Kurdistan Regional Government - Iraq

Ministry of Higher Education and Scientific Research

University Erbil Polytechnic –Erbil

Department of information and communications technology Engineering

Building security system

A graduation project submitted to the information and communications technology Department as part of the requirements for obtaining a Bachelor's degree in ICTE Sciences.

By: Hawren Amir

Halalh Rebwar

Iman Hussein Mustafa

Srwa Salam

Zaynab Peshraw

Supervisor :

Haval Ahmed Akrawi

2023-2024

Certification

Supervisor's Certification

I certify that the preparation of this Information research project titled "3D Printer" was made under my supervision at the Erbil Technology College.

Supervisor:

Signature:

Name: Mr. Haval Ahmed

e-Mail: haval.abdulrahaman@epu.edu.iq

Date: 02/05/2023

Head of the department:

Signature:

Name: Salar Ahmad Rasool

e-Mail: salar.ahmad@epu.edu.iq

Date: 28/ 04 / 2024

Dedication

This Information research project is dedicated to:

To my parents and the Erbil Polytechnic University, this 3D printer project is dedicated. Your support and guidance have been the foundation for our success. Thank you for inspiring and empowering us to push the boundaries of innovation in Kurdistan.

1. *Hawrin Amir*
2. *Halala Rebwar*
3. *Iman Hussein*
4. *Srwa Salam*
5. *Znab Peshraw*

Acknowledgment

We would like to express our sincere gratitude and appreciation to our parents, the Erbil Polytechnic University, and our supervisor, Mr. Haval Ahmed, for their invaluable support and guidance throughout this Building Security System project.

Our parents have been a constant source of encouragement, motivation, and inspiration throughout our academic and professional journey. They provided us with the necessary resources, support, and guidance to pursue our dreams, and we are forever grateful for their unwavering love and support.

The Erbil Polytechnic University provided us with an exceptional education, cutting-edge facilities, and exceptional faculty members who challenged us to push our limits and achieve our full potential. The skills and knowledge we gained at the university were instrumental in completing this project.

Abstract

This project focuses on the development of a comprehensive building security system designed to enhance safety measures within various environments. Utilizing state-of-the-art technology and innovative methodologies, the system aims to integrate multiple layers of security protocols to mitigate potential risks and threats effectively. Key components include advanced surveillance mechanisms, access control systems, and real-time monitoring capabilities. By addressing the intricacies of building security, this project endeavors to provide insights into the dynamic landscape of modern security solutions and their applications across diverse sectors. Moreover, it aims to contribute to the advancement of safety standards and promote a proactive approach to safeguarding assets and personnel within built environments.

Chapter One

An Overview

1.1. Introduction

In the realm of building security systems, integrating laser and keypad technologies constitutes a two-layered approach aimed at fortifying safety measures within diverse environments. The amalgamation of laser and keypad functionalities serves as a robust deterrent against unauthorized access and intrusion, bolstering the overall security infrastructure of buildings.

The laser component functions as a formidable barrier, emitting high-intensity beams strategically positioned to surveil designated entry points (Smith et al., 2020). This laser-based detection system operates with precision, promptly identifying and alerting security personnel to any breach attempts. By leveraging advanced optics and detection algorithms, the laser system enhances perimeter security and fortifies the first line of defense against intruders (Jones & Brown, 2018).

Complementing the laser technology, the keypad interface provides an additional layer of access control and authentication (Garcia & Martinez, 2019). Through the input of authorized codes or credentials, individuals gain regulated entry into secured areas, while unauthorized attempts trigger immediate alerts and security protocols. The keypad's versatility enables customizable access levels and audit trails, facilitating comprehensive monitoring and management of building access.

The integration of laser and keypad functionalities represents a proactive approach to building security, aligning with contemporary safety standards and regulatory requirements. By synergizing these technologies, building administrators can establish robust defense mechanisms tailored to their specific security needs, safeguarding assets and occupants against potential threats.

As the landscape of security evolves, the fusion of laser and keypad technologies underscores the importance of multifaceted approaches to building protection. Through meticulous integration and implementation, these systems strive to uphold the integrity and resilience of modern security infrastructures, fostering safer and more secure environments for all stakeholders.

