e-ISSN:2582-7219

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH IN SCIENCE, ENGINEERING AND TECHNOLOGY

Volume 7, Issue 4, April 2024

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.521

International Journal Of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| Monthly Peer Reviewed & Referred Journal |

| Volume 7, Issue 4, April 2024 |

| DOI:10.15680/IJMRSET.2024.0704066 |

Bank Locker System using Finger Print Security

T.Rakshith, A.Vasanth, G.Jagadeesh, G.Siva Koti Reddy, Mahesh V Sonth

UG Student, Department of ECE CMR Technical Campus, Hyderabad,India

UG Student, Department of ECE CMR Technical Campus, Hyderabad,India

UG Student, Department of ECE CMR Technical Campus, Hyderabad,India

UG Student, Department of ECE CMR Technical Campus, Hyderabad,India

Associate Professor, Department of ECECMR Technical Campus, Hyderabad,India

ABSTRACT: Biometric identification has become a cornerstone of security across various domains. Among these techniques, fingerprint recognition stands out as the most established and widely used method. Law enforcement has utilized fingerprints for identification for over a century, while recent advancements have enabled a broader range of applications. Personal authenti- cation for computers, networks, ATMs, vehicles, and even homes now benefits from fingerprint security. This paper delves into the development and core principles of fingerprint authentication systems, particularly focusing on electronic locks. The process involves capturing a user's fingerprint image and storing it as a reference template. Subsequent access attempts require capturing a new fingerprint image and comparing its features (minutiae) with the stored template. This comparison process ensures a high degree of accuracy, as replicating a fingerprint's intricate details is statistically improbable, with estimates suggesting a one-in- a- billion chance. Fingerprint authentication offers a significant advantage over traditional methods by providing a unique iden- tifier inherent to each individual. Unlike passwords or keys that can be lost, stolen, or shared, fingerprints are virtually impossible to forge or replicate. This inherent security characteristic makes fingerprint-based systems a reliable and cost-effective solution for user identification and access control.

KEYWORDS: Cloud-based logistics services, Cloud computing, Resource optimization, Logistics Industry, Security architecture

I. INTRODUCTION

Thefts are one of the main problems in today's world, placeslike offices and other public places should not be secured, so the problems of securing our documents and valuables, that's why we decided to create this type of security system that will be more usable by everyone people. This system ensures perfect use of fingerprints when opening and closing doors. Through the project, we can provide users with high security. Fingerprint Most banks have lockers where the user has one key, and the bank has the master key. They also havea password that the user must tell the bank before entering the locker room, now if the user loses the key, it is a big security risk. There are many thieves around us who can easily or forcefully break our lockers so that we can lose our property, so to overcome this problem we create this type of security system. Many bank lockers do not guarantee the full safety of the user. In fingerprint vault system we can easily add more than 1 fingerprint in system so we can add fingerprint of our family member as nominee. And we can insert our multi-hand fingerprint if we face an accident and if we hurt or cut our finger so that we can use our selected user's fingerprint or other multi-hand fingerprint. If we are out of our house and need an urgent document or property, our family memberscan also use our lockers. This is a unique idea instead ofkeeping or protecting the keys. Our fingerprint vault system prioritizes not just security but also user experience. By incor- porating intuitive biometric authentication, we aim to createa system that is easy to use for individuals of all technical backgrounds. This ensures broader adoption and a more secure environment for everyone.Biometric authentication represents a significant leap forward in security technology. By leveragingunique biological characteristics such as fingerprints, thesesystems provide a highly secure and reliable approach to access control. Our fingerprint vault system exemplifies this advancement, offering a user-friendly and robust solution

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| Monthly Peer Reviewed & Referred Journal |

| Volume 7, Issue 4, April 2024 |

| DOI:10.15680/IJMRSET.2024.0704066 |

for protecting valuable assets.This revised version provides a more compelling narrative, delves deeper into the technical aspects, and highlights the user-centric design philosophy behind your fingerprint vault system.

II. RELATED WORK

A. *Design of a Sensor-Based Door Opening and Closing System Using Arduino for Women's Safety*

Chaurasia, Suhashini Awadhesh, et al. In addition to the method of knocking at regular intervals for security pur- poses, modern technological advancements have introduced a plethora of sophisticated security systems. These systems incorporate various sensors such as motion detectors, infrared sensors, and even facial recognition technology to ensure enhanced security measures. Motion detectors, for instance, can detect any movement within a specified range, triggering an alarm or activating surveillance cameras to monitor the area. Similarly, infrared sensors are effective in detecting heat signatures, enabling them to detect the presence of intruders even in low light conditions.

