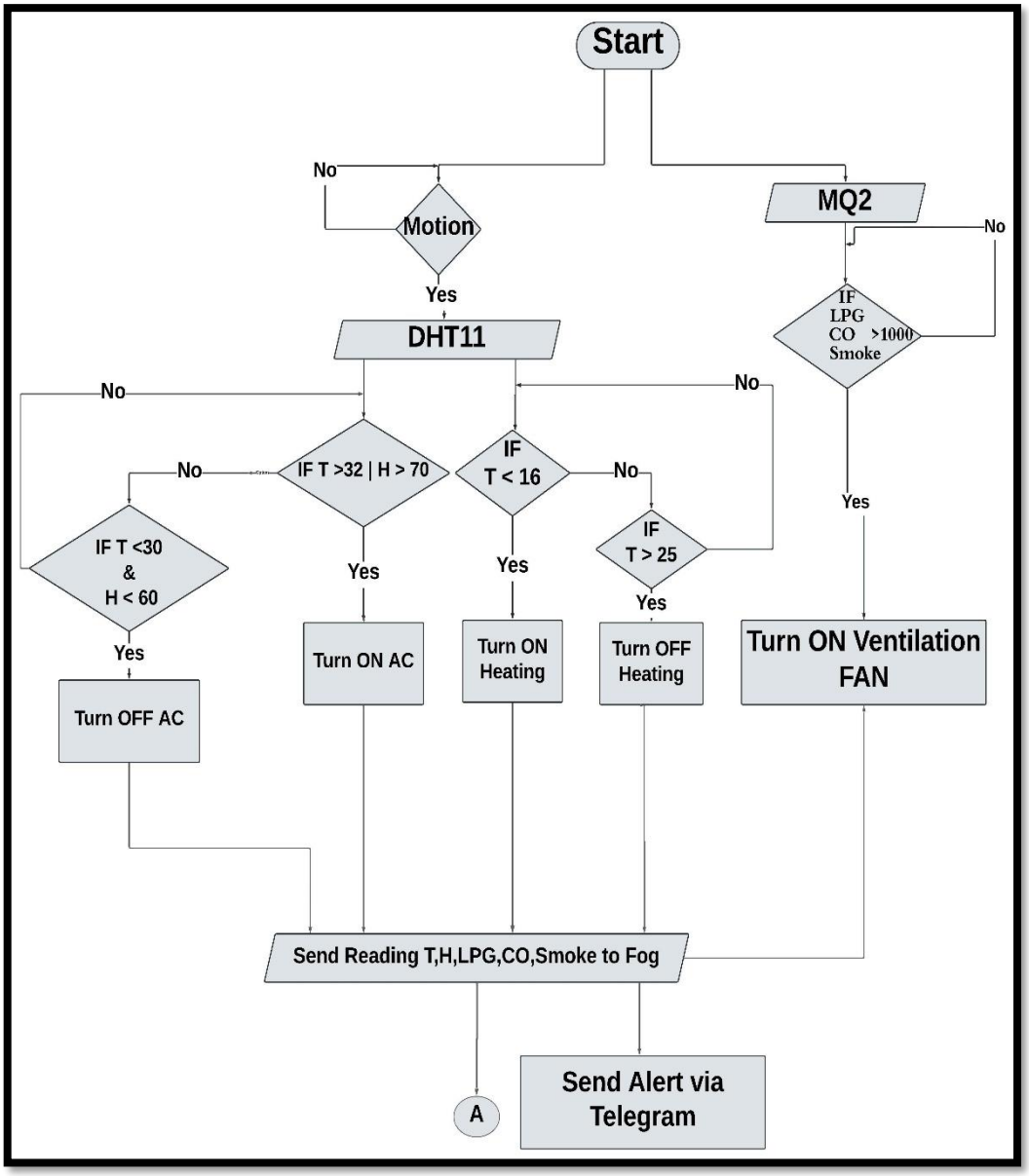

Figure 3.19 End node system operation Flow chart

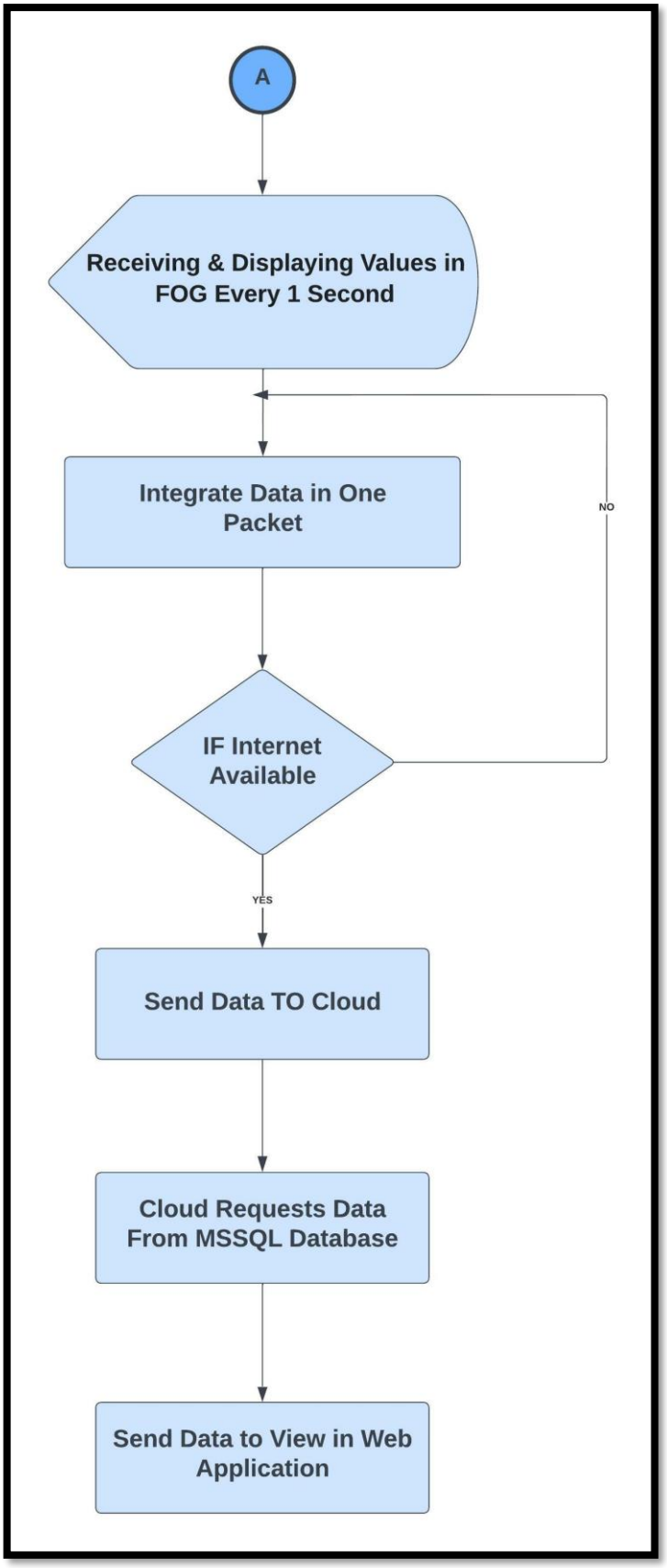

Figure 3.20 Broker node System Operation

3.4.2 Security System

The most important part is the protection and security of the home, which is the part that is done in monitoring and controlling the entry of authorized persons and the detection of strangers and intruders.

i. First, the person asked to enter the house will press the button to activate the camera. The camera will start taking photos and send them immediately to the fog computer, which will send the path of the images in Base 64 format with a unique code encrypted with API KEY and API Script keys over HTTPS to the FACE++ API application. After detecting and recognizing the face, the photo will be processed with the images previously stored on the computer. It sends the result of whether the person is reliable or not.

ii. Then, after the broker node receives the data from the Face++ API application as a JSON array, it will convert the format of String JSON to Object JSON and compare the result with the fog condition that must be greater than 85% as a comparison ratio rate. The broker will analyze the data and send it to the final node as a packet. A packet received at the end node will carry the control data to the node. Fog automatically sends a request to the MCU-ATmega328P to open the door via WIFI. The controller will instruct the relay to be in the normally open mode to open the door for the authorized person to enter. The door will open for no more than several seconds and then lock again as a kind of protection to ensure that the door is locked after people enter.

iii. If the person was not detected in the system, the comparison rate was less than 85 percent, or there was no previous data, the door would stay locked and an instant snapshot of the stranger would be transmitted from the fog to the cloud and then to the GUI. Additionally, a text message will be

delivered immediately through the Telegram app. The homeowner may communicate with the person via loudspeaker, while the individual can converse with the homeowner using the camera's microphone. The homeowner may manually unlock the door using the online application.

iv. Another feature is to enter the house via the pre-defined RFIDs in the cloud, where the holders of the defined tags can enter the house with the exact mechanism as in the images. It is possible to add new tags and delete stolen or lost cards with ease through the graphic user interface or the web application.

v. The ultrasonic sensor has been placed inside the house concerning the door and window security system. When the door or window is broken, the protection system will work when the signal is sent from the Arduino UNO via USB to the local computer, calculating the distance with the pre-set distance as a threshold value. The buzzer will deliver a warning when someone cuts off the signal; it will then transmit the data to the fog. After processing and analysis, the camera will activate and start capturing images and sending them to the cloud, from where they will be visible on the web page immediately and with less response time. At the same time, an alert message will be sent to the homeowner as a Telegram message stating that there has been a security breach in the house.

For this system not to be a nuisance or create concern for the homeowner, consideration has been given to the people that the system can recognize. When the owners enter their houses, the security system will wait sixty seconds to ensure that outsiders and intruders are detected upon admission. In other words, when a recognized person enters a residence, the ultrasonic sensor system is deactivated for sixty seconds.

The following flowchart describes the whole security system: Figure (3.21) For the RFID portion and the admission of allowed individuals, Figure (3.22),

for the camera portion and the access of individuals using face detection and recognition technology, and Figure (3.23) The security system for both the window and the door based on the internal camera.

