Khmelnytskyi National University
Faculty of Information Technologies
Department of computer engineering and information systems

BACHELOR THESIS

bachelor
Education level

Software and technical tool for controlling the door lock based on the ESP8266 microcontroller
Topic name

QWCE.20005.20.01.04 EN
Code

Field of study *12 «Information technology»*
Code, name

Major *123 «Computer Engineering»*
Code, name

Education program *«Computer Engineering and Programming »*
Name

Author: student of IV course, group КІін–20–1 _____ Chamunorwa.T.
Signature — Initials, surname

Supervisor _____ Nicheporuk A.O.
Signature, date — Initials, surname

Regulatory controller _____ Zasornova I.O.
Signature, date — Initials, surname

Admitted to defense:
Head of Computer Engineering and Information Systems Department _____ Hovorushchenko T.O.
Signature — Ініціали, прізвище

June «12», 2024

Khmelnytskyi 2024

KHMELNYTSKYI NATIONAL UNIVERSITY

Faculty INFORMATION TECHNOLOGIES

Department COMPUTER ENGINEERING AND INFORMATION SYSTEMS

Education level BACHELOR

Field of study 12 INFORMATION TECHNOLOGY

Major 123 COMPUTER ENGINEERING

Educatin program COMPUTER ENGINEERING AND PROGRAMMING

APPROVED

Head of department T.O. Hovorushchenko

"11" 01 2024 p.

TASK
FOR BACHELOR'S THESIS

Chamunorwa Tinashe

Surname, name, middle name of student

1. Thesis topic Software and Technical Tool for controlling the door lock based on the ESP8266 microcontroller

Supervisor of thesis Nicheporuk A.O., associate professor of CEIS department

Surname, name, middle name,scientific degree

Approved by order of the rector of the university from 15.02.2024 p. № 8

2. Deadline for student submission of project (work) to the department 07.06.2024 p.

3. Source data for the project (work) Task for bachelor thesis

4. The content of the explanatory note (list of issues to be developed)

Analysis of known tools and solutions

Elementary base of the smart RFID door lock system based on the ESP8266 microcontroller in a smart home

A smart RFID door lock system in a smart home based on the ESP8266 microcontroller

5. List of graphic material (with indication of mandatory drawings)

Circuit Diagram

Schematic Diagram

Block diagram

5. Consultants of sections of the bachelor thesis

Section	Surname, initials and position of the consultant	Signature, date	
		task issue	accepted the task
Regulatory control	Zasornova I.O., associate professor of CEIS department		
Anti-plagiarism	Nicheporuk A.O., associate professor of CEIS department		

6. Issue date of the task «11» 01 2024.

CALENDAR PLAN

№	Name of the stages (sections) of bachelor thesis	The term of thesis stages	Note
1	Choosing a research direction and agreeing the topic of the thesis with the supervisor	11.01.2024	passed
2	Acquaintance with the subject area; formulation of the goal and objectives of the research; definition of the object and subject of research	01.02.2024	passed
3	Work on chapter 1 - analysis of known tools and solutions	01.03.2024	passed
4	Work on chapter 2 – elementary base of system	01.04.2024	passed
5	Work on chapter 3 - a smart rfid door lock system in a smart home based on the esp8266 microcontroller	30.04.2024	passed
6	Design of explanatory note according to requirements	25.05.2024	passed
7	Preliminary defense of bachelor thesis	30.05.2024	passed
8	Defence defense of bachelor thesis	June 2024	

Student Signature Chamuunorwa T. Initials, surname

Supervisor Signature Nicheporuk A.O. Initials, surname

№ of Row	format	Designation	Name	Am. of sheets	№ instance	Note
			Text documents			
1		QWCE.20005.20.01.04 EN	Explanatory note	58		
			Graphic materials			
2		QWCE. 20005.20.01.04 E8	Circuit Diagram	1		
3		QWCE. 20005.20.01.04 E8	Schematic Diagram	1		
4		QWCE. 20005.20.01.04 E8	Block diagram	1		

M.	Let	№ of doc	Sign.	Date	QWCE. 20005.20.01.04 EN		
Author		Chamunorwa			Project information	Letter: E	Sheet: 1 / Sheets: 1
Supervisor		Nicheporuk				KhNU, KIін-20-1	
Reg. contr.		Zasornova					
Approve		Hovorushchenko		12.06			

ABSTRACT

Topic of bachelor thesis: «Software and technical tool for controlling the door lock based on the ESP8266 microcontroller».

Author: *Chamunorwa Tinashe*

Supervisor: *Nicheporuk A.O.*

Explanatory note: *58 p.*, 26 *fig.*, 2 *tables*, 4 *appendices*. 32 *references*.

The graphic part: 3 schemas

Keywords RFID DOOR LOCK SYSTEM, ESP8266

Goal: As smart home technologies become increasingly prevalent, the demand for efficient and secure door access control systems has risen significantly. This bachelor thesis focuses on the development of a software and technical tool for managing a smart RFID door lock system based on the ESP8266 microcontroller within a smart home context. The project involves the integration of hardware and software components to create a seamless and user-friendly solution for controlling access to residential properties.

Signature  Date 12.06.2024

CONTENT

INTRODUCTION

In an era where technology continues to shape the way we live, smart homes have emerged as a beacon of modern living. With the integration of intelligent devices and automated systems, homeowners can now experience unprecedented levels of convenience, comfort, and security within their living spaces. Central to this paradigm shift is the evolution of door access control systems, which have transitioned from traditional mechanical locks to sophisticated smart solutions.

As a student embarking on this bachelor thesis journey, I am captivated by the potential of smart technologies to transform everyday experiences. Recognizing the significance of door access control in the realm of home automation, I have chosen to delve into the development of a software and technical tool for managing a smart RFID door lock system within the context of a smart home environment. This endeavor not only aligns with my academic pursuits but also resonates with my passion for innovation and technology.

The foundation of this thesis rests upon the fusion of hardware and software components, with the aim of creating a cohesive and user-centric solution. At its core lies the ESP8266 microcontroller, a versatile platform renowned for its capabilities in the realm of IoT. By harnessing the power of the ESP8266, coupled with RFID technology, I seek to engineer a door access control system that seamlessly integrates into the fabric of a smart home, enhancing both security and convenience.

The significance of this project extends beyond mere technological innovation; it embodies a commitment to addressing real-world challenges faced by homeowners. In an age where security concerns loom large, the need for robust and reliable door access control solutions is more pressing than ever. By developing a software and technical tool that empowers users to remotely manage their door locks, I aspire to offer peace of mind and convenience, ultimately enriching the quality of life within smart homes. Moreover, this thesis represents an opportunity for personal and professional growth. As a student, I am eager to apply theoretical knowledge gained through coursework to a practical, hands-on project. Through meticulous planning, experimentation, and iteration, I aim to cultivate essential skills in problem-solving, project management, and interdisciplinary

collaboration. This journey of exploration and discovery not only propels me towards academic achievement but also equips me with invaluable insights and experiences that will shape my future endeavors.

With a steadfast commitment to excellence and a passion for leveraging technology to improve lives, I embark on the endeavor to develop a software and technical tool for controlling a smart RFID door lock system based on the ESP8266 microcontroller in a smart home environment. As I navigate through the intricacies of hardware design, software development, and system integration, I remain driven by the belief that small steps towards progress can lead to profound transformations in the way we live, work, and interact with our surroundings.

The purpose of the work is to design and implement a prototype of a software and technical tool for controlling a door lock based on an ESP8266 microcontroller

The object of research is the door lock control processes using the ESP8266 microcontroller

The subject of the study is a software and technical tool for controlling a door lock based on an ESP8266 microcontroller

1 ANALYSIS OF KNOWN TOOLS AND SOLUTIONS

1.1 Principles of operation of a Smart RFID Door Lock System

As a student delving into the world of smart home technology, it's essential to understand the intricate principles underlying the operation of a smart RFID door lock system. This system represents a fusion of hardware, software, and advanced RFID technology aimed at revolutionizing traditional door access control mechanisms.Here are the main principles of operation of the Smart RFID Door Lock System

- RFID Technology;
- hardware Components;
- microcontroller Integration;
- access Control Logic;
- locking Mechanism;
- user Interface;
- security Measures.

Radio Frequency Identification (RFID) technology serves as the cornerstone of modern access control systems, including smart RFID door lock systems.Delving into the intricacies of this technology for my thesis, it's crucial to understand RFID's workings in detail.

RFID operates on the principle of wireless communication via radio frequency signals. An RFID system comprises two main components: RFID tags (or cards) and RFID readers. Each RFID tag contains a unique identifier, which can be read by an RFID reader when in proximity.

RFID tags are small electronic devices embedded with a microchip and an antenna. The microchip stores unique identification data, such as a serial number or other relevant information. The antenna enables the tag to transmit and receive radio frequency signals to and from RFID readers.

RFID readers are devices equipped with antennas and circuitry designed to communicate with RFID tags. They emit radio frequency signals that power the RFID tags

within their vicinity. When an RFID tag receives power from the reader, it responds by transmitting its stored data back to the reader.

RFID systems operate across various frequency bands, including low frequency (LF), high frequency (HF), and ultra-high frequency (UHF). LF RFID operates at frequencies around 125 kHz, while HF RFID operates around 13.56 MHz, and UHF RFID operates in the range of 860-960 MHz. Each frequency band offers different advantages and limitations in terms of range, data transfer speed, and interference resistance.

The read range of an RFID system refers to the maximum distance between the RFID reader and the RFID tag for successful communication. LF RFID typically offers shorter read ranges (a few centimeters to a few meters), while HF and UHF RFID can achieve longer ranges (up to several meters). Data transfer between RFID tags and readers occurs through modulation techniques such as amplitude shift keying (ASK), frequency shift keying (FSK), or phase shift keying (PSK).

RFID technology finds applications across various industries, including access control, inventory management, asset tracking, and supply chain logistics. In the context of access control systems, RFID tags are used to grant or deny access to secured areas based on the unique identifiers stored on authorized tags. The contactless nature of RFID technology offers convenience and efficiency, making it ideal for applications requiring fast and seamless identification.

While RFID technology provides numerous benefits, security concerns such as data privacy and unauthorized access must be addressed. Encryption techniques and secure protocols can mitigate the risk of data interception or cloning of RFID tags. Access control systems incorporating RFID technology often integrate additional security features such as authentication mechanisms and audit trails to ensure accountability and traceability.

The RFID reader serves as the interface between the physical RFID tags/cards and the digital system (Figure 1.1). It typically consists of an antenna and circuitry capable of emitting radio frequency signals and receiving responses from RFID tags. The reader powers the RFID tags within its vicinity and captures the unique identifiers stored on these tags.

Figure 1.1 – RFID Reader

The electronic lock mechanism is responsible for physically controlling the locking and unlocking of the door. This mechanism can take various forms, such as electric strikes, magnetic locks, or motorized bolts, depending on the specific requirements of the system and the type of door being used. Electric strikes are often utilized in commercial settings, providing a reliable way to control access by releasing the door latch electrically. Magnetic locks, on the other hand, use a powerful electromagnet to secure the door and are known for their high holding force and durability. Motorized bolts offer a more sophisticated solution, utilizing a motor to extend or retract a bolt for securing the door. Upon receiving signals from the microcontroller, which processes input from RFID readers or other sensors, the electronic lock mechanism actuates accordingly to either secure or release the door, ensuring controlled access and enhancing the security of the premises. This integrated approach allows for seamless and automated control over door access, contributing to the overall efficiency and security of a smart home system.

Another important part is a microcontroller (e.g., ESP8266). The microcontroller serves as the central processing unit of the system, orchestrating communication between hardware components and executing control logic. In this thesis, the ESP8266

microcontroller is chosen for its versatility, built-in Wi-Fi capabilities, and compatibility with IoT applications. It receives data from the RFID reader, processes authentication requests, and sends commands to the electronic lock mechanism.

The appearance of the microcontroller ESP8266 is presented in figure 1.2.

Figure 1.2 – Esp8266 microcontroller

The power supply provides electrical energy to the system's components, ensuring continuous operation. It can be sourced from mains power or battery, depending on the system's design and requirements. Stable and reliable power is essential to maintain the functionality of the RFID reader, microcontroller, and electronic lock mechanism.

These hardware components work together harmoniously to create a robust and efficient smart RFID door lock system. The RFID reader captures data from RFID tags, the microcontroller processes this data to authenticate users, and the electronic lock mechanism physically controls access to the door. With meticulous integration and calibration, these components enable seamless access control while ensuring the security and convenience of smart home environments. Understanding the role and functionality of each hardware component is essential for designing and implementing an effective smart RFID door lock system as part of this thesis project.

As a student undertaking this thesis project, understanding the integration of the microcontroller, specifically the ESP8266, is pivotal to the success of the smart RFID door lock system. The microcontroller serves as the brain of the system, orchestrating communication between hardware components and executing control logic. Let's delve into the integration of the microcontroller within the context of this thesis.

The ESP8266 microcontroller functions as the central processing unit (CPU) of the smart RFID door lock system. It is responsible for receiving input from the RFID reader, processing authentication requests, and sending commands to the electronic lock mechanism.

The ESP8266 microcontroller interfaces with the RFID reader, enabling bidirectional communication to exchange data. It utilizes protocols such as UART (Universal Asynchronous Receiver-Transmitter) or SPI (Serial Peripheral Interface) to establish communication with the RFID reader.

One of the key features of the ESP8266 microcontroller is its built-in Wi-Fi capabilities. It can connect to local Wi-Fi networks, enabling remote access and control of the smart RFID door lock system via web or mobile applications.

Firmware development is a crucial aspect of microcontroller integration. Program code, written in languages such as C or Arduino, is uploaded to the ESP8266 microcontroller to define system behavior and functionality. The firmware implements access control logic, authentication mechanisms, and communication protocols to ensure seamless operation of the door lock system.

In addition to interfacing with the RFID reader, the microcontroller may integrate other sensors or peripherals. These sensors could include proximity sensors for detecting door status, temperature sensors for environmental monitoring, or motion sensors for security purposes. The microcontroller processes data from these sensors to enhance the functionality and versatility of the smart RFID door lock system.

The ESP8266 microcontroller manages power consumption to optimize the system's energy efficiency. It regulates power distribution to the various components, ensuring adequate supply while minimizing unnecessary energy consumption. Power

management features contribute to prolonging battery life (if applicable) and reducing overall operating costs.

Access control logic governs the system's behavior, determining who is granted or denied access based on predefined rules and criteria. Let's delve into the explanation of access control logic within the context of this thesis.

The access control logic initiates with the authentication process, where the system verifies the identity of individuals seeking access. Upon presenting an RFID tag to the reader, the system captures the unique identifier stored on the tag.

The captured RFID tag identifier is compared against a database of authorized users and their corresponding access permissions. This database may be stored locally within the microcontroller or on a remote server accessible via Wi-Fi connectivity.

Based on the database query results, the access control logic determines whether the individual is authorized to access the door. Authorized users are granted access, while unauthorized individuals are denied entry.

Access control logic manages access permissions for each authorized user stored in the database. Permissions may include granting full access, restricted access to specific times or areas, or temporary access for guests or maintenance personnel.

The access control logic incorporates error handling mechanisms to address exceptional cases and potential security breaches. For instance, the system may trigger an alarm or log suspicious access attempts, such as repeated invalid authentication attempts or tampering with the hardware.

In addition to local access control logic, the system may support remote management capabilities via web or mobile applications. Authorized users can remotely modify access permissions, add or revoke user credentials, and monitor access activity in real-time.

To enhance reliability and security, the access control logic may implement redundancy and fail-safe measures. This could include backup power sources, redundant communication channels, or backup access methods in case of system failures or network outages.

An essential aspect of access control logic is maintaining an audit trail of access events. The system logs each access attempt, recording details such as user identity, timestamp, and outcome (granted or denied access). Audit trails provide accountability, traceability, and valuable insights for security analysis and compliance purposes.

The locking mechanism is responsible for physically securing or releasing the door based on the access control decisions made by the system. Let's explore the explanation of the locking mechanism within the context of this thesis.

The smart RFID door lock system utilizes electronic locks to control access to the door. Electronic locks are a modern alternative to traditional mechanical locks, offering enhanced security and convenience.

Types of Electronic Locks:

– electric Strikes: Electric strikes are mechanisms installed within the door frame. When activated, they release the door latch, allowing the door to be opened;

– magnetic Locks: Magnetic locks consist of an electromagnet mounted on the door frame and a metal plate attached to the door. When powered, the electromagnet creates a magnetic force that holds the door securely closed;

– motorized Bolts: Motorized bolts are motor-driven mechanisms that extend or retract bolts to lock or unlock the door. They provide robust security and are suitable for both residential and commercial applications.

Upon receiving an authorization signal from the access control logic, the locking mechanism is activated to either lock or unlock the door. For electric strikes, an electrical impulse retracts the strike plate, allowing the door to open. In magnetic locks, power is supplied to the electromagnet to release the door. Motorized bolts are controlled by a motor that moves the bolts into the locked or unlocked position.

The locking mechanism is integrated with the microcontroller, such as the ESP8266, which orchestrates its operation. The microcontroller sends commands to the locking mechanism based on access control decisions and user input received from the RFID reader and user interface.

Electronic locks may incorporate additional security features to enhance protection against unauthorized access. These features may include anti-tamper sensors, which

trigger alarms if tampering is detected, and fail-secure or fail-safe modes, which specify the lock's behavior in case of power failure.

In the context of a smart home environment, the locking mechanism may support remote control capabilities. Authorized users can remotely lock or unlock the door using a web or mobile application, providing convenience and flexibility.

The chosen locking mechanism should be compatible with the door's construction and dimensions. Factors such as door material, frame type, and installation requirements must be considered to ensure proper functionality and security.

The user interface serves as the primary point of interaction between users and the system, enabling them to manage access control settings, monitor door activity, and interact with the system's features. Let's delve into the explanation of the user interface within the context of this thesis:

A web-based user interface allows users to access the smart RFID door lock system through a web browser on their desktop or mobile device. Users can log in to the interface using their credentials to access system functionalities and manage access control settings remotely.

A dedicated mobile application provides users with convenient access to the smart door lock system from their smartphones or tablets. The mobile app offers similar functionalities to the web-based interface but tailored for a mobile user experience, with optimized layout and navigation.

Figure 1.3 – Open door with your Phone

Features:

– registration of RFID Tags: Users can register new RFID tags or cards within the system through the user interface. This process involves assigning a unique identifier to each tag and associating it with the corresponding user profile;

– access Control Settings: The user interface allows users to define access permissions for each registered RFID tag. This includes specifying authorized time slots, restricting access to certain areas, and managing guest access;

– real-Time Monitoring: Users can monitor door activity in real-time through the user interface. This includes viewing access logs, tracking door status (locked or unlocked), and receiving notifications for access events;

– remote Control: The user interface enables users to remotely lock or unlock the door, providing flexibility and convenience, especially when away from home.

The user interface features a intuitive and user-friendly design, with clear navigation menus, descriptive icons, and interactive elements. User experience (UX) principles are employed to ensure seamless interaction and ease of use, minimizing user confusion and frustration.

Security is a top priority in the design of the user interface. Measures such as encrypted communication, secure authentication methods (e.g., passwords or biometrics), and access control policies are implemented to safeguard user data and system integrity. Multi-factor authentication may be incorporated to provide an additional layer of security, especially for sensitive actions such as unlocking the door remotely.

The user interface may offer customization options to tailor the system to individual user preferences. This could include customizable themes, language settings, and personalized access control profiles.

Security is paramount in ensuring the integrity and reliability of the system, safeguarding against unauthorized access and potential vulnerabilities. Let's delve into the explanation of security measures within the context of this thesis.

Implementing encryption protocols is essential to secure communication between system components. HTTPS (Hypertext Transfer Protocol Secure) or TLS

(Transport Layer Security) encryption can be employed to encrypt data transmitted between the RFID reader, microcontroller, user interface, and remote servers. Encryption ensures that sensitive information, such as RFID tag identifiers and access control commands, remains confidential and protected from interception by unauthorized parties.

Robust access authentication mechanisms are implemented to verify the identity of users and prevent unauthorized access to the system.

Password authentication: Users are required to authenticate themselves with a username and password before accessing the system's functionalities. Biometric verification: Biometric authentication methods, such as fingerprint or facial recognition, may be integrated for enhanced security.

Multi-factor authentication: Multi-factor authentication combines multiple authentication factors, such as passwords, biometrics, and one-time codes, to strengthen access control and mitigate the risk of unauthorized access.

Access control policies dictate the rules and permissions governing access to the smart RFID door lock system. Role-based access control (RBAC) may be implemented to define access levels and privileges for different user roles (e.g., administrators, residents, guests). Time-based access control allows users to specify access permissions based on predefined time slots, restricting access during certain hours or days of the week.

Logging access events and maintaining audit trails is essential for accountability, traceability, and forensic analysis. The system logs access attempts, including successful and unsuccessful authentication events, door lock/unlock actions, and system configuration changes. Audit trails provide a detailed record of system activity, enabling administrators to track user actions, identify security breaches, and investigate incidents.

In addition to digital security measures, physical security measures are implemented to protect the system from tampering and unauthorized access. Tamper-proof enclosures and tamper detection sensors can be installed to detect and deter physical attacks on the system. Secure mounting of hardware components, such as the

RFID reader and electronic lock mechanism, ensures they cannot be easily manipulated or tampered with.

Regular software updates and patches are essential to address security vulnerabilities and mitigate potential threats. The system's firmware and software components should be kept up-to-date to incorporate the latest security enhancements and patches released by the manufacturer.

1.2 Analysis of known automated door locking systems

Analyzing known automated door locking systems provides valuable insights into the design, functionality, and performance of such systems. Here's an analysis based on some well-known automated door locking systems.

August Smart Lock:

– design: August Smart Lock is a retrofit smart lock designed to replace existing deadbolts, featuring a sleek and minimalistic design;

– functionality: It offers keyless entry, remote locking and unlocking via a mobile app, and integration with popular smart home platforms like Amazon Alexa, Google Assistant, and Apple HomeKit;

– security: August Smart Lock uses encrypted communication and two-factor authentication for secure access control;

– user Experience: The system provides a user-friendly mobile app interface for managing access permissions, viewing activity logs, and controlling the lock remotely;

– integration: It integrates with other smart home devices and services, allowing users to create automation routines and scenarios;

– feedback: Users receive real-time notifications and feedback on lock status changes and activities.

In figure 1.4 present the august smart lock.

Figure 1.4 – August Smart Lock

Schlage Connect Smart Deadbolt:

– design: Schlage Connect Smart Deadbolt is a motorized deadbolt lock with a traditional design, available in various finishes to match different door aesthetics.

– functionality: It offers keyless entry, remote access via a smartphone app, and integration with smart home platforms like Amazon Alexa and Google Assistant.

– security: Schlage Connect features built-in alarm sensors to detect potential threats and tampering, along with encryption for secure communication.

– user Experience: The lock provides a keypad for code-based entry, in addition to smartphone app control, catering to different user preferences.

– integration: It seamlessly integrates with Z-Wave smart home systems, allowing for broader interoperability with other devices.

– feedback: Users receive audible feedback and visual indicators on the lock's status and battery life.

Figure 1.5 – Schlage Connect Smart Deadbolt

Yale Assure Lock SL:

– design: Yale Assure Lock SL features a slim and modern touchscreen keypad design, suitable for contemporary home aesthetics.

– functionality: it offers keyless entry, remote access via a smartphone app, and compatibility with voice assistants like Amazon Alexa, Google Assistant, and Apple HomeKit.

– security: the lock utilizes AES 128-bit encryption for secure communication and offers optional integration with a Z-Wave smart home hub for enhanced security features.

– user Experience: the touchscreen keypad provides a convenient alternative to traditional key-based entry, and the lock's mobile app interface offers intuitive control and management features.

– integration: it integrates with various smart home ecosystems, allowing users to incorporate door lock control into broader automation routines.

– feedback: Users receive notifications and activity logs via the mobile app, providing insights into door access events and lock status changes.

Figure 1.6 – Yale Assure Lock SL

Kwikset Kevo Smart Lock

– design: Kwikset Kevo Smart Lock features a traditional deadbolt design with a touch-to-open functionality, allowing users to unlock the door with a simple touch;

– functionality: it offers touch-to-open convenience, remote access via a smartphone app, and integration with smart home platforms like Amazon Alexa and Nest;

– security: Kevo Smart Lock uses multiple levels of encryption for secure communication and offers eKeys for controlled access sharing;

– user Experience: the touch-to-open feature provides a hands-free unlocking experience, while the mobile app offers additional control and management capabilities.

– integration: it integrates with select smart home platforms, enabling users to incorporate door lock control into broader smart home setups;

– feedback: users receive notifications and activity history via the mobile app, allowing them to monitor door access events and lock status changes.

Figure 1.7 – Kwikset Kevo Smart Lock

1.3 Conclusion and problem statement

As I embark on this thesis , the focus lies on addressing the pressing need for a secure, efficient, and user-friendly access control solution within smart home environments. Traditional mechanical door locks are increasingly being replaced by smart RFID door lock systems, offering enhanced convenience and security. However, existing solutions often lack comprehensive integration, robust security measures, and user-friendly interfaces, leaving homeowners vulnerable to potential security breaches and usability challenges.

The problem at hand encompasses several key issues:

– lack of Comprehensive Integration: existing smart RFID door lock systems may lack seamless integration between hardware components, software functionalities, and user interfaces. Inconsistencies or gaps in integration can result in suboptimal performance, reliability issues, and usability challenges for end-users;

– security Concerns: security is a paramount concern in smart home environments, particularly concerning access control systems. Many off-the-shelf RFID door lock systems may lack robust security measures, leaving them vulnerable to unauthorized access, data breaches, and tampering;

– usability and User Experience: the usability and user experience of smart RFID door lock systems play a crucial role in their adoption and effectiveness. Complex user interfaces, cumbersome setup processes, and lack of intuitive controls can hinder user acceptance and satisfaction;

– limited Remote Management Capabilities: remote management capabilities, such as remote access control and real-time monitoring, are increasingly essential for modern smart home environments. However, existing solutions may offer limited or unreliable remote management features, limiting homeowners' ability to control and monitor access to their properties remotely;

– lack of Customization and Flexibility: homeowners may have diverse requirements and preferences regarding access control settings, user management, and integration with other smart home devices. Existing smart RFID door lock systems may lack customization options and flexibility to accommodate varying user needs effectively.

In light of these challenges, the thesis aims to develop a comprehensive software and technical tool for controlling a smart RFID door lock system based on the ESP8266 microcontroller in a smart home environment. The goal is to address the aforementioned shortcomings by integrating hardware and software components, implementing robust security measures, designing an intuitive user interface, enhancing remote management capabilities, and offering customization options to meet the diverse needs of homeowners. By tackling these issues, the thesis seeks to contribute to the advancement of access control technology in smart home environments, ultimately enhancing security, convenience, and user experience for homeowners.

2 ELEMENTARY BASE OF THE SMART RFID DOOR LOCK SYSTEM BASED ON THE ESP8266 MICROCONTROLLER IN A SMART HOME

2.1 Smart RFID door lock system and the Elementary base

As I continue to delve into the development of a smart RFID door lock system based on the ESP8266 microcontroller, the selection of elementary components forms the foundation of the project. Here's a detailed description of each component that I will use to make the Smart RFID Door Lock System.

The proposed software-technical device consists of the following hardware components:

- ESP8266 (NodeMCU);
- RC522 RFID Reader;
- door Lock Mechanism(KF-301 Relay Module);
- KF-301 Relay Module;
- 9V Battery;
- voltage Regulators (LM7805 and AMS1117);
- breadboard and Jumper Wires.

The ESP8266 microcontroller is a low-cost Wi-Fi microchip with full TCP/IP stack and microcontroller capability (figure 2.1).

I chose the ESP8266 microcontroller because of its integrated Wi-Fi capabilities, low cost, and compatibility with Arduino IDE for easy programming. Its processing power and connectivity make it suitable for managing RFID authentication, user interface interactions, and communication with other smart home devices. It acts as the central unit of the system. It reads data from the RFID reader, processes it, controls the door lock mechanism, communicates with the LCD display, and connects to the MQTT broker over Wi-Fi for remote monitoring and control.The required voltage for the ESP8266 is 5V.

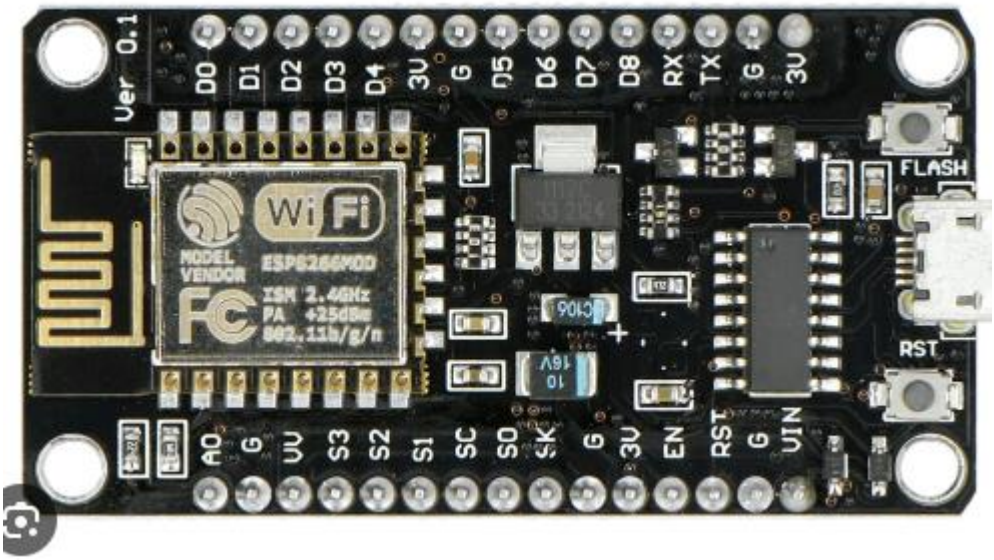


Figure 2.1 – ESP8266

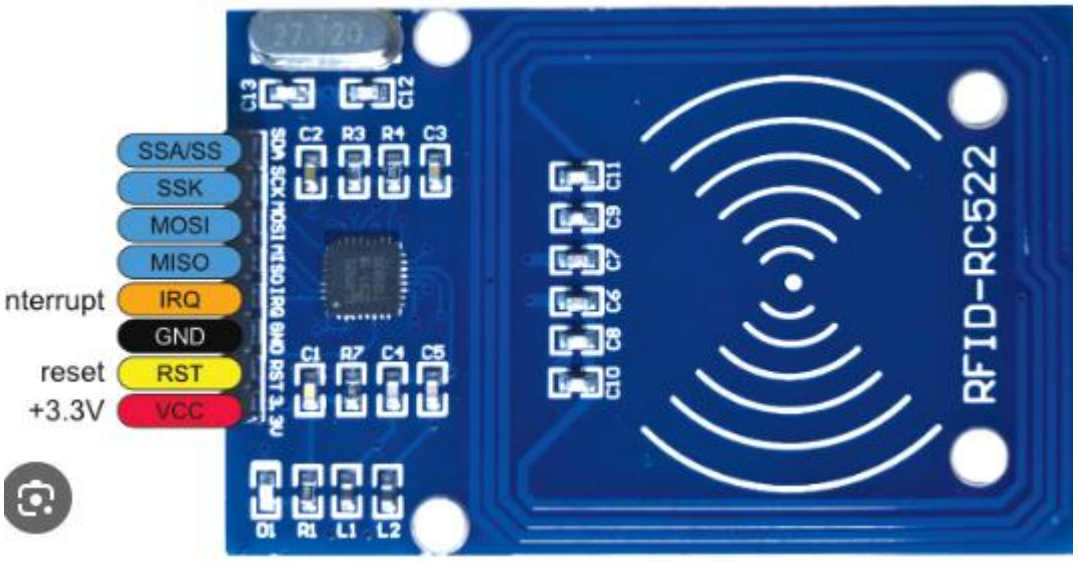


Figure 2.2 – RC522 RFID Reader

A relay module is a relay that has been mounted on a board with other components to provide isolation and protection (figure 2.3). This makes them easier to use in a variety of applications. The use of relay module devices offers a simple and convenient way to control electrical equipment systems remotely. In this thesis I am using the KF-301 relay module which will serve as a critical component for safey and effectively controlling the door locking mechanism. By using the relay module, the system can handle higher power

requirements and ensure isolation between the control circuit and the high-power load, enhancing both functionality and safety.

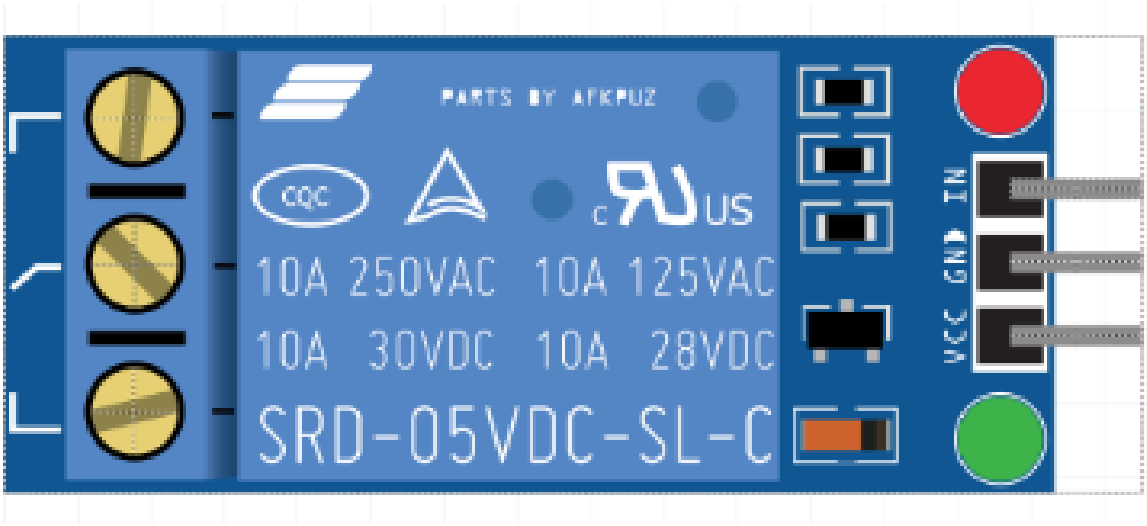


Figure 2.3 – KF-301 Relay Module

A stable power supply is essential for continuous operation of the system. For ths RFID door lock system,I am using a 9V battery as a source of power, it supplies power to the ESP8266, RFID reader, relay, and other components (figure 2.4). Typically regulated down to 5V and 3.3V using voltage regulators.

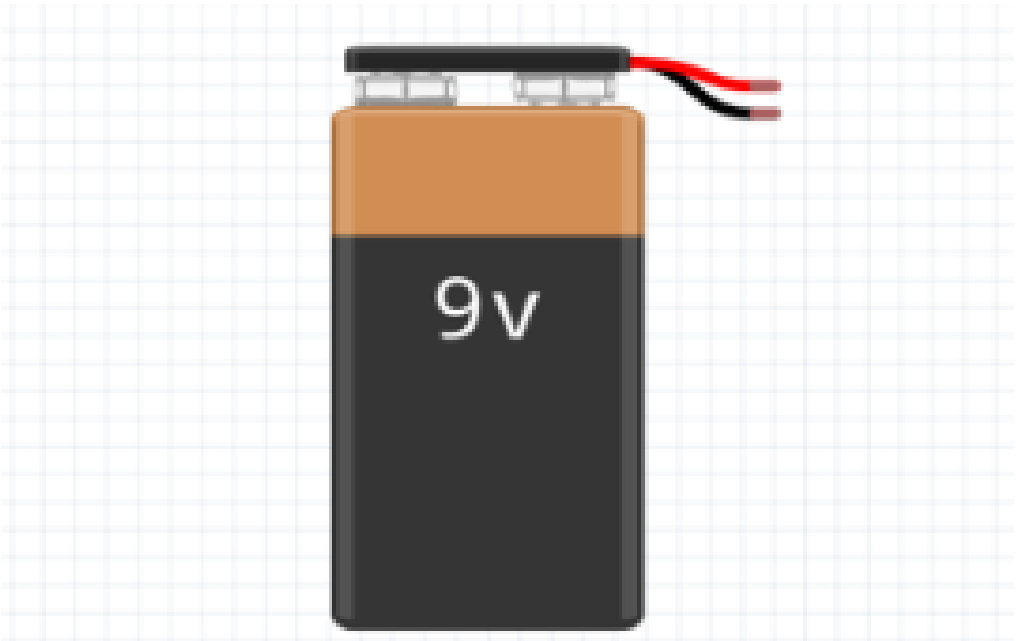


Figure 2.4 – 9V Battery

Liquid Crystal Display (LCD) with I2C Interface (figure 2.5). The I2C LCD component is used in applications that require a visual or textual display. This component is also used where a character display is needed but seven consecutive GPIOs on a single GPIO port are not possible. For this system I am using a 16x2 character LCD with an I2C interface that simplifies connections to the microcontroller.It displays status messages such as "Access Granted", "Access Denied", or the UID of the scanned RFID card. Provides visual feedback to the user.

