DESIGN AND DEVELOPMENT OF AN IoT-BASED FACE RECOGNITION SMART ACCESS CONTROL SYSTEM

By
NNAJIOFOR GEORGE ANAYO (B.Eng)

Reg No: 20204251918

Option: COMMUNICATION

SUPERVISORS:

Engr. Dr. C. K. Agubor

Engr. Dr. L.S. Ezema

SUBMITTED TO

DEPARTMENT OF ELECTRICAL AND ELECTRONIC ENGINEERING

POSTGRADUATE SCHOOL OF ENGINEERING AND ENGINEERING TECHNOLOGY, FUTO

IN A PARTIAL FULFILMENT OF THE REQUIREMENTS FOR THE AWARD OF MASTERS OF ENGINEERING (M.ENG)

APRIL 2025

CERTIFICATION

This is to certify that **"Design and Development of An IoT-Based Face Recognition Smart Access Control System"** is original work done by **NNAJIOFOR GEORGE ANAYO (20204251918)** under the supervisions of **Engr. Dr. C. K. Agubor and Engr. Dr. L.S. Ezema,** presented to the Department of Electrical and Electronic Engineering, Federal University of Technology, Owerri, Imo State, Nigeria in fulfillment for the award of the degree, Masters of Engineering (M.Eng) in Electronic Engineering.

..... Date 29/7/24.....

Engr. Dr. C. K. Agubor
(Supervisor I)

..... Date 29/7/24.....

Engr. Dr. L.S. Ezema
(Supervisor II)

..... Date 29/7/24.....

Engr. Dr. N. Chukwuchekwa
(Head of Department.)

..... Date .....

Engr. Prof. M.C. Ndinechi
(Dean, School of Electrical Systems Engineering and Technology)

..... Date .....

Prof. B.O. Esonu
(Dean, School of Postgraduate Studies)

..... Date .....

(External Examiner)

ii

DEDICATION

This work is dedicated to Almighty God for His assistance.

ACKNOWLEDGEMENTS

With a grateful heart, I want to seize this opportunity to express my unalloyed gratitude to my Supervisors, Engr. Dr. C. K. Agubor and Engr. Dr. L.S. Ezema for their supports so far. Also, I appreciate the contributions of my lecturers, Engr. Prof. G.A. Chukwudebe, Engr. Prof. E.N.C. Okafor, Engr. Prof. M.C. Ndinechi, Engr. Prof. (Mrs) G.N. Ezeh, Engr. Prof. D.O. Dike, Engr. Prof. (Mrs) I.E. Achumba. Engr. Prof. L.O. Uzoechi, Engr. Prof J.O. Onojo, Engr. Dr. O.C. Nosiri, Engr. Dr. M. Olubiwe, Engr. Dr. I.O. Akwukwaegbu, Engr. Dr. S.O. Okozi, Engr. Dr. Akande and Engr. E. Ugwueze. Finally, I extend my thanks to my family members and well-wishers.

Table of Contents

LIST OF TABLES

LIST OF FIGURES

LIST OF PLATE

ABSTRACT

This thesis presents a smart IoT-based face recognition access control system. Initially, users must enter a password. If the password is correct, the door unlocks automatically; if incorrect, the system triggers an alarm, captures images of the user, and sends a security alert with the photos to the rightful owner via the Telegram application. The system captures the intruder's face and denies access to unauthorized users if the captured face does not match the stored one. It allows authorized users to enter and exit restricted areas and features real-time image capture and transmission of the intruder's photos.

Methodology: The system uses face recognition technology with an ESP32 camera module connected to a solenoid lock via a DC relay. A 4x4 keypad was linked to the microcontroller for password entry. The ESP32 camera was integrated with the owner's Telegram account. The system connects to a network through a router or phone hotspot, providing global accessibility.

Results: A functional prototype was developed, implemented, and tested in real-time, successfully sending intruder photos when incorrect passwords were entered. This system significantly enhances security by accurately identifying individuals based on unique facial features, reducing the risk of unauthorized access through stolen keys, access cards, or PIN codes, thus improving security for homes, offices, and other facilities.

Keywords:

ESP32 Camera, IoT, RSSI, Arduino IDE, Solenoid lock, MATLAB, Telegram application, Keypad, Password, WiFi.

CHAPTER ONE

INTRODUCTION

1.0 BACKGROUND OF STUDY

Due to the prevalence of insecurity in our society today, and the rate of unwanted intrusion into restricted areas the need for a trusted security system is required in various aspects of our lives. One of such is the use of a smart access control system with automatic picture capturing and notification of intruders. For the security of lives and organisation properties, it is essential to control and monitor how homes and offices are accessed, security is the life wire of all organisations and guarantees the sustainability of any organization. Automatic monitoring and capturing of images of personnel in an access control system is very vital for proper notification of unwanted intruders who try to gain access illegally (Mukhtar, 2021).

Safety and security are the most challenging issues in modern time society, to prevent people's lives and their valuable assets from illegal handling. As a result, safety and security extend to personal social security to protect every individual's personal information, valuable things, and their day-to-day activities. Hence, personal security services are moving towards the integration of video surveillance, and door locks access control systems based on authorization information to avoid access conflicts in personalized monitored areas.

A smart access control system is a system that automates entry and exits into apartments, companies, business premises, offices, units, and amenities. Instead of a physical key, clients, employers or staff can use a key fob, code, the user's smartphone or even biometrics to unlock the usual units and access amenities or common areas(Postulka, 2019). It is a control system that identifies, authenticate and authorizes users and entities by checking required login credentials before permitting access to a restricted area or premises.

In view of proper identification and profiling of individuals or persons that can access a controlled area, there is a need for an automatic picture-capturing devices or cameras that automatically takes images of the person that wants to gain access into the restricted area. An automatic picture capturing which operates on a VLC technology camera is incorporated in the smart access control system for adequate profiling of personnel that can be allowed or permitted to have access or exit the secured area(G. C. Manjunath et al., 2022).

To have an effective access monitoring or control system, the need for proper notifications or feedback to the main system when an individual wants to access the restricted area is inevitable. This notification can come in the form of messages to the system server like beeps or alarms to notify the operators that someone wants to gain access to the secured area, either legally or illegally.

It is a feedback system to maintain checks and balances of the system. Notifications are a core function of current smart devices. They inform users about a variety of events, in this case about the intruder (Dominik Weber and Niels Henze, 2015).

Intrusion detection is the process of examining the events occurring in a computer system or network and analyzing them for signs of possible incidents, which are violations or about to happen threats of violation of computer security policies or standard security practices. An intrusion detection system (IDS) is software that automates the intrusion detection process. Intrusion prevention is the process of performing intrusion detection and attempting to stop detected possible incidents(Salikhov et al., 2021).

Password security is a crucial aspect of protecting personal information and preventing unauthorized access to sensitive data. With the increase in digitalization and the prevalence of online platforms, ensuring strong password security has become more important than ever. WiFi Card is a popular microcontroller board widely used in various electronic thesis, including security systems. It provides a versatile platform for implementing password-based security systems due to its ease of use,

affordability, and compatibility with various components. A password security system using a Wi-Fi Card can be used in numerous applications, such as home security, access control, and data protection. By combining a keypad for input and a servo motor for mechanical locking/unlocking mechanisms, the Wi-Fi Cardboard can detect and authenticate passwords, granting access or denying entry based on the input. Some potential areas of research and exploration in this study included:

a. **Password encryption:** Investigating different encryption algorithms and techniques to ensure the password is securely stored and transmitted within the system.

b. **User authentication methods:** Exploring various techniques for user authentication, such as biometric authentication (fingerprint, facial recognition) or two-factor authentication (using a combination of passwords and physical tokens).

c. **Brute-force and dictionary attack prevention:** Examining ways to protect the system from brute-force attacks or dictionary-based password cracking attempts.

d. **System robustness**: Investigating the system's ability to handle potential threats or vulnerabilities, such as input spoofing, tampering, or physical attacks. By conducting a study on password security systems using Wi-Fi cards, researchers can contribute to the development of more secure and reliable access control systems in both residential and commercial settings. The findings of such a study can help advance the field of security systems and improve the protection of personal information and assets.

1.1 STATEMENT OF THE PROBLEM

There is a need for tighter security measures in access control systems to prevent unauthorized access and ensure that only authorized individuals can enter restricted areas. In high-security environments, such as government facilities or data centers, the current access control system Radio Frequency Identification (RFID) not provide sufficient authentication methods to ensure the identity of individuals entering the premises. The integration of access control systems with other security systems, such as video surveillance or alarms or photo capture and notification, is limited or non-existent. This lack of integration hampers the ability to respond quickly to security incidents or identify potential threats.

The current IP camera system's lack of intelligent video analytics hampers its ability to detect and alert security personnel to suspicious activities or potential security threats in real-time. Poor integration between the IP camera system and other security systems, such as access control or alarms, limits the effectiveness of surveillance and incident response efforts. The current IP camera system may lack encryption and secure transmission protocols, making it vulnerable to unauthorized access and video stream interception, compromising the privacy and security of recorded footage.

1.2 OBJECTIVES OF THE STUDY

The main objective of this study is to design and develop an IoT-based face recognition smart access control system (IFRSACS). The specific objectives are to:

i. develop and implement a system that permits authorized persons to enter and exit; and deny entry to unauthorized persons into restricted areas.

ii. implement a smart system capable of capturing real-time picture and notify security personnel any attempt to gain unauthorized access into restricted areas

iii. implement a digital and editable password input panel that can automatically trigger a digital camera by the system algorithm using C++ programming language.

iv. implement a rechargeable battery circuitry to keep the system active at all times.

1.3 SIGNIFICANCE OF THE STUDY

This work plays a crucial role in maintaining the security of restricted places, assets, and information. It prevents unauthorized access and protects against security breaches. This knowledge is especially important in nowadays society, where crimes are at alarming rates. It Mitigates or reduces the risk of unauthorized access, theft, sabotage, and other security incidents.

The study of a "Face Recognition Door Lock Access Control System" holds significant importance for several reasons, reflecting advancements in technology, security, and convenience. Here are some key points highlighting its significance:

1.4 SCOPE OF STUDY

This thesis is limited to access control system operations using ESP32 Camera and a solenoid lock. It captures the photo of the user and compares it with the ones in the program and validate its authenticity before requesting for the second security check using a password keyed. If the access credentials provided the user matches with the programmed faces and password, it grants access to the user. The system uses WiFi network and be affected negatively especially in areas with poor network coverage. And this can be a huge limitation in terms of sending the intruder’s picture notification to the office owner.

CHAPTER TWO

LITERATURE REVIEW

2.1 General Overview

This chapter attempts to read, identify, locate, and evaluate previous studies, observations, opinions, comments, suggestions, and recommendations on the topic under study. It is intended to provide the researcher with a good date knowledge of the research topic. For the design and realization of a smart access control system, many technologies have been developed. In this chapter, different concepts of access control system technologies are reviewed.

2.2 Empirical Review

This study investigates users' behavior in password utilization. Good password practices are critical to the security of any information system. End users often use weak passwords that are short, simple, and based on personal and meaningful information that can be easily guessed. User ID and Password (Salikhov et al., 2021) First, users are either assigned an ID or are given the chance to create one. Once the ID has been created, the user chooses a password. The password should be secret and shared only between the user and the information systems or computer. Users should not disclose their passwords or write them down. 1.2 Log-on(Salikhov et al., 2021). During the login process, users must enter both their user IDs and passwords. The system then processes and compares the ID and password with what is stored in the database. If the user ID and password match, the user will be granted access to the system. If the user ID and password do not match, the user will not be allowed access.

2.2.1 Access Control:

Access control is a security technique that regulates who or what can view or use resources in a computing environment. It is a fundamental concept in security that minimizes risk to the business or organization. There are two types of access control: physical and logical.

i. Physical access control: limits access to campuses, buildings, rooms, and physical IT assets.

ii. **Logical access control:** limits connections to computer networks, system files, and data.

To secure a facility, organizations use electronic access control systems that rely on user credentials, access card readers, auditing, and reports to track employee access to restricted business locations and proprietary areas, such as data centers. Some of these systems incorporate access control panels to restrict entry to rooms and buildings, as well as alarms and lockdown capabilities, to prevent unauthorized access or operations. Logical access control systems perform identification authentication and authorization of users and entities by evaluating required login credentials that can include passwords, personal identification numbers, biometric scans, security tokens, or other authentication factors. Multifactor authentication (MFA), which requires two or more authentication factors, is often an important part of a layered defense to protect access control systems(Andrew, 2019).

2.2.2 Categories of Access Control Equipment

Depending on the sensitivity of the data an organization holds, there needs to be data classification levels to determine elements including who has access to that data and how long the data needs to be retained. Typically, there are four classifications for data: public, internal-only, confidential, and restricted. The following are the categories of access control systems.

i. **Physical access control systems**: are the equipment used to selectively restrict access to a location. Physical control equipment usually begins the access control process at a distance outside a

facility's perimeter mainly by controlling vehicular movement and pedestrian access near points of entry. For higher security applications, access control continues at building entrances and secure area entrances.

ii. **Token and cipher systems**: are mechanical devices or electronic systems that facilitate authentication for the bearer to enter a protected space. A token is a physical device (i.e., ID card or key fob) that is kept on the user's person for use with the token system. Cipher locks perform a similar function using a personal identification number (PIN), or code, that must be keyed in for access.

iii. **Biometric systems**: use physical or behavioural data measurements to determine access authorization.

iv. **Assistive technologies**: involve the use of alternative or specially designed equipment or implementation of special systems that enable personnel with disabilities to use the access control system.

v. **Radio Frequency Identification (RFID) system**: comprises hardware, known as interrogators or readers and tags also known as labels as well as RFID software or RFID middleware. RFID tags are of two major types, which include Active Tags and Passive tags. Plate 2.1 shows the RFID tag reader as one of the prevalent access control technologies.

Plate 2.1: RFID *Reader (Kumar, 2015)*

The tag, also known as the transponder (derived from the terms transmitter and responder), holds the data that is transmitted to the reader when the tag is interrogated by the reader. The most common tags today consist of an Integrated Circuit with memory, essentially a microprocessor chip. Other tags are chipless and have no on-board Integrated circuit. Chip-less tags are more effective in applications where a simpler range of functions is all that is required; although they can help achieve more accuracy and better detection range, at a potentially lower cost than their Integrated Circuit-based counterparts. From here on out, we will use the term tag to mean Integrated Circuit-based tag. We will refer to chip-less tags explicitly when needed. RFID tags come in two general varieties which are passive and active tags. Passive tags require no internal power source, thus being pure passive devices (they are only active when a reader is nearby to power them), whereas active tags require a power source, usually a small battery. The RFID tag is shown in plate 2.2.

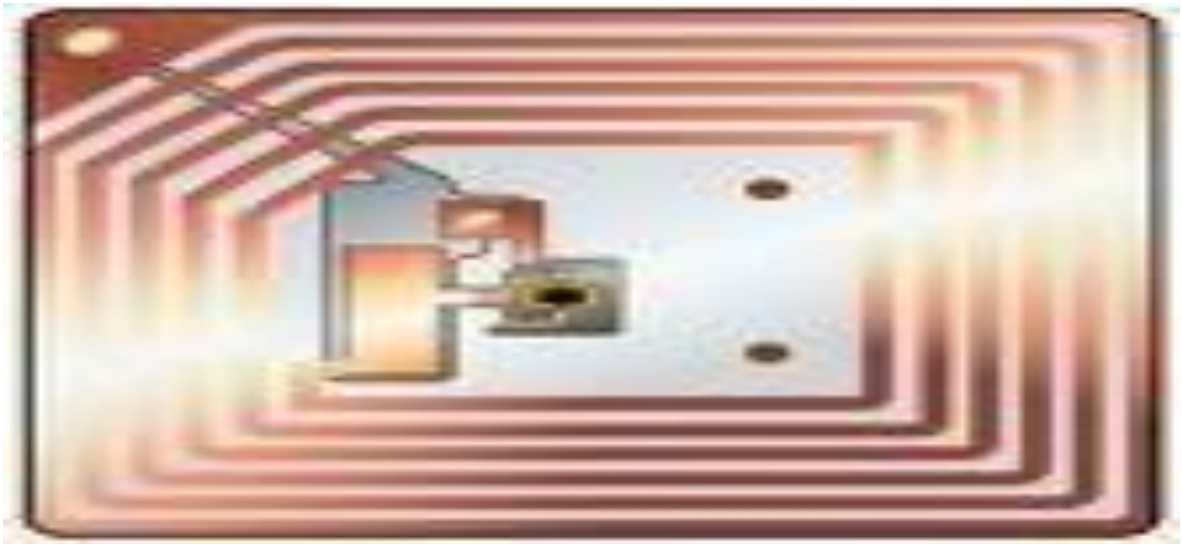

Figure 2.2: RFID Tag (Kumar, 2015*)*

The RFID reader sends a pulse of radio energy to the tag and listens for the tag's response. The tag detects this energy and sends back a response that contains the tag's serial number and possibly other information as well.

In simple RFID systems, the reader's pulse of energy functioned as an on-off switch; in more sophisticated systems, the reader's RF signal can contain commands to the tag, instructions to read or write memory that the tag contains, and even passwords. These operations are shown in figure 2.3.

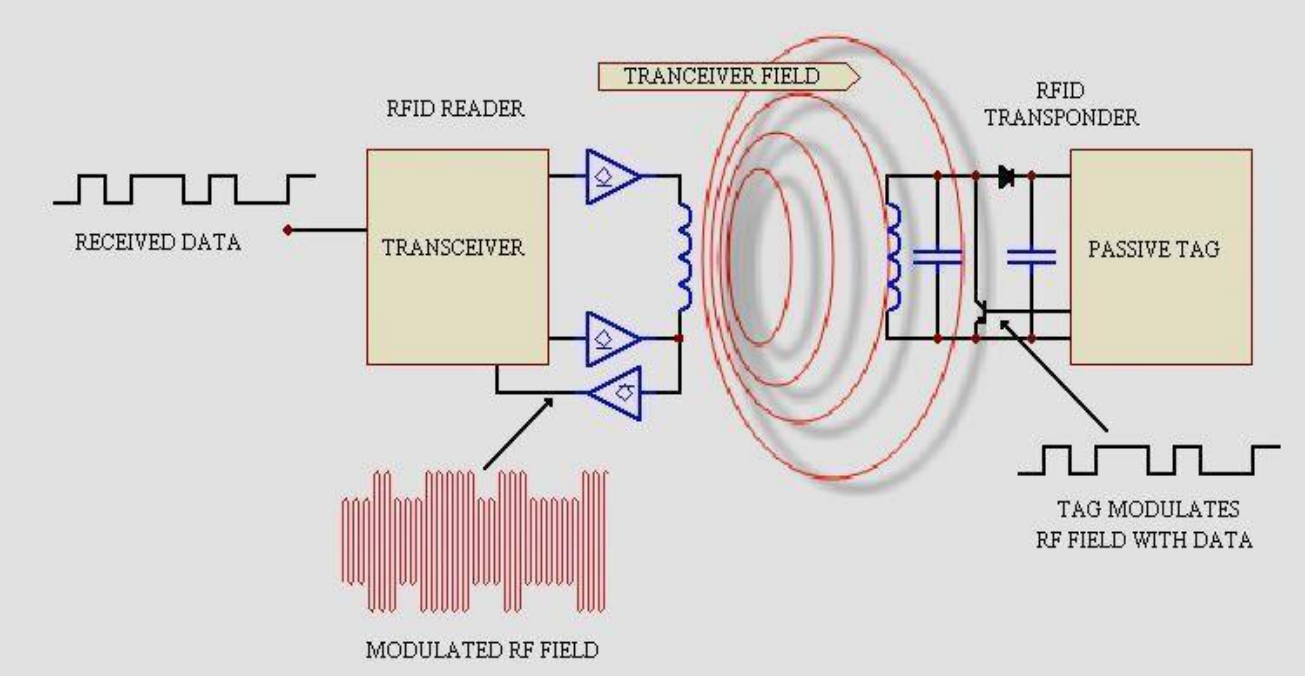

Figure 2.3: RFID transceiver that communicates with a passive Tag (Kumar, 2015)

Smart Access Control System offers the following benefits:

1. **Enhancing security**: The primary objective is to improve the security of a facility by restricting access to authorized personnel only. This helps in preventing unauthorized individuals from entering restricted areas and reduces the risk of theft, vandalism, and other security threats.