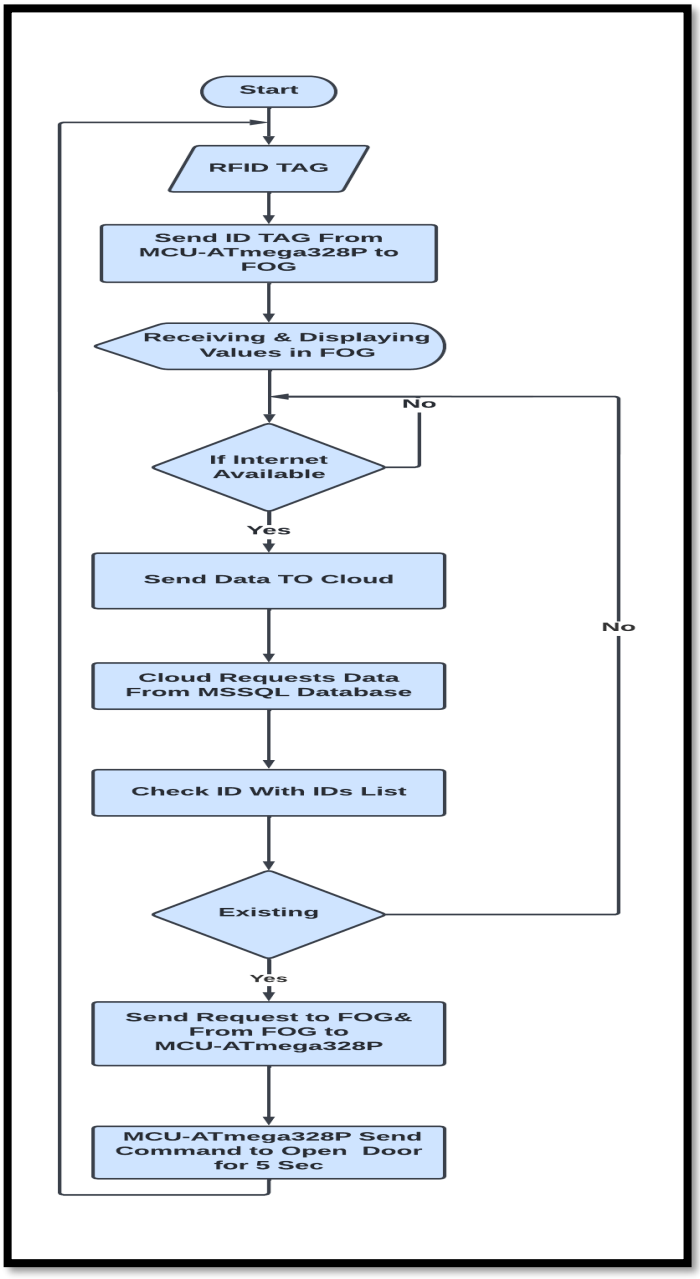

Figure 3.21 Access permission using RFID

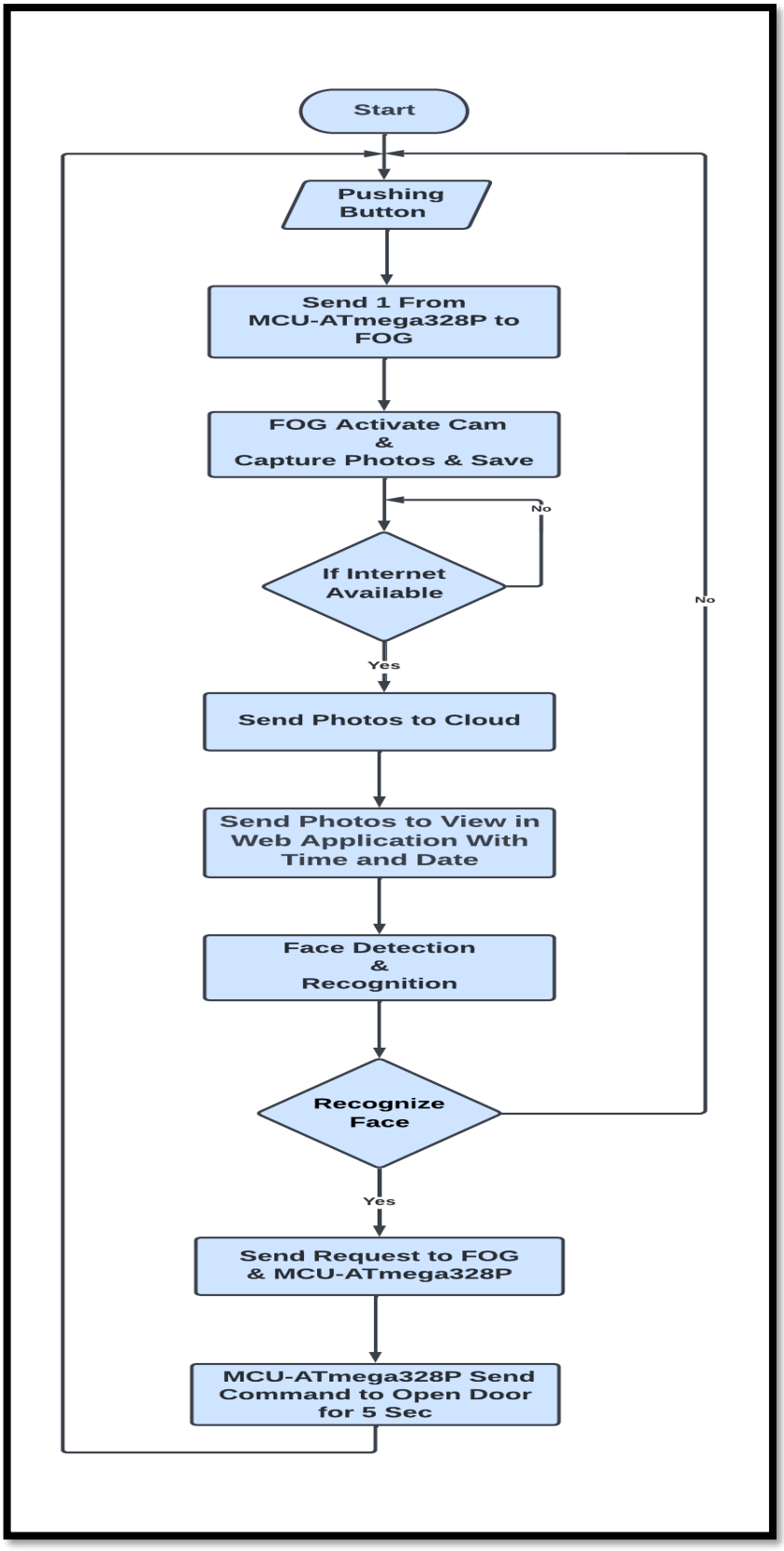

Figure 3.22 Access Permission Using Face Detection and Recognition

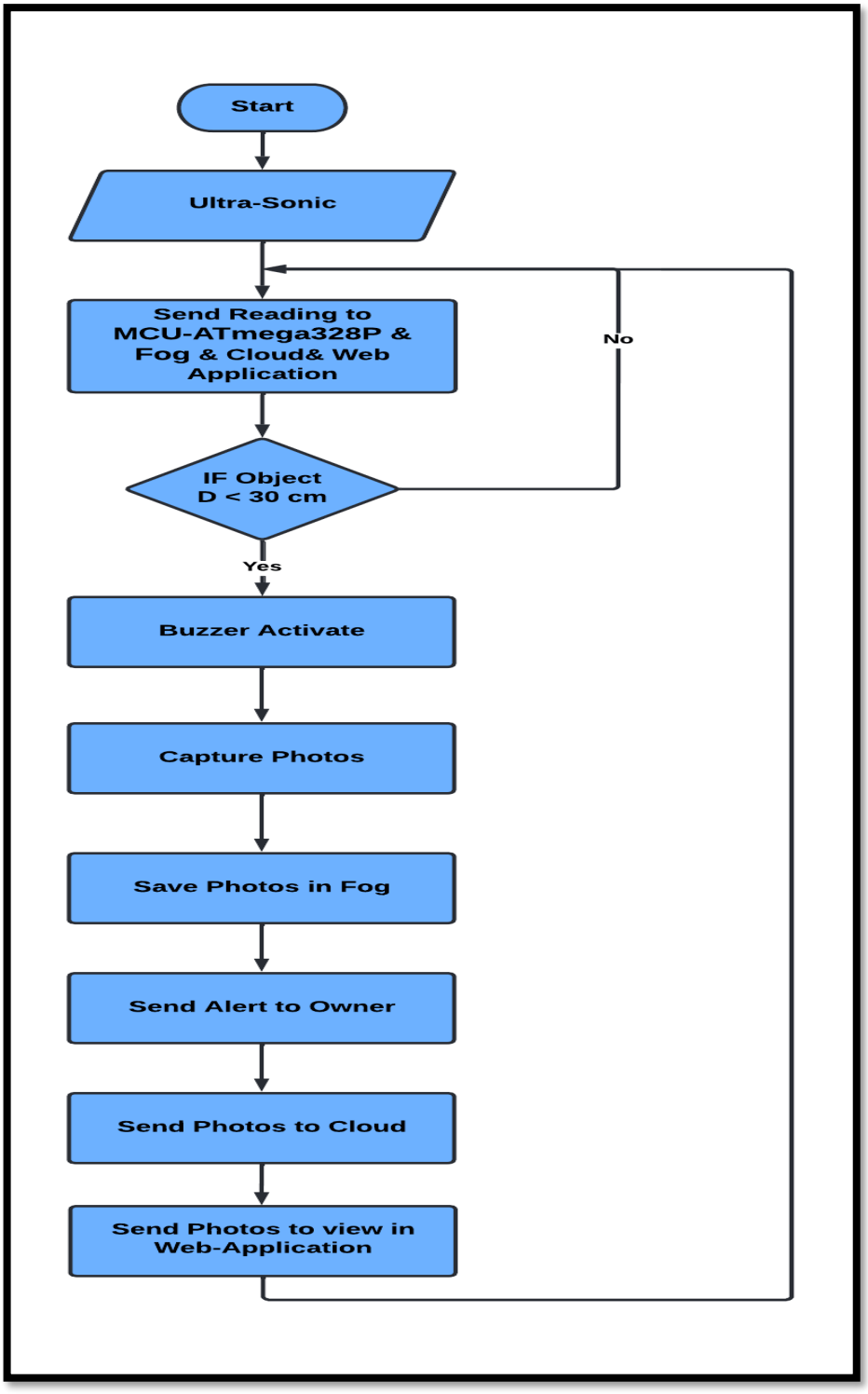

Figure 3.23 Door and window security system

Chapter Four

Results and Discussion

Chapter Four

Results and Discussion

4.1 Introduction

In this chapter, the smart home automation system will be presented and discussed from several aspects to show the positive characteristics and improvements provided by the proposed system. The system consists of four main parts: indoor and outdoor units; a broker (FOG), and a cloud (GUI) web application. So, the system's results will be talked about from the point of view of each unit.

4.2 Description of user interfaces for monitoring and controlling

It is possible to monitor and control the home through the user interface of a local computer, which is part of the system as a broker between end nodes and the cloud. At the same time, it is a means of monitoring and control to display the reading of all sensors, including Ultra-Sonic distance, temperature, humidity, and gas, and smoke percentage, as shown in figure (4.1). Indoor and outdoor surveillance cameras as shown in figure (4.2).

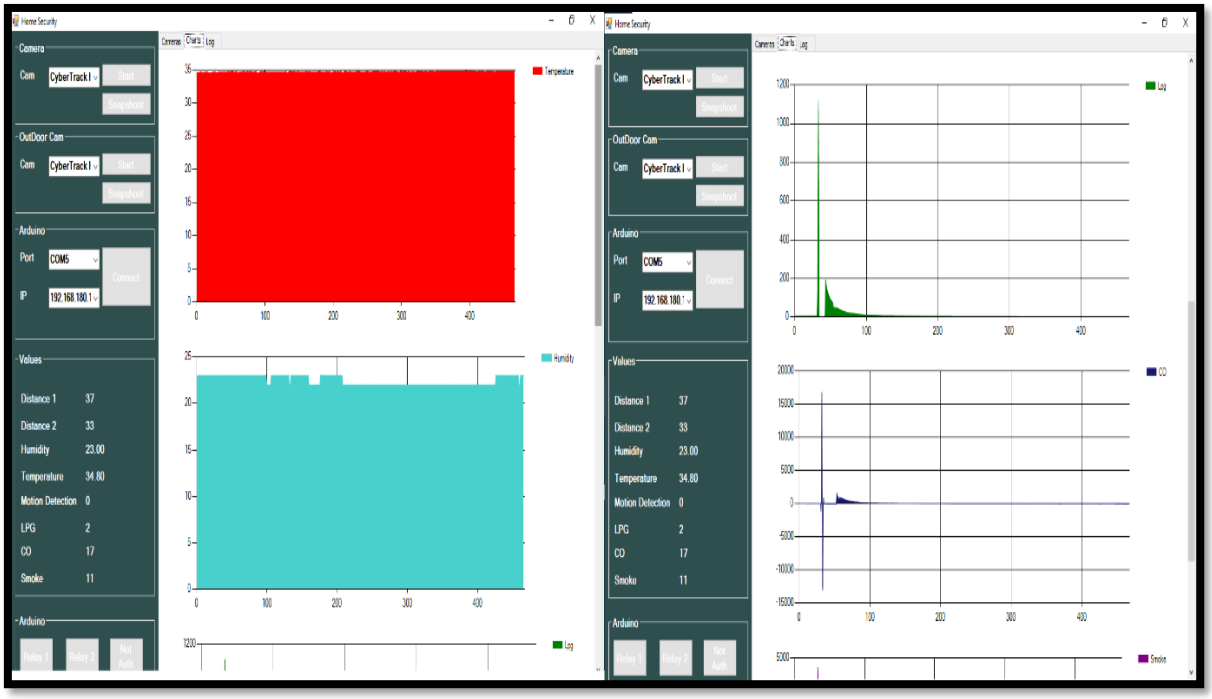

Figure 4.1 Sensors Measurements Reading from Fog Node

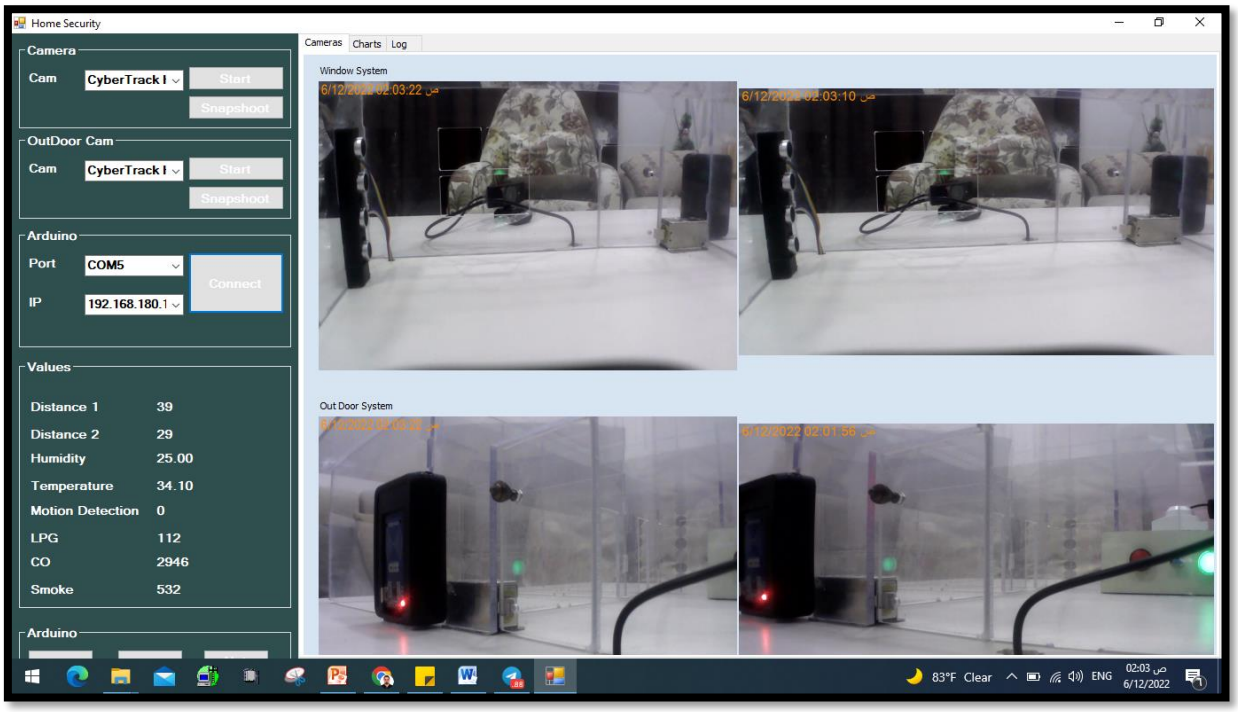

Figure 4.2 Indoor and Outdoor Surveillance Cameras from Fog Node

The home can also be monitored and controlled through a graphical user interface to show the measured sensor values sent by the broker node. The GUI consists of four parts: the login page, monitoring sensors values page, RFID list,

and security page. The first part is (login) using the username and password as shown in figure (4.3); the second part is the values, which display sensors' readings in real-time. The third part is the RFID tags registration, which displays the pre-defined tags and the possibility of deleting and adding tags. The fourth part is the media, which monitors people's entry upon each entry process. Also, it is possible to create a voice call, as shown in figure (4.4).

Figure 4.3 GUI Login page

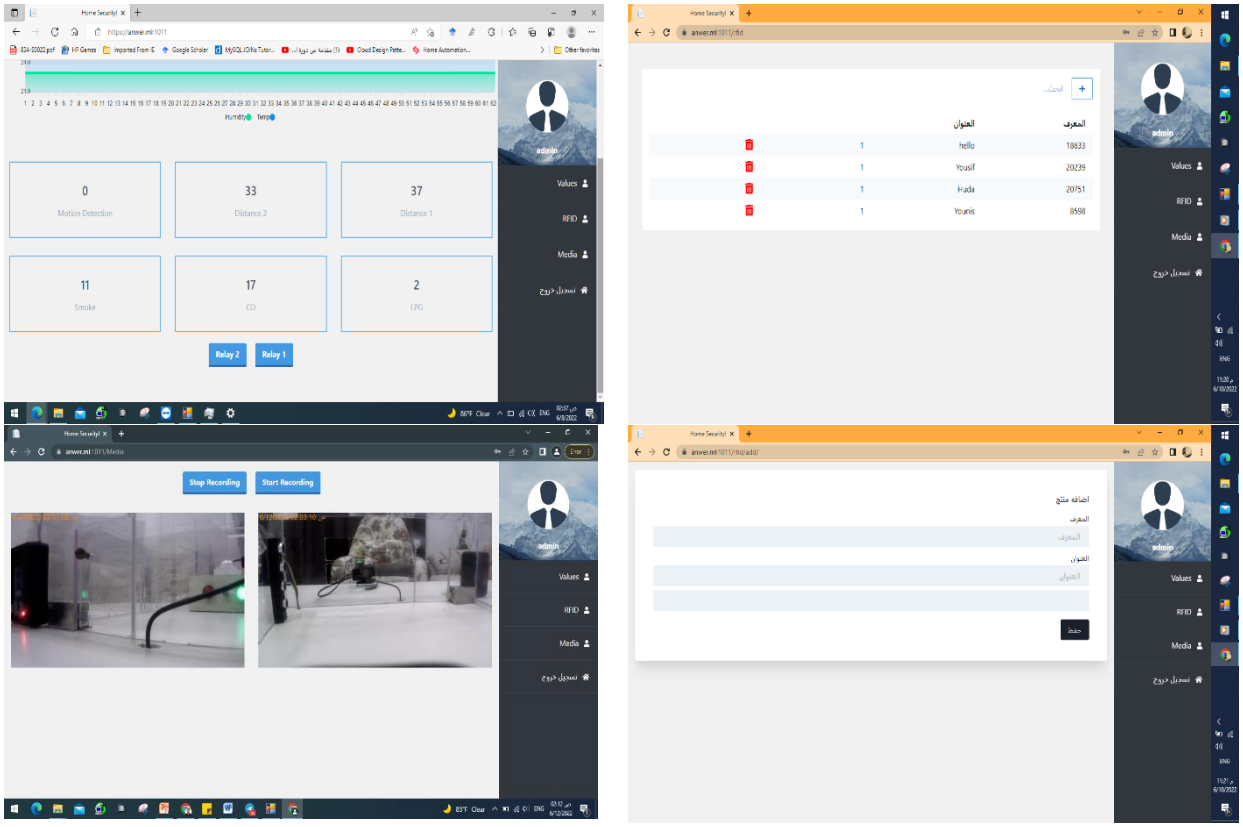

Figure 4.4 GUI Sensors reading, RFID list, and indoor/outdoor cameras

4.3 The Results from The Indoor Unit Perspective

The indoor part of the house is concerned with all issues related to living, whether it is in providing the appropriate environment and controlling the temperatures according to the user's desire, or in securing the owners of the house from the leakage of gases, smoke, and fires, or in protecting the home from intruders and burglars. and power consumption. All of these aspects will be tested and presented with their practical results.