Figure 2.5 – LCD display

Voltage Regulators (LM7805 and AMS1117). A voltage regulator is a system designed to automatically maintain a constant voltage (figures 2.6, 2.7). It may use a simple feed-forward design or may include negative feedback. It may use an electromechanical mechanism, or electronic components. Depending on the design, it may be used to regulate one or more AC or DC voltages.Since I am using a power source that provides 9V theres need to regulate the voltage so that it may suit the power need for all components,the voltage regulator will help me regulate the voltage specifically for every component .For this system I used two voltage regulators which are LM7805 and

AMS1117.The LM7805 converts higher voltages to stable 5V output.In this system I am using it to regulate 9V to 5V out for components like the relay module and LCD .The AMS1117 converts the 5V to 3.3 V which is needed by the ESP8266 and RC522.

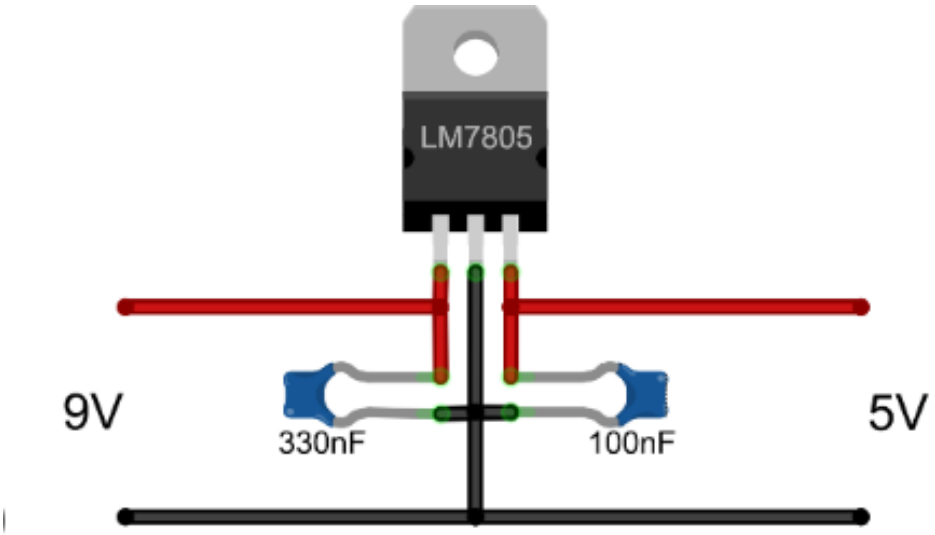


Figure 2.6 – LM7805

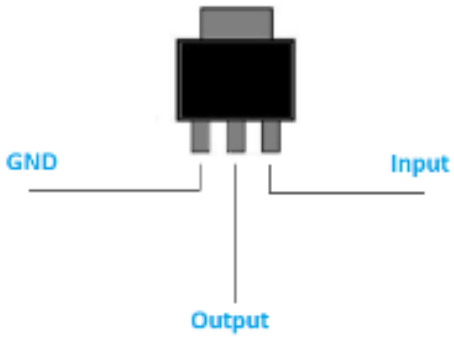


Figure 2.7 – AMS1117

Breadboard and Jumper Wires. A breadboard is a construction base for prototyping electronics, and jumper wires are used to make connections. Provides a platform to connect all components together without soldering, allowing for easy adjustments and modifications.

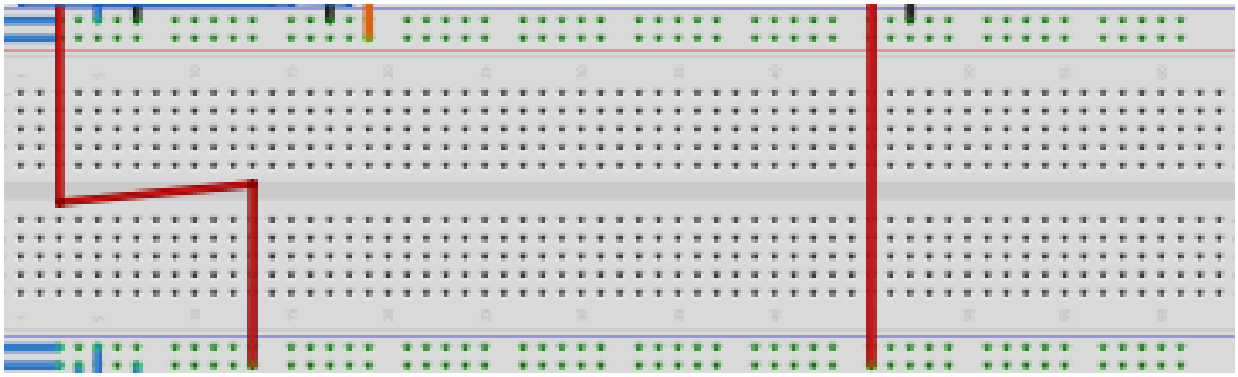


Figure 2.7 – Breadboard

User Interface (Smartphone which is a MQTT Client). The user interface enables users to interact with the system, configure access settings, and receive feedback. Options include physical interfaces like push buttons or touchpads, complemented by status indicators such as LEDs or LCD displays to provide visual feedback. Integration with digital interfaces like mobile apps or web-based dashboards may enhance usability and enable remote management of the door lock system. The mobile phone will act as a MQTT Client by monitoring the door lock status and sending remote control commands to the ESP8266. The smartphone subscribes to the status topic and publishes control commands to the appropriate topic. The mobile app will act as the user interface.

Figure 2.7 – Door loocking system

Security measures are paramount to protect against unauthorized access and ensure the integrity of the system. Implementations may include encryption of communication between components, authentication mechanisms for user access, and physical security enhancements like tamper detection or intrusion alarms. Integration of secure protocols and best practices, along with regular firmware updates, helps mitigate potential security risks.

Components should be selected to ensure compatibility and seamless integration with other smart home devices and platforms. The ESP8266 microcontroller's Wi-Fi connectivity allows integration with popular IoT platforms like MQTT or Home Assistant, enabling interoperability and expanding the system's capabilities. Considerations for communication protocols, such as MQTT for messaging or HTTP for web-based interfaces, facilitate integration with existing smart home ecosystems.

Cost-effectiveness is an important consideration in component selection, balancing performance and features within budget constraints. Evaluating the total cost of ownership, including initial setup costs, ongoing maintenance, and potential scalability, ensures the project remains financially viable.

By carefully selecting and integrating these elementary components, a solid foundation for the smart RFID door lock system based on the ESP8266 microcontroller is established. This provides the groundwork for further development, customization, and refinement to meet specific project requirements and objectives.

2.2 Basic operation of a Smart RFID Door Lock System using ESP8266 Microcontroller in a Smart Home Environment

Let’s describe the system. The Smart RFID Door Lock System integrates an RFID reader with an ESP8266 microcontroller to control access to a door in a smart home environment. It enables users to unlock the door using RFID cards or tags.

The proposed software-technical device consists of the following hardware components:

– ESP8266 Microcontroller(NodeMCU): this is the brain of the system, responsible for processing data, controlling the RFID reader, and managing the locking mechanism;

– RFID Reader: it reads RFID tags or cards to identify authorized users;

– door Lock Mechanism: the physical lock on the door that is controlled by the microcontroller;

– power Supply: provides electrical power to the system, usually through a standard AC outlet or battery.

Software Components Of The Proposed Device:

– firmware: programmed onto the ESP8266 microcontroller, the firmware manages the communication between the RFID reader and the door lock mechanism. It also handles user authentication and access control logic;

– user Interface : a smartphone app or web interface that allows users to manage access permissions, view access logs, and remotely control the door lock.

Basic Operation Of The Proposed Device:

– initialization: the system boots up, and the ESP8266 microcontroller initializes the RFID reader, connects to the local Wi-Fi network (if applicable), and prepares to receive commands;

– user Authentication: when a user approaches the door, they present their RFID card or tag to the RFID reader. The RFID reader reads the unique identifier from the card/tag and sends it to the microcontroller. The microcontroller compares the received identifier with the list of authorized users stored in its memory;

– access Control: if the identifier matches an authorized user, the microcontroller sends a signal to the door lock mechanism to unlock the door. If the identifier does not match or is not recognized, the microcontroller denies access and may trigger an alert (e.g., sound an alarm or send a notification);

– locking/Unlocking: upon receiving the unlock command from the microcontroller, the door lock mechanism disengages, allowing the user to open the door. After a specified period or when the door is closed, the microcontroller sends a signal to re-engage the lock, securing the door.

2.3 Overview of single-board computer systems and MQTT

Single-board computer (SBC) systems are complete computer systems built on a single circuit board (figure 2.8). They typically include a microprocessor, memory, input/output (I/O) ports, and other essential components required for computing tasks. SBCs are compact, affordable, and versatile, making them popular for various applications, from hobbyist projects to industrial automation.

Figure 2.8 – Raspberry Pi

Here's an overview of single-board computer systems:

Components of a single-board computer:

– SBCs often feature a microprocessor or system-on-chip (SoC) that serves as the central processing unit (CPU). Common processor architectures include ARM, x86, and RISC-V;

– SBCs come with onboard memory, including RAM for running programs and storage for storing data and operating system files. Some SBCs also support expansion via external memory cards or modules;

– SBCs include various I/O ports for connecting peripherals and external devices, such as USB ports, HDMI or DisplayPort for video output, Ethernet ports for networking, GPIO pins for general-purpose input/output, and audio jacks;

– SBCs may feature onboard storage options, such as eMMC flash memory or onboard SD card slots. They also support external storage devices like USB drives or network-attached storage (NAS) for additional storage capacity;

– Many SBCs include built-in Wi-Fi and Bluetooth capabilities for wireless connectivity. They may also feature Ethernet ports for wired networking;

– Some SBCs offer expansion slots like PCIe or mini PCIe for adding additional functionality, such as GPUs, SSDs, or other expansion cards.

Operating Systems of Single board Computer:

– SBCs support a variety of operating systems, including Linux distributions (e.g., Debian, Ubuntu, Raspbian for Raspberry Pi), Android, Windows 10 IoT Core, and custom operating systems tailored for specific applications;

– the choice of operating system depends on factors such as compatibility with the hardware, software requirements, and user preference.

Applications of a sinhle board computer:

– SBCs have a wide range of applications across various industries and domains, including;

– SBCs like the Raspberry Pi are popular in educational settings for teaching programming, electronics, and computer science concepts;

– SBCs are used in IoT projects for collecting sensor data, controlling devices, and building smart home automation systems;

– SBCs are used in embedded systems for industrial automation, robotics, automotive applications, and more;

– hobbyists and makers use SBCs for DIY projects such as media centers, retro gaming consoles, home servers, and home automation systems;

– engineers and developers use SBCs for rapid prototyping of hardware and software solutions before moving to production.

Development Tools of a single board computer:

– SBCs typically come with software development tools and resources to facilitate application development. These may include SDKs (Software Development Kits), programming libraries, community forums, and documentation;

– common programming languages for SBC development include Python, C/C++, Java, and JavaScript.

Advantages of single board computer systems:

– SBCs are compact and lightweight, making them suitable for space-constrained environments and portable applications;

– SBCs are cost-effective compared to traditional desktop or server systems, making them accessible to hobbyists, students, and small businesses;

– SBCs are versatile platforms that can be customized and adapted for a wide range of applications and projects;

– SBCs often come with user-friendly interfaces and software tools, making them accessible to users with varying levels of technical expertise.

Limitations of a single board computer:

– SBCs typically have lower processing power and memory compared to traditional desktop or server systems, limiting their suitability for resource-intensive tasks;

– SBCs may have limited I/O capabilities compared to larger systems, which can restrict their connectivity options and peripheral support;

– while some SBCs support expansion via external interfaces, they may not offer the same level of scalability and flexibility as larger systems.

MQTT Protocol. MQTT stands for Message Queuing Telemetry Transport. It is a lightweight messaging protocol for use in cases where clients need a small code footprint and are connected to unreliable networks or networks with limited bandwidth resources. It is primarily used for machine-to-machine (M2M) communication or Internet of Things types of connections.

In this thesis, MQTT or Message Queuing Telemetry Transport, is a protocol that allows smart home devices to communicate with each other. It's a messaging protocol that uses a publish-subscribe model, which means that devices can publish messages to topics, and other devices can subscribe to those topics to receive the messages.

The MQTT as several components which include the Broker and the Client. MQTT protocol simple block diagram is presented on firuge 2.8.

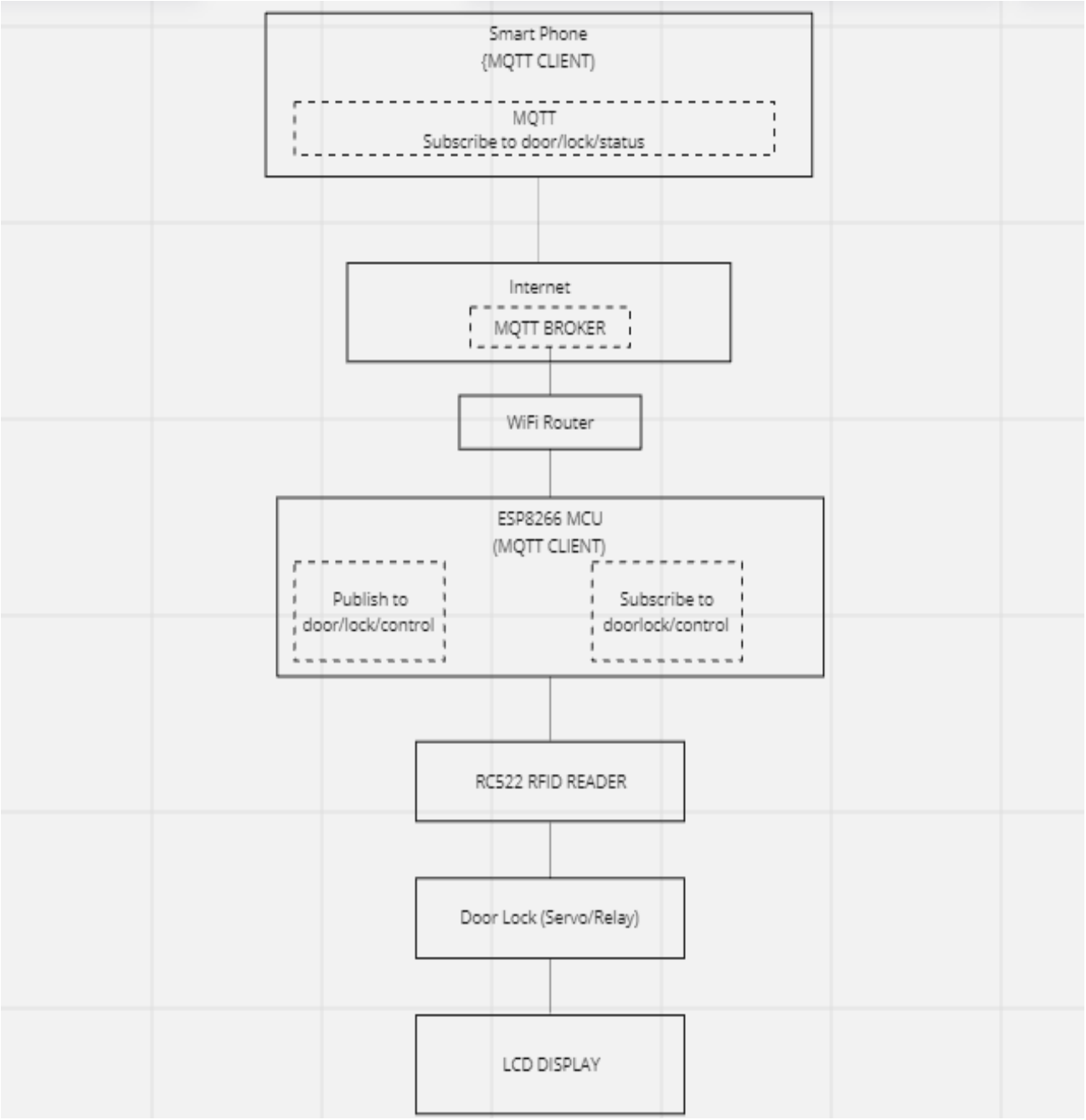


Figure 2.8 – MQTT protocol simple block diagram

The Broker is the backend system which coordinates messages between the different clients. Responsibilities of the broker include receiving and filtering messages, identifying clients subscribed to each message, and sending them the messages. A widespread broker is Mosquitto.

The Client is any device from a server to a microcontroller that runs an MQTT library. If the client is sending messages, it acts as a publisher, and if it is receiving messages, it acts as a receiver. Basically, any device that communicates using MQTT over a network can be called an MQTT client device.

The ESP8266 (MQTT Client) Publishes the UID to the MQTT broker on the topic "door/lock/status" when an RFID card is scanned.It also Subscribes to the topic "door/lock/status" to receive commands from remote devices for examples to unlock the door.

The ESP8266 connects to the WiFi router to gain access to internet and communicate with the broker.

The broker server routes messages between the ESP8266 and other MQTT clients like smart phones .It receives UID from the ESP8266 and sends control commands from the smartphone back ot the ESP8266.

Smartphones subscribe to "door/lock/status" to receive notifications when an RFID card is used,it can also publish messages to "door/lock/status" to remotely unlock the door.

As for the RC522 RFID Reader,it reads RFID cards and sends UID to the ESP8266 for processing.

The door lock is controlled by the ESP8366 to physically lock and unlock the door based on the RFID card UID or remote commands received via MQTT.

Lastly the LCD will display the status of the door lock system.Like access granted or access denied .

MQTT offers a simple and stable option for integrating Smart Lock into your home automation.It allows you to send and receive messages from your door lock system over the internet.

You can receive notifications on your phone or computer when someone uses the RFID reader and even unlock the door remotely.

It can also be used to send RFID access logs to a central server or cloud service. This data can be analyzed later to study usage patterns, security breaches, or for general record-keeping.

Using MQTT allows the door lock to integrate seamlessly with other smart devices, like lights, cameras, or alarms, enhancing the overall functionality of the smart home.

MQTT is scalable, meaning you can add more devices or extend functionality without significant changes to your existing setup. This makes it easier to add more smart locks or additional sensors.Working with MQTT has given me hands-on experience with an industry-standard protocol used widely in IoT projects. This knowledge is beneficial for my future projects or career.

2.4 Summary of Connections and Voltages of the Proposed Devise (Smart RFID Door Lock)

Power Supply: Since I am using a 9V battery ,I connected it to the input of the LM7805 voltage regulator. The LM7805 outputs 5V, which is used to power the relay module, and LCD display. The AMS1117 voltage regulator takes the 5V from the LM7805 and outputs 3.3V, which is used to power the ESP8266 and RC522 RFID reader.

ESP8266 Connection with other components : VCC pin of the ESP8266 is connected to the 3.3V rail on the breadboard. GND pin of the ESP8266 is connected to the ground rail. GPIO pins of the ESP8266 are connected to the control pins of the relay module, and LCD display.

RC522 RFID Reader: VCC pin is connected to the 3.3V rail. GND pin is connected to the ground rail. SPI pins (SDA, SCK, MOSI, MISO, RST, IRQ) are connected to corresponding GPIO pins on the ESP8266.

Relay Module: VCC pin is connected to the 5V rail. GND pin is connected to the ground rail. IN pin is connected to a GPIO pin on the ESP8266.

LCD Display (I2C): VCC pin is connected to the 5V rail. GND pin is connected to the ground rail. SDA and SCL pins are connected to corresponding GPIO pins on the ESP8266 for I2C communication

Table 2.1 – Summary of the connection amongst the components of the Door Lock

Component	Connection Points	Voltage Requirement	Comments on the components
9V Battery	V+ and GND	9V	Provides the main power supply for the system
Voltage Regulator (LM7805)	Input:9V battery V+ and GND Output:5V rail on Breadboard,GND	Input:9V Output:5V	Regulates 9V down to 5V for components requiring 5V
Voltage Regulator (AMS1117)	Input 5V rail Output 3.3V rail on breadboard,GND	Input :5V Output:3.3V	Regulates 5V down to 3.3V for components requiring 3.3V
ESP8266	VCC:3.3V rail GND:GND GPIO pins:Connected to RFID.Relay,LCD	3.3V	Main controller of the system.Powered by the 3.3V rail
RC522 RFID Reader	VCC:3.3V rail GND:GND SDA,SCK,MOSL,MIDO,RST,IRQ: Connected to ESP8266	3.3V	Communicates with ESP8266 over SPL

Continue of Table 2.1 – Summary of the connection amongst the components of the Door Lock

Relay Module	VCC:5V rail,GND:GND,IN:GPIO pin of ES8266,NO/NC and COM:connected devices	5V	Controlled by the ESP8266 to switch the lock ,the relay coil is powered by 5V
LCD Display(I2C)	VCC:5V rail,GND:GND,SDA,SCL:connected to GPIO Pins of ESP8266	5V	Displays status messages .Communicates with the ESP8266 over I2C.

2.5 Conclusion

The considered issues regarding the basic operation of the smart RFID door lock system using the ESP8266 microcontroller in the smart home environment allow the following conclusions to be drawn. The ESP8266 microcontroller-based smart RFID door lock system is an effective solution for providing security and comfort in smart homes. It provides contactless access to premises using radio frequency identification (RFID), allowing users to open doors using RFID cards or key fobs. The main elements of the system include an RFID reader, an ESP8266 microcontroller, an electromagnetic lock and a power source. The ESP8266 microcontroller acts as the central element of the system, managing the process of identification and granting of access. It receives data from the RFID reader, checks it against the database of authorized users and, in case of a positive match, activates the electromagnetic lock to open the door. In addition, the ESP8266 can connect to a Wi-Fi network, which allows you to integrate the system with other smart home components and remotely control access.

3 A SMART RFID DOOR LOCK SYSTEM IN A SMART HOME BASED ON THE ESP8266 MICROCONTROLLER

3.1 Environment preparation

Arduino IDE and ESP8266. The Arduino Integrated Development Environment contains a text editor for writing code, a message area, a text console, a toolbar with buttons for common functions and a series of menus. It connects to the Arduino hardware to upload programs and communicate with them whereas the ESP8266 is a small, low-cost Wi-Fi microchip with full TCP/IP stack and microcontroller capability. This means it can connect to Wi-Fi networks and communicate with other devices or the internet. It's commonly used in IoT (Internet of Things) projects because of its affordability and versatility.

The Arduino IDE provides a user friendly interface for writing ,compiling ,and uploading code to the microcontroller.In this thesis the Arduino IDE will allow me to write a code for controlling the ESP8266,handling the RFID authentication ,managing door locking mechanisms ,and interfacing with other components of the system.As for the ESP8266,it is the heart of this thesis or project in the sense that it serves as the microcontroller and is responsible for controlling the RFID door lock system and connecting it to the internet in a Smart Home Environment.Its built-in Wi-Fi capability enables communication with other devices and remote access to the door lock system.Because of its low cost,small size and versatility,the ESP8266 is an ideal choice for my thesis.

Let's consider in more detail the process of installing the development environment Arduino IDE.

To start working with Arduino IDE, you need to download the program from the official website: https://www.arduino.cc/en/software.

The installation steps include:

Step1:Open file and go to preferences and open it (figure 3.1).

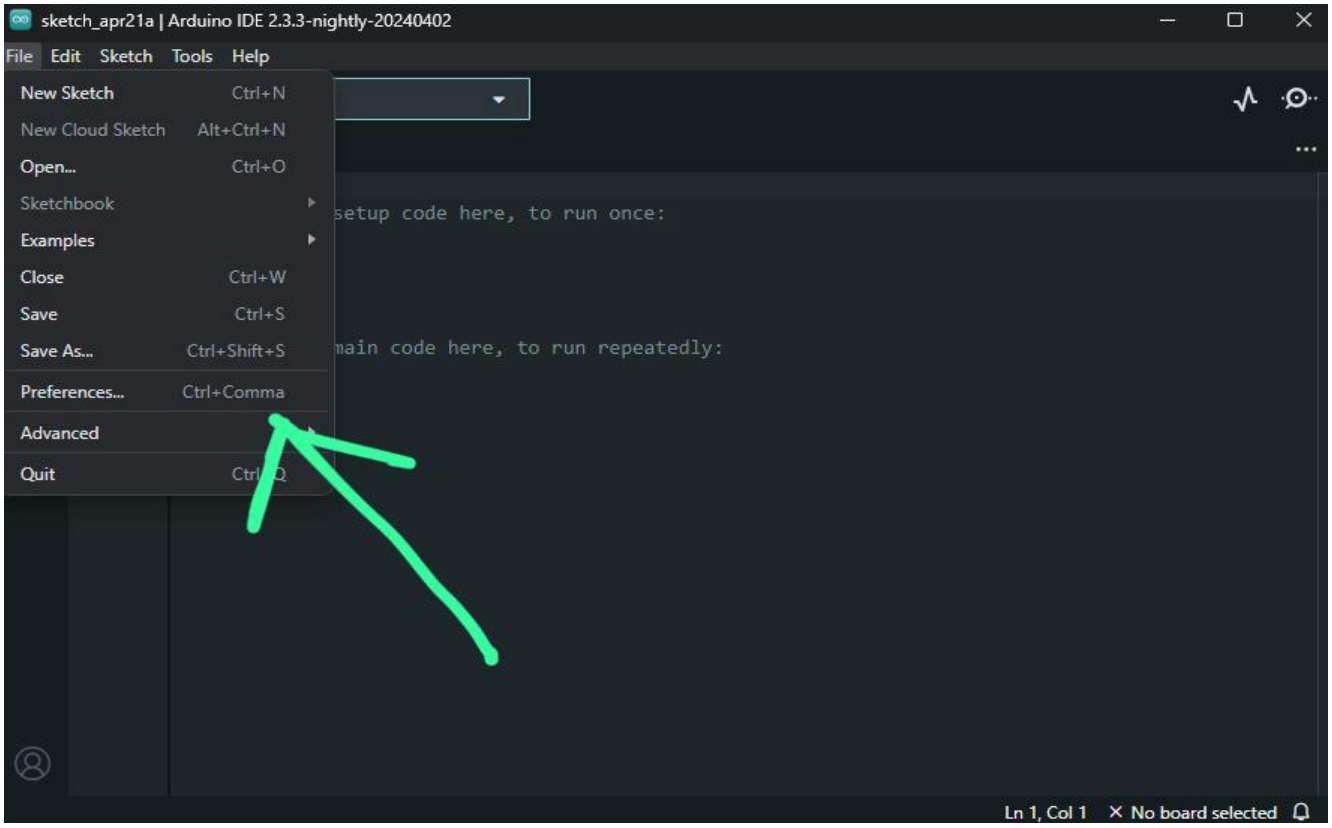


Figure 3.1 – Step1

Step 2: In the "Additional Board Manager URLs" field, add the following URL:

http://arduino.esp8266.com/stable/package_esp8266com_index.json

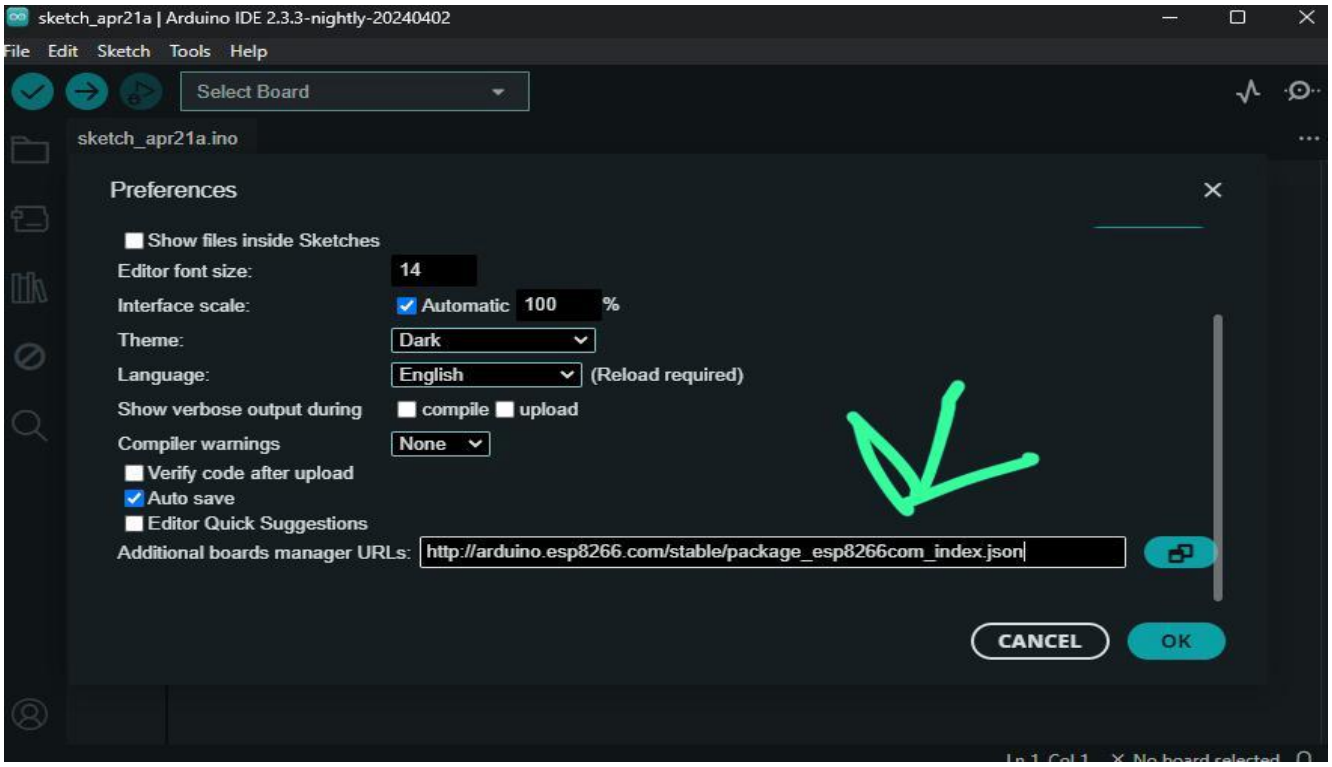


Figure 3.2 – Step2

Step 3: After adding the URL,go to Tools >Board>Boards Manager (figure 3.3).

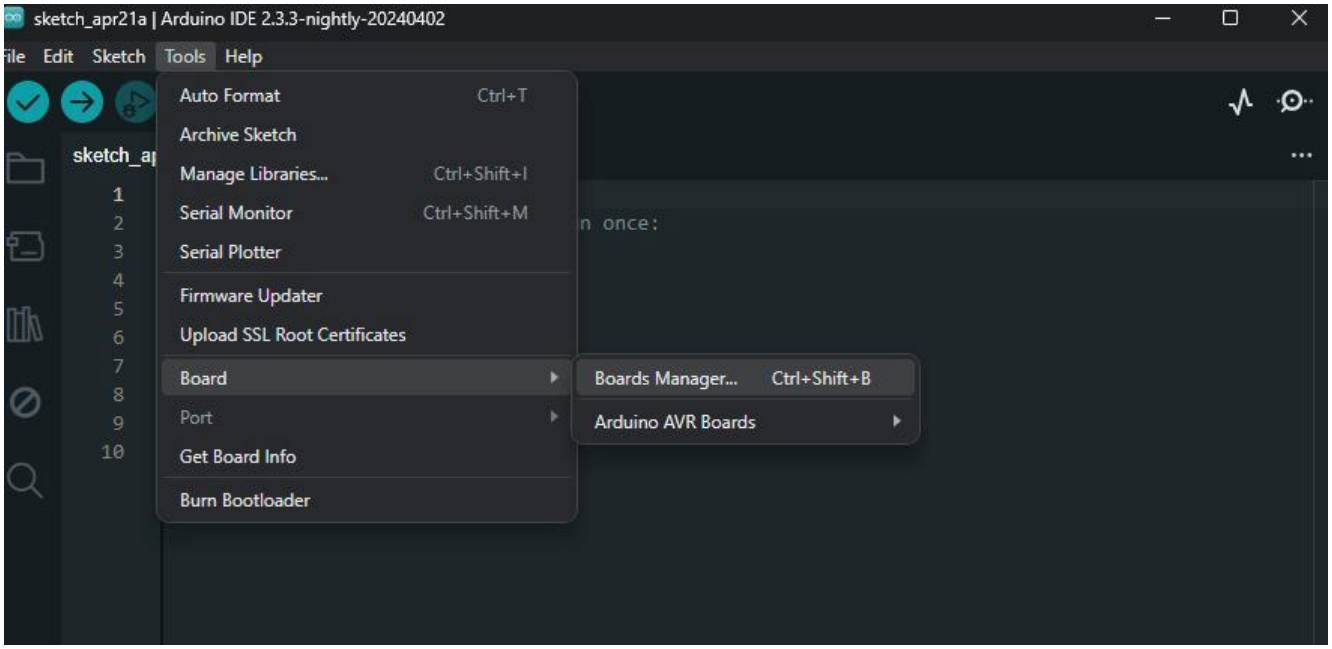


Figure 3.3 – Step3

Step 4: In the Boards Manager, type "ESP8266" into the search bar. Select the "esp8266 by ESP8266 Community" package and click the "Install" button (figure 3.4).

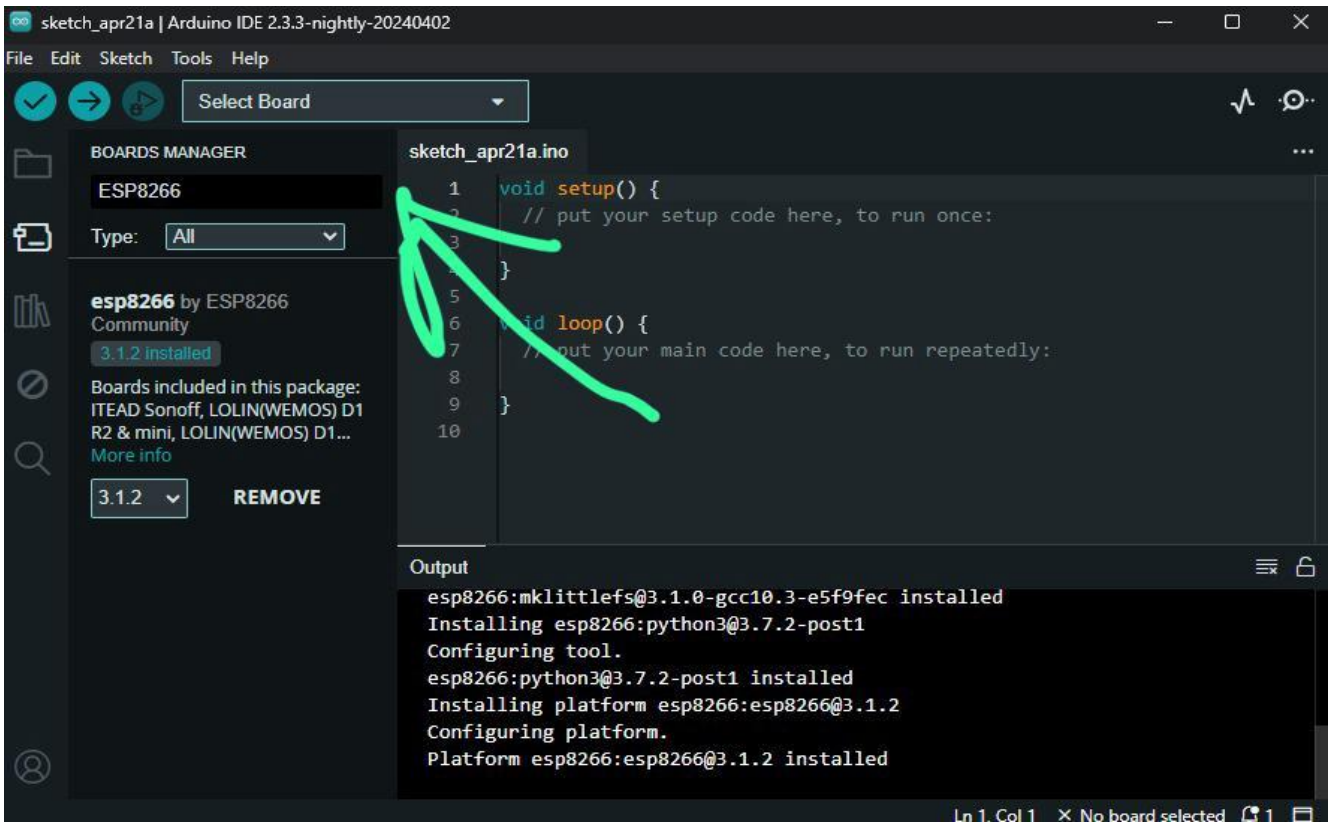


Figure 3.4 – Step4

Step 5:Confirmation of the Installation of the ESP8266 (figure 3.5).