2. **Streamlining access management**: Another objective is to simplify the process of managing access permissions for different individuals or groups. This includes configuring access levels, granting or revoking access privileges, and maintaining an accurate record of entry and exit times.

3. **Improving operational efficiency**: The thesis aims to enhance the efficiency of day-to-day operations by facilitating quick and controlled access to different areas based on authorized personnel's roles and responsibilities. This can help in minimizing delays and bottlenecks caused by manual entry processes.

4. **Enabling remote access control:** The objective can also be to provide remote access control capabilities, allowing authorized personnel to grant or deny access remotely, monitor entry activities, and respond to security incidents promptly.

5. **Integrate with other systems**: The thesis can aim to integrate the access control system with other security systems, such as CCTV cameras, alarms, and intrusion detection systems. This integration helps in providing a comprehensive security solution and enables a proactive response to potential threats.

6. **Ensuring compliance**: Another objective is to ensure compliance with industry-specific regulations, laws, and standards related to access control and security. This can involve implementing strict access control policies, maintaining audit trails, and generating reports for compliance purposes.

7. **Enhancing user experience**: The thesis can aim to improve the user experience of individuals accessing the facility by providing user-friendly interfaces, minimizing waiting times, and ensuring a seamless and efficient access control process.

8. **Reducing administrative overhead**: The objective can be to reduce administrative burdens and manual tasks associated with managing access permissions by automating processes and leveraging technologies like biometric authentication, smart cards, or mobile applications. Overall, the aim and objectives of an access control systems thesis revolve around enhancing security, streamlining access management, improving operational efficiency, and providing a safe and secure environment for individuals within a facility.

9. **Compliance and Regulation:** Many industries and organizations have specific regulatory requirements for access control. Studying access control systems helps in understanding these regulations, ensuring compliance, and avoiding penalties or legal issues. It allows organizations to align their access control practices with industry standards and best practices.

10. **Operational Efficiency**: Access control systems play a crucial role in streamlining and optimizing daily operations within a facility. Studying access control systems enables the identification of areas for improvement, such as optimizing access workflows, automating processes, and integrating with other systems for enhanced efficiency. This can lead to cost savings, faster response times, and improved overall operational performance.

11. **User Experience:** Access control systems impact the experience of individuals accessing a facility. Studying access control systems allows for the design of user-friendly interfaces, convenient access methods, and efficient entry processes. This enhances user experience, reduces waiting times, and increases overall satisfaction with access procedures.

12. **Integration with Technology**: Access control systems often integrate with other security technologies, such as CCTV cameras, alarms, and intrusion detection systems. Studying access control systems helps in understanding the integration possibilities, interoperability challenges, and the potential for leveraging emerging technologies, such as biometrics, artificial intelligence, or cloud-based solutions, to enhance security and operational efficiency.

13. **Data Analysis and Reporting**: Access control systems generate vast amounts of data, including entry logs, access requests, and user profiles. Studying access control systems allows for the analysis of this data to identify patterns, anomalies, and potential security breaches. It also helps in generating reports for auditing, compliance, and forensic purposes. In summary, studying access control systems is significant for improving security, mitigating risk, ensuring compliance, enhancing operational efficiency, improving user experience, integrating with technology, and analyzing data for better decision-making in access control and overall security management.

Door lock System Analysis

Door lock systems may be wired, which are connected to the home's electrical system, or wireless, which are usually battery-powered and transmit a radio signal to the chime. Door lock systems consist of a button, a transformer and a chime unit. These components can be replaced independently of each other.

Door locks are available with a broad selection of features to meet any need, ranging from units designed for people with special needs to models that can be customized to reflect a unique style and taste. There are two basic types of door locks: wired and smart door locks.

a. Wired Door lock: Wired door locks have an electrical cord attached to them and connect to the power supply through the electrical outlet in homes and offices.

b. Wireless Door lock: A wireless door lock is a type of door lock that operates without wires or the need to connect to the electricity supply in the house.

c. Smart Door Lock: As smart devices, video or photo-capture door locks need an internet-connected (and working) Wi-Fi connection to properly operate. Wi-Fi is how all of the smart features work, from two-way audio to video and push notifications.

Aside from Wi-Fi, wireless door locks also need some form of power to function (battery).

2.2.3 ESP32 Camera Module and Pin functions:

ESP32 is a low-cost, low-power Microcontroller with integrated Wi-Fi and Bluetooth. It is the successor to the ESP8266 which is also a low-cost Wi-Fi microchip albeit with limited vastly limited functionality. It forms the heart of the system. Plate 3.8 shows the pinout of the ESP32 Camera module.

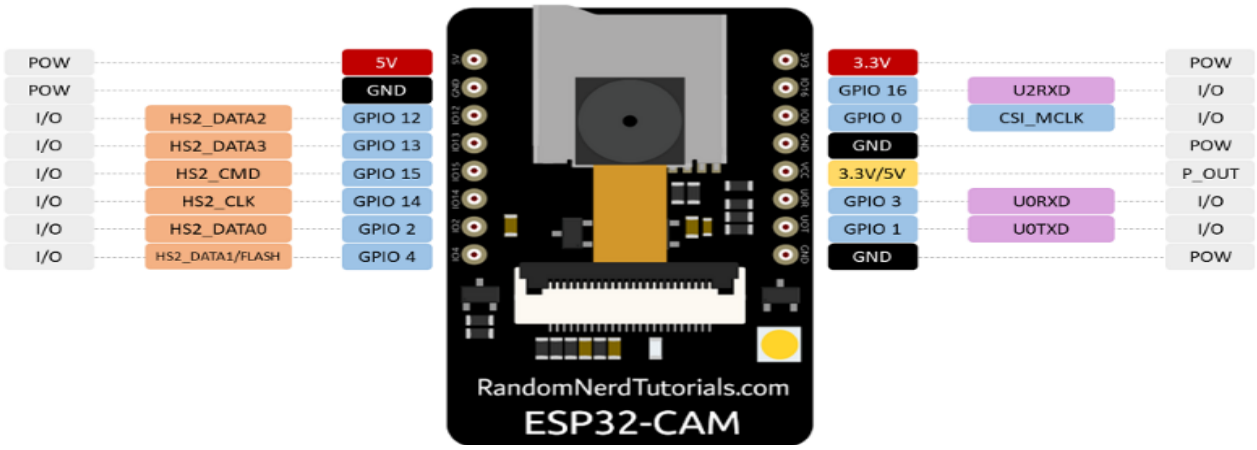

Figure 2.4: ESP32 CAMERA MODULE

2.2.4 Important features of ESP32 Camera Module

The special features of ESP32 Camera include the following:

i. The smallest 802.11b/g/n Wi-Fi BT SoC module
ii. Low-power 32-bit CPU, can also serve the application processor
iii. Up to 160MHz clock speed, summary computing power up to 600 DMIPS
iv. Built-in 520 KB SRAM, external 4MPSRAM
v. Supports UART/SPI/I2C/PWM/ADC/DAC
vi. Support OV2640 and OV7670 cameras, built-in flash lamp
vii. Support image WiFI upload
viii. Support TF card
ix. Supports multiple sleep modes
x. Embedded Lwip and FreeRTOS
xi. Supports STA/AP/STA+AP operation mode
xii. Support Smart Config/AirKiss technology
xiii. Support for serial port local and remote firmware upgrades (FOTA)

2.2.5 ESP32 Camera Pins and functions

a. Universal Asynchronous Receiver-Transmitter (UART) Pins

There are two interfaces of UART, UART0 AND UART2 on the ESP-32 S chip. The general purpose input and output pin (**GPIO) 1** (Tx), **GPIO 3** (Rx), and **GPIO 16** (Rx) are three serial pins. Serial pins are responsible for communication. The only pin of UART2 (GPIO 16) is broken out, so it doesn't take part in communication and makes UART0 the only usable UART on the chip. ESP32 doesn't have a

built-in programmer, so the GPIO 1 pin is used to transmit and GPIO 3 is used to receive the data. These pins make communication connections and upload code to the board.

GPIO1: The universal asynchronous receiver-transmitter (UART-Transmission pin) takes bytes of data and transmits the individual bits in a sequential fashion.

GPIO3: The universal asynchronous receiver-transmitter (UART1-Reception pin).

GPIO16: The universal asynchronous receiver-transmitter (UART2-Reception pin).

GPIO 33 -Built-in Red LED: There is an LED red colour on the board near the reset button. When shining bright, it indicates that there is some operation going on GPIO 0 pin – Flash Mode Selection

GPIO 0: this is a mode selection pin. When the GPIO0 is connected to the ground to make it low, it enables the flash mode. In flash mode, the code is flashed to the board. To disable the flash mode, the connection of this pin with the GND pin is removed. The microcontroller returns to the normal program execution mode.

GPIO 4 Pin: ESP-32 CAM has an inbuilt flash LED light. This is used to take pictures in the dark. This flashlight is connected to the GPIO4 pin. The GPIO 4 pin is also connected to the micro-SD card, so it needs to be programmed well when using both functions together.

2.3 REVIEW OF RELATED WORKS

According to the work done by Divya and Neetu in Performance Analysis of Authentication System: A Systematic Literature Review, Data authentication is vital nowadays, as the development of the internet and its applications allow users to have all-time data availability, attracting attention towards security and privacy and leading to authenticating legitimate users. There are diversified means to gain access to restricted areas, like passwords, biometrics, and smartcards, even by merging two or more techniques or various factors of authentication. This paper presents a systematic literature review of papers published from 2010 to 2022 and gives an overview of all the authentication techniques available in the

market. This study provides a comprehensive overview of all three authentication techniques with all the performance metrics (Accuracy, Equal Error Rate (EER), False Acceptance Rate (FAR)), security, privacy, memory requirements, and usability (Acceptability by user)) that will help one choose a perfect authentication technique for any access control device (Singla, 2023).

This chapter will present us with numerous advantages of how to effectively implement an energy management system and coordinate electrical appliances from a single control source(Aalase et al., 2023). Alkar and Buhur (2005) carried out, an Internet-based wireless flexible solution where a home piece of equipment is connected to a slave node. The slave nodes interact with the master node through Radio Frequency (RF) and the master node has a serial RS232 link with the Personal Computer server. The nodes are based on PIC 16F877μc. PC server is formed of a user interface component, the database, and the web server components. An Internet page is set up to run on a Web server. The user interface and the Internet front end are connected to a backend database server. The control of physical objects is established and their states are monitored through the Internet (Bhat et al, 2017).

Tan and Soy (2002) developed a system for controlling home electrical appliances over the Internet by using Bluetooth wireless technology to provide a link from the appliance to the Internet and Wireless Application Protocol (WAP) to provide a data link between the Internet and a mobile phone. However, technical details relating to the controller are not revealed (Bhat et al., 2017).

A Face Recognition Method for Security Applications in Smart Homes and Cities (.RaviKiran and Mani Kumari**,** 2024), This work, presents the design and implementation of a door lock system using facial recognition in conjunction with the ESP32 CAM for more accurate face detection. The ESP32 CAM, which is powered by a battery, is the system's backbone, and it controls the door's locked and unlocked systems. This door lock system is controlled by face recognition and a smartphone, face

recognition and a smartphone are used to run this door lock system. Authorized users can use the face detection system, while unauthorized users can't use the ESP32 CAM. This system is a viable one in the sense that it will go a long way in making it more convenient and easier for home use most especially where serious security is needed.

Automatic Door Access Control System Based on Facial Recognition Using ESP32-CAM (Bhavishya Reddy and Syed Jahangir, 2022), this project, presents that through IoT we can connect multiple input/output devices, multiple sensors, and actuators in a network so that they can talk to each other. the data obtained from these can be used to log monitor or control other things without human intervention and much more. As such, IoT is like global networks that provide communication between objects and people. The proposed system consists of an ESP32 cam, FTDI which is a future technology device international, a relay module, a solenoid lock, a capacitor, and a voltage regulator. The system works well in the local environment and meets the required expectations.

According to the work done by Ashish Kumar and Manish Gupta (2023) Smart Face Recognition using IoT and Machine Learning, this research work focuses on how to create a system that uses machine learning and the Internet of Things (IoT) to recognize faces in an intelligent and effective way. Traditional face recognition systems require manual input, which can be time-consuming and error-prone, and have low accuracy. But with this work, we can create a system that can recognize people accurately without user input by learning from patterns in facial features thanks to the growing use of IoT devices and machine learning techniques. Applications for this system include attendance tracking, security systems, and personalized marketing. The difficulty, however, lies in creating a system that is trustworthy and secure while simultaneously protecting the privacy of users.

Authentication with face Recognition and Sign Languages using ESP 32-CAM

(Zafer Yalcin and Omer Aydin, 2023); this work focuses on how to create a secure system using face recognition and sign language as an authentication method and application using ESP32-CAM. Its results show that secure authentication cannot be achieved with facial recognition and sign language. The developed system is low-cost and easy to implement. With this system, authentication can be done without requiring any physical contact, and it can be used for personal security and entrance and exit. Sign language, which is frequently used by hearing-impaired individuals, can play an active role in authentication. With low-cost modules such as ESP32, it will be an alternative to authentication in almost every environment.

According to the work done by Samuel Kristiyana and Amir Hamzah (2023), Smart Safe uses the face detection method ESP32 CAM; this research work is to design a smart safe, which can be opened by facial pattern recognition so that the safe can only be opened by the owner of the registered face. Therefore, to be able to recognize facial patterns, a face detector is needed in the form of a camera module, namely the ESP32 CAM, which can capture facial patterns that have been registered via the IoT system. After the face pattern is registered, the ESP32 CAM can function as a security system to open the safe using the face pattern. The safe is also equipped with a keypad as an alternative to open the safe and alarm when forcibly disturbed by others. This smart safe technology is expected to help users in safeguarding assets and valuables stored in a safe, so there is no more worry over theft.

Face Recognition Based Attendance System (Mekala V and Vibi Mammen, 2019) This work aims to eliminate human errors and proxy in recording the attendance of students or personnel in an institution or organization. This is achieved by using face recognition to monitor the attendance of students in a class. The face recognition process is carried out by using the Cognitive Face API which follows the Principal Component Analysis (PCA) algorithm. Initially, the dataset of the students in a class is collected. The dataset is collected in a manner that for each student, a set of 25 images from various

angles is collected. This project is very helpful in avoiding human error taking attendance of any organization or institution which is unavoidable.

2.4 SUMMARY OF SELECTED RELATED WORKS

The work on Access control Android Based GSM System, by (Snehal et al., 2018), this thesis focuses on developing a system, which uses mobile technology that keeps control of the various units of the automobiles, through the signal sent by mobile. In today's time, every system is automated to face new challenges. Automated systems have minimized manual operation, so the flexibility, and reliabilities are found to be highly accurate automated control systems.

"Probably, the important factor to know about the GSM is that it is an international standard. This makes it very compatible with devices using global systems for mobile communication (GSM) interoperability. With it, the user remotely controls the conditions (on or off) of electrical appliances. Only a simple SMS is sent to the global system for mobile communication modem at the nearer place, the devices can be turned on or off and the status of the devices can be sent to the prescribed mobile number registered in the microcontroller.

It can be that the "Android-based GSM System for Access control "was a successful establishment of a system. This system consists of an Arduino-Uno board, a Global System for Mobile Communication (GSM) Module, a GSM-based smartphone, power sockets, and home appliances or devices. It is user-friendly, that is flexible to handle, modern and it is mostly a cost-effective system.

RF Module Based Wireless Secured Access Control System Using Field Programmable Gate Array (FPGA) (Snehal et al., 2018) this research, is one of the emerging technologies for building intelligent surveillance. Wireless technologies like Bluetooth and Wi-Fi have been used in contemporary home security systems using low-cost, low-power, less complexity RF module. It uses multi-hop

communication for data transfer. This multi-hop technique gives out an unlimited range of communication thus giving it an edge over the other wireless technologies. Here the radio frequency transmission system employs the Amplitude-shift keying (ASK) technique with the transmitter and receiver operating at 433MHz. Due to high frequency, we can transmit data to a sufficient distance without attenuation. FPGA modules are highly suitable and compatible with the evolving technology of software-defined radios (SDR) due to their configurability, programmability, and security. This thesis arose when there was a need for data communication to be protected from corruption and unauthorized access. The security of the data can be provided by using certain Encryption techniques. If one of the stations is stationary, then we can use this application as automation. Finally, the aim is to transmit certain data wirelessly with high security and also to control output load from any remote place. Hence, to make this practical, a compact Transmitter is needed with receiver modules that can operate at 433MHz. The technologies deployed in this work are RF (multi-hop technique) and Field Programmable Gate Array (FPGA). The system offers the following advantages which include low cost, low power consumption, and high efficiency, it allows data Encryption and Decryption for security. However, the system coverage depends on the frequency of the transceiver used.

Bluetooth Remote Access Control System using Android Application (Snehal et al.; 2017) This system was designed to assist and provide support to fulfill the needs of the elderly and disabled in the home. Automation of the surrounding environment of a modern human being allows for increasing work efficiency and comfort. There has been a significant development in the area of an individual's routine tasks which can be automated. In the present times, it is common to use mobile phones and smart devices throughout the day. Analyzing the current smartphone market, novice mobile users are opting for Android-based phones. It has become a second name for a mobile phone in layman's terms. Access Control System (ACS) has been designed for mobile phones with having Android platform to automate

an 8-bit Bluetooth interfaced microcontroller that controls several home appliances like lights, fans, bulbs, and many more using on or off relay.

With the continuous growth of mobile devices in their popularity and functionality the demand for advanced ubiquitous mobile applications in people's daily lives is continuously increasing. Smart Home is the term commonly used to define a residence that integrates technology and services through home networking to enhance power efficiency and improve the quality of living.

The research work on the Automation of Irrigation systems using Android Technology (Adoju & Ahesh, 2015) focused on Agricultural technology advancements which culminate in the utilization of vast terrestrial expanses. The managerial work involved in the land is proportional to its size. Generally, most of the irrigation systems are manually operated and these techniques are being replaced with automated techniques that suggest an automated concept of irrigation to use the water effectively. An automated Irrigation system is implemented either based on the soil water content or based on the user input via Short Message Service systems. The first method is a secluded irrigation system where the farmer is not relayed information about the irrigation status which causes inefficiency in the usage of water due to the user issuing command without factoring in the soil condition. Resulting of the perpetual rise of population, modern techniques are developed to control the system. This paper proposes a novel technique to automate an irrigation system that analyzes the conditions of agricultural land in a real-time manner and provide rapid supervisory control through an Android application.

Based on the research that have been done, one of the main issues in most existing ACS is their implementation and maintenance cost which is not affordable for most users. Furthermore, some current systems provide a view of the house from a web application which is inconvenient for users, who must access the Web each time they wish to control or view the status of their houses(Kazi & Tiwari, 2016). In addition, some have lack of user-friendly interfaces for monitoring and controlling appliances.

Besides, there are some limitations in the communication technologies that have been used in the existing automation systems. For example, the communication range of Bluetooth is limited to 10 meters. If more than 10 meters, the connection will be lost and the user not able to control the home's appliances. Furthermore, ZigBee is designed for low-rate wireless personal area networks with a data rate of 250Kb/s which is an insufficient data rate. Another communication technology is GSM which can be accessed anywhere in the world but it is costly and it has a low data rate of transmission and limitations in coverage for rural areas (Kazi & Tiwari, 2016).

