Facilitating Fingerprint-based Door Automation System using RFID and Bluetooth

Dr.A.Sherly Alphonse
School of Computer Science and Engineering
Vellore Institute of Technology Chennai
sherly.a@vit.ac.in

Chitranshu Gupta
School of Computer Science and Engineering
Vellore Institute of Technology Chennai
chitranshu.gupta2021@vitstudent.ac.in

Mohammad Kamran Warsi
School of Computer Science and Engineering
Vellore Institute of Technology Chennai
mohammadkamran.warsi2021@vitstudent.ac.in

Karmokar Dhruv Shantu
School of Computer Science and Engineering
Vellore Institute of Technology Chennai
dhruv.karmokar2021@vitstudent.ac.in

Aryaman Tamotia
School of Computer Science and Engineering
Vellore Institute of Technology Chennai
aryaman.tamotia2021@vitstudent.ac.in

2023 Innovations in Power and Advanced Computing Technologies (i-PACT) | 979-8-3503-2518-8/23/$31.00 ©2023 IEEE | DOI: 10.1109/i-PACT58649.2023.10434693

***Abstract*— This paper focuses on the adoption of biometric and RFID security gadgets as innovative solutions for enhancing door lock systems. The traditional reliance on physical keys has proven vulnerable to security breaches, prompting the need for more robust measures. Biometric features such as Fingerprint, Voice and Bluetooth offer unparalleled security by leveraging unique biological characteristics for authentication. Additionally, integrating RFID technology enables convenient access control through assigned cards or tags, eliminating the need for physical keys or complex passwords. The combination of these cutting-edge solutions establishes a comprehensive security infrastructure, significantly reducing risks associated with conventional lock systems. This research highlights the benefits and applications of these technologies in various settings, emphasizing their role in creating a safer environment for individuals and organizations.**

Keywords*— Bluetooth, door, IoT, RFID, Arduino

I. INTRODUCTION

In this project, the proposed work leverages the power of fingerprints as a secure and personalized key. By implementing an Arduino UNO-based system, it integrates various devices to create an intelligent and highly secure lock. Bluetooth connectivity will enhance the functionality, allowing for seamless communication between the lock and authorized users' smartphones or other devices [1]. This project aims to maximize security levels by combining the reliability of biometric identification with advanced features to ensure fool proof protection.

Our objective is to develop an efficient and user-friendly security solution that minimizes the risk of unauthorized access and eliminates the hassle of managing physical keys [2]. By embracing this innovative approach, it is strived to provide enhanced security for homes, shops, and offices, fostering peace of mind and enabling a seamless user experience. This redefines security standards and bring greater confidence to our daily lives.

Ensuring the security of IoT connected entities is of utmost importance, particularly when dealing with personal, enterprise, or consumer data. When it comes to implementing a secure smart door lock (SDL), addressing security challenges becomes a critical task.

It is needed to establish a robust and highly secure authentication mechanism between the user's device like smartphone and the smart door lock. This authentication process needs to be reliable and resistant to various attacks. The connection protocols are used in the product to facilitate authentication and access control. Additionally, the local Wi-Fi network provide sufficient security measures to meet the required obligations for the smart door lock. Selecting an appropriate microcontroller is crucial to achieving the objectives of the product and establishing a secure IoT system. The chosen microcontroller should possess robust security features and be capable of handling the necessary encryption and authentication protocols.

Addressing these questions and challenges is essential to ensure the security of the smart door lock [2]. By focusing on strong authentication, selecting secure connection protocols, and choosing a suitable microcontroller, the aim is to create a secure IoT system that effectively protects the SDL and the associated data.

The smart door lock we are developing will possess the capability to regulate the unlocking process upon arrival at an office space. The arrival door is situated on the third floor within a big building and serves as a connection point between the office area, a stairwell, and several elevators. As a result, the smart lock must be able to manage a significant flow of traffic while maintaining reliable functionality in this specific environment [3].

One crucial requirement for the smart door lock is to ensure that only authorized individuals can unlock the door within the designated area encompassing the stairwell, elevators, and the door itself. To achieve this, the door lock

979-8-3503-2518-8/23/$31.00 ©2023 IEEE

will incorporate an accurate sensing mechanism to determine the location of the user.

In addition to the location-based access control, the smart door lock system will also utilize a fingerprint authentication mechanism. This additional layer of security enhances the overall protection and assures that only authenticated individuals with verified fingerprints can gain access to the office space [4]. By combining these three features—a location-based sensing mechanism and a fingerprint door lock system—the smart door lock will provide a robust and secure solution for controlling access to the office space.