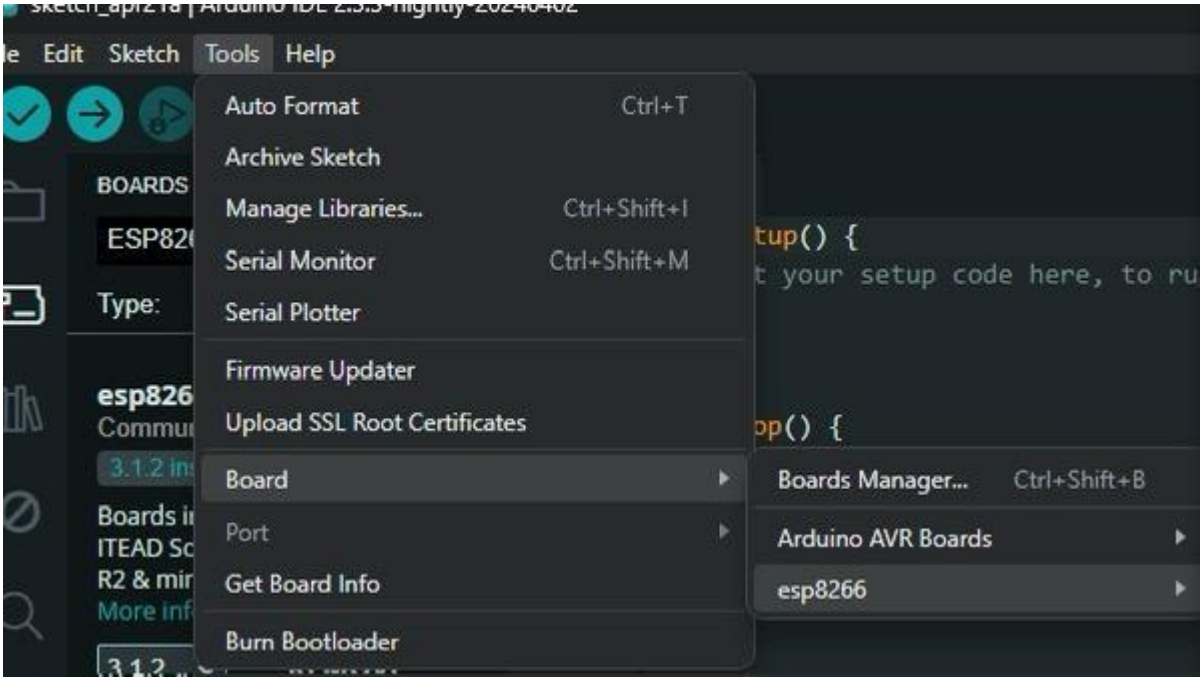


Figure 3.5 – Step5

3.2 Breadboard connection and schematic diagram

Fritzing is a software tool designed to help electronics enthusiasts and beginners create and document electronic circuits in an intuitive and visual way. It provides a platform for designing circuit diagrams, PCB layouts (printed circuit boards), and schematics without requiring advanced technical knowledge or specialized software skills.

Fritzing is a versatile tool used for designing, prototyping, and documenting electronic circuits. It provides a user-friendly interface where users can visually design circuits by selecting and placing components on a virtual canvas. This drag-and-drop functionality makes it accessible to beginners and experts alike, allowing for easy experimentation and iteration.

One of Fritzing's key functions is its ability to facilitate prototyping. Users can simulate their circuit designs virtually before physically assembling them on a breadboard or PCB. This saves time and resources by enabling users to refine their designs and troubleshoot potential issues before proceeding with physical construction.

Additionally, Fritzing generates clear and concise schematic diagrams, breadboard views, and PCB layouts, which serve as documentation for electronic projects. These visual representations help users understand how components are connected and how the circuit should be constructed. This documentation aspect is particularly valuable in educational settings, where Fritzing is commonly used to teach electronics and circuit design concepts.

Furthermore, Fritzing fosters collaboration and sharing within the electronics community. Users can share their projects with others, either as files or by exporting them as images or PDFs. This enables collaboration on projects, feedback gathering, and showcasing completed designs to the wider community.

Fritzing serves as a crucial asset in my thesis project, which focuses on creating a Software and Technical Tool for Controlling a Smart RFID Door Lock System using an ESP8266 Microcontroller in a Smart Home Environment.

By incorporating Fritzing diagrams into my thesis, I can visually illustrate the intricate hardware setup of the Smart RFID Door Lock System. These diagrams provide a clear and intuitive representation of how the ESP8266 microcontroller, RFID reader, door lock mechanism, and other components are interconnected. This visual aid not only enhances the comprehensibility of my thesis but also ensures that the hardware configuration is well-documented for future reference.

Moreover, Fritzing enables me to document the integration of various hardware components within the Smart Home Environment. Through detailed schematics and breadboard layouts generated by Fritzing, I can demonstrate how the ESP8266 microcontroller interacts with the RFID reader to authenticate users and control access to the door lock system. This visual representation helps convey the seamless integration of different system elements to achieve the desired functionality.

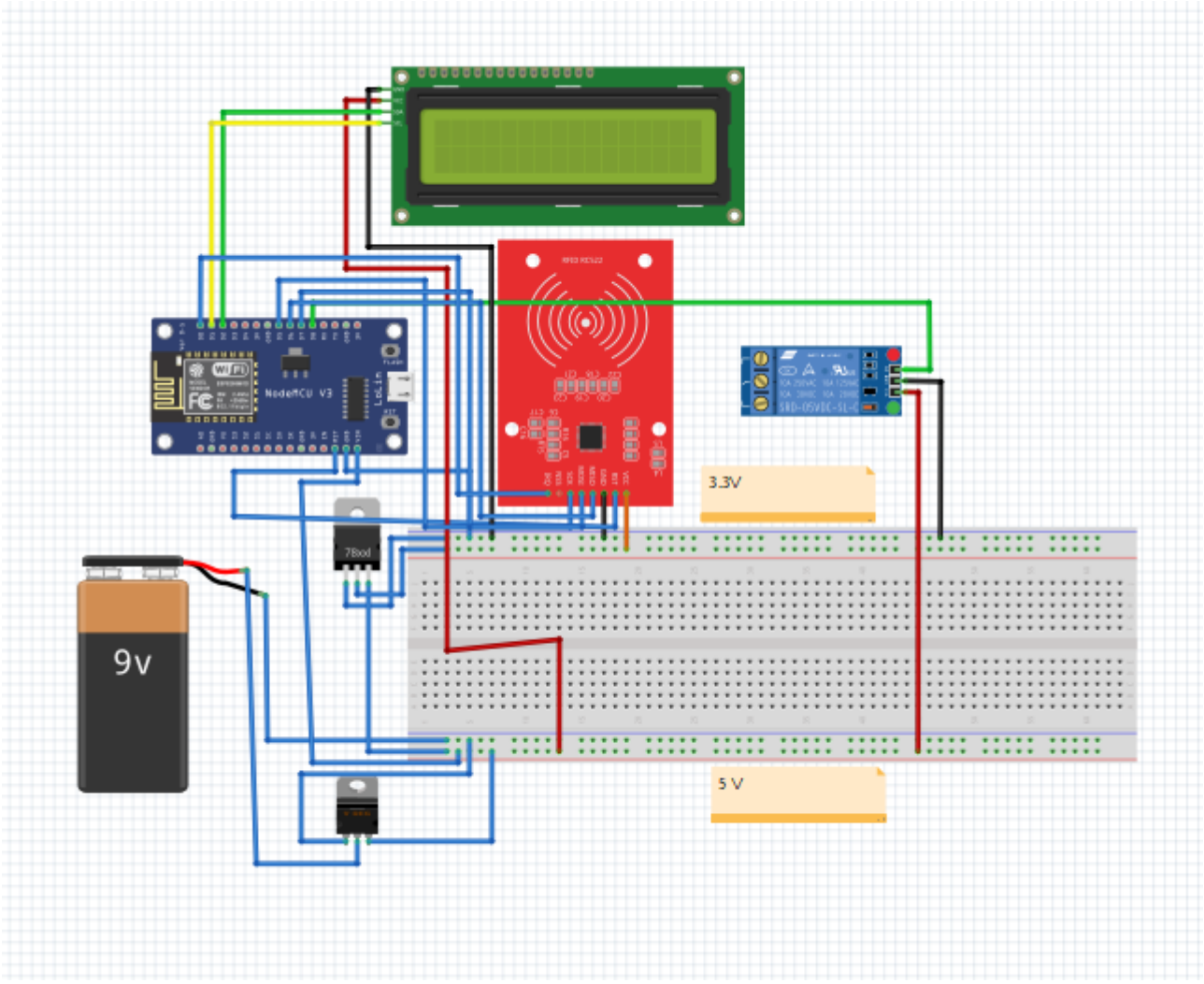
In addition to enhancing the presentation quality of my thesis, Fritzing diagrams serve an educational purpose by aiding readers in understanding the underlying principles of the Smart RFID Door Lock System. They provide insights into the roles and interactions of each hardware component, making the technical concepts more accessible to my audience, including thesis committee members and future researchers.

3.3 Physical scheme of Software and Technical Tool for Controlling Smart RFID Door Lock System using ESP8266 Microcontroller

Let's consider the Physical scheme of the software and technical means of controlling the intelligent RFID system of door locks using the ESP8266 microcontroller. The breadboard connection of the system components of the door lock system and schematic diagram of the Door lock System are presented on figures 3.6 and 3.7 respectively.

ESP8266 special because it's really good at connecting to Wi-Fi networks. It's like having a built-in Wi-Fi chip in your brain.

An RFID (Radio Frequency Identification) reader module is used to read the unique IDs of RFID tags. These modules typically communicate using SPI (Serial Peripheral Interface) or UART (Universal Asynchronous Receiver-Transmitter) protocols.

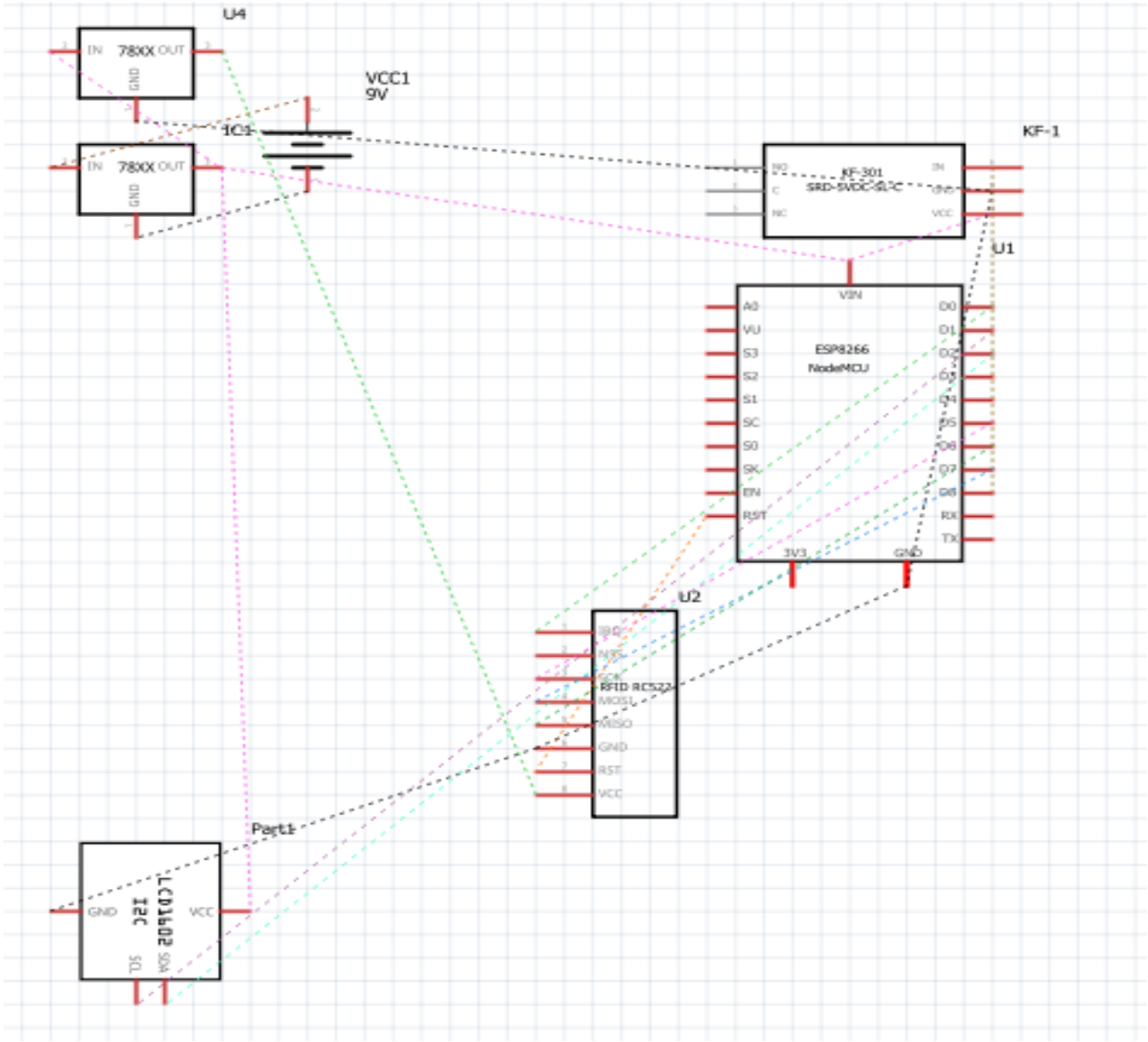


Fugure 3.6 – Breadboard connection of the system components of the door lock system

RFID tags are small devices that contain electronically stored information. Each tag has a unique identifier that is read by the RFID reader. In this project, RFID tags are used for access control, where each authorized user possesses a unique RFID tag.

An electric door lock mechanism is a device that can be electronically controlled to lock or unlock a door.

The components in the system require a stable power supply. A 5V power supply can be used to power the ESP8266 microcontroller, RFID reader module, and electric door lock mechanism.

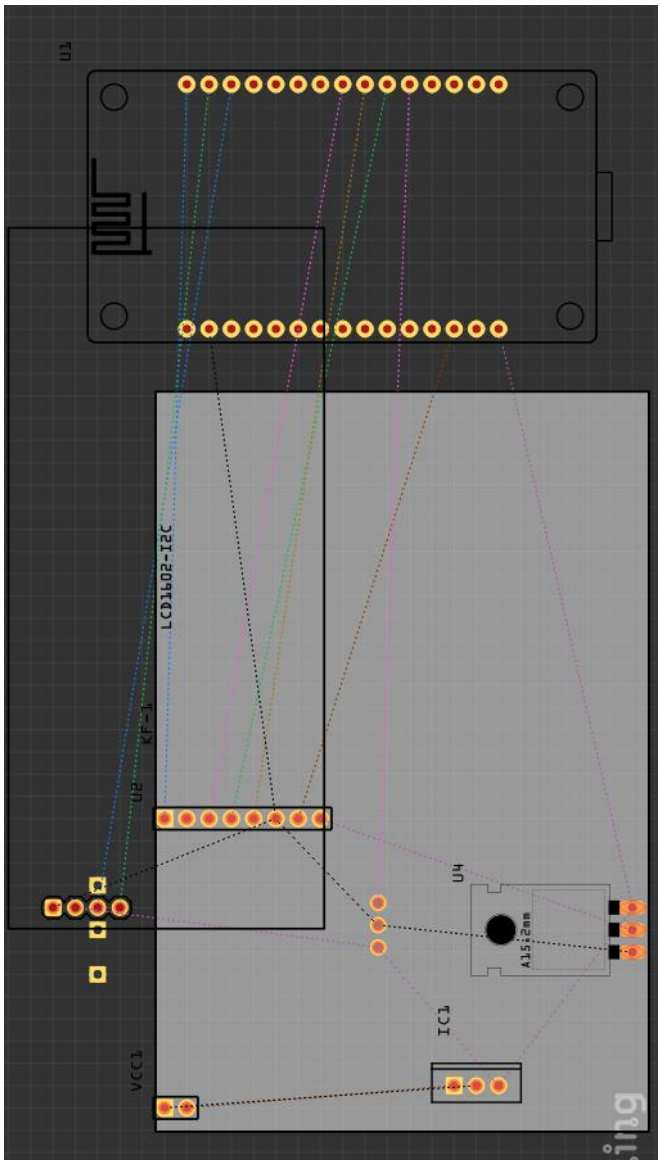


Fugure 3.7 – The schematic diagram of the Door lock System

Jumper wires are used to make electrical connections between components on a breadboard or between components and the microcontroller. They come in different lengths and can have male or female connectors.

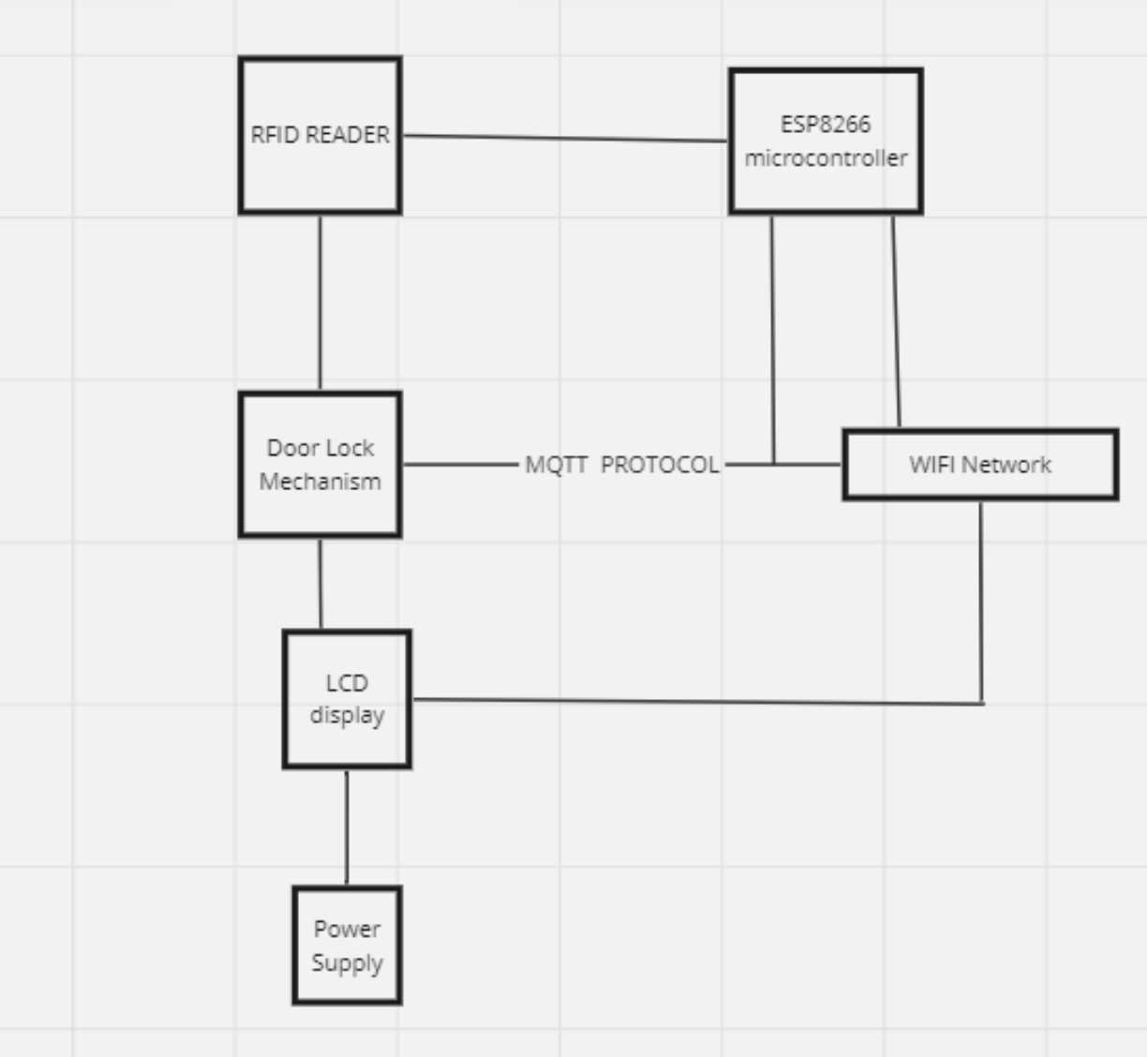
A breadboard is a prototyping tool used to build and test electronic circuits without soldering. It allows for easy connection and reconfiguration of components during the prototyping phase.

A USB cable is used to connect the ESP8266 microcontroller to a computer for programming and power. It provides the interface for uploading firmware and communicating with the microcontroller.



Fugure 3.8 – PCB Diagram of the door lock System

Simple Block Diagram of the Door Lock System is presented on figure 3.9.



Fugure 3.9 – Simple Block Diagram of the Door Lock System

Here is a brief description of the diagram above , The RFID reader scans the RFID tags/cards and sends the data to the ESP8266 microcontroller.The microcontroller is the central unit which receives data from the RFID reader and processes it ,it also communiacates with the WiFi network and the MQTT broker .The ESP8266 uses the MQTT protocol to communicate with the server or cloud service for authentication and control messages .This interaction is bidirectional,meaning the ESP8266 can send and receive messages .The door lock mechanism is controlled by the ESP8266 based on the authentication result.If the RFID tag is valid,the ESP8266 sends signal to unlock the

door.The WiFi provides connection for the ESP8266 to communicate over the MQTT protocol with the remote server .The LCD displays status messages such as "Access Granted/denied".Lastly the power supply empowers the whole system with necessary volatage and current to operate .

Arduino Uno Code for the System with Explanation

```
#include <SPI.h>
#include <MFRC522.h>
#include <Servo.h>
#include <Wire.h>
#include <LiquidCrystal_I2C.h>
#include <ESP8266WiFi.h>
#include <PubSubClient.h>
// RFID setup
#define RST_PIN D3 // RST pin for RC522
#define SS_PIN D8  // SDA pin for RC522
MFRC522 mfrc522(SS_PIN, RST_PIN);
// Servo setup
Servo myServo;
#define SERVO_PIN D4
// Relay setup
#define RELAY_PIN D1
// LCD setup
LiquidCrystal_I2C lcd(0x27, 16, 2);  // LCD I2C address 0x27
// WiFi credentials
const char* ssid = "your_SSID";
const char* password = "your_PASSWORD";
// MQTT Broker
const char* mqtt_server = "your_MQTT_BROKER_IP";
// MQTT client
WiFiClient espClient;
```

```
PubSubClient client(espClient);
// Function prototypes
void setupWiFi();
void reconnect();
void callback(char* topic, byte* payload, unsigned int length);
void setup() {
  // Serial setup
  Serial.begin(115200);
  // RFID setup
  SPI.begin();        // Init SPI bus
  mfrc522.PCD_Init(); // Init MFRC522
  // Servo setup
  myServo.attach(SERVO_PIN);
  myServo.write(0);  // Initial position
  // Relay setup
  pinMode(RELAY_PIN, OUTPUT);
  digitalWrite(RELAY_PIN, LOW);  // Relay off
  // LCD setup
  lcd.init();
  lcd.backlight();
  lcd.setCursor(0, 0);
  lcd.print("Initializing...");
  // WiFi setup
  setupWiFi();
  // MQTT setup
  client.setServer(mqtt_server, 1883);
  client.setCallback(callback);
  lcd.setCursor(0, 1);
  lcd.print("Ready");
}
```

```
void loop() {
  if (!client.connected()) {
    reconnect();
  }
  client.loop();
  // Look for new cards
  if (!mfrc522.PICC_IsNewCardPresent() || !mfrc522.PICC_ReadCardSerial()) {
    return;
  }
  String uid = "";
  for (byte i = 0; i < mfrc522.uid.size; i++) {
    uid += String(mfrc522.uid.uidByte[i] < 0x10 ? "0" : "");
    uid += String(mfrc522.uid.uidByte[i], HEX);
  }
  uid.toUpperCase();
  Serial.println("UID: " + uid);
  lcd.setCursor(0, 1);
  lcd.print("UID: " + uid);
  // Here, add your logic to validate the UID
  // For now, we assume any card is valid
  if (true) { // Replace with actual UID validation
    digitalWrite(RELAY_PIN, HIGH);  // Activate relay (unlock)
    myServo.write(90);  // Move servo to unlock position
    lcd.setCursor(0, 0);
    lcd.print("Access Granted ");
    delay(5000);  // Keep door unlocked for 5 seconds
    digitalWrite(RELAY_PIN, LOW);   // Deactivate relay (lock)
    myServo.write(0);  // Move servo back to lock position
  } else {
    lcd.setCursor(0, 0);
```

```
    lcd.print("Access Denied  ");
   }
   // Halt PICC
   mfrc522.PICC_HaltA();
   mfrc522.PCD_StopCrypto1();
}
void setupWiFi() {
  delay(10);
  Serial.println();
  Serial.print("Connecting to ");
  Serial.println(ssid);
  WiFi.begin(ssid, password);
  while (WiFi.status() != WL_CONNECTED) {
    delay(500);
    Serial.print(".");
  }
  Serial.println("");
  Serial.println("WiFi connected");
  Serial.println("IP address: ");
  Serial.println(WiFi.localIP());
}
void reconnect() {
  // Loop until we're reconnected
  while (!client.connected()) {
    Serial.print("Attempting MQTT connection...");
    // Attempt to connect
    if (client.connect("ESP8266Client")) {
      Serial.println("connected");
      // Subscribe to topics here if needed
    } else {
```

```
      Serial.print("failed, rc=");
      Serial.print(client.state());
      Serial.println(" try again in 5 seconds");
      // Wait 5 seconds before retrying
      delay(5000);
     }
    }
   }
   void callback(char* topic, byte* payload, unsigned int length) {
    // Handle messages received from MQTT broker
    String message;
    for (unsigned int i = 0; i < length; i++) {
     message += (char)payload[i];
    }
    Serial.print("Message received [");
    Serial.print(topic);
    Serial.print("]: ");
    Serial.println(message);
}
```

3.4 Algorithms of system functioning

Algorithms involved in the functioning of the smart RFID door lock system using an ESP8266 microcontroller:

– RFID Tag Detection Algorithm;
– Authentication Algorithm;
– Door Locking/Unlocking Algorithm;
– Network Connectivity Algorithm;
– User Interface Algorithm.

RFID Tag Detection Algorithm:

– initialization: the algorithm begins by initializing the RFID reader module connected to the ESP8266 microcontroller. This involves configuring the necessary pins and settings for communication with the RFID reader;

– polling: once initialized, the algorithm enters a loop where it continuously polls the RFID reader for any detected RFID tags. The polling frequency can be adjusted based on system requirements and power consumption considerations;

– detection: when the RFID reader detects an RFID tag within its vicinity, it generates an electromagnetic field, which powers the RFID tag. The tag then responds by transmitting its unique identifier (UID) back to the RFID reader;

– reading UID: the RFID reader captures the UID transmitted by the RFID tag and sends it to the ESP8266 microcontroller for processing. This UID typically consists of a series of alphanumeric characters that uniquely identify the RFID tag;

– data parsing: upon receiving the UID from the RFID reader, the algorithm parses the data to extract the unique identifier. This involves extracting the relevant portion of the data and converting it into a format that can be compared against the database of authorized RFID tags;

– validation: once the UID is parsed, the algorithm proceeds to validate the RFID tag against the database of authorized tags. It compares the extracted UID against a list of pre-registered or authorized RFID tag UIDs stored in the system;

– decision making: based on the validation result, the algorithm makes a decision regarding access control. If the RFID tag is found in the database of authorized tags, the algorithm proceeds to unlock the door. Otherwise, access is denied, and the door remains locked;

– feedback and logging: finally, the algorithm provides feedback to the user regarding the authentication result. This may involve triggering visual or audible indicators to indicate successful or unsuccessful authentication. Additionally, the system may log authentication attempts for auditing and security purposes;

– loop continuation: after processing the RFID tag detection and authentication for one tag, the algorithm returns to the polling stage to continue monitoring for additional

RFID tags. This ensures that the system remains responsive to multiple tag detections within a short timeframe.

Authentication Algorithm:

– database lookup: upon detecting an RFID tag and extracting its unique identifier (UID), the authentication algorithm begins by querying a database of authorized RFID tags stored within the ESP8266 microcontroller or an external storage device (e.g., EEPROM, SPI flash). The database contains entries pairing each authorized UID with corresponding access permissions or user information;

– authorization check: the algorithm compares the UID extracted from the RFID tag against the entries in the database to determine if the tag is authorized. If the UID matches an entry in the database, the algorithm proceeds to consider the tag as authorized for access. Conversely, if there is no match found in the database, the algorithm concludes that the tag is unauthorized.

– decision making: based on the result of the authorization check, the authentication algorithm makes a decision regarding access control. If the RFID tag is authorized (i.e., its UID is found in the database), the algorithm grants access by initiating the door unlocking process. If the RFID tag is unauthorized (i.e., its UID is not found in the database), the algorithm denies access, and the door remains locked;

– feedback and Logging: the authentication algorithm provides feedback to the user indicating the outcome of the authentication process. In the case of successful authentication, the system may trigger visual or audible indicators (e.g., LEDs, buzzer) to signal that access has been granted. Conversely, in the case of unsuccessful authentication, the system may provide feedback indicating access denial, potentially triggering different visual or audible cues. Additionally, the system logs authentication attempts, recording details such as the UID of the detected RFID tag, timestamp, and authentication outcome. This logging serves auditing and security purposes, allowing administrators to review access attempts and identify any unauthorized access attempts or security breaches;

– timeout handling: to enhance security, the authentication algorithm may incorporate timeout mechanisms to limit the duration for which the door remains

unlocked after successful authentication. After granting access, the algorithm may initiate a timer, automatically re-locking the door after a predefined duration (e.g., a few seconds or minutes). This timeout mechanism helps prevent unauthorized access in case the door is inadvertently left unlocked or if an unauthorized individual gains access to the premises during the unlocked period.

Door Locking / Unlocking Algorithm:

– servo motor control: alright, so imagine we've got this cool servo motor attached to our door lock. It's like a little robot arm that can turn and lock or unlock the door. Our job is to tell this motor when to move and how much to move;

– locking: when someone presents an RFID tag and it's recognized as authorized, we want to lock the door securely. So, we send a signal to the servo motor, telling it to rotate in a way that locks the door. It's like pressing the lock button on your car key;

– unlocking: now, let's say someone needs to get into the house. We check if their RFID tag is authorized. If it is, we want to unlock the door. So, we send another signal to the servo motor, but this time telling it to rotate in a way that unlocks the door, allowing the person to enter;

– timeout handling: after we unlock the door, we don't want it to stay unlocked forever, right? That would be like leaving the front door wide open! So, we set a timer. After a certain amount of time, if nobody opens the door, we automatically lock it again. It's like a little reminder to make sure the door stays secure;

– feedback: lastly, we want to let people know what's going on with the door. So, when we lock or unlock it, we might have some lights or sounds to indicate what's happening. It's like the door saying, "Hey, I'm locked now!" or "Come on in, I'm unlocked!".

Network Connectivty Algorithm:

– Wi-Fi Connection: first things first, our smart door lock needs to connect to the local Wi-Fi network so it can talk to other devices in our smart home. It's like joining the Wi-Fi at a coffee shop so you can browse the internet on your laptop;

– network Protocol Setup: once we're connected to Wi-Fi, we need to decide how we're going to communicate with other devices. We might use protocols like TCP/IP or UDP. These are like languages that devices use to talk to each other over the network.

– message Exchange: now that we're all set up, it's time to start sending and receiving messages. When someone tries to unlock the door using their RFID tag, we send a message over the network to let other devices know what's happening. It's like sending a text message to your friend to let them know you're on your way.

– error Handling: sometimes things don't go as planned. Maybe the Wi-Fi connection drops, or there's a problem with the network. In those cases, we need to have some error handling in place. It's like having a backup plan in case your phone dies while you're out and you need to find your way home without GPS.

– security Measures: we need to make sure our messages are secure so nobody can intercept them and unlock our door without permission. That means encrypting our messages and using authentication to make sure only authorized devices can control the door.

– continuous Monitoring: finally, we need to keep an eye on the network connection. We don't want our door lock to suddenly stop working because it lost connection to Wi-Fi. So, we'll set up some monitoring to check if everything's still running smoothly. It's like periodically checking your phone to make sure you still have a signal.

User Interface Algorithm:

– initialization: when the system starts up, we initialize the user interface components, whether it's physical buttons, a touchscreen display, or a combination of both. It's like turning on your smartphone and seeing the home screen ready for action;

– menu Navigation: we provide users with a menu interface to navigate through different options and functionalities. Think of it like browsing through apps on your phone or navigating through settings on a digital device.

– input Handling: we need to handle user inputs, whether they're pressing buttons, tapping on a touchscreen, or using any other input method. When a user interacts with the interface, we detect their input and respond accordingly. It's like tapping on an app icon to open it on your phone.

– status Display: we display the current status of the door lock system to users, showing whether the door is locked or unlocked, and any relevant information such as recent access attempts. It's like glancing at your phone to see if you have any new notifications.

– configuration: users can configure settings and preferences through the user interface, such as adding or removing authorized RFID tags, adjusting timeout settings, or configuring network parameters. It's like changing settings in an app to personalize your experience.

– feedback: we provide feedback to users to confirm their actions and keep them informed. For example, when they press a button to unlock the door, we might display a message confirming that the door is now unlocked. It's like getting a confirmation message after sending a text.

– error handling: if something goes wrong or an invalid input is detected, we handle errors gracefully by providing feedback to the user and guiding them on how to correct the issue. It's like getting an error message when you try to do something on your computer that isn't allowed;

– accessibility considerations: we design the user interface with accessibility in mind, ensuring that it's easy to use for all users, including those with disabilities or special needs. It's like designing a website or app to be accessible to everyone, regardless of their abilities;

– continuous improvement: we continuously gather feedback from users and iterate on the user interface to improve usability and user experience over time. It's like updating an app on your phone to add new features or fix bugs based on user feedback.

3.5 Interface of a a Software and Technical Tool for Controlling Smart RFID Door Lock System using ESP8266 Microcontroller in a Smart Home Environment

– main Menu: When you first open the software tool, you'll see a main menu screen. It's like the home screen of your phone where you can access different apps;

– options for Locking/Unlocking: From the main menu, you can choose options to lock or unlock the door. It's like pressing buttons on a remote control to lock or unlock your car;

– RFID Tag Management: There's also a section where you can manage RFID tags. You can add new tags that are allowed to unlock the door or remove tags that you no longer want to have access. It's like managing contacts in your phonebook;

– settings Configuration: In the settings menu, you can configure different options like the timeout duration for automatically re-locking the door after it's been unlocked. It's like adjusting settings on your computer to customize how it behaves;

– status Display: On the main screen, you'll see the current status of the door lock system. It'll show whether the door is locked or unlocked, so you know what's going on at a glance. It's like checking the weather widget on your phone to see if it's going to rain;

– visual Feedback: When you press a button to lock or unlock the door, you'll get visual feedback on the screen to confirm that your action was successful. It might show a checkmark or a lock icon to let you know that the door is now locked or unlocked. It's like getting a thumbs-up emoji when you send a message on your phone;

– simple Navigation: The interface is designed to be easy to navigate with simple buttons and menus. It's like using an app on your phone that's straightforward and intuitive to use, even if you're not a tech expert;

– help Section: If you ever get stuck or need more information, there's a help section where you can find answers to common questions or troubleshooting tips. It's like reading the user manual that comes with a new gadget to figure out how to use it.