Therefore, proposes a new system to overcome the limitations of the existing access control systems. This can be achieved by designing and fabricating a low-cost Wi-Fi-based Automation System for a Smart Home prototype using an Arduino microcontroller and an Android-based smartphone. The system is developed to control all the electrical appliances at home easily and efficiently and enable remote control by supporting the IoT concept.

Raspberry Pi Access Control Using Android Application (Himani et al., 2017). The thesis presents a low-cost and flexible home control and monitoring system using a Raspberry PI module and a Static Relay, with internet connectivity for accessing and controlling devices and appliances remotely using a Smartphone android application. The proposed system does not require a dedicated server PC concerning similar systems and offers a novel communication protocol to monitor and control the home environment with more than just the switching functionality. To demonstrate the feasibility and effectiveness of this system, devices such as Static relays and a wifi router can be integrated with the home control system.

In this busy and comfortable lifestyle of people, communication technology has evolved in such a way that any information will be accessed from anywhere, at any time, by anyone. In today's communication technology, communication is not only constrained between two computers, but it is a complete network

called the Internet. With advanced internet technology today not only can information be accessed from any place, at any time, by any person, but can also control and monitor various devices from any place, at any time, by any authenticated person, this technology is called Internet of Things (IoT). This report represents the application of IoT for a Smart Access control system which includes a Raspberry Pi as a processing unit for data which is extracted from various sub-systems like Temperature sensing system, Automatic light system, Cooling system, Gas detection system, Water level sensing system, Motion detection system and Lights on and off system. All these systems are monitored and controlled remotely by a web page.

The Access control using IOT and Mobile App Tanish (Sehgal & More, 2017), this paper presents an idea or a concept for utilization in the most open and also practical way for access control using voice recognition. Today, the access control industry is growing widely; this is powered by the need to provide systems that provide support for aged and physically handicapped people, especially people who live alone. Smart home or access control can be said as the residential extension of building automation, it also involves the automation and controlling of lighting, ACs, ventilation, and security which also includes home appliances such as dryers or washers, ovens or refrigerators or freezers which uses WiFi for monitoring via remote. Access control must have compliance with all the household standards and ease of use. This paper focuses on a flexible, cost-friendly wireless access control system which would be based on an Android App. The app will be working with the help of Voice Recognition also the Internet of Things. The App would feature the process of voice recognition that would take commands from the user in order to control different home appliances that would be connected via IOT.

Access control Using ZigBee (Hinal, 2017), This version of access control is really necessary in the modern era. Access control is the digital connectivity among different appliances. This paper shows the potential of ZigBee through the design and implementation of the access control system. ZigBee

ZigBee-based access control system provides remote access to the user for monitoring and controlling purposes. ZigBee wireless devices are preferable because of their low power consumption. ZigBee takes advantage of short-range wireless protocol and provides complete interoperability. This makes the complete access control wireless. Users can control home switches with a ZigBee enabled touch screen.

Voice Recognition-Based Access Control System for Paralyzed People ((Kumar & Shimi, 2015), this paper presents the design of a low cost voice recognition-based access control system for physically challenged people suffering from quadriplegia or paraplegia (who cannot move their limbs but can speak and listen) to control the various home appliances and can actuate the bed elevation just by the voice commands according to their need and comfort. The proposed system consists of a voice recognition module, Arduino uno microcontroller, relay circuit and an adjustable bed. The voice recognition module needs to be trained first before it can be used to recognize commands. Upon successful recognition of voice command the Arduino drives the corresponding load with the help of the relay circuit. The adjustable bed elevation can be set to the three different modes as per the user's comfort and need. The accuracy of the voice recognition module is also measured in different conditions. The experimental results validate the functions of the proposed system. The results show the system can provide great assistance to the physically challenged people without any third person's assistance.

According to the work done by Nikhil et al (2018), Agricultural technology is a rising field that culminates in the utilization of vast terrestrial expanses. The managerial work involved in the land is proportional to its size. Generally, most of the irrigation systems are manually operated and these techniques are being replaced with automated techniques that suggest an automated concept of irrigation to use the water effectively. An automated Irrigation system is implemented either based on the soil water content or based on the user input via Short Message Service systems. The first method is a secluded irrigation system where the farmer is not relayed information about the irrigation status which

causes inefficiency in the usage of water due to the user issuing command without factoring in the soil condition. Resulting of the perpetual rise of the population, modern techniques are developed to control the system. In this the novel technique deployed made it possible for the farmers to have more time for other meaner activities (Golait et al, 2017).

The research done by Kumar and Tiwari(2018) on Energy Efficient Smart Access control Systems focused on the high energy needed by home appliances (like white goods, audio/video devices, and communication equipment) and air-con systems (heating and cooling), which makes homes one among the foremost essential areas for the impact of energy consumption on natural surroundings. AIM for the planning of a system that will minimize energy waste in home environments with efficient managing device operation modes. In design, we tend to use a wireless sensing element network to observe physical parameters (like light weight and temperature) additionally because of the presence of users reception and in every of its rooms. To optimize energy consumption and value while guaranteeing the specified comfort level. When users change their habits as a result of unpredictable events, the system can notice wrong predictions by analyzing in real-time info from sensors and switch system behavior consequently. Parameters that might stop the introduction of access control systems for energy saving into the mass market (Kumar & Tiwari, 2015).

Harinath and Santhi (2015) researched and demonstrated strong competencies in "GSM (Global System Messaging) based secured device control system using App Inventor for Android mobile phones." Remote Access control turns out to be more and more significant and appealing. It improves the value of lives by automating various electrical appliances or instruments. This paper describes a GSM (Global System Messaging) based secured device control system using App Inventor for Android mobile phones(Harinath & Santhi, 2015). App Inventor is the latest visual programming platform for

developing mobile applications for Android-based smartphones. This work caught the attention of Android App users where virtually everything in their house could be controlled using an Android application.

Borkar and Karande (2018) researched Web Hosting and Live Streaming using Raspberry Pi for Access control with advanced internet technology today not only we can access information from any place, at any time, by any person, but we can also control and monitor various devices from anyplace, at any time, by any authenticated person, this technology is called the Internet of Things (IoT). This report represents the application of IoT for a Smart Access control system which includes a Raspberry Pi as a processing unit for data which is extracted from various sub-systems like Temperature sensing system, Automatic light system, Cooling system, Gas detection system, Water level sensing system, Motion detection system and Lights on and off system. All these systems are monitored and controlled remotely by a web page(Borkar & Karande, 2017).

"Design and Implementation of a WiFi Based Access Control System", this research on the implementation of a new access control system that uses WiFi technology as a network infrastructure connecting its parts, was meticulously carried out by Ahmed ElShafee and Karim Alaa Hamed. The proposed system consists of two main components; the first part is the server (webserver), which presents a system core that manages, controls, and monitors users' homes. Users and system administrators can locally (LAN) or remotely (internet) manage and control system code. The second part is the hardware interface module, which provides an appropriate interface to the sensors and actuators of access control system. Unlike most available access control systems in the market the proposed system is scalable in that one server can manage many hardware interface modules as long as it exists on WiFi network coverage. The system supports a wide range of access control devices like

power management components, and security components. The proposed system is better from the scalability and flexibility point of view than the commercially available access control systems (Ahmed and Karim, 2012). The result obtained was sustainable in the sense that the loads could be controlled via web browsers which makes it operable suing either a mobile phone or Computer.

Table 2.1: Summary of Selected Related Literature Reviews

S/N	TITLE	AUTHOR	YEAR	RESULTS	LIMITATION(S)
1	A smart access control system is a system that automates entry and exit into apartments,	Postulka	2019	The system used biometrics to grant access to places.	No picture feedback in the event of an unauthorized attempt to gain access
2	An intrusion detection system (IDS)	Salikhov et al.,	2021	The system was able to detect movements within target areas and gives an alarm notification.	It couldn't send notifications to remote users over the internet.
3	RF Module-Based Wireless Secured Access Control System	Snehal et al.,	2018	It worked perfectly	It wasn't accessible over the internet due to the technology deployed.
4	Access control Using ZigBee	Hinal	2017)	The system worked and was able to control an electric door as proposed by the author	It wasn't accessible over the internet due to the technology deployed.
5	RFID Based Access Control System	Andrew	2019	RFID tags served as the means of identification	There was a proximity challenge. The RFID tag must be very close to the RFID card reader

2.5 Research Gaps

After the review of related works, it was observed that the systems implemented lacked some key features such as face recognition only or password only, which this study addresses. The IFRSACS has the following smart features:

i. Ability to auto-capture unauthorized persons and send the captured photos to the concerned authority for notification of an illegal attempt to access a restricted area.

ii. Ability to notify the security personnel of any suspicious movements, especially at night hours for appropriate actions to be taken.

iii. Ability to communicate with the concerned authority remotely regardless of distance, provided that there is a strong between the sending end (IFRSACS) and the receiving end (user's smartphone).

CHAPTER THREE

MATERIALS AND METHODS

3.1 MATERIALS

This chapter presents both the hardware and software used in the design and implementation of the IoT-based face recognition smart access control system. The materials and methods used in the design are inclusive in this chapter.

3.1.1 Hardware materials

The following electronic components are the hardware materials that are needed for the design and implementation of the system

i. **ESP32 Camera module**
ii. **Voltage regulator**
iii. **Bipolar junction transistor (BJT**
iv. **Fixed resistor**
v. **Liquid Crystal Display (LCD**
vi. **Reset button**

vii. **Keypad:** For implementing the input panel. This is used for inputting values to the system.

viii. **Solenoid Lock:** The solenoid lock denotes a latch for electrical locking and unlocking. It is available in unlocking in the power-on mode type, and locking and keeping in the power-on mode type, which can be used selectively for situations. Door Lock Mechanism: This may be an electronically controlled lock that can be activated or deactivated by the microcontroller based on the result of the face recognition process.

The power-on unlocking type enables unlocking only while the solenoid is powered on as shown in figure 3.1.

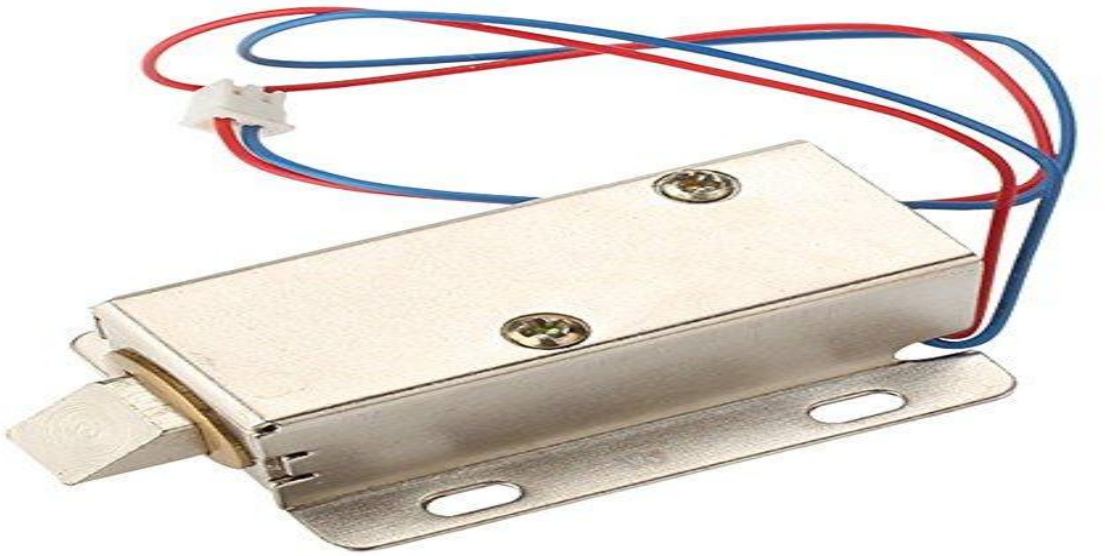

Figure 3.1: 12V DC Solenoid lock for access control of a door (Varalakshmi, 2018)

3.1.2 Design components and specifications

The hardware materials used in the design to achieve the first specific objective were itemized table 3.1. All components were seamlessly integrated to work together efficiently and the overall system latency very minimal to ensure quick response times (e.g., less than 1 second from image capture to door unlock).

Table 3.1: Design Specifications of the electronic components used, according to the manufacturers' datasheet

S/N	Component	Current Rating (mA)	Voltage Rating (V)	Power Rating (mW)	Quantity
1	Rectifier diodes: 1N4007	300	0-12	5	4
2	Electrolytic capacitor	1500	0-25	230	1
3	Transistors (BC 547 NPN)	4500	0-35	70	2
4	Resistor (100K, 2W)	500	0-230	2	2
5	5V DC 10A relay	10000	5	50000	1
6	12V DC Solenoid Lock	2500	12	30000	1
7	Quartz crystal (12MHz)	6.3	3.3 - 5	0.02 – 0.03	1
8	Non-polarized capacitor (30pF)	1	5	0.002	2
9	Variable resistor (20K)	20	0 - 50	2000	1
10	16X2 LCD	1	5	5	1
11	Fixed resistor (1k)	2	0-50	3	1
12	ESP32 CAM	180	5	900	1
13	Buzzer	20	5	100	1

3.1.2: Software Requirements

The software requirements for the system design include the following:

i. **Micro-python/ArduinoC++ programming language:** This is an open-source programming language for beginners and professionals. It was used in the programming of the ESP32 microcontroller.

ii. **Mendeley Software:** for documentation in reference management.

iii. **EASYEDA** for the circuit design. Though Proteus can also be used EASYEDA has more working tools than Proteus. It has the following features over Proteus Software:

a. Simple, Easier, Friendly, and Powerful general drawing capabilities

b. Schematic Capture

c. Printed circuit board (PCB) Layout

d. Working Anywhere, Anytime, Any Device

e. Real-time Team Cooperation

f. Sharing Online

g. Thousands of Open Source Thesis

3.2.1 Research Design

i. Development of a system that permits authorized persons to enter and exit, and deny entry to unauthorized persons into restricted areas:

This is the first research specific objective. It involves the sub-block diagrams as shown Figure 3.2. The following smaller block diagrams made up the door lock unit system. Camera module is responsible for capturing the picture of the intruder. An image is captured and passed to a face detection algorithm (e.g., using a pre-trained Haar cascade). The algorithm identifies a face and returns the coordinates of the bounding box. The cascade classifier is a multi-stage classifier where each stage consists of a strong classifier. Stages are designed to reject non-face regions quickly, allowing the classifier to focus computational resources on promising regions that may contain faces (Viola & Jones, 2022). The keypad module takes input from the user and compares with the programmed password. The data storage unit saves the pictures in the cloud for future reference. The door lock control unit is the interfacing circuit of the DC relay that controls the opening and closing the door.

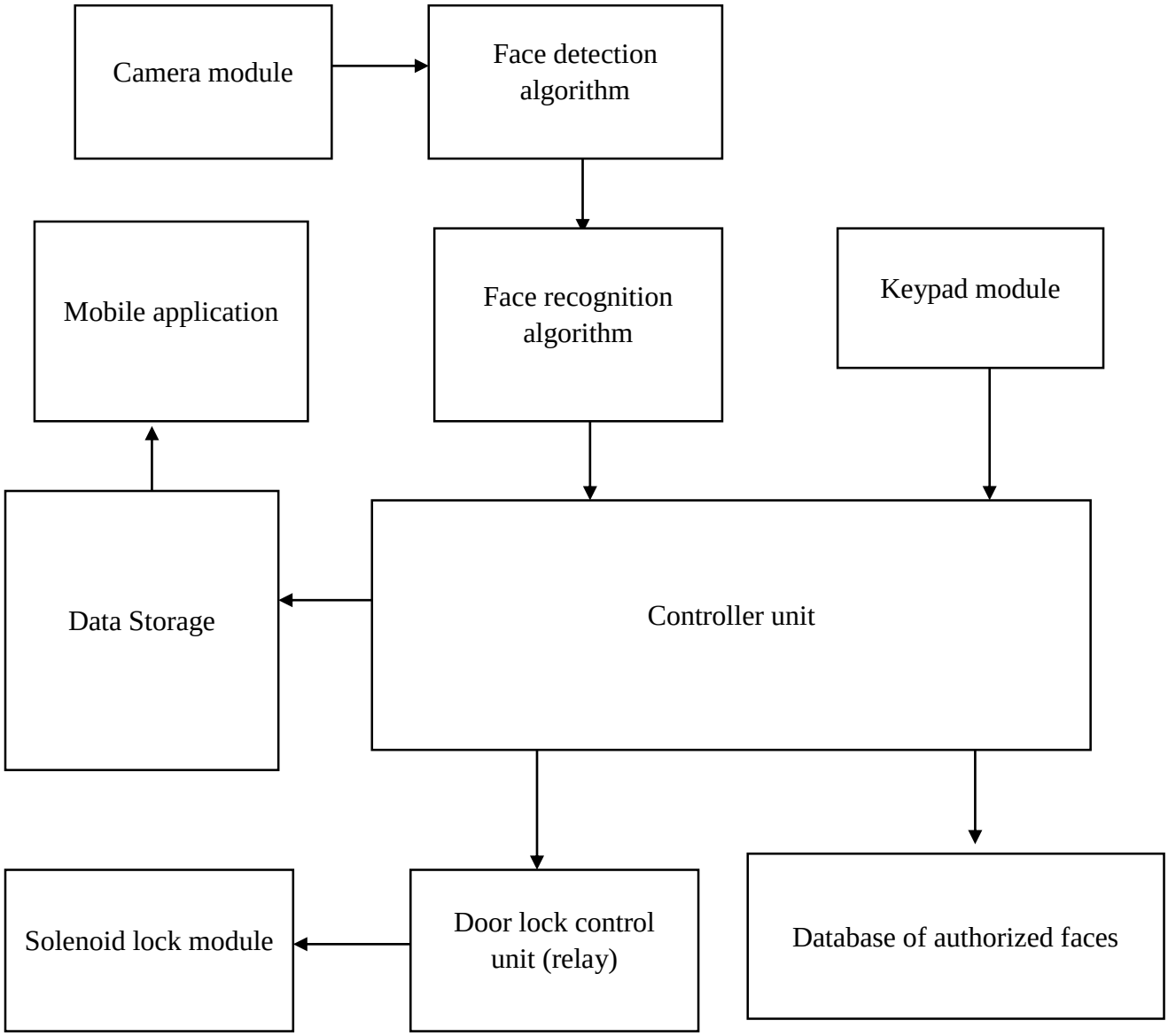

Figure 3.2: The block diagram of face recognition access control unit

After the block diagram, follows the flowchart for a face recognition door lock access control system which helps visualize the step-by-step process and interactions between different components. The system is initiated, and ready to capture and process an image. The camera captures the image of the person at the door. The captured image underwent pre-processing steps such as resizing and normalization to enhance detection accuracy. The pre-processed image is analysed by the face detection

algorithm to locate the face within the image. The system would check if the face detected was recognized or not, if yes, access would be granted and the door would be opened, but if no, access was denied the process ended. This flowchart provides a clear and structured overview of the operations and decision points in a face recognition door lock access control system. Figure 3.3 shows the clearer signal flow in the system.

