IMPLEMENTATION OF BANK LOCKER SYSTEM USING RASPBERRY PI

[1]Chenna P,[2]Dr.P.Maniganda,[3]Penchalaih C,[4]Anitha R
[1]Associate Professor,[2]Professor,[3,4]Assistant Professor
Department of ECE
Tadipatri Engineering College,Tadipatri,AP

ABSTRACT

By the title itself it can be implied that the system designed here is very useful for the banks. The security system designed with finger print scanner is aimed to provide high level safety authentication to the clients. These days most of the banks are offering hi-tech safety devices to their customers (those who are having lockers) to increase their confidence. A Finger print scanner provides more safety authentication to the client, increasing their confidence when using the bank services. It uses the features of client's unique biochemical characteristic fingerprints to pass the authentication for above said application.

To prove the concept practically, locker environment must be created, & there by the demo module is constructed with one metal box. This box is build with sliding type of door mechanism. Rock & pinion method is used to open or close the door, this door is driven through a DC motor. The finger print scanner used in this project work has in-built ROM, DSP & RAM. This module when it is operated in master mode user finger prints are scanned, & this data will be stored in ROM.

For each finger print, a separate identity is allotted in the system, this is the initial process. After completing this process, the finger print module must be operated in user mode, in this mode of operation the system acquires the fresh data & compares with the previous stored data. If this data is matched, the person will be identified & his/her name will be displayed through monitor interfaced with microcontroller unit. To enhance the safety level further, the processor is designed with additional features such that it appeals the customer through same monitor to prove his/her ID by entering user code through a small keyboard interfaced with controller. When code & finger prints both are matched, then the locker door will be opened automatically. If the code is wrong, the system raises alarm momentarily. The motor used here is having built in with reduction gear mechanism internally there by it is driven through 'H' bridge device.

DOI Number: 10.48047/nq.2020.18.10.NQ20243 NeuroQuantology 2020; 18(10):162-172

I. INTRODUCTION

1.1 INTRODUCTION OF PROJECT:

The project work described in this report exposes about banking authentication methods, mainly it is described about the technology of finger print authentication, by which the customers them self's can open their bank lockers. In this method the customer need not consult anybody from bank side.

There are multiple ways that banks can authenticate users, i.e. to identify & make sure the users. These methods range from username and password combinations to iris scanning. As technology continues to change, banks must adapt their security systems to effectively combat hackers and thieves. Selecting the right technologies for each organization cannot be generalized. However, knowing what authentication techniques are available is the first step in maintaining a

secure environment. Authentication can be completed via the use of many different methods. Some of these methods are far superior to others, but are more difficult to implement and fund. Banks are organizations that must take the authentication process very seriously. Banks are storehouses of critical personal identifiable information. This information may include: social security numbers, physical addresses, phone numbers, email addresses, account numbers, credit histories, employment histories, and other information pertaining to the organization's clients and the employees.

Banks must have multiple security measures in place. Especially for specific customers those who are having lockers, for them multilevel security systems are essential, there by in this project work in addition to the scanning of customer finger prints, digital code locking system is also implemented.

The reason for such a model is that that the bankers should create confidence to their clients. Methods for authentication can be organized into a few basic categories. They can be one of several things directly related to the user. Basically, this is something the user knows, an easy way that can be appreciated by the user.

1.2 PROBLEM STATEMENT:

There are multiple ways that banks can authenticate users, i.e. to identify & make sure the users. These methods range from username and password combinations to iris scanning. As technology continues to change, banks must adapt their security systems to effectively combat hackers and thieves. Selecting the right technologies for each organization cannot be generalized. However, knowing what authentication techniques are available is the first step in maintaining a secure environment.

Authentication can be completed via the use of many different methods. Some of these methods are far superior to others, but are more difficult to implement and fund. Banks are organizations that must take the authentication process very seriously. Banks are storehouses of critical personal identifiable information. This information may include: social security numbers, physical addresses, phone numbers, email addresses, account numbers, credit histories, employment histories, and other information pertaining to the organization's clients and the employees.

Banks must have multiple security measures in place. Especially for specific customers those who are having lockers, for them multilevel security systems are essential, there by in this project work in addition to the scanning of customer finger prints, digital code locking system is also implemented. The reason for such a model is that that the bankers should create confidence to their clients. Methods for authentication can be organized into a few basic categories. They can be one of several things directly related to the user. Basically, this is something the user knows, an easy way that can be appreciated by the user.