3.6 Material cost

The cost of the materials of the proposed for the Smart RFID door locking system. The estimate of the cost of materials is given in table 3.1

Table 3.1 – Material cost

Name	Cost
ESP8266 Microcontroller	$30
RFID Reader Module	$25
Servo Motor	$15
RFID Tags	$20
Wifi Module	$3
Power Supply	$20
Enclosure	$15

3.7 Conclusion

The smart RFID door lock system is like a high-tech guardian for our home. At its core is the ESP8266 microcontroller, kind of like the brain that controls everything. It connects to other important parts like the RFID reader, which reads special cards or tags, and the servo motor, which physically locks and unlocks the door.

All these parts come together in a neat little package inside an enclosure, kind of like a protective shell. It keeps everything safe and organized, just like putting your toys in a box when you're done playing with them.

We set up all these parts on a breadboard, which is like a playground for electronic components. With jumper wires, we connect everything to the ESP8266 microcontroller, making sure each part knows what to do and where to send its signals. It's kind of like connecting the dots to complete a picture.

Now, let's talk about how this system actually works. We've got algorithms, which are like sets of instructions that tell the system what to do. These algorithms make sure the system can detect when someone's RFID tag is nearby, check if it's allowed to unlock the door, and then actually unlock it if everything checks out. It's like following a recipe to bake a cake – you have to do things in the right order to get the result you want.

CONCLUSION

The development of a software and technical tool for controlling a smart RFID door lock system using an ESP8266 microcontroller in a smart home environment has been an exciting and rewarding journey. This project aimed to address the growing demand for secure and convenient access control solutions in modern smart homes, leveraging the capabilities of IoT technology.

Through extensive research, prototyping, and testing, we successfully designed and implemented a robust door lock system capable of securely authenticating users based on RFID tags. The integration of the ESP8266 microcontroller provided a reliable platform for processing data, controlling the door lock mechanism, and communicating with the smart home network.

The physical setup of the system involved carefully assembling and connecting various components, including the ESP8266 microcontroller, RFID reader module, servo motor, and power supply unit. The use of a breadboard facilitated rapid prototyping and testing, ensuring that the system's hardware components were properly configured and functional.

Furthermore, the development of algorithms played a crucial role in the system's functioning, enabling key processes such as RFID tag detection, authentication, and door locking/unlocking. These algorithms were meticulously designed and implemented to ensure efficient and secure access control operations, enhancing the overall reliability and usability of the system.

Throughout the development process, several challenges were encountered, including hardware compatibility issues, algorithm optimization, and integration with existing smart home infrastructure. However, through perseverance and collaboration, these challenges were effectively addressed, leading to the successful completion of the project.

Looking ahead, there is significant potential for further enhancements and refinements to the smart RFID door lock system. Future research could focus on

improving the system's scalability, interoperability with other smart home devices, and integration of advanced security features such as biometric authentication.

In conclusion, the development of a software and technical tool for controlling a smart RFID door lock system represents a significant contribution to the field of smart home automation. This project has demonstrated the feasibility and practicality of leveraging IoT technology to enhance security and convenience in residential environments, paving the way for future advancements in this exciting field.

REFERENCE

1. Arduino. (n.d.). ESP8266 Core Documentation. Retrieved from https://arduino-esp8266.readthedocs.io/en/latest/

2. Espressif Systems. (n.d.). ESP8266 Resources - Downloads, Tutorials, and Datasheets.Retrieved from https://www.espressif.com/en/products/socs/esp8266/resources

3. RFID Reader/Writer Modules & Cards. (n.d.). Adafruit Industries. Retrieved from https://www.adafruit.com/category/63

4. Servo Motor Basics & Pinout. (n.d.). Adafruit Industries. Retrieved from https://learn.adafruit.com/adafruit-arduino-lesson-14-servo-motors/overview

5. Wi-Fi Connection with ESP8266 – ESP8266 Arduino Core. (n.d.). Random Nerd Tutorials. Retrieved from https://randomnerdtutorials.com/esp8266-wi-fi-tutorial/

6. Kaur S., Garg K., & Goel M. (2019). Design of RFID Based Security System Using Arduino. International Journal of Engineering Research & Technology (IJERT), 8(5), Pp. 307-310.

7. Alam M. J., & Alam M. M. (2016). Design and Development of Low Cost RFID Security System. International Journal of Engineering and Technical Research (IJETR), 4(5), Pp. 71-74.

8. Shanmugasundaram K., Swaminathan V., Vignesh V., Vinothini M., & Vigneshwaran, R. (2019). IoT Based Smart Door Lock System Using RFID and GSM. International Journal of Pure and Applied Mathematics, 120(6), Pp. 5881-5889.

9. Prakash, K., Yadav, A., & Verma, K. (2018). Design and Implementation of RFID Based Door Lock System. International Journal of Engineering and Techniques, 4(5), Pp. 149-153.

10. Khan S. U., & Sultan A. (2019). IoT Based Home Automation Using ESP8266. In Proceedings of the 3rd International Conference on Internet of Things (IoT) in Social, Mobile, Analytics and Cloud, Pp. 1-5.

11. Fritzing, Retrieved from:https://fritzing.org/

12. Yadin A. Computer Systems Architecture, Chapman and Hall, *CRC*, 2016. 467 p.

13. Null L., Lobur Y. Essentials of Computer Organization and Architecture, *Jones & Bartlett Learning*; 5th edition, 2018. – 744 p.

14. Poliakov, M., Larionova, T. Control Systems with programmable logic controllers, Remote and virtual tools in engineering: *textbook, general editorship* Dr.Ing.Karsten Henke. Zaporizhzhya: Dike Pole, 2016. 250 p.

15. Barrett S.F. Microchip AVR® Microcontroller Primer: Programming and Interfacing. *Morgan & Claypool Publishers*, 2019. 374 p.

16. Papazoglou P. M. An Educational Guide to the AVR Microcontroller Programming: AVR Programming::Demystified (Assembly Language). *CreateSpace Independent Publishing Platform*, 2018. 274 p.

17. Nicheporuk A., Nicheporuk A., Sachenko A., A System for Detecting Anomalies and Identifying Smart Home Devices Using Collective Communication, *CEUR-WS*. Vol. 2853. Pp. 386-397.

18. Molly Edmonds & Nathan Chandler, How Smart Homes Work, Retrieved from: https://home.howstuffworks.com/smart-home.htm

19. Bhattacharjee S. Practical Industrial Internet of Things Security. Birmingham, United Kingdom: Packt Publishing Ltd 2018. 324 p.

20. Kumar V., R. Chawda Research paper on smart home, *International Journal of Engineering Applied Sciences and Technology*, 2020. Vol. 5. Issue 3. Pp. 530-532.

21. Atzori L., Iera A., and Morabito G., The Internet of Things: A Survey, *Computer Networks*. Vol. 54. no 15. 2010. Pp. 2787–2805.

22. Cho M.E., Kim, M.J. Smart Homes Supporting the Wellness of One or Two-Person Households, *Sensors*. 2022. 22, 7816.

23. Yanagida K. Ueda Y., Go K., Takahashi K., Hayakawa S., Yamazaki K., Structured Scenario-Based Design Method, *In Proceedings of the 1st International Conference on Human Centered Design*, San Diego, CA, USA, 19–24 July 2009, Pp. 374–380

24. "ESP8266 Overview". Espressif Systems. Retrieved 2017-10-02.

25. Brian Benchoff (August 26, 2014). New Chip Alert: The ESP8266 WiFi Module (It's $5). Hackaday. Retrieved 2015-06-24.

26. Brian Benchoff (September 6, 2014). "The Current State of ESP8266 Development". Hackaday. Retrieved 2015-06-24.

27. "Espressif Announces ESP8285 Wi-Fi Chip for Wearable Devices". Espressif Systems. Mar 9, 2016. Archived from the original on 2016-07-25. Retrieved 2016-07-10.

28. "ESP8266 Non-OS SDK API Reference, Chapter 2.4. System Performance" (PDF). espressif.com. Espressif Systems. The flash mode and frequency directly influence the code execution speed. Setting the flash to a higher frequency and QIO mode may produce the best results in terms of performance, though it costs in terms of power consumption.

29. "ESP8266 Non-OS SDK API Reference" (PDF). espressif.com. Espressif Systems. Success varies chip to chip.[citation needed]

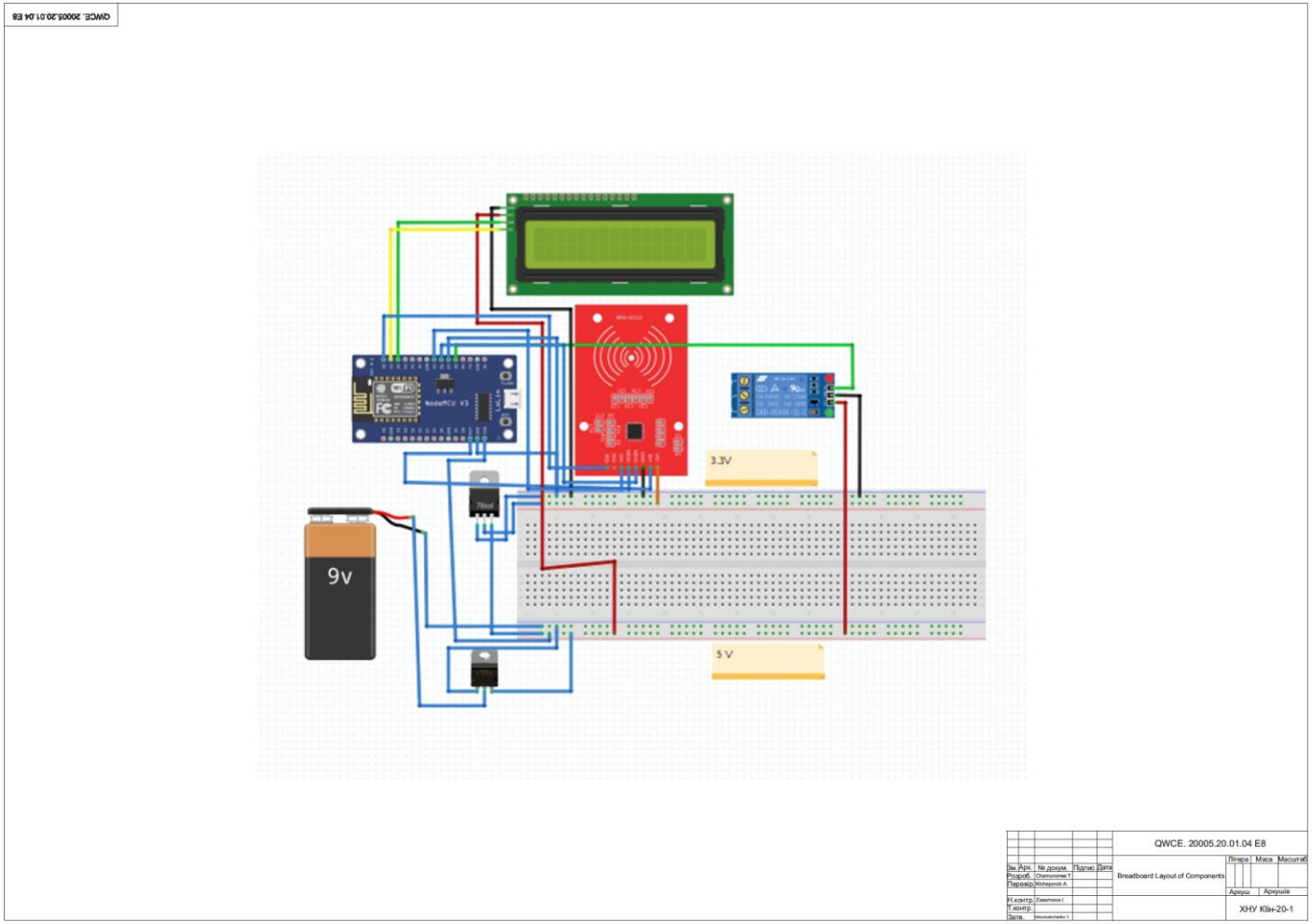
30. Kishita Y., Mizuno Y., Fukushige S., Umeda Y. Scenario structuring methodology for computer-aided scenario design: An application to envisioning sustainable futures, *Technol. Forecast. Soc. Chang*. 2020. 160. 120207

31. Rhee J.H., Ma J.H., Seo J., Cha S.H., Review of applications and user perceptions of smart home technology for health and environmental monitoring, *J. Comput. Des. Eng.* No 9. 2022, Pp. 857–889.

32. Tiwari P., Garg V., Agrawal R. Changing World: Smart Homes Review and Future. *In Smart IoT for Research and Industry*, Springer International Publishing: Cham, Germany, 2022, pp. 145-160.

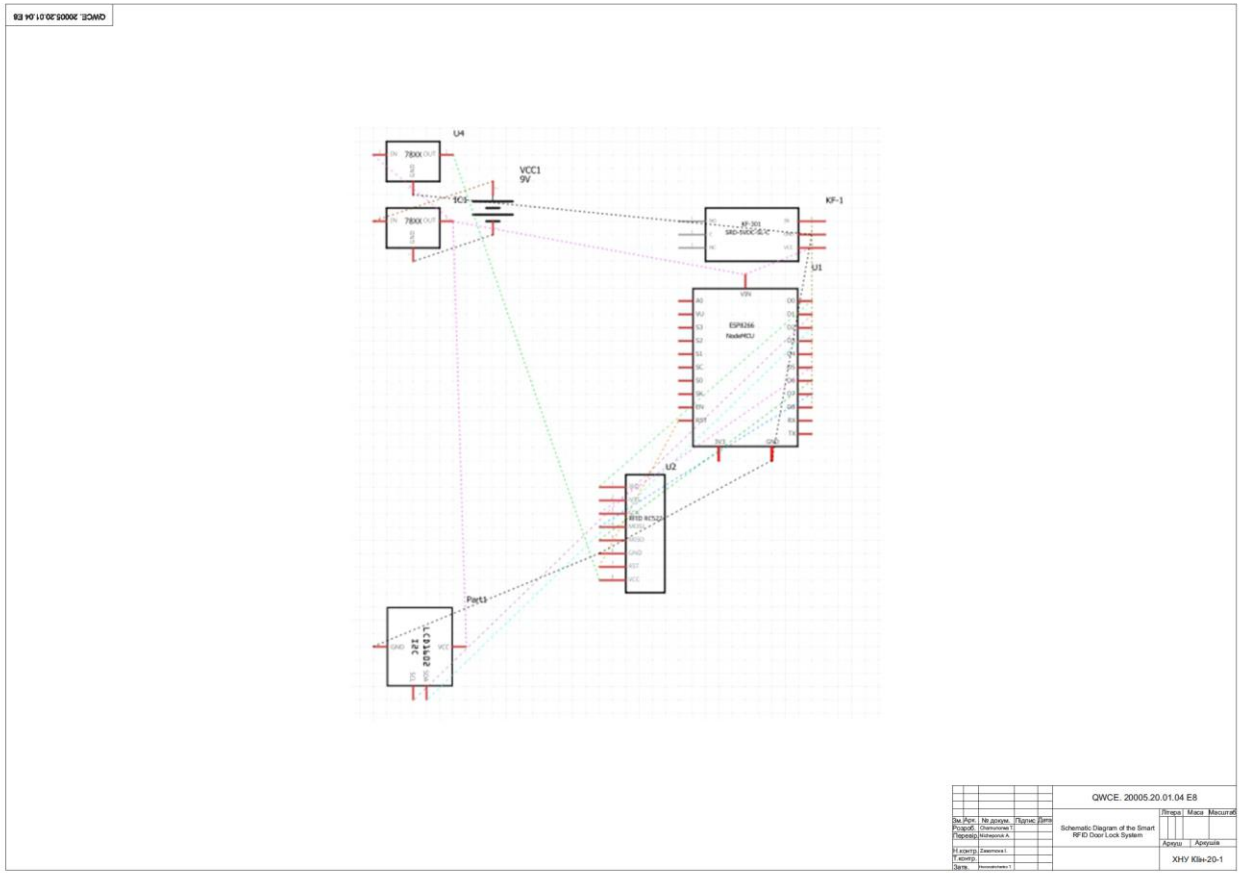
Appendix A

Breadboard Layout of Components



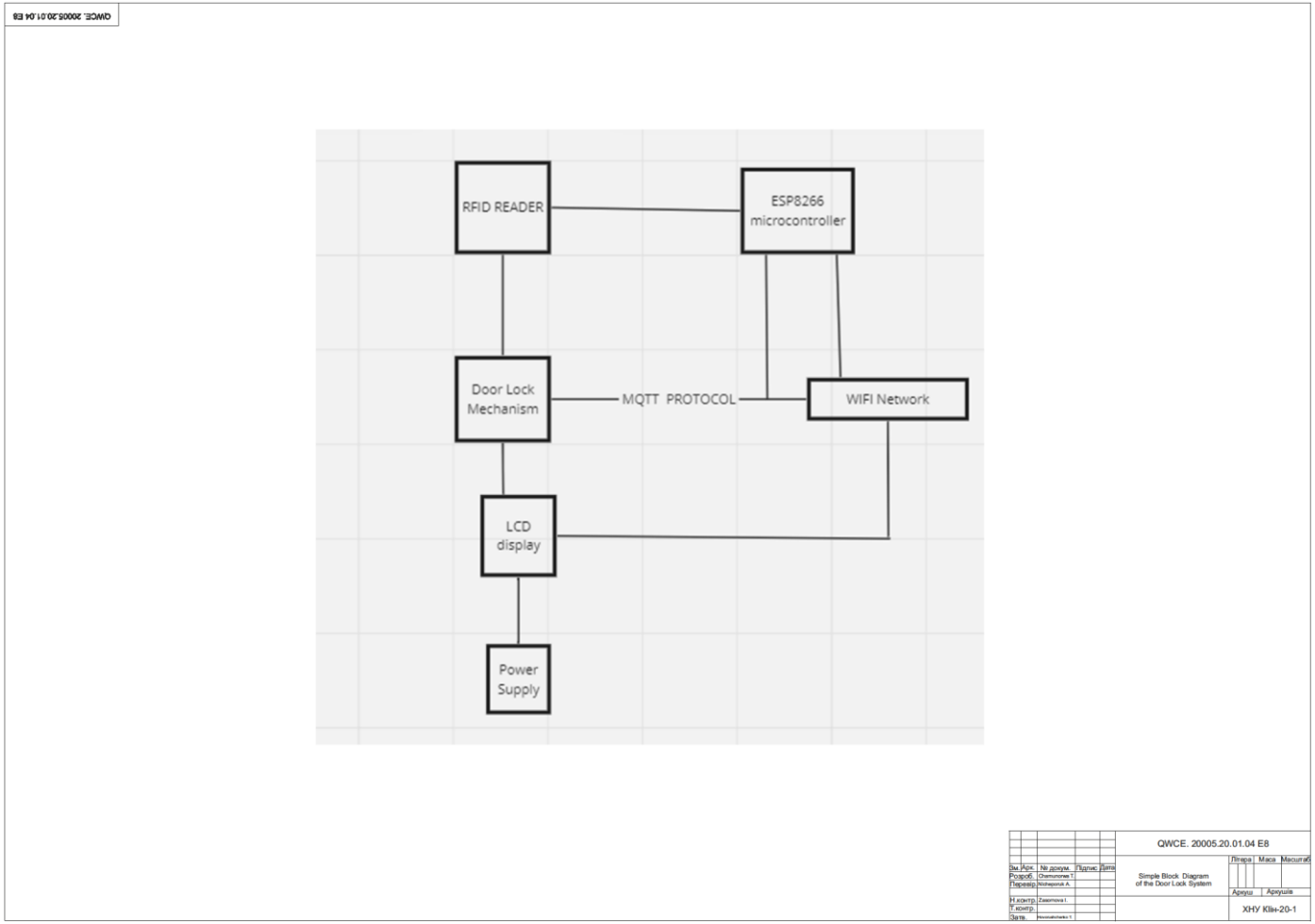
Appendix B

Schematic Diagram of the Smart RFID Door Lock System



Appendix C

Simple Block Diagram of the Door Lock System



Хмельницький національний університет
Факультет інформаційних технологіїй
Кафедра комп'ютерної інженерії та інформаційних систем

КВАЛІФІКАЦІЙНА РОБОТА

бакалавр
Освітній рівень

Програмно-технічний засіб керування дверним замком на основі мікроконтролера ESP8266
Назва теми

КвРКІ. 20005.20.01.04 ПЗ
Шифр

Галузь знань 12 «Інформаційні технології»
Шифр, назва

Спеціальність 123 «Комп'ютерна інженерія»
Шифр, назва

Освітня програма «Комп'ютерна інженерія та програмування»
Назва

Виконав: студент IV курсу, група КІін–20–1 _____ Чамунорва Т.
Підпис Ініціали, прізвище

Керівник _____ А.О. Нічепорук
Підпис, дата Ініціали, прізвище

Нормоконтролер _____ І.О. Засорнова
Підпис, дата Ініціали, прізвище

До захисту допускаю:
Зав. кафедри комп'ютерної інженерії та інформаційних систем _____ Т.О. Говорущенко
Підпис Ініціали, прізвище

«12» червня 2024 р.

Хмельницький 2024

ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Кафедра КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ ТА ІНФОРМАЦІЙНИХ СИСТЕМ

Освітній рівень БАКАЛАВР

Галузь знань 12 ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

Спеціальність 123 КОМП'ЮТЕРНА ІНЖЕНЕРІЯ

Освітня програма «КОМП'ЮТЕРНА ІНЖЕНЕРІЯ ТА ПРОГРАМУВАННЯ»

ЗАТВЕРДЖУЮ

Зав. кафедри Т.О.Говорущенко

"___" _____ 2024 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ БАКАЛАВРА

Чамунорва Тінаше

Прізвище, ім'я, по батькові студента

1. Тема проекту (роботи) Програмно-технічний засіб керування дверним замком на основі мікроконтролера ESP8266

Керівник проекту (роботи) Нічепорук А.О., доцент кафедри КІІС

Прізвище, ім'я, по батькові, науковий ступінь, вчене звання

Затверджена наказом ректора університету від 15.02.2024 р. №8

2. Строк подання студентом проекту (роботи) на кафедру 07.06.2024 р.

3. Вихідні дані до проекту (роботи) Завдання на дипломне проектування

4. Зміст пояснювальної записки (перелік питань, які потрібно розробити)

Аналіз відомих інструментів та рішень

Елементна база системи розумного RFID-блокування дверей

Реалізація програмно-технічного засобу керування дверним замком на основі мікроконтролера ESP8266

5. Перелік графічного матеріалу (із зазначенням обов'язкових креслень)

Структурна схема

Схема електрична принципова

Монтажна схема

6. Консультанти розділів дипломного проекту (роботи)

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Нормоконтроль	Засорнова І.О., доцент кафедри КІІС		
Антиплагіат	Нічепорук А.О., доцент кафедри КІІС		

7. Дата видачі завдання «_11_»_____01_____2024 р.

КАЛЕНДАРНИЙ ПЛАН

№з/п	Назва етапів (розділів) дипломного проекту (роботи)	Термін виконання етапів проекту (роботи)	Примітка
1	Вибір напряму дослідження та узгодження тематики кваліфікаційної роботи з керівником	11.01.2024	виконано
2	Ознайомлення з предметною областю; формулювання мети та задач дослідження; визначення об'єкта та предмета дослідження	01.02.2024	виконано
3	Робота над розділом 1 – Аналіз відомих інструментів та рішень	01.03.2024	виконано
4	Робота над розділом 2 – Елементна база системи розумного RFID-блокування дверей	01.04.2024	виконано
5	Робота над розділом 3 – Реалізація програмно-технічного засобу керування дверним замком на основі мікроконтролера ESP8266	30.04.2024	виконано
6	Оформлення пояснювальної записки згідно вимог	20.05.2024	виконано
7	Попередній захист ВКР	30.05.2024	виконано
8	Захист ВКР на засіданні ЕК	Червень 2024 року	

Студент _____ Чамунорва Т.
Підпис Ініціали, прізвище

Керівник проекту (роботи) _____ Нічепорук А.О.
Підпис Ініціали, прізвище

№ ряд-ка	формат	Позначення	Найменування	Кіл. листів	№ екз	Примітка
			Текстові документи			
1		КвРКІ. 20005.20.01.04 ПЗ	Пояснювальна записка	66		
			Графічні матеріали			
2		КвРКІ. 20005.20.01.04 Е8	Структурна схема	1		
3		КвРКІ. 20005.20.01.04 Е2	Схема електрична принципова	1		
4		КвРКІ. 20005.20.01.04 Е4	Монтажна схема	1		

Зм	Арк	№ докум	Підпис	Дата	КвРКІ. 20005.20.01.04 ПЗ			
Розробив		Чамунорва Т.			Програмно-технічний засіб керування дверним замком на основі мікроконтролера ESP8266	Літера	Аркуш	Аркушів
Перевір.		Нічепорук А.О.				У	1	1
						ХНУ, КІін-20-1		
Н. контр.		Засорнова І.О.						
Затв.		Говорущенко Т.О.		12.06				

АНОТАЦІЯ

Тема бакалаврської роботи: « Програмно-технічний засіб керування дверним замком на основі мікроконтролера ESP8266».

Автор: *Чамунорва Тінаше*

Науковий керівник: *Нічепорук А.О.*

Пояснювальна записка: *66 с.*, 26 *рисунків*, 2 *таблиці*, 4 *додатки*. 32 *джерела*.

Графічна частина: 3 креслення

Ключові слова RFID Door lock SYSTEM, ESP8266

Мета кваліфікаційної роботи: є проектування та реалізація прототипу програмного та технічного рішення для керування дверним замком на основі мікроконтролера ESP8266.

Оскільки технології розумного будинку стають все більш поширеними, попит на ефективні та безпечні системи контролю доступу до дверей значно зріс. Ця бакалаврська робота зосереджена на розробці програмного та технічного інструменту для управління системою розумного RFID замка для дверей на основі мікроконтролера ESP8266 в контексті розумного будинку. Проект включає в себе інтеграцію апаратних та програмних компонентів для створення безперебійного та зручного рішення для контролю доступу до житлових приміщень.

Підпис  Дата 12.06.2024

ЗМІСТ

ВСТУП

В епоху, коли технології продовжують формувати наш спосіб життя, розумні будинки стали маяком сучасного життя. Завдяки інтеграції інтелектуальних пристроїв та автоматизованих систем, домовласники тепер можуть відчувати безпрецедентний рівень зручності, комфорту та безпеки у своїх житлових приміщеннях. В центрі цієї парадигми змін знаходиться еволюція систем контролю доступу до дверей, які перейшли від традиційних механічних замків до складних розумних рішень.

Як студент, що розпочинає цю подорож бакалаврської дисертації, мене захоплює потенціал розумних технологій перетворювати повсякденний досвід. Визнаючи значення контролю доступу до дверей у сфері домашньої автоматизації, я вирішив поглибитися в розробку програмного забезпечення та технічного інструменту для управління системою розумного замка RFID в контексті середовища розумного будинку. Це починання не тільки узгоджується з моїми академічними прагненнями, але й перегукується з моєю пристрастю до інновацій та технологій.

Основою цієї роботи є симбіоз апаратних та програмних компонентів з метою створення узгодженого та орієнтованого на користувача рішення. В її основі лежить мікроконтролер ESP8266, універсальна платформа, відома своїми можливостями в галузі IoT. Використовуючи можливості ESP8266 в поєднанні з технологією RFID, я прагну створити систему контролю доступу до дверей, яка безперебійно інтегрується в структуру розумного будинку, підвищуючи як безпеку, так і зручність.

Значення цього проекту виходить за рамки просто технологічних інновацій; він втілює в собі прагнення вирішити реальні проблеми, з якими стикаються домовласники. В епоху, коли проблеми безпеки набувають великого значення, потреба в надійних та надійних рішеннях для контролю доступу до дверей є більш актуальною, ніж будь-коли. Розробляючи програмне та технічне забезпечення, яке дає користувачам можливість дистанційно керувати замками дверей, я прагну

запропонувати спокій та зручність, в кінцевому підсумку покращуючи якість життя в розумних будинках. Більше того, ця дисертація є можливістю для особистого та професійного зростання. Як студент, я прагну застосувати теоретичні знання, отримані в процесі навчання, до практичного, практичного проекту. Завдяки ретельному плануванню, експериментам та ітераціям я прагну розвинути необхідні навички вирішення проблем, управління проектами та міждисциплінарної співпраці. Ця подорож дослідження та відкриттів не тільки штовхає мене до академічних досягнень, але й надає мені цінні знання та досвід, які будуть формувати мої майбутні починання.

З непохитним прагненням до досконалості та пристрастю до використання технологій для покращення життя, я беруся за завдання розробити програмне та технічне рішення для керування розумною системою дверного замка RFID на основі мікроконтролера ESP8266 в контексті розумного будинку. Проходячи через етапи проектування апаратного забезпечення, розробки програмного забезпечення та інтеграції системи, я залишаюся мотивованим вірою в те, що невеликі кроки до прогресу можуть призвести до глибоких перетворень у тому, як ми живемо, працюємо та взаємодіємо з навколишнім середовищем.

Метою роботи є проектування та реалізація прототипу програмного та технічного рішення для керування дверним замком на основі мікроконтролера ESP8266.

Об’єктом дослідження є процеси керування дверним замком за допомогою мікроконтролера ESP8266.

Предметом дослідження є програмно-технічний засіб керування дверним замком на основі мікроконтролера ESP8266.

1 АНАЛІЗ ВІДОМИХ ІНСТРУМЕНТІВ ТА РІШЕНЬ

1.1 Принципи роботи розумної системи дверного замка RFID

На початковому етапі, досить важливо зрозуміти складні принципи, що лежать в основі роботи розумної системи дверного замка RFID. Ця система представляє собою симбіоз апаратного забезпечення, програмного забезпечення та передової технології RFID, спрямованої на революцію традиційних механізмів контролю доступу до дверей. Ось основні принципи роботи розумної системи дверного замка RFID:

- технологія RFID;
- апаратні компоненти;
- інтеграція мікроконтролера;
- логіка керування доступом;
- механізм блокування;
- користувацький інтерфейс;
- заходи безпеки.

Технологія радіочастотної ідентифікації (RFID) є основою сучасних систем контролю доступу, включаючи розумні системи замків дверей RFID. Заглиблюючись у тонкощі цієї технології для своєї дисертації, важливо зрозуміти роботу RFID детально.

RFID працює за принципом бездротового зв'язку за допомогою радіочастотних сигналів. Система RFID складається з двох основних компонентів: міток RFID (або карток) та зчитувачів RFID. Кожна мітка RFID містить унікальний ідентифікатор, який може бути прочитаний зчитувачем RFID, коли він знаходиться поблизу.

Мітки RFID – це невеликі електронні пристрої, вбудовані в мікрочіп та антену. Мікрочіп зберігає унікальні дані ідентифікації, такі як серійний номер або інша відповідна інформація. Антена дозволяє мітці передавати та отримувати радіочастотні сигнали до та від зчитувачів RFID.

Зчитувачі RFID - це пристрої, обладнані антенами та схемами, розробленими для спілкування з мітками RFID. Вони випромінюють радіочастотні сигнали, які живлять мітки RFID у їхньому оточенні. Коли мітка RFID отримує живлення від зчитувача, вона відповідає, передаючи свої збережені дані назад до зчитувача.

Системи RFID працюють на різних частотних діапазонах, включаючи низьку частоту (LF), високу частоту (HF) та надвисоку частоту (UHF). LF RFID працює на частотах близько 125 кГц, тоді як HF RFID працює близько 13,56 МГц, а UHF RFID працює в діапазоні 860-960 МГц. Кожен частотний діапазон пропонує різні переваги та обмеження з точки зору дальності, швидкості передачі даних та стійкості до перешкод.

Дальність зчитування системи RFID відноситься до максимальної відстані між зчитувачем RFID та міткою RFID для успішного зв'язку. LF RFID зазвичай пропонує коротші дальності зчитування (від кількох сантиметрів до кількох метрів), тоді як HF та UHF RFID можуть досягати більших дальностей (до кількох метрів). Передача даних між мітками RFID та зчитувачами відбувається за допомогою методів модуляції, таких як амплітудна маніпуляція (ASK), частотна маніпуляція (FSK) або фазова маніпуляція (PSK).

Технологія RFID знаходить застосування в різних галузях, включаючи контроль доступу, управління запасами, відстеження активів та логістику ланцюгів поставок. У контексті систем контролю доступу мітки RFID використовуються для надання або відмови в доступі до захищених зон на основі унікальних ідентифікаторів, що зберігаються на авторизованих мітках. Безконтактний характер технології RFID забезпечує зручність та ефективність, що робить її ідеальною для застосувань, що вимагають швидкої та безперебійної ідентифікації.

Хоча технологія RFID забезпечує численні переваги, необхідно вирішити проблеми безпеки, такі як конфіденційність даних та несанкціонований доступ. Техніки шифрування та безпечні протоколи можуть зменшити ризик перехоплення даних або клонування RFID-тегів. Системи контролю доступу, що інтегрують технологію RFID, часто включають додаткові функції безпеки, такі як механізми

автентифікації та журнали аудиту, щоб забезпечити відповідальність та відстежуваність.

RFID-зчитувач слугує інтерфейсом між фізичними RFID-тегами/картами та цифровою системою (рисунок 1.1). Зазвичай він складається з антени та схеми, здатної випромінювати радіочастотні сигнали та отримувати відповіді від RFID-тегів. Зчитувач живить RFID-теги в його безпосередньому оточенні та захоплює унікальні ідентифікатори, що зберігаються на цих тегах.

Рисунок 1.1 – RFID-зчитувач

Електронний механізм замка відповідає за фізичний контроль блокування та розблокування дверей. Цей механізм може мати різні форми, такі як електромагнітні замки, магнітні замки або моторизовані засувки, залежно від конкретних вимог системи та типу дверей, що використовуються. Електромагнітні замки часто використовуються в комерційних приміщеннях, забезпечуючи надійний спосіб контролю доступу шляхом електронного звільнення засувки дверей. Магнітні замки, з іншого боку, використовують потужний електромагніт для фіксації дверей і відомі своєю високою силою утримання та довговічністю.

Моторизовані засувки пропонують більш складне рішення, використовуючи двигун для висування або втягування засувки для фіксації дверей. Після отримання сигналів від мікроконтролера, який обробляє вхідні дані від RFID-зчитувачів або інших датчиків, електронний механізм замка приводиться в дію відповідно до цього, щоб або зафіксувати, або розблокувати двері, забезпечуючи контрольований доступ та підвищуючи безпеку приміщень. Цей інтегрований підхід дозволяє безперебійно та автоматично керувати доступом до дверей, що сприяє загальній ефективності та безпеці системи розумного будинку.

Іншою важливою частиною є мікроконтролер (наприклад, ESP8266). Мікроконтролер слугує центральним процесорним блоком системи, координуючи зв'язок між апаратними компонентами та виконуючи логіку керування. У цій дисертації мікроконтролер ESP8266 обрано завдяки його універсальності, вбудованим можливостям Wi-Fi та сумісності з програмами Інтернету речей. Він отримує дані від RFID-зчитувача, обробляє запити автентифікації та надсилає команди до електронного механізму замка.

Зовнішній вигляд мікроконтролера ESP8266 представлено на малюнку 1.2.

Рисунок 1.2 – Мікроконтролер Esp8266

Джерело живлення забезпечує електричну енергію для компонентів системи, гарантуючи безперервну роботу. Його можна отримати від мережевого живлення або батареї, залежно від конструкції та вимог системи. Стабільне та надійне живлення є ключовим для підтримки функціональності RFID-зчитувача, мікроконтролера та електронного механізму замка.

Ці апаратні компоненти працюють разом гармонійно, створюючи надійну та ефективну систему розумного RFID-замку. RFID-зчитувач зчитує дані з RFID-міток, мікроконтролер обробляє ці дані для автентифікації користувачів, а електронний механізм замка фізично керує доступом до дверей. Завдяки ретельній інтеграції та калібруванню ці компоненти забезпечують безперебійний контроль доступу, гарантуючи безпеку та зручність розумних домашніх середовищ. Розуміння ролі та функціональності кожного апаратного компонента є ключовим для проектування та реалізації ефективної системи розумного RFID-замку як частини цього дисертаційного проекту.

