10.48047/jocaaa.2025.34.04.44

A Three-Tier Intelligent Door Access System with IoT and Machine Learning

G. Mounika, Cheemala Dinne Chandrika, Indela Venkata Lavanya, Mukku Rojaswini

Department of Electronics and Communication Engineering, Geetanjali Institute of Science and Technology, Nellore, Andhra Pradesh, India.

ABSTRACT

Traditional smart door lock systems typically relied on two-step verification methods such as a password and fingerprint, offering limited security. To enhance protection, the proposed Smart Door Lock System integrates traditional methods with advanced technology, implementing a robust three-step verification process to secure homes or offices. In this system, the user first enters a password via a keypad, then scans their fingerprint using a fingerprint sensor, and finally undergoes facial recognition through an IoT-enabled camera. These authentication inputs are processed sequentially by the ESP32 microcontroller. If the entered password is incorrect, the system immediately halts further verification, triggering a buzzer alarm to alert for unauthorized access. If the password is validated, the system continues to verify the fingerprint and then the facial data. Upon successful authentication of all three steps, the ESP32 activates the door lock mechanism and stores the user's verified credentials in the cloud through IoT connectivity. This smart lock system aims to deliver enhanced security by combining password entry, biometric fingerprint scanning, and facial recognition, thereby ensuring that only authorized individuals can access the premises and significantly reducing the risk of intrusion.

Keywords: ESP 32, Buzzer, Fingerprint Authentication, Smart Door Lock, Smart Home IoT.

1. INTRODUCTION

The Internet of Things (IoT) and Machine Learning (ML) have revolutionized the way we live and work. One area that has seen significant advancements is home security, particularly door accessing systems. Traditional door accessing systems rely on physical keys or cards, which can be lost, stolen, or compromised. To address these concerns, we propose an IoT and ML integrated smart door accessing system. This system combines the benefits of IoT and ML to provide a secure, convenient, and intelligent door accessing solution.

The proposed system utilizes IoT devices, such as sensors and cameras, to collect data and transmit it to the cloud for processing. ML algorithms are then applied to the data to detect patterns, anomalies, and suspicious activity. The system can also integrate with other smart home devices, such as thermostats and lighting systems, to provide a comprehensive and connected experience. Our system incorporates multiple authentication methods, including password, fingerprint, and facial recognition, to ensure secure access. A buzzer and DC motor are also integrated to provide audible and visual alerts, as well as automated door control.

10.48047/jocaaa.2025.34.04.44

Fig. 1: Network communication embedded systems

The IoT cloud platform plays a crucial role in our system, enabling real-time data processing, storage, and analytics. The platform also facilitates seamless communication between devices, ensuring a cohesive and integrated experience. With the increasing demand for smart homes and cities, our system is designed to provide a scalable and flexible solution that can adapt to evolving needs. By leveraging IoT and ML technologies, our system offers enhanced security, convenience, and intelligence, making it an ideal solution for modern homes and businesses.

The integration of password, fingerprint, and facial recognition authentication methods provides a robust and secure access control system. The buzzer and DC motor enable automated door control and alerts, adding an extra layer of convenience and security. The IoT cloud platform enables real-time data processing and analytics, facilitating a seamless and integrated experience. With its scalable and flexible design, our system is poised to revolutionize the way we access and secure our homes and businesses. By harnessing the power of IoT and ML, we can create a safer, more convenient, and more connected world.

2. LITERATURE SURVEY

Durga K. Prasad,et al (2019) proposed solution had a unique invisible internal locking mechanism fitted inside the main door and was operated through the completion of a two-stage security verification process. One of the security stages, which involved a main key or fingerprint sensor to operate the internal locking mechanism, was kept inside a primary (preliminary) door and was invisible to outside people until the primary door was opened. **[1]**

CNS Vinoth,et al (2022) proposed system was designed to create a secure door lock security system with two-factor authentication. The user had to use a Radio Frequency Identification (RFID) tag. The tag's data was saved in a database. When the tag was read by the RFID reader, the user had to input a passcode. After the passcode was entered, the user received a one-time password (OTP) on their mobile device to unlock the door. The biggest advantage of the proposed system was the introduction of two-factor authentication to gain access to the door, which made it more secure**. [2]**