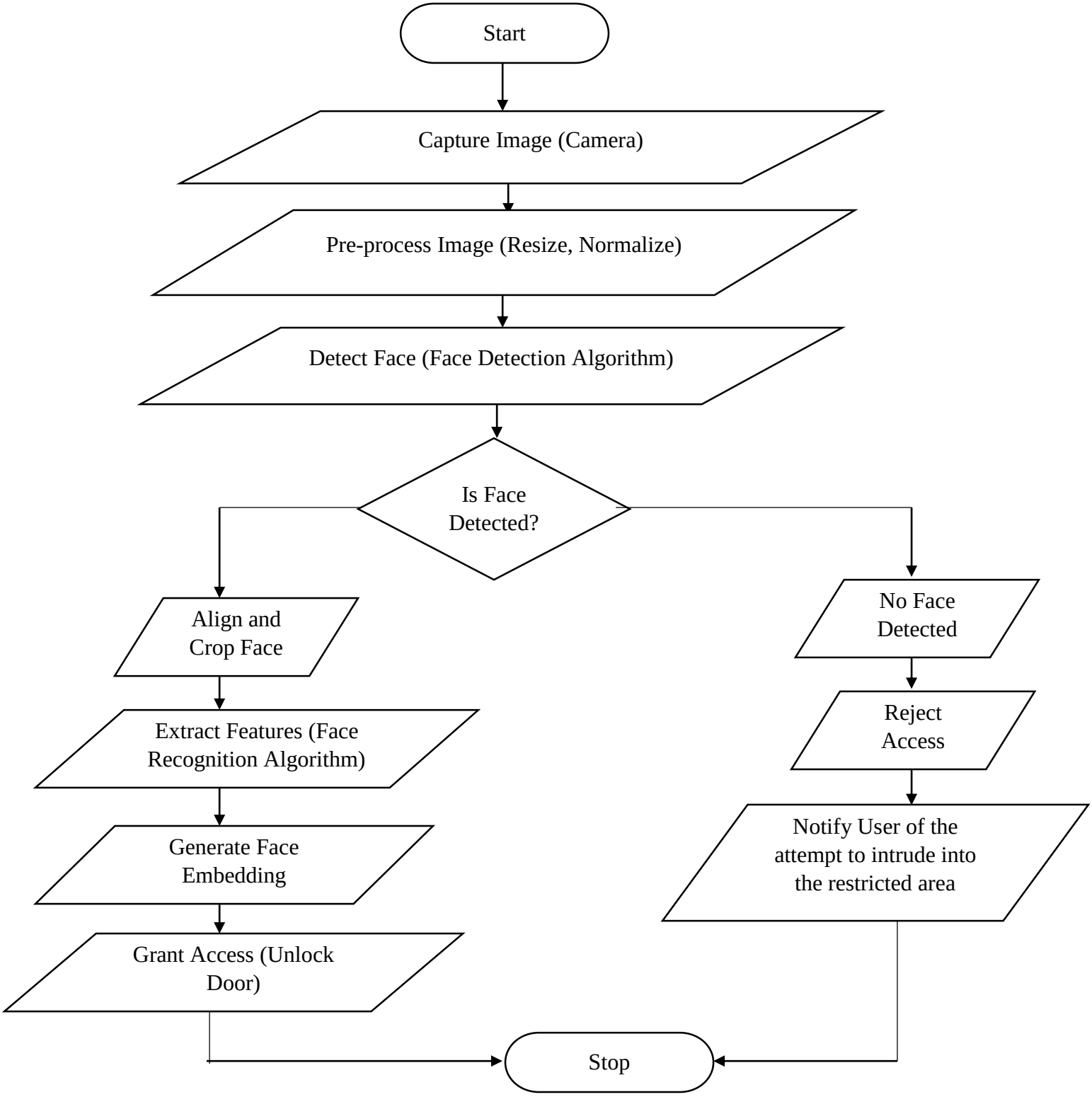

Figure 3.3: The flowchart of the face recognition and door lock control unit

ii. **Implementation of a sub-system capable of real-time picture capture and notification to the security personnel, of attempts to gain unauthorized access into restricted areas**

The second objective of this work is to design and implement a sub-system capable of capturing real-time images and notifying security personnel when there are attempts to gain unauthorized access into restricted areas. This enhances the security infrastructure by providing immediate visual evidence and timely alerts. Some of the major components in the design included: The Camera Module was used for real-time picture capture. ESP32 Microcontroller controlled the camera, processed images, and handled communication. The communication module used for sending notifications to security personnel was the IoT gateway, and it alerts the security personnel through various channels (e.g., SMS, email, telegram app, and security monitoring system and so on). However, this work specifically used the telegram application as the notification medium between the system and the user. The block diagram of the real-time picture capture and notification unit is represented in figure 3.4. To achieve this, the ESP-32 CAM was used to take pictures of events in real time, process these pictures and then send out a notification of its identification. Notifications are messages used on devices that alert users to information that are important. The notification feature of this thesis will be able to notify its users of the motion detected. The computer-based system we are using in this case is the ESP-32 controller, its main use will be to execute and control all the features of this system from within. The methods were adopted in achieving the specific objectives in chronological order:

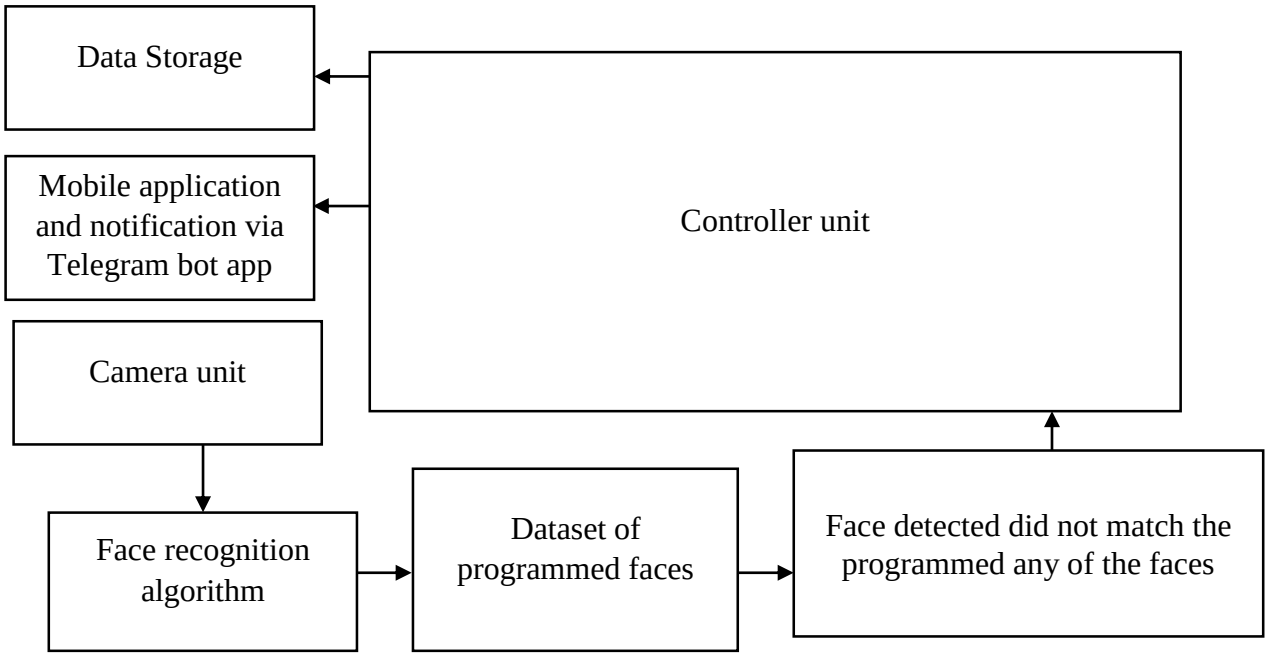

Figure 3.4: The block diagram of the real-time picture capture and notification unit

The implementation of a real-time picture capture and notification sub-system significantly enhanced the security aspect of this design by providing immediate visual verification and timely alerts of unauthorized access attempts. It leverages IoT gateway technology to ensure prompt and effective response, thereby safeguarding restricted areas against potential security breaches. Figure 3.5 shows a clearer view of the design in a flowchart.

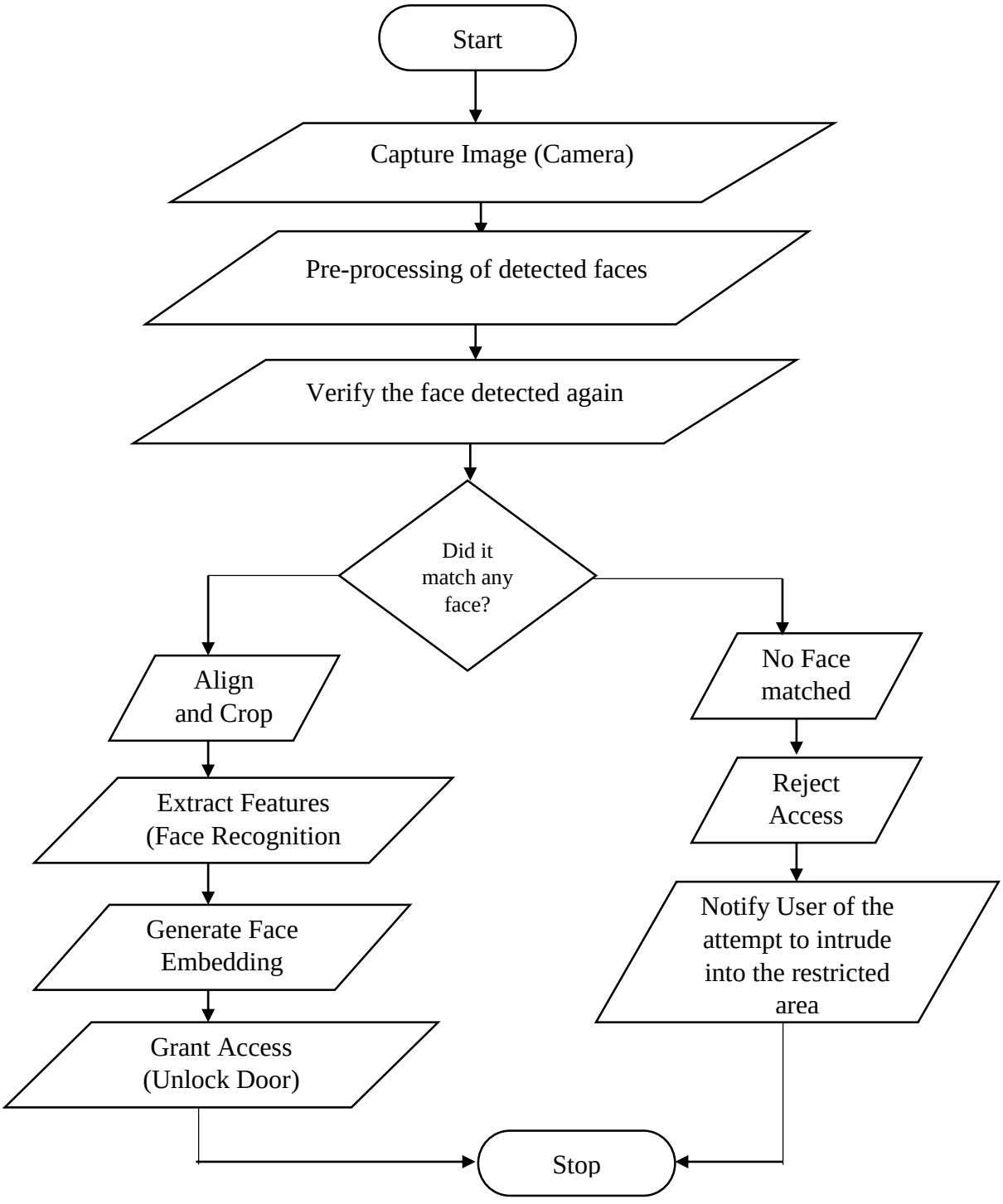

Figure 3.5: The flowchart of the real-time picture capture and notification

iii. Implementation of a digital and editable password input panel that can automatically trigger a digital camera by the system algorithm

The implementation of a digital and editable password input panel that could automatically trigger a digital camera through the system algorithm enhanced the security and usability of the face recognition capability of this system. The integration provided a dual authentication mechanism, combining facial recognition with a password entry to ensure robust access control.

Design and Functionality: Digital Password Input Panel

The digital password input panel serves as an additional layer of security. It was designed to be user-friendly, allowing users to input a password using a keypad interface. The panel was fully editable, enabling users to change their passwords periodically to maintain security.

Automatic Camera Trigger:

The system algorithm was configured to automatically trigger the digital camera when either the correct or incorrect password was entered. This ensured that every access attempt was documented with a time-stamped image, enhancing security and providing a visual log of entries and exits. Figure 3.6 shows the password subunit of the system. It gives room for the user to edit password at any time making the system more secured.

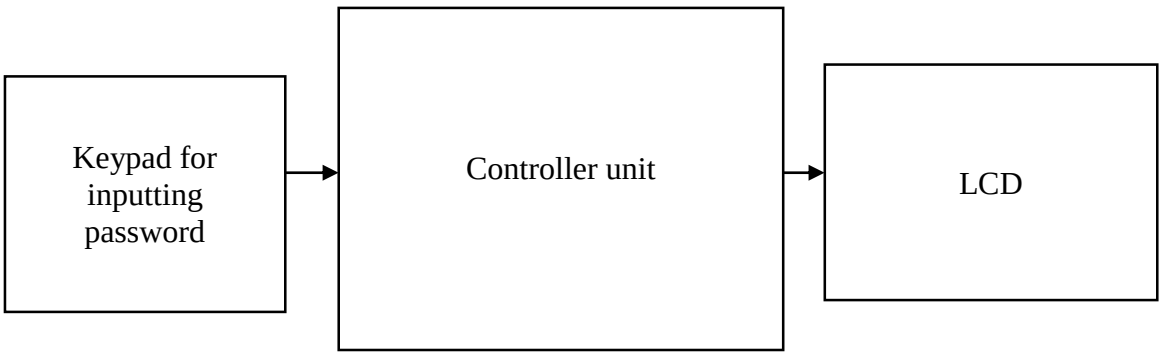

Figure 3.6: The block diagram of the password unit

3.2.2 Design Procedures of the printed circuit board (PCB):

EasyEDA is a user-friendly online platform for designing electronic circuits. The following basic steps were taken in the PCB design of this work:

1. **Creation of EasyEDA Account**: this was done through the easyEDA. A functional email address was required to create the account.

2. **Started a New Project**: Once logged in, a new project was started by clicking on the "Create a New Project" button. A was given to the project and description to keep it organized.

3. For **Schematic Design**:

i. Clicked on the "Schematic" and the circuit design was initiated.

ii. The needed electronic components were dragged and dropped from the sidebar onto the canvas, which was done through the search bar for specific components. The Components were connected by clicking on the pins of the selected component dragging a wire to the pin of another component, and so on. EasyEDA would automatically connect them.

4. **Simulated the Circuit**: EasyEDA allows one to simulate a circuit to test its functionality.

5. **PCB Layout:** this was done by clicking on the "Convert Project to PCB" button to transfer the entire schematic to the PCB layout.

Figure 3.6 shows the EasyEDA design interface, where the individual components used in this work were carefully selected according to the specifications in Table 3.1.

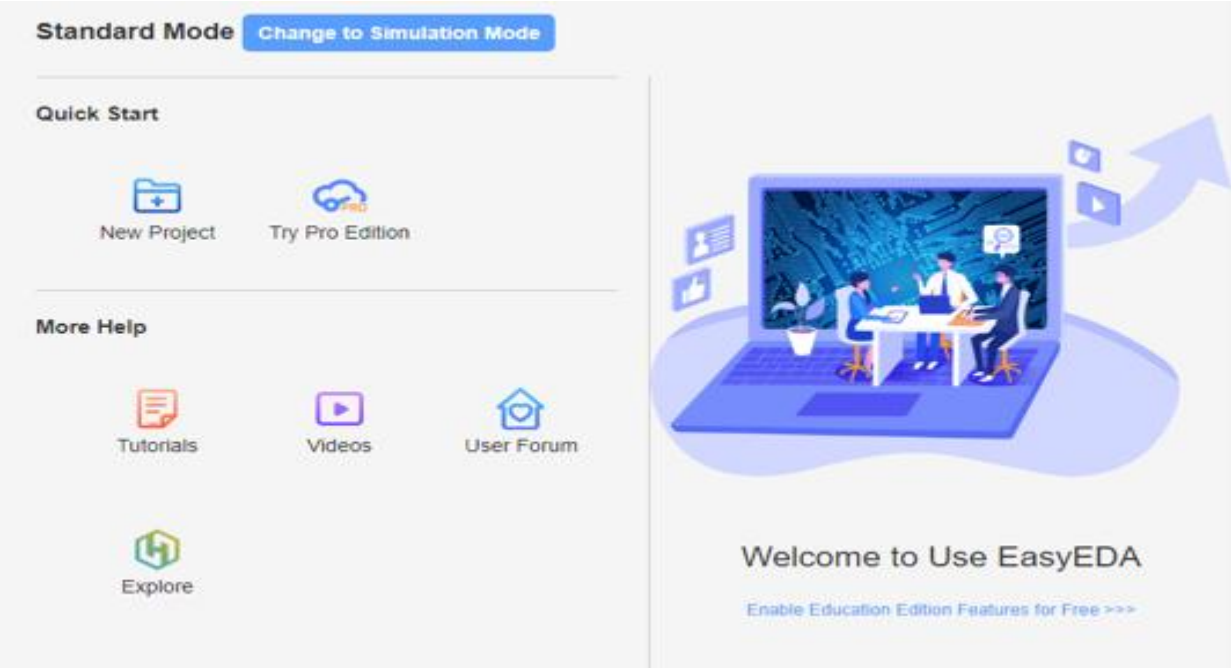

Figure 3.6: IFRSACS System PCB Design Interface (Component selection page)

Figure 3.7 shows the power supply circuit which was later routed in figure 3.8 to get a workable PCB result. Both the drawing and the wiring tools were used to pick and connect each component accordingly. Once saved, the EasyEDA server automatically any changes made during the design and can retrieved any time in the nearest future if need be.

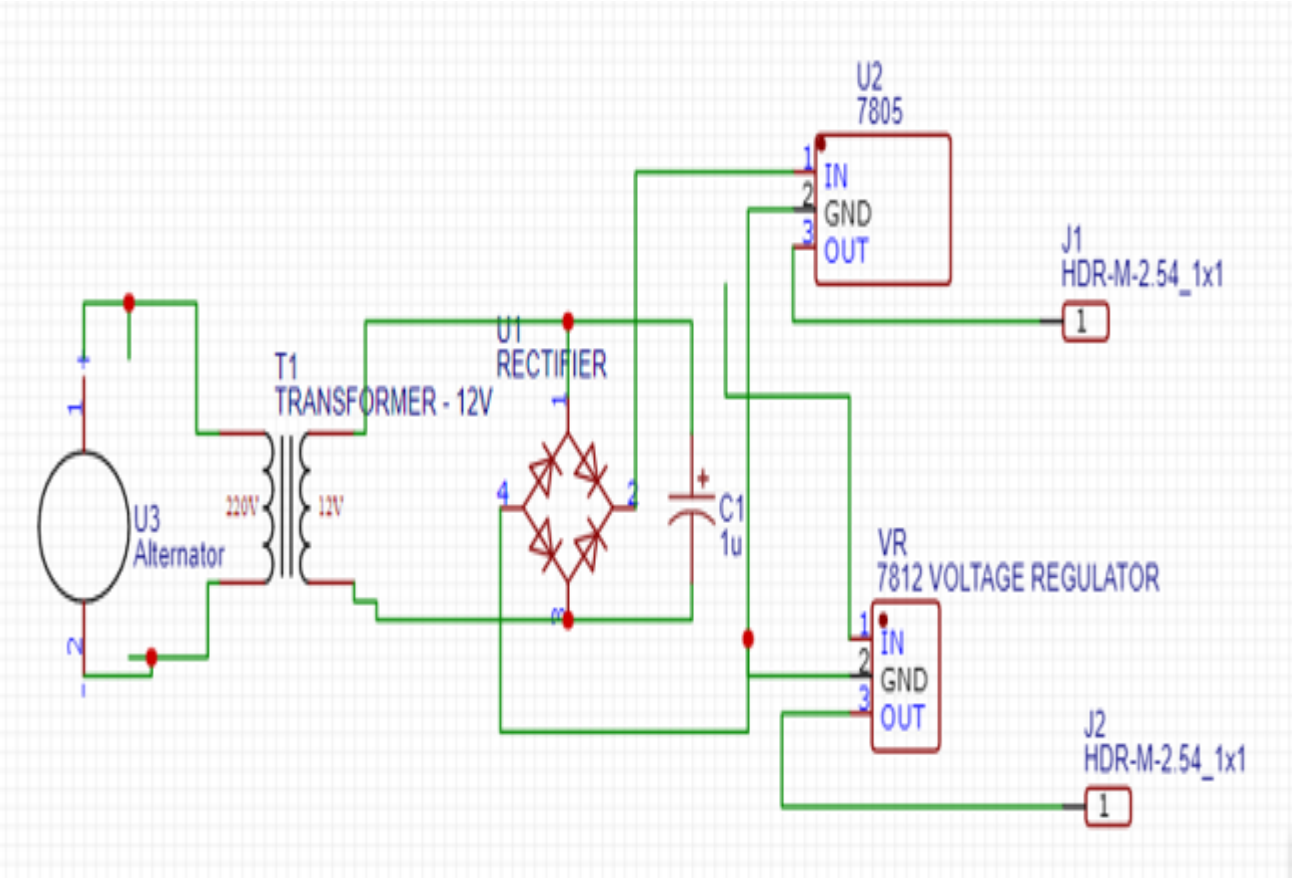

Figure 3.7: IFRSACS System PCB Design Interface (Schematic page Power Supply Unit)

Figure 3.8 shows the ESP32 Camera and the power supply circuit which was later routed according to Plate 3.6 to get a workable PCB result. The wire, Bus entry, netflag and other wiring tools were used to pick and connect each component in similar ways as in Figure 3.8 After which, updates were saved online via the server. This simply means that the whole PCB design of this thesis can be easily retrieved anytime in the future.

