Design and Implementation a Smart Door Lock based on Arduino

A Graduation Project Is Submitted To Al-Mustaqbal University College in Partial Fulfillment of the Requirements for the Degree of Bachelor of Science in Computer Techniques Engineering Department

By B.Sc.

ياسر مهند كاظم

علي حازم فاضل

غدير سعد احمد

هشام محمد فارس

رفيف سمير عبد المنعم

محمد قاسم نوماس

Supervisor Name

م.د.ليث عبد الكريم حسناوي

Babylon, Iraq

2023-2024

DEDICATION

To My Father and Mother

To My Supervisor

To My family

Supervisor's Certificate

*I certify that this thesis entitled "**Design and Implementation a Smart Door Lock based on Arduino**" has been prepared under my supervision at Computer Techniques Engineering Department, Al-Mustaqbal University College – Iraq, as a partial fulfillment of the requirements for the degree of Bachelor of Science in Computer Techniques Engineering Department.*

Signature

Dr. Layth Abdulkareem Hassnawi

2024/ 4 /

Acknowledgements

(In The Name of Allah, The Gracious, The Merciful)
(Thanks to Allah for his guidance and help)

I wish to express my deep gratitude to my supervisor for his invaluable help, advice and encouragement during the various stages of the present work.

My grateful acknowledgment is due to My father and My mother for their assistance and patience.

Finally, I record my sincere gratitude to all those who have helped me throughout this research even by a one word.

2024

TABLE OF CONTENTS

Abstract

Advancements in information technology, communications, and security pose significant challenges to modern societies. This research aims to design and implement a smart door lock system utilizing RFID and fingerprint recognition technologies in addition to Arduino microcontroller. The system seeks to provide a secure and efficient mechanism for access control to specified buildings or rooms.

Key components of the system include the main control unit based on Arduino, an RFID reader for user identification, and a fingerprint reader device. These components are integrated meticulously through custom programming to ensure security and efficiency in the door unlocking and locking process.

The system has been tested on a small scale using a prototype model, and preliminary results have demonstrated the system's effectiveness in achieving the required security and ease of use. This research is expected to contribute to the development of access control technologies in general and enhance security solutions used in various fields such as commercial enterprises and smart homes.

CHAPTER ONE

1. Introduction

Automated assimilation and access control system has turned out to be important to defeat the security dangers looked by numerous organizations. This is a time where everything is associated with the system, where anybody can get hold of data from anyplace around the globe. Therefore, hacking of one's information is a major issue. Because of these dangers, it is imperative to have some sort of personal identification (ID) to get to one's own particular information. Different systems are introduced at various points to track the individual's movement and to confine their entrance to touchy zones in the secured area.

Among standard individual ID strategies, password and ID card methods are the most observed methods. However, it is not very difficult to hack secret password now and recognizable ID cards may get lost, hence making these techniques very questionable [1]. Again, Radio frequency identification (RFID) is a remote innovation that can be utilized to evolve the entrance control system. This technology provides a revolutionary automation in various processes ranging from industrial sectors to home control [2-3]. In RFID technology, the identification of an object automatically consists of the object, location of the object or individual with a special identifier code contained with an RFID tag, which is somehow connected to or implanted in the target [4]. Because of the shaky wireless channel between RFID tag and RFID reader, security dangers against RFID system have been showing up. Numerous RFID verification conventions against the security dangers have been studied in [5].

The biometric security system is being used for a long time as a strong security system in different spaces. Numerous strategies are accessible in biometrics like the fingerprint, eye iris, retina, voice, confront and so forth. These distinctive strategies have certain focal points and inconveniences which must be considered in creating the biometric system, for example, system unwavering quality, value, adaptability, need of physical contact with the checking gadget and numerous different parameters [6]. Fingerprints are one of the numerous types of biometrics, used to distinguish people and check their identity.

The use of fingerprint for acclimatizing has been used in law prerequisite for about a century [7-8]. The investigation of fingerprints for matching purposes requires the correlation of a few highlights of the print pattern. These incorporate patterns include total qualities of edges, and minutia focuses. It is additionally important to know the structure and properties of human skin keeping in mind the end goal to effectively utilize a portion of the imaging advancements [9].

In this research, efforts have been made to use both RFID and biometric modes simultaneously to provide more safety and stronger security to access the automatic entity sensing and perform verification of the identity of the accessed entity as well as automatic operation in case of correct access. A person has to punch the RFID-tagged card and press their finger on the sensor where their fingerprint has to be verified to be matched immediately to access the security system. The motivation behind this work is to create a more convenient way to open the door than a traditional key. The RFID card and fingerprint will replace the key to unlock the door instantly. If an intruder somehow manages to get hold of an RFID card reader, they won't be able to access the door with their fingerprint because it won't match. Even the RFID reader won't be activated until the fingerprint is recognized. Therefore, it remains almost impossible for an invalid to enter.

2. Problem Statements

Using traditional keys represents a big problem in door locks since these keys may be lost or may be duplicated by unauthorized persons, on the other hand, the using of RFID is not enough since the technique may be stolen. Therefore, RFID and fingerprint were used to verify biometrics because it is something unique for each individual and using fingerprint as a key for door locks can overcome the security problem of unauthorized people entering our homes, shops, offices, etc. to a great extent. Since duplication of such a key is not possible. This system will also not lead to problems such as losing keys because we do not require carrying keys if using this system instead of traditional locks.

3. Objectives

The main objective of this research is to design and implement a robust authentication mechanism utilizing biometric fingerprint recognition and RFID technology to enhance security measures for door access.

CHAPTER TWO
Theory

2.1. RFID technology

RFID (Radio-Frequency Identification) technology traces its roots back to the early 20th century with the exploration of radio communication and automatic identification concepts.

However, real development began in the 1960s, culminating in the invention of the RFID prototype by Norman Joseph Woodland and Bernard Silver in 1969. Originally envisioned as a replacement for barcodes, RFID's practical application was limited until the 1980s when advancements in computer and wireless communication technology expanded its use, particularly in logistics and supply chain management.

By the end of the 20th century, the launch of the Electronic Product Code (EPC) standard in 1999 by the Auto-ID Center in the United States facilitated the standardization and commercialization of RFID technology [23].

2.2. System design

The proposed security system is designed to utilize both RFID technology and a fingerprint sensor as access keys for entry. The system works by keeping the RFID reader active and the fingerprint scanner ready at the door, acting as a locking mechanism. Access is only granted upon presentation of a valid RFID card and matching fingerprint. An exterior photographic view of the system is shown in Figure 1.

