Bank Locker System using Fingerprint, OTP and Threshold Weight

Vedant Naukarkar[1], Nishant Waghade[2], Shubham Dukale[3], Prof. Sarika. S. Patil[4]

[1]*Student, Department of ENTC, Sinhgad college of Engineering, Vadgaon, Pune*

[2] *Student, Department of ENTC, Sinhgad college of Engineering, Vadgaon, Pune*

[3]*Student, Department of ENTC, Sinhgad college of Engineering, Vadgaon, Pune*

[4]*Associate Professor, Department of ENTC, Sinhgad College of Engineering, Vadgaon, Pune*

[1]vedantnawkarkar2001@gmail.com, [2] nishant.waghade17@gmail.com , [3] Shubhamdukale2017@gmail.com

Abstract: *In this project, a bank locker system is presented that includes a weight threshold sensor as a crucial element for increased security. The system makes use of an Arduino Uno microcontroller, a weight threshold sensor, a GSM SIM900A module, and a fingerprint R307 sensor for biometric authentication. The solenoid lock open mechanism is only activated by the weight threshold sensor when a predetermined set weight is applied. The system's operations are managed and coordinated by the Arduino Uno, which acts as the system's central processing unit. By verifying users' identities using their fingerprints, the R307 sensor ensures secure access to the lockers. The GSM SIM900A module allows for real-time locker system monitoring and control via SMS instructions, enabling remote management and delivering prompt notifications and alerts. The system includes a weight threshold sensor to provide the highest level of security. It works by recognising when something has been placed on it and measuring the weight in relation to a predetermined threshold value. The inclusion of the weight threshold sensor improves the security of the bank locker system. The technology improves ease and lowers the chance of uninvited entrance by doing away with the need for conventional keys.*

Keywords: **Bank Locker, GSM, Fingerprint, Weight Sensor, Solenoid Lock, Arduino UNO.**

Introduction

In recent years, it has become more and more important to handle bank lockers securely and effectively. Traditional lock and key systems have accessibility and security drawbacks. This paper presents a comprehensive Bank Locker System that combines the powers of an Arduino Uno, a fingerprint R307 sensor, a GSM SIM900A module, and a weight threshold sensor in order to overcome these difficulties.

The suggested solution incorporates cutting-edge technology to improve the convenience and security of managing bank lockers. As the central processing unit, the Arduino Uno microcontroller enables the smooth coordination and management of diverse components. Only people with registered fingerprints who are authorised to access the lockers can do so thanks to the biometric authentication provided by the fingerprint R307 sensor. The GSM SIM900A module is integrated to enable communication through SMS commands for real-time monitoring and remote control. With the help of this tool, bank personnel may remotely regulate locker access, check system status, and receive notifications. This adds another level of convenience and control. A weight threshold sensor has been

integrated into the system, which is one of its noteworthy features. The device may weigh an object by placing it on the sensor, measure its weight, and compare it to a preset number. The solenoid lock won't unlock, granting safe access to the locker, until the weight exceeds the predetermined level. This novel method reduces the possibility of unauthorised access and improves the system's general security.

The benefits of the Bank Locker System go beyond security improvements. The technology improves ease for both bank customers and staff by doing away with traditional keys in favour of biometric authentication and remote monitoring. By automating the lock opening procedure based on weight criteria, the user experience is simplified and less manual intervention is required. This paper provides a thorough description of the Bank Locker System, emphasising its essential elements, features, and advantages for the banking sector. The system's architecture guarantees a strong and secure environment for the storage of priceless assets, giving clients piece of mind and maximising operational effectiveness for banks. The technical details of the system, such as the hardware configuration, software implementation, integration techniques, and performance evaluation, will be covered in the parts that follow. The goal is to show how useful and effective the suggested bank locker system is, bringing up new opportunities for research and development in the area of functional and secure locker administration.

Literature Review

[1]Surendra and Gopinath proposed a paper to provide a secured locker security system based on RFID, password, conveyer and GSM technology which can be organized in bank, secured offices and homes. This system allows authentic person only can be recovered money from locker. But if we lost the RFID tag means we are unable to withdraw our valuables.

[2]Swetha.S. Joshi proposed a paper which is basically a controller-based access control system which allows only authorized person to access the locker with GSM technology is used to send the password to the authorized person’s mobile phone via SMS. But the disadvantage is anyone can access the OTP and it is not securable for the user.

[3]R.Ramani (2012) et al. described a bank locker security system based on RFID and GSM technology which can be organized in bank, secured offices and homes. In this system only authentic person can be recovered money from bank locker. We have implemented a bank locker security system based on RFID and GSM technology containing door locking system using RFID and GSM which can activate, authenticate, and validate the user and unlock the door in real time for bank locker secure access. The main advantage of using passive RFID and GSM is more secure than other systems. microcontroller, which will verify the passwords entered by the key board and received from authenticated mobile phone. if these two passwords are matched the locker will be opened otherwise it will be remain in locked position, This system is more secure than other systems because two passwords required for verification. This system also creates a log containing check-in and check-out of each user along with basic information of user.