1.3 MOTIVATION OF PROJECT:

The use of the Raspberry Pi to develop an effective power management system for street lighting is inspired by a number of factors, including:

It is essential to conserve energy wherever feasible given the rising cost of energy and the rising demand for electricity. An effective power management system may greatly minimise energy consumption, which is significantly influenced by street lighting.

Operating conventional street lighting systems is frequently expensive and inefficient. Municipalities and other organisations in charge of street lighting can significantly reduce their energy costs and maintenance expenses by putting in place an effective power management system.

Energy waste not only raises expenses but also has a detrimental effect on the environment. We may lessen our carbon footprint and contribute to reducing the consequences of climate change by putting in place an effective power management system.

Quality of illumination is improved because of the automatic brightness adjustment function of the suggested system, which makes sure that the street lights aren't either too bright or too low. Drivers and pedestrians may feel safer and more secure as a result of this.

A single-board computer with many uses, including IoT devices, the Raspberry Pi is inexpensive and adaptable. The use of a Raspberry Pi to construct an effective power management system shows how technology has the ability to enhance the effectiveness and efficiency of public services.

In conclusion, the installation of an effective Raspberry Pi-based power management system for street lights is driven by the desire to reduce energy consumption, cut expenses, address environmental issues, enhance lighting quality, and take advantage of technology improvements.

1.4 BLOCK DIAGRAM:

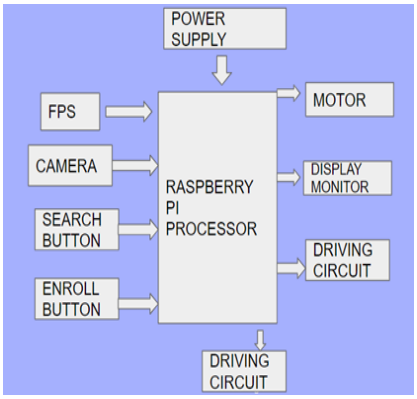

Fig. 1. Implementation of Bank Locker System using Raspberry Pi

Figure 1.1 depicts the block diagram of our project.

The arrows indicate whether the components feed the signal to the microcontroller or accept the signal given by the microcontroller. In our project, Fingerprint sensor and camera act as inputs whereas Motor and Monitor acts as output.

Each block has separate function to do and all the blocks work with the central brain of project i.e the microcontroller Raspberry Pi. Power supply, connecting wires, a circuit board are used to complete the circuit.

II. LITERATURE SURVEY

1. Sagar S. Palsodkar*, Prof S.B. Patil , “Review: Biometric and GSM Security for Lockers” Int. Journal of Engineering Research and Applications , Vol. 4, Issue 12(Part 6),December 2014.

2. R.Ramani , S. Selvaraju , S.Valarmathy, P.Niranjan , “Bank Locker Security System based on RFID and GSM Technology ’’, International Journal of Computer Applications (0975 – 8887) Volume 57– No.18, November 2012

3. P. Sugapriya#1, K. Amsavalli#2,“Smart Banking Security System Using PatternAnalyzer”,International Journal of Innovative Research in Computer and Communication Engineering ,Vol.3, Special Issue 8, October 2015

4. M.Gayathri, P.Selvakumari, R.Brindha “Fingerprint and GSM based Security System” International Journal of Engineering Sciences & Research Technology, ISSN: 2277-9655, Gayathri et al.3(4): April, 2014.

5. Mary Lourde R and DushyantKhosla “Fingerprint Identification in Biometric Security Systems” International Journal of Computer and Electrical Engineering, Vol.2, No. 5, October, 2010

6. Pramila D Kamble and Dr. Bharti W. Gawali “Fingerprint Verification of ATM Security System by Using Biometric and Hybridization” International Journal of Scientific and Research Publications, Volume 2, Issue 11, November 2012.

7. Ashish M. Jaiswal andMahipBartere “Enhancing ATM Security Using Fingerprint And GSM Technology”, International Journal of Computing Science and Mobile Computing Vol. 3, Issue. 4, April 2014.

8. Bhalekar S.D., Kulkarni R.R., Lawande A.K., Patil V.V., “On line Ration card System by using RFID and Biometrics”, International journal of Advanced Research in Computer Science & Software engineering., Vol. 5Issue 10, October 2015.

