Journal of Information System and Technology Management
JISTM
EISSN: 0128-1666
Volume 10 Issue 39 (June 2025) PP. 197-208
DOI: 10.35631/JISTM.1039013

JOURNAL OF INFORMATION SYSTEM AND TECHNOLOGY MANAGEMENT (JISTM)
www.jistm.com

IOT ENABLED MULTI FACTOR AUTHENTICATION LOCK SYSTEM

Akshith SP[1], Rashmitha Mukka[2], Ashwin Karthik[3], Sandeep Krishna V[4], J. Florence Gnana Poovathy[5*], I. Divya[6]

[1] School of Electronics Engineering (SENSE),Vellore Institute of Technology, Chennai, India
Email: akshithsunku123@gmail.com
[2] School of Electronics Engineering (SENSE),Vellore Institute of Technology, Chennai, India
Email: mukkarashmitha2005@gmail.com
[3] School of Electronics Engineering (SENSE),Vellore Institute of Technology, Chennai, India
Email: ashwinkarthikvk@gmail.com
[4] School of Electronics Engineering (SENSE),Vellore Institute of Technology, Chennai, India
Email: v.sandeepkrishna@gmail.com
[5] Electric Vehicles Incubation & Testing – Research Centre (eVIT-RC), Vellore Institute of Technology, Chennai, India
Email: florence.poovathy@vit.ac.in
[6] Artificial Intelligence and Data Science (AIDS), Rajalakshmi Institute of Technology, Chennai, India
Email: divya.i@ritchennai.edu.in
[*] Corresponding Author

Article Info:

Article history:
Received date: 31.03.2025
Revised date: 27.04.2025
Accepted date: 29.05.2025
Published date: 20.06.2025

To cite this document:

Akshith, S.P., Mukka, R., Karthik, A., Sandeep, K. V., Poovathy, F. G., & Divya, I. (2025). IoT Enabled Multi Factor Authentication Lock System. *Journal of Information System and Technology Management, 10* (39), 197-208.

DOI: 10.35631/JISTM.1039013

Abstract:

Conventional door locks are easily bypassed, posing security threats. Recent IoT advancements have led to smart door locks, but many rely on single authentication methods. This work presents an IoT-enabled multi-factor authentication door lock system, enhancing security with RFID, numeric keypad, and access control via an ESP32 microcontroller and Arduino Uno board. It requires two out of three methods: PIN, facial recognition, and RFID tag verification, unlocking within 10 seconds and re-locking in 5-6 seconds. The average success rate in face recognition with and without disturbances such as spectacles, facial hair etc., are 97% and 92% respectively. Features include robust encryption, secure communication, and fail-safe mechanisms, with a modular design for smart home integration. Thoroughly tested, the system outperforms existing solutions in accuracy and flexibility, providing enhanced security through multi-factor authentication

Keywords:

Multi-Factor Authentication, ESP32-CAM, Arduino, RFID, Keypad

Journal of Information System and Technology Management
EISSN: 0128-1666
Volume 10 Issue 39 (June 2025) PP. 197-208
DOI: 10.35631/JISTM.1039013

Introduction

Traditional door locks, such as metal locks and keys, are often vulnerable to theft, key misplacement, and unauthorized access, exposing individuals to various security threats. Over the past decade, the integration of the Internet of Things (IoT) has significantly advanced the development of smart door lock systems. However, many existing systems rely on single factor authentication, limiting their adaptability and failing to address issues such as lost access cards, damaged cameras, or malfunctioning devices (Raju et. al., 2022, Alsahlani, A. Y. F., & Popa, A., 2021).

To enhance security and adaptability, there is a growing emphasis on multi-factor authentication (MFA), which combines different layers of security to mitigate risks associated with single-point failures (Sutradhar S. et. al., 2025). This work presents an IoT-enabled multi-factor authentication door lock system that provides enhanced security through automated locking and unlocking mechanisms, intrusion detection, and real-time monitoring. The system combines RFID, a numeric keypad, and facial recognition via an ESP32 camera module. It requires successful authentication through at least two of these methods within ten seconds, offering three valid combinations: RFID and keypad, facial recognition and RFID, or facial recognition and keypad (Kodali R. K., & Soratkal S. 2016, Dhillon P. K., & Kalra S., 2018). Multi-factor user authentication scheme for IoT-based healthcare services. The proposed system ensures robust security by incorporating features such as secure communication channels, robust encryption, and fail-safe mechanisms, significantly enhancing overall security compared to traditional locking mechanisms (Kumar, T. D. et. al., 2023) The modular design allows for adaptability, making it suitable for diverse environments, from residential homes to commercial properties (Sanath K. et. al, 2021, Soni S., et. al., 2021).

