Mathematical Statistician and Engineering Applications
ISSN: 2094-0343
2326-9865

Smart and Secure Door Lock with Dual-Factor Authentication for Critical Zones

Mohammed Shoaibuddin Ahmed

Dept. of Computer Science

ISL Engineering College

Hyderabad, Telangana, India

shoaibuddin.021@gmail.com

Mohammed Noor Ahmed

Dept. of Computer Science

ISL Engineering College

Hyderabad, Telangana, India

mohammednoorahmed05@gmail.com

Mohammad Mustafa Hussain

Dept. of Computer Science

ISL Engineering College

Hyderabad, Telangana, India

hussainmohammadmustafa@gmail.com

Syed Omer Farooq

Assistant Professor

ISL Engineering College

Hyderabad, Telangana, India

omerfarooq@islec.edu.in

Article Info
Page Number: 1491-1501
Publication Issue:
Vol. 72 No. 1 (2023)

***Abstract*—**In recent years, the Internet of Things (IoT) technology has received a lot of attention, and almost every person wants their tasks to be done automatically and securely by using IOT devices. Due to increasing concerns about security, most traditional home locks are being replaced with IOT-based smart door lock systems. However, there is no appropriate solution to the requirements for organizations, banks, offices, and other critical locations that require more protection. As a result, smart home locks, which were primarily designed for residential use, are the only option left for organizations. As a solution, a security system is devised using Raspberry Pi based on two-type authentication involving either RFID or fingerprint identification in the first step and face recognition in the last

step. Along with this, there are other functionalities, such as remote door access, a log registry to keep track of persons entering and leaving the premises, alerts for suspicious activity, and a specialized IR-based door feedback system that monitors whether the door is open or closed. The presented system aims to provide organizations with a reliable and secure means of controlling access to their premises with an average processing time of around 8 seconds.

Keywords— *Internet of Things, Face recognition, Raspberry Pi, Firebase, MQTT Protocol, LBPH Algorithm.*

Article History
Article Received: 15 October 2022
Revised: 24 November 2022
Accepted: 18 December 2022

I. INTRODUCTION

Security has emerged as the primary concern in the age of technology in every domain worldwide. With the rising incidents of security breaches and risks, most banks and other organizations are looking for more secure ways to safeguard their premises and assets from theft or damage caused by unauthorized access. To address this issue, organizations are trying to adopt more modern and secure solutions, such as smart door-locking systems utilizing the Internet of Things (IoT). Even though some of these locks were originally designed for homes, they may not be suitable for the specific requirements needed by organizations. Despite this, traditional locks are still in use, along with smart locks.

A door acts as a first line of defence to keep the premises physically secure [3] with a lock must be installed on it. Initially, traditional locks that required a physical key were used to access a door. However, these locks had a number of shortcomings such as being easy to bypass, and handling keys carefully, resulting in the lock being useless if the keys were lost. In recent decades, the rise of IoT technology has led to innovation and transformation in traditional locks, making them more reliable and suitable for present-day use. These IoT-enabled locks may offer a variety of features including remote controllability, personalized access, real-time activity log maintenance, alerts, and notifications.

At present, there are many variations of IoT locking systems based on Bluetooth, RFID, Face recognition, OTP, and Passwords. Bluetooth-enabled smart locks [2] allow users to remotely control their doors from their devices through Bluetooth. However, this technology may not be suitable for all users, particularly those who do not own a Bluetooth-compatible device; RFID locks [7] use radio waves to communicate between the lock and the RFID card, which is equipped with a Low-Frequency chip. However, a misplaced RFID card can be a security problem because someone who is not authorized might use the card to enter restricted areas; OTP (One-Time Password)-based door locks [3] require a unique, randomly generated password each time to unlock the door, but the user must have their device with them to receive the OTP. Password-based smart locks [8] enable the user to enter either a PIN or a password to get access. The user may set up a unique password and update it at any moment. Furthermore, users may use weak, guessable passwords, making it much easier for intruders to get access. Biometric-based smart locks restrict access by making use of an individual's unique physical characteristics, such as a fingerprint, facial recognition, or iris scan. These locks are convenient, primarily because users do not have to remember or carry keys or cards, and they ensure a high level of security considering the fact that biometric data is unique to each individual. Moreover,

the above lock systems may also use other technologies like ZigBee, LoRa, and Z-Wave to communicate and operate.

