CONSTRUCTION OF A CONTACTLESS KEY CARD ACCESS CONTROL SYSTEM USING A RADIO FREQUENCY IDENTIFICATION (RFID) SCANNER AND ARDUINO

BY

Ikafimeh Samuel Igiegba

LSC1706051

(PHYSICS AND ELECTRONICS TECHNIQUES)

DEPARTMENT OF SCIENCE LABORATORY TECHNOLOGY

FACULTY OF LIFE SCIENCES

UNIVERSITY OF BENIN,

BENIN CITY.

MAY, 2024.

CONSTRUCTION OF A CONTACTLESS KEY CARD ACCESS CONTROL SYSTEM USING A RADIO FREQUENCY IDENTIFICATION (RFID) SCANNER AND ARDUINO

BY

Ikafimeh Samuel Igiegba

LSC1706051

A PROJECT WORK SUBMITTED TO THE DEPARTMENT OF SCIENCE LABORATORY TECHNOLOGY, FACULTY OF LIFE SCIENCE, UNIVERSITY OF BENIN, BENIN CITY, IN PARTIAL FULFILLMENT OF THE REQUIREMENT FOR THE AWARD OF BACHELOR OF SCIENCE DEGREE (B.SC) IN SCIENCE LABORATORY TECHNOLOGY (PHYSICS/ELECTRONICS TECHNIQUES).

MAY, 2024

CERTIFICATION

This is to certify that this project work was carried out by Samuel Igiegba Ikafimeh with matriculation number, LSC1706051 of the department of Science Laboratory Technology (Physics/Electronics Techniques), Faculty of Life Sciences, University of Benin, Benin City.

_____ _____

ENGR. K.O OJO **Date**

(Project Supervisor)

_____ _____

MRS. OMOZUA P. O. **Date**

(Project Coordinator)

_____ _____

PROF E.O OSHOMOH **Date**

(Head of Department)

_____ _____

(External Examiner) **Date**

DEDICATION

I dedicate this work to God Almighty, my parents, my colleagues, my supervisor, and the rest of my family for the inspiration, encouragement and support given towards the successful completion of this work.

ACKNOWLEDGMENTS

I wish to express my heartfelt gratitude to the University of Benin and its Management for providing me with the invaluable platform to pursue my academic journey. I extend my sincere appreciation to the Department of Science Laboratory Technology for the exceptional opportunity to engage in this transformative project.

My deepest thanks go to the dedicated lecturers of Physics/Electronics Techniques, whose knowledge and guidance have been instrumental in shaping my academic path.

I am profoundly grateful to my supervisor, Engr. Ojo Kennedy Odu, for his unwavering support, insightful contributions, and the countless hours devoted to mentoring me throughout this project. Your dedication has been invaluable. To my cherished family, my parents,I offer my most sincere and heartfelt gratitude for the support and encouragement that sustained me throughout the duration of this project. Your belief in me has been my driving force.

I also extend my appreciation to my colleagues and friends, Maryjane, Azeez, OZ, Blessed, Martins and others for their counsel, motivation, and prayers and support during the challenging journey of working on this paper. I also extend my gratitude to my fellow PET students for their encouragement throughout my journey.

Finally, I acknowledge that all achievements are by the grace of the Almighty. To God be the glory.

TABLE OF CONTENT

LIST OF ABBREVIATIONS

AC = Alternating Current

DC = Direct Current

GND = Ground

IDE = Integrated Development Environment

RFID = Radio Frequency Identification

LED = Light Emitting Diode

LCD = Liquid Crystal Display

MC = Micro Controller

UID = Unique Identification

LIST OF FIGURES

LIST OF TABLES

ABSTRACT

Security is needed more and becoming more important in today's world. Sometimes, physical security and access control is not always the best solution, especially in instances with large crowd or systems that requires round-the-clock security. For this reason, an Arduino-based access control system using RFID (Radio Frequency Identification Technology) was created to provide security and access control to buildings and physical spaces, and this eliminated the need for physical security at all times. The device makes use of RFID technology and Arduino to complete its work. RFID (Radio Frequency Identification) is a communication technology commonly known as electronic tags. Radio transmissions can identify targets and transfer data without direct communication. Advancements in radio frequency recognition technology have led to its widespread usage in identity documents, defence, and industrial control. When the RFID scanner recognizes a tag, it checks its UID to the stored database to ensure accuracy. Access is granted if the captured user's UID matches a previously saved UID; otherwise, access is denied.

CHAPTER ONE

INTRODUCTION

1.1 BACKGROUND OF STUDY

Nowadays, the primary concern is security and managing people in certain physical spaces. Physical security is not always the ideal solution. Implementing an access control system aims to limit physical access to physical infrastructures and spaces. It is a means of digitally restricting access to increase safety. It will track who enters specific spaces and when. (Dhanalakshmi *et al*., 2021). Access control determines who, when, and why access should be provided to a space and is essential for safeguarding structures and services. Access control systems protect essential infrastructure, spaces, properties, and assets which preserves the privacy, reliability, and accessibility of resources (Simukali, 2019).

This leads to the implementation and utilization of digital access control systems with secure authentication and authorization capabilities in buildings to meet security demands. The utilization of a contactless key card for entry and exit (access) authorization has eliminated the challenge of physical security involving padlocks or physical security personnel. For this reason, many modern organizations employ smart doors with access card scanners, primarily using RFID cards (Khabarlak and Koriashkina, 2021).

The RFID scanner is the storage device in this security system which stores all identification, authorization and authentication information about all users to be granted access to the controlled system and also scans the card that will be granted or rejected access. Arduino boards can receive inputs such as button presses, login credentials, and other data and convert them into outputs such as motion activation, and LED changing. The board accepts and transmits several sets of commands to the microcontroller (Dhanalakshmi *et al*., 2021). Both the RFID sensor and

the Arduino board are significantly key components in digital contactless key card access control systems as they are responsible for storing user information, retrieving user information, comparing user information, granting or restricting access to hardware components and other security measures needed to be taken. Basically, both the RFID scanner and the Arduino board control the whole access security system.

The main process is checking card UID. If the card UID is registered in the database and is allowed access after checking, the security system is unlocked. If granted access, the green LED is ON, which permits user access. If the UID card is false, invalid or is rejected access, the red LED is ON, the security system is locked and the buzzer is activated (Hlaing and Lwin, 2019). The successful development of this access control security system will enable infrastructures to have a reliable unmanned security system and will enable easy, efficient and reliable identification and authorization for users who are trying to access the infrastructure.

1.2 AIM

This project aims to design and construct a contactless key card access control system using a radio frequency identification (RFID) scanner and Arduino.

1.3 OBJECTIVE

The specific objectives of this study are as follows:

1. Design and construct a key card access control security system using RFID technology
2. Implement a contactless access control and security feature

1.4 SIGNIFICANCE OF THE STUDY

By using a contactless key card for easy and reliable identification and authorization, infrastructures can take advantage of proximity sensor technology which is relatively cheap, easy to install and easy to use for access control and security systems. The fast and automatic identification and authorization provide a security solution which does not include physical security confrontation, and this makes the entire system fast, reliable, and efficient, benefiting both the user and the infrastructure to be protected.

1.5 LIMITATIONS OF THE PROJECT

The limitations are:

1. The design and construction of this system will be based on an external power supply, and therefore power has to be supplied to the system at all times to ensure that the system works at all times. Alternatively, a battery can be used to power the system, but a battery is less reliable and will need to be charged or replaced at intervals.
2. The system grants access based on card UID. This means that another person can gain access to the system as long as the person has a registered card.

1.6 SCOPE OF THE PROJECT

In this project, the diagram will range from simple block diagrams to complex circuit diagrams which will comprise mostly of common electrical symbols. Some of the diagrams that will feature in this report will be used as the main block on which certain parameters will be explained.

CHAPTER TWO

LITERATURE REVIEW

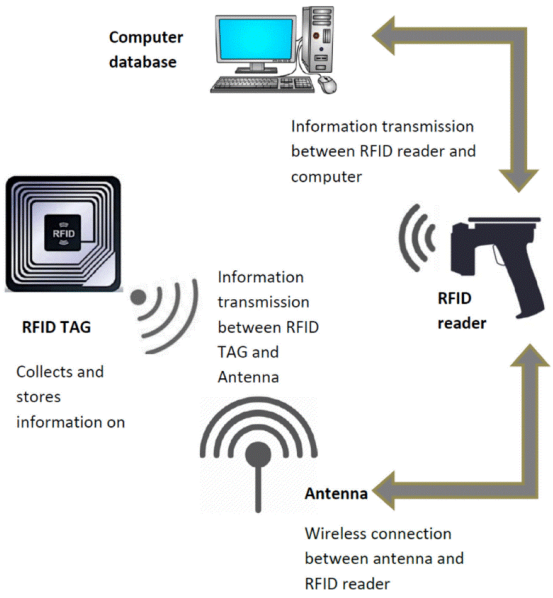
2.1 RADIO FREQUENCY IDENTIFICATION (RFID)

Radio Frequency Identification (RFID) is a common form of contactless or wireless technology, and several industries around the world employ this technology for various purposes. These include tollgate systems, book-tracking systems in libraries, supply chain management, and access control systems (Nedelkovski, 2017). Umar *et al*. (2014) were the first proponents of a security system that was based on RFID and access control. Their proposal was to have this system installed in the hostels at Punjab University.

The Radio Frequency Identification (RFID) system is a technology that combines biometrics to create a security system. RFID systems are commonly used for doors that require clearance to enter or for safes. It works by reading specific key cards that have been prearranged to be recognized by the system, commonly known as a Unique Identifier (UID) – it is a key card that doesn't make contact with the RFID system. Since owners of the UID already have their information in the database of the system, the RFID will give the person access – the lock on the door or safe will open. scans the tag or ID of the person trying to gain access, access will be granted to such individuals as long as the UID card and image captured belong to a registered user. In a situation where that is not the case, access will be denied and the RFID system turns on the alarm system to alert security personnel (Umar *et al*., 2014; Orji *et al*., 2018).