9. Abhilasha A Sayar1 , Dr. Sunil N Pawar2 , “Review of Bank Locker System Using Embedded System” , International Journal of Advanced Research in Computer and Communication Engineering .,Vol. 5, Issue 2, February 2016 .

10. SanalMalhotra, “Banking Locker System With Odor Identification & Security Question Using RFID GSM Technology”. International Journal of Advances in Electronics Engineering – IJAEE Volume 4 : Issue 3.

III. TECHNICAL DESCRIPTION

3.1.1 FUNCTIONAL DESCRIPTION

The functional description of the project work “Finger print based security system for bank

lockers" is explained in this chapter. For better understanding, the total module is divided into various blocks and each block explanation is provided here. The diagrams (block diagram, circuit diagram and flow chart) of this project work are provided in the next chapter. The following is the description of the over all function or operation of the project work.

Finger Print Scanner:

The operation of the project work starts with this unit. As the title itself is justifying that a security system should be designed based on the finger print. So a finger print scanner has been interfaced to the microcontroller. The fingerprint scanner module scans the finger print and checks with that of the print in the data base unit which is initially fed in it. If it matches with that of the data present in it then the controller displays the details of that particular person in the LCD which is interfaced to it and asks to enter the pass word through the keyboard which is also interfaced with the same controller. When the pass word is correct, then the controller opens the locker door by operating the DC motor that is interfaced to it through a H – bridge IC. And for closing the locker door, again the password should be entered. The DC motor simulates the door opening and closing mechanism by rotating in clockwise and anti clockwise directions. A 12v DC motor of reduction gear mechanism is used to drive the sliding type door mechanism horizontally through rock and pinion method of the locker room whose mechanical transmission section is coupled with the DC motor. If the password entered is wrong then the controller energizes alarm automatically and will be de-energized when the reset key is pressed in the keyboard.

Concepts in Fingerprint System

- Fingerprint Feature

Fingerprint algorithmic means capturing features from fingerprint image, it represents the finger print information. The saving, matching and capturing of fingerprint templates are all manipulated through fingerprint features.

- 1:1

Comparing two fingerprint templates, return information: matching or not matching.

- 1: N Searching

Search the matching fingerprint from numbers of fingerprint features. Return information: No matching features or having matching features and returning the matching feature's ID simultaneity.

3.1.2 Microcontroller Unit:

3 Raspberry Pi 2 - Model B

The Raspberry Pi 2 Model B is out and it's amazing! With an upgraded ARMv7 multicore processor, and a full Gigabyte of RAM, this pocket computer has moved from being a 'toy computer' to a real desktop PC

The big upgrade is a move from the BCM2835 (single core ARMv6) to BCM2836 (quad core ARMv7). The upgrade in processor types means you will see ~2x performance increase just on processor-upgrade only. For software that can take advantage of multiple-core processors, you can expect 4x performance on average and for really multi-thread-friendly code, up to 7.5x increase in speed!

That's not even taking into account the 1 Gig of RAM, which will greatly improve games and web-browser performance!

Best of all, the Pi 2 keeps the same shape, connectors and mounting holes as the Raspberry Pi B+. That means that all of your HATs and other plug-in daughterboards will work just fine. 99% of cases and accessories will be fully compatible with both versions.

Please note: The new processor on the Pi 2 means that you will need to update your existing SDcard or create a new SD card with your operating system (Raspbian, Arch, XBMC, NooBs, etc) because you cannot plug in olderscards from a Pi 1 into a Pi 2 without upgrading with **sudo apt-getupgrade** on the Pi 1 first.

Also, any precompiled software will not work at full speed (although supposedly the processor will be able to run it). Still, you'll likely want to have it recompiled for the new processor! For many people, this isn't a big deal, but if you have a pre-created Pi 1 Model A+B+ card image, just be aware it won't work without performing an 'sudo apt-get upgrade' on the older Pi 1 before installing on the Pi 2!

3.1.3 L293D "H" BRIDGE:

The motor driver package L293D is interfaced with 89C51 microcontroller through IN1 to

IN4 of H Bridge (L293D). Both the enable pins (EN1 and EN2) of motor driver L293D is combined together and fed to controller to access the command signals. Depending up on the command signals issued by the controller, the enable pins are activated to control all the four internal drivers of L293D respectively to drive geared DC motor. Hear H Bridge is required, because the microcontroller output is not sufficient to drive the DC motors, so current drivers are required for motor rotation.