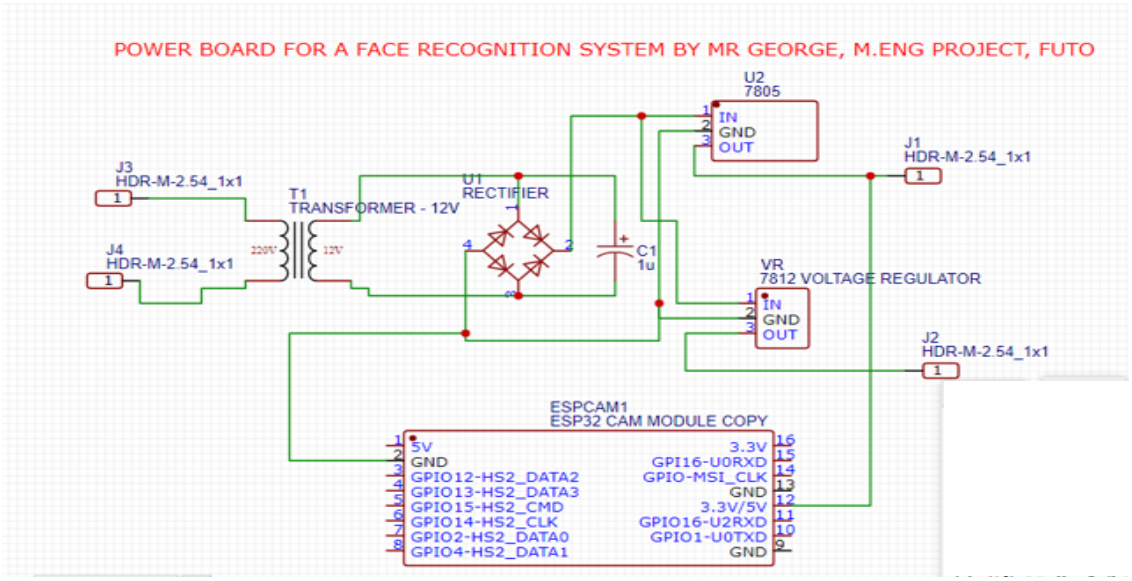

Figure 3.8: IFRSACS System PCB Design Interface (Schematic page for ESP32 CAM +

Figure 3.9 shows the routing stage of the circuit board design. The simple steps below were followed in routing the components. The auto router button from the Top Menu"Top Menu> Route > Auto Router" Config the auto router. After which, the configuration dialogue box was selected and hit the Run it button.

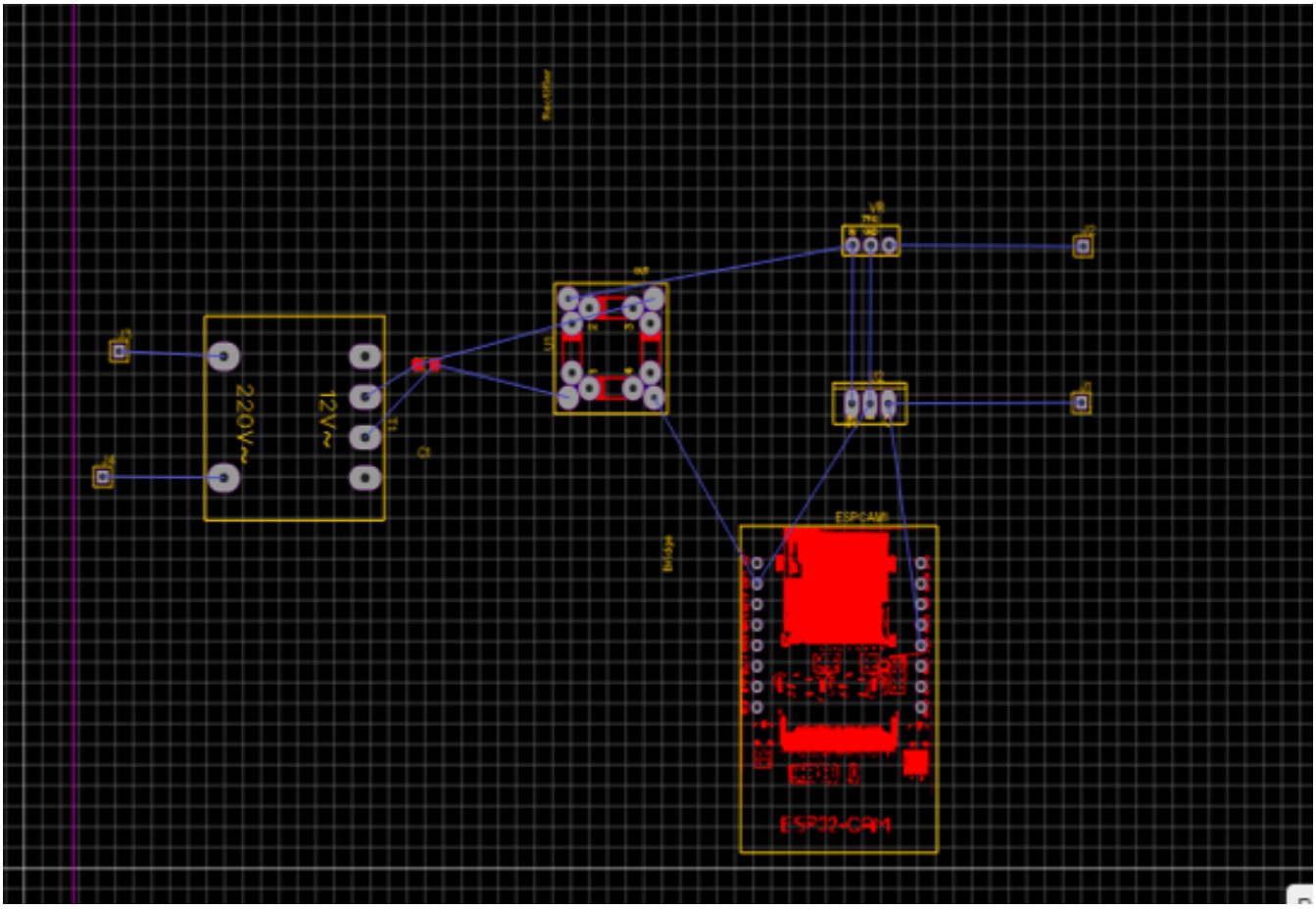

Figure 3.9: IFRSACS System PCB Design Interface/Schematic/Routing page for ESP32 CAM + Power Supply

Figure 3.10 shows the 2-dimensional view of the PCB designed in the EasyEDA environment. It made the placement of the electronic components than using usual vero board. The 2D view was achieved after converting the PCB to Photo View, resulting in the appropriate and actual appearance of the system circuit board. It was generated automatically by the server which makes EasyEDA a good PCB tool for effective online designs.

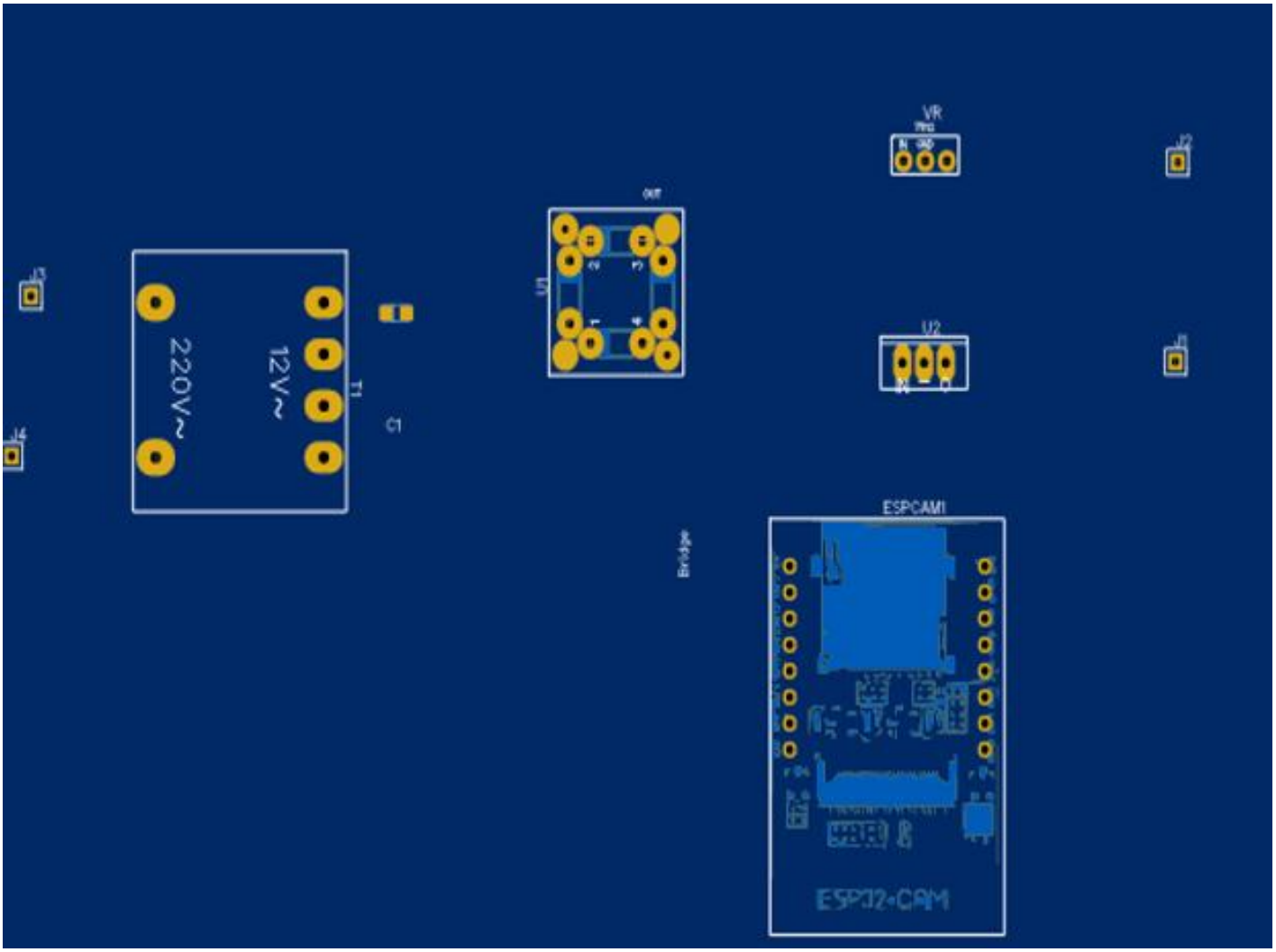

Figure 3.10: IFRSACS System PCB Design Interface (2D View of the PCB Layout)

Figure 3.11 shows the 3-dimensional view of the PCB designed in the EasyEDA environment. The 3D view was achieved after converting the PCB to Photo View, resulting in the appropriate and actual appearance of the system circuit board. It was generated automatically by the server which makes EasyEDA a good PCB tool for effective online designs.

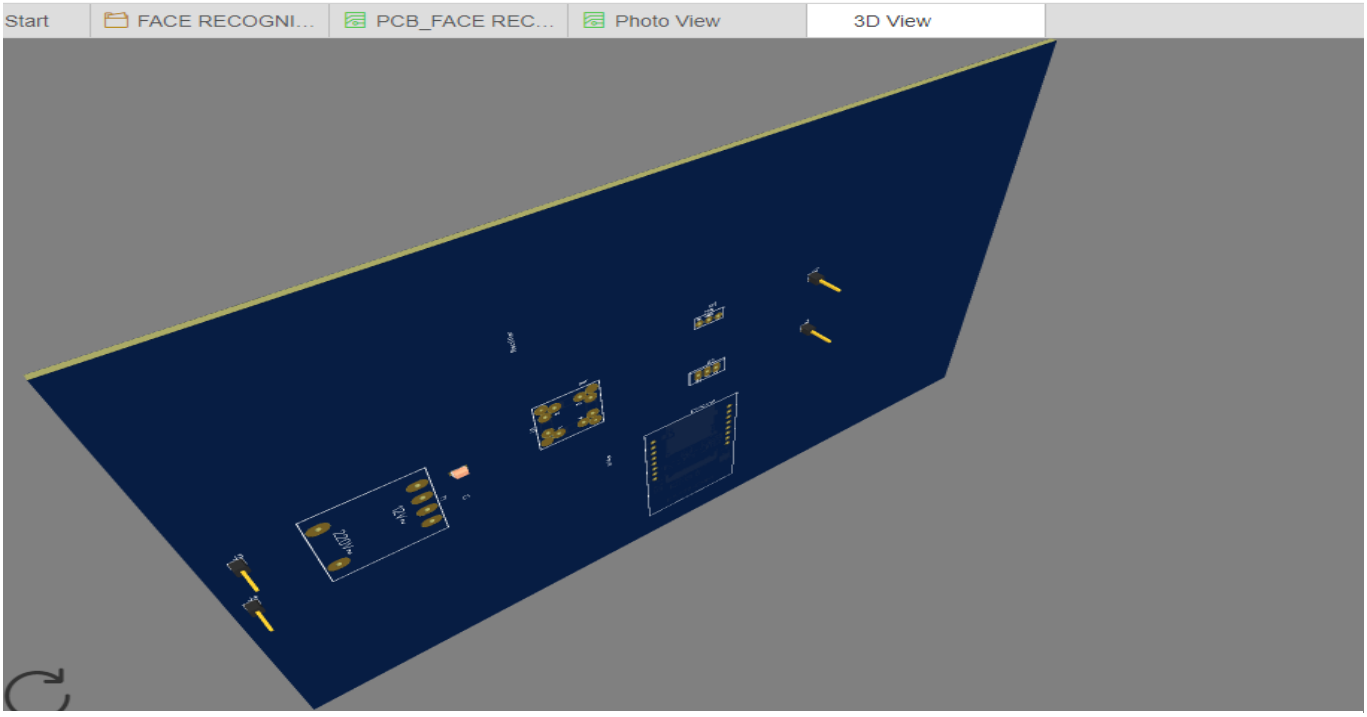

Figure 3.11: IFRSACS System PCB Design Interface (2D View of the PCB Layout)

3.2.3 Methodology used in the Development of the face recognition and access control system

In the design of this access control system, encryption parameters were used to create the password needed to enter/exit; or deny entry to unauthorized persons into a place of contraband material, such as weapons, explosives, and tools, or the entry or exit of any other material restricted by security management. Encryption scrambles the password so it's unreadable and/or unusable by hackers. It offers more protection as the password as it is usually concealed on the screen.

The implementation of the system involved the following key steps:

a. Face Detection and Recognition: Utilizing the ESP32's computational power, a face detection and recognition algorithm was developed to accurately identify individuals based on captured images.

b. Database Management: In this case, telegram application was used as the gateway between the machine and the user.

c. Integration with Door Lock: The facial recognition system was integrated with the door lock mechanism to enable automatic access control based on recognized individuals.

3.2.4 System block diagram

The system consists of different subunits such as indicated in the block diagram in figure 3.2.

The principle of operation of a face recognition door lock system using ESP32 CAMERA involves a combination of hardware components and software algorithms to capture, process, and compare a user's facial features with stored data in order to grant or deny access to a secure area. Here is an overview of how the system works:

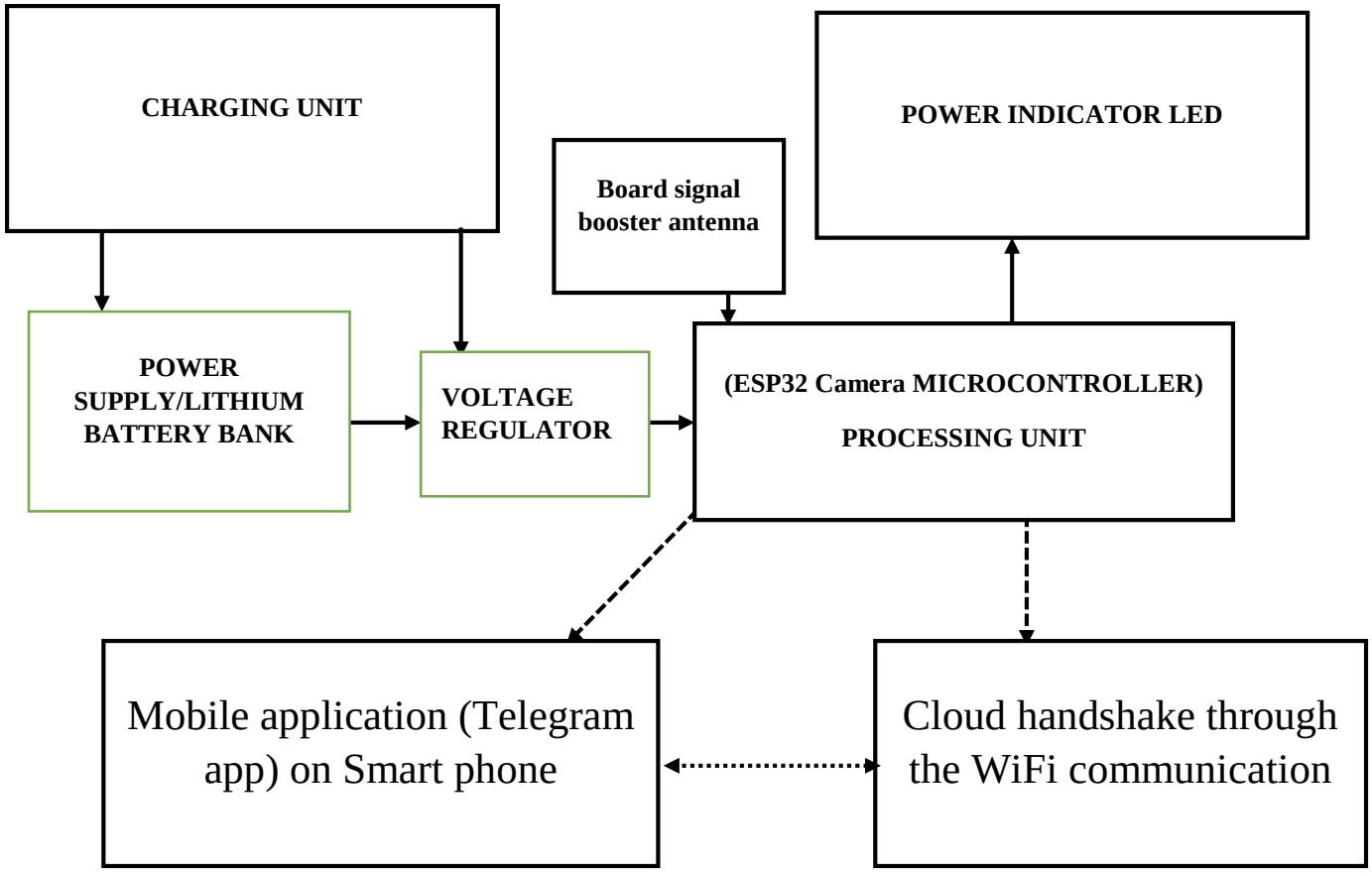

Figure 3.2: The Block Diagram of IPCSACS

3.2.4 Operation sequence and system flowchart

1. Enrolment: During the enrolment phase, authorized users' faces are captured and stored along with their unique facial features in the system's database using a computer system.