4.3.1 Temperature and Humidity

The proposed temperature and humidity systems will work based on the presence of people in the place only to reduce electrical energy consumption and turn off the devices when there is no one in the area. In case there are people in the room; the system will check the room's temperature; if it is greater than 32°C

or the humidity is greater than 70%, the cooling system will work and stop only when the temperature becomes less than 30°C and the humidity is 60%. These percentages are not fixed and can change according to users' needs. This condition will be executed automatically without human intervention, as shown in figure (4.5). The temperature reading will also be displayed in the program interface on the broker (Fog) computer screen, then sent directly to the cloud and from there to the graphical user interface to be displayed in real-time in the web application, as shown in figures (4.6) and (4.7).

Figure 4.5 Temperature More than 32 ℃

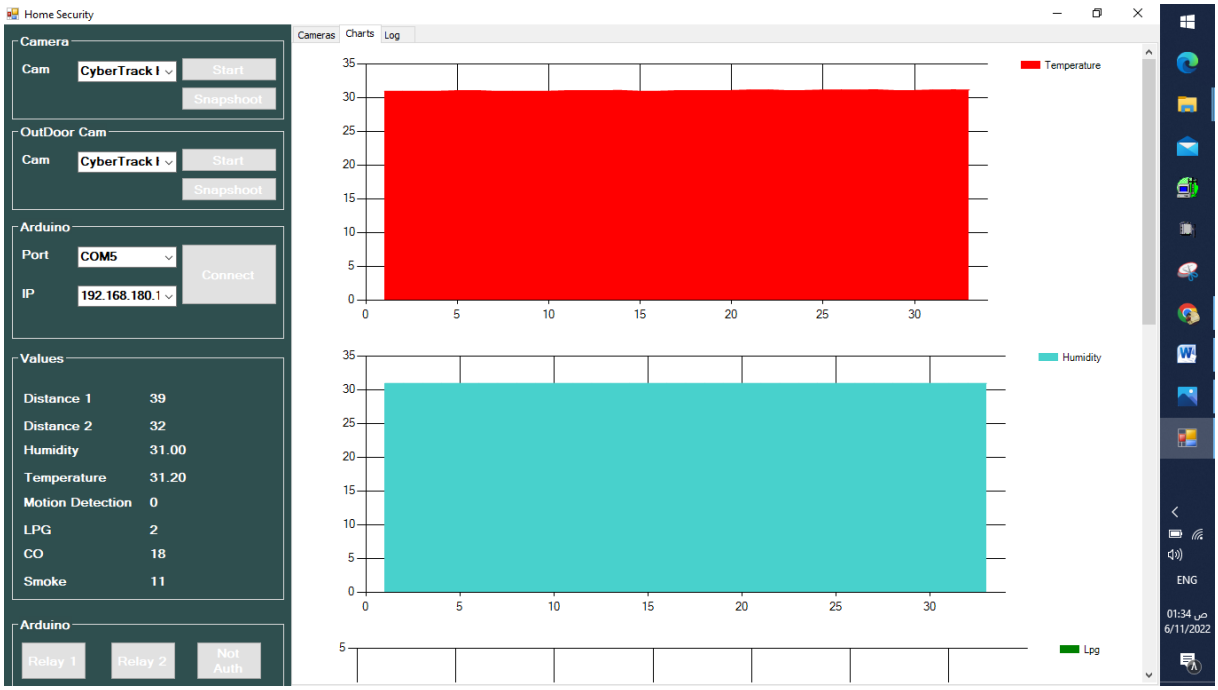

Figure 4.6 Temperature Measured from Fog user application

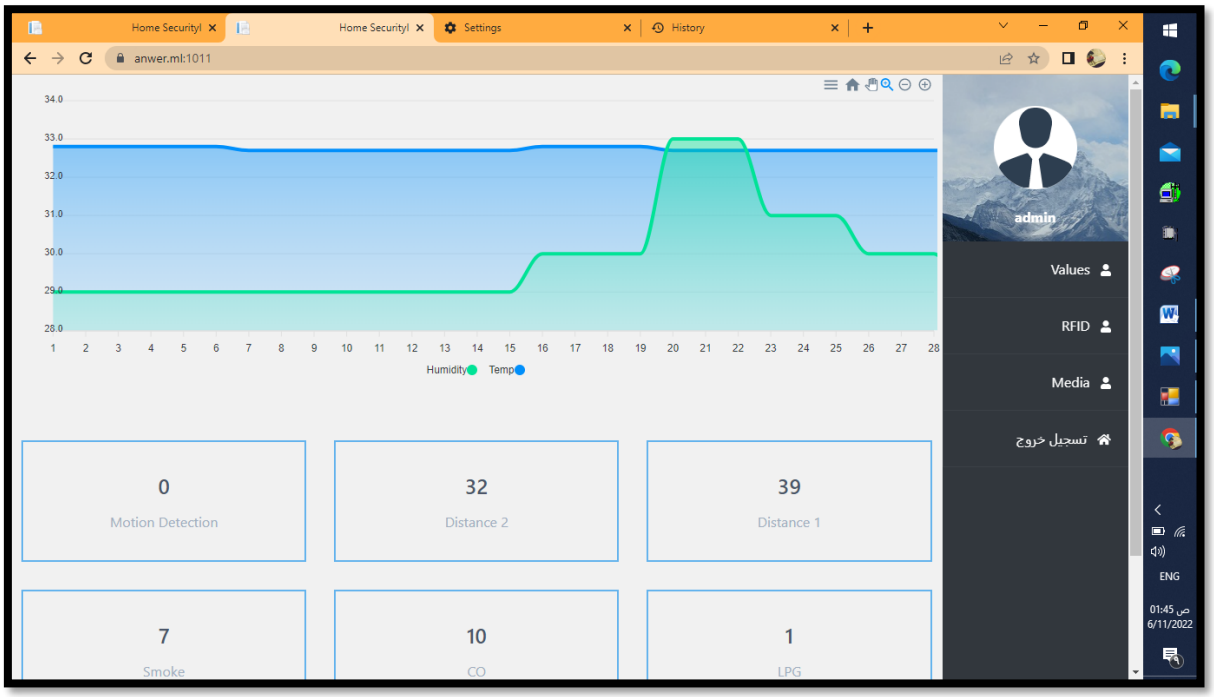

Figure 4.7 Temperature Measured from Cloud Web Application

The measured temperatures were calibrated from the DHT11 temperature sensor in the proposed system with the (Fluke 59 MAX/59 MAX+) Infrared Thermometer device. The results were very close with a small error rate, as

shown in figure (4.8). The percent error calculator equals 0.07886 % error. As the equation below:

$$\text{Percentage Error} = \frac{|\text{Approximate} - \text{Exact}|}{\text{Exact}} \times 100\ \% \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots (4.1)$$

For more information on the specifications of this device, see appendix C.

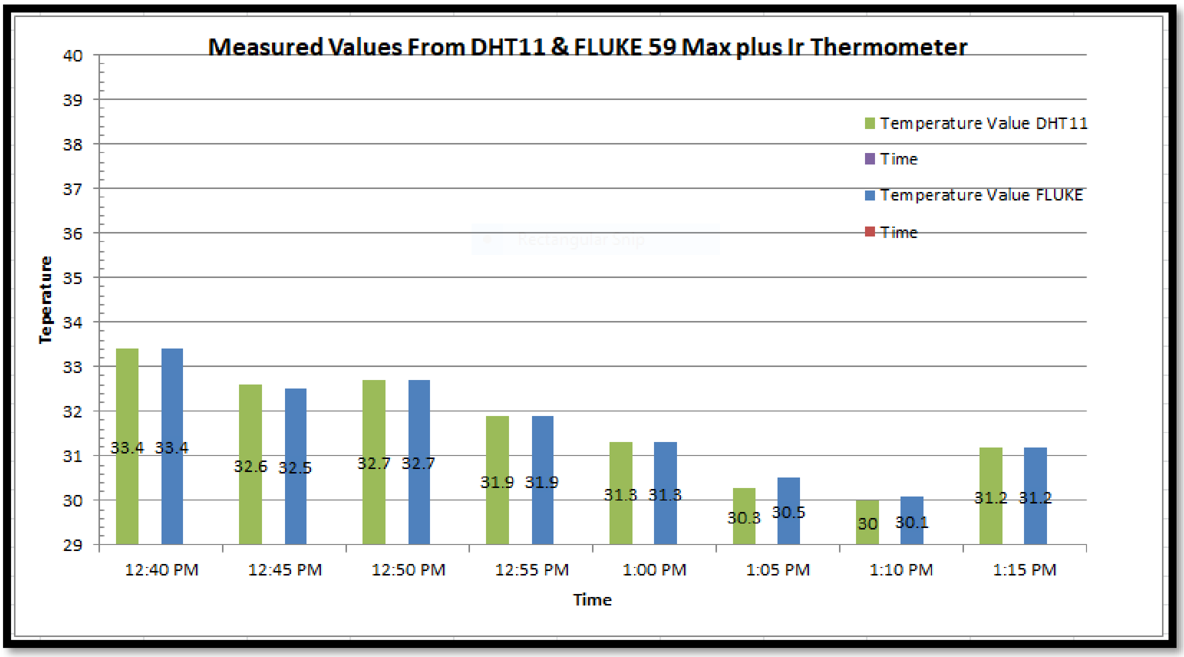

Figure 4.8 Temperature calibration results

4.3.2 LPG, CO, and Smoke Detection

Liquid petroleum gas (LPG), carbon monoxide, and smoke are considered dangerous gases, and warning about them and treating them in advance is very important. So, when these gases are in specific proportions, the ventilation fan will automatically work, as shown in the following figure (4.9). A warning message will be sent via Telegram to the personal account of the homeowner, as shown in Figure 4.10. In all cases, the readings for all these percentages will be displayed in the fog user interface and GUI as in figures (4.11) and (4.12).