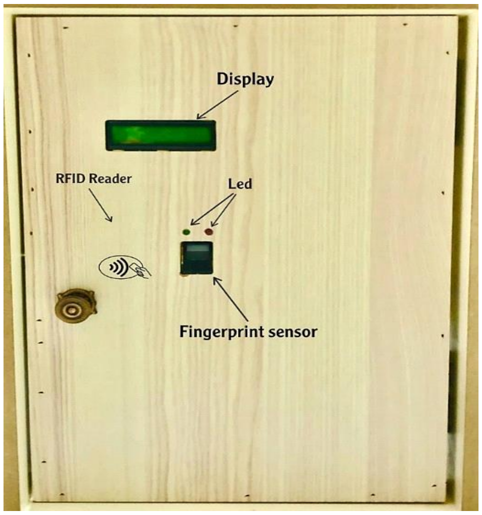


Figure 1. External view of the system

The internal circuit design as shown in Figure 2consists of several components including an RFID reader module, a fingerprint sensor, a relay, an Arduino UNO, 12V batteries, a display, an electronic lock, and a breadboard. All of these components are connected and the power supply is provided by wires.

The Arduino UNO is powered by 5 volts from the battery and powers the sensors. The electronic lock, which requires 12 volts to operate, is connected to both the battery and the relay internal circuit diagram:

The integrated approach combines the strengths of RFID and biometric authentication, enhancing security while providing an easy-to-use access control solution.

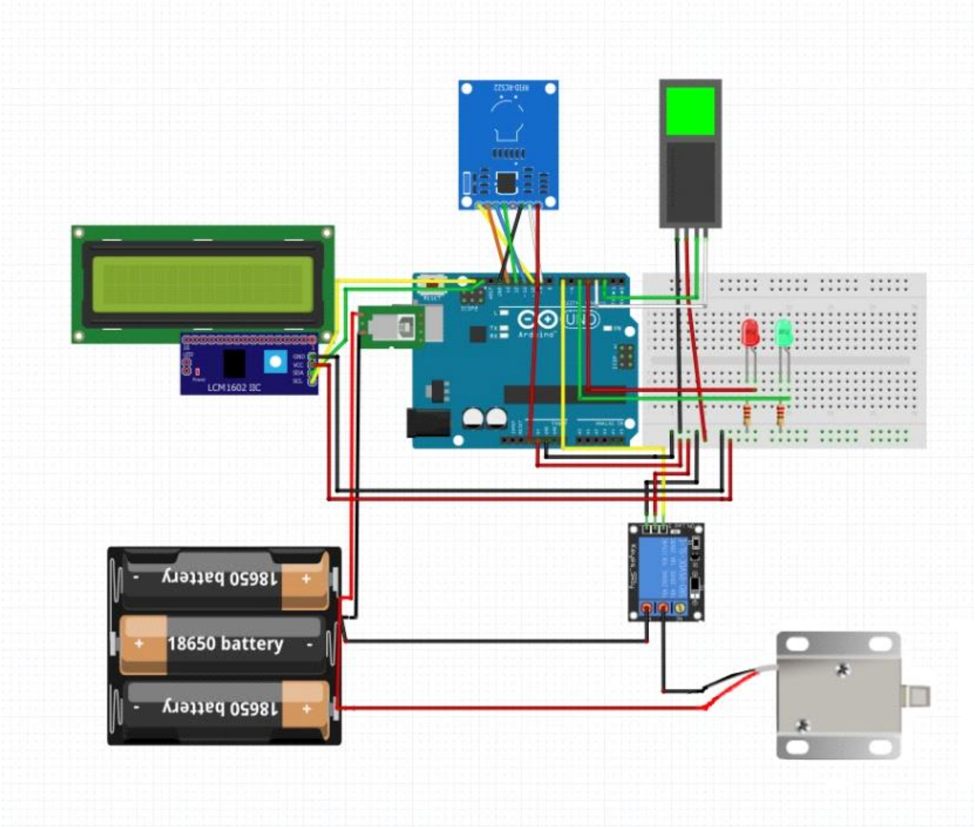


Figure 2: Circuit Diagram of the system

2.3. System Components

The designed security system consists of into six basic components: Arduino, Relay, Electronic lock, a display, RFID unit, and fingerprint unit. Each component has its prominent use with subtle functionality.

2.3.1. Arduino Board

Arduino is an open-source platform designed for building digital devices and interactive objects capable of sensing and controlling physical devices. In this project, the Arduino UNO version serves as the microcontroller device for operating the functions of the proposed security system. The Arduino UNO is equipped with a microcontroller known as ATmega328P, offering digital and analog inputs and outputs that enable interaction with various devices and sensors. Programming the Arduino is facilitated through the Arduino programming language, which is user-friendly and based on the C/C++ programming language.

2.3.2. Relay

A relay is an electrical device used to control the switching on and off of electrical loads. As shown in figure 3, the relay consists of a coil and two main switches that work together to connect or disconnect an electrical circuit. When an electric current is applied to the coil, a magnetic field is generated that attracts the moving terminals of the two switches, and the electrical circuit in the relay is closed by sending a signal from the Arduino to the coil.

2.3.2.1. Relay components

Frame: A heavy-duty frame that contains and supports the relay parts. Coil: An insulated copper wire wrapped around an iron core. Armature: A moving part called an armature: It opens and closes the contacts. Spring: A spring that returns the Armature to its original position. Contacts: There are open and closed contacts that open or close the circuit. Mounting base: The relay is installed on its own mounting base and there are some types that are installed on printed electronic cards.