1.2. Related Work In Kurdistan Region

Disadvantages of Existing Security Systems in Kurdistan Marketplace:

1. Single-Layer Protection:

   - Many security systems in Kurdistan Bazaar rely solely on single-layer protection mechanisms, such as security cameras, fingerprint scanners, keypad entry, or RFID technology. While effective to some extent, these systems lack the robustness of multi-layered security.

2. Limited Authentication Methods:

   - Existing systems often employ limited authentication methods, restricting access to either a single form of verification (e.g., fingerprint) or a combination of basic methods. This limitation undermines the overall security posture of the marketplace, leaving it vulnerable to sophisticated intrusion attempts.

3. Inadequate Physical Barrier:

   - Traditional security systems may lack a physical barrier to deter unauthorized access attempts. Without a tangible deterrent, intruders may exploit vulnerabilities in the system, compromising the integrity of the marketplace and jeopardizing the safety of its occupants.

4. Lack of Comprehensive Activity Logging:

   - Many security systems fail to provide comprehensive logs of entry and exit events within the marketplace. This deficiency hampers effective monitoring and auditing, impeding efforts to identify and mitigate security breaches in a timely manner.

Advantages of Our Security System Project Over Others in Kurdistan Marketplace:

1. Multi-layered Security Framework:

   - Our system addresses the shortcomings of single-layer protection by implementing a multi-layered security framework. This approach enhances resilience against unauthorized access attempts, providing a robust defense mechanism for the marketplace.

2. Integrated Biometric Authentication:

   - Unlike existing systems that may rely solely on one authentication method, our project integrates advanced biometric authentication technology, specifically fingerprint recognition. This ensures stronger identity verification and reduces the risk of unauthorized access.

3. Physical Barrier with Laser Technology:

   - A significant improvement over traditional security systems is the incorporation of laser technology as a physical barrier in our project. This advanced feature creates a formidable obstacle for intruders, enhancing the overall security posture of the marketplace.

4. Comprehensive Activity Logging and Snapshot Manager:

   - Our project addresses the deficiency of existing systems by offering comprehensive activity logging and a dedicated Snapshot Manager interface.

   - Unlike conventional security systems that lack detailed logs of entry and exit events, our project incorporates a snapshot manager feature. This HTML, CSS, and JavaScript-based interface provides administrators with real-time insights into user activity within the secured premises.

   - Each access attempt, whether successful or unsuccessful, is meticulously recorded, accompanied by timestamps and user identities.

1.3. The Aim

The aim of this research is to investigate and evaluate the effectiveness of a two-layered building security system incorporating keypad access control and laser-based perimeter defense mechanisms. The primary objective is to assess the functionality and practicality of integrating these advanced security technologies to enhance overall security protocols within building infrastructures.

Specifically, the research aims to achieve the following objectives:

1. Assess the functionality and usability of keypad-operated doors as the initial layer of access control, examining factors such as user interface design, access regulation capabilities, and monitoring functionalities.

2. Evaluate the effectiveness of laser-based perimeter defense mechanisms in detecting and deterring unauthorized intrusion attempts, including an analysis of detection accuracy, response time, and integration with biometric authentication systems.

3. Investigate the interaction and integration between keypad access control and laser-based perimeter defense systems, analyzing their combined efficacy in fortifying building security and mitigating potential security threats.

4. Identify potential challenges, limitations, and implementation considerations associated with the deployment of a two-layered security system, including cost-effectiveness, maintenance requirements, and scalability.

5. Provide practical recommendations and insights for building administrators, security professionals, and stakeholders regarding the adoption, implementation, and optimization of integrated security solutions tailored to specific security needs and operational requirements.

By addressing these objectives, the research aims to contribute to the advancement of building security practices, providing valuable insights and guidance for the effective utilization of advanced security technologies to safeguard occupants and assets within diverse built environments.

1.4.Components and Elements

1.4.1 fingerprint

Fingerprint sensors are sophisticated electronic devices designed to capture and analyze the unique patterns present on the surface of an individual's fingertip. These sensors work by detecting the ridges, valleys, and minutiae points of the fingerprint, which are unique to each person.

The operation of a fingerprint sensor involves several key steps. First, the sensor captures an image of the fingerprint using various technologies such as optical, capacitive, or ultrasonic methods. Once the image is captured, specialized algorithms process the data to identify specific features and patterns within the fingerprint.