Figure 4.9 ventilation fan automatically working

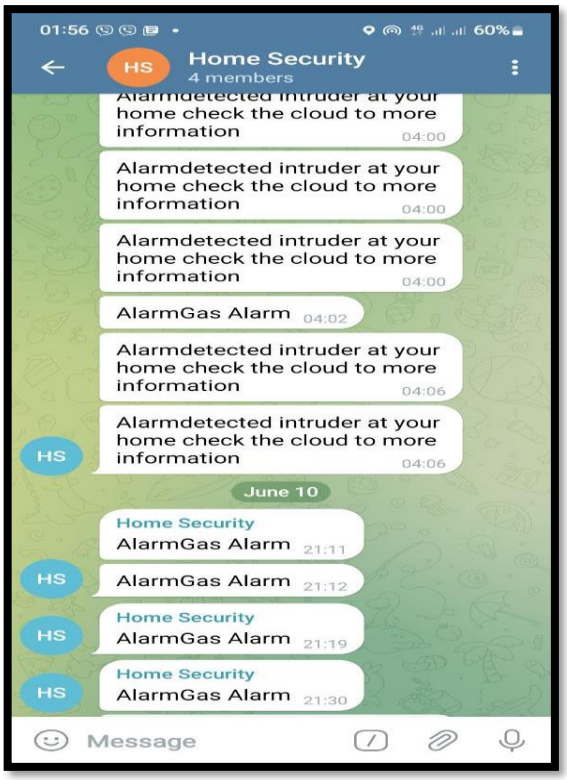

Figure 4.10 Gas alarm message via Telegram application

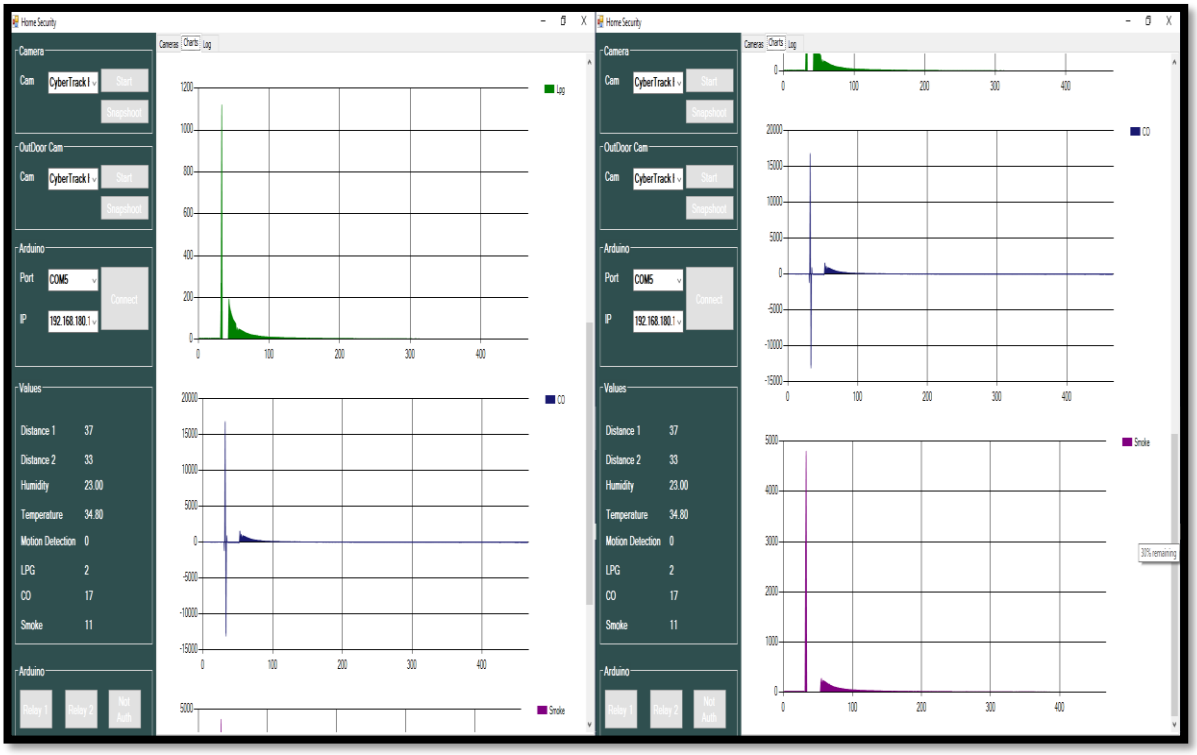

Figure 4.11 Reading rate of gases and smoke from the fog node

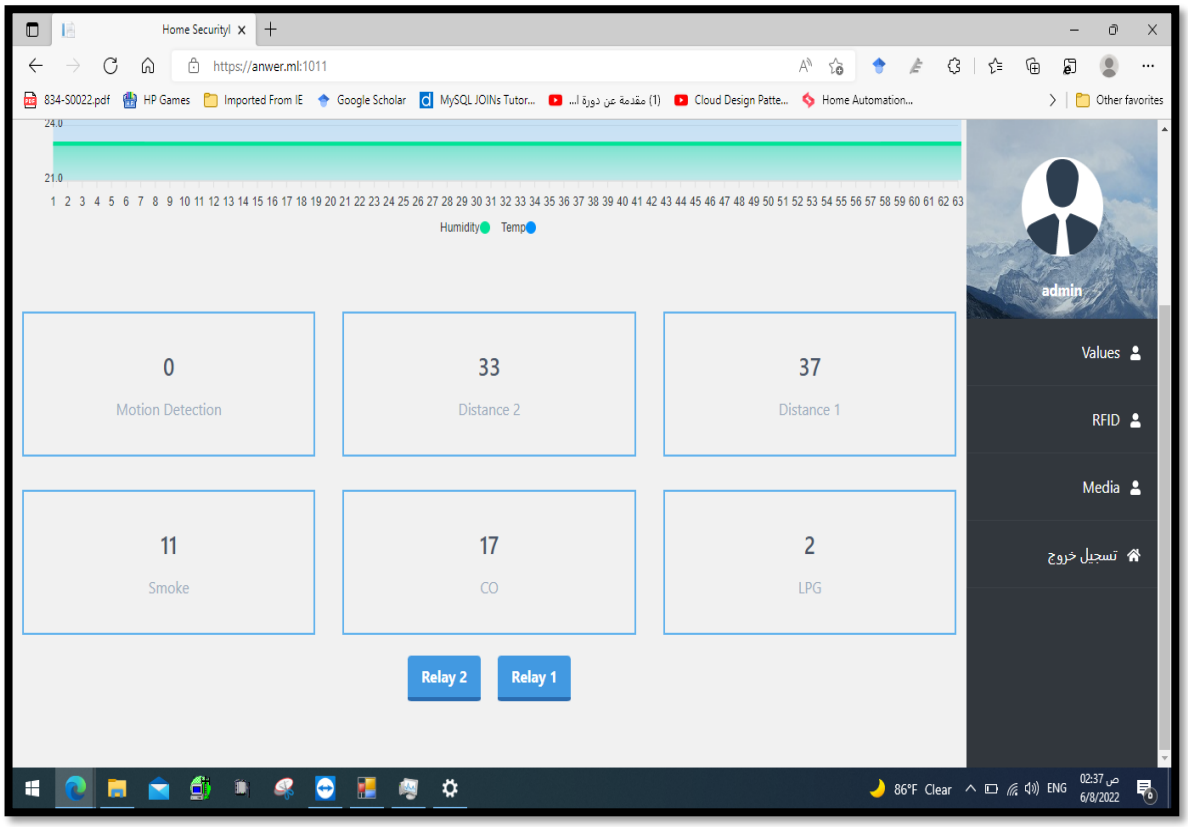

Figure 4.12 Reading rate of gases and smoke from the GUI

4.3.3 Main Door and Windows Security System

To protect the home from intruders and burglars, the proposed system secures the place with Ultra-Sonic sensors located on both the door and windows. When an object cuts off the waves, the alarm will sound immediately, after which an alert message will be sent via the Telegram app, stating that there is a security breach, as shown in figure (4.13). The second step will send instant photos through the indoor camera from the Broker (Fog) as shown in figure (4.14) and from there to the cloud to be displayed in the graphical user interface GUI as shown in figure (4.15). The homeowner can monitor the distance reading of the ultrasonic sensor through the web application, as shown in figure (4.16).

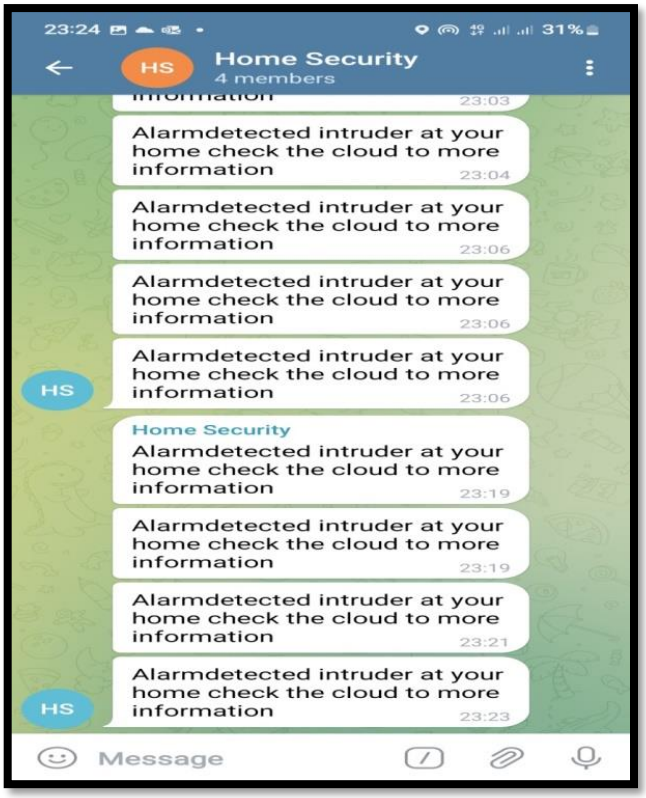

Figure 4.13 Alarm detected intruder inside the home

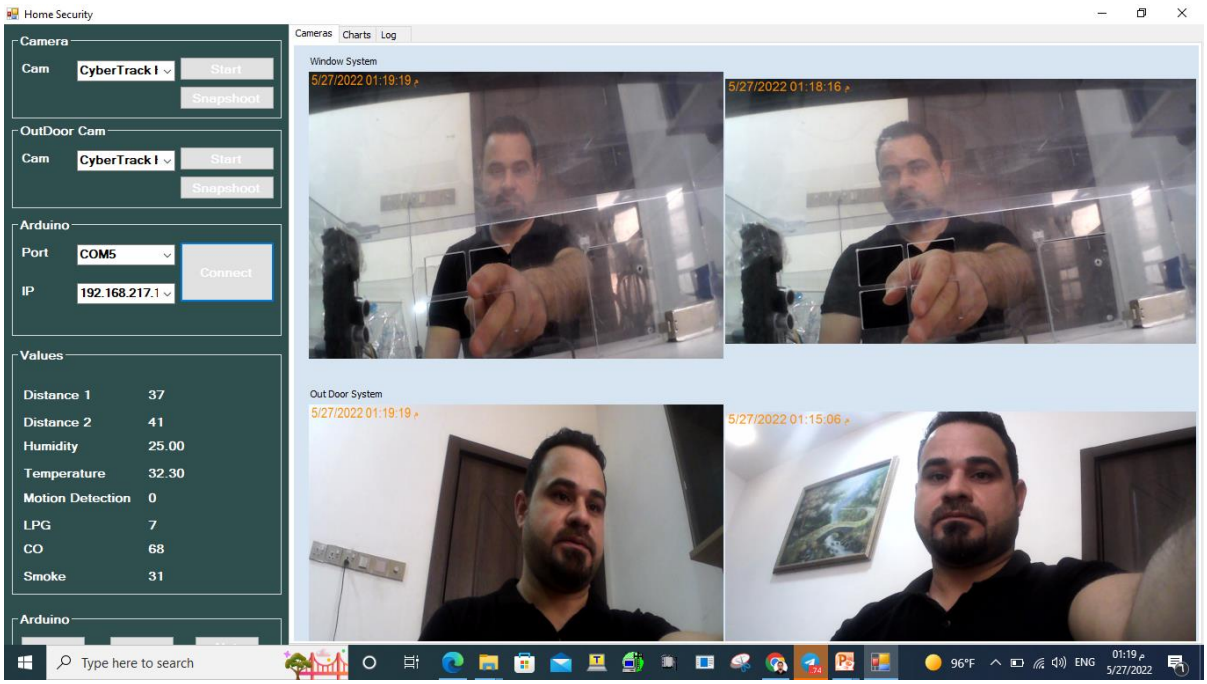

Figure 4.14 instant photos through the indoor camera from the Broker

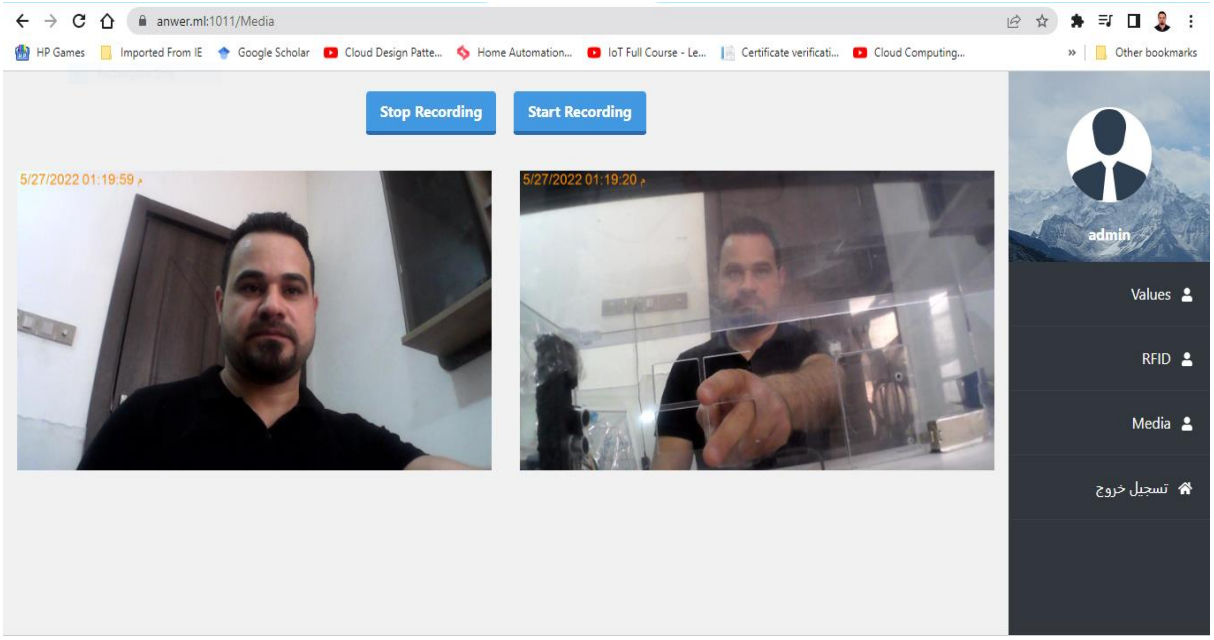

Figure 4.15 instant photos through the indoor camera from the GUI (Cloud)

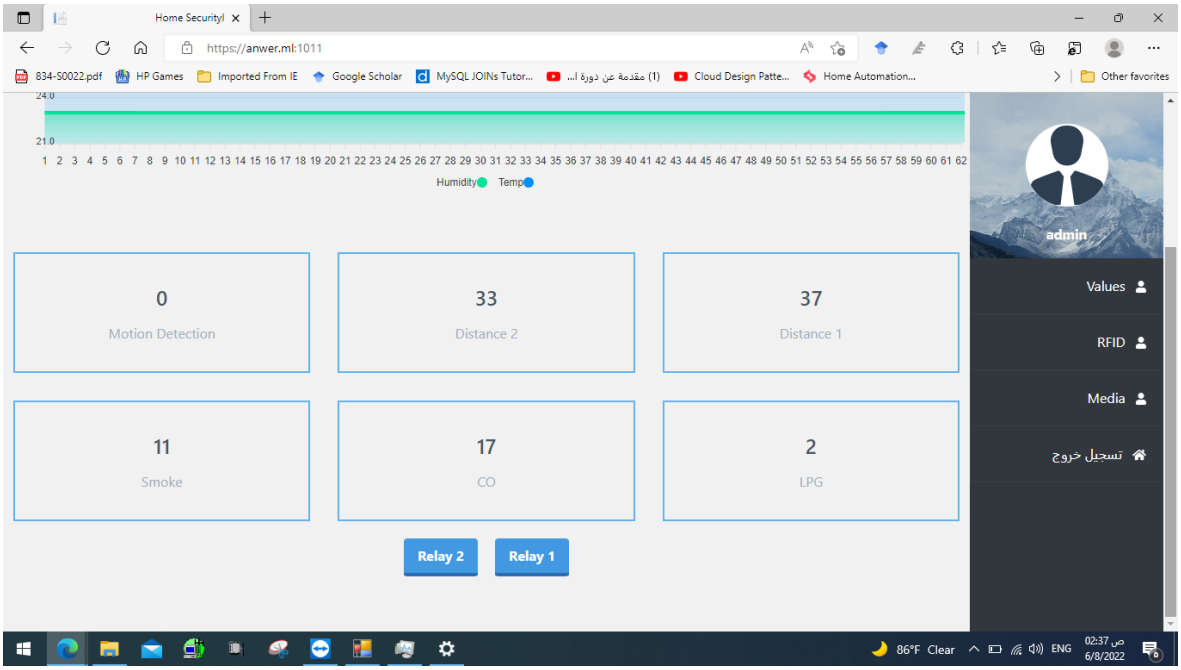

Figure 4.16 Distance reading of the ultra-Sonic sensor through the web application

4.4 Result from the Outdoor part perspective

This part of the proposed system is concerned with the procedures for entering the home by authorized or unauthorized persons. This part will test the different ways to get in, with two of them being automatic and the other being done manually.

4.4.1 Access permission using RFID

By using RFID tags and pre-defining cards in the cloud, anyone who has the registered tag can enter by placing the tag near the RFID, and the door will open automatically, as shown in figure (4.17). There is also the possibility to delete lost or stolen tags from the web application easily, as in figure (4.18). Another approach is that, through the program in Fog's computer, unknown or known tags can be read-alike, as in figure (4.19).