The major advantage of the RFID scanner system is that it can complete control and security tasks successfully through processing information from sub-controller systems such as exit monitoring controllers installed in exit gates, mess monitoring controllers installed in mess gates,

and entrance monitoring controllers that are installed in entrance gates.



2.2 RFID COMPONENTS

Figure 2.1: Basic Components of an RFID system (Borowski, 2021)

The RFID system is made up of four major components which include ();

- RFID tags
- RFID antennas
- RFID readers

2.2.1 RFID TAGS

An RFID tag contains a microprocessor or silicon chip, which functions as its memory and stores a unique code that works as an identification system, including a singular identification that is referred to as the tag ID or UID (Application Notes CAENRFID, 2008). The microchip has an

embedded circuit within it. And, the microchip is able to provide a unique identification based on a numbering technique (Garfinkel & Rosenberg, 2005). The microchip installed in the RFID tag could possess writeable or read-only features based on the type of the tag and how it was applied within the RFID solution. Each feature is dependent on the circuitry of the microchip, which included form and initialize commands when they were manufactured (Meiller & Bureau, 2009). Selection of tags is an extremely important factor in the RFID solution and selection is done based on the tag shape, size, and material (Nugraha *et al*, 2021).

One way to classify tags is based on their capability – in this case, we have read-only, further recoding, and re-write tags. Both read-only and writeable (or rewrite) tags can be reprogrammed. Although, to reprogramme the memory of read-only tags, a separate electronic equipment is needed. On the other hand, there is no need for a separate equipment in the reprogramming of re-write tags before new data can be written on it as long as the reader can enter writing commands and tags are in range; however, this depends on the protocol support on the tag (Nugraha *et al*, 2021). According to Ge *et al*. (2021), there are five tag classifications and they are represented in the image below:

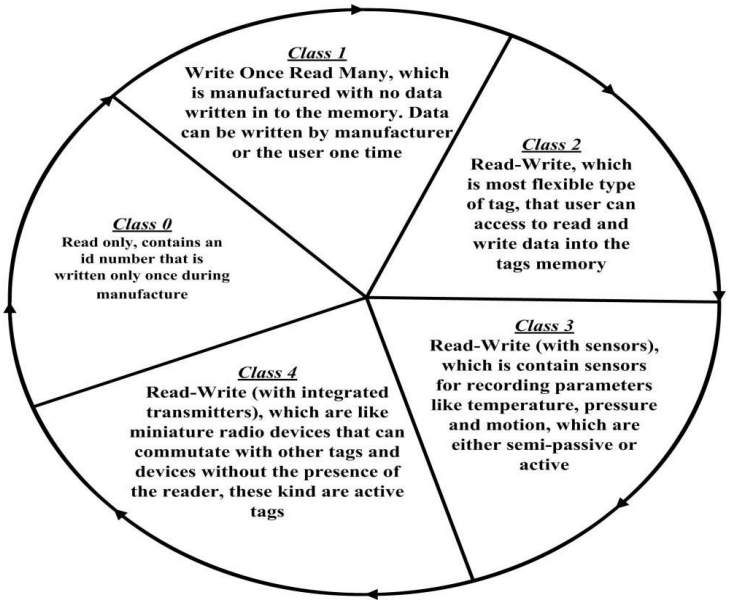


Figure 2.2: Tag Classifications based on capability (Ge et al., 2021)

Another means of classifying tags is based on type. There are three major types of tags which include passive, semi-active, and active tags. Semi-active tags have characteristics of both active and passive tags. However, there are major differences in the features of passive and active tags (Application Notes CAENRFID, 2008) – the difference lies in memory capacity, security, range,

type of data that can be recorded, and frequency, among other features (Intermec, 2009).

Tag Standards

Tags are also classified based on standards within RFID solutions and the standards are also dependent on spectra. The following are some tag standards:

ISO/IEC 18000 tags: This standard provides support for different tag architectures and principles. Meaning that, this tag standard can adapt to different ranges of frequency including microwave, low frequency (LF), long-range (UHF), and high frequency (HF) ranges. The range of tag IDs are comprised of 18000-(1 to 7) (Nugraha *et al*, 2021).

ISO/IEC 15693 tags: The range of tag IDs in this standard are not as unique as ISO 18000. Even though vendors make efforts to create unique tags – though, they don't possess a global uniqueness. These tag standards are commonly used in smart cards that are connected to contactless systems or mechanisms. They can also be used in other local scenarios such as for tracking assets or a supply chain.

EPC tags: This tag standard exists for maintaining uniqueness of tags under a select number of management bodies. The uniqueness of the tag is recognized by every vendor that is related to a single management entity. And, every management entity has their unique technique for EPC numbers and a specific object class, as well.

Tag Range and Frequencies

The range of tags depend on their frequencies and the frequency determine how much how much interference the tags are able to resist (Sharma *et al*, 2024). The different tag standards function

at diverse bands of frequency and the major organizations working with UHF bands to develop international standards are ISO and EPCglobal (Ge *et al*., 2021). Be that as it may, complete compatibility has not yet been accomplished; for that reason, the International Telecommunication Union (ITU) provide the generalized principles that many organizations use (U.S. Department of Homeland Security, 2006). The following frequency bands are included in the ITU's principles:

- **Microwave:** This works on 2.45 GHz. The reader rate of a microwave-band tag is faster than a UHF tags. The microwave frequency shows better results when applied to applications for tracking vehicles with a read range of 1 metre per tag. The downside of this frequency is that it does not provide good results when it is near metal or wet surfaces (Application Notes CAENRFID, 2008) – thus, the read rate under rain or on a metal roof will be poor.
- **Ultra High Frequency (UHF)**: The range of this band is within 860MHz – 930MHz. UHF has the capacity to, simultaneously identify a large number of tags with a fast multiple read rate. This shows that UHF has a, considerably, good reading speed. It shares the same limitation as the microwave in that it does not pick up signals properly when close to metal or wet surfaces. Be that as it may, its read rate and speed of transferring data far outranks high frequency – its reading range is 3 metres (Application Notes CAENRFID, 2008).
- **High Frequency (HF):** This operates on 13.56MHz and its reading range is less than 1 metre. However, the HF band is not expensive and also functions seamlessly with access control systems. It is also useful for identifying items on points – this is possible because it can be easily placed inside thin materials including paper (Khosla and Malhi, 2023; Application Notes CAENRFID, 2008).

- **Low Frequency (LF):** These bands work on 125kHz and have, approximately, one-half a meter read range. They are mostly used for applications with a short read range (Nugraha *et al*, 2021).

2.2.2 RFID ANTENNAS

The RFID antenna is the technological component of the system that functions as the middleman between the RFID tag and RFID reader; it provides energy to tags (that is, mostly the passive tags). Furthermore, the antennas collect data and transmit them between the reader and tags. The shape of an antenna can be altered based on the application with which it is linked as well as the rate of its feasibility. Another factor that differentiates antennas is the range (Nugraha *et al*, 2021).

Antenna has various shapes. Sometimes, the antennas are embedded in the RFID Reader. Antennas can be differentiated with various properties such as direction of signals (tags reading direction) and polarities. Stick antennas, gate antennas, patch antennas, circular polarized, di-pole or multi-pole antennas, linear polarized, beam-forming or phased-array element antennas, Omni directional antennas and adaptive antennas are the types of antennas commonly use in various applications (Sharma *et al*, 2024).

2.2.3 RFID READERS

The RFID reader is an external equipment that picks up radio signals and transmits them to the RFID system (Government Accountability Office, 2005). One RFID reader has the capacity to function on several frequencies; although, this capacity depends on the vendor (Application Notes CAENRFID, 2008). Furthermore, RFID readers sometimes possess anti-collision that are effective in the deduction of multiple tags at once; they also serve as the middleman between the

user application and tags. Readers form the core of the RFID system, which communicates between tags and the computer program – transferring information read from the UID of each tag to the computer program.

RFID readers can also write on a tag (that is, for writeable tags) and, although they can read information at several different frequencies, they can operate solely on a single frequency per time. For the reader to be able to communicate with the computer program that it is linked to it, a wireless or wired connection or link with the computer is required. Wired connections require either USB, RS-232, or RS485 – without these components, the reader will not be able to connect unless you employ a wireless, Wi-Fi, connection (usually called, a network reader) (Soares, 2018).

RFID readers can come in different sizes, shapes and models depending on the type of reader specified. Some RFID readers comes with an antenna that activates the chip of a type of RFID cards and RFID tags called Passive RFID cards and Passive RFID tags.

2.3 ARDUINO IDE

The Arduino Integrated Development Environment (IDE) is a program that runs on computers, allowing the use of a simple language to be used in writing sketches for the Arduino board – the model of the language is usually based on the Arduino Processing Language (Nedelkovski, 2017). Therefore, Arduino coding language is required for the coding of the Arduino microcontroller – the language is based on C or C++ and only two functions are needed to run the basic executable program, that is, the setup() function and the loop(). The setup() is what initializes pin modes and serial communication, among others, and the function can only be run once. The actual code is written under loop(). The function, loop(), continues to loop until the power of the device goes off.