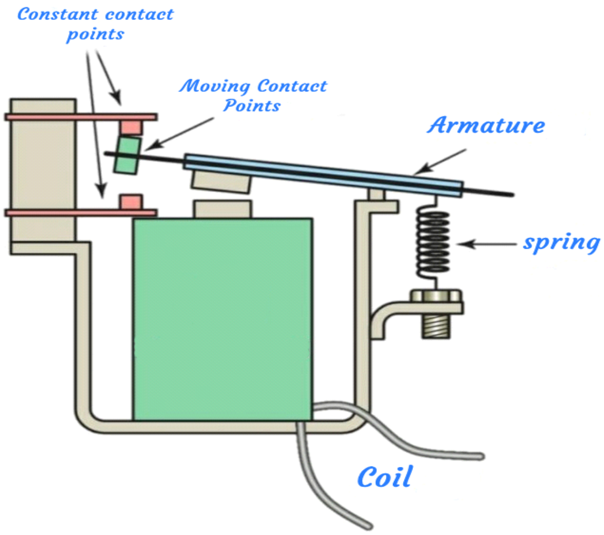
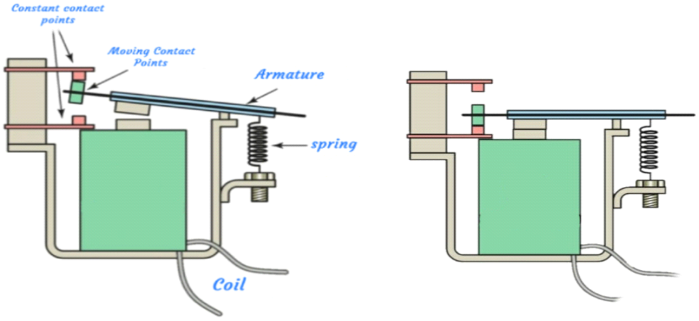


Figure 3: Relay components

2.3.2.2. Relay Operation

As shown in figure 4, when there is no current through the coil, the armature is kept away from the coil core by the tension created by the spring. When current is applied to the coil, an electromagnetic field is generated. This field, in turn, attracts the Armature. The movement of the armature causes open points NO to change to closed, and open points NC to change to closed. The points remain in this new state as long as voltage is applied to the coil, and when the voltage is disconnected from the coil, the contacts revert to their original position.



non-conductor of electricity

conductor of electricity

Figure 4. How a Relay Work

2.3.2.3. Relay Contact Points

In general, there are four types of relay terminals Coil points: Two terminals that are connected to control the relay's switching mechanism. A low-power source is connected to these terminals to energize (turn on) and de-energize the relay. The source can be AC or DC depending on the type of relay. Common Point COM: COM refers to the common terminal of the relay. This is the Output terminal of the relay where one end of the load circuit is connected. This point is internally connected to one of the open or closed points depending on the state of the relay.

Normally Open NO is a point that connects to the load and remains open when the relay is not active and when the relay is energized, the point changes to closed. Normally Closed NC Another point that connects to the load and is closed when the relay is inactive and when its coil is energized by connecting it to the current, the point changes to open.

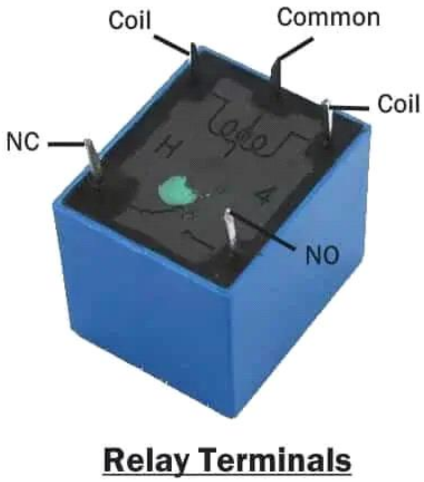


Figure 5.Relay Contact Points

2.3.3. Relay applications

There are many application used relay such are:

- Used to isolate a low-voltage circuit from a high-voltage circuit.
- They are used to control multiple circuits.
- Used for automatic switching of circuits.
- Overload relays are used to protect the motor from overload and electrical faults.

CHAPTER THREE

Design Methodologies

3.1. Connecting the Relay and Electronic Lock to the Arduino

As shown in figure 6, We use one of the Arduino's digital output pins to send a signal from the Arduino to the relay. We connect the (positive) end of the coil to the Arduino's positive voltage source (VCC), which is usually 5V. Then we connect the negative end of the coil to ground (GND) on the Arduino. We use an external 12-volt voltage source to connect the jumpers to the relay. We connect the positive wire from the external voltage source to the positive terminal of the electrical lock. Then we connect the negative lead from the external voltage source to the NO (normally open) terminal of the relay. Then connect the negative lead of the Electronic Lock to the COM (Common Point) terminal of the relay.

When the digital output port associated with the coil is turned on in the Arduino, the coil will turn on and therefore the switch in the relay will turn on. When the digital output port is turned off, the coil will be turned off and the switch in the relay will be disconnected.

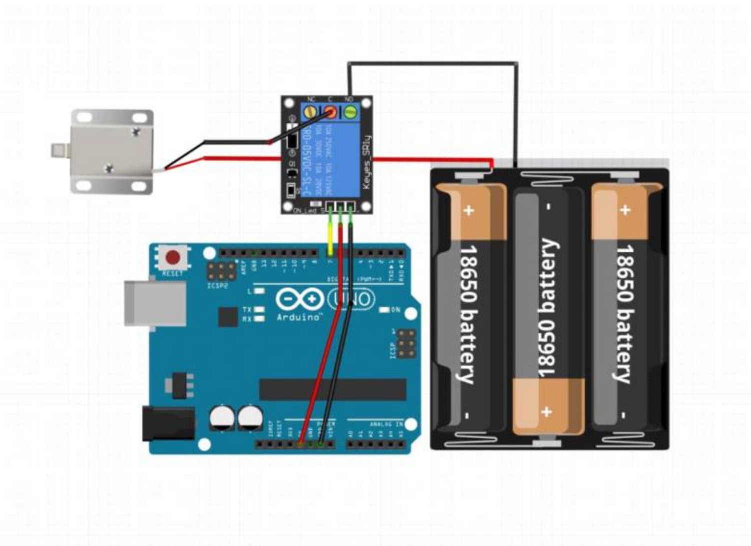


Figure 6: Connecting Relay and Electronic look to the Arduino

3.2. RFID Unit

The RC522 RFID module based on MFRC522 IC from NXP is one of the most inexpensive RFID options. It usually comes with an RFID card tag and key fob tag having 1KB memory, and best of all, it can write a tag. The RFID gadget fills an indistinguishable need from a standardized identification or an attractive strip on the back of a charge card or ATM card; it gives a one of a kind identifier to that protest. Furthermore, similarly as a scanner tag or attractive strip must be checked to get the data, the RFID gadget must be filtered to recover the recognizing data [14]. The examined data from RFID label go to RFID per user first. At that point, it is exchanged to microcontroller framework and changed over as database framework. This process of examining the data is used here to identify the validity of the person who is supposed to unlock the door. A stream chart of RFID task is appeared in following Figure 7.