Various studies highlight the limitations of current solutions. For example, Shanthini et al. developed an IoT-enhanced locking system using Arduino UNO and Bluetooth, allowing remote control via a smartphone application. While effective, this system relies on Bluetooth technology, which may introduce security vulnerabilities due to its limited range (Singh N, et. al., 2022). Similarly, a biometric authentication system utilizing an Arduino Nano has been proposed, emphasizing user authentication but recognizing that reliance on smartphone biometrics could hinder access during device malfunctions AFROZ, A. An RFID and OTP-driven locking system to enhance household security but acknowledged that delays in OTP delivery could compromise reliability, especially in urgent situations was proposed by (Shanthini M et. al., 2020). Some recent studies on voice recognition based locking systems prevail (Saad I et. al., 2023), that are faster but the false alarms and success rates can decrease to a greater extend since a single-factor authentication is used. In another work, only face recognition technique for door locking and unlocking has been used which might be disadvantageous when facial features change for example, while wearing more make-up, wearing a sweat shirt's hood, baldness or more hair etc. (Chandra M, et. al., 2023, Dharmale G et. al., 2022). Furthermore, existing systems that rely solely on smartphone-based biometrics or Bluetooth are prone to connection issues and security vulnerabilities related to wireless communication. By addressing these shortcomings, the proposed multi-factor authentication system integrates several authentication layers, greatly enhancing security and flexibility across various applications.

Journal of Information System and Technology Management
EISSN: 0128-1666
Volume 10 Issue 39 (June 2025) PP. 197-208
DOI: 10.35631/JISTM.1039013

Methodology

Requirement Analysis

The IoT-enabled multi-factor authentication door lock system is meticulously designed to enhance security through the integration of multiple authentication methods. At the core of this system is the Arduino Uno, selected for its RISC architecture, which provides adequate performance without the need for high-speed processing or pipelined execution. This choice aligns with the requirement for straightforward and reliable operations, prioritizing stability over speed. The Arduino Uno features sufficient on-chip ROM and RAM for storing and executing the necessary code, while its 20 GPIO pins facilitate connections to various peripheral components integral to the system.

Key components have been carefully selected to ensure robust security and user interaction. The ESP32 camera module serves as the biometric layer for facial recognition, significantly enhancing security by preventing unauthorized access based on facial features. The solenoid door lock functions as the physical locking mechanism, controlled by the microcontroller to lock or unlock the door based on successful authentication. User interaction is further enhanced through a 16-bit LCD display with I2C communication, which presents prompts and status updates, making the system user-friendly. The keypad allows users to enter a PIN, providing an additional layer of security, while the RFID sensor offers a convenient method for unlocking the door using an ID card, streamlining access while maintaining security.

The Arduino Uno operates within a voltage range of 3.3-5V, ensuring compatibility with the voltage levels required by the other components. Despite its lack of features such as an ADC, real-time clock, MMU, FPU, DMA, and external RAM, it effectively meets the operational demands of the system. With an 8-bit data bus, 16-bit address bus, 16MHz clock frequency, and 1µs execution speed, the Arduino Uno efficiently manages the system's operations. Communication protocols such as UART and I2C are crucial for interfacing with connected components, enabling seamless data exchange. The design does not necessitate low power mode support or a real-time operating system (RTOS), as the primary focus is on delivering a reliable and secure door-locking mechanism rather than optimizing for low power consumption or advanced multitasking. In summary, the selection of components— including the Arduino Uno, ESP32 camera module, solenoid door lock, 16-bit LCD display with I2C, keypad, and RFID sensor—has been thoroughly justified, collectively enhancing security through multi-factor authentication and ensuring a secure, adaptable, and efficient smart door lock solution that meets both technical and operational requirements.

Functional Blocks of the proposed IOT enabled system

The Figure 1. illustrates the structure of an IoT-enabled multi-factor authentication door lock system. At the core is the Arduino Uno, which coordinates various components. The RFID sensor is used for card-based authentication, while the 4x4 keypad allows for PIN entry, providing two authentication options. Both the RFID sensor and keypad are directly connected to the Arduino for input processing.

Additionally, the system incorporates an ESP32 Camera Module, responsible for face recognition. The camera communicates with the cloud, potentially for remote processing or data storage. Upon successful authentication, the Arduino Uno controls the relay to activate the solenoid lock, locking or unlocking the door. User feedback is displayed on an I2C-connected LCD screen, providing prompts or status updates. The combination of RFID,

Journal of Information System and Technology Management
JISTM
EISSN: 0128-1666
Volume 10 Issue 39 (June 2025) PP. 197-208
DOI: 10.35631/JISTM.1039013

keypad, and face recognition ensures a multi-factor, secure door-locking mechanism, where the Arduino acts as the central controller to verify user credentials before unlocking the door.