This paper proposes a smart door-locking mechanism that offers a two-type authentication process, notifications, and intruder alerts, as well as a real-time activity record, IR-based door feedback, and can provide a more modern and secure way for organizations that suits their specific need to safeguard sensitive areas.

II. LITERATURE SURVEY:

In the study [2], a smart door-locking system offers three approaches for locking and unlocking the door: keypad entry, Bluetooth connection, and SMS messaging. All three modes operate on a 4-digit password. A warning message to the owner's phone is sent if three consecutive incorrect password attempts are made by a user. The presented system can encounter some issues that may impact its operation. For instance, if the GSM network is down, the owner cannot get an intrusion detection alert.

The system shown in [9], aims to develop a secure and cost-effective biometric Smart Door Locking System that utilizes a smartphone's fingerprint to prevent unauthorized access in organizations. The Arduino Nano microcontroller and Bluetooth link are used to establish communication with the smartphone. However, relying on a smartphone's fingerprint sensor may not be as reliable as using a dedicated biometric sensor, and Bluetooth may not offer the same level of security as other wireless protocols like ZigBee or Z-Wave.

In [4], the authors utilized a Node MCU module with an ESP8266 processor microcontroller to develop a door-locking mechanism that offers two distinct interfaces with varying access controls for the owner and guest user. The guest has access only to the keypad located on the door, where they must enter the generated PIN according to the arrival time recorded by the owner. The main drawback of the proposed system is that the owner must manually input the guest's arrival date and generate a PIN for them.

In [5], the authors develop a secure fingerprint-based door-locking mechanism that aims to identify authorized individuals and prevent unauthorized access to the secured area. The system also employs a Micro Electro Mechanical System sensor to detect door tampering and sends alerts to authorized personnel.

III. IMPLEMENTATION

The primary goal of this research is to enhance the security of the existing door-locking mechanisms, which may not offer much safety in locations where additional security is required.

A. Architecture and Operation of the Proposed System

The proposed locking system operates on a Raspberry Pi 4 model B with 8GB of RAM as the main processing unit. Fig. 1 illustrates the hardware connections of the presented smart door-locking system. The mechanism is designed in such a way as to be a more robust security solution by offering dual-factor authentication with the flexibility of having two alternative

options for first-factor authentication. Each user will have a unique login credential stored in the cloud-hosted Firebase database [1]. Every time user accesses the door, they must authenticate themselves.

During the first step of authentication, a user has given the option to verify their identity in two ways: either by using their fingerprint or an RFID card. If a user misplaces their RFID card, they may still gain access by verifying their fingerprint. The fingerprint sensor won't find any matches if the finger is injured or for any other reason. In these cases, RFID can be used, which is also a faster way to gain access. When a user wants to use their RFID card, the MFRC522-based RFID Reader module reads the unique code stored on each card and compares it with the database to validate the user's identity. If the user prefers to use their fingerprint instead, the R307S fingerprint module scanner captures an image of the user's fingerprint and compares it against the stored template model in the fingerprint sensor to authenticate the user's identification.