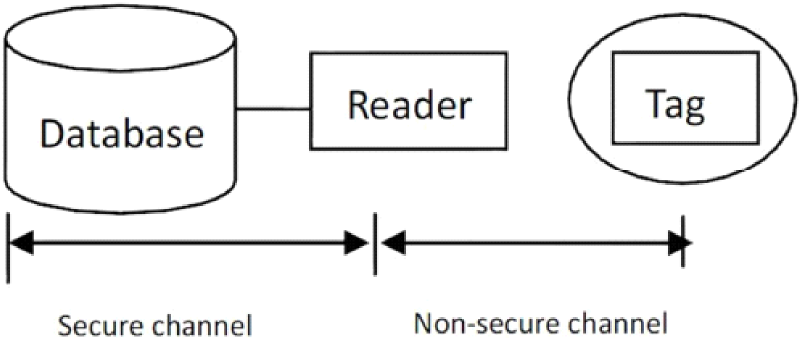


Figure 7: Flow diagram of RFID operation [15]

3.2.1. Working Principle of the RFID Reader

The RC522 RFID Reader module is designed to create a 13.56MHz electromagnetic field that it uses to communicate with the RFID tags (ISO 14443A standard tags). The reader can communicate with a microcontroller over a 4-pin Serial Peripheral Interface (SPI) with a maximum data rate of 10Mbps. It also supports communication over I2C and UART protocols.

The module comes with an interrupt pin. It is handy because instead of constantly asking the RFID module “is there a card in view yet? “, the module will alert us when a tag comes into its vicinity. The operating voltage of the module is from 2.5 to 3.3V, but the logic pins are 5-volt tolerant, so it can be easily connected to an Arduino or any 5V logic microcontroller without using any logic level converter [24].

3.2.2 RFID Module Pinout

The RC522 module has a total of 8 pins that interface it to the outside world [24]. The connections are as follows:

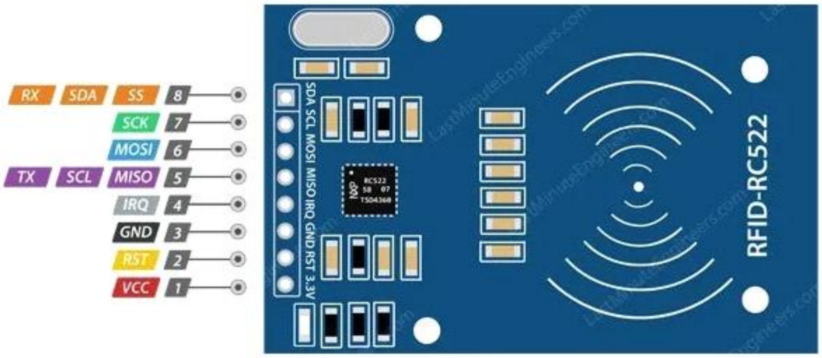


Figure 8: RC522 RFID Pins[24]

- **VCC** supplies power for the module. This can be anywhere from 2.5 to 3.3 volts. It can be connected to 3.3V output from the Arduino.
- **RST** is an input for Reset and power-down. When this pin goes low, hard power-down is enabled. This turns off all internal current sinks including the oscillator and the input pins are disconnected from the outside world. On the rising edge, the module is reset.
- **GND** is the Ground Pin and needs to be connected to the GND pin on the Arduino.
- **IRQ** is an interrupt pin that can alert the microcontroller when an RFID tag comes into its vicinity.
- **MISO / SCL / Tx** pin acts as Master-In-Slave-Out when SPI interface is enabled, acts as serial clock when I2C interface is enabled and acts as serial data output when UART interface is enabled.
- **MOSI** (Master Out Slave In) is SPI input to the RC522 module.
- **SCK** (Serial Clock) accepts clock pulses provided by the SPI bus Master i.e. Arduino.
- **SS / SDA / Rx** pin acts as Signal input when SPI interface is enabled, acts as serial data when I2C interface is enabled and acts as serial data input when UART interface is enabled. This pin is usually marked by encasing the pin in a square so it can be used as a reference for identifying the other pins.

3.2.3 Connecting the RFID Reader to the Arduino

To start hooking up the Arudino, connect the VCC pin on the module to 3.3V on the Arduino and GND pin to ground. The pin RST can be connected to any digital pin on the Arduino. Each Arduino Board has different SPI pins which should be connected accordingly [24].

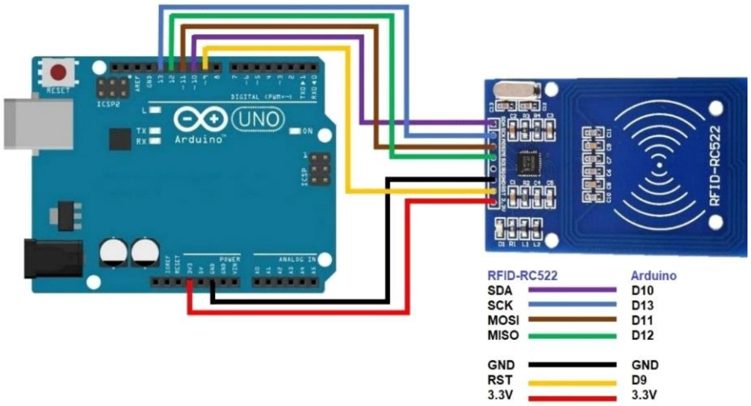


Figure 9:Wiring RC522 RFID Reader Writer Module with Arduino UNO

- **Components of RFID reader**

- **RFID antenna:** It is mainly responsible for converting the current signal in the reader into a radio frequency carrier signal and sending it to the RFID reader, or receiving the radio frequency carrier signal sent by the tag and converting it into a current signal. The design of the antenna affects the working performance of the reader. It is very important to say that for the tag, its working energy is all provided by the antenna of the reader[24].

- **RFID radio frequency interface module:** This module is the RF front-end of the RFID reader and is mainly responsible for transmitting and receiving. The modulation circuit modulates the signal to be sent and then sends it; the demodulation circuit amplifies the signal sent by the tag to ensure signal reception. .RFID radio frequency interface module is also a key part that affects the cost of the reader [24].

- **Reader logic control module:** The logic control module is the control center and intelligent unit of the entire reader. When the reader is working, the logic control module sends out instructions, and the interface module performs different operations according to different instructions. The microcontroller can complete signal encoding and decoding, data encryption and decryption, and execute anti-collision algorithms; the storage unit is responsible for storing some programs and data; the application interface is responsible for communicating with the input or output [24].