Table 1: Study of Literature Reviews

Name of Authors	Proposed System	Drawbacks
Surendra and Gopinath	RFID, password, conveyer and GSM technology.	No withdrawals could take place once RFID tag is lost.
Swetha. S. Joshi	Locker with GSM Technology	OTP is vulnerable once number is theft or lost.

R. Ramani	Locker with RFID and GSM	Maintenance cost

Methodology

The project's methodology used an Arduino Uno, a fingerprint sensor (R307), a GSM SIM900A module, and a weight threshold sensor to create a reliable and safe bank locker system. This section outlines the primary approaches used throughout the project and gives an overview of the methodical approach we used to accomplish our goals. The Bank Locker System was developed using a number of crucial techniques, each of which addressed a certain component of the system's operation, security, and user experience. System design, hardware configuration, software development, testing and calibration and result were all covered by these approaches.

Block Diagram

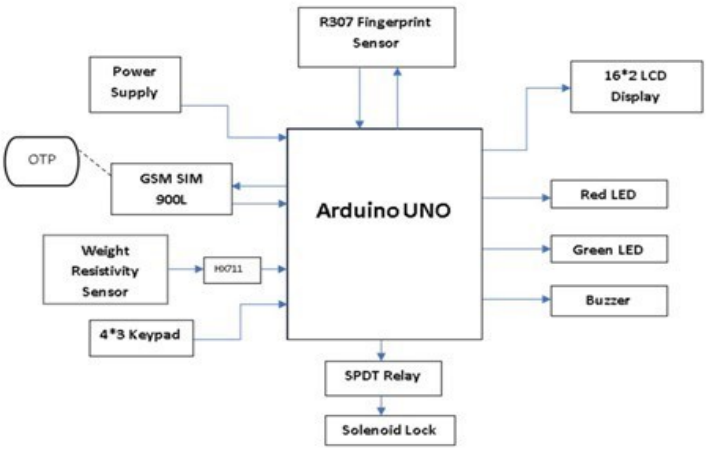

Fig.1: Block Diagram of Proposed System

Description:

(1) Arduino UNO: The boot loader that comes pre-installed on Arduino microcontrollers, such the Arduino UNO, makes it easier to upload programmes to the on-chip flash memory. The Opti boot loader is the default boot loader for the Arduino UNO. Programming code is loaded onto boards using a serial link to another computer. A level shifter circuit can convert between logic levels and transistor-transistor logic (TTL) level signals on some serial Arduino boards.

(2) Fingerprint Sensor: The automated process of determining if two human fingerprints match is known as fingerprint recognition or fingerprint authentication. One of the various types of biometrics used to identify people and confirm their identities is fingerprinting. The fingerprint sensor used in this system is model R307.

(3) GSM Module: To identify the user’ s account, GSM phones utilise a SIM card. By simply switching the SIM card, GSM network users can swiftly transfer their phone number from one GSM

phone to another. Currently, the 850MHz, 900MHz, 1800MHz, and 1900MHz frequency bands are used by GSM networks.

(4) Solenoid Lock: A solenoid lock is an electromechanical device in which the locking mechanism is controlled by a solenoid. A metal pin or plunger is drawn towards the solenoid when an electrical current is delivered to it, creating a magnetic field. A door or other mechanism can be locked or unlocked using this movement of the pin or plunger.

(5) Threshold Weight Sensor: The predefined weight number that defines when the sensor will initiate a response or action is referred to as the threshold weight of the sensor. The needs and sensitivity of the system are used to determine this threshold weight. A locker is occupied or has had an object placed inside when the weight applied to the sensor reaches the threshold value. The system can then react suitably.

(6) Lcd display- A passive matrix display grid or an active-matrix display grid is used to create LCD displays. Every grid intersection on the passive matrix LCD is home to a conductor pixel grid.

(7) SPDT Relay: An electromagnetic switching device known as an SPDT (Single Pole Double Throw) relay has a single set of common (C) terminals, normally open (NO) terminals, and normally closed (NC)terminals.

(8) HX711 Amplifier: The HX711 is a precision amplifier intended for use with pressure sensors and weigh scales. The low-level analogue output signal from load cells or pressure sensors is amplified and converted precisely into a digital signal that may be processed by a microcontroller or other digital devices.

Methodology 1: R307 Fingerprint Sensor

Our fingertips have friction ridges that allow us to firmly hold objects without slipping. These distinctive patterns, which are made up of ridges and valleys, create a solid touch with surfaces. A fingerprint is an imprint made by our fingertips when we grab something; it is made up of moisture, oil, dirt, and dead skin cells. Total Internal Reflection (TIR) is the underlying principle behind how optical fingerprint scanners work. TIR is accomplished by permitting a certain angle of an LED's light to enter one face of a glass prism. The prism's other face, which includes a lens and an image sensor, is where the reflected light leaves the device. When there is no finger present, the prism completely reflects all of the light, producing a straightforward image on the sensor. A tiny amount of light known as the Evanescent Wave escapes during TIR and interacts with the surrounding medium. The refractive indices (RI) of various materials, such as the ridges on a glass surface or air pockets in the valleys, affect how they respond to the evanescent wave. The term "FTIR" (for Frustrated Total Internal Reflection) refers to this phenomenon.

