Journal for Educators, Teachers and Trainers
The PROFESIOLab electronic, peer-reviewed, open-access Magazine

ISSN 1989-9572

DOI: 10.47750/jett.2023.14.04.33

SMART IOT-ENABLED MULTI-LAYERED SECURITY FRAMEWORK FOR ADVANCED BANK LOCKER PROTECTION

Dr. P Rama Koteswara Rao1, D Satheesh1, Dr G. Ravindranath Kumar1

Journal for Educators, Teachers and Trainers, Vol. 14 (4)

https://jett.labosfor.com/

Date of reception: 15 June 2023

Date of revision: 04 July 2023

Date of acceptance: 05 Aug 2023

Dr. P Rama Koteswara Rao1, D Satheesh1, Dr G. Ravindranath Kumar1 (2023). SMART IOT-ENABLED MULTI-LAYERED SECURITY FRAMEWORK FOR ADVANCED BANK LOCKER PROTECTION. Journal for Educators, Teachers and Trainers, Vol. 14(4)392-405

Journal for Educators, Teachers and Trainers, Vol. 14(4)
ISSN 1989 –9572

https://jett.labosfor.com/

SMART IOT-ENABLED MULTI-LAYERED SECURITY FRAMEWORK FOR ADVANCED BANK LOCKER PROTECTION

Dr. P Rama Koteswara Rao[1], D Satheesh[1], Dr G. Ravindranath Kumar[1]

[1]Department of Electronics and Communication Engineering

[1]Sree Dattha Institute of Engineering and Science, Sheriguda, Hyderabad, Telangana

ABSTRACT

A highly efficient, conflict-free address scheme was developed for a memory-based Fast Fourier Transform (FFT) processor, designed to optimize performance and reduce computational complexity. The approach leverages a high-radix decomposition method to minimize computation levels while integrating small-radix, connected multipath-delay-commutator butterfly units to simplify the processing engine. Key functionalities such as continuous-flow operation, adaptable computation size, and an efficient conflict-free addressing mechanism were seamlessly combined. To further optimize performance, a prime factor algorithm was employed, significantly reducing the number of multiplications and minimizing twiddle factor storage, especially when prime factors were present in the decomposition. Additionally, a unified Winograd Fourier Transform Algorithm (WFTA) butterfly core was designed to efficiently handle small Discrete Fourier Transforms (DFTs) of 2, 3, 4, and 5 points, further cutting down computational overhead. Simulation results demonstrated that the FFT processor consumed only 40.8 mW of power when operating at a frequency of 122.88 MHz, making it highly energy-efficient and well-suited for LTE applications

Keywords: IOT, Multi-layer security, Fingerprint lock, Fraud Prevention

1.INTRODUCTION

Banks are synonymous with high security, playing a vital role in safeguarding valuables such as important documents, expensive jewelry, cash, and other assets. In today's world, where banking transactions have become an integral part of daily life, bank lockers serve as a critical solution for financial and personal security. With rapid advancements in technology and increasing public demand, banks are continuously expanding, necessitating enhanced security measures to protect their customers' assets. As banking services become more autonomous, security threats also evolve, requiring innovative and multi-layered protection mechanisms. Research indicates that modern security systems must integrate reliable devices and technologies to ensure accountability and prevent breaches. The rise of digital banking and the increasing reliance on automated services further highlight the need for robust security infrastructures. With the expansion of banking networks and the continuous development of security protocols, implementing advanced, technology-driven solutions has become imperative to stay ahead of potential threats. Strengthening bank security with innovative

measures ensures that institutions can continue to offer safe and reliable services while adapting to the ever-changing landscape of financial security. In automatic security systems generally, passwords, identification cards and PIN verification techniques are being used but the disadvantage is that the passwords could be hacked and a card may be stolen or lost. The most secure system is fingerprint recognition because the fingerprint of one person ever matches the other. Biometrics studies commonly include fingerprint, voice, signature, and hand geometry recognition and verification. Many other modalities are in various stages of development and assessment. Among the available biometric traits fingerprint proves to be one of the best traits providing a good mismatch ratio, and high accuracy in terms of security and reliability. A biometric system is nothing but a pattern or feature extraction and authentication technique. That feature database is already stored and input will be matched with the already stored feature. Biometric systems run in two ways verification or identification. While recognition involves comparing the acquired biometric information against that stored in the database, verification involves the matching of both. That is why we are motivated to do this paper. Therefore, the study shows all the approaches intended to solve the desire problem of security in critical systems of an institution with proper authorization. Such systems are only accessible by the design at users and not by the masses. Moreover, the solution must ensure the obstruction of all possible ways of violation of security within the periphery of the secured area. It is also expected to regulate the access to certain users divided into different capacity groups. The Internet of Things (IoT) has dramatically changed the way we approach home security. With the advent of connected devices and smart technology, it is now possible to monitor and secure your home remotely using a smartphone or computer. Consolidate functionality in one place the security of money in the bank, home or office. overwhelm security. Threat, most people install a series of locks or alarm systems. There are many types of alarm systems on the market. We use different types of sensors. Sensors can detect different types of transformations that occur in the environment and environment. Transformation is handled to issue warnings according to preset values. It also lacks advanced security features. To solve this problem, All modern security features should be built into the locker including the feature to monitor it. The proposed project is an extended approach to the existing home security system. The accuracy of the system is taken from an Enter the Locker Security System. This Android application uses Internet of Things (IoT) technology to monitor the condition of your locker and enhance security. The system is based on an ESP32 microcontroller, which is installed along with a PIR sensor in the locker. The PIR sensor is used to detect movement, and the magnetic switches are used to know whether the door is locked or unlocked. If an intruder opens the locker by force, the sensors will detect the status of the locker door and the motion of his hand inside the locker. The data will then be uploaded to the firebase linked with the mobile app. If a burglary is detected, an alert notification message will be sent to the mobile immediately using the Twilit cloud, and the buzzer will also be activated in the mobile application. Any authorized user can use the app without alarm by entering the password manually, through which the system identifies the user and gives the authorized sound notification. The PIR sensor can detect the motion accurately up to 6 meters. With this system in place, you can rest assured that your belongings are safe.