- **RC522 Features**

  - 13.56MHz RFID module
  - Operating voltage: 2.5V to 3.3V
  - Communication : SPI, I2C protocol, UART
  - Maximum Data Rate: 10Mbps
  - Read Range: 5cm
  - Current Consumption: 13-26mA
  - Power down mode consumption: 10uA (min)[25].

- **RFID Tag**

Radio frequency identification (RFID) or radio frequency identification tags are used for a variety of purposes and have become increasingly popular due to their versatility and ease of use. These tags consist of a small chip and an antenna as shown in Figure 10.

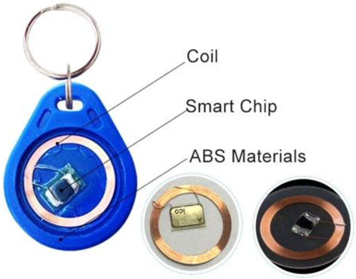
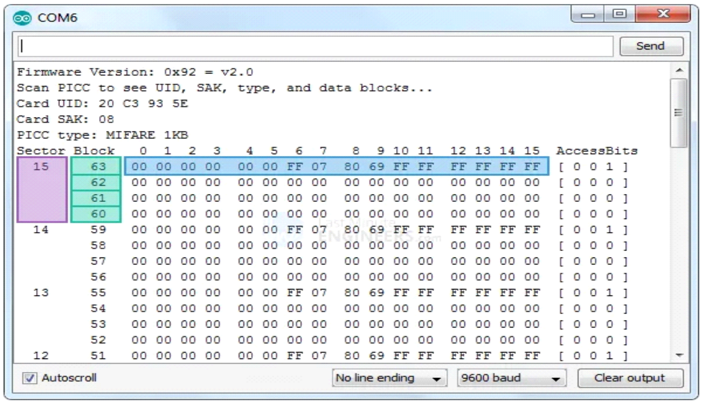


Figure 10: RFID Tag 125Khz components

RFID tags work by sending and receiving information via an antenna and a microchip (also known as an integrated circuit or IC) When an RFID tag is scanned by a reader, the reader sends energy to the tag allowing it to send the information stored in it to the reader. The reader sends this information to a computer program dedicated to handling RFID technology.

The 1K memory of the RFID Tag is organized in 16 sectors (from 0 to 15) Each sector is further divided into 4 blocks (block 0 to 3). Each block can store 16 bytes of data (from 0 to 15)[24]. 16 sectors x 4 blocks x 16 bytes of data = 1024 bytes = 1K memory



```
Firmware Version: 0x92 = v2.0
Scan PICC to see UID, SAK, type, and data blocks...
Card UID: 20 C3 93 5E
Card SAK: 08
PICC type: MIFARE 1KB
Sector Block   0  1  2  3   4  5  6  7   8  9 10 11  12 13 14 15  AccessBits
  15     63   00 00 00 00  00 00 FF 07  80 69 FF FF  FF FF FF FF  [ 0 0 1 ]
         62   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  [ 0 0 0 ]
         61   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  [ 0 0 0 ]
         60   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  [ 0 0 0 ]
  14     59   00 00 00 00  00 00 FF 07  80 69 FF FF  FF FF FF FF  [ 0 0 1 ]
         58   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  [ 0 0 0 ]
         57   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  [ 0 0 0 ]
         56   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  [ 0 0 0 ]
  13     55   00 00 00 00  00 00 FF 07  80 69 FF FF  FF FF FF FF  [ 0 0 1 ]
         54   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  [ 0 0 0 ]
         53   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  [ 0 0 0 ]
         52   00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  [ 0 0 0 ]
  12     51   00 00 00 00  00 00 FF 07  80 69 FF FF  FF FF FF FF  [ 0 0 1 ]
```

Figure 11: The whole 1K memory with sectors, blocks and data is highlighted[24]

The Block 3 of each sector is called Sector Trailer and contains information called Access Bits to grant read and write access to remaining blocks in a sector. That means only the bottom 3 blocks (block 0, 1 & 2) of each sector are actually available for data storage. Also The Block 0 of sector 0 is known as Manufacturer Block/Manufacturer Data contains the IC manufacturer data, and the Unique IDentifier (UID)[24].

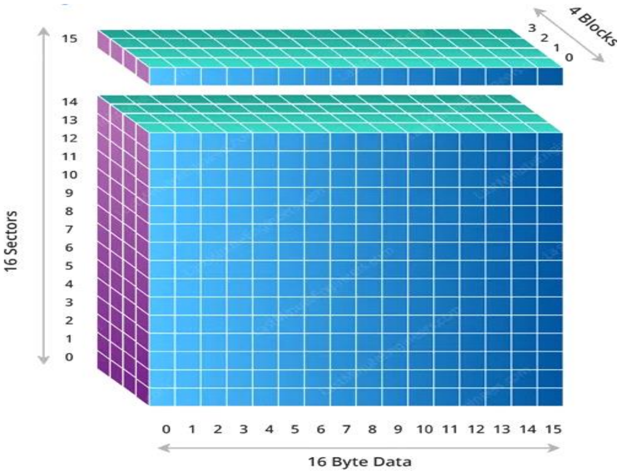


Figure 12: 3D Representation of MIFARE Classic 1K Memory Map Layout [24]

3.3 Fingerprint Unit

Fingerprint-based authentication is the most advanced and accepted biometrics technologies [16-19]. The fingerprint validation alludes to the robotized technique for checking a match between two human fingerprints. The processing of fingerprint has three essential functions: enrollment, searching, and verification. Among these functions, enrollment which catches fingerprint picture from the sensor assumes a critical part. A reason is that the way individuals put their fingerprints on a mirror to output can influence the outcome in the searching and checking process. This unit is utilized here to doubly secure the security system.