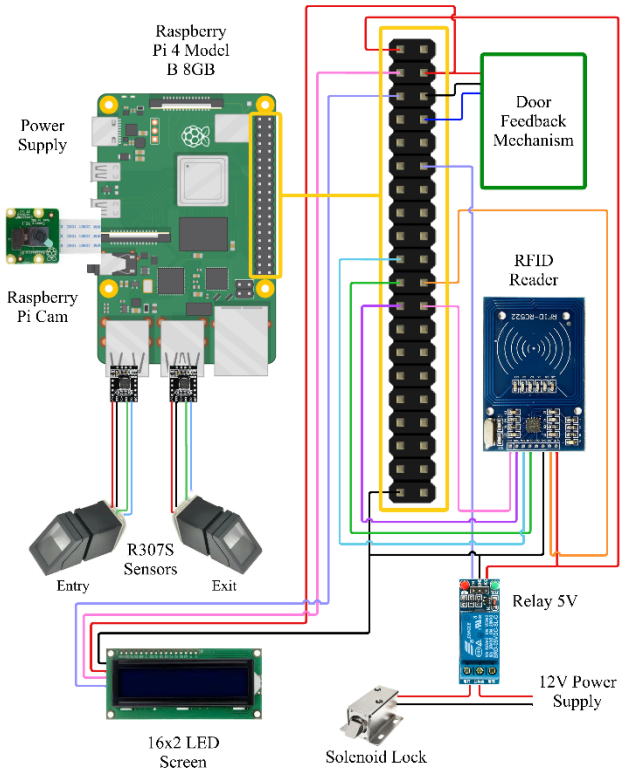

Fig. 1. Hardware connections of the proposed door locking system.

Face Recognition technology is implemented in the final step of the authentication procedure, which begins immediately only after the user has been authenticated in the previous step. The Raspberry Pi Camera module installed on the lock captures the user's visuals and passed them to the trained model. Once the user is verified, they can access the door, and a log entry is created in the database that includes their name, ID, and the time they entered the restricted area as well as the user's image taken during the facial recognition process. In addition, If the user fails to close the door properly after gaining access within the specified time limit of 5 seconds, an alert is sent to the administrator. Apart from that, while exiting, the user must verify

their identity again by using their fingerprint. If the authentication fails, the door will not unlock.

The project's step-by-step approach is visually represented in Figure 2, which shows a flowchart highlighting each stage of the process.

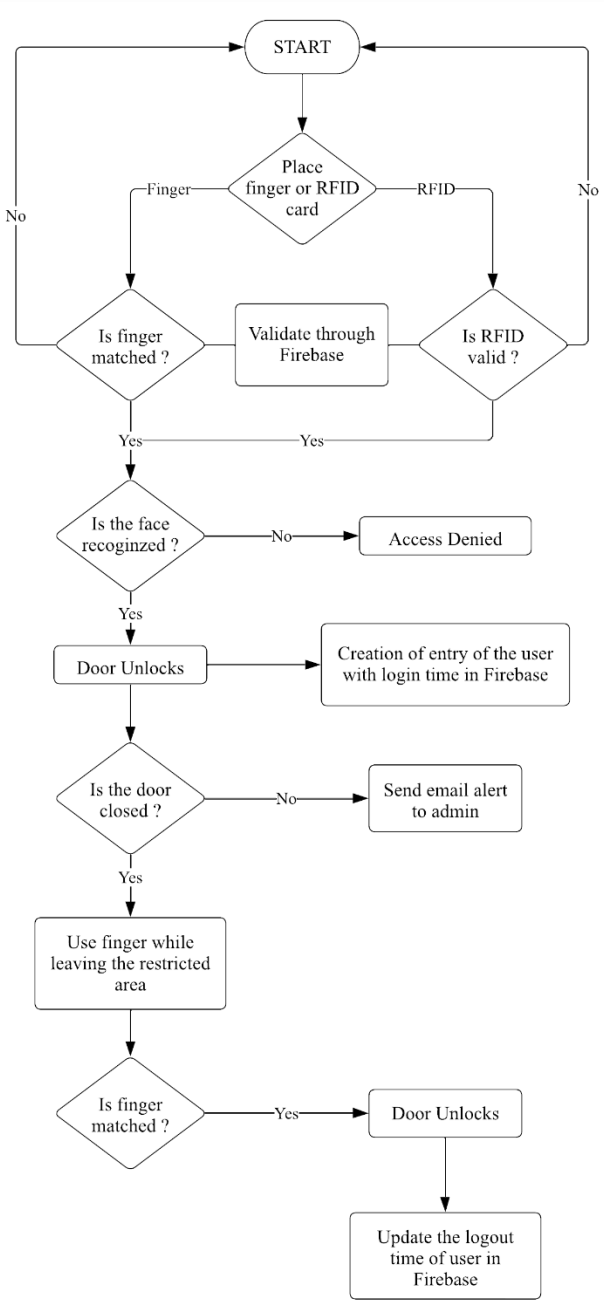

Fig. 2. Flowchart of the Proposed System.