B. *Face Recognition and OTP Based Security Lock System*

Ghai, Garvit, Akshita Khanna, and S. Jerald Nirmal Kumar the password-based verification was executed. With this tech- nology security breaches are more oftening so to overcome thisproblem face and otp based verification is introduced. When the face is recognized using machine learning and OTP will be sent through gsm module. Facial recognition technology has made significant strides in recent years, thanks to the development of deep learning algorithms that can accurately identify individuals based on their facial features. In addition to facial recognition, OTP-based verification has become a popular method for securing online transactions. OTPs aretime-sensitive codes that are sent to a user's mobile devicevia SMS or a mobile app. These codes are unique to each transaction and are valid only for a short period, making it difficult for attackers to intercept and use them for fraudulent purposes.

C. *Bank Vault Security System Based on Infrared Radiation and GSM Technology*

Dutta, Mithun, et al. Banking security has been a greatimportance now a days for this bank vault security is im- plemented using infrared radiation, gsm technologies and many other sensors. Where GSM technology will help to send messages to concerned phone number. To open vault iris scanner, pin, fingerprint scanner is used. If there is any incident like wall breaking, then there will be infrared radiationthat is implemented between the walls. It is a more effective system than any other existing system. Infrared radiation isa technology that can detect changes in temperature and motion. By installing infrared sensors between the walls ofa bank vault, any attempt to break through the walls willtrigger an alarm, alerting security personnel to the potential threat. This technology provides an additional layer of security beyond traditional physical barriers, making it more difficult for intruders to gain access to the vault. GSM technology is used to send messages to concerned phone numbers in the event of a security breach. By integrating GSM modules into the bank vault security system, security personnel can receive real-time alerts when there is an incident, enabling them to respond quickly and effectively.

III. PROPOSED METHODOLOGY

The project to create an automated locker system powered by Arduino technology is an innovative solution that addresses the limitations of conventional padlocks commonly used by students. By using a fingerprint module for secure authen- tication, this system ensures that only registered users can access their lockers, providing an additional layer of security and convenience. The primary components of this system include an Arduino Mega, a servo motor, a button, and a liquid crystal display (LCD). The Arduino Mega serves as the microcontroller, managing the system's functionality and integrating the various components. The servo motor is usedto activate the locker mechanism, enabling the user to access their locker after successful authentication. The button is used to initiate the fingerprint scanning process, while the LCD displays the system's status and provides feedback to the user.

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| Monthly Peer Reviewed & Referred Journal |

| Volume 7, Issue 4, April 2024 |

| DOI:10.15680/IJMRSET.2024.0704066 |

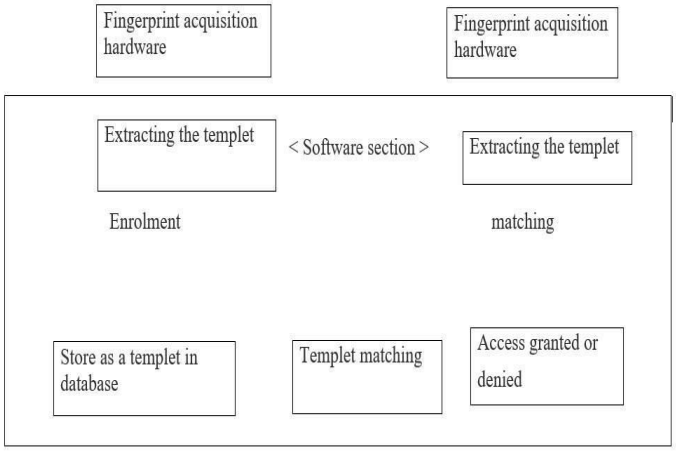

Figure 1: Block Diagram

The software controlling this system is developed using the embedded C programming language, allowing for robust functionality and customization. The software includes a finger- print recognition algorithm that detects and verifies the user's fingerprint by searching for a match in the database. After suc- cessful authentication, the system activates the corresponding locker and allows the user access. In addition to providing secure authentication, this automated locker system offers several other benefits. For example, it eliminates the needfor physical keys or combinations, reducing the risk of loss or theft. It also enables users to access their lockers more quickly and efficiently, improving the overall user experience. Furthermore, this system can be easily integrated into existing cabinet systems, making it a cost-effective solution for schools, universities, and other institutions. The modular design of the system also allows for scalability, enabling it to be customizedto meet the specific needs of different users and applications.