Як студент, який працює над цим дипломним проектом, розуміння інтеграції мікроконтролера, зокрема ESP8266, є вирішальним для успіху системи розумного RFID замка дверей. Мікроконтролер діє як мозок системи, організовуючи комунікацію між апаратними компонентами та виконуючи логіку управління. Давайте заглибимося в інтеграцію мікроконтролера в контексті цього дипломного проекту.

Мікроконтролер ESP8266 функціонує як центральний процесорний пристрій (ЦПУ) системи розумного RFID замка дверей. Він відповідає за отримання вхідних даних від RFID-зчитувача, обробку запитів автентифікації та надсилання команд до електронного механізму замка.

Мікроконтролер ESP8266 взаємодіє з RFID-зчитувачем, забезпечуючи двосторонню комунікацію для обміну даними. Він використовує протоколи, такі як UART (універсальний асинхронний приймач-передавач) або SPI (серійний периферійний інтерфейс), для встановлення зв'язку з RFID-зчитувачем.

Однією з ключових особливостей мікроконтролера ESP8266 є його вбудовані можливості Wi-Fi. Він може підключатися до локальних мереж Wi-Fi, що дозволяє

здійснювати віддалений доступ та керування системою розумного RFID замка дверей за допомогою веб- або мобільних додатків.

Розробка прошивки є ключовим аспектом інтеграції мікроконтролера. Програмний код, написаний мовами, такими як C або Arduino, завантажується на мікроконтролер ESP8266 для визначення поведінки та функціональності системи. Прошивка реалізує логіку керування доступом, механізми автентифікації та комунікаційні протоколи для забезпечення безперебійної роботи системи замка дверей.

На додаток до взаємодії з RFID-зчитувачем, мікроконтролер може інтегрувати інші датчики або периферійні пристрої. Ці датчики можуть включати датчики наближення для виявлення стану дверей, датчики температури для моніторингу навколишнього середовища або датчики руху для цілей безпеки. Мікроконтролер обробляє дані від цих датчиків для підвищення функціональності та універсальності інтелектуальної RFID-системи замка дверей.

Мікроконтролер ESP8266 керує споживанням енергії для оптимізації енергоефективності системи. Він регулює розподіл енергії до різних компонентів, забезпечуючи достатнє постачання, одночасно мінімізуючи непотрібне споживання енергії. Функції керування енергією сприяють продовженню терміну служби батареї (за наявності) та зменшенню загальних експлуатаційних витрат.

Логіка керування доступом регулює поведінку системи, визначаючи, кому надається або відмовляється в доступі на основі попередньо визначених правил і критеріїв. Давайте глибше розглянемо пояснення логіки керування доступом у контексті цієї дисертації.

Логіка контролю доступу починається з процесу автентифікації, де система перевіряє ідентичність осіб, які прагнуть отримати доступ. Після пред'явлення RFID-тегу до зчитувача система захоплює унікальний ідентифікатор, що зберігається на тегу.

Захоплений ідентифікатор RFID-тегу порівнюється з базою даних авторизованих користувачів та їх відповідними правами доступу. Ця база даних

може зберігатися локально в мікроконтролері або на віддаленому сервері, доступному через Wi-Fi-з'єднання.

Виходячи з результатів запиту до бази даних, логіка контролю доступу визначає, чи має особа право доступу до дверей. Авторизованим користувачам надається доступ, тоді як неавторизованим особам доступ забороняється.

Логіка контролю доступу керує правами доступу для кожного авторизованого користувача, що зберігається в базі даних. Дозволи можуть включати надання повного доступу, обмежений доступ до певних часів або областей або тимчасовий доступ для гостей або обслуговуючого персоналу.

Логіка контролю доступу включає механізми обробки помилок для вирішення виняткових випадків та потенційних порушень безпеки. Наприклад, система може спрацювати тривогу або зареєструвати підозрілі спроби доступу, такі як багаторазові недійсні спроби автентифікації або втручання в апаратне забезпечення.

На додаток до логіки локального керування доступом, система може підтримувати можливості віддаленого керування через веб- або мобільні додатки. Авторизовані користувачі можуть віддалено змінювати дозволи доступу, додавати або скасовувати облікові дані користувачів та моніторити активність доступу в реальному часі.

Щоб підвищити надійність і безпеку, логіка керування доступом може реалізувати надмірність і заходи безпеки. Це може включати резервні джерела живлення, резервні канали зв'язку або резервні методи доступу в разі збоїв системи або відключення мережі.

Необхідним аспектом логіки керування доступом є ведення журналу подій доступу. Система реєструє кожну спробу доступу, записуючи деталі, такі як ідентифікатор користувача, часова мітка та результат (надано або відмовлено в доступі). Журнали аудиту забезпечують відповідальність, трасування та цінні відомості для аналізу безпеки та цілей відповідності.

Механізм блокування відповідає за фізичне блокування або розблокування дверей на основі рішень щодо керування доступом, прийнятих системою. Давайте розглянемо пояснення механізму блокування в контексті цієї дисертації.

Інтелектуальна система замка дверей RFID використовує електронні замки для керування доступом до дверей. Електронні замки є сучасною альтернативою традиційним механічним замкам, пропонуючи підвищену безпеку та зручність.

Типи електронних замків включають:

– електричні засувки: електричні засувки - це механізми, встановлені в дверній коробці. При активації вони звільняють засувку дверей, дозволяючи відкрити двері;

– магнітні замки: магнітні замки складаються з електромагніту, встановленого на дверній коробці, і металевої пластини, прикріпленої до дверей. При подачі живлення електромагніт створює магнітну силу, яка надійно утримує двері закритими;

– моторизовані засувки: моторизовані засувки - це механізми з електродвигуном, які висувають або втягують засувки для блокування або розблокування дверей. Вони забезпечують надійну безпеку і підходять як для житлових, так і для комерційних приміщень.

Після отримання сигналу авторизації від логіки контролю доступу механізм блокування активується для блокування або розблокування дверей. Для електричних засувок електричний імпульс втягує засувну пластину, дозволяючи відкрити двері. У магнітних замках живлення подається на електромагніт для звільнення дверей. Моторизовані (або автоматизовані) засувки керуються двигуном, який переміщує засувки в заблоковане або розблоковане положення.

Механізм блокування інтегрований з мікроконтролером, наприклад, ESP8266, який керує його роботою. Мікроконтролер надсилає команди механізму блокування на основі рішень контролю доступу та вводу користувача, отриманого від RFID-зчитувача та інтерфейсу користувача.

Електронні замки можуть включати додаткові функції безпеки для посилення захисту від несанкціонованого доступу. Ці функції можуть включати датчики проти злому, які спрацьовують тривогу, якщо виявлено спробу злому, а також режими відмови безпеки або відмови від безпеки, які визначають поведінку замка в разі відключення живлення.

У контексті розумного домашнього середовища механізм блокування може підтримувати можливості дистанційного керування (рисунок 1.3). Авторизовані користувачі можуть дистанційно блокувати або розблоковувати двері за допомогою веб- або мобільного додатка, забезпечуючи зручність і гнучкість.

Обраний механізм блокування повинен бути сумісним з конструкцією та розмірами дверей. Необхідно враховувати такі фактори, як матеріал дверей, тип рами та вимоги до монтажу, щоб забезпечити належну функціональність і безпеку.

Користувацький інтерфейс є основною точкою взаємодії між користувачами та системою, що дозволяє їм керувати налаштуваннями контролю доступу, відстежувати активність дверей та взаємодіяти з функціями системи. Давайте розглянемо пояснення користувацького інтерфейсу в контексті цієї кваліфікаційної роботи:

Веб-інтерфейс дозволяє користувачам отримати доступ до системи розумного RFID-замку дверей через веб-браузер на своєму комп’ютері або мобільному пристрої. Користувачі можуть увійти в інтерфейс за допомогою своїх облікових даних, щоб отримати доступ до функцій системи та керувати налаштуваннями контролю доступу дистанційно.

Спеціальний мобільний додаток надає користувачам зручний доступ до системи розумного дверного замка зі своїх смартфонів або планшетів. Мобільний додаток пропонує схожі функціональні можливості, що й веб-інтерфейс, але адаптований для мобільного досвіду користувача з оптимізованим макетом і навігацією.

Рисунок 1.3 – Відкрити двері за допомогою телефону

Особливості:

– реєстрація RFID-тегів: користувачі можуть реєструвати нові RFID-теги або картки в системі через користувацький інтерфейс. Цей процес передбачає присвоєння унікального ідентифікатора кожному тегу та його асоціювання з відповідним профілем користувача;

– налаштування доступу: користувацький інтерфейс дозволяє користувачам визначати дозволи доступу для кожного зареєстрованого RFID-тегу. Це включає в себе вказівку дозволених часових проміжків, обмеження доступу до певних зон та керування доступом гостей;

– моніторинг в реальному часі: користувачі можуть відстежувати активність дверей в реальному часі через користувацький інтерфейс. Це включає перегляд журналів доступу, відстеження стану дверей (закриті або відкриті) та отримання сповіщень про події доступу;

– дистанційне керування: користувацький інтерфейс дозволяє користувачам дистанційно блокувати або розблокувати двері, забезпечуючи гнучкість і зручність, особливо коли вони перебувають поза домом.

Інтерфейс користувача має інтуїтивно зрозумілий та зручний дизайн з чіткими меню навігації, описовими піктограмами та інтерактивними елементами. Принципи користувацького досвіду (UX) застосовуються для

забезпечення безперебійної взаємодії та простоти використання, мінімізуючи плутанину та розчарування користувачів.

Безпека є головним пріоритетом у розробці інтерфейсу користувача. Заходи, такі як зашифроване спілкування, безпечні методи автентифікації (наприклад, паролі або біометричні дані) та політика контролю доступу, реалізовані для захисту даних користувачів та цілісності системи. Багатофакторна автентифікація може бути інтегрована для забезпечення додаткового рівня безпеки, особливо для чутливих дій, таких як віддалене розблокування дверей.

Інтерфейс користувача може пропонувати можливості налаштування для адаптації системи до індивідуальних уподобань користувачів. Це може включати настроювані теми, налаштування мови та персоналізовані профілі контролю доступу.

Безпека має першочергове значення для забезпечення цілісності та надійності системи, захисту від несанкціонованого доступу та потенційних вразливостей. Давайте детальніше розглянемо пояснення заходів безпеки в контексті цієї дисертації.

Реалізація протоколів шифрування є важливою для захисту зв'язку між компонентами системи. Шифрування HTTPS (Hypertext Transfer Protocol Secure) або TLS (Transport Layer Security) може бути використано для шифрування даних, що передаються між RFID-зчитувачем, мікроконтролером, інтерфейсом користувача та віддаленими серверами. Шифрування гарантує, що чутлива інформація, така як ідентифікатори RFID-тегів та команди контролю доступу, залишається конфіденційною та захищеною від перехоплення несанкціонованими особами.

Для перевірки ідентичності користувачів та запобігання несанкціонованого доступу до системи реалізовані надійні механізми автентифікації доступу.

Аутентифікація за паролем: користувачі повинні автентифікувати себе за допомогою імені користувача та пароля перед доступом до функціональних

можливостей системи. Біометрична перевірка: Для підвищення безпеки можуть бути інтегровані біометричні методи автентифікації, такі як сканування відбитків пальців або розпізнавання обличчя.

Багатофакторна автентифікація: багатофакторна автентифікація поєднує в собі кілька факторів автентифікації, таких як паролі, біометричні дані та одноразові коди, для посилення контролю доступу та зменшення ризику несанкціонованого доступу.

Політики контролю доступу визначають правила та дозволи, що регулюють доступ до інтелектуальної системи замка дверей RFID. Для визначення рівнів доступу та привілеїв для різних ролей користувачів (наприклад, адміністратори, мешканці, гості) може бути реалізовано контроль доступу на основі ролей (RBAC). Контроль доступу на основі часу дозволяє користувачам визначати дозволи на доступ на основі попередньо визначених часових проміжків, обмежуючи доступ у певні години або дні тижня.

Реєстрація подій доступу та ведення журналів аудиту є важливими для звітності, трасування та судово-кримінального аналізу. Система реєструє спроби доступу, включаючи успішні та невдалі події автентифікації, дії блокування/розблокування замка та зміни конфігурації системи. Журнали аудиту надають детальний запис активності системи, що дозволяє адміністраторам відстежувати дії користувачів, виявляти порушення безпеки та розслідувати інциденти.

На додаток до цифрових заходів безпеки, реалізовано фізичні заходи безпеки для захисту системи від несанкціонованого доступу та маніпуляцій. Для виявлення та запобігання фізичним атакам на систему можна встановити герметичні корпуси та датчики виявлення маніпуляцій. Надійне кріплення апаратних компонентів, таких як RFID-зчитувач та електронний механізм замка, гарантує, що їх неможливо легко маніпулювати або підробити.

Регулярні оновлення та виправлення програмного забезпечення є необхідними для усунення вразливостей безпеки та пом'якшення потенційних загроз. Програмне забезпечення та програмні компоненти системи повинні бути

актуальними, щоб включати останні покращення безпеки та виправлення, випущені виробником.

1.2 Аналіз відомих автоматизованих систем блокування дверей

Аналіз відомих автоматизованих систем блокування дверей дає цінні знання про конструкцію, функціональність та продуктивність таких систем. Ось аналіз заснований на деяких відомих автоматизованих системах блокування дверей.

Особливості системи August Smart Lock включають:

– конструкція: August Smart Lock - це модернізований розумний замок, розроблений для заміни існуючих засувок, що має стильний та мінімалістичний дизайн;

– функціональність: він пропонує безключовий доступ, віддалене блокування та розблокування через мобільний додаток, а також інтеграцію з популярними платформами розумного будинку, такими як Amazon Alexa, Google Assistant та Apple HomeKit;

– безпека: August Smart Lock використовує зашифрований зв'язок та двофакторну автентифікацію для безпечного контролю доступу;

– користувацький досвід: система забезпечує зручний інтерфейс мобільного додатка для керування дозволами на доступ, перегляду журналів активності та дистанційного керування замком;

– інтеграція: вона інтегрується з іншими пристроями та службами розумного дому, дозволяючи користувачам створювати автоматизацію та сценарії;

– зворотний зв'язок: користувачі отримують сповіщення в реальному часі та зворотний зв'язок про зміни статусу замка та активності.

На рисунку 1.4 представлено систему August Smart Lock.

Рисунок 1.4 – August Smart Lock

Система Schlage Connect Smart Deadbolt (рисунок 1.5) володіє наступними характеристиками:

– дизайн: Schlage Connect Smart Deadbolt – це моторизований замок з традиційним дизайном, доступний у різних оздобленнях, щоб відповідати різним естетичним вимогам дверей.

– функціональність: пропонує безключовий вхід, дистанційний доступ через мобільний додаток та інтеграцію з платформами розумного дому, такими як Amazon Alexa та Google Assistant.

– безпека: Schlage Connect оснащений вбудованими датчиками сигналізації для виявлення потенційних загроз та спроб втручання, а також шифруванням для безпечного зв'язку.

– користувацький досвід: замок забезпечує клавіатуру для введення коду, крім керування через мобільний додаток, що відповідає різним уподобанням користувачів.

– інтеграція: він безперебійно інтегрується з системами розумного дому Z-Wave, що дозволяє забезпечити ширшу взаємодію з іншими пристроями.

– зворотний зв'язок: користувачі отримують звуковий відгук та візуальні індикатори про стан замка та рівень заряду акумулятора.

Рисунок 1.5 – Розумний засув Schlage Connect

Yale Assure Lock SL (рисунок 1.6) має наступні характеристики:

– дизайн: замок Yale Assure Lock SL має тонкий та сучасний дизайн з сенсорною клавіатурою, що підходить для сучасного дизайну будинку.

– функціональність: він пропонує безключовий доступ, віддалений доступ через мобільний додаток та сумісність з голосовими помічниками, такими як Amazon Alexa, Google Assistant та Apple HomeKit.

– безпека: замок використовує 128-бітове шифрування AES для безпечного зв'язку та пропонує можливість інтеграції з хабом розумного дому Z-Wave для розширених функцій безпеки.

– користувацький досвід: сенсорна клавіатура забезпечує зручну альтернативу традиційному входу за допомогою ключів, а мобільний додаток замка пропонує інтуїтивно зрозумілі функції керування та управління.

– інтеграція: він інтегрується з різними екосистемами розумного дому, дозволяючи користувачам включати керування замком дверей в більш широкі автоматизаційні процедури.

– зворотний зв'язок: користувачі отримують сповіщення та журнали активності через мобільний додаток, що надає інформацію про події доступу до дверей та зміни стану замка.

Рисунок 1.6 – Yale Assure Lock SL

Kwikset Kevo Smart Lock (рисунок 1.7) має такі властивості:

– конструкція: Kwikset Kevo Smart Lock має традиційну конструкцію засувки з функцією відкриття дотиком, що дозволяє користувачам розблокувати двері простим дотиком;

– функціональність: він пропонує зручність відкриття дотиком, віддалений доступ за допомогою мобільного додатка та інтеграцію зі смарт-платформами, такими як Amazon Alexa та Nest;

– безпека: Kevo Smart Lock використовує кілька рівнів шифрування для безпечного зв'язку та пропонує eKeys для контрольованого спільного доступу;

– користувацький досвід: функція відкриття дотиком забезпечує безконтактний досвід розблокування, тоді як мобільний додаток пропонує додаткові можливості керування та управління.

– інтеграція: він інтегрується з певними смарт-платформами, що дозволяє користувачам включати контроль над замком дверей у більш широкі налаштування смарт-дому;

– зворотний зв'язок: користувачі отримують сповіщення та історію активності через мобільний додаток, що дозволяє їм відстежувати події доступу до дверей та зміни стану замка.

Рисунок 1.7 – Kwikset Kevo Smart Lock

1.3 Висновки. Постановка задачі

Починаючи роботу над цією кваліфікаційною роботою, я зосереджуюся на вирішенні нагальної потреби в безпечному, ефективному та зручному рішенні для контролю доступу в розумних домашніх середовищах. Традиційні механічні дверні замки все частіше замінюються розумними системами дверних замків RFID, що забезпечують підвищену зручність та безпеку. Однак існуючі рішення часто не мають комплексної інтеграції, надійних заходів безпеки та зручних інтерфейсів, що робить власників будинків вразливими до потенційних порушень безпеки та проблем із зручністю використання.

Проблема, що розглядається, охоплює кілька ключових питань:

– відсутність комплексної інтеграції: існуючі розумні системи дверних замків RFID можуть не мати безперебійної інтеграції між апаратними компонентами, програмними функціями та інтерфейсами користувача. Неузгодження або прогалини в інтеграції можуть призвести до неоптимальної продуктивності, проблем із надійністю та труднощів із зручністю використання для кінцевих користувачів;

– проблеми безпеки: безпека є найважливішим аспектом у розумних домашніх середовищах, особливо стосовно систем контролю доступу. Багато готових систем дверних замків RFID можуть не мати надійних заходів безпеки, що робить їх вразливими до несанкціонованого доступу, порушень даних та маніпуляцій;

– зручність використання та досвід користувача: зручність використання та досвід користувача розумних систем дверних замків RFID відіграють вирішальну роль у їхньому впровадженні та ефективності. Складні інтерфейси користувача, громіздкі процеси налаштування та відсутність інтуїтивно зрозумілого керування можуть перешкоджати прийняттю та задоволенню користувачів;

– обмежені можливості віддаленого керування: можливості віддаленого керування, такі як віддалений контроль доступу та моніторинг в реальному часі, стають все більш важливими для сучасних інтелектуальних домашніх середовищ.

Однак існуючі рішення можуть пропонувати обмежені або ненадійні функції віддаленого керування, обмежуючи можливості власників будинків контролювати та відстежувати доступ до своєї власності віддалено;

– відсутність налаштування та гнучкості: власники будинків можуть мати різні вимоги та уподобання щодо налаштувань контролю доступу, керування користувачами та інтеграції з іншими інтелектуальними пристроями домашнього господарства. Існуючі інтелектуальні системи замків дверей RFID можуть не мати можливостей налаштування та гнучкості для ефективного задоволення різноманітних потреб користувачів.

З огляду на ці проблеми, робота спрямована на розробку комплексного програмно-технічного засобу для керування інтелектуальною системою замків дверей RFID на основі мікроконтролера ESP8266 в інтелектуальному домашньому середовищі. Метою є вирішення вищезазначених недоліків шляхом інтеграції апаратних та програмних компонентів, реалізації надійних заходів безпеки, розробки інтуїтивно зрозумілого інтерфейсу користувача, розширення можливостей віддаленого керування та надання опцій налаштування для задоволення різноманітних потреб власників будинків. Вирішуючи ці проблеми, дисертація прагне внести свій внесок у розвиток технології контролю доступу в інтелектуальних домашніх середовищах, в кінцевому підсумку підвищуючи безпеку, зручність та досвід користувача для власників будинків.

2 ЕЛЕМЕНТА БАЗА ПРОГРАМНО-ТЕХНІЧНОГО ЗАСОБУ

2.1 Розумна система замка дверей RFID та елементна база

Продовжуючи дослідження розробки розумної системи замка дверей RFID на основі мікроконтролера ESP8266, вибір елементної бази компонентів формує основу проекту. Ось докладний опис кожного компонента, який я використовуватиму для створення розумної системи замка дверей RFID.

Пропонований програмно-технічний пристрій складається з таких апаратних компонентів:

- ESP8266 (NodeMCU);
- RFID-зчитувач RC522;
- механізм замка дверей (релейний модуль KF-301);
- релейний модуль KF-301;
- 9В акумулятор;
- стабілізатори напруги (LM7805 та AMS1117);
- макетна плата та джемперні дроти.

Мікроконтролер ESP8266 – це недорогий Wi-Fi-мікрочіп з повноцінним TCP/IP-стеком та можливостями мікроконтролера (рисунок 2.1).

Я обрав мікроконтролер ESP8266 через його вбудовані можливості Wi-Fi, низьку вартість та сумісність з Arduino IDE для простого програмування. Його обчислювальна потужність та можливості підключення роблять його придатним для керування аутентифікацією RFID (рисунок 2.2), взаємодією з інтерфейсом користувача та зв'язком з іншими пристроями розумного будинку. Він виступає центральним блоком системи. Він зчитує дані з RFID-зчитувача, обробляє їх, керує механізмом замка дверей, взаємодіє з РК-дисплеєм та підключається до MQTT-брокера через Wi-Fi для дистанційного моніторингу та керування. Необхідна напруга для ESP8266 становить 5В.

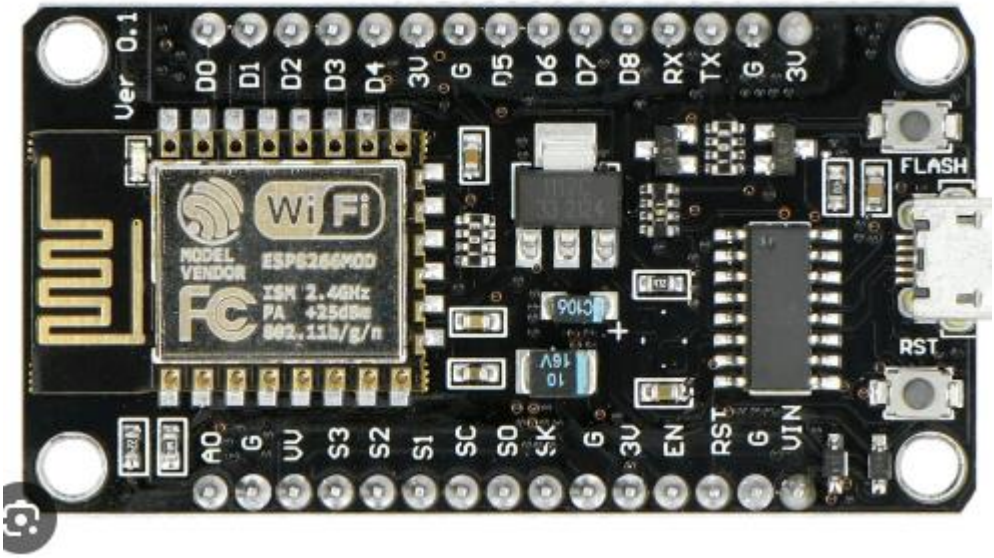


Рисунок 2.1 – ESP8266

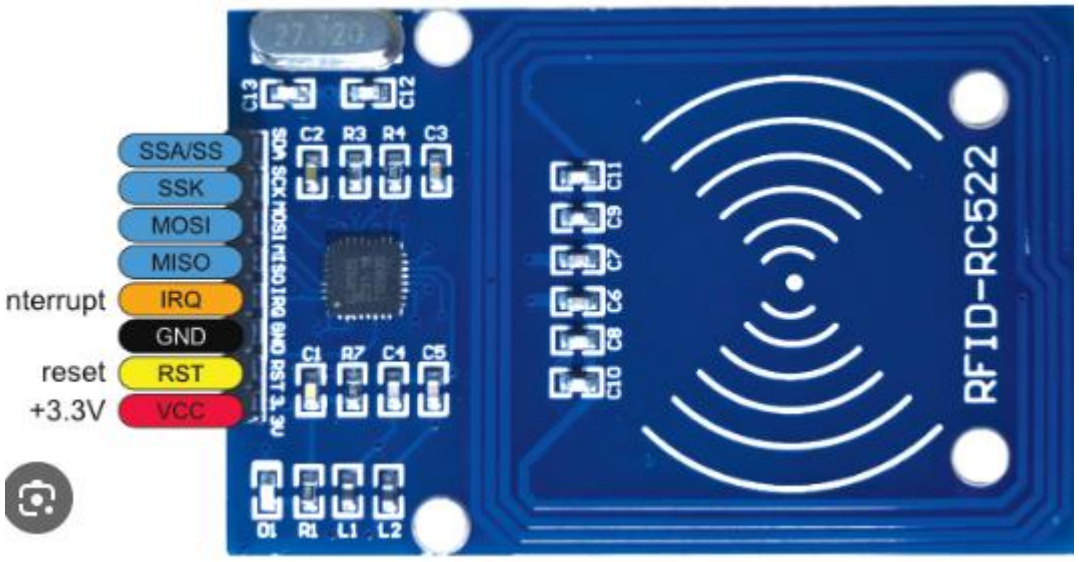


Рисунок 2.2 – Зчитувач RFID RC522

Релейний модуль - це реле, яке встановлено на платі з іншими компонентами для забезпечення ізоляції та захисту (рисунок 2.3). Це робить їх простішими у використанні в різних додатках. Використання релейних модулів пропонує простий і зручний спосіб дистанційного керування електричними системами обладнання. У цій дисертації я використовую релейний модуль KF-301, який буде служити критичним компонентом для безпеки та ефективного керування механізмом блокування дверей. Використовуючи релейний модуль, система може

обробляти вищі вимоги до потужності та забезпечувати ізоляцію між контрольною схемою та навантаженням високої потужності, що підвищує як функціональність, так і безпеку.

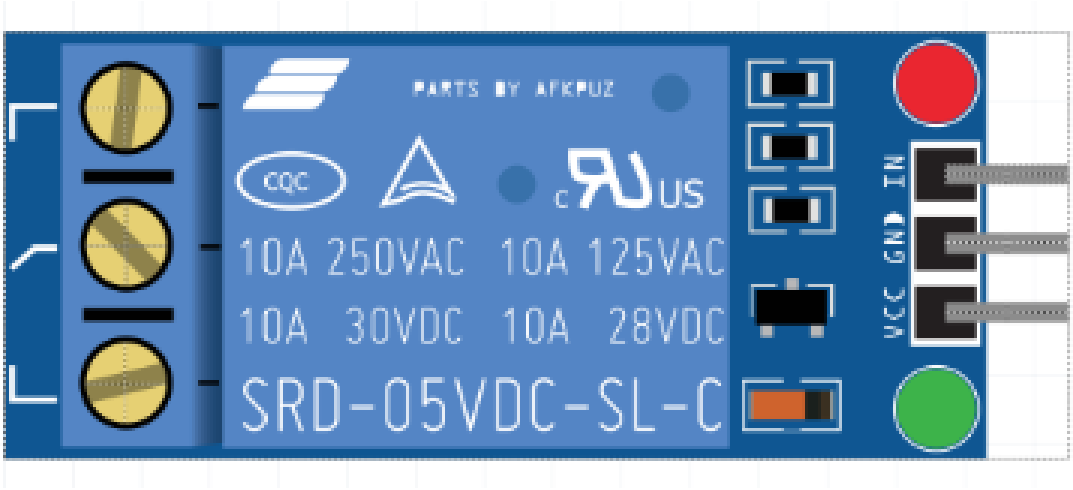


Рисунок 2.3 – Релейний модуль KF-301

Стабільне джерело живлення є необхідним для безперервної роботи системи. Для цієї системи RFID замка дверей я використовую 9В батарею як джерело живлення, вона забезпечує живлення ESP8266, зчитувача RFID, реле та інших компонентів (рисунок 2.4). Зазвичай регулюється до 5В та 3.3В за допомогою стабілізаторів напруги.

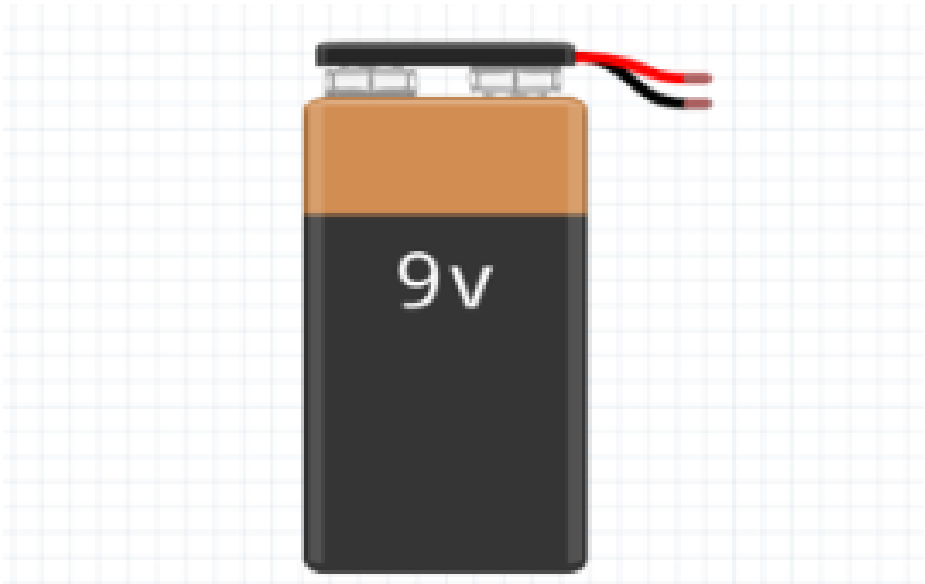


Рисунок 2.4 – 9В батарея

Рідкокристалічний дисплей (LCD) з I2C інтерфейсом (рисунок 2.5). Компонент I2C LCD використовується в програмах, які вимагають візуального або текстового відображення. Цей компонент також використовується, коли потрібен дисплей символів, але сім послідовних GPIO на одному порту GPIO неможливі. Для цієї системи я використовую 16x2 символьний LCD з I2C інтерфейсом, який спрощує підключення до мікроконтролера. Він відображає повідомлення про стан, такі як "Доступ надано", "Доступ заборонено" або UID сканованої RFID-карти. Забезпечує візуальний зворотній зв'язок для користувача.

Рисунок 2.5 – LCD дисплей

Стабілізатори напруги (LM7805 та AMS1117). Стабілізатор напруги - це система, розроблена для автоматичного підтримки постійної напруги (рисунки 2.6, 2.7). Вона може використовувати простий принцип прямої подачі або може включати негативний зворотний зв'язок. Вона може використовувати електромеханічний механізм або електронні компоненти. Залежно від конструкції, її можна використовувати для регулювання однієї або кількох змінних або постійних напруг. Оскільки я використовую джерело живлення, яке забезпечує 9В,

існує потреба в регулюванні напруги, щоб вона відповідала потребам живлення всіх компонентів. Стабілізатор напруги допоможе мені регулювати напругу спеціально для кожного компонента. Для цієї системи я використовував два стабілізатори напруги, які є LM7805 та AMS1117. LM7805 перетворює більш високі напруги на стабільний 5В вихід. У цій системі я використовую його для регулювання 9В до 5В виходу для компонентів, таких як релейний модуль та LCD. AMS1117 перетворює 5В на 3,3 В, що потрібно для ESP8266 та RC522.

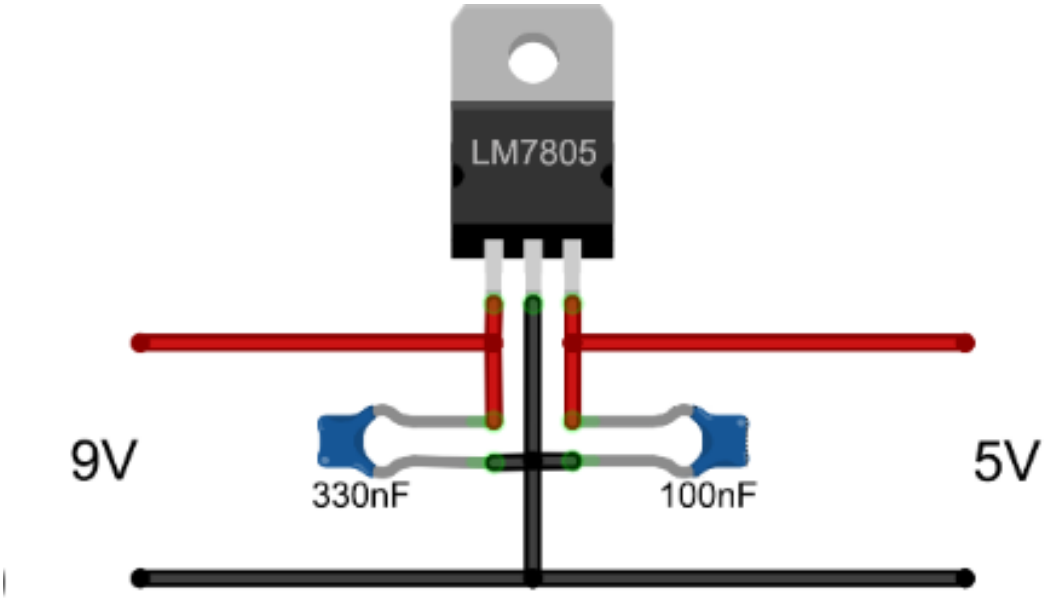


Рисунок 2.6 – LM7805

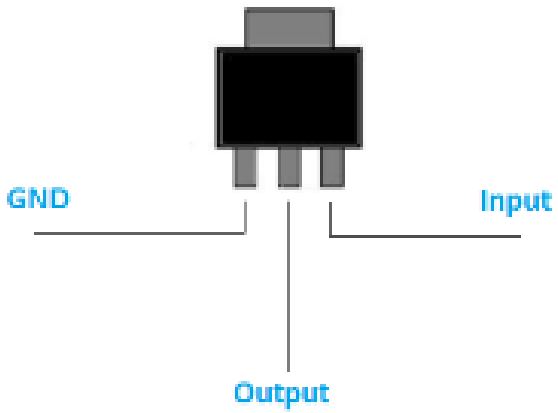


Рисунок 2.7 – AMS1117

Макетна плата та джмперні дроти. Макетна плата – це конструктивна основа для прототипування електроніки, а джмперні дроти використовуються для створення з'єднань (рисунок 2.7). Забезпечує платформу для підключення всіх компонентів разом без пайки, що дозволяє легко вносити коригування та модифікації.