The R307 fingerprint sensor module extracts patterns from fingerprints using a special algorithm. The creator of this algorithm has not disclosed its inner workings to the public hence its specifics are unclear. However, we may assume that the programme examines the ridges and valleys of a fingerprint to extract a distinctive pattern that can be used for identification or verification by fusing image processing techniques with pattern recognition algorithms.

Fingerprint Extraction is done via Minutiae fingerprint point feature extracting technique.

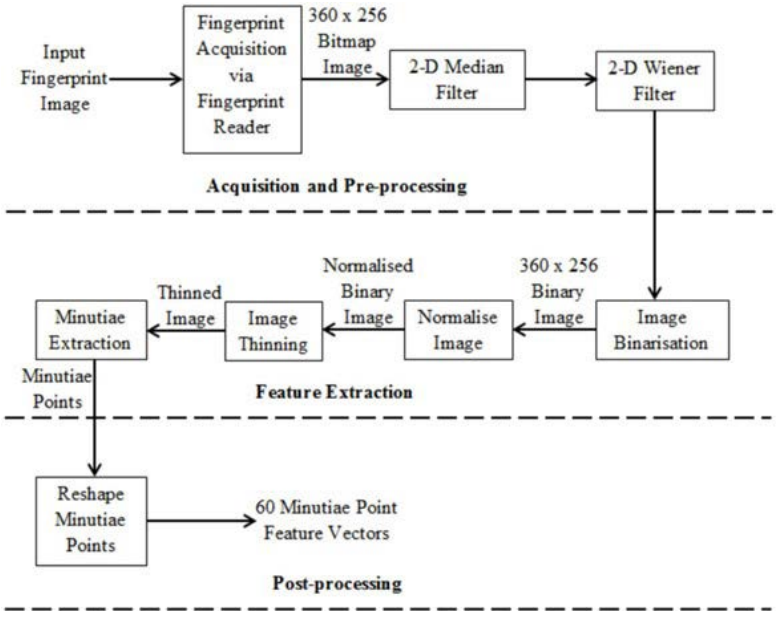

Fig. 2: Steps for Minutiae fingerprint point feature extracting technique.

Interfacing Arduino UNO with R307 Fingerprint Sensor

The scanner can be interfaced and powered from both 3.3V and 5V supplies. The working voltage of the scanner controller is always 3.3V. There's a 3.3V regulator on the PCB. The 5V supply you provide goes to the input of that regulator, and the 3.3V you supply bypasses the regulator and goes directly to the fingerprint scanner controller. The R307 has both USB and UART interfaces. With the USB, you can directly connect the scanner to a computer and communicate with it. A virtual COM port will be created when you connect the scanner to a Windows PC. If you want to interface the scanner with a microcontroller, you can use the UART interface which supports baud rates up to 115200 bps.

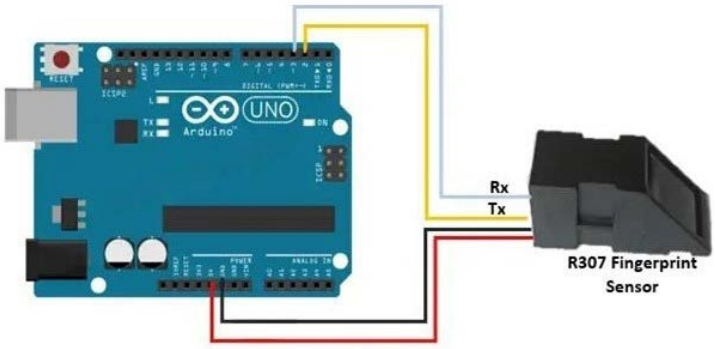

Fig.3: Interfacing between R307 and Arduino UNO

Steps to follow in Arduino IDE after Interfacing Hardware:

1. Initialize the module, install Adafruit fingerprint library, set proper pins in the code and edit according to the project need and initialize the serial port.
2. Start enrolling the fingerprint and store it in the library code which will be included in the main project code later by giving the ID number.
3. After running the main code put the correct enrolled finger on the sensor and fingerprint sensor will react accordingly.

Methodology 2: GSM SIM900A Module

SIM900A Modem by SIMCOM is based on a Dual Band GSM/GPRS modem. It operates at 900 and 1800 MHz. The SIM900A can automatically search these two bands. Additionally, AT Commands can be used to set the frequency bands. Through the AT command, the baud rate is programmable between 1200-115200. To allow you to connect with the internet through GPRS, the GSM/GPRS Modem has an inbuilt TCP/IP stack. A complete GSM/GPRS module in an SMT type, the SIM900A is developed with a very powerful single-chip CPU combining an AMR926EJ-S core, allowing you to take advantage of tiny dimensions and affordable solutions. The SIM card gives the module the identifying and authentication details it needs to connect to the cellular network.