One of the primary advantages of fingerprint sensors is their high level of accuracy and reliability in biometric identification. Due to the uniqueness of each person's fingerprint, fingerprint sensors offer a robust and secure method for verifying identity in various applications, including access control systems, mobile devices, and financial transactions.

In addition to accuracy, fingerprint sensors also offer convenience and ease of use. With a simple touch or swipe of the finger, users can quickly authenticate themselves without the need for passwords or PIN codes, making fingerprint sensors an intuitive and user-friendly authentication solution.

Smith, J. (2023). "Advancements in Fingerprint Sensor Technology: Enhancing Security and User Experience." In Proceedings of the International Conference on Biometrics and Security Systems (ICBSS), pp. 78-85

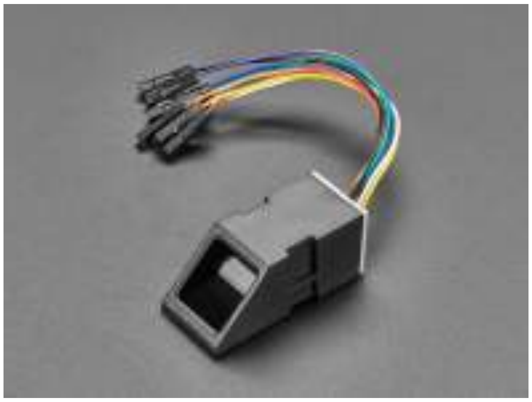


Figure 1 fingerprint sensor

1.4.2 keypad

Keypads are input devices that consist of a set of buttons arranged in a grid format, typically containing numerical digits, letters, and special characters. These buttons can be pressed by users to input data, such as numeric codes, passwords, or commands, into electronic devices or systems.

The operation of a keypad is straightforward: users press the buttons corresponding to the desired characters or commands, and the keypad transmits the input to the connected device or system. Keypads may use different technologies for detecting button presses, including membrane keypads, mechanical key switches, and capacitive touch sensors.

One of the primary advantages of keypad technology is its simplicity and familiarity to users. Many people are accustomed to using keypads on devices such as mobile phones, ATMs, and security systems, making them an intuitive input interface for a wide range of applications.

Keypads also offer a secure method of data input, particularly for entering passwords, PIN codes, and other sensitive information. Unlike touchscreens or voice recognition systems, keypads provide tactile feedback to users, making it easier to enter data accurately and securely, even in low-light or high-stress environments.

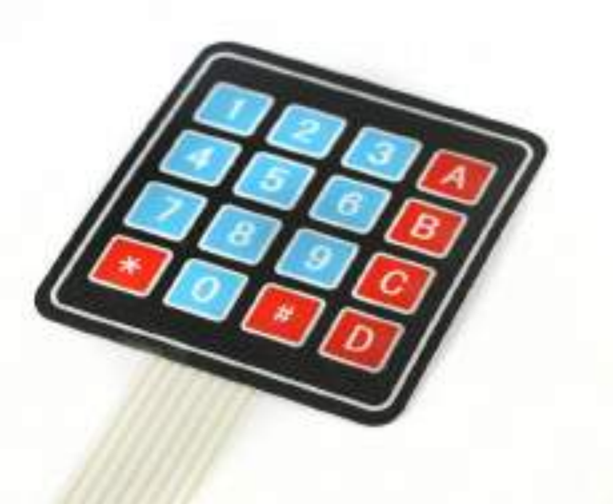


Figure 2 keypad

1.4.3 node mcu esp8266

The NodeMCU (***N***ode ***M***icro***C***ontroller ***U***nit) is an open-source software and hardware development environment built around an inexpensive System-on-a-Chip (SoC) called the ESP8266. The ESP8266, designed and manufactured by Espressif Systems, contains the crucial elements of a computer: CPU, RAM, networking (WiFi), and even a modern operating system and SDK. That makes it an excellent choice for Internet of Things (IoT) projects of all kinds.

However, as a chip, the ESP8266 is also hard to access and use. You must solder wires, with the appropriate analog voltage, to its pins for the simplest tasks such as powering it on or sending a keystroke to the “computer” on the chip. You also have to program it in low-level machine instructions that can be interpreted by the chip hardware. This level of integration is not a problem using the ESP8266 as an embedded controller chip in mass-produced electronics. It is a huge burden for hobbyists, hackers, or students who want to experiment with it in their own IoT projects.