Phan,et al (2021) proposed the biometric recognition based on the combination of fingerprint and face image to identify the homeowners who had permission to access the home. The main door would be opened if the input biometric image matched the one stored in the database. Otherwise, the system would raise an alarm with a doorbell and/or send a notification message to the homeowner. **[3]**

10.48047/jocaaa.2025.34.04.44

Hteik Htar,et al(2015) Proposed The system utilized face recognition and automatic door access control. Face detection was the process of detecting the region of the face in an image. The face was detected by using the Viola-Jones method, and face recognition was implemented by using Principal Component Analysis (PCA). Face recognition based on PCA was generally referred to as the use of Eigenfaces. If a face was recognized, it was known; otherwise, it was unknown. The door would open automatically for the known person due to the command of the microcontroller. On the other hand, an alarm would ring for the unknown person. Since PCA reduced the dimensions of face images without losing important features, facial images for many persons could be stored in the database. **[4]**

Nikolaos,et al (2015) proposed two-factor authentication protected online accounts even if passwords were leaked. Most users, however, preferred password-only authentication. One reason why two-factor authentication was so unpopular was the extra steps that the user had to complete in order to log in. Currently deployed two-factor authentication mechanisms required the user to interact with their phone to, for example, copy a verification code to the browser. Two-factor authentication schemes that eliminated user-phone interaction existed, but required additional software to be deployed. **[5]**

Khuda Bux,et al(2020) proposed the usage of the Internet of Things (IoT) devices was growing for the ease of life. From smart homes to smart cars, from smart transportation to smart cities, from smart hospitals to smart highways, these IoT devices sent and received highly sensitive data regarding the privacy of users or other information regarding the movement of users from one location to another location. The timing traced users when present at home and out of the home. The proposed solution in this chapter was a three- way authentication of IoT devices by generating tokens from the device serial number and from a few configuration devices at the network layer. For high availability of IoT device services, protection against distributed denial of service attacks was implemented at the network layer. **[6]**

Yuan,**et al(2021)** proposed contactless fault diagnosis was one of the most important techniques for fault identification of equipment. Based on the idea of contactless fault diagnosis, this paper presented a sound- based diagnosis method for railway point machines (RPMs). First, the sound signals were preprocessed using empirical mode decomposition (EMD). Entropy, time-domain, and frequency-domain statistical parameters of the first 15 intrinsic mode functions (IMFs) were then extracted. Second, a two-stage feature selection strategy blending Filter method and Wrapper method was proposed, which significantly reduced the dimension of features and selected the optimal features. **[7]**

Arun Cyril ,et al(2016) proposed this paper explained the importance of accessing modern smart homes over the Internet, and highlighted various security issues associated with it. This paper explained the evolution of the device fingerprinting concept over time, and discussed various pitfalls in existing device fingerprinting approaches. In this paper, we proposed a two- stage verification process for smart homes, using device fingerprints and login credentials, which verified the user device as well as the user accessing the home over the Internet. **[8]**

3. PROPOSED SYSTEM

The smart door lock system with three step verification, where a user inputs their password via a keypad, scans their fingerprint using a fingerprint sensor, and undergoes facial recognition through a camera module. These inputs are transmitted to an ESP32 microcontroller, which verifies the data sequentially. If the password is incorrect, the system halts, and a buzzer sounds an alarm, preventing progression to the next step. However, if the password is correct, the ESP32 proceeds to verify the fingerprint and facial recognition data. Upon successful verification of all three inputs, the ESP32 sends a signal to open the door and stores the verified user data in the cloud via IoT connectivity.