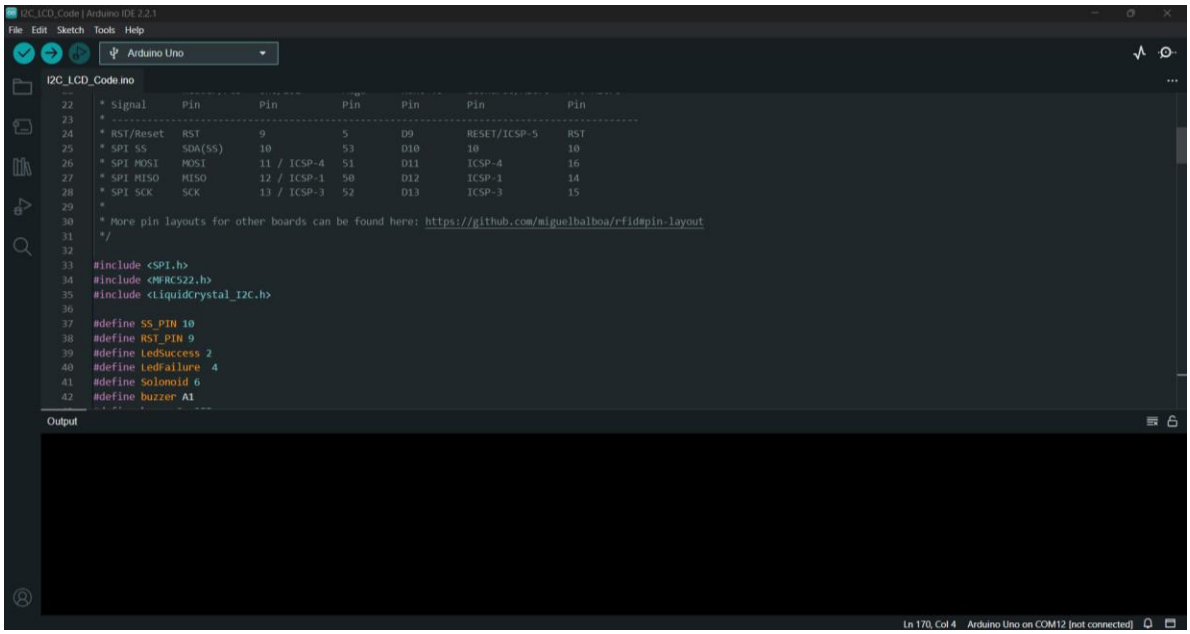


Figure 2.3: An Arduino IDE with code written in the code editor

2.4 ARDUINO UNO BOARD

The UNO board is a microcontroller board that is built on ATmega328. There are 14 digital input/output pins – 6 out of those 14 pins can function as pulse with modulation (PWM) outputs, 6 analog inputs, a 16MHz ceramic resonator, an in-circuit serial programming (ICSP) header, a universal serial box (USB) connection, a reset button, a power jack. Everything needed to serve as the support for the controller is contained in the board. The board is connected to the computer using a USB cable. The Arduino board can also be powered using an AC-to-DC battery or adapter (Nedelkovski, 2017).

Figure 2.4: An Arduino Microcontroller (Ismailov, 2022)

The Arduino UNO board has a chip on it that, when bad, could be replaced with a newer chip. And, after replacing the chip the board will work normally as before (Sharma *et al*., 2022).

CHAPTER THREE

METHODOLOGY AND DESIGN

3.1 MATERIALS FOR CONSTRUCTION

To guarantee that the system functions properly, the appropriate components for the access control system must be chosen. The key components used in this project are as follows:

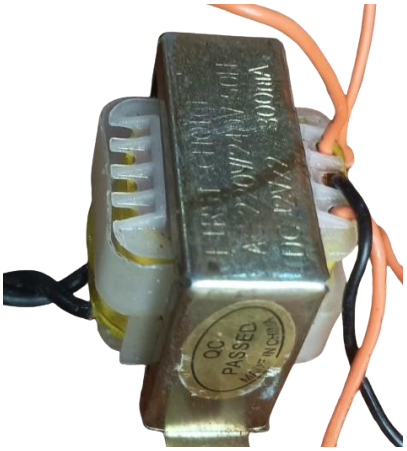
1. Transformer
2. Diodes
3. Capacitors
4. Resistors
5. Arduino Microcontroller (Arduino MC)
6. Light Emitting Diodes (LEDs)
7. Wires
8. Voltage Regulators
9. Transistors
10. Liquid Crystal Display (LCD) and I2C Module
11. RFID scanner
12. RFID card
13. RFID tag
14. Solenoid locker
15. Buzzer

3.2 TRANSFORMERS

A transformer is an electrical device that transfers energy from one circuit to another. It accomplishes this without adding any additional power or modifying the frequency of the

electrical waves. (Kokotovic, 2019). They operate based on Faraday's Law of Electromagnetic Induction, which asserts that "the magnitude of voltage is directly proportional to the rate of change in flux." When a current moves through one of the coils of a transformer, it generates a magnetic field, which induces a voltage across the other coils wrapped around the same core. (Tran *et al*, 2022).

Figure 3.1: A transformer

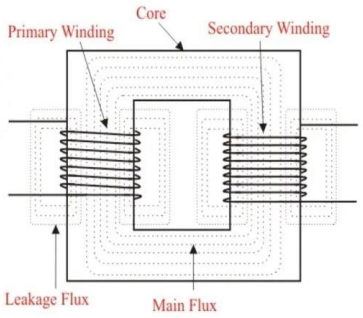


3.2.1 PARTS OF A TRANSFORMER

1. **Windings:** They are a series of copper wires coiled around the transformer core. There are two major kinds of winding: (Abror, 2020-).
    a. **Primary windings:** The primary winding of the transformer produces magnetic flux when connected to an electrical source (Abror, 2020-).
    b. **Secondary windings:** The magnetic flux produced by primary winding passing through the core links with the secondary winding. The set of winding turns from which output is taken (Abror, 2020-).
2. **Magnetic Core of Transformer**: The transformer core, which acts as a low reluctance channel for the magnetic flux connecting the primary and secondary windings, is one of

the most significant and complex components of a power transformer. (Tang *et al*., 2014).

3. **Insulation Agents**: To avoid premature ageing and eventual device failure of the transformer, the heat generated by energy loss must be removed. This is typically

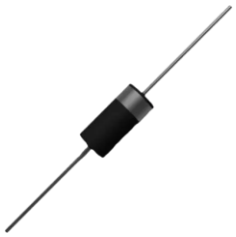


accomplished by circulating transformer oils (TO), which also ensures the electrical insulation of energised wires. (Rajnak *et al*., 2019).

Figure 3.2: Parts of a Transformer (Tran, *et al* 2022)

3.3 DIODES

A diode is an electronic component that has two terminals and typically conducts current in one way. It has low resistance in one direction and high resistance in the other. A diode's main purpose is to enable current to flow in one direction (forward) while blocking it in the opposite direction (reverse). This flow in one direction is referred to as rectification. Rectification is a single-directional behaviour that converts AC (alternating current) to DC (direct current).



(Takele, 2022).

Figure 3.3: A diode (Tran, *et al* 2022)

3.4 CAPACITORS

A capacitor is a simple electronic component that stores charge in its electric field and returns it to the electrical circuit when needed. The device consists of two plates that conduct electricity

separated by an insulating substance or dielectric. (Senamaw, 2019).

Figure 3.4: Different types of capacitors (Wikipedia, 2023)

3.5 RESISTORS

A resistor is a passive electrical component with two terminals that add resistance to the flow of electric current in an electrical circuit. Resistors are commonly used to balance active components like op-amps, microcontrollers, and other integrated circuits. Resistors are commonly used to pull up I/O lines, divide voltages, and can be used to limit current. (Jelten *et*

al., 2021).

Figure 3.5: A Resistor (Zubaer *et al.*, 2020)

3.6 ARDUINO MICROCONTROLLER

Arduino is a freely available microcontroller that can be readily programmed, removed and reconfigured at any given moment. Arduino microcontrollers provide input and output capabilities, allowing for data collection and output. Arduino microcontrollers are also capable of transmitting and receiving information over the web via HTTP requests. The Arduino platform can be divided into two: Hardware and Software (Ismailov, 2022).

Figure 3.6: An Arduino Microcontroller (Ismailov, 2022)

1. **Hardware:** Arduino utilizes a hardware device that is called the Arduino development board. The Arduino board is built up with the 8-bit Atmel AVR microcontrollers that are manufactured by Atmel or a 32-bit Atmel ARM, and they can be readily configured using the C++ or C programming language in the Arduino Integrated Development

Environment (IDE). The Arduino board has pins used for connectivity and these pins can be categorized as:

a. Analog pins

b. Digital I/O pins

c. Power and GND (Ground) pins

(Ismailov, 2022).

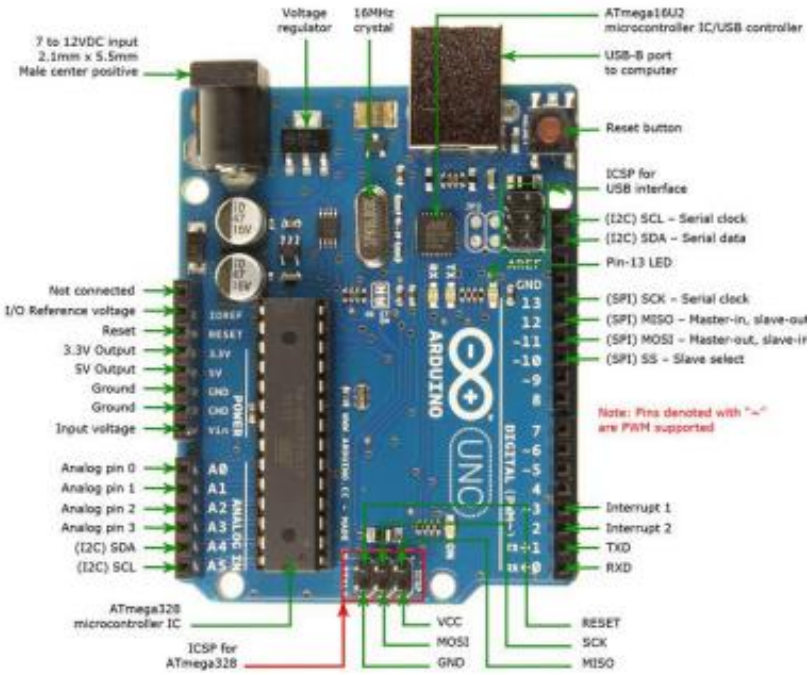


Figure 3.7: An Arduino UNO board with its specific pins (Ismailov, 2022)

2. **Software:** The code written for the Arduino board is also known as a sketch. Arduino IDE is the software which is used to program and configure the Arduino board, and it is where the sketch is written. This IDE contains the following parts:

   a. **Text editor:** The programming code is written here in either C or C++ programming language.

b. **Message area:** It is an area that displays an error and provides feedback when the code is being saved or exported.

c. **Text:** The console part of the Arduino IDE shows text output by the Arduino environment consisting of error messages and other information.

d. **Console Toolbar:** This toolbar consists of a few buttons like Compile, Upload, New, Open, Save, and Serial Monitor.