- **Optical fingerprint scanner working principle**

An optical fingerprint scanner works based on the principle of Total Internal Reflection (TIR). In such a scanner, a glass prism is used to facilitate TIR. Light from an LED (usually blue color) is allowed to enter through one face of the prism at a certain angle for the TIR to occur. The reflected light exits the prism through the other face where a lens and an image sensor (essentially a camera) are placed. When there is no finger on the prism, the light will be completely reflected off from the surface, producing a plain image in the image sensor. When TIR occurs, a small amount of light is leaked to the external medium and it is called the Evanescent Wave. Materials with different refractive indexes (RI) interact with the evanescent wave differently. When we touch a glass surface, only the ridges make good contact with it. The valleys remain separated from the surface by air packets. Our skin and air have different RIs and thus affect the evanescent field differently. This effect is called Frustrated Total Internal Reflection (FTIR). This effect alters the intensities of the internally reflected light and is detected by the image sensor. The image sensor data is processed to produce a high-contrast image which will be the digital version of the fingerprint. In capacitive sensors, which are more accurate and less bulky, there is no light involved. Instead, an array of capacitive sensors are arranged on the surface of the sensor and allowed to come in contact with the finger. The ridges and air packets affect the capacitive sensors differently. The data from the sensor array can be used to generate a digital image of the fingerprint [13].

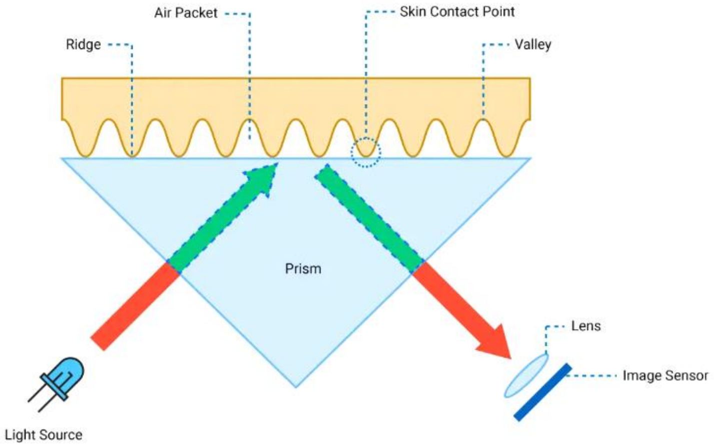


Figure 13:Optical fingerprint scanner working principle [13]

- **Components optical fingerprint sensor**

- Glass protective layer
- Illuminating light source (such as LEDs)
- Prism for reflecting light off the surface of the finger
- Lens for focusing the reflected light onto an image sensor camera (CCD or CMOS)
- Micro Control Unit (MCU) or Digital Signal Processor (DSP) for control, data conversion, and analysis
- UART, SPI, or USB interfaces for transferring digital data to a computer or mobile device [13]

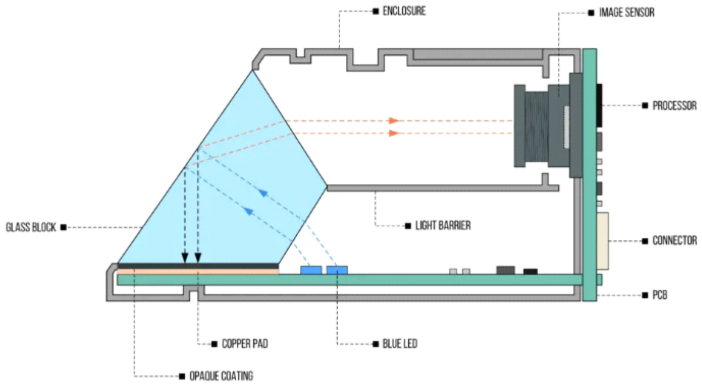


Figure 14: R307 Fingerprint Scanner cross-section [13]

- **Connecting fingerprint with Arduino**

The fingerprint sensor is connected to the Arduino

The red wire is connected to 5v and the black wire to the GND pin

The green wire is connected to pin 3 and the yellow wire

to pin 2 on the Arduino and as in the following Table 1

Table 1.Connect fingerprint with Arduino

V+(Red)	5V
TXD(Yellow)	Pin D2
RXD (Green)	Pin D3
GND (Black)	GND

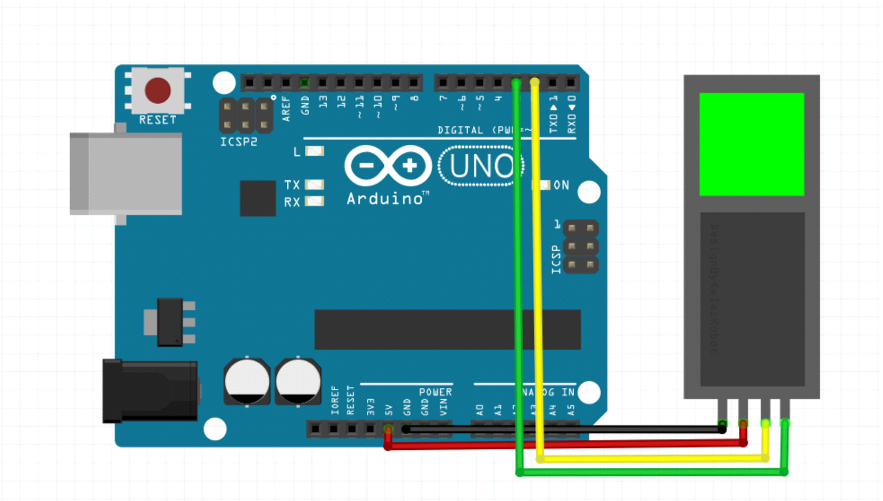


Figure 15. *Connect fingerprint with Arduino*

- **Working Principle of the System**

The working principle of the system is divided into three sections. They are detailed below:

- **RFID Card Punching and Operation**

RFID is a key and modest innovation that enables transmit information wirelessly [20]. RFID reader The Arduino's RFID reader module is powered by 5V. To connect RFID reader with the Arduino, five RFID wires are connected wires are connected to five digital ports of the Arduino. Both the grounding pin of the Arduino and the RFID reader are connected.

The RFID reader reads RFID labels, a controller is used to acknowledge information received from the RFID reader and control the output of the security door lock and LED. The RFID reader is set virtually from the input and is disconnected from the controller secretly so that no one can break the RFID reader to avoid security. The controller gets the controller in this task gets the serial data from the RFID reader and controls the door lock and LEDs.

- **Fingerprint Sensing**
- **Enrolling the Fingerprint**

A pattern of interleaved ridges and valleys are the main component of a fingerprint. They easily stream in parallel and once in a while end or bifurcate. The pattern of ridges and valleys can show a specific shape called minutiae at a local level [21]. There are a few kinds of minutiae as shown in Figure 16, yet for pragmatic reasons, just two sorts of details are considered: ridge ending and ridge bifurcation [6].