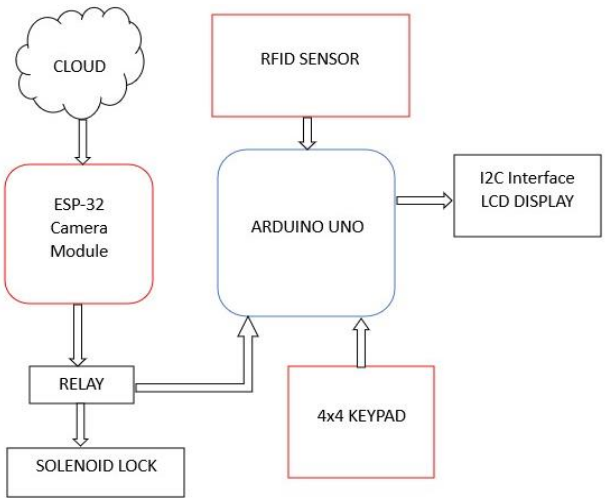

Figure 1: Hardware Implementation Of Multi Factor Authentication

Work flow

The Figure 2. illustrates a multi-factor authentication system for unlocking a door, where users can select two out of three available methods: Face Lock, RFID, and PIN. The process starts by prompting the user to choose any two of these options. Based on the chosen methods, the system verifies each one sequentially. For example, if the user selects Face Lock and RFID, the system first checks the Face Lock. If the Face Lock authentication is successful, it then proceeds to verify the RFID. If both are verified, the door is unlocked. However, if the Face Lock fails, the user is given two additional attempts to authenticate. Similarly, if RFID verification fails, the user is also allowed two more attempts.

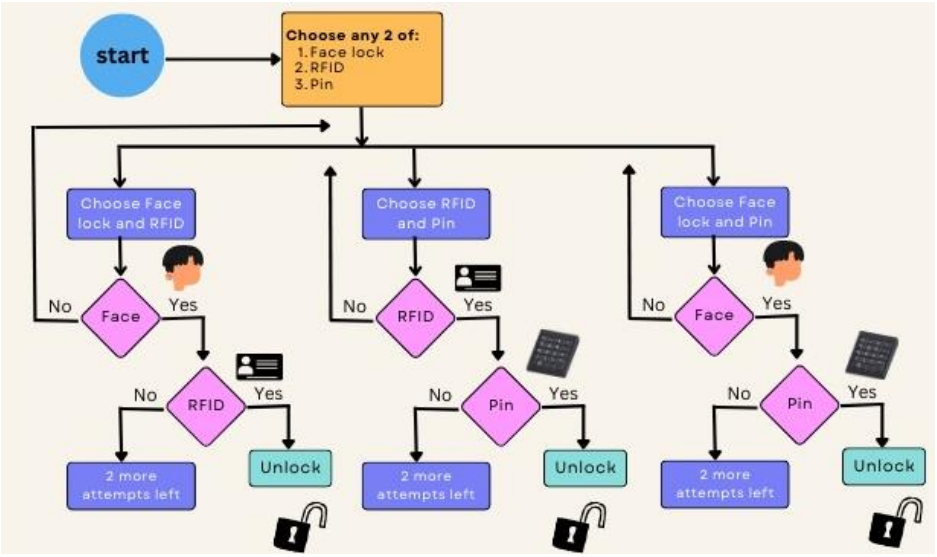

Figure 2: Multi Factor Authentication

Journal of Information System and Technology Management
EISSN: 0128-1666
Volume 10 Issue 39 (June 2025) PP. 197-208
DOI: 10.35631/JISTM.1039013

The same process applies if the user selects RFID and PIN or Face Lock and PIN. In each case, after successfully passing both verifications, the door unlocks. However, a failure in any of the chosen methods triggers the option for two more attempts. This system ensures security by requiring successful verification of two authentication factors while allowing retries in case of failure. This multi-factor process enhances security by requiring the user to successfully pass two independent authentication checks before gaining access.

Working

Working

The IoT-enabled multi-factor authentication door lock system enhances security by requiring successful authentication through three methods: entering a PIN via a keypad, facial recognition using an ESP32 camera module, and RFID tag verification. The door unlocks only when at least two of these methods are validated, regardless of the order.