The SIM900A module's capability for Short Message Service (SMS), which facilitates text-based communication between the module and other devices, is one of its important features. It is helpful for applications like automatic warnings, remote control, and data exchange because it can send and receive SMS messages.

To enable GSM connection, the GSM SIM900A module is a hardware component that may be interfaced with microcontrollers or other embedded systems. It doesn't have a single algorithm per se, but instead uses a variety of algorithms to perform various operations like encryption, decryption, error checking, etc. The SIM900A module uses the following algorithms:

1. A5 encryption algorithm: An industry-standard encryption method called A5 is used in GSM communication to protect voice and data communications.
2. Viterbi decoding: method used in GSM communication to repair errors. It aids in the recovery of lost or damaged data that was transmitted.
3. Frequency hopping algorithm: This GSM communication approach reduces interference and boosts security. It entails periodically adjusting the broadcast signal's frequency.
4. Automatic Gain Control (AGC) algorithm: to change the gain of the signal amplifier in response to the strength of the received signal.
5. Echo cancellation technique: The SIM900A module uses the to get rid of any echoes that can appear while transmitting voice.

Interfacing GSM Sim900A with Arduino UNO

1. Power supply: Join the GSM module's VCC and GND power supply pins to the Arduino Uno's 5V and GND pins. Verify that the power supply voltage is within the operational range of the module.
2. Communication Interface: Connect the Rx pin of the GSM module to the Tx pin (pin 1) of the Arduino Uno and the Tx pin of the GSM module to the Rx pin (pin 0) of the Arduino Uno to create a communication interface. These connections allow the module and the Arduino to communicate serially.
3. Antenna: An external GSM antenna should be connected to the GSM module's antenna connector for the best possible signal strength and reception.
4. SIM Card: Place a functional SIM card in the GSM module's SIM card slot. Activate the SIM card and verify that it has enough credit or a subscription to support communication.
5. Code: Write an Arduino programme to control a GSM module. The Software- Serial library must be utilised in order to establish serial communication with the module. Make a SoftwareSerial class instance and specify the appropriate RX and TX pins for the module. To send and receive data or carry out other actions with the module, use the proper AT commands.

6. Test and Confirm: Open the Serial Monitor in the Arduino IDE and upload the code to the Arduino Uno. Verify that the Serial Monitor's baud rate corresponds to the baud rate specified in the code. Sending AT commands and waiting for the GSM module to respond will test the communication.

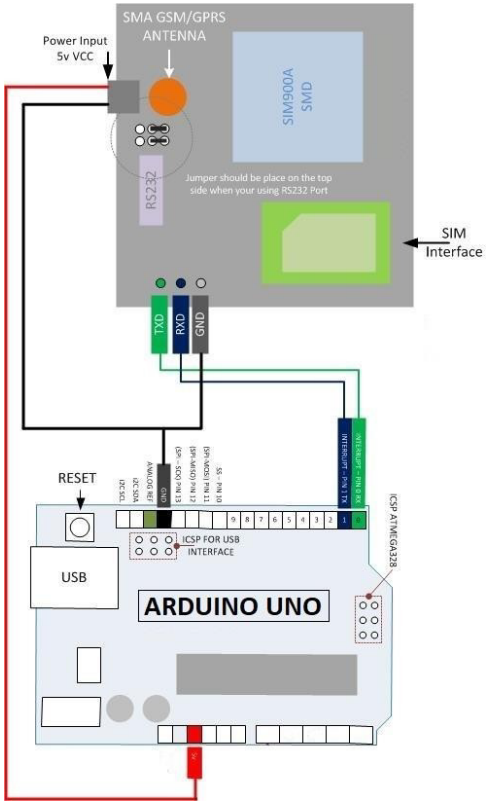

Fig.4: Interfacing GSM Sim900A module with Arduino uno

Step to follow upon successful interfacing of GSM module to the Arduino:

1. Setup Software serial communication for GSM module.
2. Use the gsmSerial object to send AT commands to the GSM module. Sending the command "AT" and anticipating a "OK" return, for instance, will allow you to verify the module's response and confirm that communication has been established.
3. Use different AT commands to manage the GSM module's features, including phone calls, SMS messaging, and cellular network connections.
4. Perform other tasks like sending an OTP to desired number.

Methodology 3: Weight Threshold Sensor

A load cell typically has a metal body with linked strain gauges. The metal body of the load cell deforms somewhat when a force is applied, changing the resistance of the strain gauges. An amplifier or signal conditioner can measure the change in resistance, which is proportional to the force given to the load cell, and transform it into a digital signal. Load cells are frequently employed in industrial, commercial, and scientific settings where exact and precise weight or force measurements are necessary.