2. Face Detection and Feature Extraction: When a user approaches the door, the camera captures an image of their face. The system then detects the face within the image and extracts the relevant facial features.

3. Face Recognition: The extracted facial features are compared to the stored data in the system's database. If a match is found, the system authenticates the user as an authorized individual.

4. Access Control: If the user is authenticated, the system triggers the door lock mechanism to grant access. If not, access is denied.

Generally, a face recognition door lock system using ESP32 CAMERA offers a sophisticated and secure method for controlling access to a physical space, leveraging the capabilities of microcontrollers, cameras, and advanced facial recognition algorithms.

3.2.5 SYSTEM FLOWCHART

The following is the simplified system algorithm of the IoT sub-system:

i. The system first turns on
ii. the system initializes the input/output pins of the ESP32 Camera controller
iii. the scans for available networks in its vicinity and gets connected if the available network has the same network credentials as the ones programmed into the WiFi controller.
iv. gets its input or output pins ready for easy communications on the mobile application
v. now ready to respond to the mobile application page on the user’s smartphone

vi. Now the system is ready to respond to the online notification if the user enters a wrong password as predefined in the specific objectives.

vii. Likewise, the state of the electronic door is monitored on the smartphone.

viii. The loop repeats over and over, except otherwise, maybe disconnected from the power source. The flowchart of the system is shown in figure 3.3.

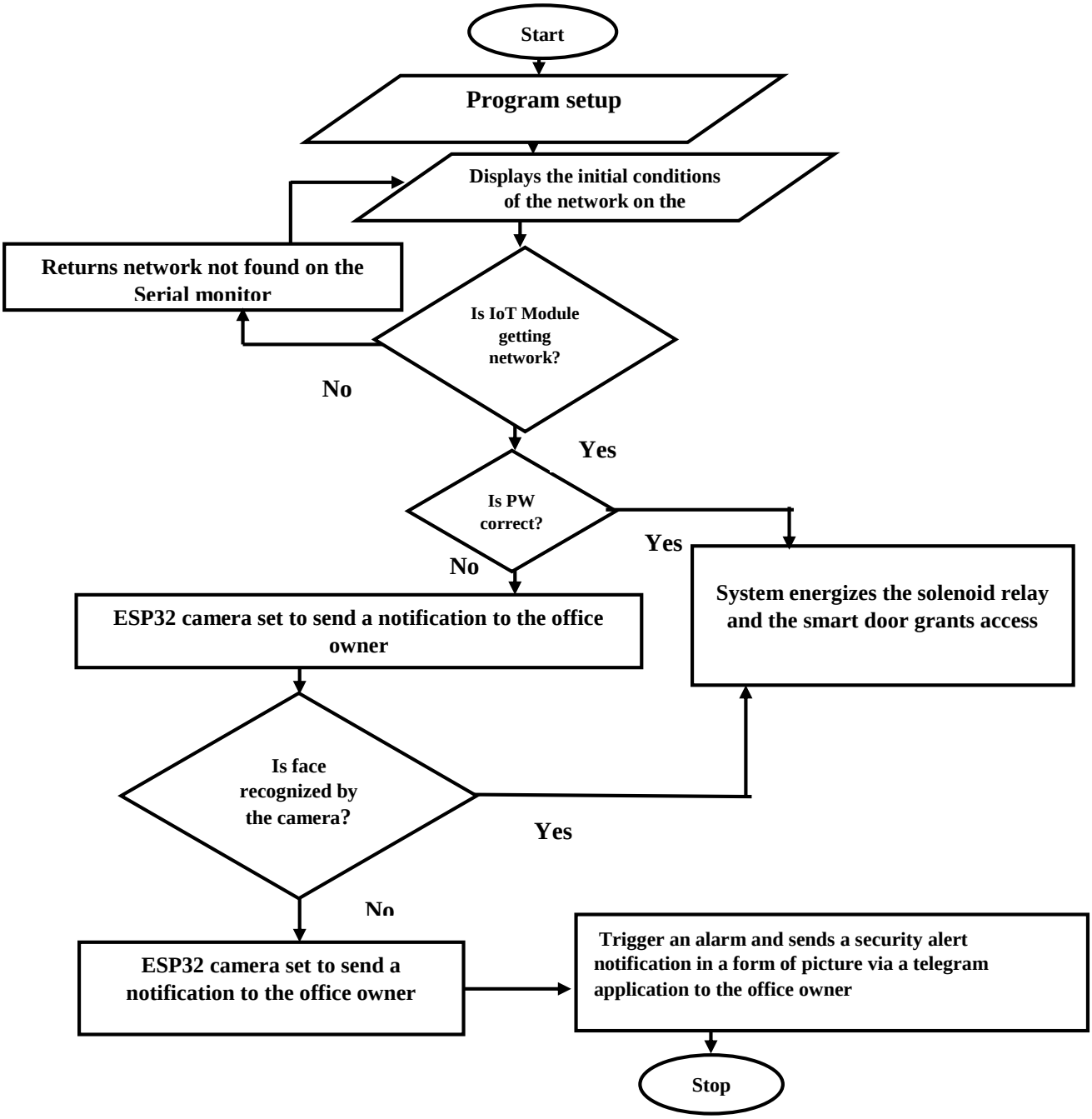

Figure 3.3: System Flowchart

3.2.6 Biasing Resistor value and Transistor calculations

BC547 has two operation statuses: forward bias and reverse bias. In the status of the forward bias, the current can pass when the collector and emitter are connected. While in the status of the reverse bias, it acts as a disconnect switch and current cannot pass. BC 547 common-emitter current gain and the associated calculations:

From the datasheet of the BC547 NPN transistor:

The following values were obtained;

(i) Emitter current = I_E = -100mA

(ii) Base current = I_B = 20mA

(iii) Collector current = I_C = 100mA

(iv) Base-Emitter Voltage = V_{BE} = 0.7v

Calculating the gain factor (β) of the NPN transistor used:

Recall:

$$\text{Gain factor } (\beta) = \frac{I_C}{I_B} \qquad \textbf{(3.1)}$$

$$= \frac{100 \times 10^{-3}}{20 \times 10^{-3}} = 5$$

This implies that an input current to the emitter will have a gain factor of 5.

This is enough to switch the DC relay in the circuit.

Finding the relationship of collector current (output current) to emitter current (input current) known as α. It's calculated thus;

$$\alpha = \frac{\Delta I_C}{\Delta I_E} \text{ or } = \frac{\beta}{\beta + 1} \quad \textbf{(3.2)}$$

Therefore $\alpha = \frac{\beta}{\beta+1} = \frac{5}{5+1} = \frac{5}{6} = 0.83$

This implies that the input current at the emitter reached the collector at 83% output current to input current.

To find the accurate value for the biasing resistor connected at the base of the transistor, Plate 3.9 was used in accordance with the associated equations.

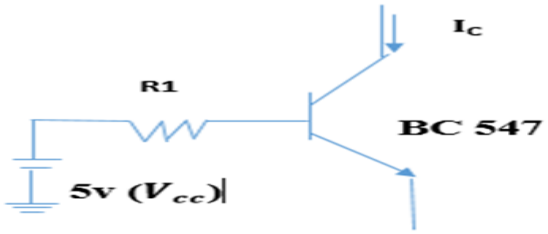

Plate 3.9: Relay Switching transistor (BC 547)

Recall Ohm's law;

$$V = IR \quad \textbf{(3.3)}$$

Base-emitter of BC 547 transistor = 0.7v (Datasheet). That is V_{BE} = 0.7v

$$\text{The voltage across R1 resistor} = \frac{V_{CC-V_{BE}}}{I_B} \quad \textbf{(3.4)}$$

$$= \frac{5v-0.7v}{20\,x \times 10^{-3}}$$

$$= \frac{4.3}{20 \times 10^{-3}}$$

$$= \frac{4.3}{2}\, x\, 10^2$$

$$= 2.15 \times 10^2$$

$$= 215\Omega.$$

The biasing resistor value is 215Ω, approximately 220Ω which is commonly available in the market.

3.2.7 Power Consumption Calculation

Power consumption is a fundamental metric that quantifies the amount of electrical power used by a device over time. For the ESP32 CAMERA module used in the system, the power consumption was calculated using the following considerations:

i. **Voltage and Current Requirements**: The ESP32 CAMERA module operates with specific voltage and current requirements, typically supplied by a power source such as a battery or a regulated power supply unit (PSU), which in this work, PSU was used.

ii. **Operational Modes**: Devices like the ESP32 CAMERA often operate in different modes (e.g., sleep mode, active mode, transmit/receive mode), each consuming varying amounts of power. The power consumption may differ significantly depending on the operational state.

iii. **Power Calculation Formula**: The general formula for power consumption used:

a. $P_{consumption}=V_{ESP32}\times I_{ESP32}$

b. Where:

V_{ESP32} was the operating voltage supplied to the ESP32 CAMERA module and I_{ESP32} was the current drawn by the ESP32 CAMERA module.

Real-World Considerations: To accurately determine power consumption, it was essential to measure the following:

Operating Voltage of ESP32 CAM: The voltage supplied to the ESP32 CAMERA module, typically ranges from 3.3V to 5V(Putra & Setyawan, 2021).

Current Consumption of ESP32 CAM: ESP32 CAM's current consumption is 180mA(Putra & Setyawan, 2021) ;

Idle State: When the module is idle, waiting for input or in a low-power sleep mode, the current consumption is minimal but not negligible.

Active State: During face recognition processing, image capture, and communication tasks, the module draws higher currents.

Peak Loads: Transmitting data wirelessly (e.g., via Wi-Fi or Bluetooth) or activating peripherals like the camera module may cause temporary spikes in current consumption.

1. **Energy Efficiency Optimization**: Optimizing firmware, minimizing unnecessary wake-ups, and utilizing low-power modes when feasible can enhance overall energy efficiency and prolong battery life in battery-operated systems.

The ESP32 CAMERA module operates at 5V and consumes 180mA (milliamps) during active operation (e.g., image processing and wireless communication):

ESP32 CAM's current consumption = 180mA;

ESP32 CAM voltage rating = 5v:

Pconsumption=5V×0.18A=0.9W

Therefore, the power consumption of the ESP32 CAM module, operating at 5V and consuming 180mA of current, was approximately 0.9 watts. The calculation provided a more accurate estimate of the power consumption for the ESP32 CAM module during active operation.

3.2.8 Facial Recognition Accuracy Calculation:

$$\text{Accuracy} = \frac{Number\ of\ correct\ recognitions}{Total\ number\ of\ attempts}\ x\ 100\% \quad (3.5)$$

Equation 3.5 quantified the accuracy of the face recognition system based on the number of successful recognitions made.

To calculate the accuracy of a facial recognition system, the system performance based on several metrics, such as True Positives (TP), False Positives (FP), True Negatives (TN), and False Negatives (FN) was evaluated. The following step-by-step approaches and terminologies were maintained in calculating facial recognition accuracy:

i. True Positives (TP)**:** Number of correctly recognized faces.

ii. False Positives (FP)**:** Number of faces incorrectly recognized as authorized.

iii. True Negatives (TN)**:** Number of correctly rejected unauthorized faces.

iv. False Negatives (FN)**:** Number of authorized faces incorrectly rejected.

Accuracy Formula:

$$\text{Accuracy}=\frac{TP+TN}{TP+TN+FP++FN} \tag{3.6}$$

Precision and Recall:

Precision: Measures the accuracy of positive predictions.

$$\text{Precision} = \frac{TP}{FP+TP} \tag{3.7}$$

Recall (Sensitivity): Measures the ability to find all relevant instances.

$$\text{Recall} = \frac{TP}{FN + TP} \tag{3.8}$$

$$\textbf{False Positive Rate} = \frac{\text{FP}}{FP+TN} \tag{3.9}$$

F1 Score: The F1 score is the harmonic mean of precision and recall, providing a single metric for the system's accuracy.

$$\text{F1 Score} = 2\,x\,\frac{Precision \times RecallPrecision}{Precision + RecallPrecision} \quad (3.10)$$

3.2.7 Signal-to-Noise Ratio (SNR) Calculation:

$$\text{SNR} = \frac{Signal\ PowerNoise\ Power}{Noise\ PowerSignal\ Power} \quad (3.11)$$

Equation 3.10 evaluated the quality of the signal relative to the background noise, crucial for assessing system performance.

3.3 SYSTEM CIRCUIT DIAGRAM

The Circuit Diagram for the ESP32-CAM Faces Recognition Door Lock System is combined with an FTDI board, Relay Module, and Solenoid Lock. The FTDI board is employed to flash the code into ESP32-CAM because it doesn't have a USB connector while the relay module is employed to modify the Solenoid lock on or off. The door lock system using an ESP32 CAMERA includes several components that work together to provide security and access control. Here's a basic circuit diagram explanation for the system: the system circuit is shown in Plate 3.4.

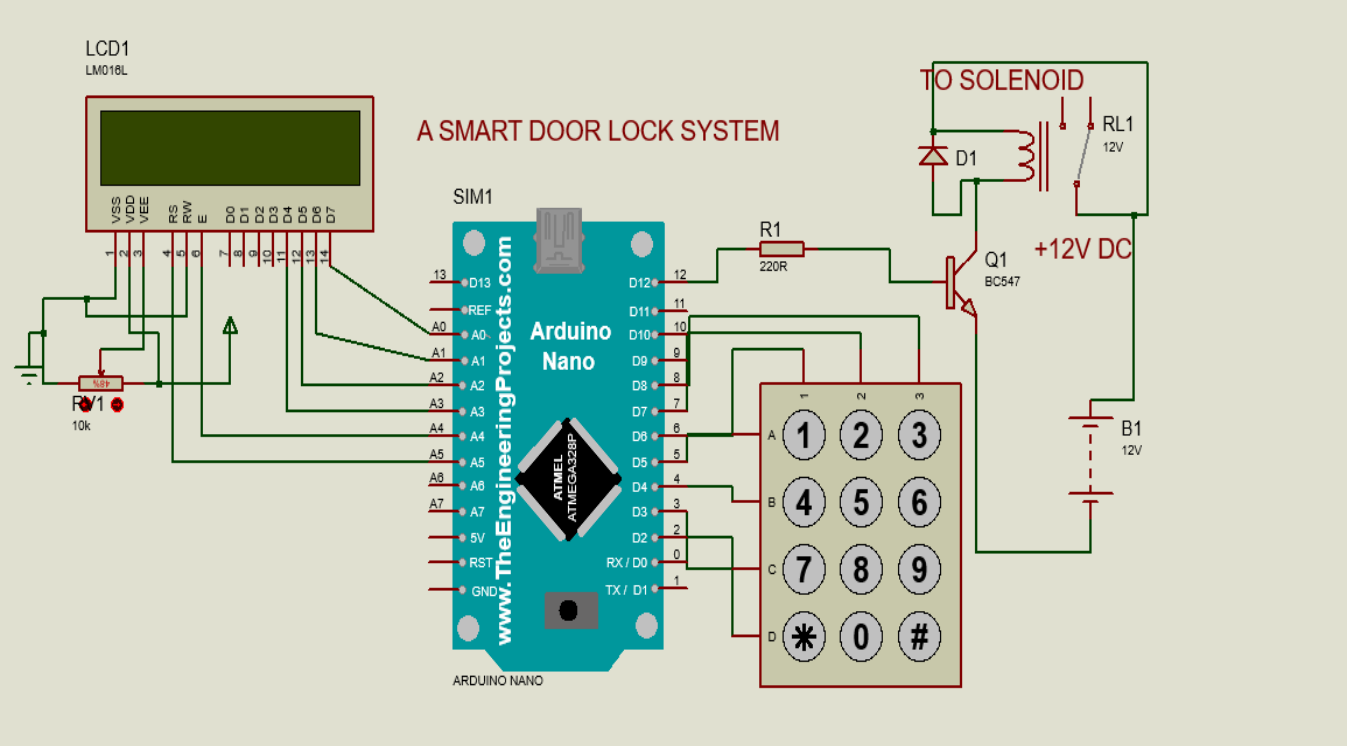

Plate 3.10: A Smart door lock system circuit diagram

3.4 Connection Method between the Esp32 Camera Module and the FTDI Programmer (Programming circuit)

Here the ESP32-CAM board was accessed via a local network. The phone hotspot/router acted as the access point and the ESP32-CAM board was configured as a station. Then connected to a local network to control and access the ESP32-CAM through a web server. The network access point was routed in such a way that the ESP32-Cam module could integrate with WiFi connectivity allowing it to send photos in real time, the module consists mainly of a microprocessor that behaves like an Arduino, for this reason, it was really easy programming it through the Arduino software.

Plate 3.11 shows the programming circuit of the Internet Protocol Camera and the (Future Technology Devices International) FTDI Programmer. Description: The FTDI cable is a USB to Serial Transistor-transistor logic (TTL level) converter which allows for a simple way to connect TTL interface devices to the universal serial bus (USB). The I/O pins of this FTDI cable are configured to operate at 5V. The FTDI cable is designed around an FT232RQ, which is housed in a USB A connector. There is a cross-connection between the two modules/devices viz; the Transmitter (TX) of the ESP32 CAM was connected to the receiver (RX) pin of the FTDI programmer. Similarly, the Transmitter (TX) of the FTDI was connected to the receiver (RX) pin of the ESP32 CAMERA module. Then, the Vcc (5V) of the ESP32 CAMERA was connected to the Vcc (5V) of the FTDI programmer. The GND of both modules were connected together.