2.LITERATURE REVIEW

Shruthi, CH M., Sai Kumar Bandari et.al [1] developed

As a priority in today's society, security is of the highest importance, and safeguarding our properties from intruders is no small task. The main objective of the offenders is to obtain valuable items kept in the locker. To address this issue, an Android application called Locker Security System uses Internet of Things (IoT) technology to monitor the locker's condition and enhance security. The project is based on an ESP32 microcontroller installed along with a PIR sensor implemented in the locker to

detect the movement and magnetic switches to know whether the door is locked or unlocked, When the intruder opens the locker by force it detects the status of the locker door using magnetic switch sensor and the motion of his hand inside the locker using PIR sensor, the data is uploaded to the firebase linked with the mobile app. If a burglary is detected, it sends an alert notification message to the mobile immediately using Twilio cloud and the buzzer is also rung in the mobile application.

Marie, Osama Amin et.al [2] Intelligent Security System

The use of many different sorts of security systems in our day-to-day lives has suddenly skyrocketed at a rate that is exponentially higher than before. Everyone living in this day and age is aware of the critical need to implement sufficient safety precautions in settings such as workplaces, organizations, and bank vaults. In recent years, companies have become increasingly interested in installing surveillance cameras to create workplaces that are less prone to danger. The fundamental objective of this research is to develop methods that are capable of improving the performance of traditional security systems. The platform-based security system that is based on the Internet of Things (IoT) has the potential to communicate in real time with the device. Components of the system include the speech sensor/microphone, motion/activity sensor, LTE/Wi-Fi module, and camera. Each of these sensors is interfaced with the central processing unit (CPU), which is the most important part of the system.

BALASUBRAMANİAN, Kishore et.al [3] developed

In this technologically evolving era, security plays a significant role in preventing different assets and crimes. This inconsistency developed an innovative idea to improve the level and solve the existing problems. This paper proposes a well-suited multilayer security system for homes, bank lockers, and more locations where we can use it. Traditionally, password and biometric double-layer security systems are used everywhere, but this embedded solution combines RFID, OTP, and fingerprint identification in sequence. Essential modules are connected and controlled through a microcontroller with a GSM module. Every operation done by the system is pushed to the IoT cloud, and the mobile application shows the status of every action. The right authorized access can let the magnetic switch open, and every unauthorized access turns on the alarm with appropriate message notifications. The Proposed system is more effective and reliable due to multistage security, and it is not easy to crack with the combination of all three stages. The whole system's workings are indicated by LED flashes. This implementation has shown better results and a higher performance rate than existing methods.

Sudarshan Akshaya, R. k Mohan Reddy B Srinivasa Ramya L.K [4] developed

High Protection Voice Identification Based Bank Locker Security System With Live Image Authentication B. Sudarshan Akshaya, R. k Mohan Reddy B Srinivasa Ramya L. K. When human beings were on earth, need of various things emerged. As years passed and with tremendous development people started earning money, property, jewellery and many more precious things. With huge development people felt a need to secure their earnings. In today’s a man’s life the money security is an important aspect as he earns the money by his hard work, and banking is known for this. It is not enough to have these accessories, but security of this is very important, for this purpose we keep them in a bank locker. Still, we often hear or read in a newspaper that some fake person has access the locker of another person and have stolen money. In order to overcome this type of frauds, authentication of the person who wants to use the locker is very important. To overcome this security threat, a security system has been proposed using voice identification, face detection and GSM technology.