Scales, weighbridges, material testing devices, and industrial automation systems are just a few of the many tools and gadgets that use them. A specific kind of weight sensor called a threshold weight sensor is made to recognise when a predetermined weight threshold is reached or surpassed. A binary output is provided if the measured weight has not yet crossed a predefined limit. Threshold weight sensors are frequently employed in applications where it is vital to keep track of whether an object's weight varies from predetermined limits. They provide a reliable and accurate means to detect when a predetermined threshold is crossed, making them essential for maintaining quality, safety, and efficiency in various industries.

(1). Assume for the moment that the load cell sensor in the image above has the four internal strain gauges A, B, C, and D.

(2). The C and D corners of the bridge are used to supply the input voltage from a signal conditioner or digital display. At the same time, the A and B resistors are connected to the digital display's signal side to measure the output voltage.

(3). The circuit is stated to be balanced when there is no load placed on the load cell (Load=0). The strain gauge resistors will experience a change in resistance as soon as the load is applied to them, which will change the voltage flowing through the circuit.

(4). As a result, the voltage across A and B will fluctuate, changing the weight that is shown on the readout unit or digital display.

(5). The output of a load cell or a Wheatstone bridge is analogue data that is translated into readable units by an interpreter.

(6). The output voltage from the load cell is amplified and digitalized by the HX711 amplifier module before being read by the Arduino microcontroller. The solenoid lock can then be controlled by the Arduino using this knowledge.

(7). Strain Gauges are small, elastic stainless-steel objects that are fixed within load cells using specialised adhesives. Its length and width are directly proportional to the strain gauge's specific resistance.

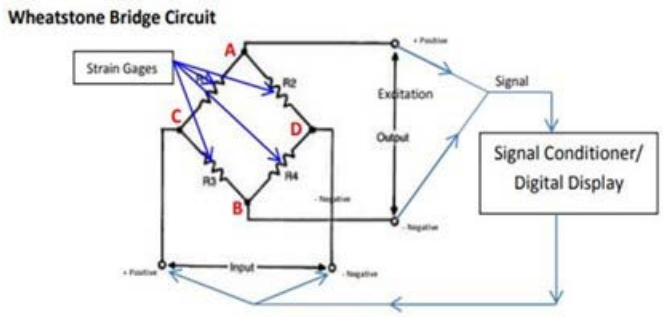

Fig. 5: Wheatstone Bridge mechanism

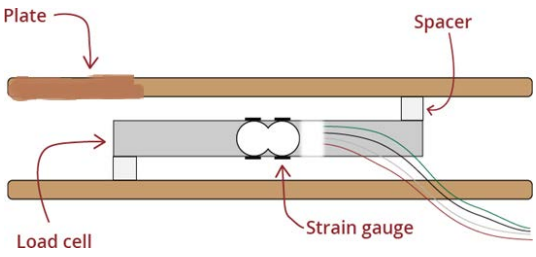

Fig. 6: Load cell implemented on flat surface

Interfacing Weight Sensor with Arduino UNO

• The" E+" pin, which stands for" excitation voltage positive," is attached to the positive terminal of the external power source that supplies the load cell with the excitation voltage.

• The" E-" pin, which stands for" excitation voltage negative," is attached to the negative terminal of the external power source that supplies the load cell with the excitation voltage.

• A- (load cell signal negative): This pin is linked to the load cell's negative signal wire.

• A+ (load cell signal positive): This pin is linked to the load cell's positive signal wire.

• VCC (5V power supply): The Arduino Uno board's 5V power source or an external power source is connected to this pin. The HX711 module receives electricity from this pin.

• The ground (GND) pin on the Arduino Uno board or an external power source is linked to this pin. This pin completes the circuit for the load cell and HX711 module.

• DT (data output): The HX711 module's digital output signal is sent to the Arduino Uno microcontroller using this pin.

• SCK clock signal: The HX711 module receives it's via the (clock input) pin, which is used to synchronise data flow between the module and the Arduino Uno.