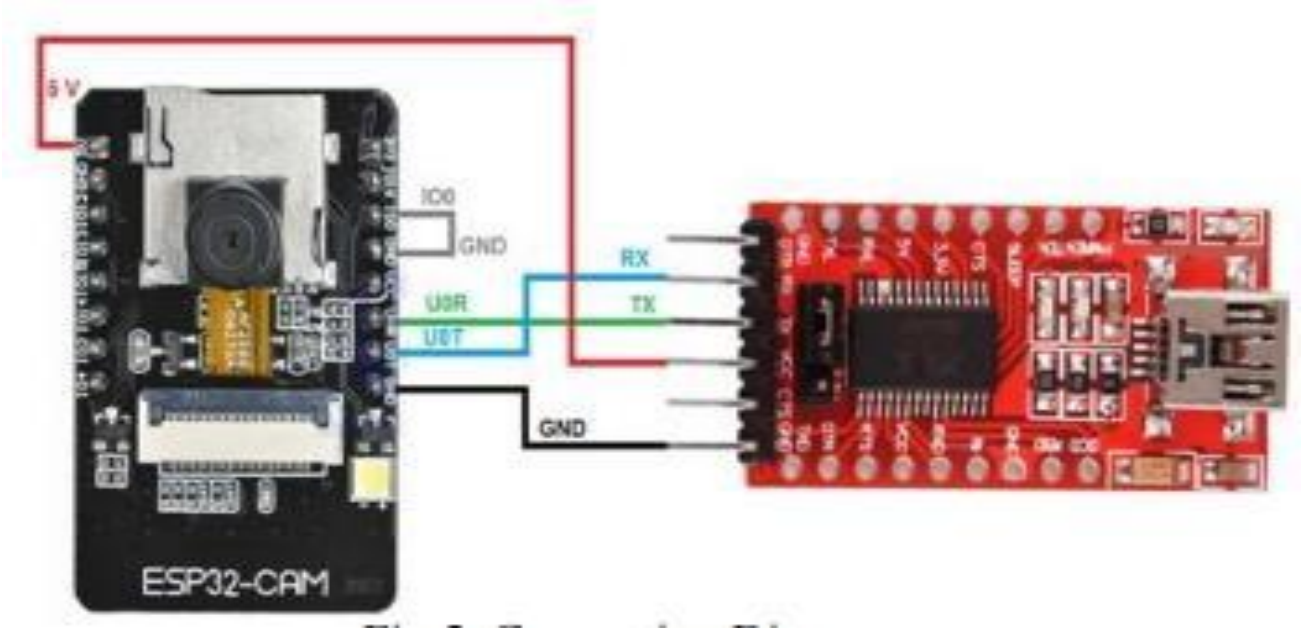

Plate 3.11: Esp32 Camera Module and the FTDI Programmer

3.5 Implementation and Testing

After completing the stages of Requirements Gathering, Analysis, and Design, the next step is Implementation. During this phase, the deliverable product is built. For the software aspect of the system, this involves translating the solution domain into source code, implementing the attributes and methods of each object, and integrating them into a single system. On the other hand, for the hardware aspect of the system, the system sub-units were implemented on an ESP32 CAM and connected to the Cloud. The system was also paired with a mobile application that sends commands to it. Finally, an electric actuator (solenoid lock) was used for the mechanical engineering aspect of the system. The implementation and testing are shown in Plates 3.13 and 3.14 respectively. Plate 3.12 shows the stream of photos (64) saved in EEPROM of the microcontroller which was used as the basics for face recognition. If the face of the intending user matches with any of the 64 photos/faces, the system automatically grants access by energising the relay and the solenoid lock opens.

Plate 3.12: 64 photo signatures used on the system for the face recognition configuration

Plate 3.13 shows the implementation stage where each unit such as the keypad for password, solenoid lock, was tested, confirmed working perfectly, before connecting them together to form the complete system. At first, it displays a welcome message with the name of the device and then prompts the user to key in the correct password after the face has been recognized. Access is granted when both face recognition and password are validated.

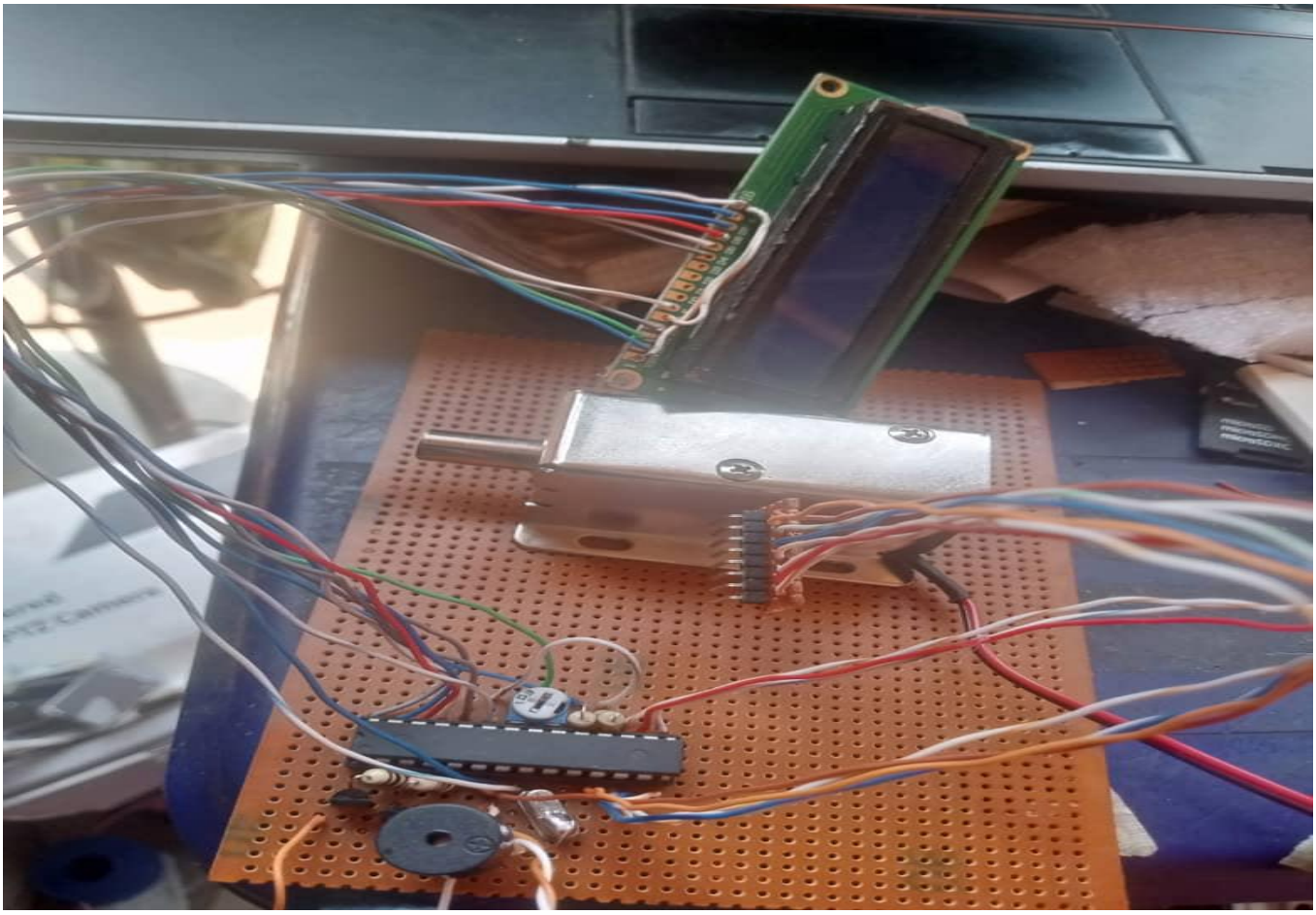

Plate 3.13: Implementation stage of the door lock system

Plate 3.14 shows the working mode of the during the system testing. At first, it displays a welcome message with the name of the device and then prompts the user to key in the correct password after the face has been recognized. Access is granted when both face recognition and password are validated.

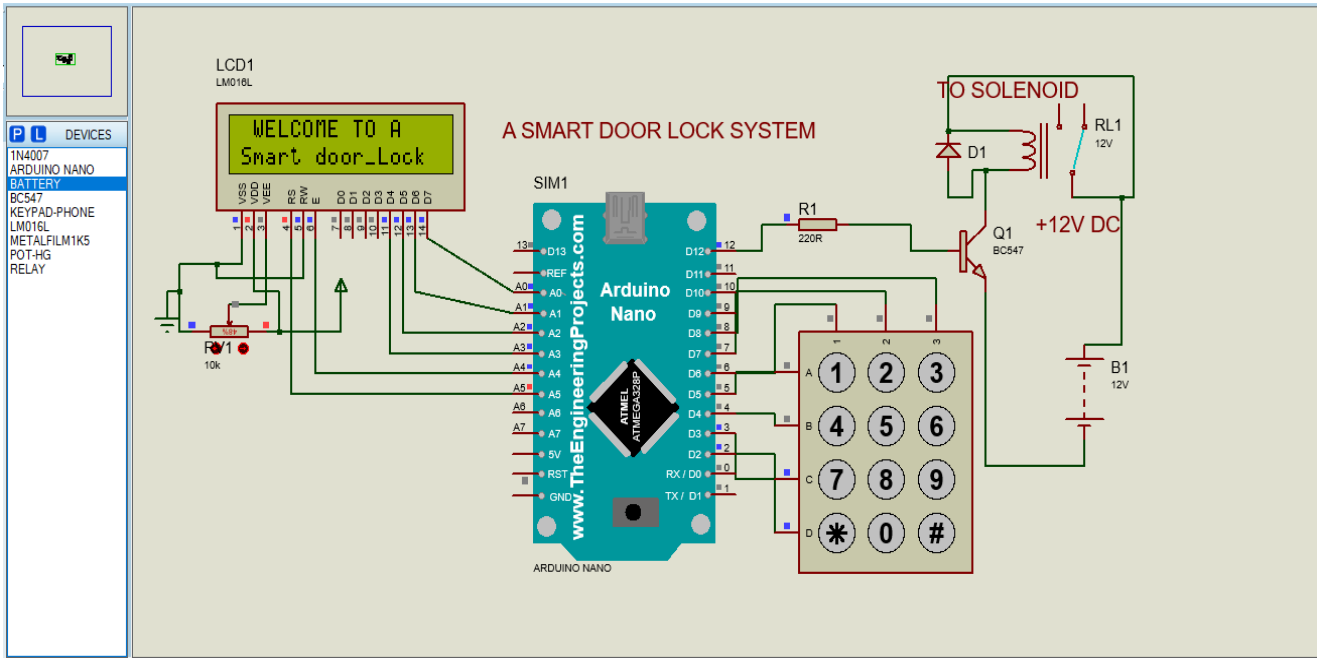

Plate 3.14: A Working circuit diagram of the smart door lock system

3.6 System Test(s)

When the system was tested, the following results were obtained using the Arduino IDE environment:

True Positives (TP): 90

False Positives (FP): 5

True Negatives (TN): 80

False Negatives (FN): 10

Recalling equations 3.6 to 3.9, the following calculations were carried out accordingly:

$$\text{Accuracy}=\frac{90+80}{90+5+80+10}=91.9\%$$

Precision and Recall:

Precision: Measures the accuracy of positive predictions.

Precision = $\frac{90}{90+5} = 94.7\%$

Recall (Sensitivity): Measures the ability to find all relevant instances.

Recall = $\frac{90}{90+10}$ = 90%

False Positive Rate was calculated as:

False Positive Rate = $\frac{5}{5+80}$ = 5.26%

F1 Score: The F1 score is the harmonic mean of precision and recall, providing a single metric for the system's accuracy.

F1 Score= $2\ x\ \frac{0.947 \times 0.947}{0.947+ 0.947}$ = 92.2%

Based on the sample data:

Accuracy: 91.9%

Precision: 94.7%

Recall: 90%

F1 Score: 92.2%

These metrics provided a comprehensive view of the facial recognition system's performance. High precision indicated a low false positive rate, and high recall indicated a low false negative rate. The F1 score balanced both precision and recall, offering a single measure of overall accuracy. The results obtained were discussed in chapter four of this work.

CHAPTER FOUR

RESULTS AND DISCUSSIONS

4.1 Results:

The implementation of a face recognition door lock system using ESP32 CAMERA has demonstrated promising results in terms of accuracy, efficiency, and practicality. Through a series of tests and evaluations, the system has shown a reliable capability to recognize and authenticate individuals based on facial features captured by the ESP32 CAMERA module. The integration of ESP32, a powerful microcontroller with built-in Wi-Fi and Bluetooth connectivity, combined with a camera module capable of capturing and processing images, has enabled the development of a compact and versatile face recognition solution suitable for diverse access control applications.

The experimental results have indicated high accuracy in facial recognition, with the system successfully identifying authorized individuals and denying access to unauthorized persons. The performance evaluation under various lighting conditions and environmental factors has showcased the robustness of the system, indicating its suitability for real-world deployment. Furthermore, the response times for authentication have been within acceptable limits, ensuring a smooth and efficient user experience. These results validate the practicality and effectiveness of leveraging ESP32 CAMERA for implementing a face recognition door lock system. Plate 4.1 shows the Serial monitor page of the smart door lock and the telegram dashboard.

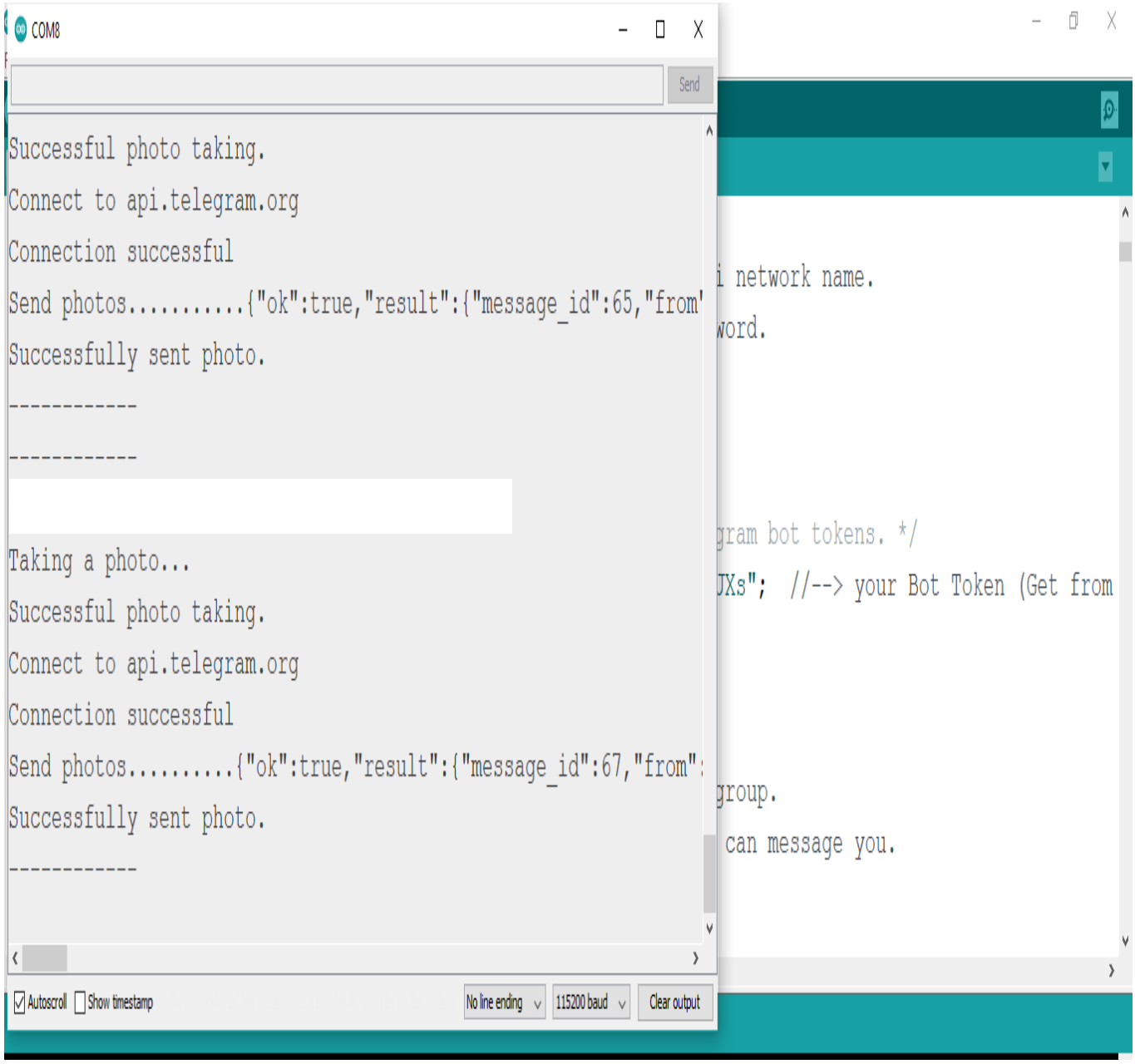

Plate 4.1: Serial monitor and Telegram page showing ESP32 camera taking picture intruders

Plate 4.2 shows the complete system in testing mode. It prompts the user to look at the camera eye and if successfully validated, it quickly prompts the user to enter the correct password.

Plate 4.2: A Smart door lock system showing power up state

Plate 4.3 shows the complete system in operation mode. The camera validates the user's face and then quickly prompts the user to enter the correct password. And when the correct password was entered, the system granted the user access. After five (5) seconds, the door locks again and expects the next user tom follow the aforementioned prompts to gain access. It is also shown in Plate 4.3 where the solenoid lock was switched on and access was granted.

Plate 4.3: The smart door lock in operation showing access granted

Plate 4.4 shows the photo captured and sent to the telegram application of the office owner as a security alert. It was observed that whenever the system recognized any of the faces as programmed, it then prompted for a password verification, and when that failed, a security alert message was sent automatically to the concerned person.

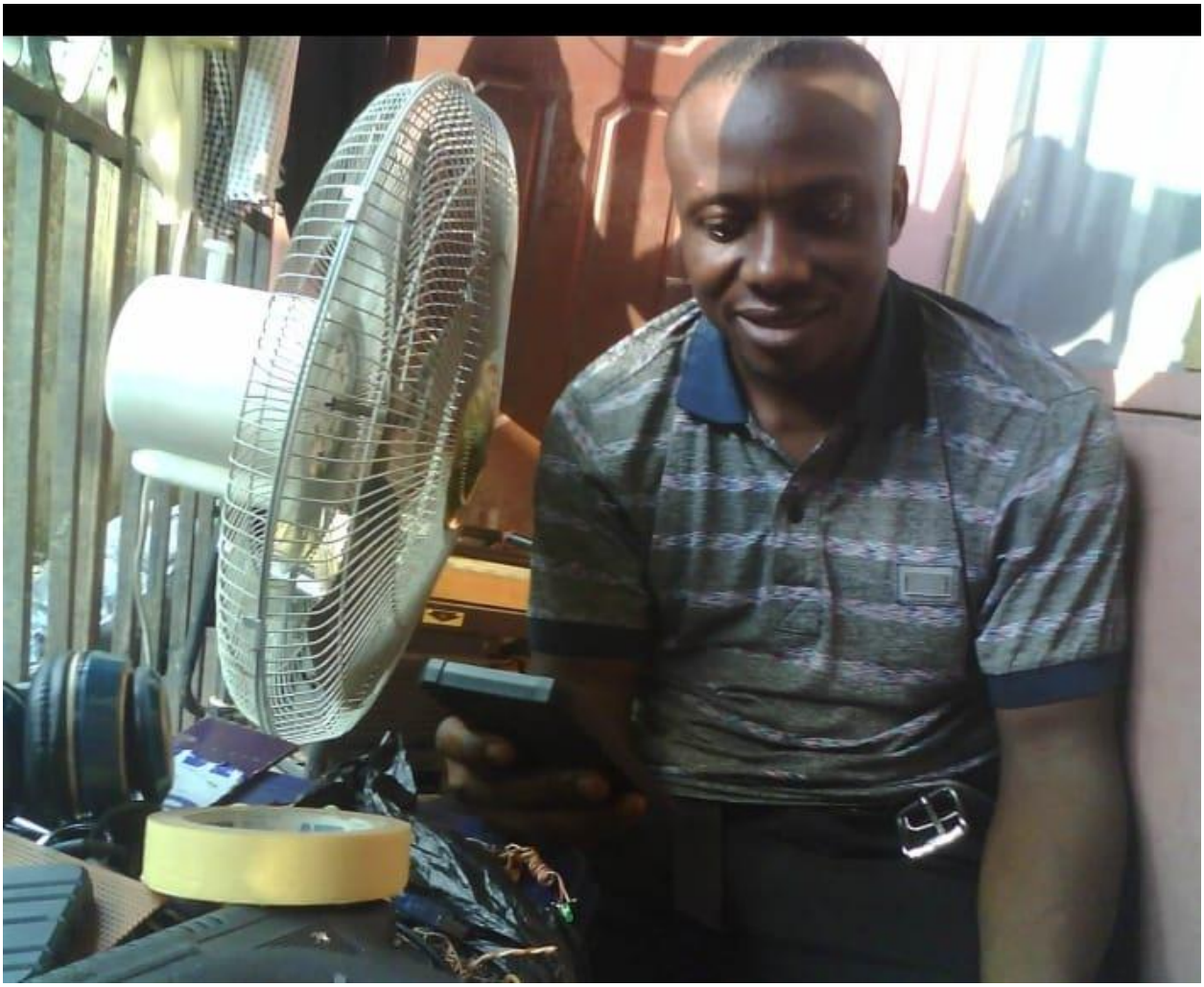

Plate 4.4: Intruder's Photo captured and sent to the office owner for security checks

4.1.2 System WiFi Communication Range and Received Signal Strength Indicator (RSSI) values

ESP32 Camera WiFi module gives the strength of signal flow between the prototype (transmitter) and the user's smartphone (receiver), which is called the RSSI. The RSSI maintained very high stability only a few fluctuations were observed even when the distance kept changing during the system test in an open space. The changes encountered in the values of the transceiver's RSSI during the test were recorded in Table 4.1 and the graphical representation was clearly shown in Plates 4.4.