Khokher, Bhawna, Mamta B. Savadatti et.al [5] developed

In today's world, security is a very important issue. People should always keep their belongings safe. To increase security, this research work proposes a IoT-based smart lockers with sensors and access keys with security, verification, and user-friendly tools. This model alerts the user when someone else tries to access their locker and quickly sends an alarm to the authorized user, and provides the option to either grant or reject access to the valid user. In this paper, smart locker is kept registered early to use a locker in the bank, office, home, etc. to ensure safety. The user demands to send an unlock direction with the help of microcontroller NUDE MCU ESP8266 and after accepting the command from the cloud (BLYNK APP), only the user can unlock the closet and access the valuables. This study has also introduced the encroachment detection in lockers with sensors and finally installed smart lockers with fire alarms for security and reliability

Raman, Ramakrishnan, S. Prabhakar et.al [6] developed

Nowadays, people often withdraw money from Automated Teller Machines (ATMs). Every user receives a unique card and personal identification code to perform all transactions secretly and anonymously. Developing an ATM crime prevention system is crucial to avoid theft. The proposed solution uses an embedded system using a Raspberry Pi to process the real-time data collected by the vibration sensor. In this instance, robberies are detected using a vibration sensor that hears buzzer sounds and senses vibration. The sensor provides information to a police station through the Internet of Things, and the main doors corresponding to the ATM close on their own so that the thief cannot be escaped. An IoT transmits data to a Wi-Fi module through a cloud server, which displays it in real-time. The mechanism alerts the bank staff automatically when an ATM is misplaced. Also, the proposed system uses cameras since they help us find theft suspects.

Dhanasekaran, S., S. Boopathy et.al [7] developed

Among the most common means of communication between haptic devices and humans nowadays is vibrating response. Important vibrational considerations must be looked into and used to haptic devices in order to precisely and effectively communicate a greater variety of data. In this article, we present a cutting-edge and reliable defense against side-channel attacks that aim to steal the PINs and other locker credentials. To strengthen the resistance to surveillance assaults, some PIN-entry mechanisms for portable devices based on audios and/or haptics have been created. Unfortunately, none of the PIN-entry systems currently in use can successfully combine high usability with strong protection against surveillance threats. In this article, we suggest Loc-Hap PIN, a new PIN-entry system that is immune to observation assaults and works with touchscreen devices that offer localized haptic feedback.

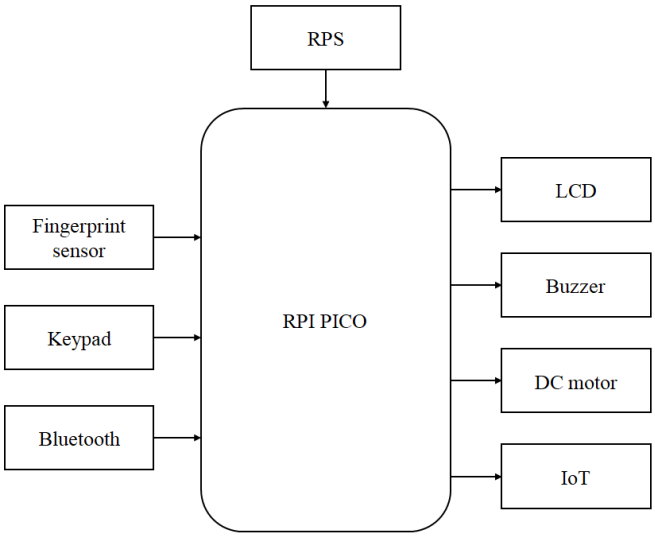
Wankhede, Nilashree et.al [8] Enhancing Biometric Speaker Recognition

While extensive research has been conducted in the field of biometrics, particularly in face and fingerprint recognition, remote speaker recognition has yet to gain global acceptance due to challenges related to accuracy and data integrity. Previous studies in speaker recognition have explored techniques such as Mel Frequency Cepstral Coefficients (MFCC) and Convolutional Neural Networks (CNN), yielding accuracy rates of 90.4% and 92.8%, respectively over a fixed and small database with a standalone system. To address the data integrity and accuracy issues for enhancement in remote speaker recognition, a novel approach is proposed in this paper. Initially, remote speaker recognition is implemented using a client-server setup, but the presence of channel noise hindered any noticeable improvement in accuracy compared to existing methods.

3.PROPOSED SYSTEM

In this project, we present a working model of IoT- Multi secure bank Locker access system. The main objective for implementing this project is to enhance the security of the locker**.** This multi-layer bank locker access system incorporates keypad password, finger lock, and voice authentication operates on the principle of multi-factor authentication. Implemented using IOT, RPI Pico microcontroller, keypad, RPS, LCD, buzzer, Arduino IDE tool, and embedded c language.