A. Fingerprint Registration:

Initially, users need to register their fingerprints in the system. During registration, the fingerprint module captures animage of the user's fingerprint and creates a unique template for that fingerprint. The Arduino then stores this template inits memory or uploads it to a database accessible via the WiFi module. The fingerprint minutiae extraction process involves several steps. First, the fingerprint image is preprocessed to enhance its quality and remove noise. This is followed by the extraction of the fingerprint's unique features, such as ridge endings and bifurcations. These features are then converted into a set of data points, which are used to create the unique template. Once the template is created, it is stored in the Arduino's memory or uploaded to a database. The template is then used for authentication purposes, by comparing it to the fingerprints of users attempting to access the locker system.If a match is found, the system activates the corresponding locker and allows the user access. It's worth noting that the registration process is an essential step in ensuring the security and accuracy of the fingerprint recognition system. By creating a unique template for each user's fingerprint, the system can accurately identify and authenticate users, reducing the risk of unauthorized access and improving the overall security of the locker system.

B. Verification Process:

When the user approaches the locker, they initiate the authentication process, usually by pressing a button. The fin- gerprint module recaptures the user's fingerprint and extracts the minutiae points. The Arduino compares these mark points with the stored fingerprint templates to see if there is a match. If a match is found, the Arduino sends a signal to the motor control IC to unlock the cabinet using the servo motor.On the other hand, if no match is found, the Arduino sends a signal to the motor control IC to keep the locker door locked, denying access to the user. The system may also provide feedback to the user through the LCD or an LED indicator, indicating that the authentication process has failed. It's important to note that the fingerprint recognition process is highly accurate and reliable, with a low false acceptance rate (FAR) and false rejection

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| Monthly Peer Reviewed & Referred Journal |

| Volume 7, Issue 4, April 2024 |

| DOI:10.15680/IJMRSET.2024.0704066 |

rate (FRR). The FAR is the likelihood that the systemwill incorrectly authenticate an unauthorized user, while the FRR is the likelihood that the system will incorrectly reject an authorized user. To further improve the accuracy and reliabilityof the fingerprint recognition system, the Arduino's firmware may include additional features such as liveness detection, which verifies that the fingerprint being scanned is froma living person, and anti-spoofing measures, which prevent attackers from using fake fingerprints to gain unauthorized access.

C. Locker control

After successful authentication, the Arduino sends com-mands to the motor control IC to activate the servo motorand unlock the cabinet door. After the user retrieves their belongings, the Arduino can send another command to lock the locker. This can be achieved by calling the unlockDoor() function with a negative value for the durationTime variable. This will cause the servo motor to rotate back to its minimum position, locking the cabinet door. It is important to note that the servo motor's position should be controlled carefully to avoid damaging the motor or the locking mechanism. The servo motor's maximum and minimum positions should be determined based on the specific requirements of the system, and the write() function should be used to control the servo motor's position gradually.

D. Wi-Fi Integration:

The Wi-Fi module can be used for additional functions such as sending notifications to users or administrators on successful/failed authentication. This can help to improve security and provide users with peace of mind, knowing that they will be notified if anyone tries to access their locker without authorization. In addition to notifications, the Wi- Fi module can facilitate remote monitoring and managementof the locker system. Administrators can access the system from any location with an internet connection, allowing them to add or remove users' fingerprints, view access logs, and perform other management tasks. This can help to reduce the administrative burden of managing the locker system, making it easier to add or remove users as needed. The Wi- Fi module can also enable integration with other systems and services, such as building management systems or access control systems. For example, the locker system could be integrated with a building access control system, allowing users to access their lockers using the same credentials they use to enter the building. This can help to streamline the user experience and improve overall security.

E. Integration with Fleet Management Software

The IoT-based protection system is seamlessly integrated with fleet management software, allowing operators to cen- trally control and monitor their entire fleet of service vehicles. Integration allows for efficient route planning, scheduling, and dispatching by providing real-time visibility into vehicle po- sition, status, and performance. Data-driven decision-making and continuous improvement programs are made possible by customizable dashboards and reports that give stakeholders practical insights into important indicators and KPIs. One of the primary benefits of this integration is efficient route planning, scheduling, and dispatching. By knowing the exact location and status of each vehicle in real-time, operators can optimize routes and reduce travel time, leading to increased productivity and cost savings. They can also quickly respond to changes in customer needs or emergencies, ensuring that their fleet is always operating at maximum efficiency. Another benefit of this integration is improved vehicle maintenance and repair. By continuously monitoring vehicle performance and identifying potential issues before they become major problems, operators can reduce downtime and extend the lifespan of their vehicles. Customizable dashboards and reportscan provide practical insights into important indicators such as fuel consumption, engine temperature, and battery life, allowing operators to proactively address potential issues and optimize vehicle performance. In addition, the integration of the IoT-based protection system with fleet management software can help operators improve their overall security and safety. By monitoring vehicle location and status in real-time, operators can quickly respond to potential security threats or accidents, ensuring the safety of their drivers and cargo. They can also implement customizable alerts and notifications to keep stakeholders informed of important events or issues.