10.48047/jocaaa.2025.34.04.44

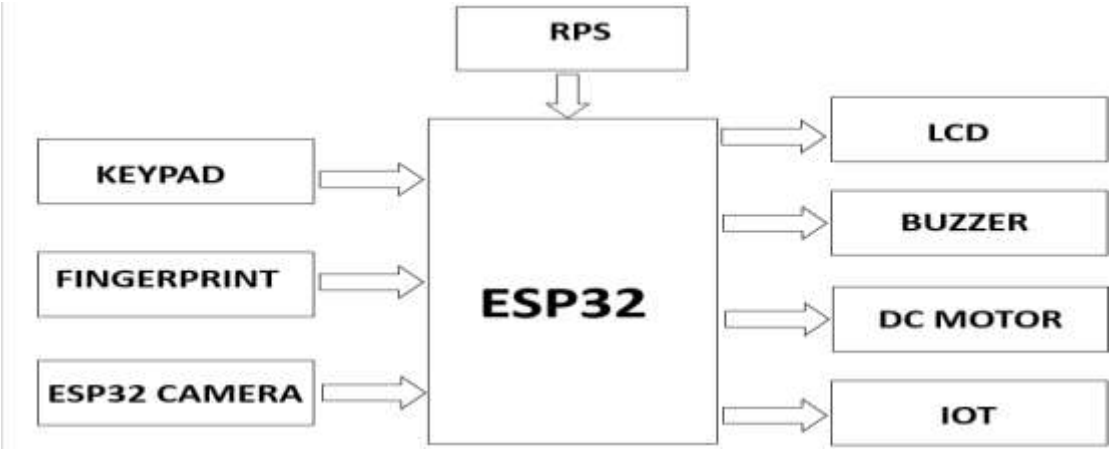


Fig. 2: Block Diagram.

An IoT server manages and processes data from connected devices. It handles tasks like device control, data collection, storage, analysis, and security. IoT servers can be in the cloud, on- site, or a mix of both, helping to extract valuable insights from IoT data.

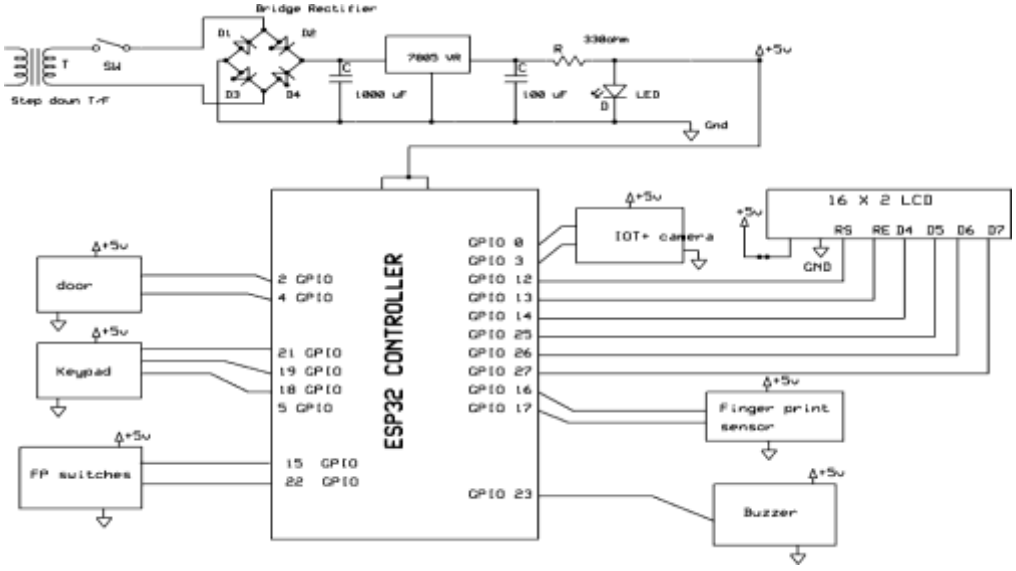


Fig. 3: Schematic diagram

The power supply section of the system consists of a step-down transformer that reduces the AC voltage, followed by a bridge rectifier (D1–D4) that converts the AC to DC. A 7805 voltage regulator is used to provide a stable 5V DC output, and smoothing capacitors (1000µF and 100µF) help eliminate voltage ripples. An LED indicator with a 330Ω resistor is included to show power status. At the core of the system is the ESP32 microcontroller, which functions as the main controller interfacing with various modules through multiple GPIO (General Purpose Input/Output) pins. The system includes a door lock mechanism controlled via GPIO 2 and GPIO 4, and a keypad connected to GPIO 5, 18, 19, and 21 for user input. A fingerprint sensor is integrated for biometric authentication, while an IoT-enabled camera captures images for facial recognition. A 16x2 LCD display provides real-time status updates, and a buzzer delivers sound alerts based on authentication results. Additional fingerprint switches (FP switches) enhance the security. This comprehensive access control system employs keypad entry, fingerprint scanning, and facial recognition to ensure highly secure and multi-layered door access.