Facial Recognition With ESP32 Camera Module

The system employs an ESP32 camera for facial recognition, programmed through an FTDI232 USB to Serial interface. After establishing a connection to a specified Wi-Fi hotspot, the user enrols their face by taking samples. The system stores this data for comparison during subsequent access attempts. Upon successful recognition, the system signals to unlock the door and illuminates a white LED, displaying a "Welcome" message.

RFID Verification

Each authorized user is assigned a unique RFID tag, read by an MFRC522 IC-based module. The tag information is programmed into the system, allowing the Arduino Uno to verify if the scanned tag is authorized. Successful verification leads to the next authentication step.

PIN Entry

A 4x4 keypad is used for entering a predetermined PIN. The Arduino Uno checks the entered PIN against stored data. If matched, the system proceeds to the next step; if incorrect, access is denied. The I2C-connected LCD provides user prompts and feedback throughout the authentication process, displaying messages like "Enter PIN," "Scan RFID," or "Face Recognition." Upon successful authentication, the LCD shows "Access granted," while failure results in an "Access denied" message.

Integrated Operation

The system requires at least two successful authentication steps for unlocking. The relay module connected to the Arduino Uno controls the solenoid lock based on verification outcomes. The integration of the ESP32 camera with cloud capabilities enables remote management and monitoring, significantly enhancing the system’s overall security and functionality. This multi-layered approach effectively prevents unauthorized access, ensuring a robust locking mechanism.

Circuit Diagram

The Figure 3. illustrates the operation of an IoT-enabled multi-factor authentication (MFA) door lock system, incorporating various components such as the ESP32CAM, Arduino UNO, 4x4 keypad, relay module, LCD display, and RFID module. The ESP32CAM serves as the primary interface for wireless communication and processes facial recognition data for enhanced security. Meanwhile, the Arduino UNO manages inputs from the keypad,

Journal of Information System and Technology Management
EISSN: 0128-1666
Volume 10 Issue 39 (June 2025) PP. 197-208
DOI: 10.35631/JISTM.1039013

communicates with the relay module, and controls the LCD display. In this MFA system, users can unlock the door through one of three methods: facial recognition via the ESP32CAM, RFID card identification, or PIN entry using the keypad. Upon system initialization, the user is prompted to present their face to the ESP32CAM, scan their RFID card, or enter a password on the keypad. If face detection is enabled and the ESP32CAM successfully recognizes the user's face, it activates the relay module and sends a signal to the Arduino UNO to unlock the door. Alternatively, access can be granted by scanning an authorized RFID card or entering the correct PIN.

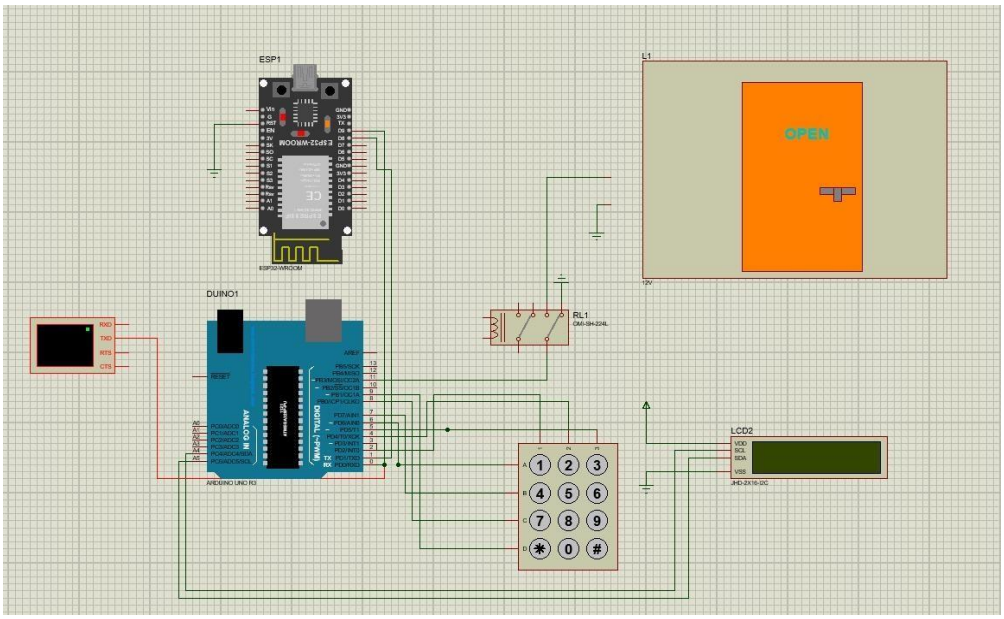

Figure 3: Proteus Circuit Diagram

The LCD display provides real-time feedback, showing messages such as "Access Granted" or "Door Open" upon successful authentication. If any of the authentication attempts fail, the system displays "Access Denied," and the door remains locked. Additionally, the relay module controls the solenoid lock mechanism, ensuring that the door is secured after a brief unlock period of 10 seconds, followed by automatic relocking within 5-6 seconds if no further action is taken. This comprehensive approach ensures that the IoT-enabled multi-factor authentication door lock system is robust, flexible, and highly secure, effectively mitigating unauthorized access while offering a user-friendly experience