II. LITERATURE SURVEY

The survey drawn from a few related articles are addressed below:

[1] Sriskanthan highlighted a variety of approaches that can be used with advanced technology. Home automation is one of the most cutting-edge technologies available today. In order to realize home automation, several tasks of managing home appliances have been completed, such as door locking and unlocking using smartphone-based door lock system.

[2] Bhardwaj and K. Kaushik discussed about the RFID RC-522, a 13.56MHz contactless communication chip, designed for low-cost and small-sized applications. It integrates advanced modulation and demodulation techniques for various passive contactless communication methods. The Arduino Uno microcontroller board is also mentioned, with its key features including 14 digital I/O pins (6 of them PWM capable), 6 analog inputs, and 16MHz clock speed. It supports the microcontroller and can be powered via USB or an AC-to-DC adapter.

[3] Toschi developed a mobile application that integrates home automation systems. The study focuses on extending the functionality of home automation by leveraging the capabilities of a mobile platform.

[4] In their study, Ponmalar et al. discussed the use of fingerprint-based locks and attendance record-keeping devices in offices. However, due to the pandemic, these methods are no longer considered suitable. To address this issue, this system utilizes a solenoid lock for door security. Additionally, a mobile application is employed to verify and validate the fingerprint data, along with the user's ID, which is then sent to an Arduino board via Bluetooth. The smartphone's fingerprint sensor is used to lock and unlock the entryway.

[5] This study proposes a door automation system using infrared sensors and voice command authentication. The system detects individuals approaching the door through infrared sensors. User authentication is performed through voice commands, matching against pre-registered voice patterns. This eliminates the need for physical keys and offers a convenient hands-free approach. The system ensures accurate and reliable voice recognition for enhanced security.

[6] In their project, Sricharan et al. proposed a novel security system that incorporates multiple authentication methods such as password, OTP (One-Time Password), biometrics, and RFID cards/tags. The system allows authorized access through the correct input of a password and OTP, or by utilizing an authorized RFID card/tag. In emergency situations, biometric access through a mobile phone is available. The project highlights the cost-effectiveness and practicality of the system for daily use. This information can be utilized in the literature survey as an example of a comprehensive security system that employs multiple authentication techniques to ensure secure access.

[7] Verma and Tripathi proposed a solution to the vulnerabilities of traditional locks by combining door locks with biometrics. They suggest using fingerprint recognition as a unique identifier for enhanced security. By implementing this system, they aim to prevent unauthorized access and eliminate the issues associated with key loss. The researchers utilize Arduino to augment the security features of the system. Their study highlights the potential of biometric-based door locks to improve overall security.

[8] Kulkarni et al. proposed a biometric-based door access system using Arduino and fingerprints for enhanced security. Traditional locks are prone to unauthorized access, and pattern-based systems have vulnerabilities. The utilization of biometrics ensures a higher level of security as fingerprints are unique to everyone. The project aims to minimize costs by utilizing a simple door lock. The system provides a unique and secure method of personal identification to prevent unauthorized entry into homes, offices, and shops.

[9] In their study, Md Mostafizur Rahman Komolet discussed the pattern of interleaved ridges and valleys that make up a fingerprint. These ridges and valleys form specific shapes called minutiae, with ridge ending and ridge bifurcation being the most considered types. The study provides definitions for fingerprint structures and their components. The utilization of an optical fingerprint sensor requires the enrollment of fingerprints by assigning ID numbers to each print. The RFID technology is used to enable wireless data transmission, and an RFID reader module is interfaced with an Arduino to control the security door lock and RGB LED. This research provides valuable insights into the implementation of fingerprint-based security systems.

[10] Salih et al. suggests an information service and Attendance Management System (AMS) based on RFID for institutions. The system aims to efficiently manage student attendance, track absenteeism, and provide relevant information services. By integrating RFID technology, a programmable Logic Circuit (e.g., Arduino), and a web-based application, the proposed system reduces documentation efforts, saves time, and minimizes power consumption. The study also evaluates existing RFID-based attendance systems and identifies future research directions.

[11] Deepty et al. proposed the application of technology in the field of security, specifically focusing on door access systems. The study presents an IoT and Wi-Fi based door

access control system that utilizes smartphone biometrics and cloud-based verification. The system ensures multiple layers of automated security, preventing unauthorized access. Raspberry Pi and other advanced devices are used to validate the system in practical environments.