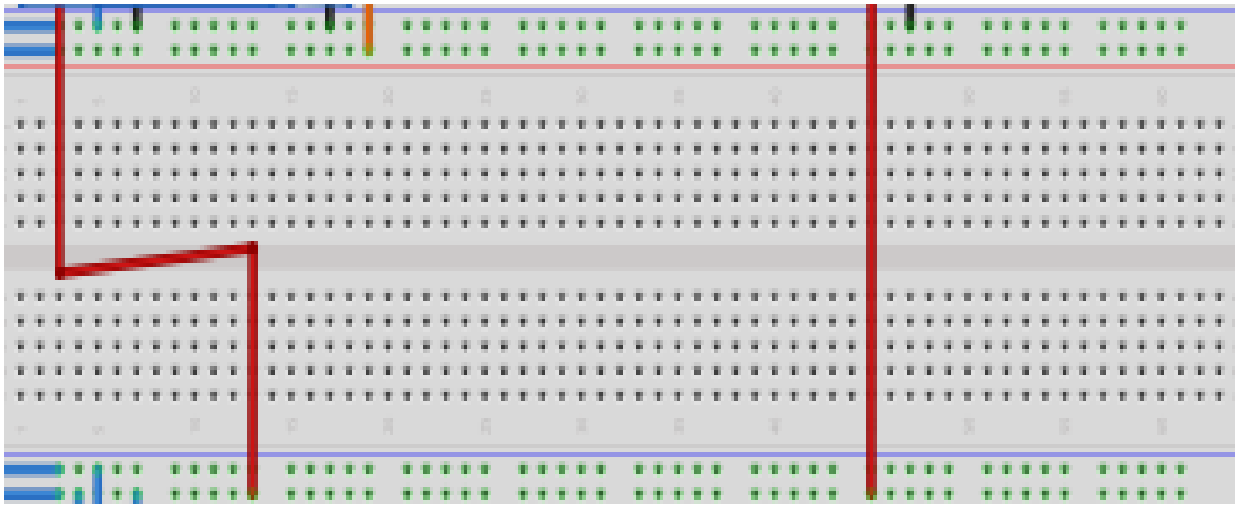


Рисунок 2.7 – Макетна плата

Користувацький інтерфейс (смартфон, який є клієнтом MQTT). Користувацький інтерфейс дозволяє користувачам взаємодіяти з системою, налаштовувати параметри доступу та отримувати зворотній зв'язок. До варіантів належать фізичні інтерфейси, такі як кнопки натискання або сенсорні панелі, доповнені індикаторами стану, такими як світлодіоди або РК-дисплеї, для надання візуального зворотного зв'язку. Інтеграція з цифровими інтерфейсами, такими як мобільні додатки або веб-панелі, може покращити зручність використання та забезпечити віддалене керування системою замка дверей. Мобільний телефон буде діяти як клієнт MQTT, відстежуючи стан замка дверей та надсилаючи команди дистанційного керування на ESP8266. Смартфон підписується на тему стану та публікує команди керування на відповідну тему. Мобільний додаток буде діяти як користувацький інтерфейс.

Рисунок 2.7 – Система блокування дверей

Заходи безпеки є надзвичайно важливими для захисту від несанкціонованого доступу та забезпечення цілісності системи. Реалізації можуть включати шифрування зв'язку між компонентами, механізми автентифікації для доступу користувачів та фізичні засоби безпеки, такі як виявлення спроб втручання або сигналізації вторгнення. Інтеграція безпечних протоколів та кращих практик, а також регулярні оновлення мікропрограмного забезпечення допомагають зменшити потенційні ризики безпеки.

Компоненти слід обирати, щоб забезпечити сумісність та безперебійну інтеграцію з іншими пристроями та платформами розумного будинку. Wi-Fi-з'єднання мікроконтролера ESP8266 дозволяє інтегрувати його з популярними платформами Інтернету речей, такими як MQTT або Home Assistant, що забезпечує взаємодію та розширює можливості системи. Розгляди щодо комунікаційних протоколів, таких як MQTT для обміну повідомленнями або HTTP для веб-інтерфейсів, сприяють інтеграції з існуючими екосистемами розумного будинку.

Економічність є важливим фактором при виборі компонентів, збалансовуючи продуктивність та функції в межах бюджетних обмежень. Оцінка загальної вартості володіння, включаючи початкові витрати на налаштування, поточне

обслуговування та потенційну масштабованість, гарантує фінансову життєздатність проекту.

Ретельно підбираючи та інтегруючи ці елементарні компоненти, створюється міцна основа для інтелектуальної системи RFID-замків дверей на основі мікроконтролера ESP8266. Це забезпечує основу для подальшого розвитку, налаштування та вдосконалення для задоволення конкретних вимог та цілей проекту.

2.2 Принципи функціонування інтелектуальної системи RFID-замків дверей з використанням мікроконтролера ESP8266 в умовах розумного будинку

Проведемо опис системи. Інтелектуальна система RFID-замків дверей інтегрує RFID-зчитувач з мікроконтролером ESP8266 для керування доступом до дверей в умовах розумного будинку. Вона дозволяє користувачам розблокувати двері за допомогою RFID-карт або тегів.

Пропонований програмно-технічний пристрій складається з таких апаратних компонентів:

– мікроконтролер ESP8266 (NodeMCU): це мозок системи, відповідальний за обробку даних, керування RFID-зчитувачем та управління механізмом блокування;

– RFID-зчитувач: зчитує RFID-теги або карти для ідентифікації авторизованих користувачів;

– механізм блокування дверей: фізичний замок на дверях, який керується мікроконтролером;

– джерело живлення: забезпечує електроживлення системи, зазвичай через стандартну розетку змінного струму або батарею.

Програмні компоненти запропонованого пристрою:

– прошивка: Запрограмована на мікроконтролер ESP8266, прошивка керує зв'язком між зчитувачем RFID та механізмом замка дверей. Вона також обробляє автентифікацію користувачів та логіку керування доступом;

– користувацький інтерфейс: мобільний додаток або веб-інтерфейс, який дозволяє користувачам керувати дозволами на доступ, переглядати журнали доступу та дистанційно керувати замком дверей.

Основна робота запропонованого пристрою включає:

– ініціалізація: система запускається, і мікроконтролер ESP8266 ініціалізує зчитувач RFID, підключається до локальної Wi-Fi мережі (якщо це можливо) та готується до отримання команд;

– автентифікація користувача: коли користувач підходить до дверей, він пред'являє свою RFID-карту або брелок зчитувачу RFID. Зчитувач RFID зчитує унікальний ідентифікатор з карти/брелка та надсилає його на мікроконтролер. Мікроконтролер порівнює отриманий ідентифікатор зі списком авторизованих користувачів, що зберігається в його пам'яті;

– керування доступом: якщо ідентифікатор відповідає авторизованому користувачеві, мікроконтролер надсилає сигнал механізму замка дверей для розблокування дверей. Якщо ідентифікатор не відповідає або не розпізнається, мікроконтролер відмовляє в доступі та може активувати сигнал тривоги (наприклад, включити сирену або надіслати сповіщення);

– блокування/розблокування: після отримання команди розблокування від мікроконтролера механізм замка дверей розблоковується, дозволяючи користувачеві відкрити двері. Після закінчення заданого періоду або після закриття дверей мікроконтролер надсилає сигнал для повторного блокування замка, забезпечуючи безпеку дверей.

2.3 Огляд систем одноплатних комп'ютерів та MQTT

Системи одноплатних комп'ютерів (SBC) - це повні комп'ютерні системи, побудовані на одній друкованій платі (рисунок 2.8). Вони зазвичай включають мікропроцесор, пам'ять, порти введення/виведення (I/O) та інші необхідні компоненти для обчислювальних завдань. SBC компактні, доступні за ціною та

універсальні, що робить їх популярними для різних застосувань, від хобі-проектів до промислової автоматизації.

Рисунок 2.8 – Raspberry Pi

Ось огляд систем одноплатних комп'ютерів:

Компоненти одноплатного комп'ютера:

– SBC часто мають мікропроцесор або систему на кристалі (SoC), яка слугує центральним процесорним блоком (CPU). Поширені архітектури процесорів включають ARM, x86 та RISC-V;

– SBC постачаються з вбудованою пам'яттю, включаючи оперативну пам'ять (RAM) для запуску програм та сховище для зберігання даних та файлів операційної системи. Деякі SBC також підтримують розширення за допомогою зовнішніх карт пам'яті або модулів;

– SBC включають різні порти введення-виведення (I/O) для підключення периферійних пристроїв та зовнішніх пристроїв, таких як порти USB, HDMI або DisplayPort для виведення відео, порти Ethernet для мережі, висновки GPIO для універсального введення-виведення та аудіороз'єми;

– SBC можуть мати вбудовані варіанти зберігання, такі як флеш-пам'ять eMMC або вбудовані слоти для SD-карт. Вони також підтримують зовнішні пристрої зберігання, такі як USB-накопичувачі або мережеві сховища (NAS) для додаткової ємності зберігання;

– багато SBC включають вбудовані можливості Wi-Fi та Bluetooth для бездротового підключення. Вони також можуть мати порти Ethernet для дротового підключення до мережі;

– деякі SBC пропонують розширювальні слоти, такі як PCIe або mini PCIe, для додавання додаткових функцій, таких як графічні процесори (GPU), твердотільні накопичувачі (SSD) або інші розширювальні карти.

Операційні системи одноплатних комп'ютерів:

– SBC підтримують різні операційні системи, включаючи дистрибутиви Linux (наприклад, Debian, Ubuntu, Raspbian для Raspberry Pi), Android, Windows 10 IoT Core та власні операційні системи, розроблені для певних застосувань;

– вибір операційної системи залежить від таких факторів, як сумісність з апаратним забезпеченням, вимоги до програмного забезпечення та переваги користувача.

Застосування одноплатного комп'ютера включає:

– одноплатні комп'ютери мають широкий спектр застосування в різних галузях та сферах, включаючи;

– одноплатні комп'ютери, такі як Raspberry Pi, популярні в освітніх закладах для навчання програмуванню, електроніці та концепціям комп'ютерних наук;

– одноплатні комп'ютери використовуються в проектах Інтернету речей (IoT) для збору даних з датчиків, керування пристроями та створення систем автоматизації розумного будинку;

– одноплатні комп'ютери використовуються в вбудованих системах для промислової автоматизації, робототехніки, автомобільних застосувань тощо;

– аматори та творці використовують одноплатні комп'ютери для проектів DIY, таких як медіацентри, ретро-ігрові консолі, домашні сервери та системи автоматизації будинку;

– інженери та розробники використовують одноплатні комп'ютери для швидкого прототипування апаратних та програмних рішень перед переходом до виробництва.

Інструменти розробки одноплатного комп'ютера:

– одноплатні комп'ютери зазвичай постачаються з інструментами розробки програмного забезпечення та ресурсами для полегшення розробки додатків. До них можуть входити SDK (набори для розробки програмного забезпечення), бібліотеки програмування, форуми спільноти та документація;

– поширені мови програмування для розробки SBC включають Python, C/C++, Java та JavaScript.

Переваги систем одноплатних комп'ютерів включають:

– SBC компактні та легкі, що робить їх придатними для просторів з обмеженим простором та портативних застосунків;

– SBC є економічно ефективними порівняно з традиційними настільними або серверними системами, що робить їх доступними для любителів, студентів та малого бізнесу;

– SBC є універсальними платформами, які можна налаштувати та адаптувати для широкого кола застосунків та проектів;

– SBC часто поставляються з дружчими до користувача інтерфейсами та програмними інструментами, що робить їх доступними для користувачів з різним рівнем технічних знань.

Обмеження одноплатного комп'ютера:

– SBC зазвичай мають меншу обчислювальну потужність і пам'ять порівняно з традиційними настільними або серверними системами, що обмежує їх придатність для ресурсомістких завдань;

– SBC можуть мати обмежені можливості вводу-виводу порівняно з більшими системами, що може обмежити їх варіанти підключення та підтримку периферійних пристроїв;

– хоча деякі SBC підтримують розширення за допомогою зовнішніх інтерфейсів, вони можуть не пропонувати той самий рівень масштабованості та гнучкості, що й більші системи.

Протокол MQTT. MQTT означає Message Queuing Telemetry Transport. Це легкий протокол обміну повідомленнями, який використовується у випадках, коли клієнтам потрібен невеликий розмір коду, і вони підключені до ненадійних мереж або мереж з обмеженими ресурсами пропускної здатності. Він в основному використовується для зв'язку між машинами (M2M) або для підключень типу Інтернету речей.

У цій роботі MQTT або Message Queuing Telemetry Transport - це протокол, який дозволяє пристроям розумного будинку спілкуватися один з одним. Це протокол обміну повідомленнями, який використовує модель публікації-підписки, тобто пристрої можуть публікувати повідомлення на теми, а інші пристрої можуть підписуватися на ці теми, щоб отримувати повідомлення.

MQTT має кілька компонентів, які включають брокер та клієнт. Проста блокова діаграма протоколу MQTT представлена на рисунку 2.8.

Брокер - це бекенд-система, яка координує повідомлення між різними клієнтами. До обов'язків брокера належить отримання та фільтрація повідомлень, ідентифікація клієнтів, які підписані на кожне повідомлення, та відправка їм повідомлень. Широко поширеним брокером є Mosquitto.

Клієнт - це будь-який пристрій, від сервера до мікроконтролера, який запускає бібліотеку MQTT. Якщо клієнт надсилає повідомлення, він діє як видавець, а якщо він отримує повідомлення, він діє як одержувач. По суті, будь-який пристрій, який спілкується за допомогою MQTT через мережу, можна назвати пристроєм клієнта MQTT.

ESP8266 (клієнт MQTT) публікує UID на MQTT-брокер на тему "door/lock/status" під час сканування RFID-карти. Він також підписується на тему

"door/lock/status", щоб отримувати команди від віддалених пристроїв, наприклад, для розблокування дверей.

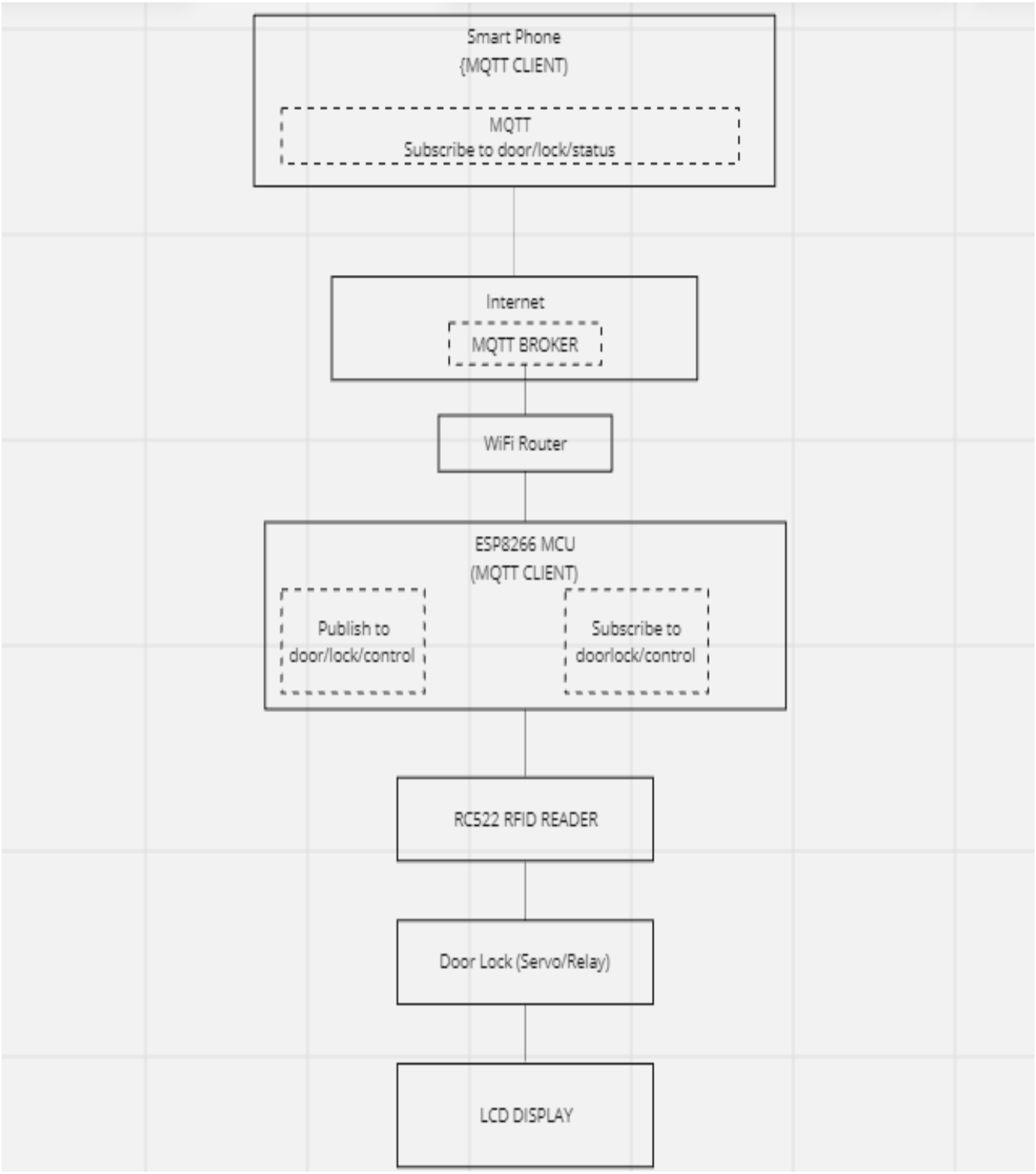


Рисунок 2.8 – Проста блокова діаграма протоколу MQTT

ESP8266 підключається до маршрутизатора Wi-Fi, щоб отримати доступ до Інтернету та спілкуватися з брокером.

Сервер брокера маршрутизує повідомлення між ESP8266 та іншими клієнтами MQTT, такими як смартфони. Він отримує UID від ESP8266 і надсилає команди керування зі смартфона назад на ESP8266.

Смартфони підписуються на "door/lock/status", щоб отримувати сповіщення, коли використовується RFID-карта, вони також можуть публікувати повідомлення на "door/lock/status", щоб розблокувати двері віддалено.

Щодо зчитувача RFID RC522, він зчитує RFID-картки та надсилає UID на ESP8266 для обробки.

Дверний замок контролюється ESP8266 для фізичного блокування та розблокування дверей на основі UID RFID-картки або віддалених команд, отриманих через MQTT.

Нарешті, РК-дисплей відображатиме стан системи дверного замка. Наприклад, доступ надано або доступ заборонено.

MQTT пропонує простий і стабільний варіант інтеграції Smart Lock у вашу домашню автоматизацію. Він дозволяє надсилати та отримувати повідомлення з вашої системи дверного замка через Інтернет.

Ви можете отримувати сповіщення на свій телефон або комп'ютер, коли хтось використовує зчитувач RFID, і навіть віддалено розблокувати двері.

Його також можна використовувати для надсилання журналів доступу RFID на центральний сервер або хмарний сервіс. Ці дані можна проаналізувати пізніше, щоб вивчити шаблони використання, порушення безпеки або для загального ведення записів.

Використання MQTT дозволяє дверному замку безперебійно інтегруватися з іншими розумними пристроями, такими як освітлення, камери або сигналізації, що підвищує загальну функціональність розумного будинку.

MQTT масштабований, тобто ви можете додавати більше пристроїв або розширювати функціональність без значних змін до вашої існуючої конфігурації. Це спрощує додавання більше розумних замків або додаткових

датчиків. Робота з MQTT дала мені практичний досвід роботи з галузевим стандартом протоколу, який широко використовується в проектах IoT. Ці знання корисні для моїх майбутніх проектів або кар'єри.

2.4 Електричні характеристики пропонованого програмного-технічного пристрою

Розглянемо електричні характеристики пропонованого програмного-технічного пристрою.

Джерело живлення: Оскільки я використовую 9-вольтову батарею, я підключив її до входу стабілізатора напруги LM7805. LM7805 видає 5 В, що використовується для живлення релейного модуля та РК-дисплея. Стабілізатор напруги AMS1117 отримує 5 В від LM7805 і видає 3,3 В, що використовується для живлення ESP8266 та зчитувача RFID RC522.

З'єднання ESP8266 з іншими компонентами: контакт VCC ESP8266 підключений до шини 3,3 В на макетній платі. Контакт GND ESP8266 підключений до шини заземлення. Контакти GPIO ESP8266 підключені до керуючих контактів релейного модуля та РК-дисплея.

Зчитувач RFID RC522: контакт VCC підключений до шини 3,3 В. Контакт GND підключений до шини заземлення. SPI контакти (SDA, SCK, MOSI, MISO, RST, IRQ) підключені до відповідних контактів GPIO на ESP8266.

Реле-модуль: Пін VCC підключений до шини 5В. Пін GND підключений до шини землі. Пін IN підключений до GPIO-піна на ESP8266.

LCD-дисплей (I2C): Пін VCC підключений до шини 5В. Пін GND підключений до шини землі. Піни SDA та SCL підключені до відповідних GPIO-пінів на ESP8266 для I2C-комунікації.

Таблиця 2.1 – Підсумок з'єднань між компонентами замка дверей

Компонент	Точки з'єднання	Вимоги до напруги	Коментарі щодо компонентів
9В батарея	V+ та GND	9В	Забезпечує основне живлення для системи
Стабілізатор напруги (LM7805)	Вхід: 9В батарея V+ та GND Вихід: 5В шина на макетній платі, GND	Вхід: 9В Вихід: 5В	Стабілізує 9В до 5В для компонентів, які потребують 5В
Стабілізатор напруги (AMS1117)	Вхідна шина 5В Вихідна шина 3.3В на макетній платі, GND	Вхід: 5В Вихід: 3.3В	Стабілізує 5В до 3.3В для компонентів, які потребують 3.3В
ESP8266	VCC: 3.3В шина GND:GND Виводи GPIO: Підключені до RFID, реле, LCD	3.3В	Головний контролер системи. Живиться від 3.3В шини
Зчитувач RFID RC522	VCC: 3.3В шина GND:GND SDA,SCK,MOSL,MIDO,RST,IRQ: Підключений до ESP8266	3.3В	Спілкується з ESP8266 через SPI

Продовження Таблиці 2.1 – Підсумок з'єднання між компонентами замка дверей

Реле модуль	VCC:5V шина, GND:GND, IN:GPIO контакт ES8266, NO/NC і COM:підключені пристрої	5V	Керується ESP8266 для перемикання замка, котушка реле живиться від 5V
LCD дисплей (I2C)	VCC:5V шина, GND:GND, SDA, SCL:підключені до GPIO контактів ESP8266	5V	Відображає повідомлення про стан. Спілкується з ESP8266 через I2C.

2.5 Висновки

Розглянуті питання щодо основної роботи інтелектуальної RFID системи замка дверей за допомогою мікроконтролера ESP8266 в середовищі розумного будинку дозволяють зробити такі висновки. Інтелектуальна RFID система замка дверей на основі мікроконтролера ESP8266 є ефективним рішенням для забезпечення безпеки та комфорту в розумних будинках. Вона забезпечує безконтактний доступ до приміщень за допомогою радіочастотної ідентифікації (RFID), дозволяючи користувачам відкривати двері за допомогою RFID-карт або брелоків. Основними елементами системи є RFID-зчитувач, мікроконтролер ESP8266, електромагнітний замок та джерело живлення. Мікроконтролер ESP8266 діє як центральний елемент системи, керує процесом ідентифікації та надання доступу. Він отримує дані від RFID-зчитувача, перевіряє їх у базі даних авторизованих користувачів і, у разі позитивного збігу, активує електромагнітний замок для відкриття дверей. Крім того, ESP8266 може підключатися до Wi-Fi мережі, що дозволяє інтегрувати систему з іншими компонентами розумного будинку та дистанційно керувати доступом.

3 РЕАЛІЗАЦІЯ ПРОГРАМНО-ТЕХНІЧНОГО ЗАСОБУ КЕРУВАННЯ ДВЕРНИМ ЗАМКОМ НА ОСНОВІ МІКРОКОНТРОЛЕРА ESP8266

3.1 Підготовка середовища

Arduino IDE та ESP8266. Інтегроване середовище розробки Arduino містить текстовий редактор для написання коду, область повідомлень, текстову консоль, панель інструментів з кнопками для загальних функцій та ряд меню. Вона підключається до апаратного забезпечення Arduino для завантаження програм та спілкування з ними, тоді як ESP8266 - це невеликий, недорогий Wi-Fi мікрочіп з повним TCP/IP стеком та можливостями мікроконтролера. Це означає, що він може підключатися до Wi-Fi мереж та спілкуватися з іншими пристроями або Інтернетом. Його часто використовують у проектах IoT (Інтернет речей) через його доступність та універсальність.

Arduino IDE надає зручний інтерфейс для написання, компіляції та завантаження коду на мікроконтролер. У цій дисертації Arduino IDE дозволить мені написати код для керування ESP8266, обробки автентифікації RFID, керування механізмами блокування дверей та взаємодії з іншими компонентами системи. Що стосується ESP8266, то він є серцем цієї дисертації або проекту в тому сенсі, що він служить мікроконтролером і відповідає за керування системою замка дверей RFID та підключення її до Інтернету в середовищі розумного будинку. Вбудована функція Wi-Fi дозволяє спілкуватися з іншими пристроями та віддалено отримувати доступ до системи замка дверей. Завдяки низькій вартості, невеликому розміру та універсальності ESP8266 є ідеальним вибором для моєї дисертації.

Розглянемо детальніше процес встановлення середовища розробки Arduino IDE.

Щоб розпочати роботу з Arduino IDE, вам потрібно завантажити програму з офіційного веб-сайту: https://www.arduino.cc/en/software.

Кроки встановлення включають:

Крок 1: Відкрийте файл і перейдіть до налаштувань, а потім відкрийте його (рисунок 3.1).

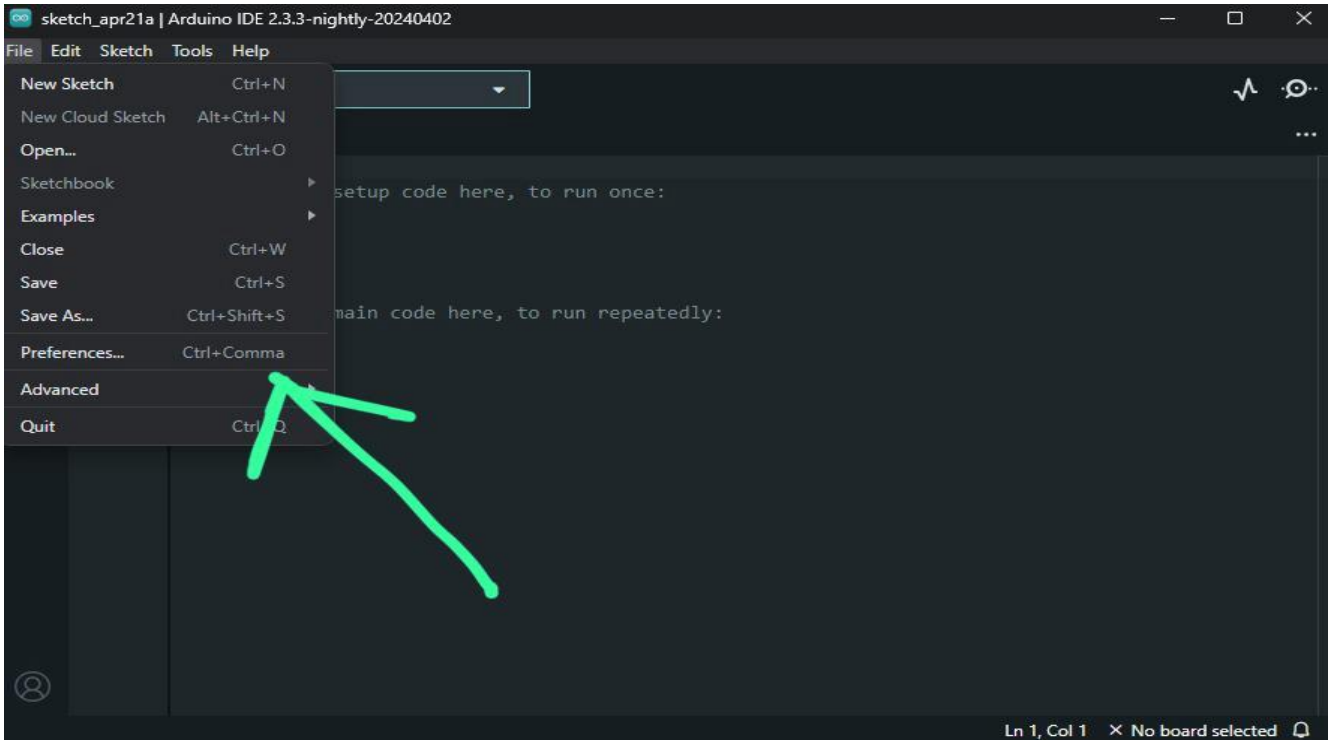


Рисунок 3.1 – Крок 1

Крок 2: У полі "Additional Board Manager URLs" додайте наступний URL: http://arduino.esp8266.com/stable/package_esp8266com_index.json (рисунок 3.2)

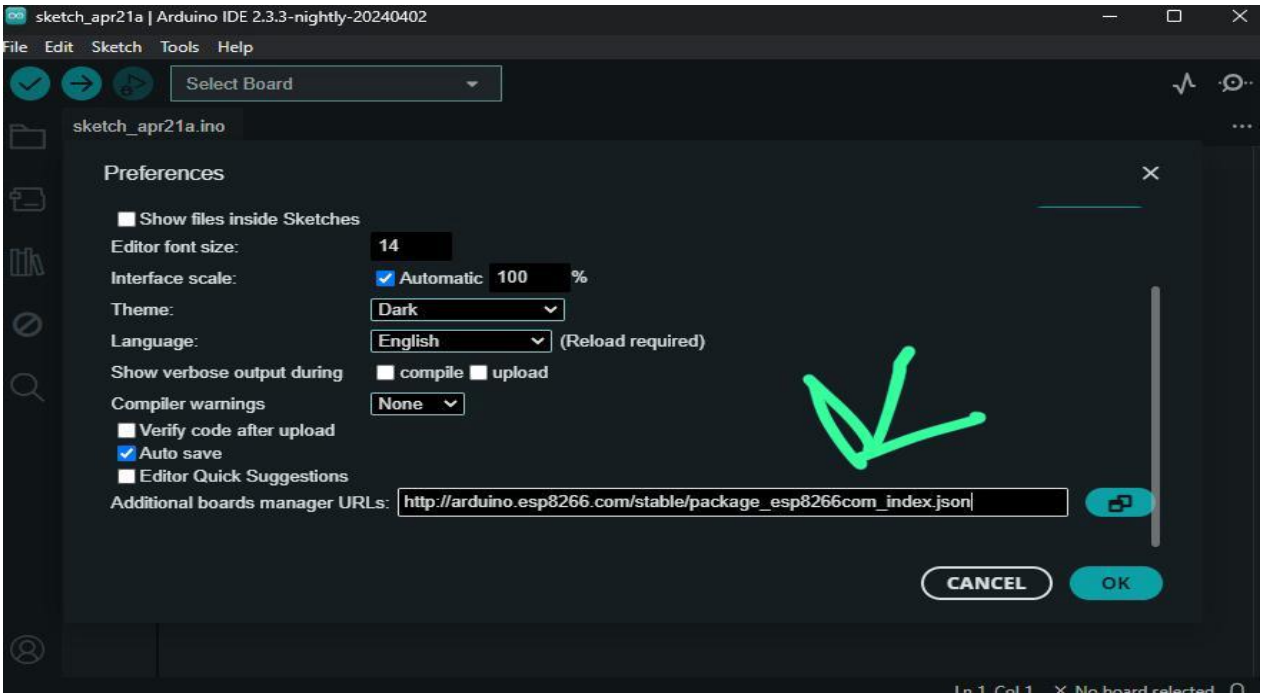


Рисунок 3.2 – Крок 2

Крок 3: Після додавання URL перейдіть до Інструменти > Плата > Диспетчер плат (рисунок 3.3).

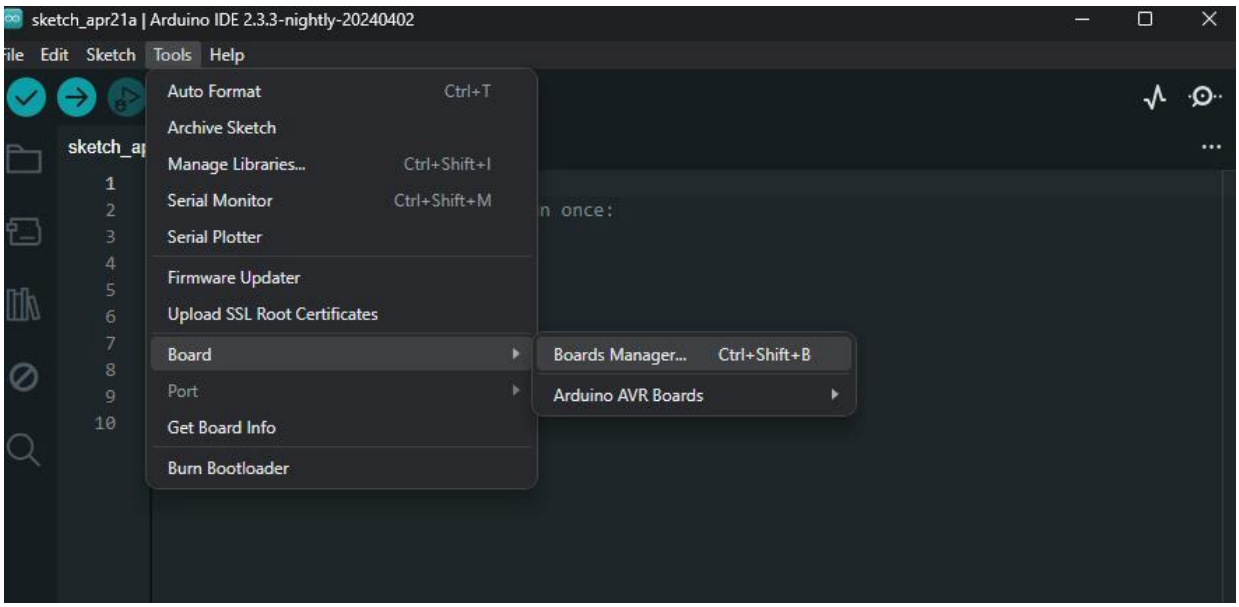


Рисунок 3.3 – Крок 3

Крок 4: У Диспетчері плат введіть "ESP8266" у рядок пошуку. Виберіть пакет "esp8266 by ESP8266 Community" і натисніть кнопку "Встановити" (рисунок 3.4).

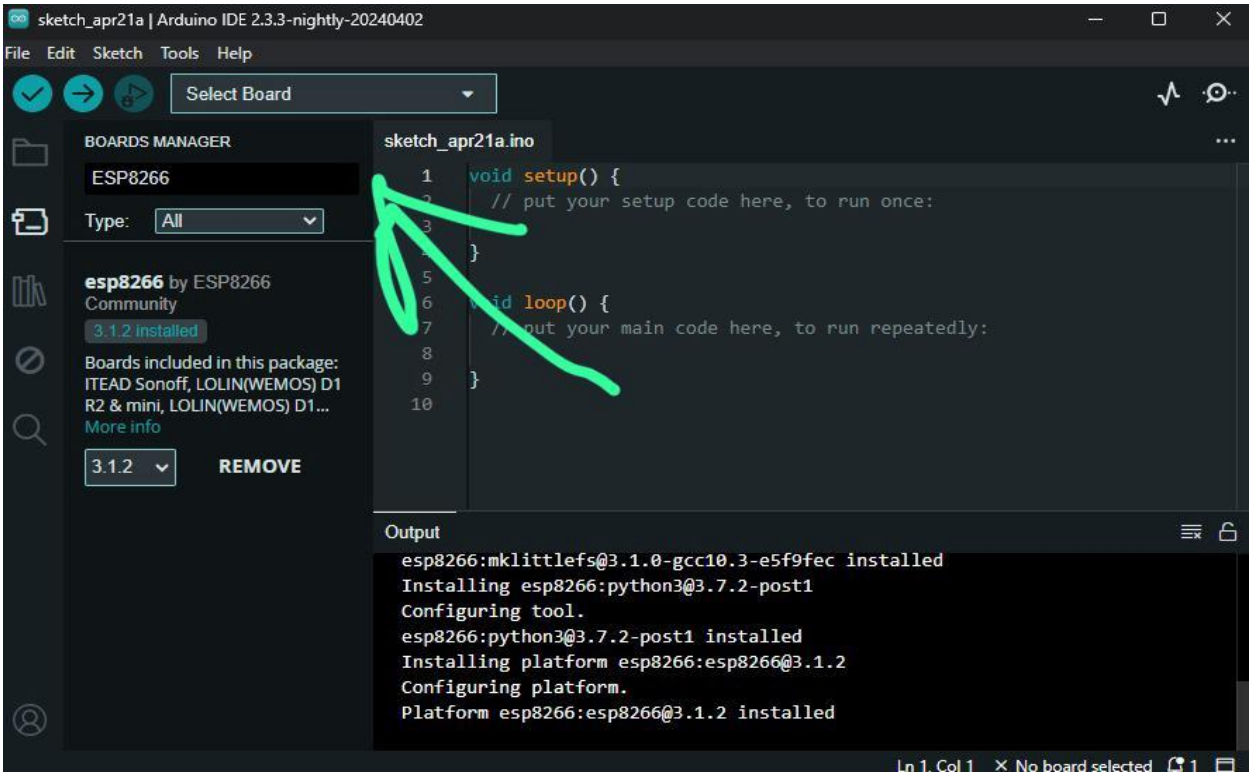


Рисунок 3.4 – Крок 4

Крок 5: Підтвердження встановлення ESP8266 (рисунок 3.5).