Results and Discussions

The system was initially evaluated under ideal conditions, achieving an impressive average efficiency of 97% in face detection without obstructions. However, performance slightly declined to 92% when participants wore glasses or had facial modifications like beards, reflecting the inherent limitations of face recognition technology. In addition to facial recognition, the RFID and keypad functionalities were tested, demonstrating high reliability. The RFID module successfully identified authorized users without errors, while the keypad function maintained a perfect efficiency rate. Overall, the system showcased robust performance across various methods of authentication.

Journal of Information System and Technology Management
JISTM
EISSN: 0128-1666
Volume 10 Issue 39 (June 2025) PP. 197-208
DOI: 10.35631/JISTM.1039013

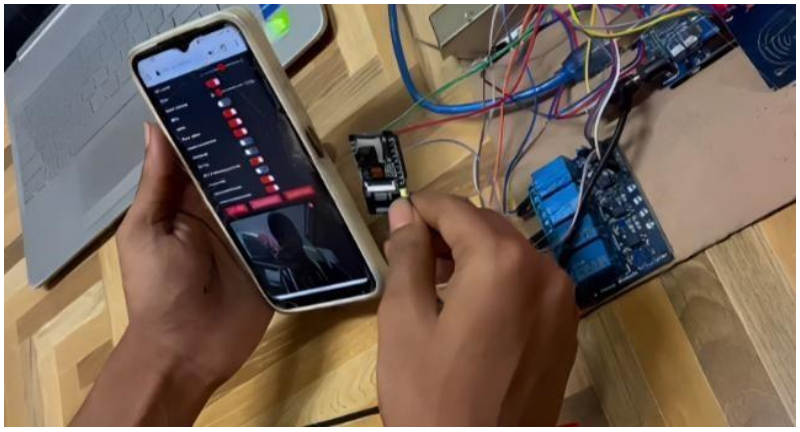

Figure 4: Image Capturing

In Figure 4, we demonstrate the implementation of a facial recognition system using the ESP32-CAM module. The system allows users to upload images for face recognition via a control interface [Figure 6], providing instant feedback on the recognition process. The ESP32-CAM performed efficiently in both image capture and face recognition, making this configuration suitable for IoT applications such as smart security systems, where facial recognition enhances access control and security management.

Figure 5: Face Recognition

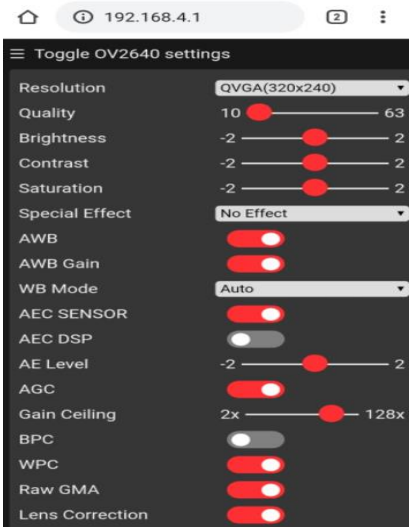

Figure 6: Esp32 CAM Interface

In Figure 5. the facial recognition system, powered by the ESP32-CAM module, successfully detects a face. Once the recognition is complete, the solenoid lock opens, demonstrating the seamless integration of facial recognition for access control. The ESP32-CAM efficiently processes the uploaded image and matches it against stored data, triggering the lock mechanism. This setup highlights the practical application of ESP32-CAM in real-time security systems, enabling automated, secure access management based on facial identification.