III. COMPONENTS AND HARDWARE

1. Arduino UNO:
   The Arduino UNO, as shown in Fig. 1, is a microcontroller board that functions as the brain of our project. It gives the needed computational power as well as interfaces for many other components to control the lock system.

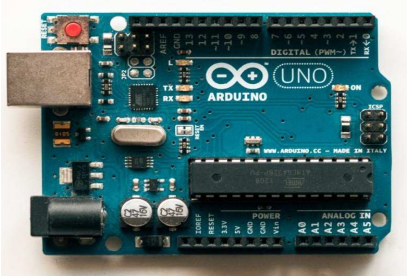

Fig. 1. Arduino UNO

2. Fingerprint Sensor:
   One essential component for biometric authentication is the fingerprint sensor R307, as shown in Fig. 2. It records and examines distinctive fingerprint patterns to enable authorised individuals to open the lock [12]. A fingerprint sensor embedded with a TTL UART interface is known as the R307 fingerprint module. The owner or user configures the module in either 1:1 or 1:N mode and additionally stores the fingerprint data template to enable the identification of registered or authorized individuals.

Fig. 2. Fingerprint sensor R307.

3. Solenoid Lock:
   Solenoid Lock is a robust and dependable DC 12V electric lock assembly equipped with a solenoid mechanism. As shown in Fig. 3, this lock is well-suited for ensuring the security of vending machines, storage shelves, and file cabinets. It incorporates an emergency unlocking feature and activates instantly upon circuit disconnection. With the inclusion of an energy-efficient relay, this lock not only delivers enduring performance but also conserves power.

Fig. 3. Solenoid Lock

This electric lock helps for robust security and seamless access control.

4. Relay Module:
   This relay module, as shown in Fig. 4, has one channel. The high-power circuit that is run by the microprocessor and the low and high voltage circuit that are measured by the microcontroller are not linked. Every circuit is protected by the relay module from every port.

Fig. 4. Relay Module

5. Bluetooth**:**
   Bluetooth technology enables wireless

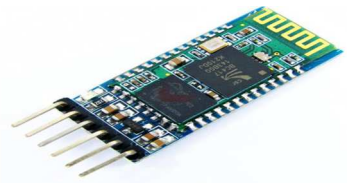

Fig. 5. Bluetooth

communication between the lock system and authorized devices such as smartphones. By integrating Bluetooth as in Fig.5, users can remotely control and manage the lock, providing added convenience and accessibility.

6. RFID:
   The RFID RC522 module, as shown in Fig. 6, is commonly used in door lock systems for efficient and secure identification. It reads RFID tags or cards, enabling quick and contactless identification. When an authorized user presents their RFID card or tag, the module retrieves the unique identification information stored on it using radio frequency signals. Operating at 13.56 MHz, the RC522 supports multiple RFID protocols for compatibility with various applications. Integrating it into door lock systems enhances security and convenience by

eliminating physical keys and providing seamless access for authorized individuals.

Fig. 6. RFID Sensor

7. Breadboard & Jumper Wires**:**
   The breadboard and jumper wires, as shown in Fig. 7, are essential for prototyping and connecting various components together. The breadboard provides a platform for temporary circuit connections, while the jumper wires facilitate the transfer of electrical signals between the components.

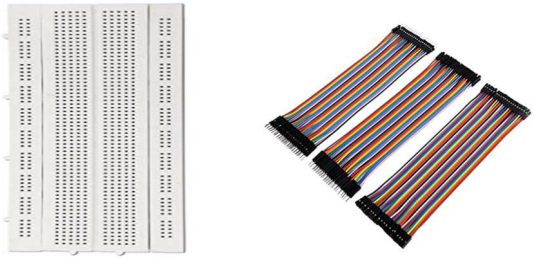

Fig. 7. Breadboard & Jumper Wires

IV. COMPUTING CONCEPTS AND METHODOLOGY

The concept behind the smart door lock system involves the following steps:

1. Enrolling Fingerprint: The fingerprint enrollment process is carried out using the Arduino IDE, as shown in Fig. 8, and relevant libraries. This involves capturing the fingerprint data from a user and storing it securely for future reference.
2. Storing and Testing: The enrolled fingerprint data is stored in a secure manner, such as in the Arduino's memory or external storage. The stored data is then used for testing and verification purposes during the authentication process.
3. Algorithm for Serial Communication: The Arduino Uno, which serves as the central controller for the smart door lock system, utilizes an algorithm to handle the serial communication. This algorithm facilitates communication between different components of the system, such as the fingerprint sensor, Bluetooth module, and other necessary modules.
4. Dual Serial Communication: The Arduino Uno establishes two separate serial communication channels. One channel is dedicated to communicating with the fingerprint sensor, allowing for the capture and verification of fingerprint data. The other channel is used for communication with external devices, such as a Bluetooth module, as shown in Fig. 5, to enable wireless unlocking of the door. By implementing this concept, the smart door lock system can accurately capture and verify user fingerprints, store the data securely, and utilize an algorithm for efficient serial communication.