B. Hardware and Software Requirements

To implement the digital door security system mechanism, several hardware components and software tools were utilized, which are listed in Table I.

TABLE I. HARDWARE AND SOFTWARE REQUIREMENTS

Category	**Component**	**Function**
Hardware	Solenoid lock	To Open/Close the door
	Raspberry pi	As Microprocessor
	LCD Display	To display messages
	Raspberry pi Camera	Face recognition
	Fingerprint sensor (R307S)	Biometric authentication
	RFID sensor	Non-Biometric authentication
	Door Feedback	To verify the status of the door: open/close
Software	Thonny IDE	To run the program
	Firebase database	To maintain log register and user profiles.
	MQTT Protocol	To establish communication between the lock and the admin's device.
	Website	For admin to monitor user activity and control the door lock remotely.

IV. FEATURES OF THE SYSTEM

A. Specialized Door Feedback

The automated door lock system has a dedicated mechanism that ensures the door is perfectly closed. The IR transmitter on the door sends a unique binary pulse which is received by the IR receiver on the door frame. IR receiver will be activated only when the door is closed by forming a closed circuit using nails as shown in Fig 3. If the door is not properly closed, the feedback mechanism alerts the system, which then takes action by sending an alert to the admin via Email. The entire process begins every time whenever the door is unlocked for entry and exit. This feature improves overall system security by preventing unauthorized access or attempts caused by a poorly secured door.

Fig .3. Specialized IR-based door feedback.

B. Remote Access of Door

The automated door security system allows the administrator to control access to the restricted area by giving him remote access to the door lock. This feature is implemented using the MQTT Protocol. It allows the administrator to grant temporary access through a web interface to individuals or staff members as needed without requiring them to authenticate. By giving the administrator control over the lock, the system helps ensure that the area remains secure at all times while still allowing for necessary temporary access.

C. Logout While Exiting from the Restricted Area

The user is required to log out using their fingerprints before leaving the critical area. If the user fails and exits the area when someone else unlocks the door for entry or exit, the entry will be denied the next time they attempt to access the door. In addition to this, an email will be sent to the administrator alerting them of the suspected individual along with their details.

D. Log Registry and Admin Operations

The system maintains a log register having the name, id, image, and time of each user entering and exiting the area. The activity record will be shown on a password-protected website that is specifically designed for admin. Furthermore, the admin has the ability to manage the user profiles by creating new profiles and deleting the existing ones.

V. RESULTS

A working prototype of the suggested system has been created and tested for the critical areas as shown in Fig. 4, and our model can be deployed at places where security plays an important role such as server rooms, bank lockers, research labs with sensitive or confidential data, government offices with classified information, and various other areas.

Fig. 4(a). Locking system view from outside.

Fig. 4(b). Locking system view from inside.

The facial recognition mechanism used in the research is shown in Fig. 5. The HOG used in this system is more accurate than V-J for face detection, it can represent local appearance very well [10]. Moreover, the accuracy of face recognition depends on the lighting conditions. But in order to eliminate it, we used LED lights for greater accuracy as shown previously in Fig. 4(a).

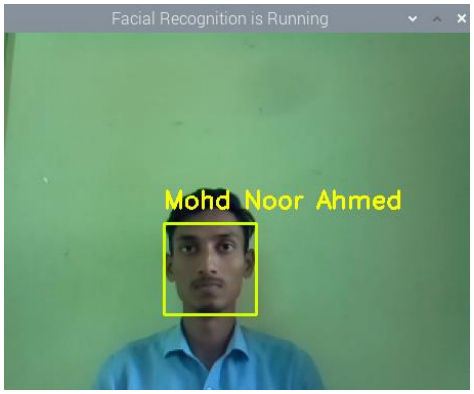

Fig. 5. Face Recognition of a user in Step 2.

Fig. 6 shows the web interface designed for the admin. The alerts that are sent to the admin via email when a person fails to properly close the door are displayed in Fig. 7.