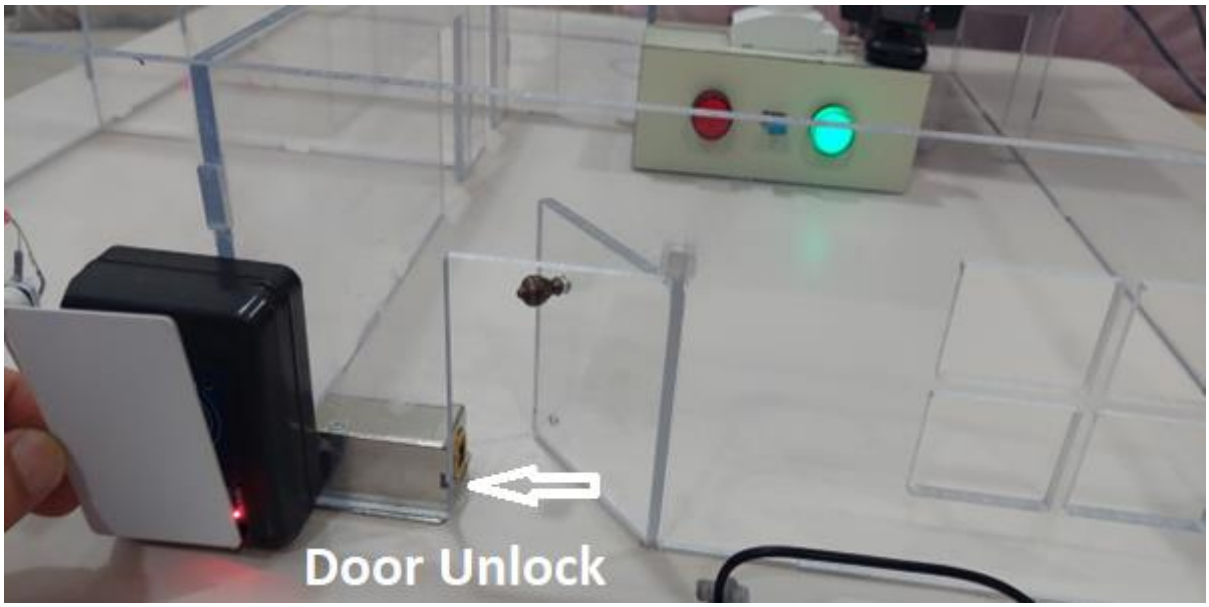

Figure 4.17 Opening the door with the registered tag

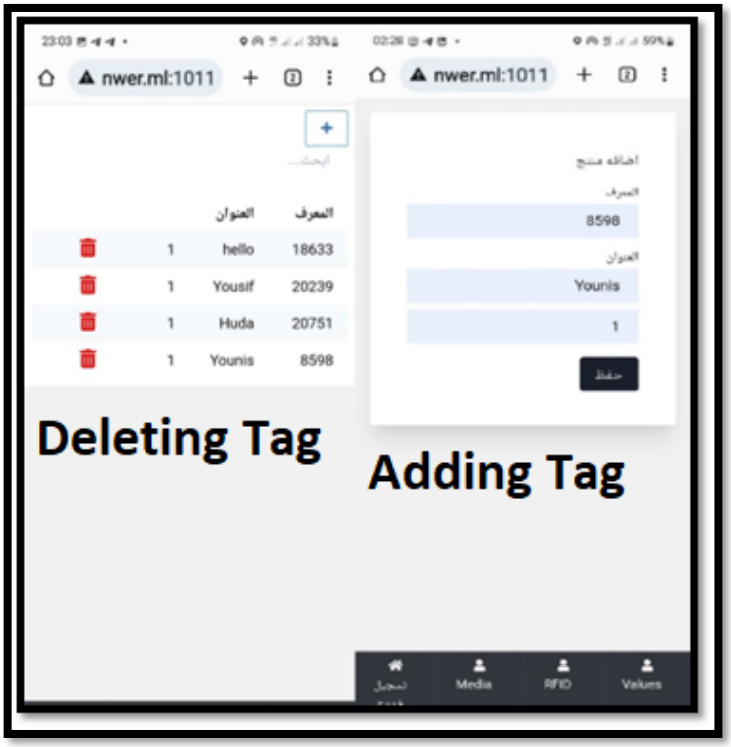

Figure 4.18 Adding/deleting tags from GUI

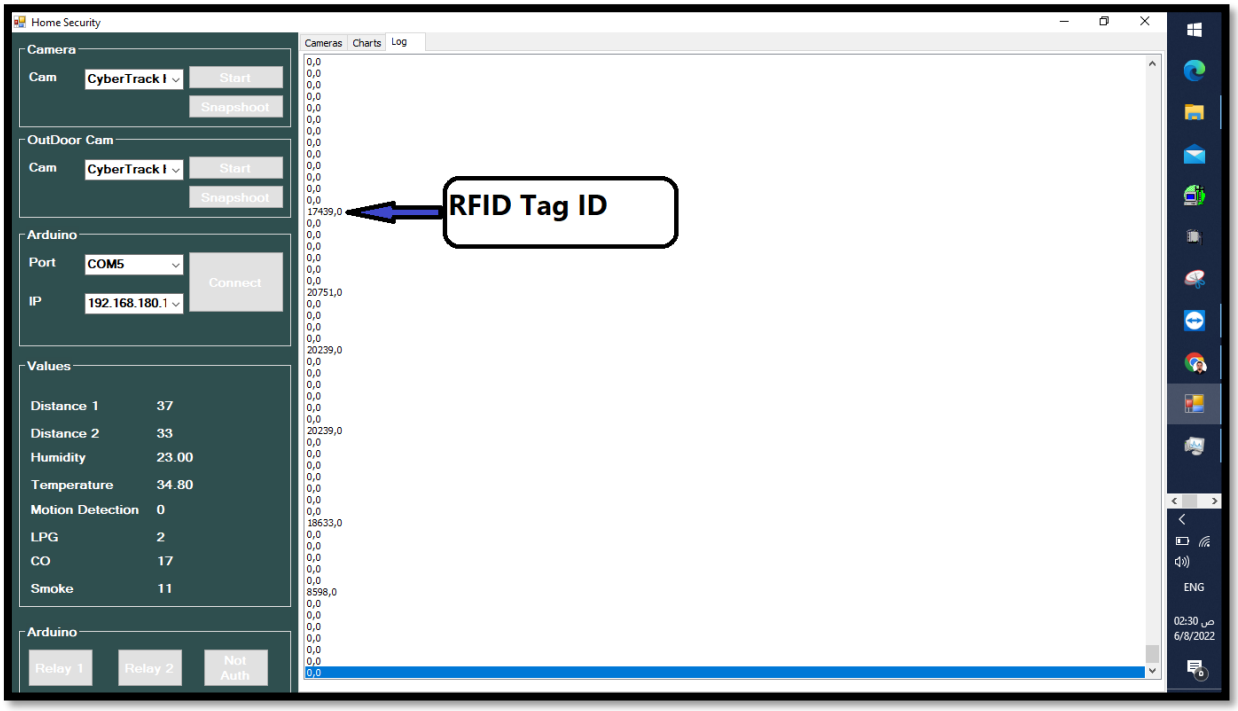

Figure 4.19 RFID tag ID reading from Fog node

4.4.2 Access Permission using Face detection and recognition

Initially, pre-images are saved for all family members on the broker's computer, as a database for verification, for one time only, as they are stored in a specific folder on the computer. When you press the button at the door, the camera will open directly and start to take a picture of the person after processing and matching the photo with the previous photo. When the authentication occurs, and the percentage of matching is 85%, enough to verify the person's identity, the door will open automatically, as shown in figure (4.20). At any rate, less than the specified percentage does not open the door to anyone who does not have prior information. At the same time, the system will send a warning message via Telegram as a notification of an unreliable login attempt. Each time an authorized or unauthorized person accesses the system, the photo will be stored and shown in the fog, then directly uploaded to the cloud and shown in the web application, as shown in Figures (4.21) and (4.22).

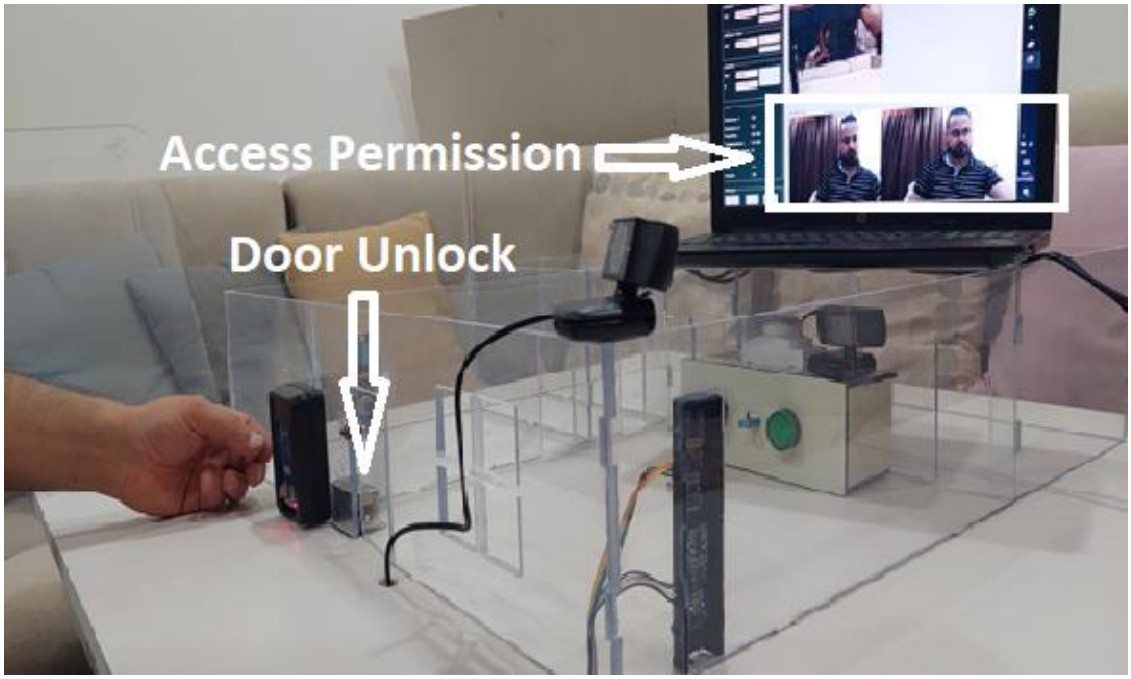

Figure 4.20 opening the door with based on face detection and recognition

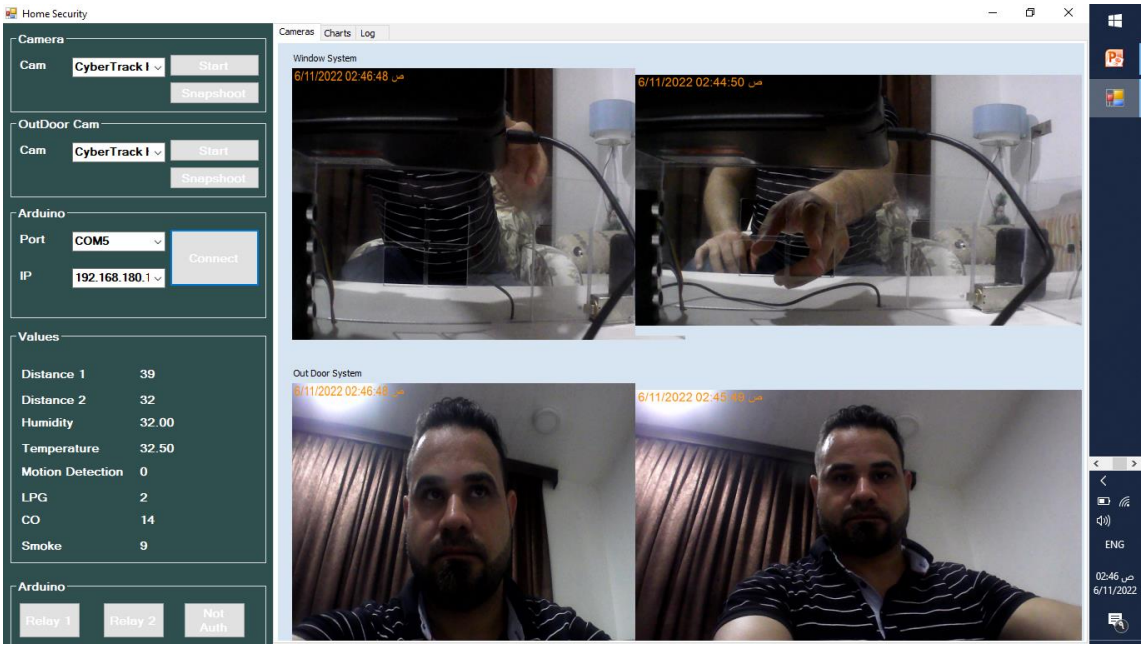

Figure 4.21 instant photos through the outdoor camera from the Fog node

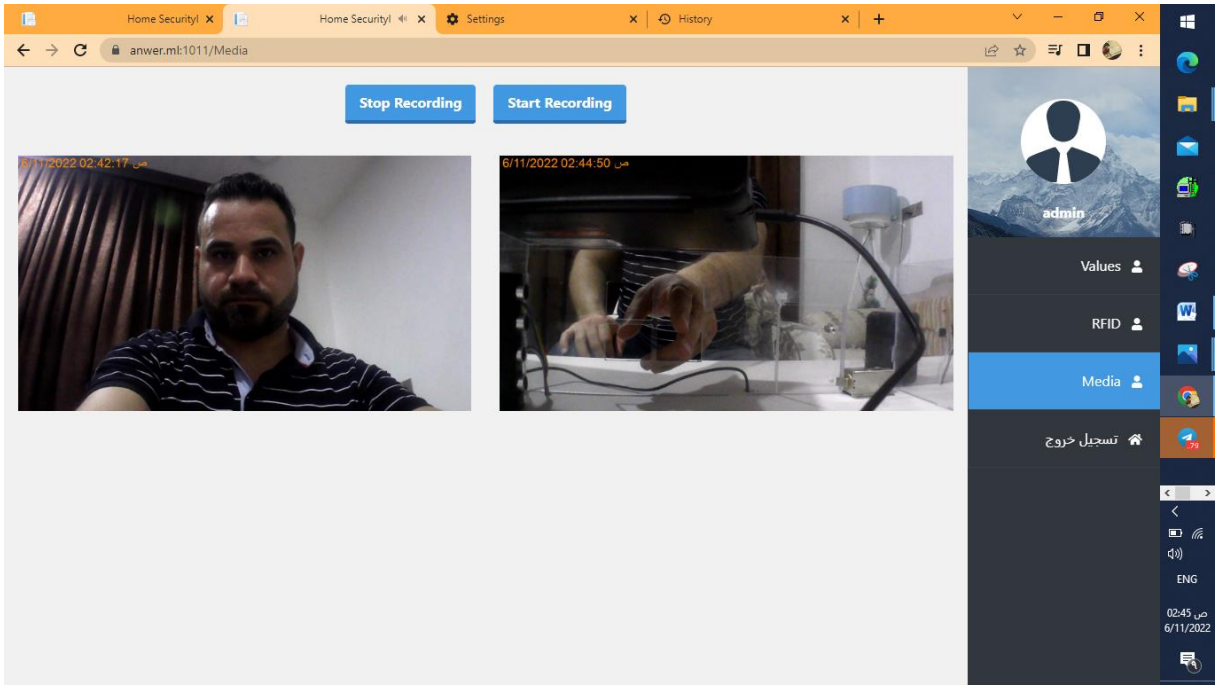

Figure 4.22 instant photos through the indoor camera from the GUI (Cloud)

There is the possibility of updating members' data and deleting or adding a new person by simply removing or adding the photo of the person concerned from the folder.