This approach combines hardware components, software programming [13], and data storage techniques to create a robust and secure door lock system with fingerprint and Bluetooth capabilities. This chapter outlines the methodology and approach employed in this project.

The work consists of four main stages: Pilot Study, Implementation of Design, Design of Prototype, and Testing. The first two phases will be carried out in a sequential manner, while the latter two will be executed repetitively. This structure aims to mitigate risks and challenges related with the project, such as incorrect code implementation or prototype misalignment. It also provides a deeper consideration of the definition of the problem and helps establish the project's scope and boundaries [14].

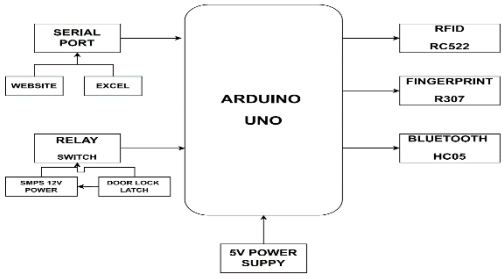

Fig. 8. Architectural Diagram

V. SOFTWARE DEVELOPMENT, REPRESENTATION, AND RESULTS

The primary result of the door lock system, as shown in Figs. 8,9, and 10 is a secure and efficient access control solution. The system allows users to unlock the door using their fingerprint, providing a convenient and reliable method of authentication. The system also includes features that enhance usability and functionality.

Firstly, the system integrates with an Excel spreadsheet, updating it with timestamps whenever the door is unlocked. This feature enables easy tracking and monitoring of access activity.

Secondly, the system includes Bluetooth connectivity, allowing authorized users to unlock the door using their smartphones. This wireless access control provides flexibility and convenience.

Thirdly, the integration with MIT App Inventor enables the development of an Android application that provides a user-friendly interface for controlling the door lock. Users can unlock the door, monitor access logs, and perform other functions through the app.

Furthermore, the system incorporates voice command functionality using Google voice control. This enables users to unlock the door by simply speaking a command, adding an additional layer of convenience and accessibility. Overall, the door lock system's primary result is a comprehensive and versatile access control solution that combines fingerprint authentication, Bluetooth connectivity, integration with Excel and local host websites.

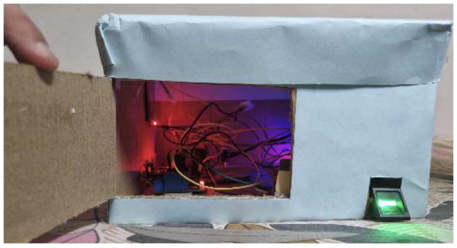

Fig. 9. Working Model

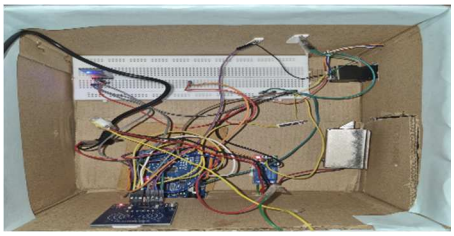

Fig. 10. Working Model with Sensors

VI. CONCLUSION

In this IoT project, as shown in Fig. 10, our team designed a highly secure and user-friendly smart door lock system, incorporating cutting-edge biometric and RFID technologies along with Bluetooth connectivity. The system utilized an Arduino UNO microcontroller as the central controller and featured a robust fingerprint sensor (R307) for biometric authentication. Users could enroll their fingerprints securely, and the system stored this data for future verification. To enhance accessibility and convenience, the system integrated Bluetooth technology, enabling users to remotely unlock the door using their smartphones. Moreover, RFID technology was employed for quick and contactless identification, adding an extra layer of security by eliminating the need for physical keys. The system's versatility extended to voice command authentication, further enhancing accessibility. Additionally, the project incorporated features like access logging in an Excel spreadsheet and Android application integration through MIT App Inventor. In summary, our IoT-based smart door lock system successfully combined advanced technologies to offer a comprehensive and secure access control solution, ensuring only authorized individuals could unlock the door while providing seamless user experiences.