F. Continuous Improvement and Optimization:

The IoT-based protection system is constantly improved and optimized to meet changing security threats and operational requirements. System updates and enhancements are informed by data analytics insights and feedback from real-world deployments. Ensuring system reliability, performance, and compliance with industry standards and regulations is ensured through routine maintenance and software upgrades. Logistics firms may consistently improve the security, efficiency, and safety of their service vehicles by utilizing IoT technology and data-driven insights. This will lead to an improvement in operational outcomes and customer satisfaction within the logistics industry.

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| Monthly Peer Reviewed & Referred Journal |

| Volume 7, Issue 4, April 2024 |

| DOI:10.15680/IJMRSET.2024.0704066 |

IV. RESULTS AND DISCUSSIONS

This research investigated the implementation of fingerprint security in a bank locker system. The primary objective was to enhance security for valuables stored within the bank. The project successfully integrated a fingerprint scanner with the locker mechanism, enabling access only for authorized users. The incorporation of fingerprint recognition significantly elevates bank locker security compared to traditional key-based systems. However, the implemented system goes beyond basic fingerprint access. The inclusion of environmental sensors like gas, object detection, and fire sensors creates a multi-layered security approach. This comprehensive system not only safeguards against unauthorized access but also protects valuables from environmental threats.

Future research could explore integrating additional security measures, such as two-factor authentication using a PIN or a mobile app notification for added access control. Additionally, improvements in fingerprint sensor technology could further enhance the system's accuracy and reliability.

By combining biometric authentication with environmental monitoring, this research project paves the way for a more secure and robust bank locker system, offering peace of mind to users and financial institutions alike.

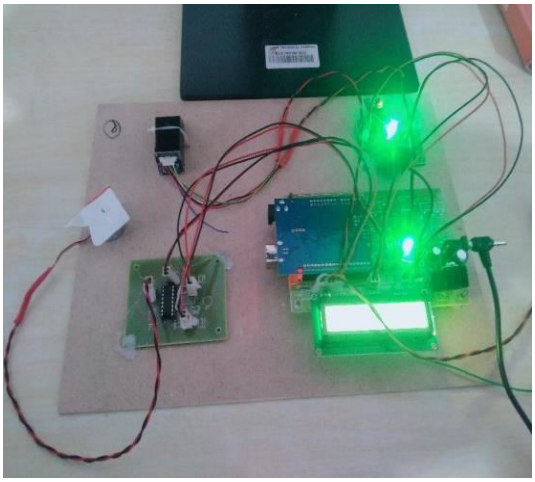

Figure 2: Circuit Board

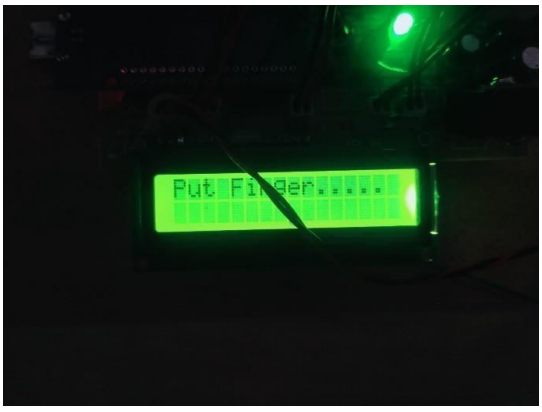

Figure 3: Finger Detection

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| Monthly Peer Reviewed & Referred Journal |