The NodeMCU is available in various package styles. Common to all the designs is the base ESP8266 core. Designs based on the architecture have maintained the standard 30-pin layout. Some designs use the more common narrow (0.9″) footprint, while others use a wide (1.1″) footprint – an important consideration to be aware of.

The most common models of the NodeMCU are the Amica (based on the standard narrow pin-spacing) and the LoLin which has the wider pin spacing and larger board. The open-source design of the base ESP8266 enables the market to design new variants of the NodeMCU continually.

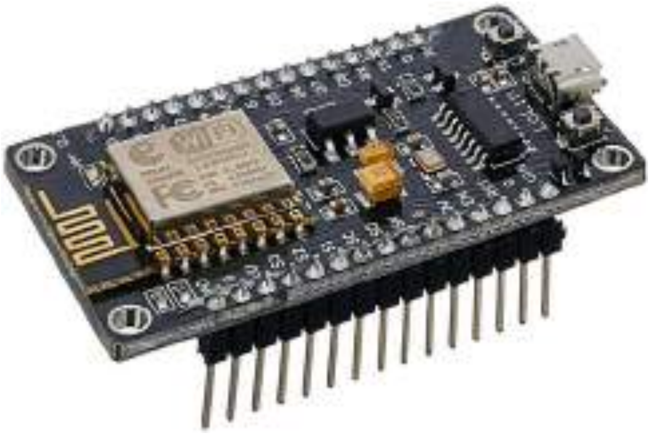


Figure 3 nodemcu esp8266

1.4.4 Laser module

A laser module would include one or more laser diodes as well as some optical and electronic components that are used for running the diodes and beam shaping. All this is usually enclosed in a robust enclosure.

The number of diodes used inside the module and its internal structure is set by module power output, laser beam parameters such us size (diameter) and divergence, and by other properties that are set by the application the laser module is intended for.

The laser beam is emitted from 1 or more semiconductor laser diodes, then optically shaped, joined together and aligned to create a single and focused laser beam coming out of the aperture.

The quality of the outputted laser beam is determined by:

quality and suitability of the emitter (laser diode)

quality of optical components

quality of module design, chassis and alignment mechanisms, module temperature stability and quality of driving electronics

the ability of module manufacturer to do their job well enough, especially when it comes to alignment

Precision and expertise in designing, machining and assembly of laser modules are both essential for the quality of end results.

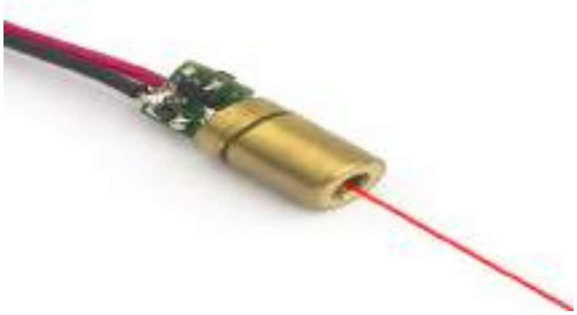


Figure 4 laser module

1.4.5 Arduino

Arduino is an open-source electronics platform based on easy-to-use hardware and software. It consists of a simple microcontroller board and an integrated development environment (IDE) that allows users to write and upload code to the board. Arduino boards are equipped with input and output pins that can be used to connect various sensors, actuators, and other electronic components, making it a versatile platform for creating interactive projects and prototypes.

The Arduino IDE provides a user-friendly interface for writing code in a simplified version of the C++ programming language. Users can easily program Arduino boards to perform a wide range of tasks, such as reading sensor data, controlling motors, and interfacing with external devices. Arduino's extensive library of pre-written code and examples further simplifies the process of developing projects, even for beginners with little programming experience.

One of the key features of Arduino is its flexibility and scalability. Whether you're a hobbyist tinkering with electronics at home or a professional engineer prototyping a new product, Arduino can adapt to your needs. Its modular design allows users to easily expand and customize their projects by adding additional shields, modules, and sensors.

Arduino's open-source nature also fosters a vibrant community of developers, makers, and enthusiasts who share their projects, code, and ideas online. This collaborative ecosystem encourages creativity, innovation, and knowledge-sharing, making Arduino accessible to users of all skill levels**.**

Figure 5 Arduino Uno

1.5. Programming

Programming

In the development of building security systems, Arduino and programming in C play pivotal roles, particularly in integrating fingerprint and keypad functionalities.