4.4.3 Access Permission Using Mic and Speaker

For the entry of visitors and persons known to the homeowner, anyone with no prior data in the system can use the Mic button to speak directly to the homeowner as a voice call. The homeowner can receive the call through the web application. The homeowner could open the door manually through the web application as well. as shown in figure (4.23).

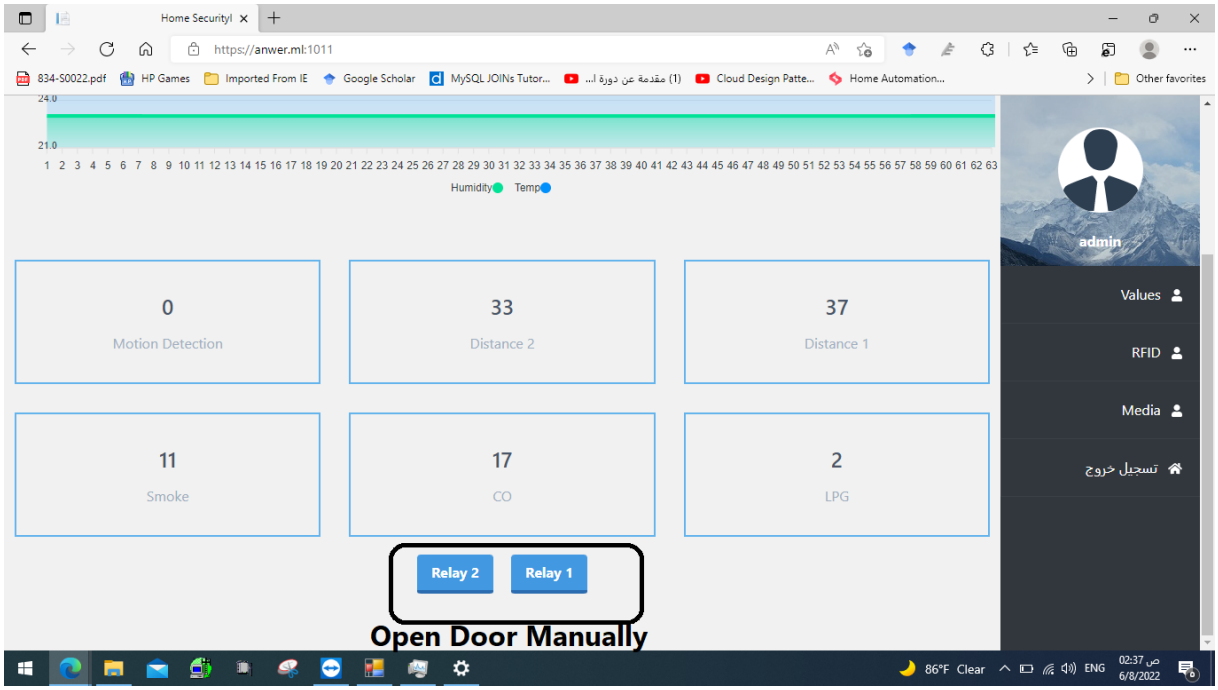

Figure 4.23 Opening the Door Manually

The table 4.1 represents the time Response for access Permission for the main door of the home by different methods:

Table 4.1 Time Response for access Permission

Access Mode	Test1	Test2	Test3	Test4
Manually (Fog)	1.65 Sec	2 Sec	1.74 sec	1.86 sec
Manually (Cloud)	4.37 sec	4.25 Sec	3.33 Sec	2.93 Sec
RFID Tag	3 Sec	2.66 Sec	2.39 Sec	3.1 Sec
Camera	4.05 Sec	3.055 Sec	2.25 Sec	3.055 Sec

Table 4.2 shows the comparison between our proposed system and the system presented by Musaddak M. Abdul Zahra et al.2020 [8]. Many enhancements

have been added concerning security and the environment, as will be summarized in the following table.

Table 4.2 Summarize the comparison between the two systems

The Proposed System	**Related work**[8]
Automatic monitoring for Sensor readings such as (Temperature, Humidity, gas, and Smoke) and control for home appliances	automatic monitoring of sensor readings such as (Temperature, Humidity, gas, and Smoke)
Telegram Urgent Notifications for Security & Environment requirement	GSM SMS Notifications
Capture images in case of Intrusion or authorized or unauthorized access with Telegram notifications	Live Video using Wi-Fi Camera without notifications
Access to home by using face detection and recognition and RFID	Not support
Keeping the door and window under monitoring by the indoor and outdoor camera and Ultra-Sonic	Door only by PIR
Power consumption By Motion Sensor, DHT11	Not support

Table 4.3 shows the test results of face recognition where 7 participants were taken to perform the test to find out the success rate. 10 trials were carried out per person. The test was conducted on 5 well-known participants, including the owner, and 2 unknown participants:

Table 4.3 results of face recognition

Participants	No. of Trials	RFID, Success Rate (%)	Camera, Success Rate (%)
User1	10	100	100
User2	10	100	100
User3	10	100	100
User4	10	90	100
User5	10	100	90
Unknown	10	100	100
Unknown	10	100	100

$$Average\ success\ rate\ = \frac{\sum Success\ of\ Each\ Participant}{No.of\ Participants} \times 100 \ldots\ldots\ldots\ldots\ldots (4.2)$$

$$= \frac{\sum 100\ +\ 100\ +\ 80\ +\ 80\ +\ 90\ +\ 100\ +\ 100}{7} \times\ 100$$

$Average\ success\ rate$ =98.57 %

Table 4.4 below represents a comparison between the techniques used in face detection and recognition with the percentage of accuracy for previous works and the proposed system:

Table 4.4 Comparison with other Algorithms:

Research Papers	Algorithm	System Accuracy (%)
Pawar et al 2018 [61]	LBP	80
Gunawan et al. 2017[62]	PCA, Eigenface	90
Dhobale et al. [5] 2020[63]	LBP	80-90
Mohi Uddin et al 2020[64]	Haar Cascade, LBPH	92.86
The proposed system	F++ API	98.57

4.5 Discussion

Studies and research on smart home automation have shown that there are a lot of problems, which helped this proposed system show how to solve the most important problems in this field.

1- Building a system that can inform the owner of any security breach in real time. The proposed approach focuses on this issue by using a server close to IoT devices to handle receiving, analyzing, and processing the data as a broker between the embedded devices on one side and the cloud server on the other side (fog computing). There are several advantages to using fog computing technology. In addition to reducing latency, it is possible to store and encrypt data before sending it to the cloud as a protection system that maintains the security of the transmitted data using the latest data encryption methods and keeps sensitive data near the end node, reducing the cost of reserving storage spaces in the cloud.

2- Homeowners face many problems and security threats if their RFID cards are lost or stolen. So, it makes sense to be able to quickly delete trusted tags or add new ones from the web application interface.

3- Ease of use and flexibility in changing the permission to enter the house manually and automatically from the local computer and cloud, whether adding or deleting defined people such as photos or RFID tags.

4- The door can be opened for a trusted person for 5 seconds and then closed automatically. This way, if the person forgets to close the door behind him

5- Alerts are sent only in emergencies to reduce the inconvenience to the homeowner

6- The system is designed to send alerts via Telegram in the event of a broken door or window or only in the event of a gas leak and make the system work automatically without human intervention.

7- The system is designed to reduce energy consumption and, at the same time, maintain a suitable atmosphere for homeowners, using a motion detection sensor with a temperature and humidity sensor

8- There is a case observed. To the results, if you set the temperature sensor to a specific value and make the air conditioner or heating system run at that temperature, there will be a fluctuation in the performance of the devices at this temperature, which is an unstable point; Consequently, the air conditioning or heater will work intermittently when the system reaches this point, so this state has been addressed by allocating two threshold value points.

9- The equipment for the designed system with the price for each piece is shown in table 4.5 below:

Table 4.5 Number of the equipment for the designed system with the price

No.	Part	Quantity	Price in $	Total price
1	DHT11 Sensor	1	5	5
2	MQ2 Sensor	1	3.95	3.95
3	Ultra-Sonic Sensor HC-SR04	2	0.78	1.56
4	Microwave motion sensor	1	3.69	3.69
5	RFID-RC522	1	1.13	1.13
6	Buck Converter-Step-down, 12V LM2596	1	5.75	5.75
7	Arduino Uno	1	9.41	9.41
8	Uno R3-Atmega328p-MCU ESP8266	1	7.98	7.98
9	Relay HL-52S	3	1.25	3.75
10	Momentary Pushbutton Switch	1	0.45	0.45
11	TMB09A03 3V Integrated Active buzzer sound	1	1.69	1.69
12	Solenoid Door Lock	1	10.95	10.95
13	BLDC FAN 12V	1	1.51	1.51
14	USB-Webcam RAPOO C200	2	19.98	39.96
16		Total	73.52	96.78

3.5 Features of the System

The following is a description of the proposed system features:

1. Instantaneous observation and management.
2. Sensor values and data can be displayed on web applications at any time, anywhere.
3. Both manual and automated control are supported by the design system.
4. By regulating the temperature within the home, the system created an atmosphere that was suited for living comfortably.
5. The system contributed to reducing electrical energy consumption through the operation of air conditioners in the presence of humans only through the use of a motion sensor with a DHT11 sensor.
6. The system protects the house from flames and toxic gases using a ventilation fan and pre-warnings.
7. The system is flexible in terms of adding authorized people to enter or delete them, such as RFID Tags and Photos, with ease through a simple user interface suitable for everyone.
8. Three security systems were installed to allow entry to the home through the camera, RFID, microphone, and speaker to identify the individual.
9. The online application is protected with a login and password, as well as HTTPS protocols.

Chapter Five

Conclusion and Future Works

Chapter Five

Conclusion and Future Works

5.1 Conclusion

This thesis presents the design and implementation of a home automation system using cloud computing based on enhancing security and the environment. The conclusion may be drawn from the following points:

1- The implemented system can display different sensor values (temperature, humidity, distance from window and door, LPG gas level, smoke level, and CO) locally from the broker`s computer user interface and remotely from the GUI.

2- Without human assistance, the whole system may be operated automatically within the home, for instance, by managing the ventilation fan, cooling, and heating devices based on the temperature, humidity, gases, smoke, and carbon dioxide levels.

3- The user can use a mobile phone, a tablet, or a personal computer to get to the web application panel.

4- The system makes use of a Wi-Fi network, which allows wireless connections between two or more devices for data exchange. A lot of users today utilize it on a variety of devices, including PCs, laptops, cameras, numerous home appliances, cell phones, etc.

5- In case of a leakage of toxic or flammable gases, fire, or smoke, the system will directly turn on the ventilation fan and send a telegram message. Installing a fire extinguishing system is possible.

6- The system contributed to reducing electrical energy consumption by linking the work of heating and cooling devices with the motion sensor.

So, the devices won't work unless the allocated temperature is met and some people are present.

7- There are three methods to unlock the entrance to the house: the first uses facial detection and recognition technology, RFID technology and manually operates the third approach is via the web application, the fog computer's user interface.

8- The system takes photographs and sends them immediately to the application, notifying the homeowner only in the case of a security breach via a door or window by text messages through the Telegram app

9- The system is characterized by ease of use and flexibility in deleting and adding RFID cards through the web page described in the fourth chapter. and the ability to delete and add personal photos to the system database from the fog computer.

5.2 Future Works

It is possible to make some improvements and additions to the proposed system using some modern technologies, which may contribute to reducing costs or adding convenience and safety in a wider and more reliable way. There are still many ideas and applications on the way to development regarding automated smart homes. We will mention some of these ideas:

1- Increasing home security and reliable access by adding voice and iris recognition systems to household members Recognize Iris-based solutions as the most accurate modern security technology. It has been largely used for identity authentication, as it has been used to control access at doors and entrances

2- It is expected that the satellite Internet service, especially the Star Link company, will be launched in multiple places, so the idea of transmitting data between the fog and the cloud through it is a good idea in terms of service stability and data transfer, which reaches nearly 300 Mbit/s and real-time transmission plus information security.

3- The system can be developed to include the garage door and automatically unlock it based on the car plate number and color pre-set in the system.

4- Based on occupancy sensors, we aspire to design a system for turning on/off air conditioners inside the sleeping room, where persons are present without movement during sleep, and thus to ensure that the various devices continue to operate during sleep.

5- Added more control options to the web application. For example, buttons or voice commands to operate various home appliances such as TV, music, heating, cooling, etc. Which can serve the elderly, the disabled, and children

6- Replacing the fog computer with an (Intel NUC) that is small in size, high in processing capabilities, and at an affordable price is a successful option for the home computer.
7- Distributing the powers of automation and control to the members of the house according to the needs of the person, for example, making the control of some household appliances under the control of the parents and other important matters.

References

[1] R. A. Sowah *et al.*, "Design of a Secure Wireless Home Automation System with an Open Home Automation Bus (OpenHAB 2) Framework," *J. Sensors*, vol. 2020, 2020, doi: 10.1155/2020/8868602.

[2] R. K. Radha, "Smart home design flexibility as an enabler of sustainability and the reception in Sulaiymaniah, Kurdistan Region-Iraq," *J. Build. Pathol. Rehabil.*, vol. 5, no. 1, p. 29, 2020, doi: 10.1007/s41024-020-00094-y.

[3] K. Mehaboob Subhani and D. S. Manoj Kumar, "An investigative study for smart home security: Issues, challenges and countermeasures," *Int. J. Pharm. Technol.*, vol. 8, no. 4, pp. 19448–19459, 2016, doi: 10.4236/wsn.2016.84006.

[4] I. K. N. Trisnawan, A. N. Jati, N. Istiqomah, and I. Wasisto, "Detection of Gas Leaks Using the MQ-2 Gas Sensor on the Autonomous Mobile Sensor," *2019 Int. Conf. Comput. Control. Informatics its Appl. Emerg. Trends Big Data Artif. Intell. IC3INA 2019*, pp. 177–180, 2019, doi: 10.1109/IC3INA48034.2019.8949597.

[5] A. Rafati, H. R. Shaker, and S. Ghahghahzadeh, "Fault Detection and Efficiency Assessment for HVAC Systems Using Non-Intrusive Load Monitoring: A Review," *Energies*, vol. 15, no. 1, 2022, doi: 10.3390/en15010341.

[6] M. Rahimi, M. Songhorabadi, and M. H. Kashani, "'Fog-based smart homes: A systematic review.'.," *J. Netw. Comput. Appl. 153*, vol. 102531, pp. 1–37, 2020.

[7] K. Sehgal, "Iot Based Smart Wireless Home Security Systems," *2019 3rd Int. Conf. Electron. Commun. Aerosp. Technol.*, pp. 323–326, 2019.

[8] M. M. A. Zahra, M. J. Mohsin, and L. A. Abdul-Rahaim, "Artificial

intelligent smart home automation with secured camera management-based GSM, cloud computing and arduino," *Period. Eng. Nat. Sci.*, vol. 8, no. 4, pp. 2160–2168, 2020, doi: 10.21533/PEN.V8I4.1718.G697.