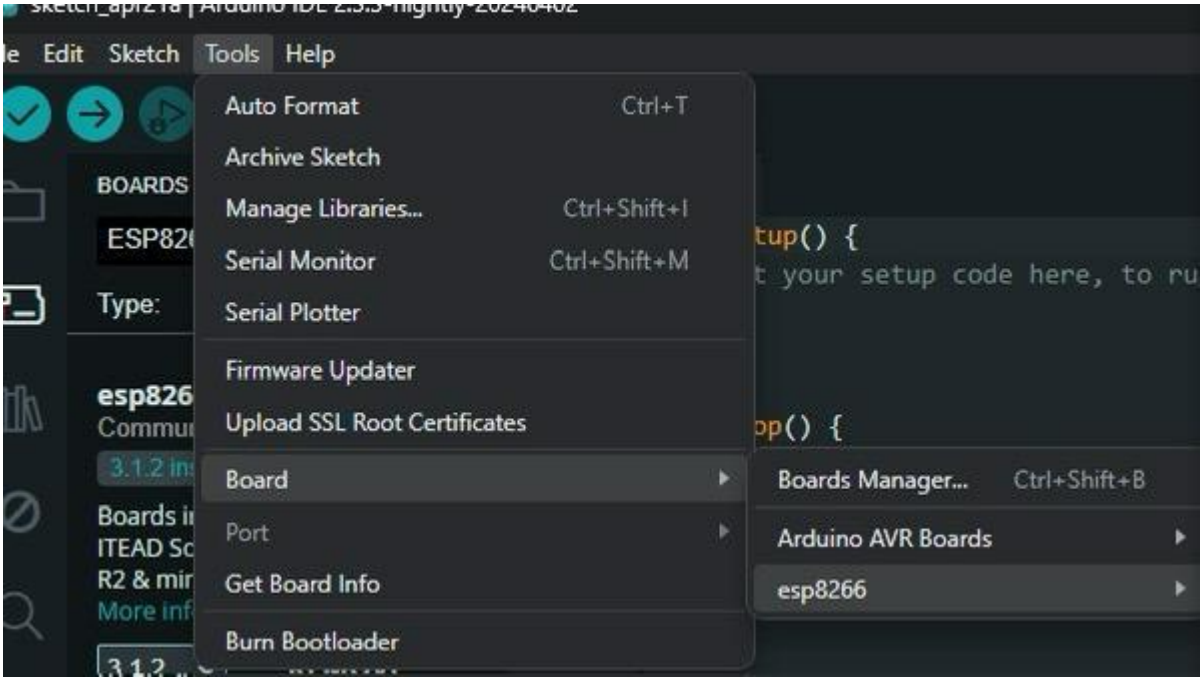


Рисунок 3.5 – Крок 5

3.2 Підключення до макетної плати та монтажна схема

Fritzing - це програмний інструмент, розроблений для допомоги ентузіастам електроніки та новачкам у створенні та документуванні електронних схем інтуїтивним та візуальним способом. Він надає платформу для проектування схем, макетів друкованих плат (PCB) та схем без необхідності вдосконалених технічних знань або спеціалізованих програмних навичок.

Fritzing - це універсальний інструмент, який використовується для проектування, прототипування та документування електронних схем. Він надає зручний інтерфейс, де користувачі можуть візуально проектувати схеми, вибираючи та розміщуючи компоненти на віртуальному полотні. Ця функція перетягування робить його доступним як для початківців, так і для досвідчених користувачів, дозволяючи легко експериментувати та ітерувати.

Однією з ключових функцій Fritzing є його здатність сприяти прототипуванню. Користувачі можуть віртуально імітувати свої проекти схем, перш ніж фізично збирати їх на макетній платі або PCB. Це економить час та

ресурси, дозволяючи користувачам вдосконалювати свої проекти та усувати потенційні проблеми, перш ніж приступати до фізичного будівництва.

Додатково, Fritzing генерує чіткі та лаконічні схематичні діаграми, схеми з'єднань на макетній платі та макети друкованих плат, які слугують документацією для електронних проектів. Ці візуальні представлення допомагають користувачам зрозуміти, як компоненти з'єднані та як слід будувати схему. Цей аспект документації є особливо цінним в освітніх закладах, де Fritzing широко використовується для навчання електроніки та концепцій проектування схем.

Крім того, Fritzing сприяє співпраці та обміну в межах спільноти електроніки. Користувачі можуть ділитися своїми проектами з іншими, як у вигляді файлів, так і експортуючи їх як зображення або PDF-файли. Це дозволяє співпрацювати над проектами, збирати відгуки та демонструвати завершені проекти широкій спільноті.

Fritzing є важливим активом у моєму дипломному проекті, який зосереджений на створенні програмного та технічного засобу для керування розумною системою замка дверей RFID за допомогою мікроконтролера ESP8266 в середовищі розумного будинку.

Включення діаграм Fritzing в мою дипломну роботу дозволяє мені візуально проілюструвати складну апаратну конфігурацію системи розумного замка дверей RFID. Ці діаграми забезпечують чітке та інтуїтивно зрозуміле представлення того, як мікроконтролер ESP8266, зчитувач RFID, механізм замка дверей та інші компоненти взаємопов'язані. Цей візуальний посібник не тільки підвищує зрозумілість моєї дипломної роботи, але й гарантує, що апаратна конфігурація добре задокументована для майбутнього використання.

Більше того, Fritzing дозволяє мені документувати інтеграцію різних апаратних компонентів у середовищі розумного будинку. За допомогою детальних схем та макетів друкованих плат, згенерованих Fritzing, я можу продемонструвати, як мікроконтролер ESP8266 взаємодіє з RFID-зчитувачем для автентифікації користувачів та керування доступом до системи замків дверей. Це візуальне

представлення допомагає передати безперебійну інтеграцію різних елементів системи для досягнення бажаної функціональності.

Крім підвищення якості презентації моєї дисертації, діаграми Fritzing слугують освітній меті, допомагаючи читачам зрозуміти основні принципи роботи розумної RFID-системи замків дверей. Вони надають уявлення про ролі та взаємодію кожного апаратного компонента, роблячи технічні концепції більш доступними для моєї аудиторії, включаючи членів комітету з дисертації та майбутніх дослідників.

3.3 Фізична схема програмно-технічного засобу керування дверним замком на основі мікроконтролера ESP8266

Розглянемо фізичну схему програмного та технічного засобу керування інтелектуальною RFID-системою замків дверей за допомогою мікроконтролера ESP8266. З'єднання компонентів системи замків дверей на макетній платі та схема системи замків дверей представлені на рисунках 3.6 та 3.7 відповідно.

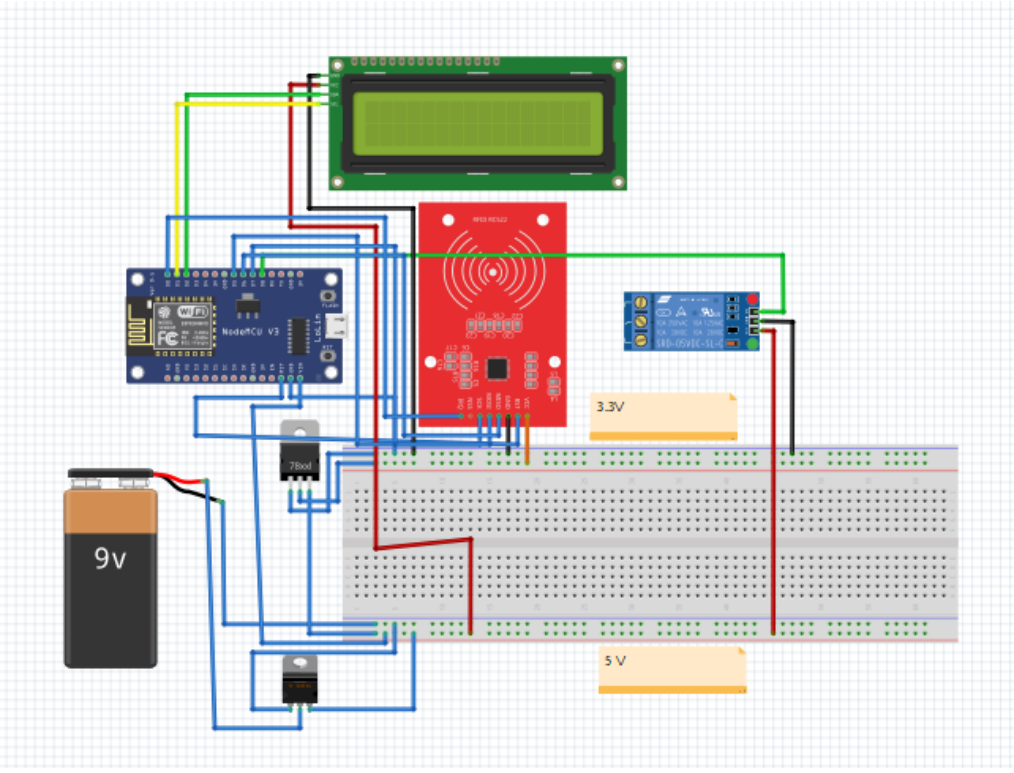


Рисунок 3.6 – Підключення компонентів системи замка дверей на макетній платі

ESP8266 спеціальний, оскільки він дуже добре підключається до Wi-Fi мереж. Це як мати вбудований Wi-Fi чіп у своєму мозку.

Модуль зчитувача RFID (радіочастотної ідентифікації) використовується для зчитування унікальних ідентифікаторів міток RFID. Ці модулі зазвичай спілкуються за допомогою протоколів SPI (послідовний периферійний інтерфейс) або UART (універсальний асинхронний приймач-передавач).

Мітки RFID - це невеликі пристрої, які містять електронно збережену інформацію. Кожна мітка має унікальний ідентифікатор, який зчитується зчитувачем RFID. У цьому проекті мітки RFID використовуються для контролю доступу, де кожен авторизований користувач має унікальну мітку RFID.

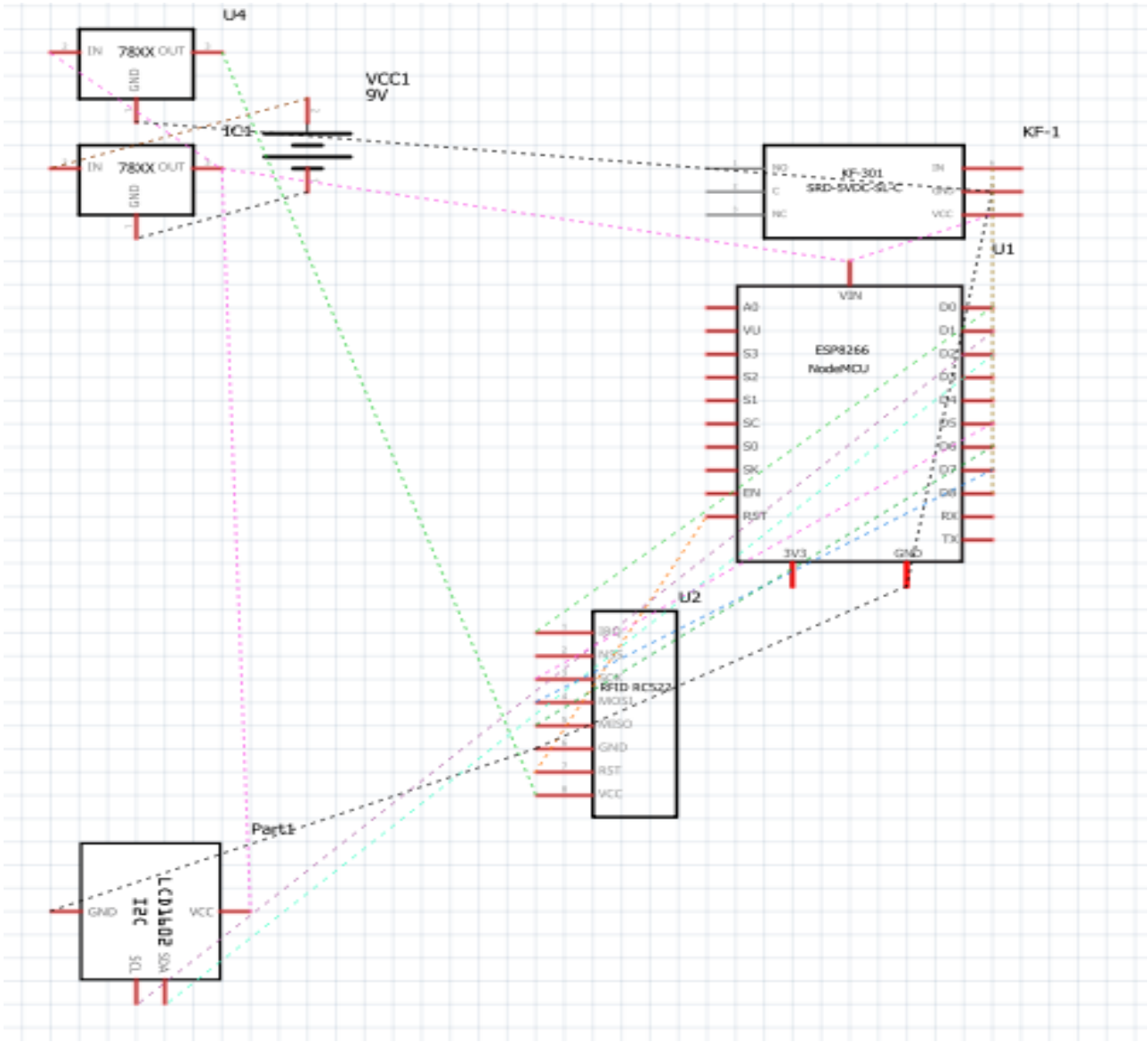


Рисунок 3.7 – Електрична схема

Електромеханізм замка дверей - це пристрій, який можна електронно керувати для блокування або розблокування дверей.

Компоненти в системі потребують стабільного джерела живлення (рисунок 3.8). Джерело живлення 5 В можна використовувати для живлення мікроконтролера ESP8266, модуля зчитувача RFID та електромеханізму замка дверей.

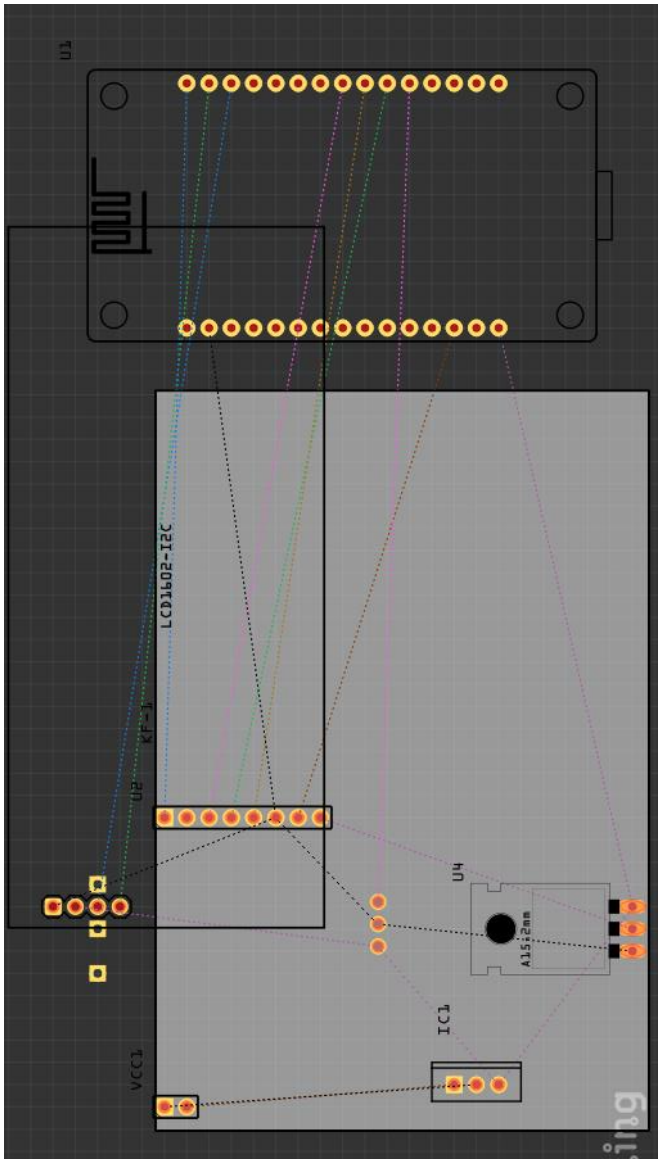


Рисунок 3.8 – Діаграма друкованої плати системи

Перемички використовуються для створення електричних з'єднань між компонентами на макетній платі або між компонентами та мікроконтролером. Вони бувають різної довжини і можуть мати чоловічі або жіночі роз'єми.

Макетна плата - це інструмент прототипування, який використовується для побудови та тестування електронних схем без пайки. Вона дозволяє легко підключати та переконфігуровувати компоненти під час фази прототипування.

USB-кабель використовується для підключення мікроконтролера ESP8266 до комп'ютера для програмування та живлення. Він забезпечує інтерфейс для завантаження мікропрограми та спілкування з мікроконтролером.

Проста блокова діаграма системи замка дверей представлена на рисунку 3.9.

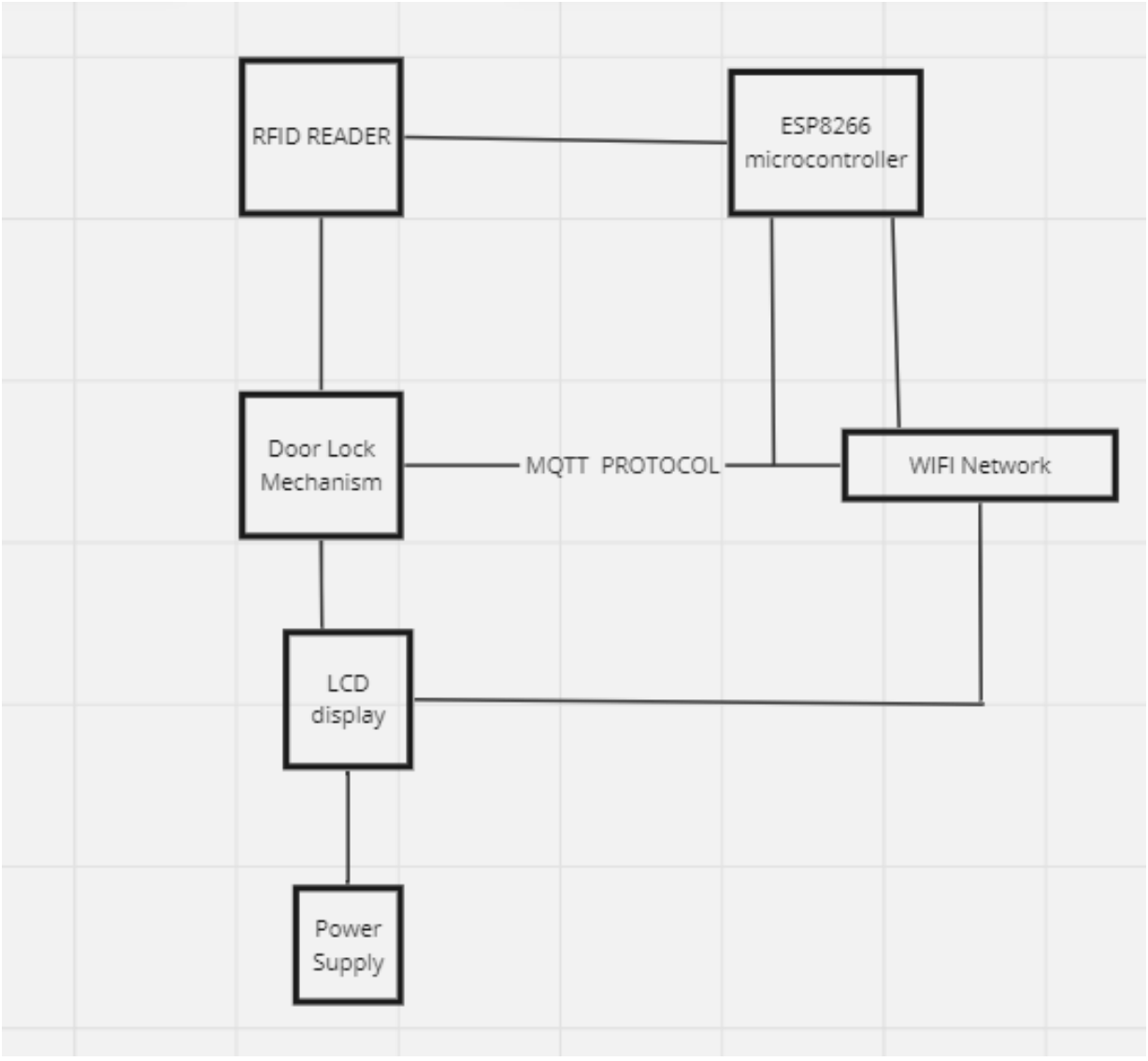


Рисунок 3.9 – Структурна схема системи

Ось короткий опис вищевказаної діаграми. RFID-зчитувач сканує RFID-теги/картки та надсилає дані до мікроконтролера ESP8266. Мікроконтролер є

центральним блоком, який отримує дані від RFID-зчитувача та обробляє їх, він також спілкується з мережею Wi-Fi та MQTT-брокером. ESP8266 використовує протокол MQTT для спілкування з сервером або хмарним сервісом для автентифікації та керування повідомленнями. Ця взаємодія є двосторонньою, тобто ESP8266 може надсилати та отримувати повідомлення. Механізм замка дверей керується ESP8266 на основі результату автентифікації. Якщо RFID-тег дійсний, ESP8266 надсилає сигнал для розблокування дверей. Wi-Fi забезпечує з'єднання для ESP8266 для спілкування за протоколом MQTT з віддаленим сервером. РК-дисплей відображає службові повідомлення, такі як «Доступ надано/відмовлено». Нарешті, блок живлення забезпечує всю систему необхідною напругою та струмом для роботи.

Код Arduino Uno для розробленої системи:

```
#include <SPI.h>
#include <MFRC522.h>
#include <Servo.h>
#include <Wire.h>
#include <LiquidCrystal_I2C.h>
#include <ESP8266WiFi.h>
#include <PubSubClient.h>
// Налаштування RFID
#define RST_PIN D3 // RST-пін для RC522
#define SS_PIN D8  // SDA-пін для RC522
MFRC522 mfrc522(SS_PIN, RST_PIN);
// Налаштування сервоприводу
Servo myServo;
#define SERVO_PIN D4
// Налаштування реле
#define RELAY_PIN D1
// Налаштування РК-дисплея
LiquidCrystal_I2C lcd(0x27, 16, 2);  // Адреса LCD I2C 0x27
```

```
// Дані для Wi-Fi
const char* ssid = "your_SSID";
const char* password = "your_PASSWORD";
// MQTT-брокер
const char* mqtt_server = "your_MQTT_BROKER_IP";
// MQTT-клієнт
WiFiClient espClient;
PubSubClient client(espClient);
// Прототипи функцій
void setupWiFi();
void reconnect();
void callback(char* topic, byte* payload, unsigned int length);
void setup() {
  // Налаштування послідовного порту
  Serial.begin(115200);
  // Налаштування RFID
  SPI.begin();         // Ініціалізація SPI шини
  mfrc522.PCD_Init(); // Ініціалізація MFRC522
  // Налаштування сервоприводу
  myServo.attach(SERVO_PIN);
  myServo.write(0);  // Початкове положення
  // Налаштування реле
  pinMode(RELAY_PIN, OUTPUT);
  digitalWrite(RELAY_PIN, LOW);  // Реле вимкнене
  // Налаштування LCD
  lcd.init();
  lcd.backlight();
  lcd.setCursor(0, 0);
  lcd.print("Ініціалізація...");
  // Налаштування Wi-Fi
```

```
  setupWiFi();
  // Налаштування MQTT
  client.setServer(mqtt_server, 1883);
  client.setCallback(callback);
  lcd.setCursor(0, 1);
  lcd.print("Готово");
}
void loop() {
  if (!client.connected()) {
    reconnect();
  }
  client.loop();
  // Шукаємо нові картки
  if (!mfrc522.PICC_IsNewCardPresent() || !mfrc522.PICC_ReadCardSerial()) {
    return;
  }
  String uid = "";
  for (byte i = 0; i < mfrc522.uid.size; i++) {
    uid += String(mfrc522.uid.uidByte[i] < 0x10 ? "0" : "");
    uid += String(mfrc522.uid.uidByte[i], HEX);
  }
  uid.toUpperCase();
  Serial.println("UID: " + uid);
  lcd.setCursor(0, 1);
  lcd.print("UID: " + uid);
  // Тут додайте свою логіку для перевірки UID
  // Наразі ми припускаємо, що будь-яка картка дійсна
  if (true) { // Замініть на реальну перевірку UID
    digitalWrite(RELAY_PIN, HIGH);  // Активувати реле (розблокування)
    myServo.write(90);  // Перемістити сервомотор у положення розблокування
```

```
            lcd.setCursor(0, 0);
            lcd.print("Доступ надано ");
            delay(5000);  // Тримати двері розблокованими протягом 5 секунд
            digitalWrite(RELAY_PIN, LOW);   // Деактивувати реле (блокування)
            myServo.write(0);      // Перемістити сервомотор назад у положення блокування
          } else {
            lcd.setCursor(0, 0);
            lcd.print("Доступ заборонено ");
          }
          // Зупинити PICC
          mfrc522.PICC_HaltA();
          mfrc522.PCD_StopCrypto1();
        }
        void setupWiFi() {
          delay(10);
          Serial.println();
          Serial.print("Підключення до ");
          Serial.println(ssid);
          WiFi.begin(ssid, password);
          while (WiFi.status() != WL_CONNECTED) {
            delay(500);
            Serial.print(".");
          }
          Serial.println("");
          Serial.println("WiFi підключено");
          Serial.println("IP адреса: ");
          Serial.println(WiFi.localIP());
        }
        void reconnect() {
```

```
  // Цикл, поки не буде відновлено з'єднання
  while (!client.connected()) {
    Serial.print("Спроба встановити з'єднання MQTT...");
    // Спроба встановити з'єднання
    if (client.connect("ESP8266Client")) {
      Serial.println("підключено");
      // Підписка на теми, якщо потрібно
    } else {
      Serial.print("не вдалося, rc=");
      Serial.print(client.state());
      Serial.println(" спробувати ще раз через 5 секунд");
      // Зачекати 5 секунд перед повторною спробою
      delay(5000);
    }
  }
}

void callback(char* topic, byte* payload, unsigned int length) {
  // Обробка повідомлень, отриманих від MQTT-брокера
  String message;
  for (unsigned int i = 0; i < length; i++) {
    message += (char)payload[i];
  }
  Serial.print("Повідомлення отримано [");
  Serial.print(topic);
  Serial.print("]: ");
  Serial.println(message);
}
```

3.4 Алгоритми функціонування системи

Алгоритми, що беруть участь у функціонуванні розумної системи замка дверей RFID з використанням мікроконтролера ESP8266:

– алгоритм виявлення RFID-мітки;

– алгоритм автентифікації;

– алгоритм блокування/розблокування дверей;

– алгоритм мережевої зв'язності;

– алгоритм користувацького інтерфейсу.

Алгоритм виявлення RFID-міток:

– ініціалізація: алгоритм починає з ініціалізації модуля RFID-зчитувача, підключеного до мікроконтролера ESP8266. Це передбачає налаштування необхідних контактів та параметрів для зв'язку з RFID-зчитувачем;

– опитування: після ініціалізації алгоритм входить в цикл, в якому він постійно опитує RFID-зчитувач на наявність виявлених RFID-міток. Частота опитування може бути відрегульована залежно від вимог системи та енергоспоживання;

– виявлення: коли RFID-зчитувач виявляє RFID-мітку в своїй зоні дії, він генерує електромагнітне поле, яке живить RFID-мітку. Потім мітка відповідає, передаючи свій унікальний ідентифікатор (UID) назад до RFID-зчитувача;

– зчитування UID: RFID-зчитувач захоплює UID, переданий RFID-міткою, і надсилає його до мікроконтролера ESP8266 для обробки. Цей UID зазвичай складається з ряду буквено-цифрових символів, які унікально ідентифікують RFID-мітку;

– розбір даних: після отримання UID від RFID-зчитувача, алгоритм розбирає дані, щоб витягти унікальний ідентифікатор. Це передбачає вилучення відповідної частини даних та перетворення її у формат, який можна порівняти з базою даних авторизованих RFID-міток;

– валідація: після того, як UID розпарсовано, алгоритм переходить до перевірки RFID-тегу щодо бази даних авторизованих тегів. Він порівнює

витягнутий UID зі списком попередньо зареєстрованих або авторизованих UID RFID-тегів, що зберігаються в системі;

– прийняття рішення: на основі результату перевірки алгоритм приймає рішення щодо контролю доступу. Якщо RFID-тег знайдено в базі даних авторизованих тегів, алгоритм переходить до розблокування дверей. В іншому випадку доступ заборонено, і двері залишаються заблокованими;

– зворотний зв'язок і ведення журналу: нарешті, алгоритм надає користувачеві зворотній зв'язок щодо результату автентифікації. Це може включати активацію візуальних або звукових індикаторів для позначення успішної або невдалої автентифікації. Крім того, система може вести журнал спроб автентифікації для аудиту та цілей безпеки;

– продовження циклу: після обробки виявлення та автентифікації RFID-тегу для одного тегу алгоритм повертається до етапу опитування, щоб продовжувати моніторинг наявності додаткових RFID-тегів. Це гарантує, що система залишається чутливою до кількох виявлень тегів протягом короткого проміжку часу.

Алгоритм автентифікації включає:

– пошук у базі даних: після виявлення RFID-тегу та вилучення його унікального ідентифікатора (UID) алгоритм автентифікації починає з запиту до бази даних авторизованих RFID-тегів, що зберігаються в мікроконтролері ESP8266 або зовнішньому пристрої зберігання (наприклад, EEPROM, SPI flash). База даних містить записи, що з'єднують кожен авторизований UID з відповідними дозволами доступу або інформацією про користувача;

– перевірка авторизації: алгоритм порівнює UID, витягнутий з RFID-мітки, з записами в базі даних, щоб визначити, чи є мітка авторизованою. Якщо UID збігається із записом у базі даних, алгоритм продовжує розглядати мітку як авторизовану для доступу. І навпаки, якщо в базі даних не знайдено збігу, алгоритм робить висновок, що мітка не авторизована.

– прийняття рішень: на основі результатів перевірки авторизації алгоритм автентифікації приймає рішення щодо контролю доступу. Якщо RFID-мітка

авторизована (тобто її UID знайдено в базі даних), алгоритм надає доступ, ініціюючи процес розблокування дверей. Якщо RFID-мітка не авторизована (тобто її UID не знайдено в базі даних), алгоритм відмовляє в доступі, і двері залишаються заблокованими;

– зворотний зв'язок та ведення журналу: алгоритм автентифікації надає користувачеві зворотний зв'язок, що вказує на результат процесу автентифікації. У разі успішної автентифікації система може активувати візуальні або звукові індикатори (наприклад, світлодіоди, дзвінок), щоб сигналізувати про надання доступу. І навпаки, у разі невдалої автентифікації система може надати зворотний зв'язок, що вказує на відмову в доступі, можливо, активуючи різні візуальні або звукові сигнали. Крім того, система веде журнал спроб автентифікації, записуючи такі деталі, як UID виявленої RFID-мітки, позначку часу та результат автентифікації. Це ведення журналу слугує для аудиту та безпеки, дозволяючи адміністраторам переглядати спроби доступу та виявляти будь-які спроби несанкціонованого доступу або порушення безпеки;

– обробка тайм-ауту: для підвищення безпеки алгоритм автентифікації може включати механізми тайм-ауту, щоб обмежити тривалість, протягом якої двері залишаються розблокованими після успішної автентифікації. Після надання доступу алгоритм може ініціювати таймер, автоматично блокуючи двері після заздалегідь визначеного часу (наприклад, кілька секунд або хвилин). Цей механізм тайм-ауту допомагає запобігти несанкціонованому доступу в разі, якщо двері випадково залишилися розблокованими або якщо несанкціонована особа отримала доступ до приміщення протягом розблокованого періоду.

Алгоритм блокування/розблокування дверей:

– керування сервомотором: добре, уявіть, що у нас є цей крутий сервомотор, приєднаний до нашого замка дверей. Це як маленька робоча рука, яка може повертатися і блокувати або розблоковувати двері. Наша задача - сказати цьому мотору, коли рухатися і скільки рухатися;

– блокування: коли хтось пред'являє RFID-мітку, і вона розпізнається як авторизована, ми хочемо надійно заблокувати двері. Отже, ми надсилаємо

сигнал до сервомотора, наказуючи йому обертатися таким чином, щоб заблокувати двері. Це як натискання кнопки блокування на ключі вашого автомобіля;

– розблокування: зараз, скажімо, хтось хоче потрапити до будинку. Ми перевіряємо, чи їхній RFID-тег авторизований. Якщо так, ми хочемо розблокувати двері. Тому ми надсилаємо інший сигнал до сервомотора, але цього разу наказуючи йому обертатися таким чином, щоб розблокувати двері, дозволяючи людині увійти;

– обробка тайм-ауту: після того, як ми розблокуємо двері, ми не хочемо, щоб вони залишалися розблокованими назавжди, чи не так? Це було б як залишити вхідні двері широко відкритими! Тому ми встановлюємо таймер. Після певного часу, якщо ніхто не відкриє двері, ми автоматично знову їх замикаємо. Це як невелике нагадування, щоб переконатися, що двері залишаються безпечними;

– зворотний зв'язок: нарешті, ми хочемо, щоб люди знали, що відбувається з дверима. Тому, коли ми їх замикаємо або розмикаємо, у нас можуть бути деякі вогні або звуки, щоб вказати, що відбувається. Це як двері кажуть: "Гей, я зараз зачинені!" або "Заходьте, я розблокований!".

Алгоритм мережевої зв'язності:

– підключення до Wi-Fi: перш за все, наш розумний дверний замок повинен підключитися до локальної мережі Wi-Fi, щоб він міг спілкуватися з іншими пристроями в нашому розумному будинку. Це як приєднання до Wi-Fi в кав'ярні, щоб ви могли переглядати Інтернет на своєму ноутбуці;

– налаштування мережевого протоколу: як тільки ми підключимося до Wi-Fi, нам потрібно вирішити, як ми будемо спілкуватися з іншими пристроями. Ми можемо використовувати протоколи, такі як TCP/IP або UDP. Це мови, які пристрої використовують для спілкування один з одним по мережі;

– обмін повідомленнями: тепер, коли все налаштовано, настав час почати надсилати та отримувати повідомлення. Коли хтось намагається розблокувати двері за допомогою свого RFID-тегу, ми надсилаємо повідомлення по мережі,

щоб повідомити інші пристрої про те, що відбувається. Це як відправити текстове повідомлення своєму другові, щоб повідомити його, що ви в дорозі;

– обробка помилок: іноді все йде не за планом. Можливо, з'єднання Wi-Fi перервалося або виникла проблема з мережею. У таких випадках нам потрібно мати певну обробку помилок. Це як мати резервний план, якщо ваш телефон розрядиться, коли ви будете на вулиці, і вам потрібно знайти дорогу додому без GPS;

– заходи безпеки: нам потрібно переконатися, що наші повідомлення безпечні, щоб ніхто не міг перехопити їх і розблокувати двері без дозволу. Це означає шифрування наших повідомлень і використання автентифікації, щоб переконатися, що лише авторизовані пристрої можуть керувати дверима;

– безперервний моніторинг: нарешті, нам потрібно стежити за мережевим з'єднанням. Ми не хочемо, щоб наш замок дверей раптово перестав працювати, тому що він втратив з'єднання з Wi-Fi. Тому ми налаштуємо моніторинг, щоб перевірити, чи все працює безперебійно. Це як періодично перевіряти свій телефон, щоб переконатися, що у вас все ще є сигнал.