(Ismailov, 2022).

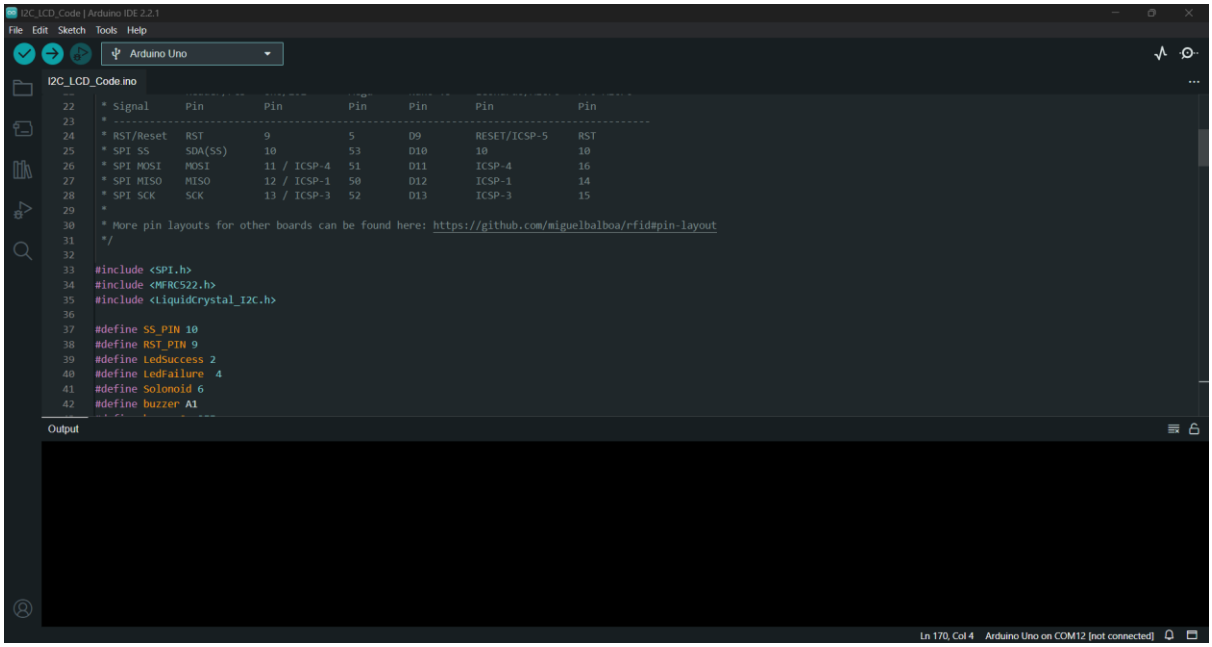


Figure 3.8: An Arduino IDE with code written in the text editor

3.7 LIGHT EMITTING DIODES

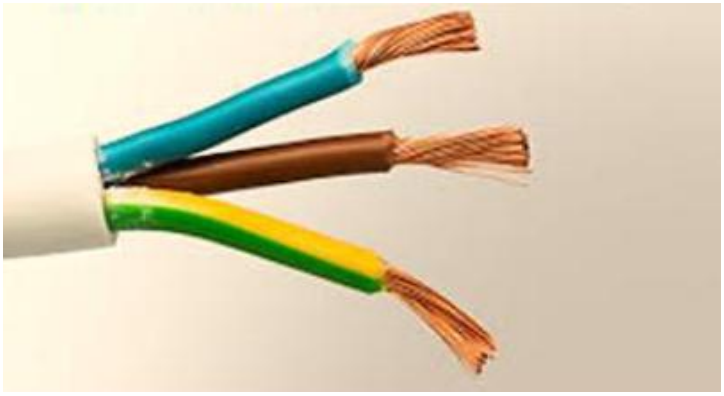
Light-emitting diodes (LEDs) are semiconductors that produce light when a forward voltage is passed through them. The LED is a solid-state electronic component. Which means it is more

similar to an electronic chip than to an actual light bulb. (Bourget, 2008). LEDs are semiconductor devices that emit light when a current flows through them. This is a two-lead semiconductor light source. It is a p-n junction diode that produces light when activated. When an appropriate current is applied, electrons can recombine with electron holes in the device, releasing energy as photons. (John, 2018)

Figure 3.9: LEDs (Wikipedia, 2024)

3.8 WIRES

Wires are conductors used to connect electronic components together in a circuit. They come in different sizes, lengths, and colors ,and the use of the wire depends on the width and color of the



wire.

Figure 3.10: Wires (Alhashimi, 2019)

3.9 VOLTAGE REGULATORS

The voltage regulator, as the name implies, maintains a steady voltage in a circuit. Following rectification, the voltage regulator acts as additional protection, ensuring that only the required voltage enters the circuit. The voltage regulator consists of three primary pins and an adjustable output voltage. (Pimpalkar *et al*., 2020).

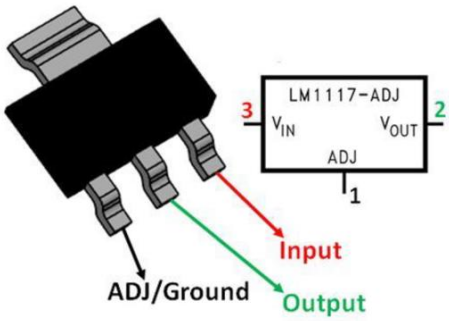


Figure 3.11: Voltage Regulator (LM1117) (Jyothi *et al*., 2017)

3.10 TRANSISTORS

A transistor functions as both a switch and an amplifier; it is a semiconductor device that conducts and insulates electrical voltage/current. Transistors are three-terminal devices that regulate the flow of electrical current, allow for quick switching, and are utilized to create a

single integrated circuit (Turner, 2013).

Figure 3.12: A Bipolar junction transistor (Othman, 2019)

3.11 LIQUID CRYSTAL DISPLAY and I2C MODULE

A liquid-crystal display (LCD) is an electronically modified optical system that utilizes liquid crystals and polarizers to manipulate light. Liquid crystals produce color or monochrome images by using a backlight or reflector, rather than emitting light directly. LCDs can display either arbitrary graphics (as in a computer display) or fixed images with limited information content (e.g., preset words, numerals, or seven-segment displays in a digital clock). (Kuria *et al.*, 2020). The LCD screen communicates via an I2C interface. The LCD display requires only four pins. The pins are VCC, GND, SDA, and SCL.VCC and GND are wired to Arduino's 5V and GND pins. SDA and SCL are connected to Arduino's pins A4 and A5. It saves at least four Arduino analog or digital pins. It is extensively utilized due to the Arduino Uno's tendency to exhaust pin

resources quickly. (Jahan and Noman, 2020)

Figure 3.13: An LCD (Jahan and Noman, 2020)

Figure 3.14: An I2C module (Jahan and Noman, 2020)

3.12 RFID SCANNER OR READER

The RFID reader is a device that is used to gather data from the radio RFID system. The RFID system uses radio waves to transfer the data from the RFID tag to the RFID reader. The RFID reader also called the interrogator, is the brain of the RFID system and must be present for any

system to function. (Nababa and Baballe, 2021)

Figure 3.15: A RFID Reader (Saste *et al*, 2021)

3.13 RFID CARD and RFID TAG

The RFID tag and RFID card are digital tags that uses radio waves to transmit data to an RFID reader. The antenna and IC are the two main components of almost all RFID tags. The IC is used to process and save information, and the antenna is utilized to receive radio frequency waves. Any information that the user desires can be written on the RFID microchip. (Nababa and Baballe, 2021)

The tags are classified according to working frequency:

- **Low Radio Frequency (LRF) tag:** Frequency that operates between 100 and 500 kHz
- **High Radio Frequency (HRF) tag:** Frequency that operates between 850 and 950 MHz
- **Ultra-high Radio Frequency (UHRF) tag:** Frequency that operates between 2.4 and 5.8

GHz.