The L293D is a quad, high current, half-H driver designed to provide bidirectional drive currents of up to 600mA at voltages from 4.5V to 36V. It makes it easier to drive the DC motors. The L293D consists of four drivers. Pins IN1 through IN4 and OUT1 through OUT4 are input and output pins, respectively, of driver 1 through driver 4. Drivers 1 and 2, and drivers 3 and 4 are enabled by enable pin 1 (EN1) and pin 9 (EN2), respectively. When enable input EN1 (Pin1) is high, drivers 1 and 2 are enabled and the outputs corresponding to their inputs are active. Similarly, enable input EN2 (Pin9) enables drivers 3 and 4.

So once the password is entered through the keyboard in the sequence defined in the controller, the controller drives the motor using the L293D H – bridge IC by which the sliding door will be opened (moves horizontally). And for the closing of the door again the password should be entered from the keyboard. And the controller closes the locker room door automatically without any manual involvement to close the door.

3.1.4 Facial Recognition:

Facial recognition devices have been difficult to substantiate in practice and extravagant claims have sometimes been made them. Facial recognition is very attractive from the user perspective and they may eventually become a primary biometric methodology.

Applications:

Most of the biometric applications are related to security and are used extensively for military purposes and other government purposes. The applications in the public domain that are available to common people include:

- Prison visitor systems, where visitors to inmates are subject to verification procedures in order that identities may not be swapped during the visit - a familiar occurrence among prisons worldwide.
- Driver's licenses, whereby drivers are expected to have multiple licenses or swapped licenses among themselves when crossing state lines or national borders.
- Canteen administration, particularly on campus where subsidized meals are available to bona fide students, a system that was being heavily abused in some areas.
- Benefit payment systems - In America, several states have saved significant amounts of money by implementing biometric verification procedures. The numbers of individuals claiming benefit has also dropped dramatically in the process, validating the systems as an effective deterrent against multiple claims.
- Border control - A notable example for this is the INSPASS trial in America where travelers were issued with a card enabling them to use the strategically based biometric terminals and bypass long immigration queues. There are other pilot systems operating elsewhere in this respect.
- Voting systems, where eligible politicians are required to verify their identity during a voting process. This is intended to stop ‘proxy’ voting where the vote may not go as expected.
- Junior school areas where problems are experienced with children being either molested or kidnapped.

In addition there are numerous applications in gold and diamond mines, bullion warehouses and bank vaults as well as the more commonplace physical access control applications in industry.

3.1.5 DC MOTORS:

At the most basic level, electric motors exist to convert electrical energy into mechanical

energy. This is done by way of two interacting magnetic fields -- one stationary, and another attached to a part that can move. A number of types of electric motors exist, but most BEAM bots use DC motors in some form or another. DC motors have the potential for very high torque capabilities (although this is generally a function of the physical size of the motor), are easy to miniaturize, and can be "throttled" via adjusting their supply voltage. DC motors are also not only the simplest, but the oldest electric motors.

The basic principles of electromagnetic induction were discovered in the early 1800's by Oersted, Gauss, and Faraday. By 1820, Hans Christian Oersted and Andre Marie Ampere had discovered that an electric current produces a magnetic field. The next 15 years saw a flurry of cross-Atlantic experimentation and innovation, leading finally to a simple DC rotary motor. A number of men were involved in the work, so proper credit for the first DC motor is really a function of just how broadly you choose to define the word "motor."

DC motors are configured in many types and sizes, including brushless, servo, and gear motor types. A motor consists of a rotor and a permanent magnetic field stator. The magnetic field is maintained using either permanent magnets or electromagnetic windings. DC motors are most commonly used in variable speed and torque applications.

Brushed DC motors have built-in commutation, meaning that as the motor rotates, mechanical brushes automatically commutate coils on the rotor. Brushless DC motors use an external power drive to allow commutation of the coils on the stator. Brush-type motors are used when cost is a priority, while brushless motors are selected fulfill specific requirements, such as maintenance-free operation, high speeds, and hazardous environments where sparking could be dangerous.