Block Diagram:



The working of the three level security system is explained here, a voice password is set during registration and converted to a text format for storage. The user is provided with a unique keypad password that they must memorize and this password is programmed. The keypad password is stored securely in the system. When the user wants to access their bank locker, the user need to enter the password that was initially set, once it is verified the first layer of authentication is successful and next process begins. In this step, the system prompts the user to place their finger on the fingerprint scanner. The fingerprint sensor captures the fingerprint, and the system compares it with the stored fingerprint template. Here we are using R305 If the fingerprint matches, the second layer of authentication is successful and the final process begins. In this step, the system prompts the user to speak their voice password. The voice detection system converts the spoken words into text using automatic speech recognition (ASR) technology. The converted text is compared with the stored text of the programmed voice password. If the text matches, the voice detection authentication is successful. If all authentication factors match successfully, the system grants access to the user's locker. The locker door unlocks, allowing the user to access their belongings. Every access attempt and successful access are logged for security and auditing purposes. The system maintains an audit trail to track and investigate any suspicious activities. The system may have timeouts to prevent unauthorized access in case of prolonged attempts. Security measures, such as alarms or notifications, may be triggered in case of repeated failed authentication attempts or any suspicious activities. This multi-layered approach combines different authentication factors to provide a robust and secure access control mechanism for bank lockers, reducing the risk of unauthorized access. Throughout the process, all details will be displayed in the LCD display.

Project Working:

In this system there are totally five sections:

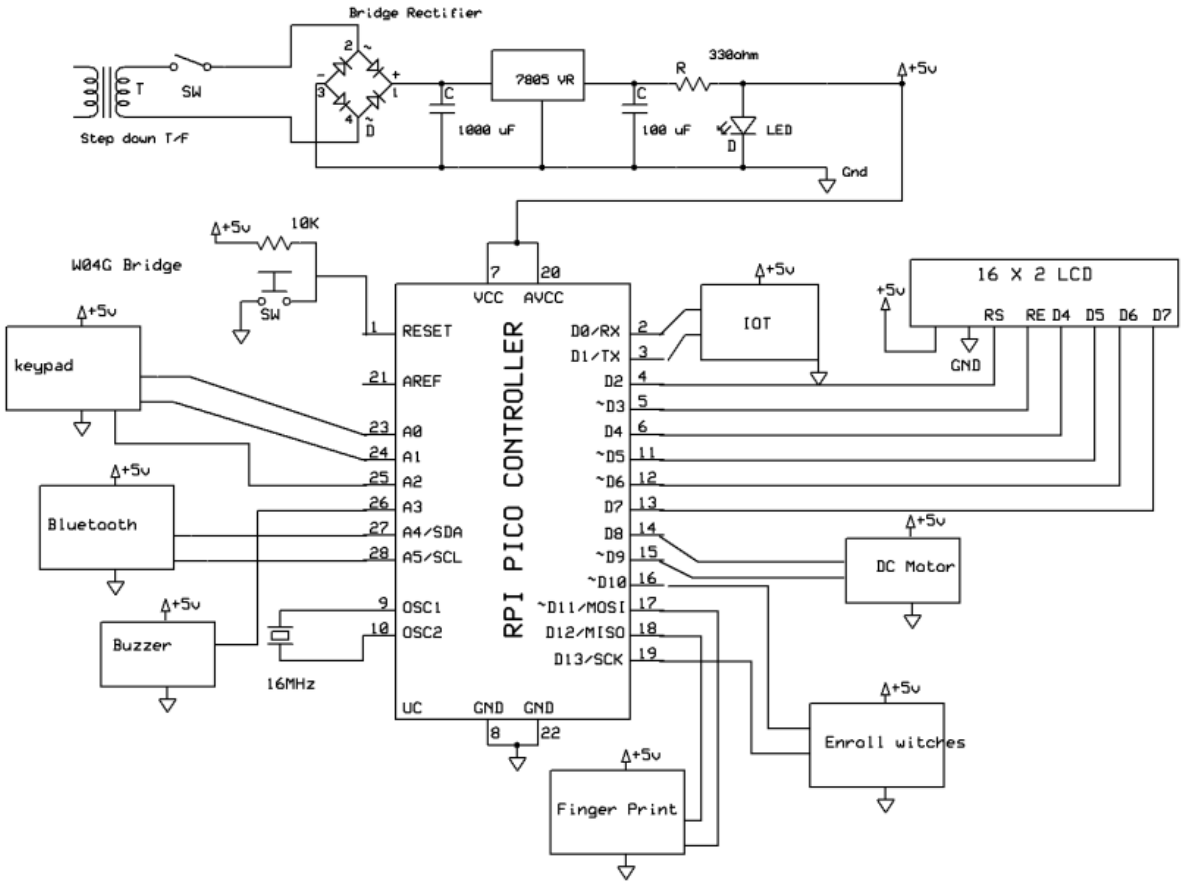
1. Regulated Power Supply
2. Input Section
   - Keypad
   - Voice Bluetooth app
   - Fingerprint sensor
3. Output Section
   - LCD
   - Buzzer
   - Door
4. Raspberry Pi pico Microcontroller

There are five modules Controller, RPS, Input, software and output module. The power is supplied to the RPS module through an adapter. The adapter converts 230v AC to 12v DC and this 12v DC is give to the RPS module. The RPS module consists of voltage regulator 7805 which converts the 12v DC into 5v DC, capacitors are used to reduce noise and LED is used which indicates whether the power is supplied or not. This 5v DC power supply goes to each and every module. The Input modules are keypad, Bluetooth and fingerprint module. The keypad is used to enter the password, the voice password is given by using an Bluetooth module which is controlled by an application and the fingerprint module enrolls and identifies the fingerprints of the user. The output modules are LCD, Buzzer and door. The LCD module shows the data while working with the kit. The Buzzer indicates if the invalid password or fingerprint are identified. Finally the door is controlled by DC motor to open and close. All the input and output modules are connected to the RPI microcontroller which controls the data.