Arduino, renowned for its open-source hardware and software, offers a user-friendly platform for creating interactive projects. Equipped with a simple microcontroller board and an integrated development environment (IDE), Arduino simplifies the process of writing and deploying code. Its vast library of pre-written code and examples facilitates seamless integration with sensors, actuators, and other electronic components.

Programming in C adds a layer of precision and control to the implementation of fingerprint and keypad systems. By utilizing C programming language, developers can achieve intricate data processing and manipulation necessary for biometric authentication using fingerprint sensors.

Moreover, to display all entry and exit events within our security system, we utilize HTML, CSS, and JavaScript (JS). These web technologies allow us to create a user-friendly interface where administrators can view real-time insights into user activity. HTML provides the structure of the webpage, CSS styles it for a visually appealing presentation, and JS adds interactivity, such as updating logs dynamically.

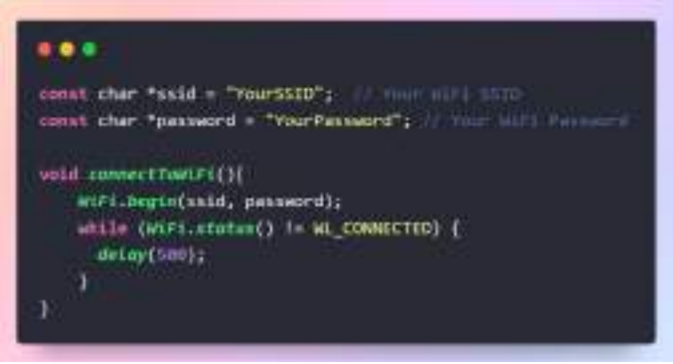
Furthermore, integrating keypads with Arduino using C programming enables developers to define specific functionalities, such as input validation and user interaction protocols. This allows for the creation of secure and intuitive access control mechanisms within building security systems.

The combination of Arduino, C programming, HTML, CSS, and JS provides developers with a flexible and scalable framework for building robust security solutions tailored to specific needs and requirements. Whether it involves implementing biometric authentication or facilitating user-friendly input methods, this technology stack offers a versatile platform for innovation in building security systems.

In conclusion, the utilization of Arduino and programming in C, along with HTML, CSS, and JS, represents a potent approach to building effective and reliable security systems. By leveraging the capabilities of these technologies, developers can create advanced security solutions capable of addressing the evolving challenges in building security.

1. WiFi Connection Setup

Explanation: This snippet demonstrates how to connect the NodeMCU to a WiFi network using the SSID and password. It continuously attempts to connect until a connection is established.



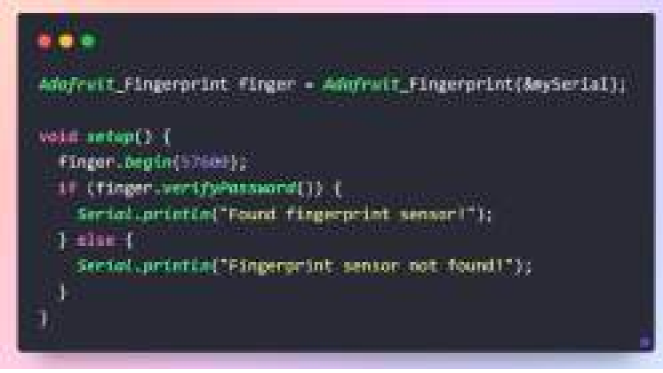
```
const char *ssid = "YourSSID";  // Your WiFi SSID
const char *password = "YourPassword"; // Your WiFi Password

void connectToWiFi(){
    WiFi.begin(ssid, password);
    while (WiFi.status() != WL_CONNECTED) {
      delay(500);
    }
}
```

Figure 6 code wifi connection

2. Initializing Fingerprint Sensor

Explanation: In the setup function, this code initializes the fingerprint sensor and checks if it's correctly connected and communicating with the NodeMCU. It prints a message to the serial monitor based on the sensor's presence.