| Volume 7, Issue 4, April 2024 |

| DOI:10.15680/IJMRSET.2024.0704066 |

Figure 4: Finger Print Enrolling

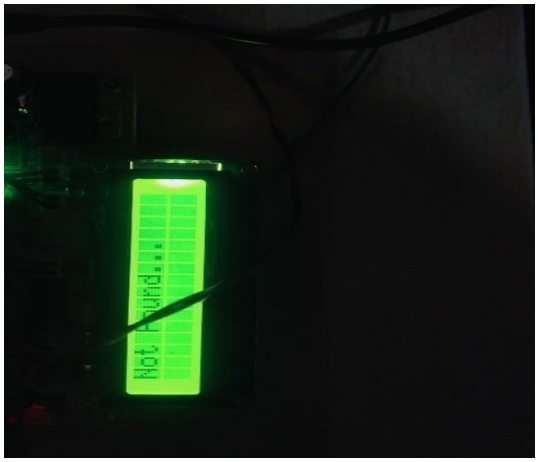

Figure 5: Finger Print Not Found

Figure 6: Opening and Closing of Lock

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| Monthly Peer Reviewed & Referred Journal |

| Volume 7, Issue 4, April 2024 |

| DOI:10.15680/IJMRSET.2024.0704066 |

V. CONCLUSION

In conclusion, we reviewed some papers which have worked on this project. In our paper we introduced biometric based locker which provide high degree of security. Any authorised user will unable to access the locker. We use fingerprint as theverification system as duplication of fingerprint is like unable. The system is cheap and easy to use. This system can be mounted anywhere, where you need high degree of security thelow cost of the project is very important factor in this project. These locker system is very reliable and safe.Beyond enhanced security, this system boasts several additional benefits. Its user-friendly design makes fingerprint scanning a quick and convenient process. Furthermore, the system's affordability makes it an attractive option for various applications. Thecompact design allows for versatile mounting, making it ideal for securing valuables in homes, offices, gyms, or anywherea high level of security is paramount. The project prioritizes not only security but also reliability and cost-effectiveness. By utilizing readily available components, the system remains affordable without compromising on its core functionality. This combination of robust security, user-friendliness, and affordability makes this biometric locker system a compelling solution for a wide range of security needs.

REFERENCES

1. Chaurasia, Suhashini Awadhesh, et al. "Design of a Sensor-Based Door Opening and Closing System Using Arduino for Women's Safety." AI Tools and Applications for Women's Safety. IGI Global, 2024. 74-90.
2. Ghai, Garvit, Akshita Khanna, and S. Jerald Nirmal Kumar. "Face Recognition and OTP Based Security Lock System." International Conference on Communications and Cyber Physical Engineering 2018. Singapore: Springer Nature Singapore, 2024
3. Dutta, Mithun, et al. "Bank vault security system based on infrared radiation and GSM technology." Intelligent Data Communication Tech- nologies and Internet of Things: ICICI 2019. Springer International Publishing, 2020.
4. Mounika, N. Chandra, and M. Vamsi Krishna. "ANDROID BASED SECURITY SYSTEM FOR BANK LOCKERS." Journal of EngineeringSciences 14.05 (2023).
5. Siswanto, Apri, Hendra Gunawan, and Rafiq Sanjaya. "Prototype Stor- age Locker Security System based on Fingerprint and RFID Technol- ogy." (2019): 11-14.
6. Soni, Shubham, Rajni Soni, and Akhilesh A. Waoo. "RFID-based digital door locking system." Indian Journal of Microprocessors and Microcontroller (IJMM) 1.2 (2021): 17-21.
7. Thomas, Akash, Kezia Mariam Varghese, and Sheba Elizabeth Kurian3Er Ashly John. "Fingerprint Based Bank Locker Security System." Int. Res. J. Eng. Technol 8.7 (2021): 2076-2082.
8. Singh, Prabhdeep, and Dibyahash Bordoloi. "Visual Cryptography Authentication for Locker Systems using Biometric Input." Webology 18.5(2021): 3126-3131.
9. Kosar, Kosar, et al. "GSM Based Bank Vault Surveillance Process with Fingerprint and Password and Preventative Action Against Unauthorized Person." Proceedings of the 11th International Conference on Robotics, Vision, Signal Processing and Power Applications: Enhancing Research and Innovation through the Fourth Industrial Revolution. Singapore: Springer Singapore, 2022
10. Dewangan, Rekha, Vishnu Kumar Mishra, and Megha Mishra. "A review on secured bank locker system using fingerprint, image and RFID technique." Int. Res. J. Eng. Technol. (IRJET) 7.07 (2020): 4786-4789.
11. Bhanushali, Mahesh, et al. "Biometric Authentication System using Arduino." Journal of Advancement in Parallel Computing 3.3 (2020): 1- 5.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH

IN SCIENCE, ENGINEERING AND TECHNOLOGY

| Mobile No: +91-6381907438 | Whatsapp: +91-6381907438 | ijmrset@gmail.com |

www.ijmrset.com