Figure 3.16: A RFID Reader (Nababa and Baballe, 2021)

3.14 SOLENOID LOCKER

The solenoid lock indicates the lock for electrical locking and opening. It is available for use in locking and keeping within the control on mode sort, as well as opening within the control on mode sort, depending on the situation. While the solenoid is powered on, the control on the

opening effectively empowers the opening. (Moje *et al.*, 2023)

Figure 3.17: A Solenoid Locker (Moje *et al.*, 2023)

3.15 BUZZER

Buzzers are devices that produce sound throughout a more precise frequency range. An endless variety of electrical gadgets, such as fire alarms, medical equipment, alarm clocks, and intruder

alarms, use buzzers. (Dixit *et al.*, 2019)

Figure 3.18: A buzzer module (Ramkrishna *et al*, 2019)

3.16 BLOCK DIAGRAM OF PROPOSED DESIGN

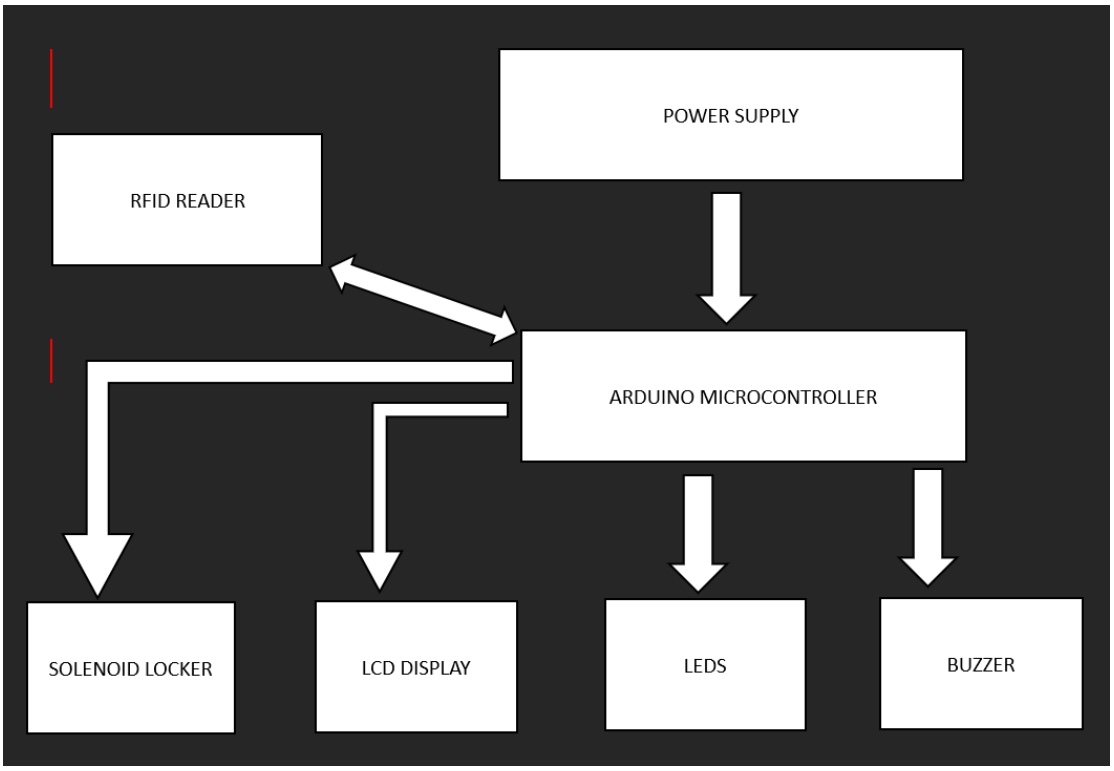


Figure 3.19: System Block Diagram

3.16.1 MODE OF OPERATION

All the available Power or AC source are used as input into the power supply to make sure that as long as there is a supply from any of the AC sources, the system can be turned ON. The RFID reader is connected to the microcontroller and communication happens between them. Other components like the solenoid locker, buzzer, LEDs and LCD are connected to different pins in the microcontroller. When the RFID reader scans a card or tag it gets the UID of the card or tag and sends it to the microcontroller as input. The code in the microcontroller runs and check if the UID is registered. If it is registered, the microcontroller gives an ouput to the green LED, the LCD, the buzzer and the solenoid locker for some seconds. If the UID is not registered, the microcontroller gives an output to the red LED, and the LCD for some seconds.

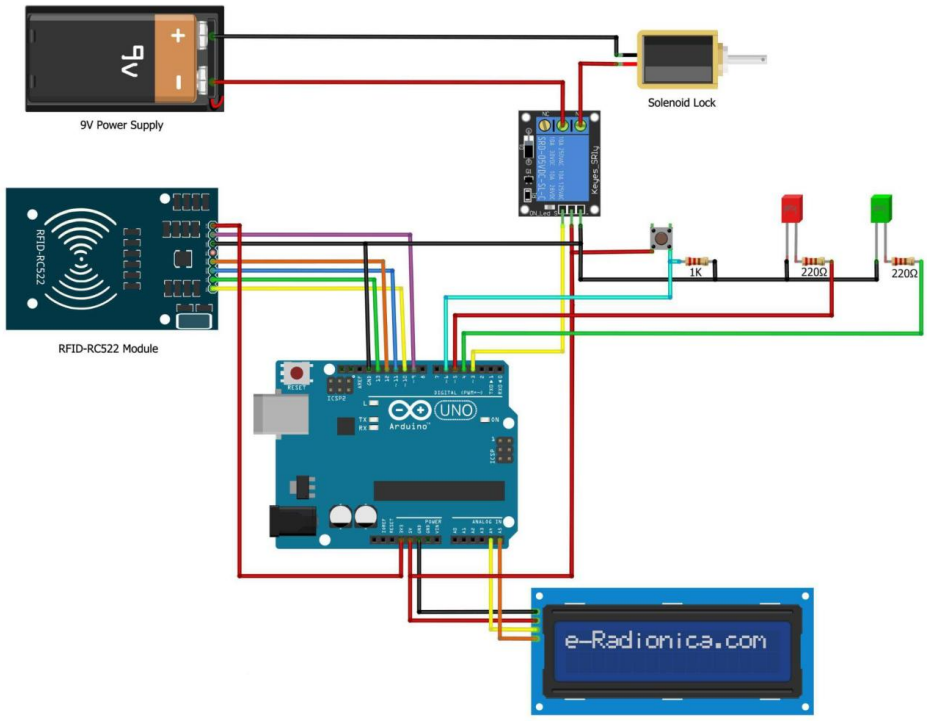


Figure 3.20: Complete Circuit Diagram

CHAPTER FOUR

SYSTEM TESTING IMPLEMENTATION AND EVALUATION

4.1 SYSTEM TESTING

After the model is completed, testing is required to confirm that the system performs properly per the project's goals. The model has many components and circuitry that must be tested individually and collectively to ensure that the components work effectively, the individual circuits accomplish the function for which they were built, and the complete system functions well.

4.2 TEST PLAN

The test plan encompasses all the steps taken in checking the functionality of each module that makes up the entire system design.

4.2.1 SIMULATION

The test plan begins with a simulation of the complex work using an electronics software called Proteus. The simulation test results ensured that the system design was feasible and fully functional in its logical decision.

4.2.2 POWER SUPPLY TEST

The setup for the power supply test circuit is shown in Figure 4.1 below. The setup comprises a 240V – 24V step-down centre tap transformer, a full wave rectifier, a 1000uf 100v filtering capacitor, and 1 voltage regulator (L7805CV). This test was carried out with no load connected.

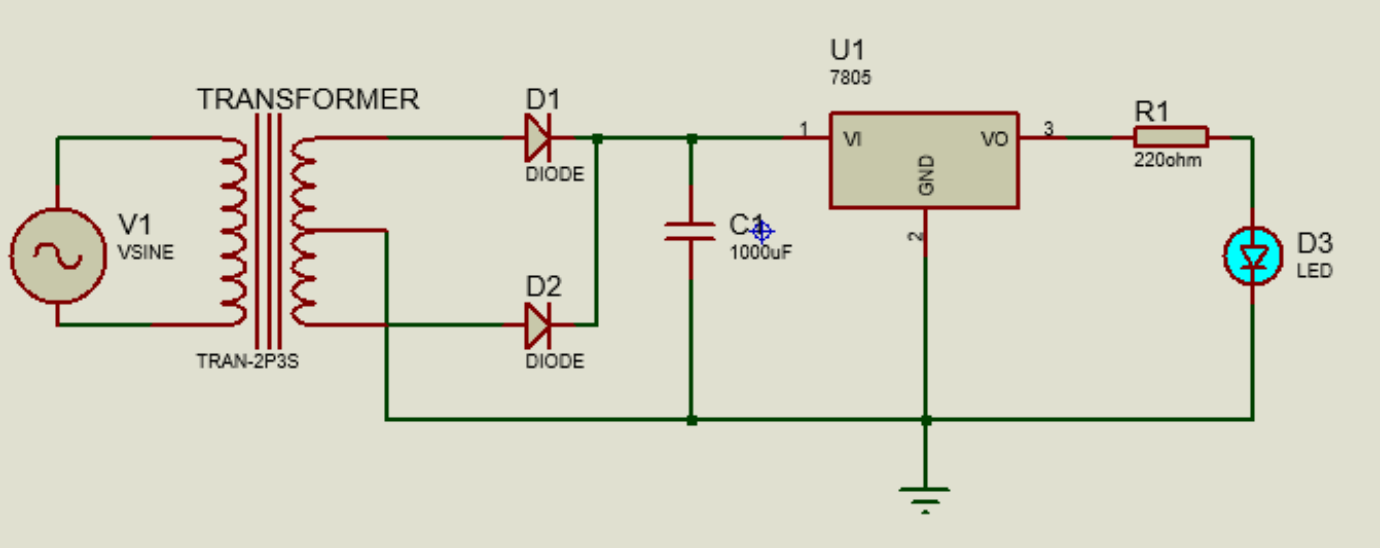


Figure 4.1: Power supply setup

AC INPUT	5 VOLTS OUTPUT
212.35 V	5.04 V
215.57 V	5.08 V
204.17 V	5.06 V
195.19 V	4.99 V
188.20 V	4.97 V

Table 4.1: Power Supply Test

Table 4.1 shows a negligible voltage drop in the output of the voltage regulator. This is because the input AC voltage dropped. From the table above it can be deduced that the power supply design will still work fine. Even if the AC voltage input drops significantly to around 160V from the 240V expected, the voltage drop at the voltage regulators will not significantly affect the system.

4.2.3 ARDUINO MICROCONTROLLER AND LED CIRCUIT TEST

The Arduino microcontroller is a crucial component in the system, as it receives input from the RFID reader and translates it into commands. The setup for the Arduino microcontroller and LED test circuit is shown in Figure 4.2 below. The setup comprises an Arduino Microcontroller Digital board, a 220ohm resistor, a switch or button and an LED. This test confirms that the Arduino Board and the Arduino Software are all working properly.