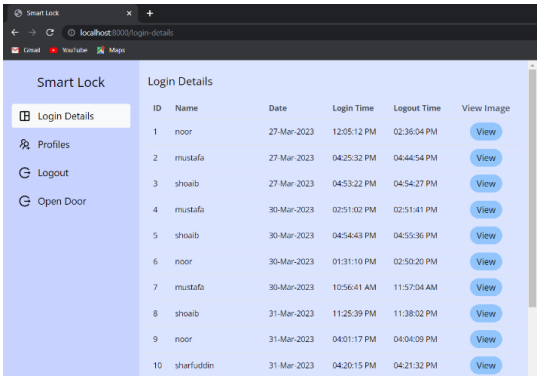

Fig. 6(a). Log activity of users accessing the door.

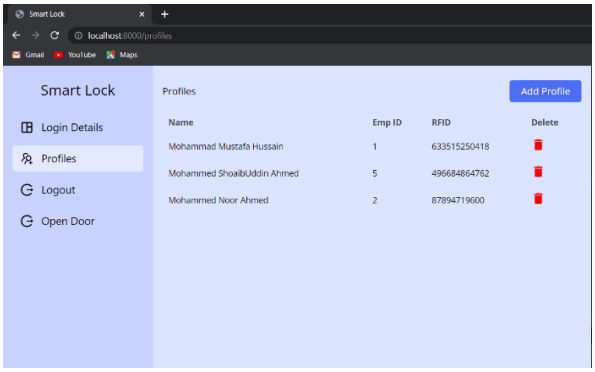

Fig. 6(b). Profiles of authorized users.

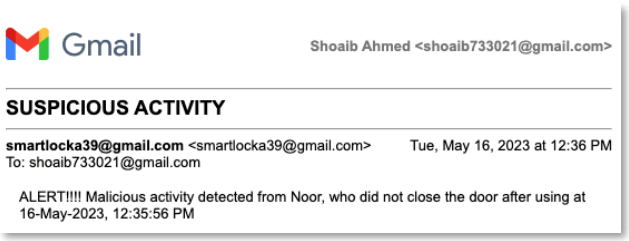

Fig. 7(a). Alert when the user did not close the door.

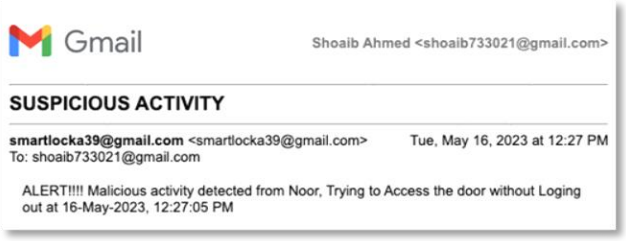

Fig. 7(b). Alert when a user attempts to login without logging out.

VI. CONCLUSION

In this paper, a secure door-locking system has been proposed to enhance security for key locations such as server rooms, and labs with confidential data. The system operates on dual-factor authentication and the user validation is effectively carried out using the Firebase database. In the second step, face recognition is carried out using the LBPH method to handle variations in face images caused by different lighting angles or intensities. By deploying this system, security measures can be greatly strengthened, giving organizations and individuals peace of mind and safety.

REFERENCES

1. M. Shanthini, G. Vidya and R. Arun, "IoT Enhanced Smart Door Locking System," 2020 Third International Conference on Smart Systems and Inventive Technology (ICSSIT), Tirunelveli, India, 2020, pp. 92-96, DOI: 10.1109/ICSSIT48917.2020.9214288.
2. S. Umbarkar, G. Rajput, S. Halder, P. Harname and S. Mendgudle, “Keypad/ Bluetooth/GSM Based Digital Door Lock Security System,” in ICCASP/ ICMMD-2016, Vol. 137, Pp.749-757.
3. K. Patil, N. Vittalkar, P. Hiremath, and M. Murthy, “Smart Door Locking System using IoT,” Int. J. Eng. Technol., vol. 7, pp. 56– 2395, May 2020.
4. J. Baikerikar, V. Kavathekar, N. Ghavate, R. Sawant, and K. Madan, "Smart door locking mechanism", International Conference on Nascent Technologies in Engineering (ICNTE), 2021.
5. Hashem Alnabhi, Yahya Al-naamani, Mohammed Al-madhehagi, and Mohammed Alhamzi (2020), “Enhanced Security Methods of Door Locking Based Fingerprint”, International Journal of Innovative Technology and Exploring Engineering, 9(03), 1173-1178
6. Y. T. Park, P. Sthapit, and J. Pyun, “Smart digital door lock for the home automation,” in TENCON 2009 - 2009 IEEE Region 10 Conference, 2009, pp. 1–6, DOI: 10.1109/TENCON.2009.5396038. RFID
7. M. Mathew and R. S. Divya, "Super secure door lock system for critical zones," 2017 International Conference on Networks & Advances in Computational Technologies (NetACT), Thiruvananthapuram, India, 2017, pp. 242-245, DOI: 10.1109/NETACT.2017.8076773.