Journal of Information System and Technology Management
JISTM
EISSN: 0128-1666
Volume 10 Issue 39 (June 2025) PP. 197-208
DOI: 10.35631/JISTM.1039013

Table 1: Face Detection Without Any Disturbance

Labels	True	False	Efficiency
Person-1	10	0	100%
Person-2	9	1	90%
Person-3	10	0	100%
Person-4	10	0	100%
Average Efficiency - 97%			

The Table 1. presents the face detection results obtained using the ESP32-CAM under ideal conditions, without any disturbances such as obstructions or environmental challenges. The samples were tested, each with 10 observations. Person 1, Person 3, and Person 4 achieved perfect accuracy with 10 correct detections and 0 false detections, resulting in 100% efficiency. Person 2 had 9 correct detections and 1 false detection, leading to a slightly lower efficiency of 90%. Overall, the system achieved an average detection efficiency of 97%, indicating a strong performance by the ESP32-CAM in clear and undisturbed conditions.

The Figure 7. illustrates the performance of face detection using the ESP32-CAM in ideal, disturbance-free conditions. We tested for some samples, with each undergoing 10 detection trials. The system demonstrated flawless accuracy for three individuals, where all 10 attempts resulted in correct face detections, yielding 100% efficiency. For one individual, there was a minor deviation, with 9 successful detections out of 10 attempts, resulting in a 90% efficiency rate. Overall, the face detection system displayed high reliability, achieving strong and consistent performance across all individuals, with an overall average efficiency of approximately 97%.

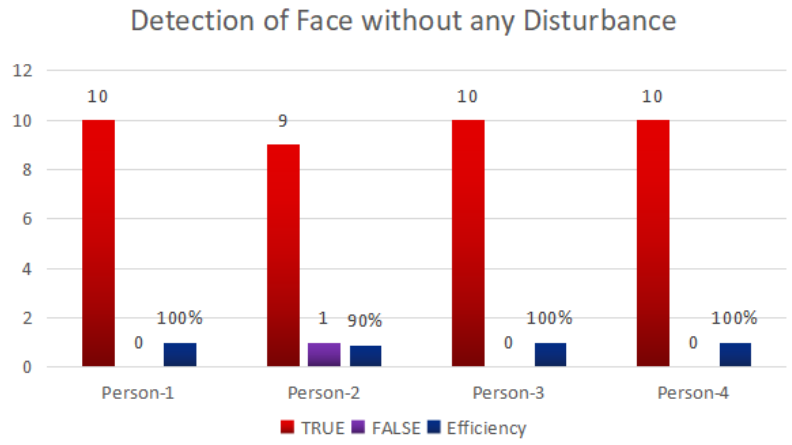

Figure 7: Face Detection Without Any Disturbance Factors

Table 2: Face Detection with Disturbance Like Spectacles And Facial Hair

Labels	True	False	Efficiency
Person-1	10	0	100%
Person-2	8	2	80%
Person-3	9	1	90%
Person-4	10	0	100%
Average Efficiency - 92%			

Journal of Information System and Technology Management
JISTM
EISSN: 0128-1666
Volume 10 Issue 39 (June 2025) PP. 197-208
DOI: 10.35631/JISTM.1039013

The Table 2. summarizes face detection results using the ESP32-CAM in the presence of disturbances like spectacles and facial hair. The samples were tested, each undergoing 10 detection attempts. Person-1 and Person-4 maintained perfect detection accuracy, with all 10 detections being true, resulting in 100% efficiency for both. Person-3 had 9 successful detections and 1 false detection, yielding a 90% efficiency rate. Person-2 encountered more challenges, with 8 correct detections and 2 false detections, lowering their efficiency to 80%. The overall average efficiency across all individuals was 92%, indicating that while disturbances such as spectacles and facial hair introduced some variability in performance, the ESP32-CAM remained highly reliable in most cases.

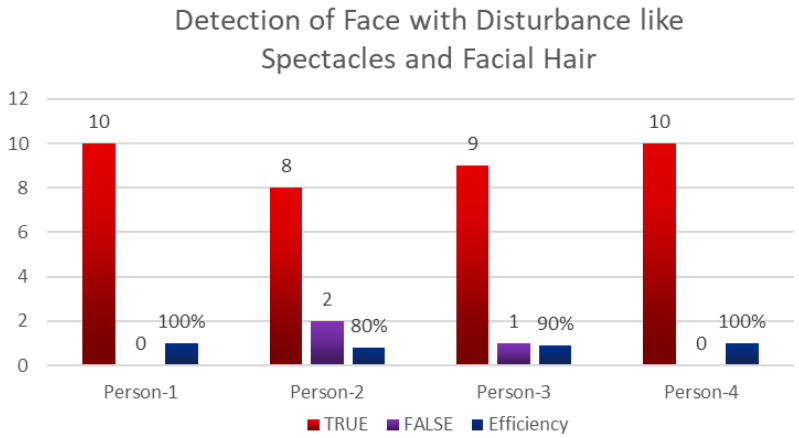

Figure 8: Face Detection with Disturbance Factors

Table 3: Comparison of Average Efficiency for Proposed Method with that of Existing MFA Method