After connecting all the modules properly switch ON the kit, the power is supplied to the kit, initially press the Reset button to clear all the existing data and to connect Wi-Fi to IOT server. The IOT server needs internet to upload data in the server so the Wi-Fi module is used to connect to mobile phone Hotspot and to provide Internet to the IOT module, if the hotspot is connected it shows in LCD that “WIFI is ready”. Firstly the user need to enroll their fingerprint into the fingerprint module then by using switching keypad the password is entered which is displayed on the LCD, if the password matches with the initially set password then the system enters into next verification step otherwise the buzzer activates. In the second step the voice detection system, is activated which uses the AMR voice Bluetooth application that converts the speech into text, so the user need to say speak the password where the speech password converted into text and compared with the original programmed password. If the voice password matches then it enters into next step otherwise the buzzer activates. Now, after the successful verification of second step the system enters into the final step which is fingerprint Identification. Here, the enrolled user need to verify their identification by using fingerprint module, if this final step also verified then the door opens which is controlled by DC motor if fingerprint is not identified the buzzer actives. The main use of the buzzer is that if any invalid password, invalid voice password or invalid fingerprint identified the buzzer activates to

indicate the unauthorized user accesses the system. All the data audit is uploaded into the IOT server or website which is available to the user to check out who is using when the locker is using.

Schematic Diagram



This is the pin diagram where all the hardware components are been connected components. this RPI PICO microcontroller having 28 pins. In which 14 GPIO pins as digital pins and 6 GPIO pins. 16MHz crystal oscillator connected internally. The step down transformer, Bridge rectifier capacitor with 1000f Resisters and led are connected in Regulated power supply which provide the 5v to the Arduino and all input/output modules.

16*2 LCD Monitor has connected with the Digital pins 4,5,6,11,12,13

WIFI has connected to Digital Pins 2,3 internal Transmitter and receiver pins.

Bluetooth has connected to Digital Pins 27,28

DC Motor connected to digital pin 14,15

Buzzer alarm connected to digital pin 26

Keypad has connected to Analog Pins 23, 24,25

Enroll switches connected to 16,19

ADVANTAGES:

- Enhanced Security
- Convenience

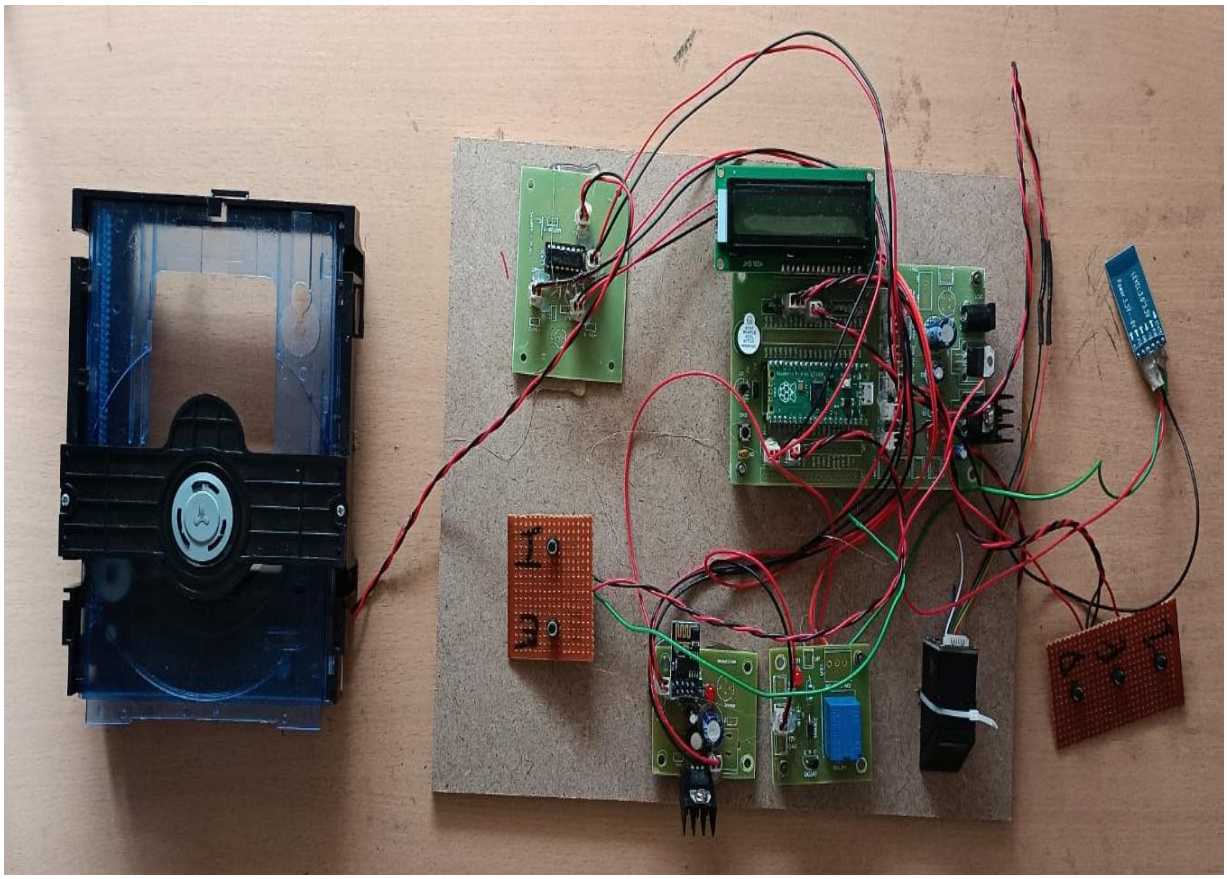
- Improved Efficiency
- Audit Trail and Accountability
- Scalability
- Remote Management and Monitoring
- Customization and Personalization
- Compliance and Data Protection