[9] Shaik Anwar and D. Kishore, "IOT based Smart Home Security System with Alert and Door Access Control using Smart Phone," *Int. J. Eng. Res.*, vol. V5, no. 12, pp. 504–509, 2016, doi: 10.17577/ijertv5is120325.

[10] V. K. P. A. T. A.Anne Frank Joe, "Home Security System Using Raspberry Pi With IOT," vol. 7, pp. 5–8, 2021.

[11] S. S. Chowdhury, S. Sarkar, S. Syamal, S. Sengupta, and P. Nag, "IoT Based Smart Security and Home Automation System," *2019 IEEE 10th Annu. Ubiquitous Comput. Electron. Mob. Commun. Conf. UEMCON 2019*, pp. 1158–1161, 2019, doi: 10.1109/UEMCON47517.2019.8992994.

[12] M. Medhat, K. El-Shafey, and A. Rashed, "IoT-fog based smart-building security system design and performance evaluation," *J. Comput. Sci.*, vol. 16, no. 9, pp. 1325–1333, 2020, doi: 10.3844/jcssp.2020.1325.1333.

[13] T. Juhana and V. G. Anggraini, "Design and implementation of Smart Home Surveillance system," *Proceeding 2016 10th Int. Conf. Telecommun. Syst. Serv. Appl. TSSA 2016 Spec. Issue Radar Technol.*, 2017, doi: 10.1109/TSSA.2016.7871101.

[14] S. F. Kak and F. M. Mustafa, "Smart Home Management System Based on Face Recognition Index in Real-Time," *2019 Int. Conf. Adv. Sci. Eng. ICOASE 2019*, pp. 40–45, 2019, doi: 10.1109/ICOASE.2019.8723673.

[15] M. R. Dhobale, "Smart Home Security System using Iot , Face Recognition and Raspberry Pi," no. April, pp. 44–47, 2020, doi: 10.5120/ijca2020920105.

[16] N. Tkauc, T. Tran, K. Hernandez-Diaz, and F. Alonso-Fernandez, "Cloud-Based Face and Speech Recognition for Access Control Applications," *2020 IEEE Conf. Commun. Netw. Secur. CNS 2020*, pp. 2–9, 2020, doi: 10.1109/CNS48642.2020.9162165.

[17] Y. Findawati, A. Idris, Suprianto, Y. Rachmawati, and E. A. Suprayitno, "IoT-Based Smart Home Controller Using NodeMCU Lua V3 Microcontroller and Telegram Chat Application," *IOP Conf. Ser. Mater. Sci. Eng.*, vol. 874, no. 1, 2020, doi: 10.1088/1757-899X/874/1/012009.

[18] R. R. Hariadi, A. Yuniarti, I. Kuswardayan, D. Herumurti, S. Arifiani, and A. A. Yunanto, "Termo: Smart air conditioner controller integrated with temperature and humidity sensor," *Proc. 2019 Int. Conf. Inf. Commun. Technol. Syst. ICTS 2019*, pp. 312–315, 2019, doi: 10.1109/ICTS.2019.8850953.

[19] Tonage Suraj and D. Phillips, "IoT Based Home Automation using NODE MCU ESP8266," vol. 8, no. 5, p. 589, 2018.

[20] S. C. Madhu B R, Vaishnavi K R, Dushyanth N Gowda, Tushar Jain, "IoT Based Home Automation System over Cloud," *Int. J. Trend Sci. Res. Dev.*, vol. Volume-3, no. Issue-4, pp. 966–968, 2019, doi: 10.31142/ijtsrd24005.

[21] H. Yar and M. S. and Z. K. , Ali Shariq Imran , Zulfiqar Ahmad Khan, "Towards Smart Home Automation Using IoT-Enabled Edge-Computing Paradigm," *sensors Artic.*, 2021.

[22] M. Mrinal, L. Priyanka, M. Saniya, K. Poonam, and A. B. Gavali, "Smart home - Automation and security system based on sensing mechanism," *Proc. 2017 2nd IEEE Int. Conf. Electr. Comput. Commun. Technol. ICECCT 2017*, pp. 1–3, 2017, doi: 10.1109/ICECCT.2017.8117986.

[23] A. HAYES, "https://www.investopedia.com/terms/s/smart-home.asp," 2022.

[24] D. N. Gujarati and D. C. Porter, *Essentials of CLOUD COMPUTING*, no. March. 2015.

[25] A. Sether and C. Computing, "Running head : CLOUD COMPUTING BENEFITS," no. June, p. 20, 2016, doi: 10.13140/RG.2.1.1776.0880.

[26] M. Z. M. E. P. M. · C. Rong, *Cloud Computing and Big Data: Technologies, Applications and Security*, vol. 49, no. September 2018. 2019.

[Online]. Available: http://link.springer.com/10.1007/978-3-319-97719-5

[27] H. Sabireen and V. Neelanarayanan, “A Review on Fog Computing: Architecture, Fog with IoT, Algorithms and Research Challenges,” *ICT Express*, vol. 7, no. 2, pp. 162–176, 2021, doi: 10.1016/j.icte.2021.05.004.

[28] ed. Mahmood, Zaigham, *Fog computing: concepts, frameworks and technologies.Springer*. 2018. doi: 10.1002/9781119720430.ch8.

[29] M. Rahimi, M. Songhorabadi, and M. H. Kashani, “Fog-based smart homes : A systematic review,” pp. 1–37.

[30] J. Salazar, *WIRELESS NETWORKS*, 1st Editio. Technicka 2, Prague 6, Czech Republic: Czech Technical University of Prague Faculty of electrical engineering, 2017.

[31] RABBIT, “An Introduction to Wi-Fi,” *Digi Int. corp, USA*, pp. 1–74, 2008, [Online]. Available: http://ftp1.digi.com/support/documentation/0190170_b.pdf

[32] A. Engineering, W. Communication, and B. Unit, “The Wi-Fi Evolution,” no. March 2020, pp. 1–6.

[33] and L. V. Cirani, Simone, Gianluigi Ferrari, Marco Picone, *Internet of Things Architectures, Protocols and Standards. John Wiley & Sons*, vol. 7, no. 2. 2018.

[34] Q. F. Hassan, “Internet of things A to Z: technologies and applications,” *John Wiley Sons*, 2018.

[35] D. Happ and A. Wolisz, “Towards gateway to Cloud offloading in IoT publish/subscribe systems,” *2017 2nd Int. Conf. Fog Mob. Edge Comput. FMEC 2017*, pp. 101–106, 2017, doi: 10.1109/FMEC.2017.7946415.

[36] B. Zhang *et al.*, “The cloud is not enough: Saving IoT from the cloud,” *7th USENIX Work. Hot Top. Cloud Comput. HotCloud 2015*, 2015.

[37] F. Luis and G. Moncayo, *A Hands-On Course in Sensors Using the Arduino and Raspberry Pi*. 2018.

[38] T. Islam, *Advanced interfacing techniques for the capacitive sensors*, vol.

25. 2017. doi: 10.1007/978-3-319-55369-6_2.

[39] B. Davidovic and A. Labus, “A smart home system based on sensor technology,” no. February, 2017, doi: 10.2298/FUEE1603451D.

[40] Deeksha Srivastava, Awanish Kesarwani, and Shivani Dubey, “Measurement of Temperature and Humidity by using Arduino Tool and DHT11 Measurement of Temperature and Humidity by using Arduino Tool and DHT11,” *Int. Res. J. Eng. Technol.*, vol. 876, pp. 876–878, 2018, [Online]. Available: www.irjet.net

[41] W. Hasan, “Design and Implementation Smart Transformer based on IoT,” no. December, 2019, doi: 10.1109/iCCECE46942.2019.8941980.

[42] I. A. Id, M. Umer, R. Majeed, A. Mehmood, and W. A. Id, “Home automation using general purpose household electric appliances with Raspberry Pi and commercial smartphone,” pp. 1–20, 2020, doi: 10.1371/journal.pone.0238480.

[43] M. Mahbub, “Toxic and hazardous gas detection , measurement and monitoring system for safety assurance in home and industrial application of wireless sensor node,” vol. 1, no. July, pp. 89–98, 2019, doi: 10.15413/etr.2019.0108.

[44] T. Mudawi, “IoT-HASS : A Framework For Protecting Smart Home Environment IOT-HASS : A FRAMEWORK FOR PROTECTING SMART HOME ENVIRONMENT,” 2020.

[45] I. Mashal and A. Shuhaiber, “What makes Jordanian residents buy smart home devices?,” *Kybernetes*, vol. 48, no. 8, pp. 1681–1698, Jan. 2019, doi: 10.1108/K-01-2018-0008.

[46] H. M. Marhoon, M. I. Mahdi, E. D. Hussein, and A. R. Ibrahim, “Designing and Implementing Applications of Smart Home Appliances,” *Mod. Appl. Sci.*, vol. 12, no. 12, p. 8, 2018, doi: 10.5539/mas.v12n12p8.

[47] P. Gupta and J. Chhabra, “IoT based Smart Home design using power and security management,” *2016 1st Int. Conf. Innov. Challenges Cyber Secur.*

ICICCS 2016, no. February 2016, pp. 6–10, 2016, doi: 10.1109/ICICCS.2016.7542317.

[48] E. Ilie-zudor, Z. Kemény, P. Egri, and L. Monostori, “the Rfid Technology and Its Current Applications,” no. May, pp. 29–36, 2006, [Online]. Available: http://igor.xen.emi.sztaki.hu/~zudor/Publications/RFID_technology and applications.pdf

[49] Z. Meng and Z. Li, “RFID Tag as a Sensor - A Review on the Innovative Designs and Applications RFID Tag as a Sensor - A Review on the Innovative Designs and Applications,” no. September 2019, 2016, doi: 10.1515/msr-2016-0039.

[50] L. Patrono, *RFID Technologies & Internet of Things*, vol. 9, no. 1. 2013. doi: 10.24138/jcomss.v9i1.152.

[51] Z. Meng and Z. Li, “RFID Tag as a Sensor - A Review on the Innovative Designs and Applications,” *Meas. Sci. Rev.*, vol. 16, no. 6, pp. 305–315, 2016, doi: 10.1515/msr-2016-0039.

[52] Patel, *RFID Design Fundamentals and Applications*. 2019.

[53] J. G. Kolo, E. Dogo, and O. O. Mikail, “Development of Secure RFID Authentication System for Electronic Inter- Campus Transportation Billing,” no. December, 2017.

[54] A. B. R. Apratim Halder, “Ultrasonic Sensor Based Smart Fan,” *Int. J. Adv. Res. Electr. Electron. Instrum. Eng.*, vol. 04, no. 07, pp. 5837–5843, 2015, doi: 10.15662/ijareeie.2015.0407005.

[55] P. Cholasta, “S12ZVL LIN Enabled Ultrasonic Distance Measurement Based on the MC9S12ZVL32 MagniV Device,” pp. 1–26, 2014.

[56] Asit Kumar Datta, *Face Detection and Recognition Theory and Practice*. 2016.

[57] J. Nussey, *Arduino ® 2nd Edition*. 2018. [Online]. Available: http://www.wiley.com/go/permissions.

[58] and L. V. Cirani, Simone, Gianluigi Ferrari, Marco Picone, “Internet of Things Architectures, Protocols and Standards,” *Gastron. ecuatoriana y Tur. local.*, vol. 1, no. 69, pp. 5–24, 2018.

[59] “https://components101.com/microcontrollers/arduino-uno”.

[60] H. T. Sihotang, S. Efendi, E. M. Zamzami, and H. Mawengkang, “Design and Implementation of Rivest Shamir Adleman’s (RSA) Cryptography Algorithm in Text File Data Security,” *J. Phys. Conf. Ser.*, vol. 1641, no. 1, 2020, doi: 10.1088/1742-6596/1641/1/012042.

[61] S. S. Pawar, V. Kithani, S. Ahuja, “Smart Home Security using IoT and Face Recognition,” *Fourth Int. Conf. Comput. Commun. Control Autom. (ICCUBEA), IEEE, Pune, India, 2018, pp. 1-6.%0B %0B*, 2018.

[62] T. S. Gunawan, M. Hamdan, H. Gani, F. Diyana, A. Rahman, and M. Kartiwi, “Development of Face Recognition on Raspberry Pi for Security Enhancement of Smart Home System,” vol. 5, no. 4, pp. 317–325, 2017, doi: 10.11591/ijeei.v5i4.361.

[63] M. R. Dhobale, “Smart Home Security System using Iot , Face Recognition and Raspberry Pi,” vol. 176, no. 13, pp. 45–47, 2020.

[64] K. M. Mohi Uddin, S. Afrin Shahela, N. Rahman, R. Mostafiz, and M. M. Rahman, “Smart Home Security Using Facial Authentication and Mobile Application,” *Int. J. Wirel. Microw. Technol.*, vol. 12, no. 2, pp. 40–50, 2022, doi: 10.5815/ijwmt.2022.02.04.

Appendices

Appendix A

Uno Wi-Fi R3 AtMega328p+NodeMCU ESP8266 capacity 8 Megabyte Memory USB-TTL CH340G

Specifications

Microcontroller	ATmega328
IC Wi-Fi	ESP8266
USB-TTL converter	CH340G
Power Out	5V-800mA
Power IN. USB	5V (500mA max.)
Power IN. VIN/DC Jack	9-24V
Power Consumption	5V 800mA
Logic Level	5V
Wifi	Wi-Fi 802.11 b/g/n 2.4 GHz
USB	Micro USB
Clock Frequency	16MHz
Operating Supply Voltage	5V
Digital I/O	14
Analog I/O	6
Memory Size	32Mb
Interface Type	serial\OTA
Operating temperature	−40C°/+125C°
Length×Width	53.34×68.58mm
Weight	8
antenna	Buil-in\external antenna

A-1

	1	2	3	4	5	6	7	8
CH340 connect to ESP8266 (upload sketch)	OFF	OFF	OFF	OFF	ON	ON	ON	NoUSE
CH340 connect to ESP8266 (connect)	OFF	OFF	OFF	OFF	ON	ON	OFF	NoUSE
CH340 connect to ATmega328 (upload sketch)	OFF	OFF	ON	ON	OFF	OFF	OFF	NoUSE
Mega328+ESP8266	ON	ON	OFF	OFF	OFF	OFF	OFF	NoUSE
All modules work independent	OFF	OFF	OFF	OFF	OFF	OFF	OFF	NoUSE

After choosing the mode of the board can proceed to setting up the IDE

It is important that when the ESP8266 module is programming, it is necessary to press the button "ESP Reboot"

A-2

Appendix B

USB-Webcam RAPOO C200

Main features:

1. 720P full HD;

It adopts high-definition photosensitive chip, with 5-layer coating lens, supports 1280*720 resolution, and the maximum frame rate is 30 frames.

2. 100° wide-angle viewing angle;

3. Omnidirectional dual noise reduction microphone;

It can receive a range of about 3 meters, and the call is clear and stable.