Fig 2. Buzzer

3.1.6 Buzzer:

Basically, the sound source of a piezoelectric sound component is a piezoelectric diaphragm. A piezoelectric diaphragm consists of a piezoelectric ceramic plate which has electrodes on both sides and a metal plate (brass or stainless steel, etc.). A piezoelectric ceramic plate is attached to a metal plate with adhesives. Applying D.C. voltage between electrodes of a piezoelectric diaphragm causes mechanical distortion due to the piezoelectric effect. Here we are using the buzzer as an indicator for the false biometric verification, i.e, if the biometrics of the user does not match then the buzzer indicates it with a beep sound to alert the user.

IV. SYSTEM ANALYSIS

4.1 EXISTING SYSTEM

Street light is ineffectively designed and deficiency kept up, there is huge number of scorched out lights which prompts instability. There is a complaint register in every zonal office street light section. Presently street light management is done through manual process such as a physical activity is required to switch on and off the street lights according to their needs. It is so hard to maintain the activity in physical methodology because once the manual process fails there will be no lightening into the respective streets. As well as the manual process is time consuming for fault finding and corrections hence takes more and more time to manipulate each and every activity such as failures of lamps and either it is on or off. And it is difficult to identify the light in the respective location because of the present system doesn't use any advanced devices such as Global position System [GPS] and internet facilities, so that it is very difficult to

identify and inform the control messages to the control room as well as these kind of street light mechanism cannot receive the control messages from the control room.

For all the entire manual process will cause poor efficiency and cost & time wastages in both performance wise as well as efficiency wise. At the state level, a large part of the State Electricity Boards are reeling under enormous losses by virtue of a combination of assistance and under-recoveries. The National Tariff Policy of 2006 stipulates that the State Electricity Regulatory Commission (SERC) settle tax inside +/ - 20% of the cost of supply. Unfortunately, most states fail to meet this.

Disadvantages:

- Performance is low because of manual operations and
- controls.
- Cannot monitor the street light from remote places,
- physical intervention is required at every point of time.
- Wastage of Power
- Expensive process.

Existing techniques like enlisting the objection, turning on/off the light physically is tedious and requires labor. The new strategy programmed ON/OFF and fault recognition without
human intercession is less demanding when contrasted with the current system.

4.2 PROPOSED SYSTEM:

The proposed system for the implementation of a Bank Locker System using Raspberry Pi with Fingerprint and Face Recognition. This project aims to enhance the security and convenience of bank lockers by incorporating biometric authentication methods, namely fingerprint and face recognition. By leveraging the capabilities of Raspberry Pi, this system ensures a robust and reliable solution for secure access control to bank lockers.

System Overview:

The Bank Locker System is designed to provide authorized access to bank lockers through a combination of biometric authentication techniques. Raspberry Pi, a low-cost, credit card-sized computer, serves as the central processing unit for the system. It connects various hardware components, such as fingerprint sensors, a camera module for face recognition, and electronic locks, to create a seamless and secure access control mechanism.

System Components:

Raspberry Pi:

The Raspberry Pi acts as the brain of the Bank Locker System, responsible for processing data from different sources, coordinating the authentication process, and controlling the electronic locks. Its compact size, low power consumption, and computational capabilities make it an ideal choice for this project.

Fingerprint Sensor:

A high-quality fingerprint sensor is integrated into the system to capture and verify the unique fingerprint patterns of authorized users. This sensor communicates with the Raspberry Pi, which performs fingerprint matching against a pre-registered database to grant or deny access.

Face Recognition:

To further enhance the security of the bank locker system, a camera module is utilized for face recognition. The Raspberry Pi processes live images captured by the camera module, compares them with stored facial features of authorized users, and grants access based on the match.

V. RESULTS

5.1 Result of Our Project:

5.1.1 How the project set-up looks!

Fig 3. Project Kit initially

5.1.2 Actual result verification:

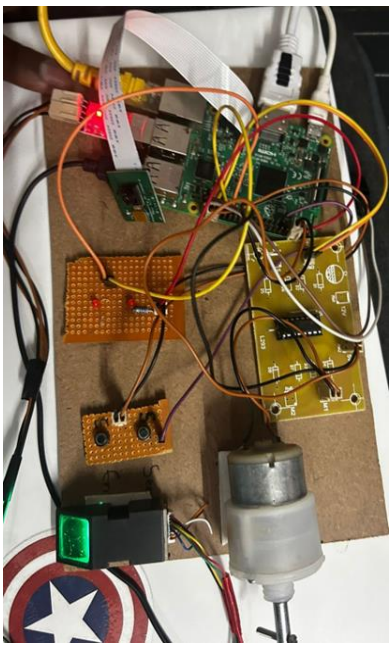

Fig 4. FPS Glowing to check the fingerprint.