Алгоритм користувацького інтерфейсу:

– ініціалізація: коли система запускається, ми ініціалізуємо компоненти користувацького інтерфейсу, будь то фізичні кнопки, сенсорний екран або їх поєднання. Це як увімкнути смартфон і побачити домашній екран, готовий до дії;

– навігація по меню: ми надаємо користувачам меню інтерфейсу для переходу до різних опцій і функцій. Уявіть це як перегляд додатків на телефоні або навігацію по налаштуваннях на цифрових пристроях;

– обробка вводу: нам потрібно обробляти ввід користувача, незалежно від того, чи натискають вони кнопки, торкаються сенсорного екрану чи використовують будь-який інший метод вводу. Коли користувач взаємодіє з інтерфейсом, ми виявляємо його ввід і реагуємо відповідно. Це як натискання на піктограму програми, щоб відкрити її на телефоні;

– відображення стану: ми відображаємо поточний стан системи замка дверей користувачам, показуючи, чи двері зачинені чи відчинені, а також будь-яку відповідну інформацію, наприклад, про останні спроби доступу. Це як погляд на телефон, щоб перевірити, чи є у вас нові сповіщення;

– налаштування: користувачі можуть налаштовувати параметри та налаштування через користувацький інтерфейс, наприклад, додавати або видаляти авторизовані RFID-теги, регулювати налаштування тайм-ауту або налаштовувати мережеві параметри. Це як зміна налаштувань у програмі, щоб персоналізувати свій досвід;

– зворотний зв'язок: ми надаємо користувачам зворотний зв'язок, щоб підтвердити їхні дії та тримати їх в курсі. Наприклад, коли вони натискають кнопку, щоб розблокувати двері, ми можемо відобразити повідомлення, що підтверджує, що двері тепер розблоковані. Це як отримання повідомлення про підтвердження після відправки тексту;

– обробка помилок: якщо щось пішло не так або виявлено недійсний ввід, ми обробляємо помилки граціозно, надаючи зворотній зв'язок користувачеві та керуючи його щодо виправлення проблеми. Це як отримати повідомлення про помилку, коли ви намагаєтеся зробити щось на своєму комп'ютері, що не дозволено;

– розгляди доступності: ми розробляємо інтерфейс користувача з урахуванням доступності, гарантуючи, що він простий у використанні для всіх користувачів, включаючи людей з інвалідністю або особливими потребами. Це як розробка веб-сайту або програми, щоб зробити її доступною для всіх, незалежно від їхніх можливостей;

– безперервне вдосконалення: ми постійно збираємо відгуки від користувачів та ітеруємо інтерфейс користувача, щоб покращити зручність використання та досвід користувачів з часом. Це як оновлення програми на вашому телефоні, щоб додати нові функції або виправляти помилки на основі відгуків користувачів.

3.5 Інтерфейс програмно-технічного засобу керування дверним замком на основі мікроконтролера ESP8266

Інтерфейс програмно-технічного засобу керування дверним замком на основі мікроконтролера ESP8266 включає:

– головне меню: коли ви вперше відкриєте програмний інструмент, ви побачите екран головного меню. Це як головний екран вашого телефону, де ви можете отримати доступ до різних програм;

– опції блокування/розблокування: З головного меню ви можете вибрати опції для блокування або розблокування дверей. Це як натискання кнопок на пульті дистанційного керування для блокування або розблокування автомобіля;

– керування RFID-тегами: Також є розділ, де ви можете керувати RFID-тегами. Ви можете додавати нові теги, яким дозволено розблокувати двері, або видаляти теги, які ви більше не хочете мати доступ. Це як керування контактами в телефонній книзі;

– налаштування конфігурації: У меню налаштувань ви можете налаштувати різні параметри, наприклад, тривалість тайм-ауту для автоматичного переблокування дверей після їх розблокування. Це як налаштування параметрів на комп'ютері для налаштування його поведінки;

– відображення статусу: На головному екрані ви побачите поточний стан системи блокування дверей. Він покаже, чи заблоковані двері чи розблоковані, щоб ви знали, що відбувається з першого погляду. Це як перевірка виджету погоди на телефоні, щоб дізнатися, чи буде дощ;

– візуальний зворотний зв'язок: Коли ви натискаєте кнопку для блокування або розблокування дверей, ви отримаєте візуальний зворотний зв'язок на екрані, щоб підтвердити, що ваша дія була успішною. Він може показати галочку або значок замка, щоб повідомити вам, що двері тепер заблоковані або розблоковані. Це як отримання смайлика «великий палець вгору», коли ви надсилаєте повідомлення на телефоні;

– проста навігація: Інтерфейс розроблений для простоти навігації за допомогою простих кнопок і меню. Це як використання програми на вашому телефоні, яка проста та інтуїтивно зрозуміла у використанні, навіть якщо ви не фахівець з технологій;

– розділ допомоги: Якщо ви коли-небудь застрягли або вам потрібна додаткова інформація, є розділ допомоги, де ви можете знайти відповіді на поширені запитання або поради щодо усунення несправностей. Це як читання інструкції з експлуатації, яка поставляється з новим гаджетом, щоб розібратися, як його використовувати.

3.6 Вартість матеріалів

Вартість матеріалів, запропонованих для системи розумних RFID замків дверей. Оцінка вартості матеріалів наведена в таблиці 3.1

Таблиця 3.1 – Вартість матеріалів

Назва	Вартість
Мікроконтролер ESP8266	$30
Модуль зчитувача RFID	$25
Сервомотор	$15
RFID-мітки	$20
Модуль Wi-Fi	$3
Блок живлення	$20
Корпус	$15

3.7 Висновки

Система розумних RFID замків дверей – це як високотехнологічний охоронець нашого будинку. У її основі лежить мікроконтролер ESP8266, щось на

зразок мозку, який керує всім. Він підключається до інших важливих частин, таких як зчитувач RFID, який зчитує спеціальні картки або мітки, і сервомотор, який фізично блокує та розблоковує двері.

Всі ці деталі збираються в один компактний пакет всередині корпусу, що нагадує захисну оболонку. Вона зберігає все в безпеці та організовано, як коли ви складаєте іграшки в коробку після гри.

Ми розміщуємо всі ці деталі на макетній платі, яка є своєрідним майданчиком для електронних компонентів. За допомогою джмперних проводів ми з'єднуємо все з мікроконтролером ESP8266, переконуючись, що кожна деталь знає, що робити і куди надсилати свої сигнали. Це схоже на з'єднання точок, щоб завершити малюнок.

Система працює на основі набору інструкцій, що вказують системі, що робити. Ці алгоритми гарантують, що система може виявити, коли поблизу знаходиться RFID-тег, перевірити, чи йому дозволено розблокувати двері, а потім фактично розблокувати їх, якщо все в порядку. Це схоже на дотримання рецепту для випічки торта – ви повинні робити все в правильному порядку, щоб отримати бажаний результат.

ВИСНОВОК

Розробка програмного та технічного інструменту для керування розумною системою замка дверей на основі RFID, використовуючи мікроконтролер ESP8266 в середовищі розумного будинку, була захоплюючою та винагороджуючою подорожжю. Цей проект був спрямований на задоволення зростаючого попиту на безпечні та зручні рішення для контролю доступу в сучасних розумних будинках, використовуючи можливості технології IoT.

Завдяки широким дослідженням, прототипуванню та тестуванню, ми успішно розробили та реалізували надійну систему замка дверей, яка здатна безпечно автентифікувати користувачів на основі RFID-тегів. Інтеграція мікроконтролера ESP8266 забезпечила надійну платформу для обробки даних, керування механізмом замка дверей та спілкування з мережею розумного будинку.

Фізична конфігурація системи включала ретельну збірку та підключення різних компонентів, включаючи мікроконтролер ESP8266, модуль RFID-читача, сервомотор та блок живлення. Використання макетної плати сприяло швидкому прототипуванню та тестуванню, забезпечуючи правильну конфігурацію та функціональність апаратних компонентів системи.

Крім того, розробка алгоритмів відіграла вирішальну роль у функціонуванні системи, забезпечуючи ключові процеси, такі як виявлення RFID-тегів, автентифікація та блокування/розблокування дверей. Ці алгоритми були ретельно розроблені та реалізовані для забезпечення ефективних та безпечних операцій контролю доступу, підвищуючи загальну надійність та зручність використання системи.

Протягом процесу розробки виникло декілька викликів, включаючи проблеми сумісності обладнання, оптимізацію алгоритмів та інтеграцію з існуючою інфраструктурою розумного дому. Однак завдяки наполегливості та співпраці ці виклики були ефективно вирішені, що призвело до успішного завершення проекту.

Дивлячись у майбутнє, існує значний потенціал для подальших удосконалень та вдосконалень системи розумного RFID замка. Майбутні дослідження можуть зосередитися на покращенні масштабованості системи, взаємодії з іншими пристроями розумного дому та інтеграції розширених функцій безпеки, таких як біометрична автентифікація.

На завершення, розробка програмного та технічного інструменту для керування системою розумного RFID замка є значним внеском у сферу автоматизації розумного дому. Цей проект продемонстрував доцільність та практичність використання технології IoT для підвищення безпеки та зручності в житлових приміщеннях, прокладаючи шлях для майбутніх досягнень у цій захоплюючій галузі.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

1. Arduino. (n.d.). ESP8266 Core Documentation. Retrieved from https://arduino-esp8266.readthedocs.io/en/latest/

2. Espressif Systems. (n.d.). ESP8266 Resources - Downloads, Tutorials, and Datasheets.Retrieved from https://www.espressif.com/en/products/socs/esp8266/resources

3. RFID Reader/Writer Modules & Cards. (n.d.). Adafruit Industries. Retrieved from https://www.adafruit.com/category/63

4. Servo Motor Basics & Pinout. (n.d.). Adafruit Industries. Retrieved from https://learn.adafruit.com/adafruit-arduino-lesson-14-servo-motors/overview

5. Wi-Fi Connection with ESP8266 – ESP8266 Arduino Core. (n.d.). Random Nerd Tutorials. Retrieved from https://randomnerdtutorials.com/esp8266-wi-fi-tutorial/

6. Kaur S., Garg K., & Goel M. (2019). Design of RFID Based Security System Using Arduino. *International Journal of Engineering Research & Technology (IJERT*), 8(5), Pp. 307-310.

7. Alam M. J., & Alam M. M. (2016). Design and Development of Low Cost RFID Security System. *International Journal of Engineering and Technical Research (IJETR),* 4(5), Pp. 71-74.

8. Shanmugasundaram K., Swaminathan V., Vignesh V., Vinothini M., & Vigneshwaran, R. (2019). IoT Based Smart Door Lock System Using RFID and GSM. International Journal of Pure and Applied Mathematics, 120(6), Pp. 5881-5889.

9. Prakash, K., Yadav, A., & Verma, K. (2018). Design and Implementation of RFID Based Door Lock System. *International Journal of Engineering and Techniques,* 4(5), Pp. 149-153.

10. Khan S. U., & Sultan A. (2019). IoT Based Home Automation Using ESP8266. *In Proceedings of the 3rd International Conference on Internet of Things (IoT) in Social, Mobile, Analytics and Cloud*, Pp. 1-5.

11. Fritzing, URL: https://fritzing.org/

12. Yadin A. Computer Systems Architecture, Chapman and Hall, *CRC*, 2016. 467 p.

13. Null L., Lobur Y. Essentials of Computer Organization and Architecture, *Jones & Bartlett Learning*; 5th edition, 2018. – 744 p.

14. Poliakov, M., Larionova, T. Control Systems with programmable logic controllers, Remote and virtual tools in engineering: *textbook, general editorship* Dr.Ing.Karsten Henke. Zaporizhzhya: Dike Pole, 2016. 250 p.

15. Barrett S.F. Microchip AVR® Microcontroller Primer: Programming and Interfacing. *Morgan & Claypool Publishers*, 2019. 374 p.

16. Papazoglou P. M. An Educational Guide to the AVR Microcontroller Programming: AVR Programming::Demystified (Assembly Language). *CreateSpace Independent Publishing Platform*, 2018. 274 p.

17. Nicheporuk A., Nicheporuk A., Sachenko A., A System for Detecting Anomalies and Identifying Smart Home Devices Using Collective Communication, *CEUR-WS*. Vol. 2853. Pp. 386-397.

18. Molly Edmonds & Nathan Chandler, How Smart Homes Work, URL: https://home.howstuffworks.com/smart-home.htm

19. Bhattacharjee S. Practical Industrial Internet of Things Security. Birmingham, United Kingdom: Packt Publishing Ltd 2018. 324 p.

20. Kumar V., R. Chawda Research paper on smart home, *International Journal of Engineering Applied Sciences and Technology*, 2020. Vol. 5. Issue 3. pp. 530-532.

21. Atzori L., Iera A., and Morabito G., The Internet of Things: A Survey, *Computer Networks*. Vol. 54. no 15. 2010. Pp. 2787–2805.

22. Cho M.E., Kim, M.J. Smart Homes Supporting the Wellness of One or Two-Person Households, *Sensors*. 2022. 22, 7816.

23. Yanagida K. Ueda Y., Go K., Takahashi K., Hayakawa S., Yamazaki K., Structured Scenario-Based Design Method, *In Proceedings of the 1st International Conference on Human Centered Design*, San Diego, CA, USA, 19–24 July 2009, pp. 374–380

24. "ESP8266 Overview". Espressif Systems. Retrieved 2017-10-02.

25. Brian Benchoff (August 26, 2014). "New Chip Alert: The ESP8266 WiFi Module (It's $5)". Hackaday. Retrieved 2015-06-24.

26. Brian Benchoff (September 6, 2014). "The Current State of ESP8266 Development". Hackaday. Retrieved 2015-06-24.

27. "Espressif Announces ESP8285 Wi-Fi Chip for Wearable Devices". Espressif Systems. Mar 9, 2016. Archived from the original on 2016-07-25. Retrieved 2016-07-10.

28. "ESP8266 Non-OS SDK API Reference, Chapter 2.4. System Performance" (PDF). espressif.com. Espressif Systems. The flash mode and frequency directly influence the code execution speed. Setting the flash to a higher frequency and QIO mode may produce the best results in terms of performance, though it costs in terms of power consumption.

29. "ESP8266 Non-OS SDK API Reference" (PDF). espressif.com. Espressif Systems. Success varies chip to chip.[citation needed]

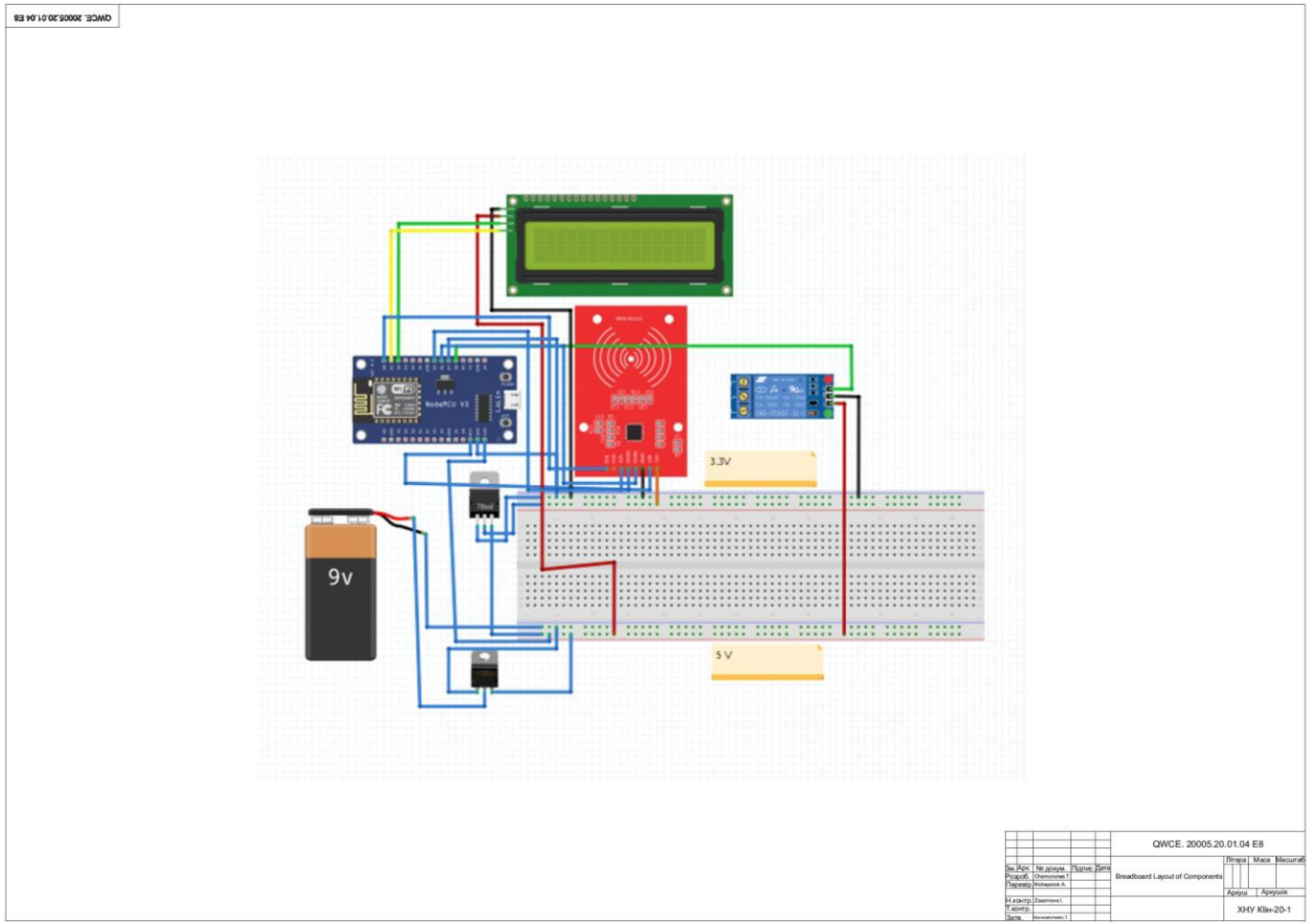
30. Kishita Y., Mizuno Y., Fukushige S., Umeda Y. Scenario structuring methodology for computer-aided scenario design: An application to envisioning sustainable futures, *Technol. Forecast. Soc. Chang*. 2020. 160. 120207

31. Rhee J.H., Ma J.H., Seo J., Cha S.H., Review of applications and user perceptions of smart home technology for health and environmental monitoring, *J. Comput. Des. Eng.* No 9. 2022, pp. 857–889.

32. Tiwari P., Garg V., Agrawal R. Changing World: Smart Homes Review and Future. *In Smart IoT for Research and Industry*, Springer International Publishing: Cham, Germany, 2022, Pp. 145-160.

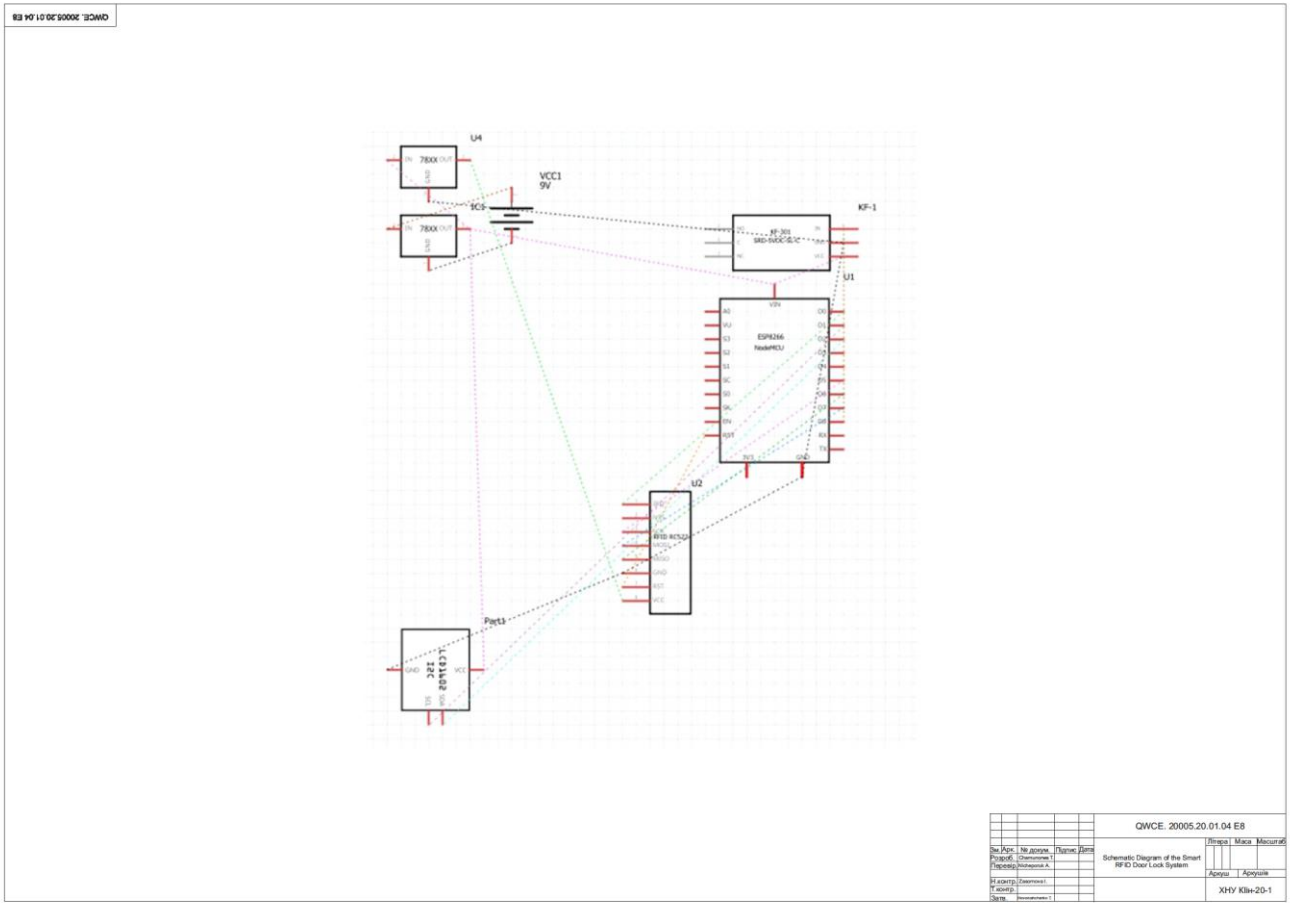
Додаток А

Копія креслення «Монтажна схема»



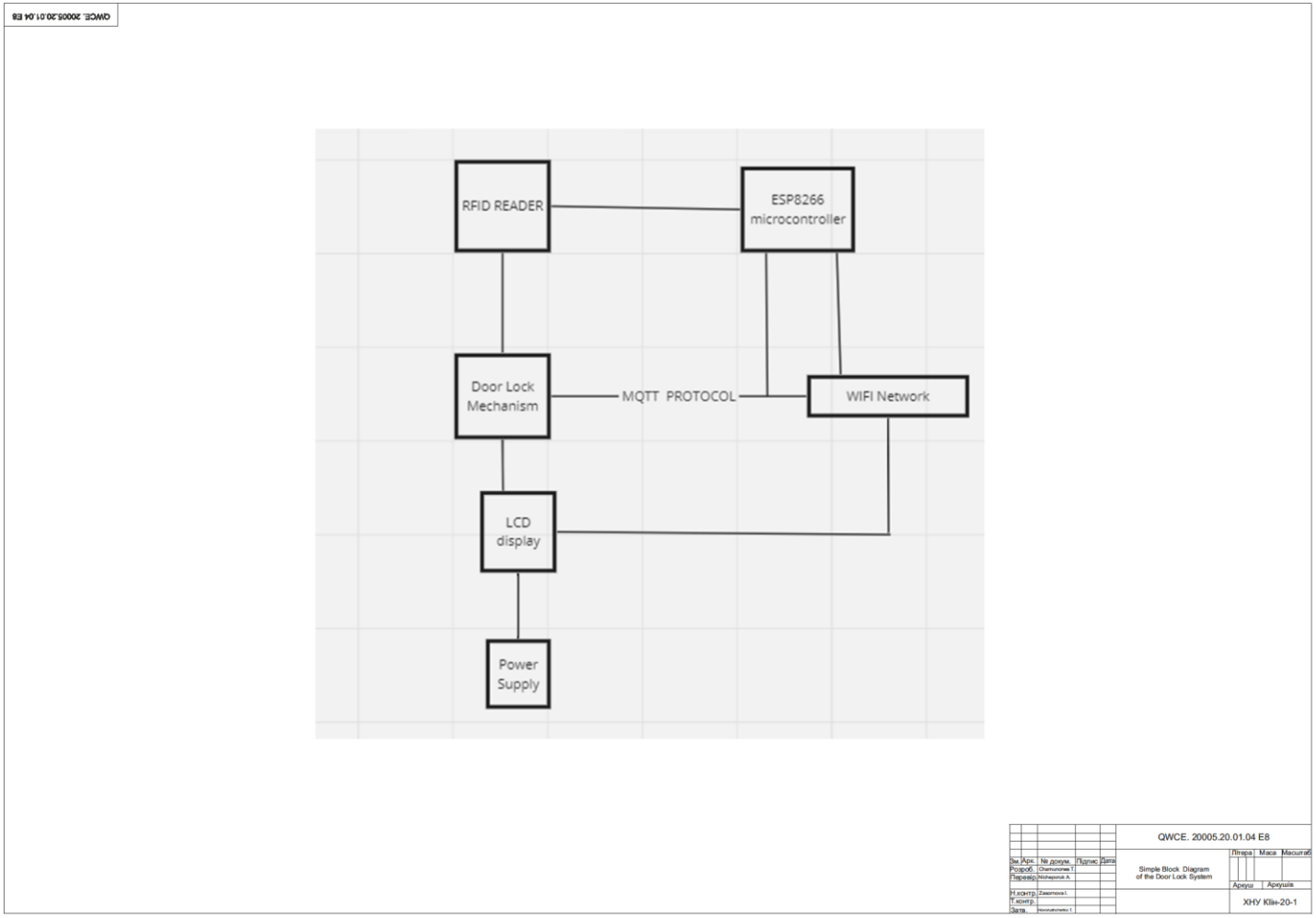
Додаток Б

Копія креслення «Схема електрична принципова»



Додаток В

Копія креслення «Структурна схема»



UNICHECK
by Turnitin

Ім'я користувача:
Кафедра KI

ID перевірки:
1016344942

Дата перевірки:
10.06.2024 23:24:42 EEST

Тип перевірки:
Doc vs Internet + Library

Дата звіту:
11.06.2024 20:23:09 EEST

ID користувача:
100005591

Назва документа: Chamunorwa_Software and Technical Tool for controlling the door lock based on the ESP8266 microcontro..

Кількість сторінок: 62 **Кількість слів:** 13486 **Кількість символів:** 90501 **Розмір файлу:** 2.62 MB **ID файлу:** 1016146606

7.7%
Схожість

Найбільша схожість: 1.35% з джерелом з Бібліотеки (ID файлу: 1016146613)

6.68% Джерела з Інтернету	448	Сторінка 64
2.4% Джерела з Бібліотеки	12	Сторінка 69

2.94% Цитат

Цитати	11	Сторінка 70
Посилання	1	Сторінка 70

0%
Вилучень

Немає вилучених джерел

UNICHECK
by Turnitin

Ім'я користувача:
Кафедра КІ

ID перевірки:
1016344958

Дата перевірки:
10.06.2024 23:24:42 EEST

Тип перевірки:
Doc vs Internet + Library

Дата звіту:
11.06.2024 20:25:11 EEST

ID користувача:
100005591

Назва документа: Чамунорва_Програмно-технічний засіб керування дверним замком на основі мікроконтрол...

Кількість сторінок: 70 **Кількість слів:** 12090 **Кількість символів:** 94570 **Розмір файлу:** 2.63 MB **ID файлу:** 1016146613

4.1%
Схожість

Найбільша схожість: 2.12% з джерелом з Бібліотеки (ID файлу: 1016146606)

3.26% Джерела з Інтернету	353	Сторінка 72
3.42% Джерела з Бібліотеки	112	Сторінка 75

0.04% Цитат

Цитати	5	Сторінка 76
Посилання	1	Сторінка 76

0%
Вилучень

Немає вилучених джерел

Tue Jun 11 19:43:07 EEST 2024, Медзатий Дмитро Миколайович, Хмельницький національний університет, ХНУ

Anti-Plagiarism v-15.257

Максимальне співпадіння з одним документом 4.0%

Словники перевірки: en_US, ru_RU, ua_UA. **Помилок в документах: 12%**

	Документ		Сумарний збіг по Базі Даних	
ID: 129785 Назва: БКР Програмно-технічний засіб керування дверним замком на основі мікроконтролера ESP8266 Додано в БД: 2024-06-11 Автора: Чамунорва Т. Керівники: А.О. Нічепорук Консультанти: Опоненти:	Символи	Лексеми	Символи	Лексеми
	81820	665	3767 (5%)	49 (7%)

Джерело плагіату

ID	Опис	Наявність плагіату в документі	
		Символи	Лексеми

Tue Jun 11 19:37:57 EEST 2024, Медзатий Дмитро Миколайович, Хмельницький національний університет, ХНУ

Anti-Plagiarism v-15.257

Максимальне співпадіння з одним документом 2.0%

Словники перевірки: en_US, ru_RU, ua_UA. **Помилок в документах: 28%**

ID: 129781 Назва: БКР Software and Technical Tool for controlling the door lock based on the ESP8266 microcontroller Додано в БД: 2024-06-11 Автора: Chamunorwa.T. Керівники: Nicheporuk A.O. Консультанти: Опоненти:	Документ		Сумарний збіг по Базі Даних	
	Символи	Лексеми	Символи	Лексеми
	77026	634	2387 (3%)	27 (4%)

Джерело плагіату

ID	Опис	Наявність плагіату в документі	
		Символи	Лексеми

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

РЕЦЕНЗІЯ НА КВАЛІФІКАЦІЙНУ РОБОТУ

Дипломник: Чамунорва Тінаше

Тема: Програмно-технічний засіб керування дверним замком на основі мікроконтролера ESP8266

Спеціальність: 123 «Комп'ютерна інженерія»

Обсяг дипломної роботи:

Кількість листів креслень 3; кількість сторінок записки 66

1. Короткий зміст роботи та прийнятих рішень У роботі було спроєктовано програмно-технічний засіб керування дверним замком на основі мікроконтролера ESP8266

2. Висновок про відповідність роботи дипломному завданню Дипломний проект відповідає виданому завданню

3. Характеристика виконання кожного розділу, ступінь використання останніх досягнень науки і техніки і передових методів роботи: У першому розділі проведено відомих засобів та систем. У другому розділі виконано аналіз та вибір елементної бази для проєктованого програмно-технічного засобу. У третьому розділі виконано реалізацію програмно-технічного засобу керування дверним замком на основі мікроконтролера ESP8266.

4. Позитивні сторони роботи: Спроєктовано програмно-технічний засіб керування дверним замком на основі мікроконтролера ESP8266

5. Негативні сторони роботи: У пропонованій системі не розглянуто питання керування та збереження RFID міток.

6. Оцінка графічного оформлення та пояснювальної записки роботи: пояснювальна записка та листи креслення виконані згідно діючих вимог

7. Відгук про роботу в цілому: В загальному робота виконана на задовільному рівні.

8. Інші зауваження: –

9. Оцінка дипломної роботи:

Розглянувши позитивні та негативні сторони представленої дипломної роботи вважаю, що робота заслуговує оцінки «задовільно» 3,50 (D)

Рецензент (прізвище, ім'я, по батькові, посада, місце роботи) Бахтіяр Руслан Олександрович, доц. КНІ

"12" 06 2024р.

РІШЕННЯ ЕКСПЕРТНОЇ КОМІСІЇ

КАФЕДРИ КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ ТА ІНФОРМАЦІЙНИХ СИСТЕМ

ПРО ДОПУСК КВАЛІФІКАЦІЙНОЇ РОБОТИ ДО ЗАХИСТУ

Підтверджуємо ознайомлення з результатом звіту подібності щодо роботи, генерованого системою виявлення текстових збігів/ідентичності/схожості:

Назва: Програмно-технічний засіб керування дверним замком на основі мікроконтролера ESP8266

Автор: Чамунорва Тінаше

Спеціальність: 123 – Компютерна інженерія

Освітня програма: освітньо-професійна

Науковий керівник: Нічепоруку Андрій Олександрович, к.т.н, доцент

Після аналізу звіту подібності зроблено такий висновок:

№	Висновок	Позначка про відповідність
1	Запозичення, виявлені в роботі, є законними і не є плагіатом. Робота приймається до захисту.	відповідає
2	Виявлені запозичення не є плагіатом, розміщені в розділах, які не описують безпосередньо авторське дослідження, але кількість цитат перевищує обсяг, виправданий поставленою метою роботи Робота приймається до захисту, але має бути відкоригована. Відкоригований варіант має бути поданий на кафедру за 2 дні до захисту, разом із заявою щодо самостійності виконання письмової роботи та ідентичності друкованої та електронної версії роботи	
3	Виявлені запозичення не є плагіатом, але частково розміщені в розділах, які описують безпосередньо авторське дослідження, а кількість цитат перевищує обсяг, виправданий поставленою метою роботи. В зв'язку з цим мета роботи та поставлені завдання не були досягнені. Робота може бути допущена до захисту (наступного року) після того як буде відкоригована та допрацьована і успішно пройде повторну перевірку на академічний плагіат.	
4	Робота містить навмисні текстові спотворення, передбачувані спроби укриття запозичень або інші прояви академічного плагіату. Робота містить фабрикацію або фальсифікацію даних. Робота не допускається до захисту.	

Підтвердження:

Запозичення, виявлені в роботі, є законними і не є плагіатом, оскільки:

1) запозичення розміщені в розділі аналізу існуючих аналогів та відомих рішень, які не описують безпосередньо авторське дослідження і не стосуються результатів роботи;
2) усі запозичення фрагментарні, або мають належним чином оформленні посилання;

Сумарний обсяг всіх запозичень, визначений системою виявлення збігів/ ідентичності/схожості Unicheck для кваліфікаційної роботи на українській мові складає 4,1% і адресується до 465 першоджерела, а на англійській мові 7,7 і адресується до 460 першоджерел; та системою Anti-Plagiarism для кваліфікаційної роботи на українській мові складає 4%, а на англійській мові 2%, що, з урахуванням наведених обґрунтувань, відповідає характеру наукового дослідження і свідчить на користь кваліфікаційної роботи.

Керівник роботи _____ А.О. Нічепорук

Гарант ОП _____ А.О. Нічепорук

Завідувач кафедри КІІС _____ Т. О. Говорущенко

Завідувачу кафедри КІІС
д-р.техн.наук, проф. Говорущенко Т. О.

Чамунорва Тінаше
ПІБ здобувача вищої освіти

ФІТ, 4 курсу, групи КІін-20-1

ЗАЯВА

З правилами чинного Положення «Про дотримання академічної доброчесності в Хмельницькому національному університеті» від 26.09.2020 (зі змінами від 26.11.2020), згідно з яким виявлення плагіату є підставою для відмови в допуску кваліфікаційної роботи до захисту та застосування заходів дисциплінарної та академічної відповідальності, ознайомлений (а). Про використання програмно-технічних засобів для перевірки кваліфікаційних робіт здобувачів вищої освіти на плагіатоповіщений (а) та надаю свою згоду на обробку та збереження університетом моєї роботи в інституційному репозитарії університету.

Також надаю університету право на передачу моєї роботи для обробки та збереження в базах даних програмно-технічних засобів (Unicheck та Anti-Plagiarism) та використання роботи для виявлення плагіату в інших роботах, які перевіряються програмно-технічними засобами та користувачами, що мають доступ до цих програмно-технічних засобів, виключно в обмежених цілях для виявлення плагіату в текстах робіт.

Робота для перевірки університетом надається в друкованому та електронному варіанті. Електронна версія моєї роботи збігається (ідентична) з друкованою.

10.06.2024
дата

підпис