The average output power in mW was calculated using Equation 5.

$$\text{Output power (Pout)} = 10\frac{\text{dBm}}{10} \tag{4.1}$$

where the average RSSI is the input parameter measured in dBm.

Table 4.2: Communication Range and RSSI values at distance >> 50 meters (1 unit division)

Distance (m)	Largest RSSI Value (dBm)	Smallest RSSI Value (dBm)	Average (Round off) RSSI Value (dBm)	Average Output Power (mW)
1	-54	-53	-53.5	0.0000029
2	-54	-53	-53.5	0.0000029
3	-54	-54	-54	0.0000040
4	-54	-52	-53	0.0000050
5	-54	-53	-53.5	0.0000029
6	-55	-54	-54.5	0.0000035
7	-56	-54	-55	0.0000032
8	-54	-53	-53.5	0.0000029
9	-54	-52	-53	0.0000050
10	-55	-54	-54.5	0.0000035
11	-54	-51	-52.5	0.0000056
12	-54	-53	-53.5	0.0000029
13	-53	-50	-51.5	0.0000071
14	-54	-51	-52.5	0.0000056
15	-55	-53	-54	0.0000040
16	-54	-52	-53	0.0000050
17	-57	-53	-55	0.0000032
18	-51	-50	-50.5	0.0000089
19	-51	-50	-50.5	0.0000089
20	-51	51	-51	0.0000079

4.2 Discussions:

The utilization of ESP32 CAMERA, keypad, and solenoid lock for face recognition door lock system introduces several pertinent discussions regarding its functionality, performance, and potential improvements. The results of the average output power from Table 4.1 show that there was minimum power and maximum power at RSSI of -53.5 dBm and -50.5 dBm respectively.

4.2.1 Output (Received) Power Measurement

In a wireless network, a cell data device is a radio device and the signal strength and signal quality both are measured in dBm (i.e. decibels relative to one milliwatt). RSSI is a negative dBm value, values closer to 0 dBm are strong signals.

After calculating the average output power, it was observed that the average output power was greater at -50.5dBm showing that the closer the user's smartphone was to the receiver (prototype device), the more the output power and vice versa. The maximum output power was 0.0000089mW whereas the minimum output power was 0.0000029mW as shown in tables 4.1

Plate 4.5 shows the detailed graphical representation of the corresponding changes in the RSSI at locations far greater than 50m. It was observed that there was a bit of fluctuation in the RSSI due to the usual network challenges.

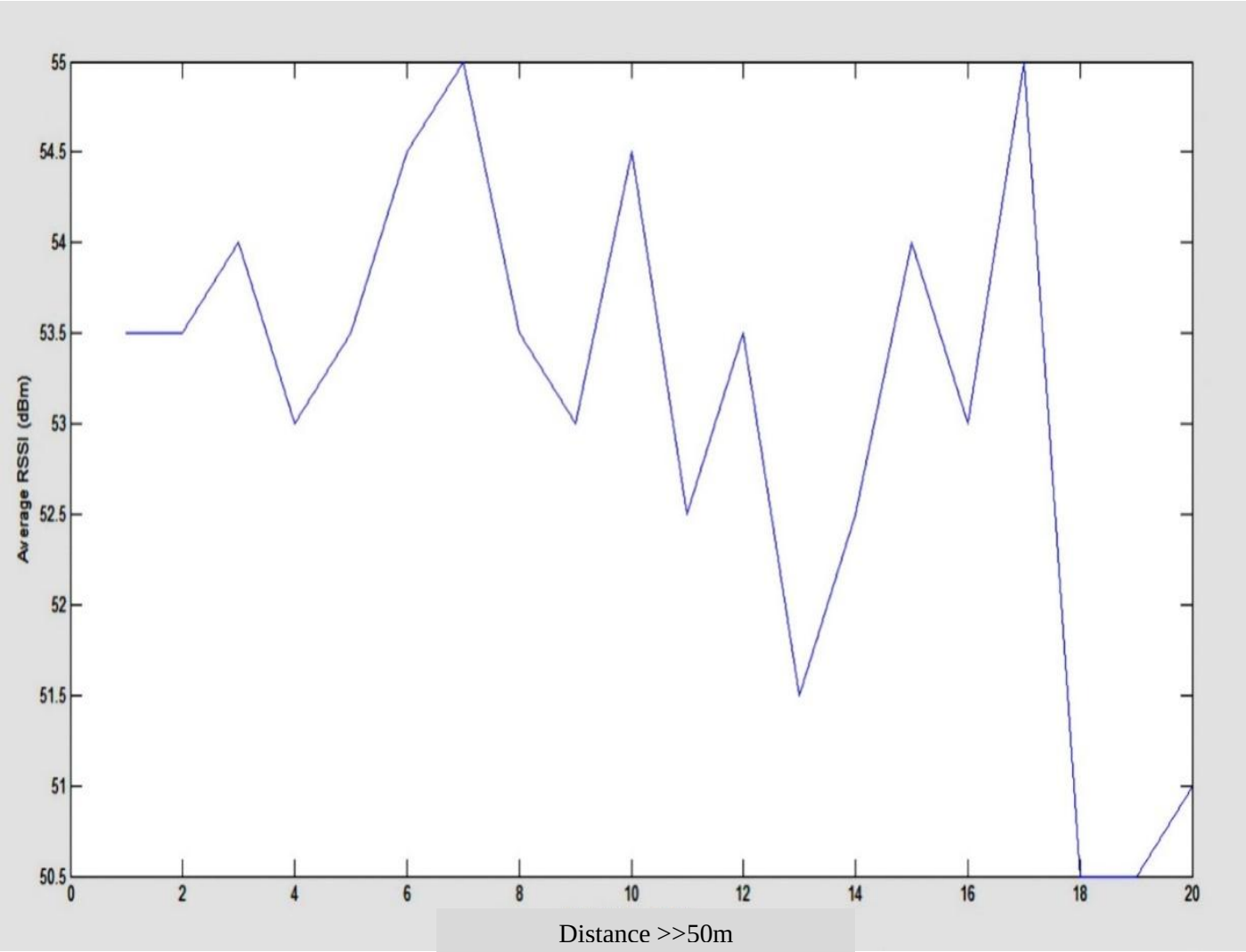

Plate 4.5: Graphical representation of RSSI values obtained as recorded in table 4.1

conditions. The accuracy of the system was measured using metrics such as True Positive Rate (TPR), False Positive Rate (FPR), Precision, Recall, and F1 Score. Those metrics helped in understanding the system's performance in recognizing authorized individuals and rejecting unauthorized ones.

True Positive (TP): The system correctly identifies an authorized individual.

True Negative (TN): The system correctly rejects an unauthorized individual.

False Positive (FP): The system incorrectly identifies an unauthorized individual as authorized.

False Negative (FN): The system incorrectly rejects an authorized individual.

Table 4.2 gives a summary of the facial recognition results obtained during the tests.

Table 4.2: Facial Recognition Performance Metrics

S/N	Metric	Value
1	True Positives (TP)	95
2	True Negatives (TN)	90
3	False Positives (FP)	5
4	False Negatives (FN)	10
5	Accuracy	92.5%
6	Precision	95%
7	Recall	90.48%
8	F1 Score	92.68%
9	False Positive Rate	5.26%

4.2.3 Discussions

The face recognition door lock system using ESP32 CAMERA has shown high accuracy in identifying authorized individuals while maintaining a low false positive rate. The following sections discuss various aspects of the system's performance, potential improvements, and real-world applicability.

4.2.4 Analysis of Results

The accuracy of the system was 92.5%, which was indicative of its reliability in recognizing faces under different conditions. Precision and Recall values of 95% and 90.48%, respectively, demonstrated that the system was proficient at correctly identifying authorized individuals while minimizing false positives. The F1 Score of 92.68% reflected a good balance between Precision and Recall.

4.2.5 Discussions on System Performances

The performance of this System face recognition using ESP32 CAMERA depended on various factors such as:

a. **Image Quality**: The quality of the images captured by the ESP32 camera such as resolution, brightness, and contrast affect image quality were clear enough and could be used to identify the person involved in the event of security threats

b. **Processing Power**: The ESP32's processing power and memory were appreciated. The speed and accuracy of face recognition were enhanced when the camera was positioned in a vicinity with higher network strength.

c. **Angle and Orientation**: Face recognition performance was affected by the angle and orientation of the face.

The discussions surrounding the face recognition door lock system using ESP32 CAMERA encompass hardware integration, algorithm performance, security and privacy considerations, user experience, and integration, as well as real-world deployment and scalability, had it that the system performed optimally and could be useful, especially in some offices or firms where full automation is being deployed in the access control units. These discussions provided a holistic viewpoint for evaluating the system's strengths, identifying areas for further enhancement, and shaping the future development and implementation strategies for face recognition-based access control solutions. The system sent a photo notification of the intruder to the office when the user’s face was mismatched with the programmed ones.

CHAPTER FIVE

CONCLUSION AND RECOMMENDATIONS

5.1 CONCLUSION:

In conclusion, the face recognition door lock system offers a convenient and secure means of access control that has been successfully designed, implemented, tested, and worked accordingly. Through the use of advanced facial recognition technology, this system provides a reliable method of authentication that can effectively replace traditional key or card-based entry systems. The integration of machine learning and computer vision algorithms has greatly improved the accuracy and efficiency of facial recognition, making it a viable option for residential and commercial applications. Additionally, the system's ability to adapt to various environmental conditions and lighting scenarios further enhances its reliability, making it suitable for real-world deployment.

Generally, this research has advanced the knowledge and understanding of face recognition door lock systems, paving the way for further innovation and improvement in access control technology. The face recognition door lock system presents a promising and sophisticated approach to access control, offering a blend of convenience, security, and technological innovation. Through the incorporation of advanced facial recognition technology, such systems provide a reliable and efficient means of authentication that can significantly enhance security and streamline access management processes. The contributions to knowledge in this area encompass advancements in technology, insights into usability and reliability, considerations for security and privacy, and a deeper understanding of user experience and adoption factors. Moving forward, continuous improvement, heightened security measures, and a focus on user accessibility and privacy will

further propel the development and adoption of face recognition door lock systems, shaping the future of access control solutions.

5.2 RECOMMENDATIONS:

Based on the research and analysis conducted, several recommendations can be made to further enhance the face recognition door lock system:

a. Continuous Improvement: Developers and manufacturers should continue to invest in research and development to further improve the accuracy, speed, and robustness of the face recognition technology. This includes refining algorithms, enhancing hardware capabilities, and improving the overall user experience.

b. Security Enhancements: It is crucial to continually update and strengthen the security measures implemented within the system to mitigate any potential vulnerabilities. This includes regular software updates, encryption protocols, and protection against spoofing and hacking attempts.

c. Accessibility and Integration: Efforts should be made to ensure the system is accessible to individuals with diverse facial features and expressions to avoid bias and exclusivity. Additionally, seamless integration with smart home and building automation systems should be prioritized to provide a comprehensive access control solution.

d. Privacy Considerations: Respect for user privacy is paramount, and developers should adhere to best practices for data protection and user consent. Clear guidelines for handling and storing facial data must be established to maintain trust and compliance with privacy regulations.

5.3 CONTRIBUTIONS TO KNOWLEDGE:

This research on face recognition door lock systems has contributed to knowledge in the following key areas:

a. Technology Advancements: The study has highlighted the advancements in facial recognition technology and its application within access control systems. By exploring the underlying algorithms and hardware components, valuable insights have been gained regarding the current state and future potential of this technology.

b. Usability and Reliability: Through comprehensive testing and analysis, the research has shed light on the usability and reliability of face recognition door lock systems in real-world scenarios. By addressing performance under varying conditions, the study has provided a better understanding of the system's capabilities and limitations.

c. Security Implications: The research has emphasized the importance of security in face recognition door lock systems, drawing attention to the need for robust security measures to safeguard against potential threats and breaches. Insights into potential vulnerabilities and countermeasures have been outlined, contributing to the overall understanding of system security.

d. User Experience and Adoption: By evaluating user experiences and perceptions, the study has offered valuable insights into the factors that influence the adoption and acceptance of face recognition door lock systems. Understanding user concerns and preferences can help guide future development and implementation strategies.

REFERENCES

Aalase, A., Bandgar, P., Kamble, K., Bhosale, S., & Udgave, A. A. (2023). International Journal of Research Publication and Reviews Surveillance Monitoring Using ESP32-CAM Module. *International Journal of Research Publication and Reviews*, *4*(3), 4297–4300. www.ijrpr.com

Adak, D., Pain, M. K., & Dey, U. K. (2017). Rfid Based Security System Using. *International Journal of Scientific and Engineering Research*, *8*(3), 143–145.

Ahmed ElShafee, K. A. H. (2012). *Design and Implementation of a WiFi Based Home Automation System", International Journal of Computer, Electrical, Automation, Control and Information Engineering Vol: 6, No: 8*. *6*(8), 1074–1080.

Andreas, Aldawira, C. R., Putra, H. W., Hanafiah, N., Surjarwo, S., & Wibisurya, A. (2019). Door security system for home monitoring based on ESp32. *Procedia Computer Science*, *157*, 673–682. https://doi.org/10.1016/j.procs.2019.08.218

Andrew, A. M. (2019). Intelligent Control Systems: An Introduction with Examples. *Kybernetes*, *32*(4), 1–29. https://doi.org/10.1108/k.2003.06732dae.003

Arsić, N., Jakšić, B., & Petrovic, M. (2016). Overview, Characteristics and Advantages of IP Camera Video Surveillance Systems Compared to Systems with other Kinds of Camera Creating the Network of Knowledge Labs for Sustainable and Resilient Environments-KLABS View project. *Certified International Journal of Engineering Science and Innovative Technology (IJESIT*, *9001*(5), 356–362. https://www.researchgate.net/publication/355484230

Bhat, A., Sharma, S., Pranav, K. R., & G, M. R. H. (2017). *HOME AUTOMATION USING INTERNET OF THINGS*. 917–920.

Borkar, A. A., & Karande, R. R. (2017). *Web Hosting and Live Streaming Using Raspberry-Pi for Home Automation*. *3*, 598–602.

Computing, M. (2015). GSM-Based Home Automation System Using App-Inventor For Android Mobile Phones. *International Journal of Computer Science and Mobile Computing*, *4*(4), 158–167.

G. C. Manjunath, Mr. B. Mahendra, Ms. Rashmi, Mrs G. Bhuvana, & Ms Keerthi. (2022). Home Security System using ESP32-CAM and Telegram Application. *International Journal of Advanced Research in Science, Communication and Technology*, *May*, 580–582. https://doi.org/10.48175/ijarsct-5093

Gaikwad, P., Narule, S., Thakre, N., & Chandekar, P. (2017). RFID Technology-Based Attendance Management System. *International Journal Of Engineering And Computer Science*, 2–7. https://doi.org/10.18535/ijecs/v6i3.10

IEA Report, 2014. (2017). *Voice Recognition Based Home Automation System for Paralyzed People*. *3*(02).

Kantha & Priyanka, P. (2020). *Realization of an IoT System to Ensure Doorway Security by Integrating ESP32-CAM with Cloud Server*. 1235–1238.

Kazi, R., & Tiwari, G. (2016). IoT based Interactive Industrial Home wireless system, Energy management system and embedded data acquisition system to display on web page using GPRS, SMS & E-mail alert. *International Conference on Energy Systems and Applications, ICESA 2015, August*, 290–295. https://doi.org/10.1109/ICESA.2015.7503358

Kumar, A., & Tiwari, N. (2015). *Energy Efficient Smart Home Automation System*. *3*(1), 11–13.

Kumar, M., & Shimi, S. L. (2015). *Voice Recognition Based Home Automation System for Paralyzed People*. *4*(10), 2508–2515.

Kundu, D., Nandy, S., & Kumar, A. (2019). Development of an Attendance System for Students with SMS Notification to Parents. *Ijarcce*, *6*(6), 49–54. https://doi.org/10.17148/iarjset.2019.6607

Mukhtar, A. (2021). Nigeria's Security Challenges and the Crisis of Development: Towards a New Framework for Analysis. *International Journal of Developing Societies*, *1*(3), 107–116.

Online, I., Chasokela, D., Tshuma, L. S., Matshe, K., & Sibanda, M. (2022). *Indiana Journal of Multidisciplinary Research Password Based Door Locking System*. 1–5.

Postulka, M. B. and J. (2019). Open Access books Built by scientists , for scientists TOP 1 %. *Intech*, *32*(July), 137–144.

Putra, W. S., & Setyawan, A. (2021). Room Security System Design using ESP32 CAM with Fuzzy Algorithm. *Mobile and Forensics*, *3*(2), 66–74. https://doi.org/10.12928/mf.v3i2.5554

Ravi, K. S., Varun, G. H., Vamsi, T., & Pratyusha, P. (2019). RFID based security system. *International Journal of Innovative Technology and Exploring Engineering*, *2*(5), 132–134.

Salikhov, R. B., Abdrakhmanov, V. K., & Safargalin, I. N. (2021). Internet of things (IoT) security alarms on ESP32-CAM. *Journal of Physics: Conference Series*, *2096*(1). https://doi.org/10.1088/1742-6596/2096/1/012109

Sehgal, T., & More, S. (2017). Home Automation using IOT and Mobile App. *International Research Journal of Engineering and Technology (IRJET)*, 694–698.

Shah, H., Chauhan, V., & Sharma, R. (2017). *Home Automation Using ZigBee*. *6*(3), 99–102.

Singla, D. (2023). *Performance Analysis of Authentication system : A Systematic Literature Review Performance Analysis of Authentication system : A*. 0–26.

Snehal Arun Khulape; Sakshi Rajendra Malage; Manasi Sudhir Patil; Arfa Aslam Bargir; Sagar V. Chavan. (2018). Home Automation Android-Based GSM System. *International Journal of Trend in Scientific Research and Development*, *2*(6), 774–777. url: http://www.ijtsrd.com/papers/ijtsrd18740.pdf%0ADirect Link: http://www.ijtsrd.com/engineering/computer-engineering/18740/home-automation-android-based-gsm-system/miss-snehal-arun-khulape

Snehal N. Bawane, P. Gautam, Ashish Dewase, V. Mishra, S. G. (2017). Automation of Irrigation System using Android Technology. *INTERNATIONAL JOURNAL OF ENGINEERING SCIENCE AND COMPUTING*, *7*(3), 5580–5582.

Soe, Z. N., Win, D. A. M., & Thoung, D. T. H. (2018). Implementation of Fingerprint-based Student Attendance System with Notification by GSM Module. *International Journal of Science and Engineering Applications*, *7*(9), 260–264. https://doi.org/10.7753/ijsea0709.1002

Viola, P., & Jones, M. (2022). Rapid object detection using a boosted cascade of simple features. *Proceedings of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition*, *1*(July). https://doi.org/10.1109/cvpr.2001.990517