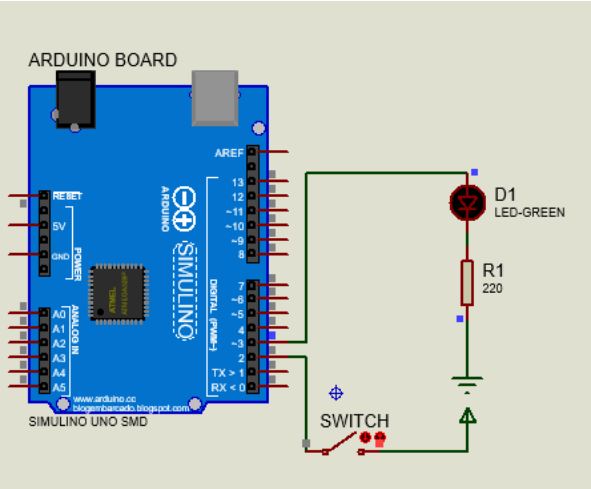


Figure 4.2a: Setup with open switch

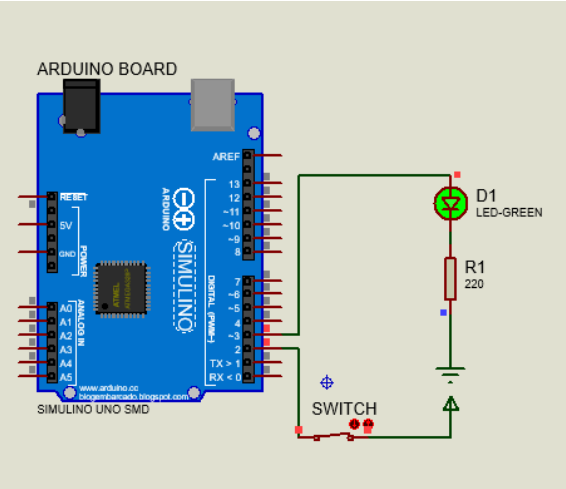


Figure 4.2b: Setup with closed switch

Figure 4.2: Arduino Microcontroller and LED setup

From Figure 4.2 above, when the switch is open as in Figure 4.2a, the LED is off, and when the switch is closed as in Figure 4.2b, the LED turns on. This test confirms that both the Arduino board and the Arduino software are working as expected.

The code to test the LED with the Arduino microcontroller can be found in Appendix A.

The typical maximum current the LED can work with is roughly 25mA, and the Arduino board gives an output of 5V. This means the total resistance of the resistor we need to add and the LED should be:

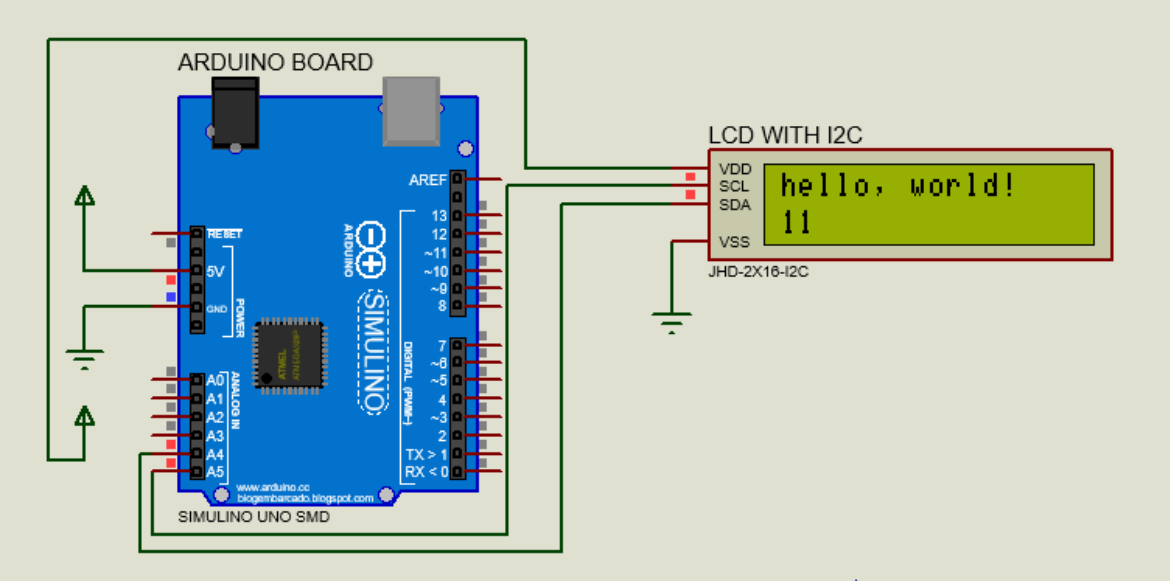
R = □ / □ (4.1)

V = 5V, I = 25mA ≃ 0.025A (4.2)

∴ R = 5 / 0.025 (4.3)

R = 200Ω (4.4)

The resistance of the LED would be extremely small in this direction, thus the resistance of the resistor would be larger than 200 Ohm. For safety reasons, we used 220 Ohm which still worked.

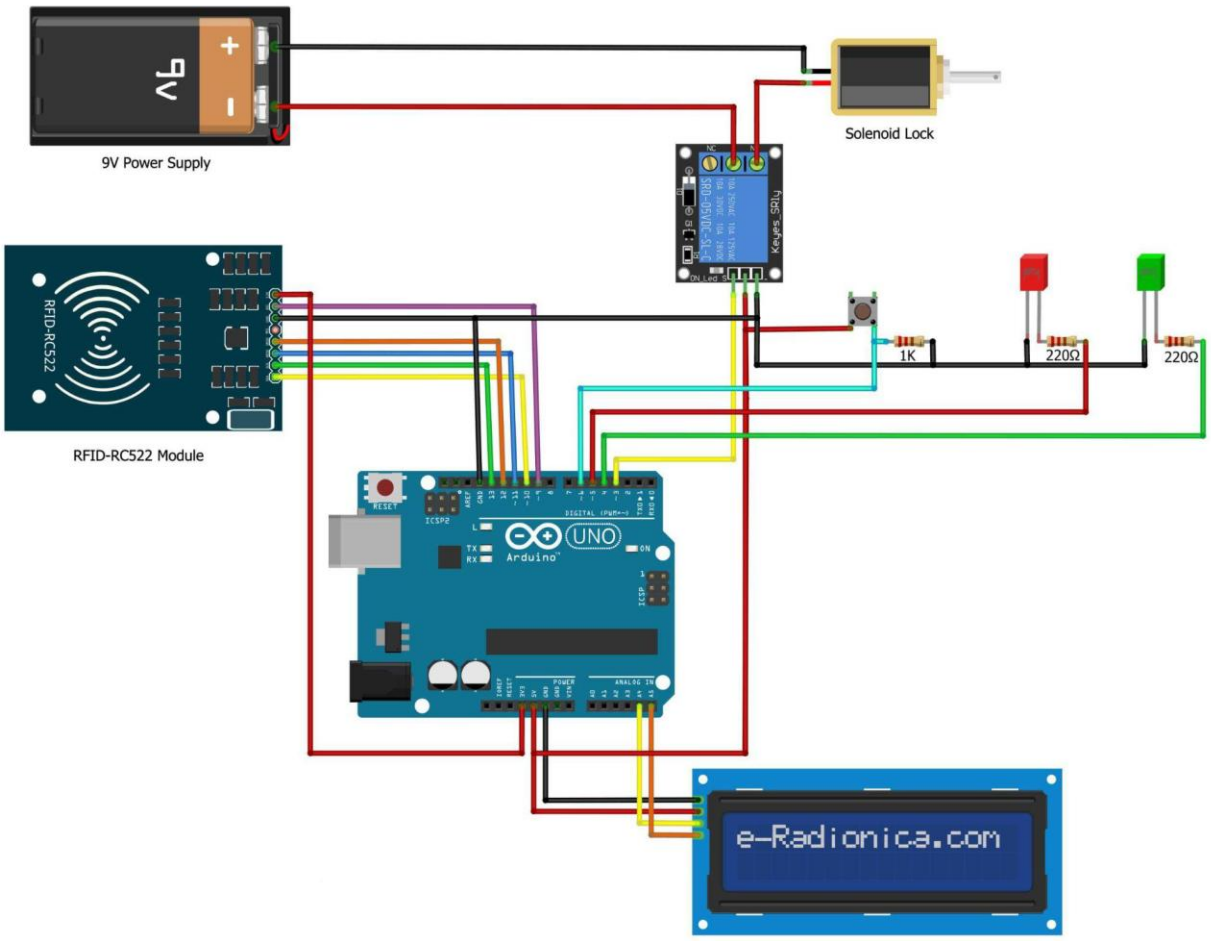


4.2.4 LCD WITH I2C MODULE CIRCUIT

Figure 4.3: Arduino Microcontroller and LCD with I2C module setup

Figure 4.3 above shows the setup for the LCD to microcontroller circuit using the I2C module, simulated in the Proteus CAD software. The setup above consists of an Arduino microcontroller and a 2 by 16 Liquid Display Crystal (LCD).

The code to test the LCD to microcontroller circuit using the I2C module can be found in Appendix B.



4.2.5 COMPLETE ACCESS CONTROL SYSTEM CIRCUIT TEST

Figure 4.4: Complete access control system setup

After the setup was completed, a full system test was carried out using an RFID card and an RFID tag. This test was carried out to verify the connectivity of the system as well as to make sure the code and software were running properly. Figure 4.4 above shows the setup for testing the circuit simulated using the Proteus CAD software. This set consists of an Arduino microcontroller, two LEDs, three resistors, a capacitor, an LCD, a solenoid lock, a buzzer, an

RFID reader, a 9v battery, and 5v power terminal from the power supply. The code in Appendix C was uploaded into the microcontroller to control the access based on the UID of either an RFID card or tag and these controlled the turning ON and OFF of the LED circuit. A prompt, a success message and an error message were displayed on the LCD based on whether access is gained or not, and the buzzer makes a sound if access is gained.