APPLICATIONS:

1. **Retail Banking:**
   - Retail banks can deploy IoT-based locker access systems to provide customers with secure storage for valuables such as jewellry, documents, or electronic devices.
   - Customers can access their lockers using biometric authentication, eliminating the need for keys or access cards and enhancing convenience.
2. **Private Banking:**
   - Private banking institutions catering to high-net-worth individuals often offer personalized banking services, including secure storage solutions.
   - IoT-based locker access systems can provide an added layer of security for storing valuable assets and confidential documents belonging to private banking clients.
3. **Corporate Banking:**
   - Corporate banks may offer locker facilities to business clients for secure storage of important documents, contracts, or backup data.
   - IoT-enabled lockers can be integrated with corporate banking systems to streamline access management and billing processes for corporate clients.
4. **Wealth Management:**
   - Wealth management firms may use IoT-based locker access systems to offer secure storage solutions to their clients for valuable assets such as precious metals, collectibles, or investment documents.
   - These systems can provide detailed access logs and audit trails, ensuring transparency and accountability in asset management.
5. **Safe Deposit Boxes:**
   - Banks commonly offer safe deposit box services to customers for storing valuable items securely.
   - IoT-based locker access systems can enhance the security and efficiency of safe deposit box operations by replacing traditional lock-and-key mechanisms with biometric authentication and remote management capabilities.
6. **Electronic Data Storage:**
   - With the increasing digitization of banking services, IoT-based locker access systems can also be used for secure storage of electronic data and backups.
   - Customers can securely store digital assets such as encrypted files, USB drives, or hardware wallets in IoT-enabled lockers with advanced security features.
7. **Compliance and Regulatory Requirements:**
   - Banks are subject to various regulatory requirements related to data protection, security, and customer privacy.
   - IoT-based locker access systems can help banks comply with regulatory standards by implementing robust security measures, maintaining audit trails, and protecting sensitive customer information.
8. **Integration with Banking Systems:**
   - IoT-based locker access systems can be integrated with existing banking systems and platforms to provide a seamless user experience.

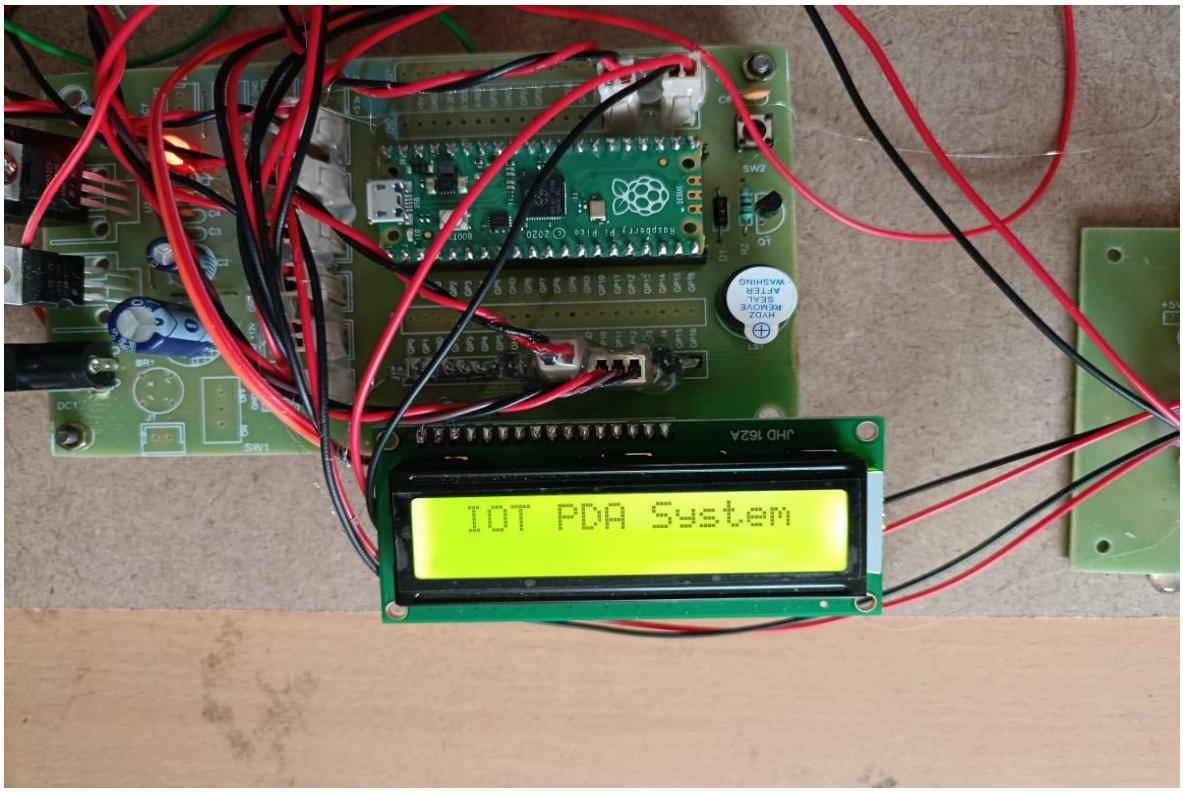
- Integration with core banking systems enables automatic billing, account management, and reporting functionalities for bank administrators.