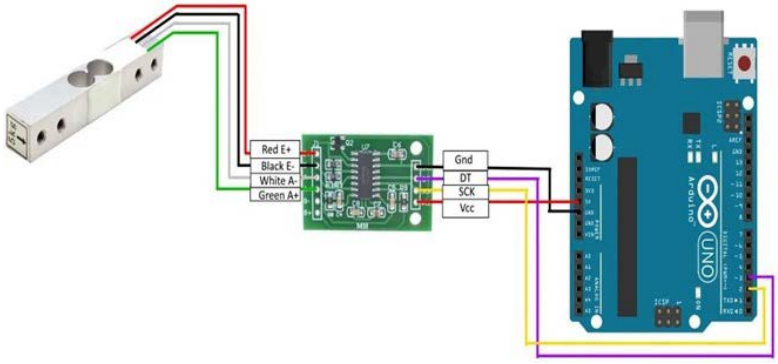

Fig. 7: Interfacing Weight Sensor with Arduin UNO

Flowchart

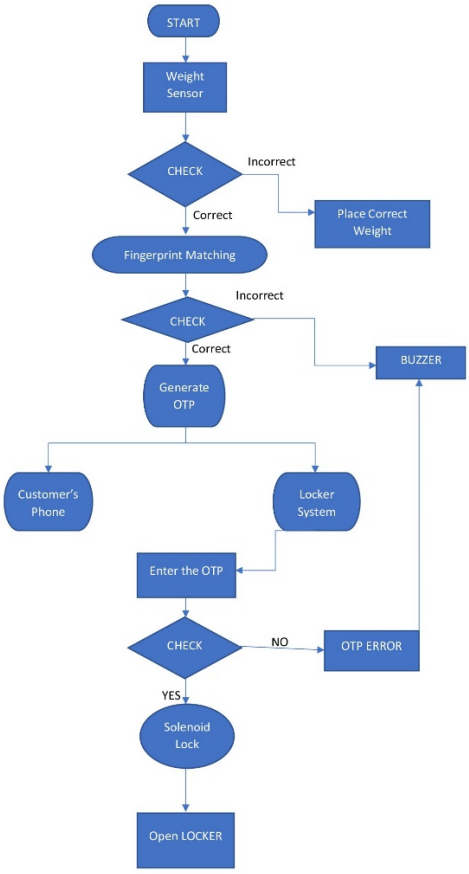

Fig. 8: Flowchart of Proposed System

Schematic Diagram

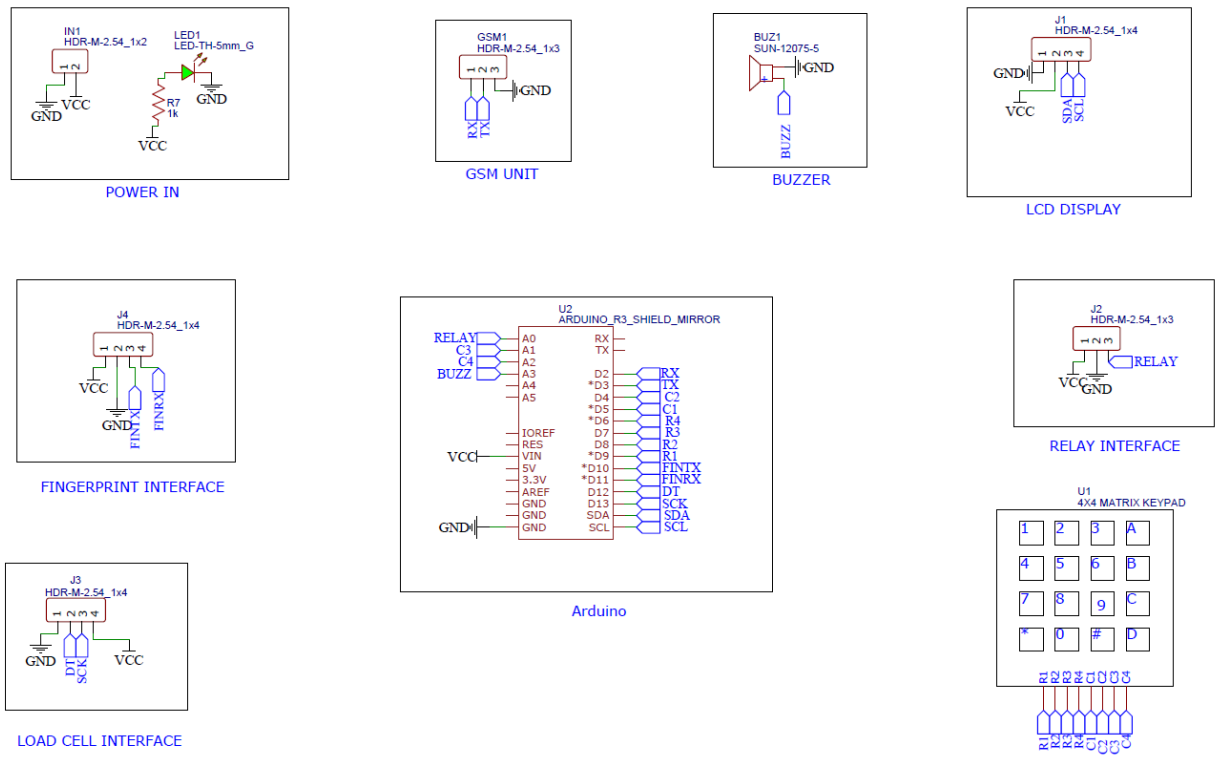

Fig. 9: Schematic Diagram of Proposed System

Results

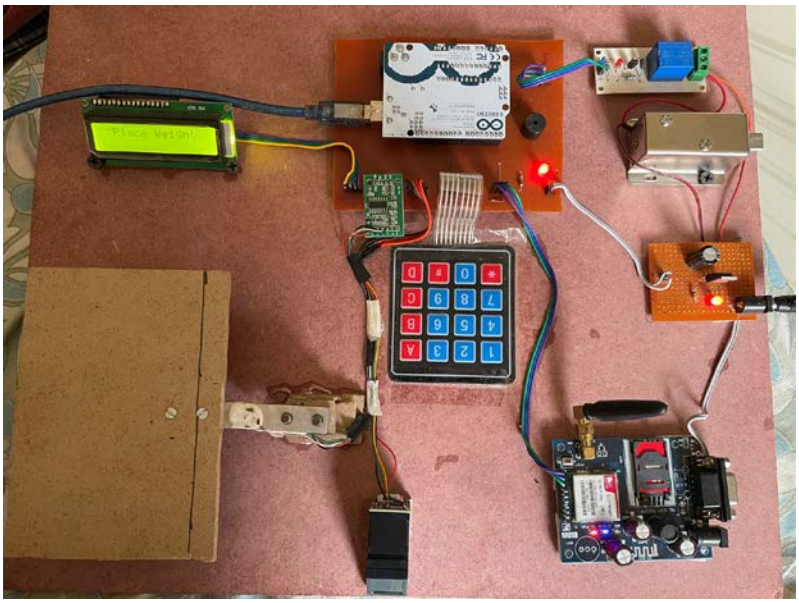

Fig. 10: Project Overview

Steps for Result

Step 1: Power ON the project using an external power adapter and interface Arduino UNO to the laptop via USB cable, after connection check whether GSM Initialization is successful in Arduino

IDE. The predetermined value for the weight sensor is 1000g with a calibration factor of 6.86, Hence by applying a weight of 1000g (Here a 1 litre Water Bottle) the weight sensors will trigger.

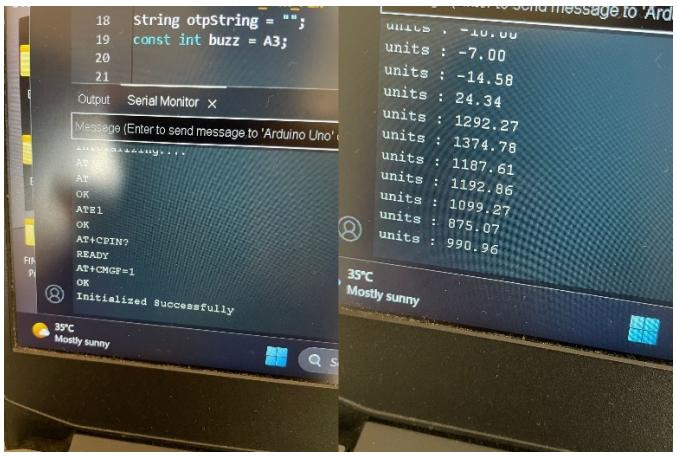

Fig. 11: Initializing and taking reading of applied weight.