The system was tested with an RFID card with a UID that was allowed access by the controller code and an RFID tag with an unknown UID. When both were scanned by the RFID reader, the card was successfully granted access while the tag wasn't granted access.

4.3 BILL OF CONSTRUCTION MATERIAL AND ESTIMATION

Table 4.2 provides a list of all the materials used in the construction of the RFID and Arduino-based access control system, alongside the quantity used, and the cost per unit price. Table 4.3 shows the total cost of materials and the total estimate for the project.

S/N	PARTICULAR	QUANTITY	UNIT PRICE (NAIRA)	AMOUNT (NAIRA)
1	220v / 12v transformer	1	1,700	1,700
2	Arduino UNO MC	1	15,000	15,000
3	LCD + I2C	1	5,000	5,000
4	L7805 voltage regulator	1	200	200
5	Solenoid lock	1	5,000	5,000
6	Buzzer	1	400	400
7	Diodes	5	20	100
8	LED	5	20	100
9	1000uf capacitor	1	100	100
10	9v battery	1	1,000	1,000

Table 4.2: Bill of construction material

Total Calculation Table

S/N	PARTICULAR	AMOUNT
1	Initial total	28,600
2	Miscellaneous	70,000
3	Total	98,600

Table 4.3: Total calculation

CHAPTER FIVE

DISCUSSION AND CONCLUSION

5.1 DISCUSSION

After considering the physical design of the hardware, as well as the installation of the components, the RFID and Arduino-based access control system was successfully developed and implemented. The system was able to grant access to an RFID card with known and registered UID and rejected access to an RFID tag with unknown UID.

5.2 CHALLENGES ENCOUNTERED DURING PROJECT EXECUTION

While navigating the complexities of the project's execution, several challenges emerged that required innovative problem-solving and technical finesse. These challenges underscored the intricate nature of developing an RFID and Arduino-based access control system.

The first challenge encountered was the problem of trying to determine the amount of current allowed to enter the microcontroller from the power supply. The Arduino board used can only be powered with current of up to 1A. This means that if the current entering the board from the power supply exceeds 1A, it could damage the board. This made the design and construction of the power supply very important to the project. While the project was ongoing, an abnormal amount of current passed through the board, which damaged the board. A new Arduino board was purchased for the project to continue.

Another challenge encountered was that the Arduino board could not power the solenoid lock independently. The solenoid lock used for the project required a voltage of 12v and the output

voltage of the Arduino board was 5v. Because of this, a 9v battery was connected to the Arduino board to increase the voltage output and this enabled the Arduino to power the solenoid lock.

5.3 CONCLUSION

The design and construction of an RFID and Arduino-based access control system offers numerous benefits for efficient and effective security and access control management. The developed system is also flexible in a way that each RFID card and RFID tag can be registered and unregistered in the system using the microcontroller code. The system can be widely applied to both personal and industrial systems, and it can easily be modified to include more security measures. With this system, security need not be physical and this can be extremely advantageous especially with systems and spaces that requires security at all times.

5.4 RECOMMENDATION

As this project comes to a close, it is critical to recognize potential areas for future growth and improvement of the RFID and Arduino-based access control system. The following suggestions are made to improve the system's performance, accessibility, and versatility:

1. Explore options to utilize a more effective power supply system, preferably a solar panel to enable round-the-clock functioning of the system.
2. A further security measure can be added like biometrics or face scanner, to ensure almost perfect access control.
3. The microcontroller’s code can be rewritten to be more secure.

REFERENCES

Abror, Q. 2020. Development of Magnetic Characteristics of Power Transformers. *The American Journal of Applied sciences* **2**(9): 46-50.

Alhashimi, M. T. M., Nukhailawi, J. K. Y., and Ali, A. T. (2019). Review on Electrical Wiring (Types, Sizes and Installation). *Journal of Instrumentation Technology and Innovations.* **9**(3):31-40.

Application Notes CAENRFID, (2008), Introduction to RFID Technology, CAENRFID: *The Art of Identification*

Arduino Forum, (n.d). RFID 125kHz PCB antenna [online]. Retrieved from: https://forum.arduino.cc/t/rfid-125khz-pcb-antenna/194328 Accessed: March 9, 2024

Borowski, P. F. (2021). Digitization, digital twins, blockchain, and industry 4.0 as elements of management process in enterprises in the energy sector. *Energies*. **14**(7): 1885

Bourget, C. M. (2008). An Introduction to Light-emitting Diodes. *HortScience horts*. **43**(7):1944-1946.

Department of Homeland Security, (2006). "Enhanced Security Controls needed for US-Visit's System using RFID Technology", *Department of Homeland Security (Office of Inspector General),* 06-39.

Dhanalakshmi, K. S., Praghna, A., Reddy, E. T., and Prabhavathy, S. K. (2021). Rfid based Access Control System Using Arduino. *Annals of the Romanian Society for Cell Biology*, **25**(6), 17614-17622.

Dixit, S., Tale, M., Agrawal, T., Tidke, S., Umredkar, S., and Taori, D. (2019). STUDY OF PIEZOELECTRICITY AND TESTING THE EFFICINECY USING SOUND SENSOR. *5th International Conference on Research Developments in Applied Science, Engeneering and Management.* 52 -58

Garfinkel, S. and Rosenberg, B. (2005). “RFID Application, Security, and Privacy”, *USA.*

Ge, L., Zhang, C., Tian, G., Xiao, X., Ahmed, J., Wei, G., and Robinson, M. (2021). Current trends and perspectives of detection and location for buried non-metallic pipelines. *Chinese Journal of Mechanical Engineering*. **34:** 1-29.

Government Accountability Office, (2005). Information Security: Radio Frequency Identification Technology in the Federal Government, Report to Congressional Requesters, US. Government Accountability Office, available at: www.gao.gov/new.items/d05551.pdf, GAO-05-551

Intermec, (2009). “ABCs of RFID: Understanding and using radio frequency identification”, *White Paper.*

Ismailov, A. S., and Jo‘Rayev, Z. B. (2022). Study of arduino microcontroller board. *Science and Education*. **3**(3):172-179.

Jahan, I., and Noman, F. O. (2020). GSM Based Home Automation. *Chittagong University of Engineering and Technology Electronics and Telecommunication Engineering*. 1-12.

Jelten, B.N., Shuaibu, A.N. and Dajab, D.D., 2021. Development of A Resistance Colour Codes Interpreter and Finder Application. *Red.* ***2***(2):100.

John, S. (2018). Different Types of in Light Emitting Diodes (LED) Materials and Challenges- A Brief Review. *International Journal for Research in Applied Science & Engineering Technology*. **6**(4):4418-4420.

Khabarlak, K., and Koriashkina, L. (2021). Mobile access control system based on RFID tags and facial information. *arXiv preprint arXiv:2103.06767*.

Khosla, D., and Malhi, K. S. (2023). A review on RFID using different dielectric resonator antennas for industry 4.0. *Materials Today: Proceedings.*

Kokotovic, M. (2019). Automatic transfer switch between three power sources (analysis of schemes)". Retrieved from: https://electrical-engineering-portal.com/automatic-transfer-switch-three-power-sources. [Retrieved date: 11th-March-2024].

Kuria, K. P., Robinson, O. O., & Gabriel, M. M. (2020). Monitoring temperature and humidity using Arduino Nano and Module-DHT11 sensor with real time DS3231 data logger and LCD display. **9**(12):416-422

Meiller, Y., and Bureau, S. (2009). Logistics projects: how to assess the right system? The case of RFID solutions in healthcare. *AMCIS 2009 Proceedings.* 547.

Moje, R. K., Khadke, C. H., Lahore, T. M., and Patil V. S. (2023). Door Lock System using Password and Arduino. *International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering.* **11**(5): 98-102

Nababa, F. A., and Baballe, M. A. (2021). A comparative study on radio frequency identification system and its various applications. *International Journal of Advances in Applied Sciences.* **10**(4): 392-398

Nedelkovski, D. (2017). How RFID Works and How To Make an Arduino-based RFID Door Lock. *How To Mechatronics*

Nugraha, A., Daniel, D. R., and Utama, A. A. G. S. (2021). Improving multi-sport event ticketing accounting information system design through implementing RFID and blockchain technologies within COVID-19 health protocols. *Heliyon*. **7**(10).

Orji, E. Z., Oleka, C. V., and Nduanya, U. I. (2018). Automatic access control system using arduino and RFID. *Journal of Scientific and Engineering Research*. **5**(4): 333-340.

Pimpalkar, V.M., Damini, G., Chetan, B., Punam, A. and Payal. K. (2020). *International Journal of Engineering Applied Sciences and Technology*. **4**(10):242-246.

Radiant RFID, (2022). RFID System Components: What are the Core Elements of an RFID Solution? [online]. Retrieved from: https://rb.gy/xcg7ff Accessed: March 8, 2024

Rajnak, M., Wu, Z., Dolnik, B., Paulovicova, K., Tothova, J., Cimbala, R., Kurimský, J., Kopcansky, P., Sunden, B., Wadsö, L., Timko, M. (2019). Magnetic Field Effect on Thermal, Dielectric, and Viscous Properties of a Transformer Oil-Based Magnetic Nanofluid. *Energies*. **12**(23): 4532.

Ramkrishna, Y., Leelavathi, D., Sreenivas, V. S. and Kishore, S. S. (2019). Intruder Alert and Security System. *International Journal of research and Analytical Reviews.* **6**(1): 469-472

San Hlaing, N. N., and San Lwin, S. (2019). Electronic door lock using RFID and password based on arduino. *International Journal of Trend in Scientific Research and Development*, **3**(2), 799-802.

Saste, V., Jagtap, T., Khan, M., and Bogiri, N. (2021). RFID Student ID Cards. *International Journal of Advanced Research in Computer and Communication Engineering.* **10**(12): 178-182

Senamaw, M. Z. (2019). A Review Paper on the Study of Charging and Discharging the Capacitor. *American Journal of Quantum Chemistry and Molecular Spectroscopy.* **3**(2): 48-55.