4.RESULTS

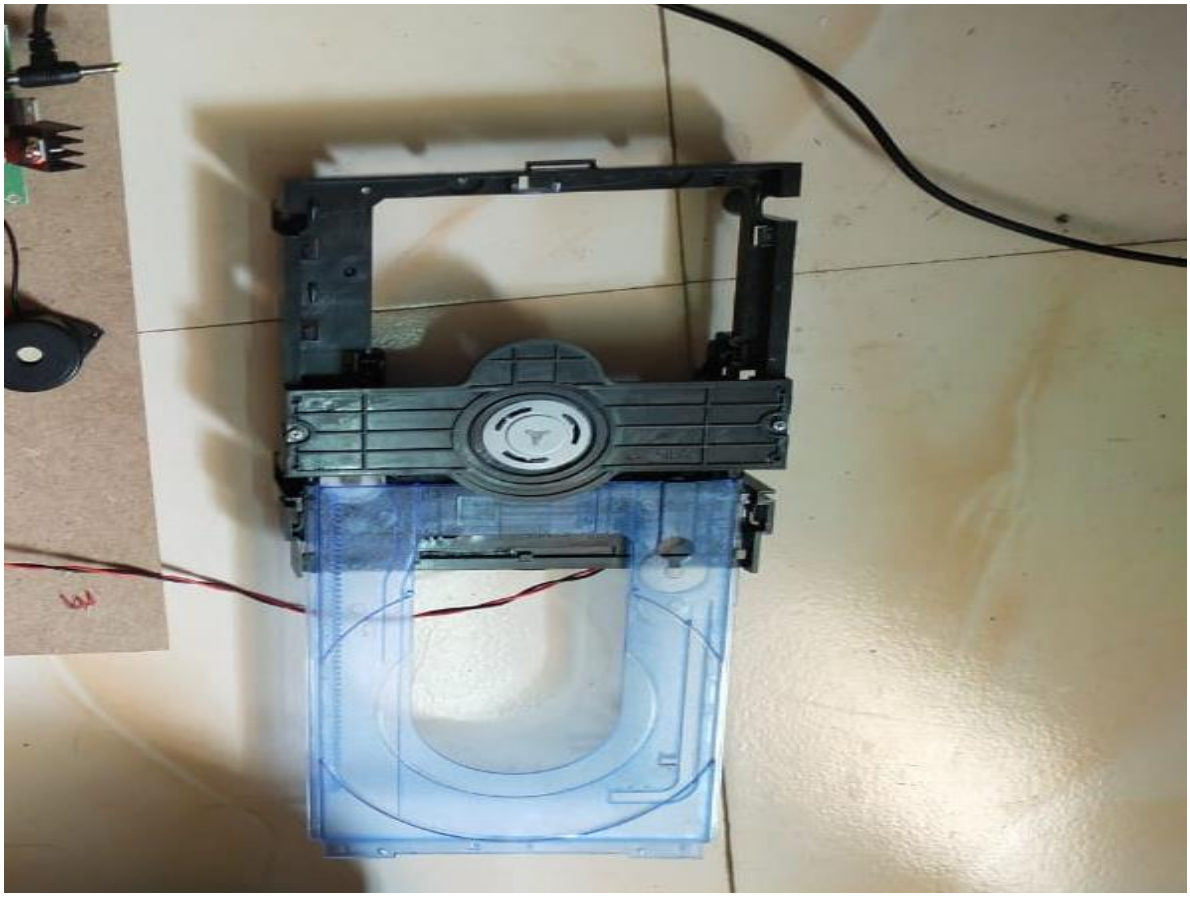


The above image shows the hardware equipment of the project. The kit is turned ON by giving the regulated power supply of 12v which is then converted to 5v dc current. The LED is the indication for 5v current so, if there is 5v current then automatically the LED glows. The generated 5v dc current

passes to every hardware co component in the circuit.