4. 360° horizontal rotation;

It can be rotated 360° horizontally, and the upper and lower viewing angles can be adjusted freely within a specific angle to meet different framing compositions.

5. Adjustable base;

Adapt to various sizes of monitors, can be placed flat or hung, can also be equipped with a tripod (this product does not include a tripod)

6. Support multiple systems and platforms

Windows 7/8/10 or higher, Mac OS X 10.6 or higher, Chrome OS, Android 5.0 or higher

Package Including

1 * Webcam (Comes with original box)

1 * User Manual

1 * USB

B

Appendix C

Fluke 59 MAX/59 MAX+

FLUKE.

Fluke 59 MAX/59 MAX+ Infrared Thermometer

Fits your budget. Fits your job.

With 65 years of expertise as the leader in the test tools industry, Fluke has built the 59 MAX and 59 MAX+ IR thermometers with the precision you need to do your job accurately and within your budget. Designed to withstand a 1 meter drop, you can count on these lightweight, compact IR thermometers to work when you need them.

Technical Data

Product highlights

- Precise laser technology for more accurate and repeatable measurements
- Large, easy-to-read backlit LCD display for easy viewing
- Small and lightweight design fits easily fits into your tool box
- IP40 rated for extra protection
- 10:1 Distance to Spot ratio, 59 MAX+ (8:1 Distance to Spot ratio, 59 MAX)
- Displays the minimum, maximum or average temperature, or the difference between two measurements
- Hi and Lo alarms for rapid display of measurements outside the limits
- Powered by one (1) AA battery
- One year warranty

FLUKE®

Specifications

	59 MAX		59 MAX+	
Temperature range	-30 °C to 350 °C (-22 °F to 662 °F)		-30 °C to 500 °C (-22 °F to 932 °F)	
Accuracy (Calibration geometry with ambient temperature 23 °C ±2 °C)	≥ 0 °C:	± 2.0 °C or ± 2.0 % of reading, whichever is greater	≥ 0 °C:	± 1.5 °C or ± 1.5 % of reading, whichever is greater
	≥ -10 °C to <0 °C:	± 2.0 °C	≥ -10 °C to <0 °C:	± 2.0 °C
	< -10 °C:	± 3.0 °C	< -10 °C:	± 3.0 °C
	≥ 32 °F:	± 4.0 °F or ± 2.0 % of reading, whichever is greater	≥ 32 °F:	± 3.0 °F or ± 1.5 % of reading, whichever is greater
	≥ 14 °F to <32 °F:	± 4.0 °F	≥14 °F to <32 °F:	± 4.0 °F
	< 14 °F:	± 6.0 °F	<14 °F:	± 6.0 °F
Response rime (95 %)	< 500 ms (95 % of reading)		< 500 ms (95 % of reading)	
Spectral response	8 µm to 14 µm			
Emissivity	0.10 to 1.00			
Distance to spot ratio	8:1 (calculated at 90 % energy)		10:1 (calculated at 90 % energy)	
Display resolution	0.1 °C (0.2 °F)			
Repeatability (% of reading)	± 1.0 % of reading or ± 1.0 °C (±2.0 °F), whichever is greater		±0.8 % of reading or ±1.0 °C (±2.0 °F), whichever is greater	
General specifications				
Power	1 AA IEC LR06 Battery			
Batter life	12 hours with laser and backlight on			
Weight	220 g (7.76 oz)			
Size	(156 x 80 x 50) mm (6.14 x 3.15 x 2) inches			
Operating temperature	0 °C to 50 °C (32 °F to 122 °F)			
Storage temperature	-20 °C to +60 °C (-4 °F to 140 °F), (without battery)			
Operating humidity	10 % to 90 % RH non-condensing @ 30 °C (86 °F)			
Operating altitude	2000 meters above mean sea level			
Storage altitude	12,000 meters above mean sea level			
Drop test	1 m			
Safety specifications				
Ingress protection rating	IP40 per IEC 60529			
Vibration and shock	IEC 68-2-6 2.5 g, 10 to 200 Hz, IEC 68-2-27, 50 g, 11 ms			
Compliance	EN/IEC 61010-1			
Laser safety	FDA and EN 60825-1 Class II			
Electromagnetic compatibility	61326-1 EN 61326-2			

C-2

Appendix D

D-1. Environment System:

```
#include <MQ2.h>
int Analog_Input = 1;
int lpg, co, smoke;

MQ2 mq2(Analog_Input);

#include "DHT.h"
#define DHTPIN 8
#define DHTTYPE DHT11   // DHT 11
DHT dht(DHTPIN, DHTTYPE);

int pirPin = 7;
int pirStat = 0;
int countt = 0;

#define echoPin 2
#define trigPin 3
#define echoPin2 4
#define trigPin2 5
long duration;
int distance;

long duration2;
int distance2;

void setup() {
  pinMode(trigPin, OUTPUT);
```

```
  pinMode(echoPin, INPUT);
  pinMode(trigPin2, OUTPUT);
  pinMode(echoPin2, INPUT);
  pinMode(12, OUTPUT);
  Serial.begin(9600);
  dht.begin();
  pinMode(pirPin, INPUT);
  pinMode(9, OUTPUT);
  pinMode(10, OUTPUT);
  pinMode(6, OUTPUT);
  mq2.begin();
  digitalWrite(9, HIGH);
  digitalWrite(10, HIGH);
digitalWrite(6, HIGH);



}
String str = "";
void loop() {
  str = "";
  delay(100);

  digitalWrite(trigPin, LOW);
  delayMicroseconds(2);
  digitalWrite(trigPin, HIGH);
  delayMicroseconds(10);
  digitalWrite(trigPin, LOW);
  duration = pulseIn(echoPin, HIGH);
  distance = duration * 0.034 / 2;
```

```
str += (distance);
str += (",");


digitalWrite(trigPin2, LOW);
delayMicroseconds(2);
digitalWrite(trigPin2, HIGH);
delayMicroseconds(10);
digitalWrite(trigPin2, LOW);
duration2 = pulseIn(echoPin2, HIGH);
distance2 = duration2 * 0.034 / 2;
str += (distance2);
str += (",");

float h = dht.readHumidity();
float t = dht.readTemperature();
float f = dht.readTemperature(true);
float hif = dht.computeHeatIndex(f, h);
float hic = dht.computeHeatIndex(t, h, false);
str += (h);  str += (",");
str += (t); str += (",");
pirStat = digitalRead(pirPin);


if (pirStat == HIGH) {
  str += ("1"); str += (",");
  countt = 0;
}
else {
```

```
  str += ("0"); str += (",");
  countt = countt + 1;
 }
 if (t > 32 | h > 70 ) {
  digitalWrite(10, LOW);
 }
 else if (t < 30 && h <60) {
  digitalWrite(10, HIGH);
 }

 if (t <16 ) {
  digitalWrite(6, LOW);
 }
 else if (t >25

 ) {
  digitalWrite(6, HIGH);
 }
 float* values = mq2.read(false); //set it false if you don't want to print the values in the Serial
 lpg = mq2.readLPG();
 co = mq2.readCO();
 smoke = mq2.readSmoke();

 if ( lpg > 1000 | co > 1000 | smoke > 1000) {
  digitalWrite(9, LOW);
 }
 else {
  digitalWrite(9, HIGH);
```

```
  }

  str += (lpg);  str += (",");
  str += (co); str += (",");
  str += (smoke);
  Serial.println(str);

  if (distance < 20 | distance2 < 20)
  {
    for (int i = 0; i <= 10; i += 1)
    {
      digitalWrite(12, HIGH);
      delay (100);
      digitalWrite(12, LOW);
      delay (100);
    }
  }
}
```

D-2. RFID System

```
#include <SPI.h>
#include <MFRC522.h>
#define SS_PIN 10
#define RST_PIN 9

const int ledPin =  2;
const int buttonPin = 3;
int buttonState = 0;
MFRC522 mfrc522(SS_PIN, RST_PIN);   // Create MFRC522 instance.
unsigned long code = 000;
void setup() {
  Serial.begin(9600); // Initialize serial communications with the PC
  SPI.begin();           // Init SPI bus
  mfrc522.PCD_Init(); // Init MFRC522 card
  pinMode(ledPin , OUTPUT);
  pinMode(buttonPin, INPUT);
  pinMode(4 , OUTPUT);
  pinMode(5 , OUTPUT);
  digitalWrite(4, HIGH);
  digitalWrite(5, HIGH);



}

void loop() {
  if (Serial.available()) {
    String val = Serial.readString();
```

```
  if (val == "1") {
    digitalWrite(4, LOW);
    delay (2000);
    digitalWrite(4, HIGH);
  }
  else if (val == "2") {
    digitalWrite(5, LOW);
    delay (2000);
    digitalWrite(5, HIGH);
  }
}



if (mfrc522.PICC_IsNewCardPresent()) {
  unsigned long uid = getID();
  code = uid;
}
else {
  code = 0;
}




buttonState = digitalRead(buttonPin);
if (buttonState == HIGH) {
  // turn LED on:
  digitalWrite(ledPin, HIGH);
```

```
    Serial.println(String(code) +','+ String(1));

  } else {
    // turn LED off:
    digitalWrite(ledPin, LOW);
    Serial.println(String(code) +','+ String(0));
  }


if (code == 4294967295 | code == 4294955029) {
  digitalWrite(4, LOW);
  delay (5000);
  digitalWrite(4, HIGH);

}
else if (code == 21411)
{
  for (int i=1 ; i<30 ; i++)
  {
  digitalWrite(ledPin, HIGH);
  delay (80);
  digitalWrite(ledPin, LOW);
  delay(80);
    }

  }
delay (500);

}
```

```
unsigned long getID() {
  if ( ! mfrc522.PICC_ReadCardSerial()) { //Since a PICC placed get Serial and continue
    return -1;
  }
  unsigned long hex_num;
  hex_num =  mfrc522.uid.uidByte[0] << 24;
  hex_num += mfrc522.uid.uidByte[1] << 16;
  hex_num += mfrc522.uid.uidByte[2] <<  8;
  hex_num += mfrc522.uid.uidByte[3];
  mfrc522.PICC_HaltA(); // Stop reading
  return hex_num;
}
```

الخلاصة

تعد أتمتة المنزل الذكي أحد الموضوعات الرئيسية في هذا العصر والتي جذبت انتباه الباحثين لعدة سنوات. تساهم أتمتة المنزل الذكي في تحقيق العديد من القدرات، والتي كان لها تأثير حقيقي على حياتنا اليومية. نسعى في جميع جوانب حياتنا إلى الراحة وكذلك توفير الوقت والجهد لذلك بدأ الناس في البحث عن الراحة والأمان والحماية من الحوادث والكوارث بأقل خسارة ممكنة وبما أن المنازل هي مكان للراحة، فقد بدأ المختصون باستغلال الثورات التكنولوجية والعلمية في هذا الصدد. عندما بدأ عصر الأتمتة والإنترنت وإنترنت الأشياء، كانت المنازل الذكية تتطور وتنمو لتشمل العديد من الميزات المهمة التي ساعدت كثيرًا في توفير الطاقة، وخلق بيئة جيدة، ومنع الحرائق وتسرب الغازات السامة، والحفاظ على المنزل آمنًا.

يشتمل النظام المقترح، الذي تم تصميمه وتنفيذه عمليًا، على عدد من الجوانب المهمة والحيوية للمنازل الذكية. ركز النظام أولاً على أمن المنزل، وهو أحد أهم هذه الجوانب. تم بذل العديد من الجهود في البحث والمقالات التي تركز على هذا المجال بسبب زيادة معدل الجريمة والسرقة. يهدف النظام المقترح إلى بناء منزل ذكي يتحكم ويراقب جميع مداخل المنزل التي غالبًا ما تكون عرضة للتسلل من قبل اللصوص. يعتمد نظامنا على التعريف الشخصي باستخدام تقنية اكتشاف الوجه والتعرف عليه، بالإضافة إلى استخدام تقنية تحديد ترددات الراديو (RFID) كآلية لتحسين أداء أنظمة الأمن المنزلي. يقوم الخادم السحابية بتحليل هوية العضو المستلمة لاسترداد تصريح الدخول إلى المنزل. كان النظام فعالاً وسريع الاستجابة في نقل لقطات حية لأي نشاط تدخلي غير قانوني عند باب أو نوافذ المنزل. تمت إضافة العديد من الميزات لتحقيق مراقبة وتحكم سلس في هذا المجال.

نهج آخر تم تنفيذه في نظام أتمتة المنزل الذكي المقترح هو اكتشاف أي تسرب للغازات أو الدخان أو الحرائق مع تحذير مسبق عبر تطبيق التلكرام عند اكتشاف أي خطر. آلية أخرى تحقق المناخ المناسب للمنزل وتقلل من استهلاك الطاقة. يمكن لصاحب المنزل أيضًا التحكم في الأجهزة المنزلية عن بُعد من خلال واجهة مستخدم سهلة الاستخدام والوصول إليها في أي مكان. تم بناء النظام المقترح باستخدام جهاز استشعار لاكتشاف الحرائق والغازات السامة والدخان. جهاز آخر يقيس درجة الحرارة والرطوبة ويتحكم في تشغيل أنظمة التبريد والتدفئة بناءً على القيمة المحددة لتشغيل / إيقاف تشغيل كل منها، مع مستشعر حركة يضمن عدم عمل أي من هذه الأجهزة عندما يكون المنزل فارغًا. تمت إضافة قيمتين حديتين لتجنب تشغيل وإيقاف تشغيل الآلات بشكل مستمر عندما تتقلب درجة الحرارة عند قيمة معينة. ترتبط هذه المستشعرات أيضًا بمتحكم صغير مفتوح المصدر ينقل البيانات والقيم عبر Wi-Fi إلى السحابة، ثم يعرض النتائج المهمة لمالك المنزل.

مع نمو وتوسع مفهوم المنازل الذكية يأتي مقدار المعلومات المنقولة ونقاط الضعف في أمن المعلومات واضطرابات وقت الاستجابة لذلك تم استخدام بنية حوسبة الضباب في المنازل الذكية كوسيط بين أجهزة إنترنت الأشياء والخوادم السحابية لتقليل زمن الوصول وتخزين البيانات والحفاظ على أمن المعلومات. تسمح تقنية حوسبة الضباب لصاحب المنزل بمراقبة النظام والتحكم فيه من داخل المنزل باستخدام واجهة المستخدم الموجودة على كمبيوتر الوسيط، ويمكن أيضًا التحكم فيه ومراقبته من أي مكان باستخدام واجهة المستخدم الرسومية.

جمهوريه العراق

وزارة التعليم العالي والبحث العلمي

جامعـــــه بابـــــــل

كلية الهندسه/ قسم الهندسه الكهربائية

تنفيذ كفوء لنظام اتمتة منزل ذكي يعتمد على الحوسبة السحابية

رسالة

مقدمة الى كلية الهندسة/ جامعة بابل

كجزء من متطلبات نيل درجة الماجستير

في الهندسة/ الهندسة الكهربائية/اتصالات

من قبل

أنور ستار حمزة هادي

أشراف

أ. د ليث علي عبد الرحيم

1444 هـ

2022 مـ