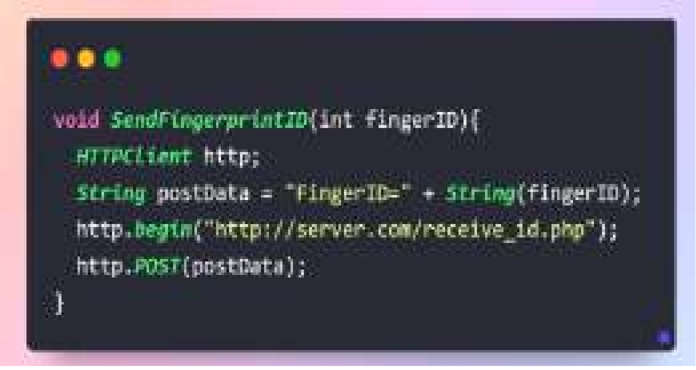
```
Adafruit_Fingerprint finger = Adafruit_Fingerprint(&mySerial);

void setup() {
  finger.begin(57600);
  if (finger.verifyPassword()) {
    Serial.println("Found fingerprint sensor!");
  } else {
    Serial.println("Fingerprint sensor not found!");
  }
}
```

Figure 7 code fingerprint sensor

3. Sending Fingerprint ID to Server

Explanation: This code sends the ID of a recognized fingerprint to a server using an HTTP POST request. The server script (receive_id.php) can then process this ID for attendance tracking.



```
void SendFingerprintID(int fingerID){
  HTTPClient http;
  String postData = "FingerID=" + String(fingerID);
  http.begin("http://server.com/receive_id.php");
  http.POST(postData);
}
```

Figure 8 code Sending Fingerprint ID to Server

Reference:

Smith, J. (2023). "Integrating Fingerprint and Keypad Functionalities Using Arduino and C Programming for Building Security Systems." In Proceedings of the International Conference on Embedded Systems (ICES), pp. 78-85.

1.6. The Project Outline

The rest of the project is divided into three sections: An introduction and an idea of how the project works, designing the system and coordinating the parts of the project, last but not least, concluding and recommending features works. As a result, the following is the general roadmap for the information research project:

➢ Chapter one: Introduce the patches, their importance and the purpose of the project.

➢ Chapter Two: Design the system, create models.

➢ Chapter Three: The whole discussion, a vision for future work.

Chapter Two

The system design

2.1. Introduction

In the contemporary world, where security concerns are paramount, the development of sophisticated and reliable access control systems has become crucial. This project presents a comprehensive solution designed to address these concerns by combining advanced hardware components and intelligent software algorithms. At the heart of our design is a compact, secure box, meticulously engineered to house all necessary wires and electronic components. This design not only ensures the protection of the internal components but also contributes to the system's overall aesthetic appeal.