When we hit the reset button after providing the regulated power supply, the LCD displayed the IOT PDA System.The output is seen in the following image after we have connected the IOT module via a WIFI connect and after completing all the security verifications.



If all three security verification steps i.e., keypad password, voice password and fingerprint are verified successfully then the door opens, which is controlled by DC motor. DC motor is controlled by L2930 controller to move door forward and backward direction. When the dc motor moves forward direction it will automatically trigger the gate to open and vice versa.

S.No	Status	Date
1	Wrong_Password	2024-02-16 10:03:46
2	FP_Not_Match	2024-02-16 09:30:54
3	Wrong_Password	2024-02-16 09:24:35
4	Correct_Pwd_FP_Match_Accessed	2024-02-15 11:58:01
5	Correct_Pwd_FP_Match_Accessed	2024-02-15 11:56:46
6	Correct_Pwd_FP_Match_Accessed	2024-02-15 11:55:26
7	FP_Not_Match	2024-02-15 11:39:56
8	Correct_Pwd_FP_Match_Accessed	2024-02-15 11:35:55
9	Wrong_Password	2024-02-15 11:29:48
10	Correct_Pwd_FP_Match_Accessed	2024-02-14 11:46:50
11	Correct_Pwd_FP_Match_Accessed	2024-02-11 10:51:19

The entries of each and every person data is uploaded in the website by using ESP8266 IoTmodule.Here the authorized persons data and also if the unauthorized persons access the system then also the IoT module uploads data indicating wrong password, FP not match. This website is very useful to the owner of the bank locker to observe their system at any time and anywhere.

CONCLUSION

We Design and Implement the "IOT-MULTI SECURE BANK LOCKER ACCESS SYSTEM" The main aim of the project is to protect valuable things like jewellery,money,documents..,etc. In this project, we are using the RPS, Keypad, Fingerprint, Voice Bluetooth, LCD, Buzzer, Door, and IOT Module to transmit the data.And the data can be controlled by the Raspberry Controller.By using the Wi-Fi connect the IOT Server. The data can be displayed on the LCD and at the same time IOT server. If The voice, keypad password, and fingerprint Security verifications are accessed then only the Door will open, otherwise the buzzer activates and the data is uploaded to the server by using the IOT module through which the user can identify the error. This system is simple to operate and highly secured for the users which is used in banks, personal devices, lockers etc……..

REFERENCES

[1] Shruthi, CH M., Sai Kumar Bandari, Chandra Kiran Reddy Ala, and Muralidhar Reddy. "Locker Security System using Internet of Things." In E3S Web of Conferences, vol. 391, p. 01153. EDP Sciences, 2023.

[2] Marie, Osama Amin. "An Intelligent Security System for Commercial Establishments Based on the Internet of Things (IoT)." International Journal of Intelligent Systems and Applications in Engineering 11, no. 11s (2023): 209-220.

[3] BALASUBRAMANİAN, Kishore, V. Karthik, and V. K. Padmanaban. "Smart Multi Verification Based Security System." El-Cezeri 10, no. 2: 193-207.

[4] SudarshanAkshaya ,R.k Mohan Reddy B SrinivasaRamya L.K High Protection Voice Identification Based Bank Locker Security System With Live Image Authentication

[5] Khokher, Bhawna, Mamta B. Savadatti, Anish Kumar, TV Mourya Nikhil, Pranav Raj, and Aditya Vilas Thakre. "Advance Computing in IoT based High-Security Smart Bank Locker." In 2023 7th International Conference on Computing Methodologies and Communication (ICCMC), pp. 1331-1335. IEEE, 2023.

[6] Raman, Ramakrishnan, S. Prabhakar, and T. Bernatin. "IoT based Anti-Theft Controlling and Security System for ATM Machine." In 2023 5th International Conference on Inventive Research in Computing Applications (ICIRCA), pp. 1272-1277. IEEE, 2023

[7] Dhanasekaran, S., S. Boopathy, S. Siva Ganesh, V. Thanya, SCK SuriyaVishwa, and S. Thasneem. "Intelligent Security System with Haptic Device and Random Number Generator on Touch Enabled Devices." In 2023 2nd International Conference on Advancements in Electrical, Electronics, Communication, Computing and Automation (ICAECA), pp. 1-5. IEEE, 2023

[8] Wankhede, Nilashree, and SushamaWagh. "Enhancing Biometric Speaker Recognition Through MFCC Feature Extraction and Polar Codes for Remote Application." IEEE Access 11 (2023): 133921-133930.