ADVANTAGES

10.48047/jocaaa.2025.34.04.44

The three-step verification system significantly enhances security by incorporating multiple layers of authentication, making unauthorized access extremely difficult. This layered approach typically includes something the user knows (such as a PIN or password), something they have (like a smartphone or key fob), and something they are (such as a fingerprint or facial recognition). By using multiple factors, the system drastically reduces the risk of hacking; even if one layer is compromised, the others continue to provide strong protection. Additionally, the system offers convenience and flexibility, allowing users to select the most suitable authentication method based on the situation, and enabling different levels of access for different users. It is also highly resilient to theft, as stealing a physical item like a key or phone is not sufficient without passing biometric checks. Furthermore, the system can be customized to set access levels or modify verification steps based on factors such as time, location, or specific user roles, offering enhanced adaptability and control.

4. RESULTS AND DISCUSSION

Our Smart Door System has three ways to keep you safe. It uses a password, your fingerprint, and your face to unlock. This makes it very secure and reliable. By leveraging advanced technologies such as biometric authentication and IoT connectivity, this system offers a secure, convenient, and futuristic solution for smart homes, offices, and industrial facilities.

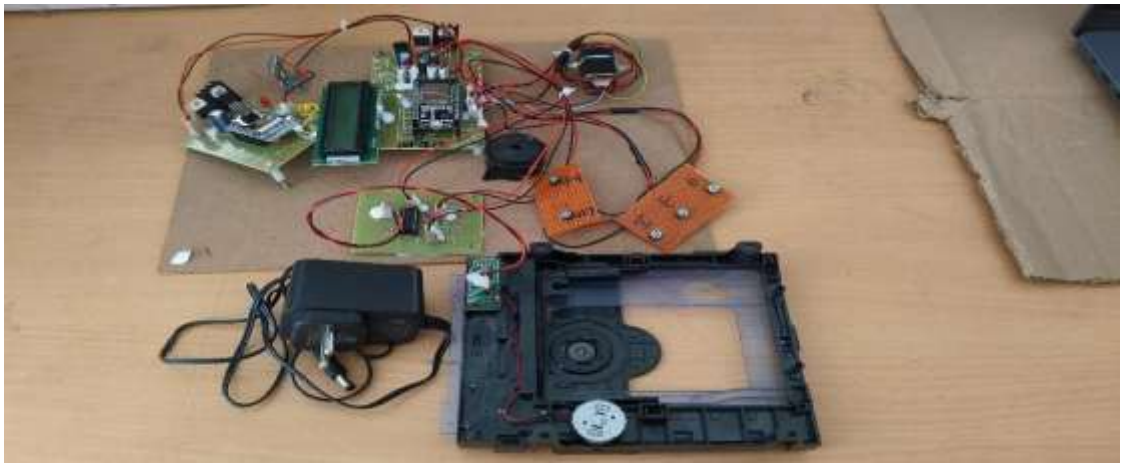


Fig. 4: the Final view of our project

The 3-Step Verification Smart Door Accessing System is an innovative security solution that integrates password authentication, fingerprint recognition, and facial recognition to provide robust and reliable access control mechanism.