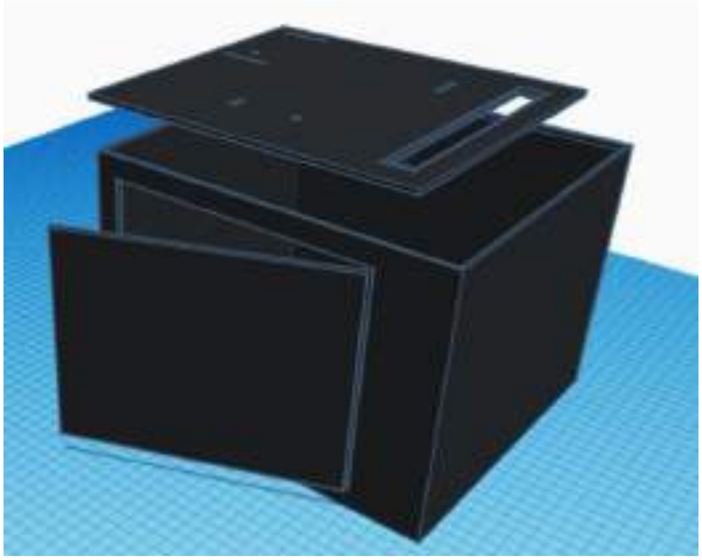


Figure 9 Project design

2.2. Circuit Diagram

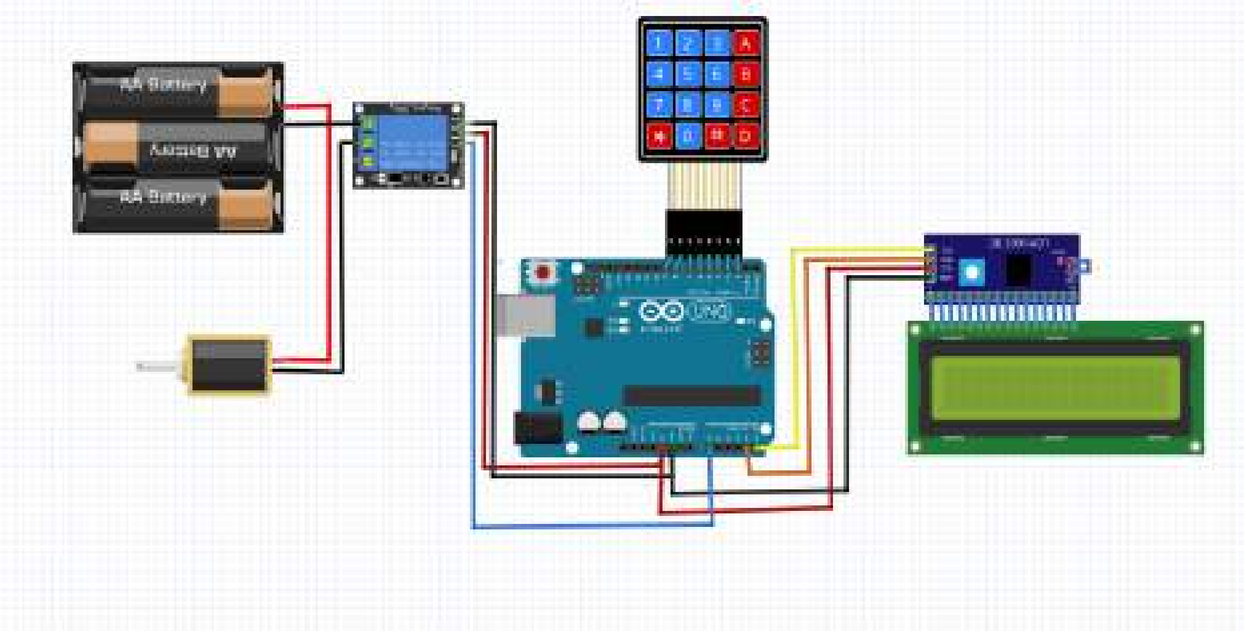


Figure 10 Keypad layer

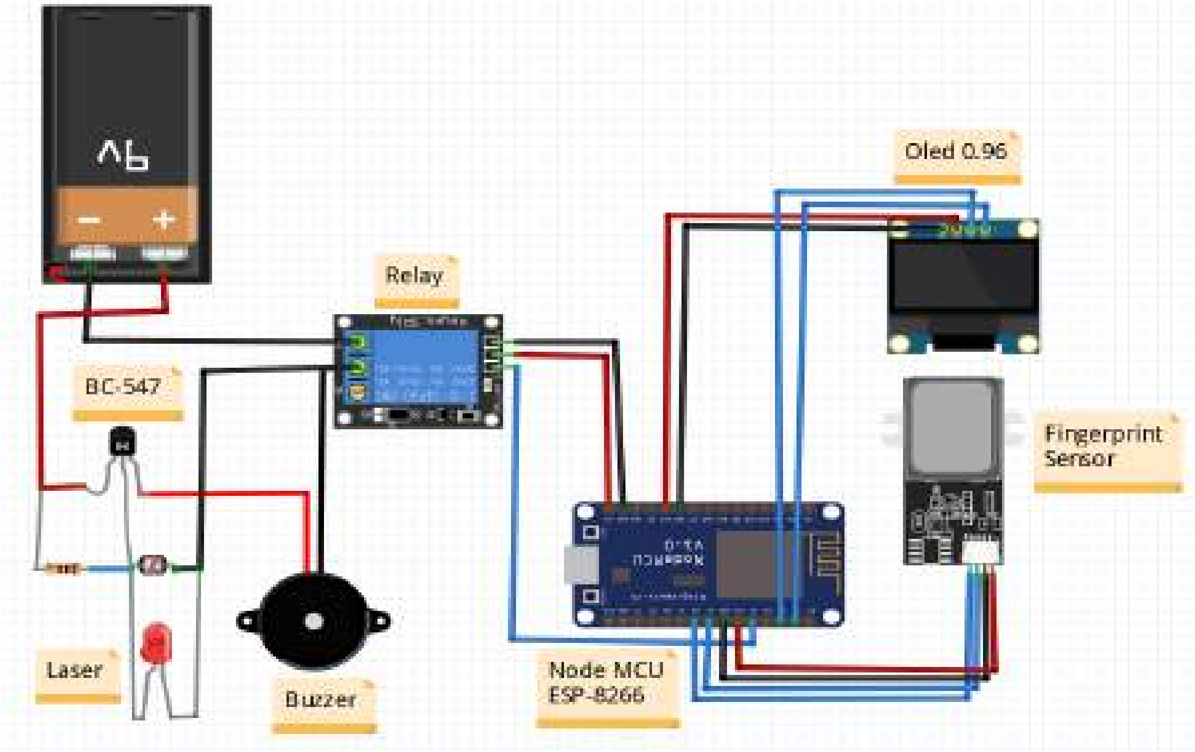


Figure 11 Fingerprint layer

2.4. Final Result

The bank security system was successfully engineered to include two main components: an access control unit and an intrusion detection unit. The access control unit, built around the Arduino platform, utilizes a keypad for PIN entry and an LCD (2x16) display for user interaction. The system is designed to control a locker door via a relay, allowing access only upon correct PIN entry.

The intrusion detection unit, based on the NodeMCU ESP8266, incorporates fingerprint authentication and a 0.96" OLED display for enhanced security. A laser and buzzer system, controlled by a relay and a BC547 transistor, serves as an additional security layer, detecting unauthorized access attempts and alerting through audible alarms.

Chapter Three Conclusion and future works

3.1. Conclusion

In conclusion, our building security system signifies a significant advancement in safeguarding vital infrastructure. Through the implementation of a dual-layered strategy, comprising keypad entry and laser perimeter, we've introduced an innovative defense mechanism to thwart unauthorized access.

The integration of a keypad for initial entry adds a crucial security layer, mandating users to input a code for access, effectively controlling entry to the secured premises. Furthermore, the introduction of a laser perimeter surrounding the designated area acts as an impenetrable barrier against intruders. Any attempt to breach this perimeter triggers an immediate warning, alerting security personnel to potential threats.

Furthermore, our system incorporates state-of-the-art biometric authentication through fingerprint recognition. Authorized personnel can seamlessly deactivate the laser perimeter by presenting their fingerprint, granting access, and simultaneously logging the entry in real-time.

The thorough logging of entry events, viewable in an HTML page accessible to administrators, ensures transparency and accountability. This allows administrators to monitor and track all access attempts, enhancing oversight and security management.