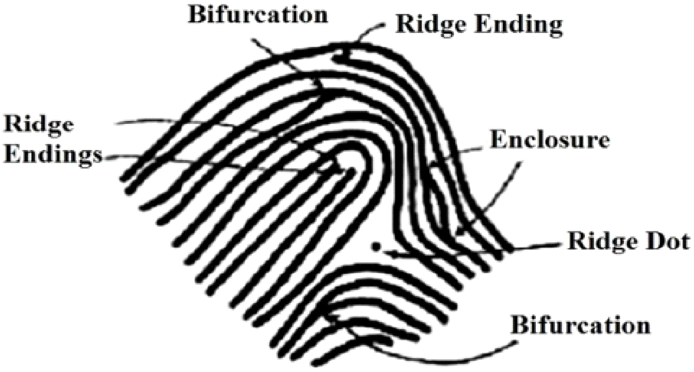


Figure 16. *Different ridge features on fingerprint image [11]*

There are fundamentally two prerequisites for utilizing the optical fingerprint sensor. Firstly, the fingerprints should be enrolled - that implies designating ID #'s to each print so that they can be checked later. Once enlisted all prints, the sensor can easily be searched by asking which ID (assuming any) is at present being shot. This enrollment is done by utilizing the windows programming software or with the Arduino programming.

3.4 Door control by electric lock

The electric lock works through an external power source (12V batteries) where the positive pole of the battery is connected to the positive pole of the electric lock and the negative pole of the battery is connected to the relay through the COM (Common Point) output to control the lock through the relay, where when the validity of both the RFID card and fingerprint is detected, a signal is sent to the relay through the Arduino via a wire connected to the digital pin 7 to connect the electrodes of the electric lock through the COM (Common Point) output on the relay, where when the two electrodes of the electric lock are connected to the positive pole of the battery A signal is sent to the relay through the Arduino via a wire connected to pin 7 to connect the poles of the electric lock through the COM (Common Point) output on the relay, where when the negative and positive poles of the lock are connected, the tongue is pulled by a magnet and the door is opened for 5 seconds. The poles are then disconnected through the relay and the tongue is no longer pulled by the magnet and the door closes

3.5 System construction

Emphasis is placed on electrical parts for a strong security system to prevent any invalid access to the door. The electrical part consists of Connecting the RFID module, fingerprint sensor module, electric lock, and relay connecting the Arduino board and connecting the overall circuit and providing a program to operate these electrical components by the required means. The system relies on both RFID and fingerprint. So if one system fails, the other system will back up the security. Both fingerprint and RFID are required to break the security. RFID system consists of an RFID reader and an RFID tag. When the fingerprint gets a valid fingerprint will activate the RFID reader and the RFID reader will command the lock when it gets a valid input. Only the fingerprint holder and RFID tag can unlock the system. The electric lock is also used for the door to be opened or closed.

3.6 Programming Code

```
#include <SPI.h>
#include <MFRC522.h>
#include <Adafruit_Fingerprint.h>
#include <Wire.h>
#include <LiquidCrystal_I2C.h>
#include <SoftwareSerial.h>


#define SS_PIN 10
#define RST_PIN 9

MFRC522 rfid(SS_PIN, RST_PIN);
SoftwareSerial mySerial(2, 3);
Adafruit_Fingerprint finger = Adafruit_Fingerprint(&mySerial);
LiquidCrystal_I2C lcd(0x27, 16, 2);

byte masterCard[4] = {0xC0, 0xF3, 0xD1, 0x1D};
byte masterCard1[4] = {0xFA, 0x92, 0x09, 0x6F};


int authorizedFingerprintID = 1;

int lockOutput = 7;
int greenLED = 5;
int redLED = 4;
int buttonPin = 6;


void setup() {
  Serial.begin(9600);
  SPI.begin();
  rfid.PCD_Init();
  finger.begin(57600);

  lcd.begin(16, 2);
  lcd.backlight();
  printWelcomeMessage();

  pinMode(lockOutput, OUTPUT);
  digitalWrite(lockOutput, HIGH);
  pinMode(greenLED, OUTPUT);
  pinMode(redLED, OUTPUT);
  pinMode(buttonPin, INPUT);
```

```
}

void loop() {
      int buttonState = digitalRead(buttonPin);{

  if (buttonState == HIGH) {
    digitalWrite(lockOutput, LOW);
    delay(5000);

    digitalWrite(lockOutput, HIGH);
    resetArduino();
  }
      }


  if (scanFingerprintAndCard()) {

    openDoor();
    delay(5000);
    closeDoor();
    resetArduino();

  }
}

bool scanFingerprintAndCard() {
  while (!finger.getImage()) {
  }

  uint8_t p = finger.image2Tz();
  if (p != FINGERPRINT_OK) return false;

  p = finger.fingerFastSearch();
  if (p == FINGERPRINT_OK && finger.fingerID == authorizedFingerprintID) {
    displayMessage("Place your RFID card...");

    while (!rfid.PICC_IsNewCardPresent()) {
      delay(100);

    }
    printWelcomeMessage();
    if (rfid.PICC_ReadCardSerial()) {
      for (byte i = 0; i < 4; i++) {
        if (rfid.uid.uidByte[i] != masterCard[i] && rfid.uid.uidByte[i] != masterCard1[i]) {

          digitalWrite(redLED, HIGH);
          displayMessage(" Access Denied!");
          delay(2000);
          digitalWrite(redLED, LOW);
          printWelcomeMessage();
          return false;

        }

      }
      return true;

    }
  }

  return false;
}

void openDoor() {
  digitalWrite(lockOutput, LOW);
  digitalWrite(greenLED, HIGH);
  displayMessage(" Access Granted!");
  delay(3000);
  printWelcomeMessage();

}

void closeDoor() {
  digitalWrite(lockOutput, HIGH);
  digitalWrite(greenLED, LOW);

}

void displayMessage(const char* message) {
  lcd.clear();
  lcd.setCursor(0, 0);
  lcd.print(message);
}

void printWelcomeMessage() {
  displayMessage("<Access Control>");
  lcd.setCursor(0, 1);
  lcd.print("Scan Your Fingerprint!");
}
```

```
void resetArduino() {
  asm volatile ("  jmp 0");
}
```

CHAPTER FOUR
Results and Conclusion

4.1 Performance Test

In order to verify the performance of the system, performance testing was performed in several steps, these are:

- Turn on the system.
- A finger is placed is placed on the fingerprint sensor.
- The fingerprint sensor takes an image of the finger and checks the fingerprint in the image with the pre-installed fingerprints, if the fingerprint in the image matches the pre-installed fingerprints, the RFID reader is activated.
- The RFID tag is placed near the RFID reader.
- If the RFID reader finds a valid RFID tag the Arduino microcontroller will confirm it as a valid tag and send a command to activate the relay, and the relay will connect the lock electrodes to pull the lock tab to open the door. The door will automatically close after 5 seconds
- So five seconds after the door opens, the Arduino will again command the relay to turn off the Electric Lock to close the door

4.2 Conclusion

The world is being modernized day by days and it needs a technological backup with stronger protection and security of valuable secret code, hiding data, and items. This research work has the very purpose of providing robust security system with automatic sensing and operating action to access or decline. It is a developed safety security and impermeable to baffle this security system. Security is maintained with sequential operation of RFID and fingerprint sensor and without the missing of one, an abscess is denied. This security system is cheaper, flexible, less time consuming and also needs not to commit any code or password to access. Fingerprint scanning and sensing can also be used to protect computer files and data. It is very reliable security system and can provide the highest security and automatic operation for any kind of user.

References

[1] J. Baidya, T. Saha, R. Moyashir and R. Palit, “Design and implementation of a fingerprint based lock system for shared access,” 2017 IEEE 7th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, NV, 2017, pp. 1-6.

[2] U. Farooq, M. Hasan, M. Amar, A. Hanif, and M. U. Asad, “RFID based security and access control system”, in International Journal of Engineering and Technology, Vol. 6, No. 4, August, 2014, pp. 309–314.

[3] L. Wu, W. W. Y. Ng, D. S. Yeung and H. L. Ding, “A brief survey on current RFID applications,” Proc. in International Conference on Machine Learning and Cybernetics, Baoding, 2009, pp. 2330-2335.

[4] Yu-Chih Huang, “Secure access control scheme of RFID system application” in Proc. Fifth International Conference on Information Assurance and Security, China, 2009.

[5] A. Juels, “RFID security and privacy: A Research survey, selected areas in communications”, IEEE Journal on Publication, Volume: 24, Issue: 2, Feb. 2006, pp. 381-394.

[6] I. Yugashini, S. Vidhyasri, K. Gayathri Devi, “Design and implementation of automated door accessing system with face recognition”, International Journal of Science and Modern Engineering (IJISME) ISSN: 2319-6386, Vol. 1, Issue-12, November 2013.

[7] O. Omidiora, O. A Fakolujo, O. T. Arulogun, D. O. Aborisade, “A prototype of a fingerprint based ignition systems in vehicles”, in European Journal of Scientific Research, Vol. 62, Issue 2, October, 2011, pp. 164.

[8] A. Kawale, "Fingerprint based locking system" in International Journal of Scientific & Engineering Research, Vol. 4, Issue 5, May-2013.
[9] R. P. Wildes. “Iris recognition: an emerging biometric technology”, Proceedings of the IEEE, vol. 85, no. 9, September, 1997, pp. 1348-1363.

[10] X. L. Meng, Z. W. Song, and X. Y. Li, “RFID-Based security authentication system based on a novel face-recognition structure,” in Proc. WASE International Conference on Information Engineering, 2010, pp. 97-100.

[11] D. L. Wu, W. W. Y. Ng, P. P. K. Chan, H. L. Ding, B. Z. Jing and D. S. Yeung, "Access control by RFID and face recognition based on neural network," Proc. in International Conference on Machine Learning and Cybernetics, Qingdao, 2010, pp. 675-680.

[12] L. H. Thai, H. N. Tam, “Fingerprint recognition using standardized fingerprint model” in International Journal of Computer Science Issues, Vol. 7, Issue 3, No 7, May 2010.

[13] Handson Technology User Guide (9 November 2021). HT AS608 Optical Finger Print Sensor Module User Guide. blog article retrieved from (https://device.report).
[14] S. L. Ting, S. K. Kwok, A. H. C. Tsang and G. T. S. Ho, “The Study on using passive RFID tags for indoor positioning tagged objects”, in International Journal of Engineering Business Management, Volume: 3, January 1, 2011, pp. 9-16.

[15] M. Wang, J. Pan, “Authentication test-based the RFID authentication protocol with security analysis”, Sensors & Transducers IFSA Publishing, S. L., Vol. 176, Issue 8, August 2014, pp. 196-202.

[16] N. K. Ratha, J. H. Connell, R. M. Bolle, “Secure data hyding in wavelet compressed fingerprint images”, ACM Multimedia workshop Marina Del Rey CA USA, 2000.

[17] A. Nagar, K. Nandakumar, A. K. Jain, “A hybrid biometric crypto system for securing fingerprint mutiae templates”, Pattern recognition Letters, Vol. 31, 2010, pp. 733-741.

[18] A. Farina, Z. M. Kovács-Vajna and A. Leone, “Fingerprint minutiae xtraction from skeletonized binary images,” Journal of the pattern recognition society, Vol. 32, Issue 5, Bologna Italy 1999, pp. 877-889.

[19] A. K. Jain, S. Prabhakar, L. Hong and S. Pankanti, "Filterbank-based fingerprint matching," in IEEE Transactions on Image Processing, vol. 9, no. 5, pp. 846-859, May 2000.

[20] F. L. Podio, “Personal authentication through biometric technologies”, in Proc. 2002 IEEE 4th International Workshop on Networked Appliances (Cat. No. 02EX525), Gaithersburg, MD, 2002, pp. 57-66.

[21] L. M. Mwaringa and T. Biketi. “Finger print based automotive security lock system.”, 2016 Annual Conference on Sustainable Research and Innovation, 4 - 6 May 2016, pp. 295-298.

[22] M. M. H. Ali, V. H. Mahale, P. Yannawar and A. T. Gaikwad, "Overview of fingerprint recognition system," 2016 International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT), Chennai, 2016, pp. 1334-1338.

[23] Website CXJ RFID Factory February 2, 2024 RFID History [https://www.cxjrfidfactory.com/rfid-history/]

[24] Ruthu S Sanketh (May 26, 2020). An Introduction to RFID, (AUTONOMOUS ROBOTICS) blog article retrieved from (https://medium.com).

[25] (June 20,2022.). What are the components of RFID reader/writer?, blog article retrieved from (https://www.marktraceiot.com).

[26] (12 June 2019). RC522 RFID Module. blog article retrieved from (https://components101.com).