The project's outcome was a functional and adaptable smart door lock system that combined fingerprint, RFID, and Bluetooth technologies to enhance security and convenience. Users could enroll their fingerprints for biometric authentication, remotely unlock the door via Bluetooth-enabled devices, and utilize RFID tags or cards for swift and contactless access. The system also featured voice command authentication for added convenience. Furthermore, it logged access activity in an Excel spreadsheet and offered an Android application interface for easy control. This project achieved its objectives of developing a secure and user-friendly door lock system, demonstrating the potential of IoT and advanced technologies in redefining security standards for various settings, from homes to offices.

REFERENCES

[1] N. Sriskanthan, F. Tan, and A. Karande, “Bluetooth based home automation system,” Microprocessors and Microsystems, vol. 26, no. 6, pp. 281–289, Aug. 2002, doi: https://doi.org/10.1016/s0141-9331(02)00039-x.

[2] Bhardwaj A, Kaushik K. ISF: IoT Firmware security analysis to secure IoT-based Smart Home Ecosystems. Authorea Preprints; May 2022. DOI: 10.22541/au.165216257.78827590/v1.

[3] G. M. Toschi, L. B. Campos, and C. E. Cugnasca, “Home Automation Networks: A survey,” *Computer Standards & Interfaces*, vol. 50, pp. 42–54, February 2017. doi:10.1016/j.csi.2016.08.008.

[4] A.Ponmalar, J.Anand, S.Dharshini, K.Aishwariya, S.Mahalakshmi and S.Abinaya, “Smartphone controlled fingerprint door lock system (SCFDLS),” *Advances in Parallel Computing Technologies and Applications*, November 2021. doi:10.3233/apc210164.

[5] S.Ganesh, R.Prem Kumar, “Implementation of Secure Door Automation Systems using Infrared Sensors,” *International Journal of Trendy Research in Engineering and Technology*, vol. 4, no. 6, pp. 1-7, October 2020.

[6] B. Sricharan, J. U. Sanjana, T. V. Vani, and C. N. Sujatha, “RFID based ATM security system using IOT,” *2022 International Conference on Intelligent Controller and Computing for Smart Power (ICICCSP)*, July 2022. doi:10.1109/iciccsp53532.2022.9862486.

[7] G. K. Verma and P. Tripathi, “A digital security system with door lock system using RFID technology,” *International Journal of Computer Applications*, vol. 5, no. 11, pp. 6–8, August 2010. doi:10.5120/957-1334.

[8] P. Kulkarni, Y. Patil, A. Dagade, and A. Kapse, “Finger print based attendance system using Arduino,” *SSRN Electronic Journal*, April 2020. doi:10.2139/ssrn.3645323.

[9] M. Mostafizur Rahman Komol, “RFID and finger print based dual security system: A robust secured control to access through Door Lock Operation,” *American Journal of Embedded Systems and Applications*, vol. 6, no. 1, pp. 15, June 2018. doi:10.11648/j.ajesa.20180601.13.

[10] H. D. Rjeib, N. Salih, A. Al, B. Al-Sadawi, and H. Alsharqi, “Attendance and information system using RFID and web-based application for academic sector,” *International Journal of Advanced Computer Science and Applications*,” vol. 9, no. 1, pp. 1-5, January 2018. doi:10.14569/ijacsa.2018.090137.

[11] R. R. Deepty, A. Alam, and Md. E. Islam, “IOT and Wi-Fi based door access control system using mobile application,” *2019 IEEE International Conference on Robotics, Automation, Artificial-intelligence and Internet-of-Things (RAAICON)*, May 2019. doi:10.1109/raaicon48939.2019.09.

[12] A. Baniukevic, D. Sabonis, C. S. Jensen, and H. Lu, “Improving wi-fi based indoor positioning using bluetooth add-ons,” *2011 IEEE 12th International Conference on Mobile Data Management*, June 2011. doi:10.1109/mdm.2011.50.

[13] K. Wijaya, J. A. Heriyanto, D. I. Satya, J. Godjali, and R. Rahmania, “Smart RFID system for Locker Cabinet Security using Android App,” *2022 4th International Conference on Cybernetics and Intelligent System (ICORIS)*, February 2022.

doi:10.1109/icoris56080.2022.10031313.

[14] A. A. Najib, R. Munadi, and N. B. Aditya Karna, “Security system with RFID control using E-KTP and internet of things,” *Bulletin of Electrical Engineering and Informatics*, vol. 10, no. 3, pp. 1-8, June 2021. doi:10.11591/eei.v10i3.2834.