Fig. 5: The title of the our project which is based on three step verification

10.48047/jocaaa.2025.34.04.44

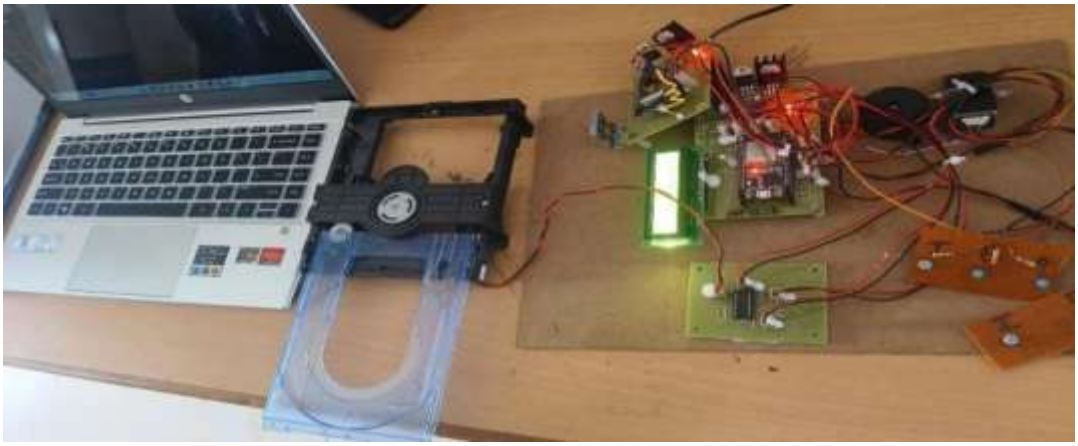
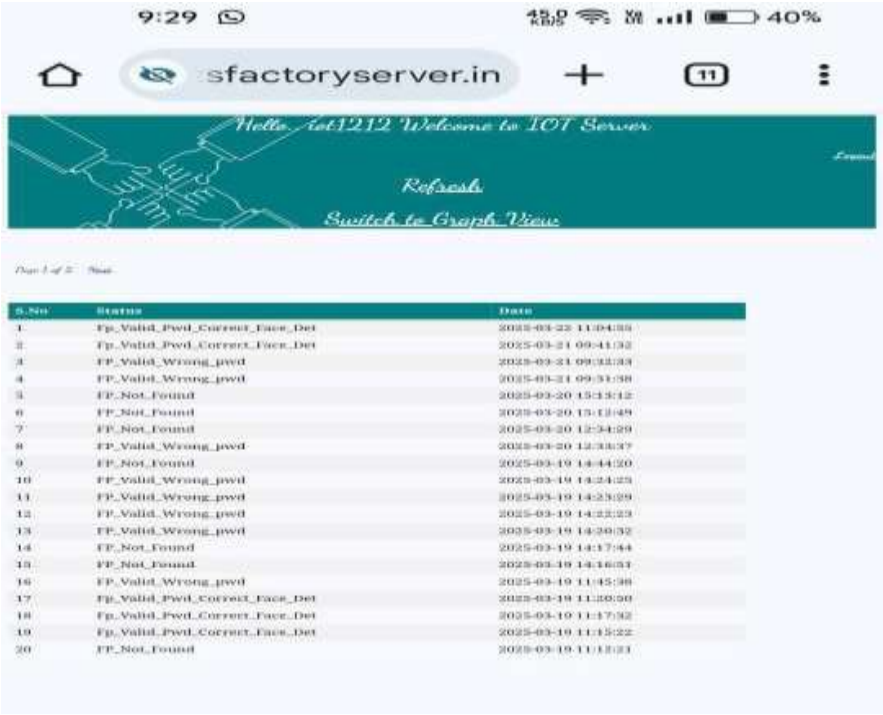


Fig. 6: The final output of the project based on three step smart door accesing system

After the completion of all the 3 steps ,then the door (CD drive)will open after the 5 seconds automatically the door will closed.



S.No	Status	Date
1	Fp_Valid_Pwd_Correct_Face_Det	2025-03-22 11:04:55
2	Fp_Valid_Pwd_Correct_Face_Det	2025-03-21 09:41:32
3	FP_Valid_Wrong_pwd	2025-03-21 09:33:33
4	FP_Valid_Wrong_pwd	2025-03-21 09:31:58
5	FP_Not_Found	2025-03-20 15:13:12
6	FP_Not_Found	2025-03-20 15:12:49
7	FP_Not_Found	2025-03-20 12:34:29
8	FP_Valid_Wrong_pwd	2025-03-20 12:33:37
9	FP_Not_Found	2025-03-19 14:44:20
10	FP_Valid_Wrong_pwd	2025-03-19 14:24:25
11	FP_Valid_Wrong_pwd	2025-03-19 14:23:29
12	FP_Valid_Wrong_pwd	2025-03-19 14:22:23
13	FP_Valid_Wrong_pwd	2025-03-19 14:20:32
14	FP_Not_Found	2025-03-19 14:17:44
15	FP_Not_Found	2025-03-19 14:16:51
16	FP_Valid_Wrong_pwd	2025-03-19 11:45:38
17	Fp_Valid_Pwd_Correct_Face_Det	2025-03-19 11:20:50
18	Fp_Valid_Pwd_Correct_Face_Det	2025-03-19 11:17:52
19	Fp_Valid_Pwd_Correct_Face_Det	2025-03-19 11:15:22
20	FP_Not_Found	2025-03-19 11:11:21