Whenever the code is run and executed first when the enroll button is pressed then the user needs to enroll their fingerprint and after that the user should then press the search button. If the fingerprint is matched with the previous enrolled fingerprint then the dc motor which works as the door of the locker opens and if the fingerprints doesnot match then the buzzer sound is occurred to alert the owner of the bank locker .

5.2 Advantages:

- Enhanced Security: The integration of a Raspberry Pi with a fingerprint sensor (FPS) adds an extra layer of security to the bank locker system. Biometric authentication through fingerprints is more secure than traditional methods like keys or passwords, reducing the risk of unauthorized access.
- Convenience: With a bank locker system using Raspberry Pi and FPS, customers can access their lockers using their fingerprints, eliminating the need to carry physical keys or remember passwords. This provides convenience and ease of use for customers.
- Real-time Monitoring: Raspberry Pi can be connected to a central monitoring system, allowing bank staff to monitor locker access in real time. This enables them to keep track of locker usage, identify any suspicious activities, and take immediate action if required.
- Efficient Management: The integration of Raspberry Pi with a bank locker system can streamline the management process. It can provide automated logging of locker access, reducing manual paperwork for bank staff and enabling accurate record-keeping.
- Scalability: Raspberry Pi is a versatile and easily scalable platform. It can be expanded to accommodate a large number of bank lockers, making it suitable for both small and large-scale deployments.

5.3 Disadvantages:

- Cost: Implementing a bank locker system using Raspberry Pi with FPS may require an initial investment in hardware, software, and setup. This cost could be higher compared to traditional lock and key systems.
- Technical Expertise: Developing and maintaining a bank locker system using Raspberry Pi with FPS requires technical expertise. Banks may need to invest in training their staff or hire specialized personnel to handle the system effectively.
- Reliability: While Raspberry Pi is generally reliable, any hardware or software failures could disrupt the bank locker system. It is essential to have backup systems and contingency plans in place to minimize downtime and ensure uninterrupted access to lockers.
- Integration Challenges: Integrating a Raspberry Pi-based system with existing bank infrastructure, such as security systems and databases, may present challenges. Compatibility issues or the need for additional customization can complicate the integration process.
- User Acceptance: Some customers may be unfamiliar or uncomfortable

with using fingerprint authentication for locker access. Ensuring user acceptance and providing alternative access methods for those who prefer them is crucial for a successful implementation.

5.4 Applications:

- Secure Storage: The primary application of the bank locker system is to provide secure storage for customers' valuable belongings. The Raspberry Pi and FPS integration enhance security by using biometric authentication, ensuring that only authorized individuals can access the lockers.
- Access Control: The system enables efficient access control to bank lockers. Customers can use their fingerprints to access their lockers, eliminating the need for physical keys or passwords. This improves convenience and eliminates the risk of lost or stolen keys.
- Audit Trail: The bank locker system can maintain an audit trail of locker access. Every time a customer accesses their locker, the system can log the date, time, and identity of the user. This audit trail can be useful for security purposes and in resolving any disputes or discrepancies.
- Real-time Monitoring: The integration of Raspberry Pi allows for real-time monitoring of the bank locker system. Bank staff can monitor locker access, receive instant notifications of any unauthorized attempts, and take immediate action if required. This enhances security and allows for proactive measures.
- Management and Reporting: The system can assist bank staff in managing and reporting locker usage. It can generate reports on locker availability, usage patterns, and occupancy rates. This data can be valuable for operational planning, optimizing locker allocation, and improving customer service.
- Integration with Banking Systems: The bank locker system can be integrated with existing banking systems, such as core banking software. This integration enables seamless integration of locker access with customer profiles and facilitates efficient management of locker rentals and fees.
- Multi-factor Authentication: The Raspberry Pi and FPS integration allow for multi-factor authentication in the bank locker system. For enhanced security, additional authentication factors, such as PIN codes or access cards, can be combined with fingerprint authentication, further ensuring the identity of the locker user.
- Scalability: The system can be easily scaled to accommodate a large number of lockers, making it suitable for both small and large banking institutions. Raspberry Pi's flexibility allows for easy expansion and integration with additional hardware modules or sensors.
- Remote Management: With the integration of Raspberry Pi, the bank locker system can be remotely managed and monitored. This enables banks to perform system maintenance, updates, and troubleshooting without the need for physical presence at the lockers' location.