8. Akshay Krishnadas Bhat, Siddhesh Praveen Kini, 0, Password Enabled Door Locking System using Arduino and IoT, International Journal Of Engineering Research & Technology (IJERT) ICRTT – 2018 (Volume 06 – Issue 15).
9. Karthik A Patil, Niteen Vittalkar, Pavan Hiremath, Manoj A Murthy, " Smart Door Locking System using IoT", International Journal Of Engineering Research & Technology (IJERT) ICRTT – 2018 (Volume 07 – Issue 05).
10. Dhabliya, D., & Dhabliya, R. (2019). Key characteristics and components of cloud computing. International Journal of Control and Automation, 12(6 Special Issue), 12-18. Retrieved from www.scopus.com
11. Dhabliya, D., & Parvez, A. (2019). Protocol and its benefits for secure shell. International Journal of Control and Automation, 12(6 Special Issue), 19-23. Retrieved from www.scopus.com
12. Dhabliya, D., & Sharma, R. (2019). Cloud computing based mobile devices for distributed computing. International Journal of Control and Automation, 12(6 Special Issue), 1-4. doi:10.33832/ijca.2019.12.6.01
13. Dhabliya, D., Soundararajan, R., Selvarasu, P., Balasubramaniam, M. S., Rajawat, A. S., Goyal, S. B., . . . Suciu, G. (2022). Energy-efficient network protocols and resilient data transmission schemes for wireless sensor Networks—An experimental survey. Energies, 15(23)doi:10.3390/en15238883
14. C. Rahmad, R. Asmara, D. Putra, I. Dharma, H. Darmono and I. Muhiqqin, "Comparison of viola-jones haar cascade classifier and histogram of oriented gradients (hog) for face detection", *IOP conference series: materials science and engineering*, vol. 732, no. 1, pp. 012038, 2020.
15. Shahanawaj Ahamad, Mohammed Abdul Bari, Big Data Processing Model for Smart City Design: A Systematic Review ", VOL 2021: ISSUE 08 ISSN: 0011-9342; Design Engineering (Toronto) Elsevier SCI OC
16. Mohammed Abdul Bari, Shahanawaj Ahamad, Mohammed Rahmat Ali," Smartphone Security and Protection Practices", International Journal of Engineering and Applied Computer Science (IJEACS); ISBN: 9798799755577 Volume: 03, Issue: 01, December 2021.
17. Mohammed Abdul Bari, Shahanawaj Ahamad, Mohammed Rahmat Ali," Smartphone Security and Protection Practices", International Journal of Engineering and Applied Computer Science (IJEACS); ISBN: 9798799755577 Volume: 03, Issue: 01, December 2021 (International Journal, U K) Pages 1-6.
18. Mr. Pathan Ahmed Khan, Dr. M.A Bari: Impact Of Emergence With Robotics At Educational Institution And Emerging Challenges", International Journal of Multidisciplinary Engineering in Current Research (IJMEC), ISSN: 2456-4265, Volume 6, Issue 12, December 2021, Page 43-46.
19. Khan, 1. Pathan Ahmed, & Waheed Farooqi, 2. M. R. M. (n.d.). *Functional outsourcing of linear programming in secured cloud computing*. Pen2print.org. Retrieved May 10, 2023, from https://journals.pen2print.org/index.php/ijr/article/download/4968/4783