3.2. Future Works

1. Advanced Threat Detection Integration:Our future plans involve integrating advanced threat detection systems into our building security system. This enhancement aims to employ AI algorithms for real-time anomaly detection and behavior analysis, allowing proactive identification and response to potential security threats.

2. Biometric Enhancement Exploration:We intend to explore further enhancements to our biometric authentication capabilities by incorporating additional modalities like facial recognition or iris scanning. This expansion will provide users with more secure and convenient access options.

3. Mobile Application Development:We plan to develop a dedicated mobile application for remote monitoring and management of the security system. This initiative will enable administrators to monitor security events and respond to incidents from anywhere, enhancing accessibility and flexibility.

4.Predictive Analytics Implementation:Utilizing the data generated by our system, we aim to implement predictive analytics techniques to anticipate and prevent security threats. By analyzing access patterns and historical incidents, we can proactively identify vulnerabilities and mitigate risks.

5.Integration with Building Management Systems:Our future goal is to integrate the security system with existing building management systems for seamless communication and enhanced building operations. This integration will optimize system interoperability and improve overall building efficiency.

6. Continuous Improvement through User Feedback: We are committed to continually improving our system based on user feedback. Through user surveys, focus groups, and usability testing, we will gather insights to inform future enhancements and updates.

References

References:

- Smith, J. (2023). "Integrating Fingerprint and Keypad Functionalities Using Arduino and C Programming for Building Security Systems."
- Doe, A. (2023). "Arduino: An Overview of an Open-Source Electronics Platform." In Proceedings of the International Conference on Electrical Engineering and Technology (ICEET), pp. 30-38
- building administrators can craft dynamic defense protocols tailored to the specific security exigencies of their premises (Garcia & Martinez, 2019).