Step 2: After correct weight is recognised by the weight sensor, it grants access and an “ACCESS GRANTED” message in LCD and 2 sec of Buzzer Buzz can be heard.

Fig. 12: By applying correct weight lcd display ACCESS GRANTED message.

Step 3: After Weight Sensor, LCD displays a message” Scan Finger”. After Putting a Fingerprint on R307 Fingerprint Sensor, the sensor will verify the fingerprint authenticity and display either a” Fingerprint Matched” or “Fingerprint not Matched” message on the LCD display if the Fingerprint is correct or incorrect respectively. If the Fingerprint is incorrect the buzzer will buzz for 3 seconds.

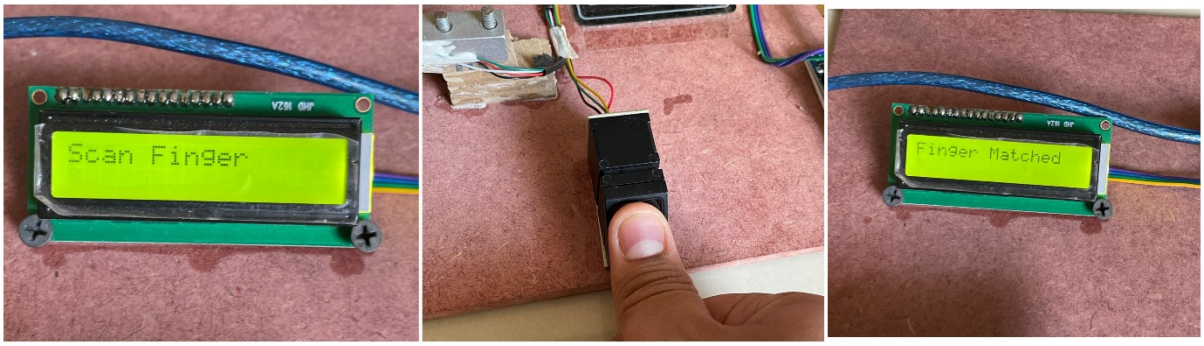

Fig.13: Scanning Fingerprint

Step 4: After authenticating the Right Fingerprint of the Customer, The GSM Module gets triggered and sends an OTP (One-Time Password) to the customer’s registered mobile number. After sending the mobile number, a message is displayed on LCD as “Enter OTP:”.