Fig. 7: The data accessing information

The IoT server is a centralized data repository that securely stores and manages access logs, tracking authorized users and validating passwords. With robust security features, it ensures that sensitive data is protected from unauthorized access and breaches.

5. CONCLUSION

The 3-Step Verification Smart Door Accessing System is a revolutionary security solution that provides unparalleled protection and convenience. This innovative system combines three layers of verification - password, fingerprint, and facial recognition - to ensure that only authorized individuals can gain access. By leveraging advanced technologies, this system offers a robust and reliable solution for

10.48047/jocaaa.2025.34.04.44

securing homes, offices, and other sensitive facilities. The first layer of verification is password protection, which serves as a traditional yet effective barrier against unauthorized access. The second layer is fingerprint recognition, which utilizes advanced biometric technology to verify an individual's identity. The third and final layer is facial recognition, which employs sophisticated algorithms to match an individual's facial features with their stored biometric data. The 3-Step Verification Smart Door Accessing System is a cutting-edge security solution that provides unparalleled protection and convenience. By combining password, fingerprint, and facial recognition technologies, this system offers a robust and reliable solution for securing sensitive facilities. With its advanced biometric technologies, customization options, and user-friendly interface, this system is the perfect solution for individuals and organizations seeking to enhance their security and peace of mind**.**

REFERENCES

[1] Gudavalli, Durga K. Prasad, I. Swetha Monica, and MEC Vidya Sagar. "A Novel Door Lock Operation Using Two Staged Smart Security Verification." In *2019 Global Conference for Advancement in Technology (GCAT)*, pp. 1-6. IEEE, 2019.

[2] Kumar, CNS Vinoth, Vasim Babu, R. Naresh, and V. Bharathi. "Real time door security system with three point authentication." In *2021 4th International Conference on Recent Trends in Computer Science and Technology (ICRTCST)*, pp. 228-233. IEEE, 2022.

[3] Van Vinh, Phan, Phan Xuan Dung, Pham Thuy Tien, Tran Thi Thuy Hang, Truong Hong Duc, and Tran Duy Nhat. "Smart home security system using biometric recognition." In *International Conference on Internet of Things as a Service*, pp. 405-420. Cham: Springer International Publishing, 2020.

[4] Lwin, Hteik Htar, Aung Soe Khaing, and Hla Myo Tun. "Automatic door access system using face recognition." *international Journal of scientific & technology research* 4, no. 6 (2015): 294-299.

[5] Karapanos, Nikolaos, Claudio Marforio, Claudio Soriente, and Srdjan Capkun. "{Sound-Proof}: Usable {Two-Factor} authentication based on ambient sound." In *24th USENIX security symposium (USENIX security 15)*, pp. 483-498. 2015.

[6] Jalbani, Khuda Bux, Akhtar Hussain Jalbani, and Saima Siraj Soomro. "IoT security: To secure IoT devices with two-factor authentication by using a secure protocol." In *Industrial Internet of Things and Cyber-Physical Systems: Transforming the Conventional to Digital*, pp. 98-118. IGI Global, 2020.

[7] Cao, Yuan, Yongkui Sun, Guo Xie, and Peng Li. "A sound-based fault diagnosis method for railway point machines based on two-stage feature selection strategy and ensemble classifier." *IEEE Transactions on Intelligent Transportation Systems* 23, no. 8 (2021): 12074-12083.

[8] Jose, Arun Cyril, Reza Malekian, and Ning Ye. "Improving home automation security; integrating device fingerprinting into smart home." *IEEE Access* 4 (2016): 5776- 5787.