VI. CONCLUSION

6.1 Conclusion :

The increased need of privacy and security in our daily life has given birth to this new area of science. These devices are here and are present around us everywhere in the society and are here to stay for a long time to come. Indeed, it will be interesting to watch the future impact that they will have on our day-to-day lives.

The project work “Finger print based security system for bank lockers” is designed and developed successfully. For the demonstration purpose, a prototype module

is constructed; and the results are found to be satisfactory. Since it is a prototype module, a simple module is constructed, which can be used for many applications like highly confidential area or where high level security is required. In this project we have explained why security is important in an Ambient Intelligent environment. In order to achieve Trust and Security not only cryptographic algorithms are needed but also secure methods for generation and storage of secret keys. By constriction of such security devices the keys can be made tamper proof and avoid them from destruction by the anti social elements or the unofficial persons.

6.2. Future Scope :

In addition to this the future scope of this project is to develop smart bank Locker security system based on "FACE", Scanning for visual identification of the person and making it more secure for the users to keep their valuable things.

- Biometric Integration: As biometric technology evolves, future iterations of the bank locker system could integrate additional biometric modalities such as facial recognition or iris scanning, further enhancing security and user convenience.
- IoT Integration: With the growth of the Internet of Things (IoT), the bank locker system could be integrated with other smart devices and systems within the bank. For example, connecting lockers to a central IoT network could enable features like automatic inventory tracking or remote monitoring of locker status.
- Mobile App Integration: Developing a mobile application that works in conjunction with the bank locker system would provide customers with a seamless experience. Users could reserve lockers, receive notifications, and access locker contents through their smartphones, adding convenience and accessibility.
- Enhanced Security Features: Future advancements in security technologies, such as advanced encryption algorithms, tamper-proof sensors, or intrusion detection systems, could be integrated into the bank locker system to provide even higher levels of security against physical and cyber threats.
- Blockchain Integration: Blockchain technology offers decentralized and tamper-resistant data storage. Integrating blockchain into the bank locker system could provide an immutable record of locker access and enhance data security and integrity.
- Artificial Intelligence (AI) and Machine Learning (ML): AI and ML algorithms could be utilized to analyze locker usage patterns, identify suspicious activities, or optimize locker allocation based on customer behavior, leading to more efficient and secure locker management.
- Integration with Smart Cities: As cities become smarter and more interconnected, the bank locker system could be integrated into the larger smart city infrastructure. For example, lockers could be accessible through a unified smart city card, allowing users to access lockers across various locations within the city.
- Biometric Payment Integration: With the rise of biometric payment systems, the bank locker system could be extended to allow secure payment transactions through fingerprint authentication, providing customers with a seamless experience and reducing the need for physical payment cards or cash.
- Data Analytics and Insights: By leveraging the data collected from the bank locker system, banks can gain valuable insights into customer behavior, occupancy rates, peak usage hours, and other patterns. This data can be used to improve operational efficiency, optimize locker utilization, and enhance customer service.

6.3 REFERENCES:

While designing and fabrication of this project work, we gathered information from websites & consulted experts in various fields. The information is gathered from yahoo.com search Engine. Regarding micro controllers plenty of books are available, the following are the references made during design, development and fabrication of the project work.

(1) Electronic Circuit guide book – Sensors – By JOSEPH J.CARR
(2) The 8051 Micro-controller Architecture, programming & Application By: Kenneth J. Ayala
(3) Mechanism and Machine Theory By: J.S. Rao, R.V. Dukkipati
(4) Programming and Customizing the 8051 Micro-controller By: Myke Predko
(5) The concepts and Features of Micro-controllers By: Raj Kamal
(6) E. Aarts and S. Marzano, The New Everyday: Views on Ambient Intelligence, 010 Publishers Rotterdam, 2003.
(7) Ross Anderson and Markus Kuhn, Tamper Resistance A Cautionary Note, in Proc. 2nd USENIX Workshop on Electronic Commerce, 1996.
(8) Ross Anderson and Markus Kuhn, Low Cost Attacks on Tamper Resistant Devices, in Mark Lomas (ed.), Security Protocols: 5th International Workshop, Paris, France.