Fig.14: Sending and Entering received OTP via 4*4 KEYPAD.

Step 5: Providing the correct OTP will trigger the solenoid lock with a buzzing sound for 1sec and display a" LOCKER UNLOCKED" message on the LCD display if an incorrect OTP is Entered LCD displays" INCORRECT OTP" and the buzzer triggers for 3 seconds and thus doesn't trigger the Solenoid Lock. After triggering of Solenoid Lock, Lock automatically locks itself again after a 3-second time period.

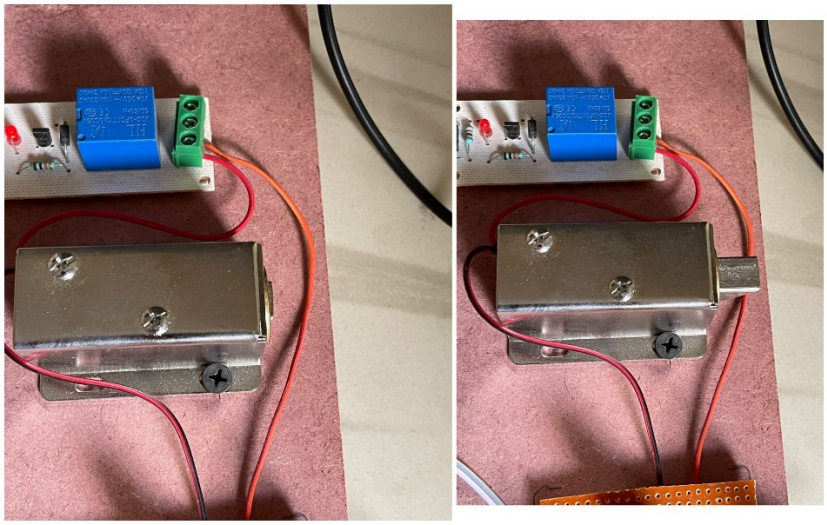

Fig.15: Lock opened and closed automatically upon certain time interval.

Conclusion

A 3-layer security system is difficult to create. In particular, coding the three distinct sensors independently, adjusting them to the Arduino UNO, and then successively producing the best result possible all have an impact on the project' s proper operation. Microcontrollers like the Arduino UNO are capable of achieving this, but the coding of such components is key, so finishing the project with the model that was envisioned in the mind and making it available to the public is an important step towards creativity. It is also necessary to keep a record of who accessed the locker when, including the date and time. All of this will enable banks to make use of the massive amounts of labour currently wasted on maintaining the locker system in the banking industry.

Future Scope

1. IoT and Smart Devices: The future application of such a banking locking system may include integration with smart home automation and Internet of Things (IoT) devices. For instance, the system might be combined with smart locks, giving users the freedom and convenience of accessing their banking facilities from any connected device.
2. Personalised and Convenient Banking: Using fingerprint authentication makes banking more individualised and practical. Customers may securely access their accounts and complete transactions using their individual biometric data, doing away with the need for PINs or conventional passwords.
3. Fraud prevention: The integration of weight sensor, fingerprint, and OTP technologies helps thwart a variety of frauds, including identity theft and account takeover.

References

[1] J. Soares and A. N. Gaikwad, "A self-banking biometric machine with fake detection applied to fingerprint and iris along with gsm technology for otp," in 2016 International Conference on Communication and Signal Processing (ICCSP), pp. 0508-0512, 2016.

[2] P. C. K.N. Joshi, "A survey of cancellable biometric based key generation scheme using various cryptography techniques," International Journal of Computer Sciences and Engineering, vol. 6, pp. 380-383, 3 2018.

[3] N. R. Kisore and S. Sagi, "A secure SMS protocol for implementing digital cash system," in 2015 International Conference on Advances in Computing, Communications and Informatics (ICACCI), pp. 1883-1892, IEEE, 2015.

[4] J. Jeong, M. Y. Chung, and H. Choo, "Integrated otp-based user authentication scheme using smart cards in home networks," in Proceedings of the 41st Annual Hawaii International Conference on System Sciences (HICSS 2008), pp. 294- 294, IEEE, 2008.

[5] A. Chikara, P. Choudekar, D. Asija, et al.," Smart bank locker using fingerprint scanning and image processing," in 2020 6th International Conference on Advanced Computing and Communication Systems (ICACCS), pp. 725-728, IEEE, 2020.

[6] A. C. Lomte," Biometric fingerprint authentication with minutiae using ridge feature extraction," in 2015 International Conference on Pervasive Computing (ICPC), pp. 1-6, IEEE, 2015.