Proposed Method Without disturbance factor	Existing Method Without disturbance factor [14]	Proposed Method With disturbance factor	Existing Method With disturbance factor [14]
97	96	92	90

The Figure 8. illustrates the performance of face detection using the ESP32-CAM under conditions involving disturbances such as spectacles and facial hair. We tested several individuals, each undergoing 10 detection trials. The system demonstrated flawless accuracy for two individuals, where all 10 attempts resulted in correct face detections, yielding 100% efficiency. For the other two individuals, there were minor deviations. One individual had 9 successful detections out of 10, resulting in a 90% efficiency rate, while another had 8 correct detections, leading to an 80% efficiency rate. Overall, the face detection system displayed high reliability despite the disturbances, achieving strong and consistent performance, with an overall average efficiency of approximately 92%.

Journal of Information System and Technology Management
JISTM
EISSN: 0128-1666
Volume 10 Issue 39 (June 2025) PP. 197-208
DOI: 10.35631/JISTM.1039013

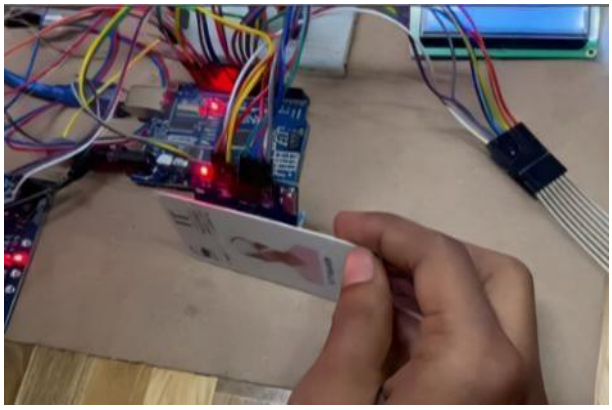

Figure 9: RFID Authentication

The RFID-based authentication system efficiently scanned and processed card data for access control. As shown in Figure 9. the RFID reader successfully detected and transmitted the card's unique information to the microcontroller, which then authenticated the card and triggered the unlock mechanism. The system was tested under various conditions and consistently demonstrated 100% accuracy in scanning and identification. This confirms the RFID system's reliability for secure, real-time access management.

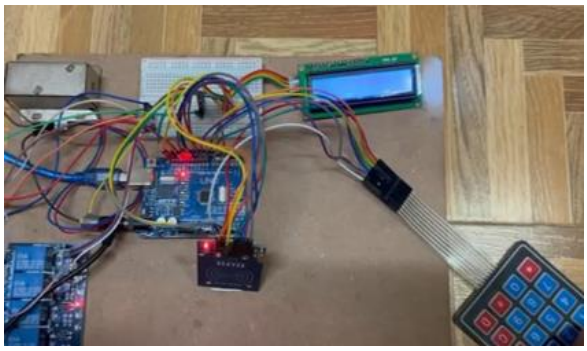

Figure 10: Keypad Authentication

Figure 11: LCD Display

We have utilized a keypad-based door lock system that operates with complete accuracy as shown in Figure 10. Users can enter a predefined passcode using the keypad, which is then processed by the microcontroller. When the correct code is entered, the system immediately unlocks the door and displays "Access Granted!" on the LCD screen, as shown in Figure 11. This ensures that only authorized users can unlock the door. The system performed flawlessly during testing, achieving a 100% success rate in recognizing the correct passcode, confirming its reliability as a secure access control mechanism.

Conclusion

The development and implementation of the IoT-Enabled Multi-Factor Authentication Door Lock System, integrating facial recognition via ESP32-CAM, RFID, and keypad-based authentication, have proven effective in enhancing access control through the combination of multiple security layers. The system's modular design offers flexibility and scalability, enabling the integration of additional authentication methods or IoT devices to suit various security requirements. While RFID and keypad components achieved a 100% success rate in user authentication, the facial recognition system exhibited an overall efficiency of 92%, with minor deviations due to factors such as spectacles or facial hair. Under optimal conditions, average detection accuracy reached 97%, confirming the system's robustness. This multi-layered

Journal of Information System and Technology Management
JISTM
EISSN: 0128-1666
Volume 10 Issue 39 (June 2025) PP. 197-208
DOI: 10.35631/JISTM.1039013
approach significantly reduces the risk of unauthorized access and provides a secure, adaptable solution suitable for a wide range of environments. The system demonstrates strong performance across all components, with the potential for future expansions to further enhance security capabilities.