Sharma, M., Talwar, R., Pandey, D., Nassa, V. K., Pandey, B. K., and Dadheech, P. (2024). A Review of Dielectric Resonator Antennas (DRA)-Based RFID Technology for Industry 4.0. *Robotics and Automation in Industry 4.0*. 303-324.

Sharma, M. V., Singh, V., Mahar, V. K., Naryani, S., and Kumawat, S. (2022). RFID Based Access Control System Using Arduino. *International Research Journal of Modernization in Engineering Technology and Science*. **4**(6): 654-659.

Simukali, C. M. (2019). Multi factor authentication access control for student and staff based on RFID, barcode and GIS. *Doctoral dissertation, University of Zambia*.

Soares, R. C. (2018). Theoretical aspects of RFID security.

Takele, T. S. (2022). Characteristics of Semiconductor Diode and Its Application. *International Journal of Engineering Management.* **6**(3): 20-29.

Tang, Q., Wang, Z. D. and Jarman, P. (2012). Electrical steels and power transformer cores in deep saturation. *IEEE International Conference on Condition Monitoring and Diagnosis, Bali, Indonesia.* 1035-1038.

Tran, Q., Roose, L., Binh, D. and Quang, N. (2022). A Low-Cost Online Health Assessment System for Oil-Immersed Service Transformers Using Real-Time Grid Energy Monitoring. Energies. *Researchgate*, **15**(16): 5932.

Turner, L. (2013). Electronics Engineer's Reference Book. *Butterworth-Heinemann.* **4**: 8-22.

Umar Farooq, Mahmood ul Hasan, Muhammad Amar, Athar Hanif, and Muhammad Usman Asad, (2014), "RFID Based Security and Access Control System" *IACSIT International Journal of Engineering and Technology*. **6**(4)

APPENDIX

A. THE MICROCONTROLLER AND LED TEST CODE

The controller and LED test code was developed in an Integrated Development Environment called Arduino IDE, using C programming language. The code sample is displayed below;

```
const int SWITCH = 2;
const int LED = 3;
int SWITCH_STATE = 0;

void setup() {
  pinMode(SWITCH, INPUT);
  pinMode(LED, OUTPUT);
}

void loop() {
  SWITCH_STATE = digitalRead(SWITCH);
  if (SWITCH_STATE == HIGH) {
    digitalWrite(LED, HIGH);
  } else {
    digitalWrite(LED, LOW);
  }
}
```

B. LCD WITH I2C MODULE TEST CODE

The controller and LCD with I2C module test code was developed in an Integrated Development Environment called Arduino IDE, using C programming language. The code sample is displayed below;

```
/*!
 * @file HelloWorld.ino
 * @brief Show helloworld.
 * @copyright Copyright (c) 2010 DFRobot Co.Ltd (http://www.dfrobot.com)
 * @licence     The MIT License (MIT)
 * @maintainer [yangfeng](feng.yang@dfrobot.com)
 * @version  V1.0
 * @date  2021-09-24
 * @url https://github.com/DFRobot/DFRobot_RGBLCD1602
 */
#include "DFRobot_RGBLCD1602.h"

const int colorR = 255;
const int colorG = 0;
const int colorB = 0;

/*
Change the RGBaddr value based on the hardware version
----------------------------------------
```

```
      Moudule        | Version| RGBAddr|
----------------------------------------
 LCD1602 Module      |  V1.0  | 0x60   |
----------------------------------------
 LCD1602 Module      |  V1.1  | 0x6B   |
----------------------------------------
 LCD1602 RGB Module  |  V1.0  | 0x60   |
----------------------------------------
 LCD1602 RGB Module  |  V2.0  | 0x2D   |
----------------------------------------
*/

DFRobot_RGBLCD1602 lcd(/*RGBAddr*/0x60 ,/*lcdCols*/16,/*lcdRows*/2);  //16
characters and 2 lines of show

void setup() {
    /**
     *  @brief initialize the LCD and master IIC
     */
    lcd.init();

    lcd.setRGB(colorR, colorG, colorB);

    // Print a message to the LCD.
```

```
    lcd.print("hello, world!");


    delay(1000);
}


void loop() {
    // set the cursor to column 0, line 1
    // (note: line 1 is the second row, since counting begins with 0):
    /**
     *  @brief set cursor position
     *  @param col columns optional range 0-15
     *  @param row rows optional range 0-1,   0 is the first row, 1 is the second row
     */
    lcd.setCursor(0, 1);
    // print the number of seconds since reset:
    lcd.print(millis()/1000);


    delay(100);
}
```

C. THE MICROCONTROLLER CODE

The controller code was developed in an Integrated Development Environment called Arduino IDE, using C programming language. The code sample is displayed below;

```
#include <SPI.h>

#include <MFRC522.h>

#include <LiquidCrystal_I2C.h>

#define SS_PIN 10

#define RST_PIN 9

#define LedSuccess 2

#define LedFailure  4

#define Solonoid 6

#define buzzer A1

#define buzzerOn 255

#define buzzerOff 0



 char PassKey[13] ="179214113246";

void printHex(byte *buffer, byte bufferSize) ;
```

```
void printDec(byte *buffer, byte bufferSize);

MFRC522 rfid(SS_PIN, RST_PIN); // Instance of the class

LiquidCrystal_I2C lcd(0x27,20,4);

MFRC522::MIFARE_Key key;



// Init array that will store new NUID



String nuidPICC;



void setup() {

  pinMode(Solonoid, OUTPUT);

  pinMode(LedSuccess,OUTPUT);

  pinMode(LedFailure,OUTPUT);

  pinMode(buzzer,OUTPUT);

  digitalWrite(Solonoid,LOW);

  analogWrite(buzzer,buzzerOff);

  digitalWrite(LedFailure,HIGH);//Off by defualt
```

```
  digitalWrite(LedSuccess,HIGH); // Off by defualt
  Serial.begin(9600);
  SPI.begin(); // Init SPI bus
  rfid.PCD_Init(); // Init MFRC522


  for (byte i = 0; i < 6; i++) {
    key.keyByte[i] = 0xFF;
  }


  Serial.println(F("This code scan the MIFARE Classsic NUID."));
  Serial.print(F("Using the following key:"));
  printHex(key.keyByte, MFRC522::MF_KEY_SIZE);
  lcd.init();
  lcd.backlight();
}
```

```
void loop() {


 lcd.print("               "); // clear the field

 lcd.setCursor(0,0);

 lcd.printstr("  Scan tag to   ");

 lcd.setCursor(0,1);

 lcd.println("   Open Door!   ");


 // Reset the loop if no new card present on the sensor/reader. This saves the entire process when idle.

 if ( ! rfid.PICC_IsNewCardPresent())

   return;


 // Verify if the NUID has been readed

 if ( ! rfid.PICC_ReadCardSerial())

   return;

analogWrite(buzzer,buzzerOn);
```

```
delay(150);

analogWrite(buzzer,buzzerOff);

Serial.print(F("PICC type: "));

MFRC522::PICC_Type piccType = rfid.PICC_GetType(rfid.uid.sak);

Serial.println(rfid.PICC_GetTypeName(piccType));



// Check is the PICC of Classic MIFARE type

if (piccType != MFRC522::PICC_TYPE_MIFARE_MINI &&

  piccType != MFRC522::PICC_TYPE_MIFARE_1K &&

  piccType != MFRC522::PICC_TYPE_MIFARE_4K) {

  Serial.println(F("Your tag is not of type MIFARE Classic."));

  return;

}



  // Store NUID into nuidPICC array

  for (byte i = 0; i < 4; i++) {

    nuidPICC += rfid.uid.uidByte[i];
```

```
  }
  Serial.println(F("The NUID tag is:"));
  Serial.print(F("In hex: "));
  printHex(rfid.uid.uidByte, rfid.uid.size);
  Serial.println();
  Serial.print(F("In dec: "));
  printDec(rfid.uid.uidByte, rfid.uid.size);
  Serial.println();
// Halt PICC
rfid.PICC_HaltA();
// Stop encryption o6n PCD
rfid.PCD_StopCrypto1();
if(strcmp(PassKey,nuidPICC.c_str())==0){
  Serial.println("Successful");
  lcd.clear();
  lcd.setCursor(0,0);
  lcd.printstr("    Successful   ");
```

```
  lcd.setCursor(0,1);
  lcd.println("   Door Opened   ");
  digitalWrite(LedSuccess,LOW);
  digitalWrite(Solonoid,HIGH);
  analogWrite(buzzer,buzzerOn);
 // delay(500);
  //analogWrite(buzzer,buzzerOff);
}else{
  Serial.println("Failure");
  digitalWrite(LedFailure,LOW);
  lcd.setCursor(0,0);
  lcd.printstr("    Failure!!    ");
  lcd.setCursor(0,1);
  lcd.println("  Invalid Card   ");
}
nuidPICC="";
  delay(5000); //Wait for 3 seconds before another swip
```

```
    digitalWrite(LedSuccess,HIGH);
    digitalWrite(LedFailure,HIGH);
    analogWrite(buzzer,buzzerOff);
   digitalWrite(Solonoid,LOW);
}
/**
 * Helper routine to dump a byte array as hex values to Serial.
 */
void printHex(byte *buffer, byte bufferSize) {
  for (byte i = 0; i < bufferSize; i++) {
    Serial.print(buffer[i] < 0x10 ? " 0" : " ");
    Serial.print(buffer[i], HEX);
  }
}

/**
 * Helper routine to dump a byte array as dec values to Serial.
```

```
 */

void printDec(byte *buffer, byte bufferSize) {

  for (byte i = 0; i < bufferSize; i++) {

    Serial.print(' ');

    Serial.print(buffer[i], DEC);

  }

}
```