Acknowledgements
We would like to express our sincere gratitude to Florence Gnana Poovathy, our corresponding author, for her exceptional guidance, constant encouragement, and unwavering support throughout the research project. Her leadership and dedication greatly contributed to the successful completion of this work. We are truly grateful for her valuable suggestions and for being a strong pillar for our entire team from the beginning to the end of the research. We would also like to extend our heartfelt thanks to our team members — Akshith, Mukka Rashmitha, Ashwin Karthik, Sandeep Krishna, and Divya — for their consistent efforts, creative ideas, and strong collaboration. Each member of the team made meaningful contributions, whether it was through research, analysis, discussions, or writing. The success of this project would not have been possible without the collective effort and dedication of every individual involved. We are thankful for the spirit of teamwork, mutual respect, and support that kept us motivated throughout the journey. This research has not only enriched our knowledge but also strengthened our bond as a team.

References
Alsahlani, A. Y. F., & Popa, A. (2021). LMAAS-IoT: Lightweight multi-factor authentication and authorization scheme for real-time data access in IoT cloud-based environment. *Journal of Network and Computer Applications*, *192*, 103177.

AFROZ, A. (2022). Digital Smart Door Lock Security System Using Arduino Uno Microcontroller. *Iconic Research and Engineering Journals*, *6*(1).

Chandra, M., Sandeep, M., Reddy, P. P. K., Reddy, R. S. K., Sowrya, P. C., & Kumar, A. (2023, December). Door Lock System Using HumanFaces With ESP32-CAM. In *2023 Fourth International Conference on Smart Technologies in Computing, Electrical and Electronics (ICSTCEE)* (pp. 1-5). IEEE.

Dharmale, G. J., Katti, J., Waghere, S., Patankar, T., & Ati, K. (2022, October). Door Lock using RFID and Arduino. In *2022 13th International Conference on Computing Communication and Networking Technologies (ICCCNT)* (pp. 1-5). IEEE.

Dhillon, P. K., & Kalra, S. (2018). Multi-factor user authentication scheme for IoT-based healthcare services. *Journal of Reliable Intelligent Environments*, *4*, 141-160.

Kodali, R. K., & Soratkal, S. (2016, December). MQTT based home automation system using ESP8266. In *2016 IEEE Region 10 Humanitarian Technology Conference (R10-HTC)* (pp. 1-5). IEEE.

Kumar, T. D., Archana, M. A., Umapathy, K., Gayathri, G., Bharathvaja, V., & Anandhi, B. (2023, July). RFID based smart electronic locking system for electric cycles. In *2023 4th International Conference on Electronics and Sustainable Communication Systems (ICESC)* (pp. 76-81). IEEE.

Raju, N., Navya, A., Koteswaramma, N., Mounika, B., & Rajeshwari, T. (2022). IoT-based Door Access Control System using ESP32 CAM. *International Journal of Engineering Inventions*, *11*(12), 9-15.

Saad, I., Amran, N. S., Haris, H., & Tan, M. K. (2023, September). Development of contactless door lock system using text-dependent voice authentication. In *2023 IEEE International Conference on Artificial Intelligence in Engineering and Technology (IICAIET)* (pp. 301-306). IEEE.

Journal of Information System and Technology Management
JISTM
EISSN: 0128-1666
Volume 10 Issue 39 (June 2025) PP. 197-208
DOI: 10.35631/JISTM.1039013
Sanath, K., Meenakshi, K., Rajan, M., Balamurugan, V., & Harikumar, M. E. (2021, April). RFID and face recognition based smart attendance system. In *2021 5th International Conference on Computing Methodologies and Communication (ICCMC)* (pp. 492-499). IEEE.

Shanthini, M., Vidya, G., & Arun, R. (2020, August). IoT enhanced smart door locking system. In *2020 Third International Conference on Smart Systems and Inventive Technology (ICSSIT)* (pp. 92-96). IEEE.

Singh, N., Singh, D. R., Kumar, R., Paliwal, S., & Srivastava, S. (2022). ESP32 CAM Face Detection Door Lock. *International Research Journal of Engineering and Technology (IRJET)*, *9*(2), 1392-1393.

Soni, S., Soni, R., & Waoo, A. A. (2021). RFID-based digital door locking system. *Indian Journal of Microprocessors and Microcontroller (IJMM)*, *1*(2), 17-21.

Sutradhar, S., Bose, R., Majumder, S., Khan, A. A., Roy, S., Ullah, F., & Prashar, D. (2025). MediGuard: A Survey on Security Attacks in Blockchain-IoT Ecosystems for e-Healthcare Applications.