International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 09 Issue: 04 | April - 2025 SJIF Rating: 8.586 ISSN: 2582-3930

RFID and IoT Based Personalized Access System

Safa R. Mhaskar[1] Gautami M. Mestri[2] Rayan H. Mhate[3]

Dr. Suhasini Goilkar[4]

[1,2,3] *Electronics and Telecommunication Engineering,*

Finolex Academy of Management and Technology Ratnagiri.

[4] *Associate Professor Electronics and Telecommunication,*

Finolex Academy of Management and Technology Ratnagiri.

Abstract: The increasing demand for secure and intelligent access control systems has led to the integration of emerging technologies such as RFID, IoT, and biometrics. This project presents a comprehensive RFID and IoT-based personalized access system enhanced with face recognition to ensure robust security. The proposed system employs Radio Frequency Identification (RFID) for initial user authentication, followed by biometric verification through facial recognition using a Raspberry Pi. Upon arrival, the system prompts the individual on an LCD display to scan their ID card. The RFID reader scans the ID card or tag and verifies it against a stored database within the microcontroller. If the ID is valid, the system confirms the person's identity by displaying their name and sends a unique, pre-assigned password to the user's registered mobile number via a GSM module. In the event of an unauthorized card scan, the system alerts all authorized users through SMS, signaling an attempted breach. To add an extra layer of security, the system integrates facial recognition. The Raspberry Pi captures the face of the individual standing before the camera and compares it with the stored facial data of registered users. If a match is identified, the door unlocks, and the system acknowledges the user by displaying their name. If no match is found, the individual is marked as "Unknown" and access is denied. To handle the increased storage needs for facial data, an external storage device is connected to the Raspberry Pi. This dual-layer authentication system ensures that only authorized personnel can access secure areas, offering a combination of RFID technology for identification and facial recognition for biometric verification. The use of IoT technologies like GSM enhances real-time communication and alerts, making the system suitable for applications in residential buildings, offices, and high-security zones.

Key Words - RFID, IoT, GSM, Facial Recognition, Raspberry Pi, Access Control, Biometric Security, Keypad.

Introduction:

In an era where security breaches and unauthorized access are growing concerns, advanced authentication system have become a necessity. The RFID and IoT-based personalized access system is designed to enhance security by integrating RFID authentication, GSM communication, and face recognition using a Raspberry Pi. This system ensures that only authorized individuals gain access to security areas, combining multiple layers of authentication for robust protection. Initially, users are prompted via an LCD display to scan their RFID card or tag, which is then checked against a pre-stored databased in the microcontroller. If the ID is verified, the system grants access by displaying the person's name on the LCD and sending a unique, pre-assigned password to their registered mobile number via GSM. Each authorized users has a distinct password, further strengthening the authentication process. However, if an unauthorizes RFID card is detected, access is denied, and an alert SMs is immediately sent to all authorized users, notifying them of the attempted breach.

To reinforce security, the system incorporates a face recognition feature using a Raspberry Pi, which stores the facial data of authorized individuals for identity verification. When a person approaches the access point, the system captures and compares their facial features with the stored data. Of a match is is found, access is granted,

and the person's name is displayed. Conversely, if no match is identified, the individual is marked as "Unknown" and access remains restricted. Since facial recognition requires significant storage capacity, an external storage device is integrated with the Raspberry Pi to accommodate the necessary data. The dual-layer security system not only strengthens access control but also reduces the risk of unauthorized entry by ensuring that both RFID-based authentication and biometric verification are required for access approval. By leveraging IoT technology, real-time communication, and multi-factor authentication, this system provides a comprehensive and intelligent security solution suitable for high-security environments, including corporate offices, research facilities, and restricted zones.

Literature Survey:

Security and access control systems have evolved significantly with advancements in technology, particularly with the integration of Radio Frequency Identification (RFID), the internet of Things (IoT), and biometric authentication methods. RFID-based access control has been widely studied and implemented due to its efficiency in providing seamless and contactless authentication. Several studies highlight RFID's role in enhancing security by enabling unique identification and real-time monitoring of access attempts. Traditional RFID-based system, however, often face security vulnerabilities such as unauthorized duplication of RFID tags and lack of robust authentication mechanisms. To address these concerns, researchers have explored multi-factor authentication techniques by integrating GSM-based communication, ensuring that users receive real-time alerts and unique passwords, thereby reducing the risk of unauthorized access. Biometric security, particularly face recognition, has gained prominence due to its reliability in providing identity verification based on unique facial features. Various studies emphasize the advantages of facial recognition over traditional authentication methods such as password and RFID tags, which can be stolen or duplicated. The use of Raspberry Pi for face recognition has been explored in multiple research works, demonstrating its effectiveness in real-time image processing and storage, prompting researchers to integrate external storage solutions for efficient data handling. The combination of RFID authentication and biometric verification has ben extensively analyzed in recent literature, showcasing its effectively implementing dual-layer security systems. Studies indicate that integrating these two technologies significantly enhances access control by requiring both possession-based (RFID) and biometric-based (face recognition) authentication, reducing the chances of unauthorized entry. Moreover, IoT-based security solutions have been investigated for their ability to enable remote monitoring and real-time communication, making access control system more dynamic and responsive. Research on GSM-based security alerts highlights their importance in notifying users of access attempts, ensuring continuous monitoring of restricted areas. The reviewed literature suggests that integrating RFID, IoT, and biometric authentication, as proposed in the current system, aligns with modern security trends, offering a reliable and efficient access control, mechanism. By combining RFID authentication, GSM-based alerts, and face recognition, this system addresses the limitations of standalone RFID or biometric systems, reinforcing security with a multilayered approach.

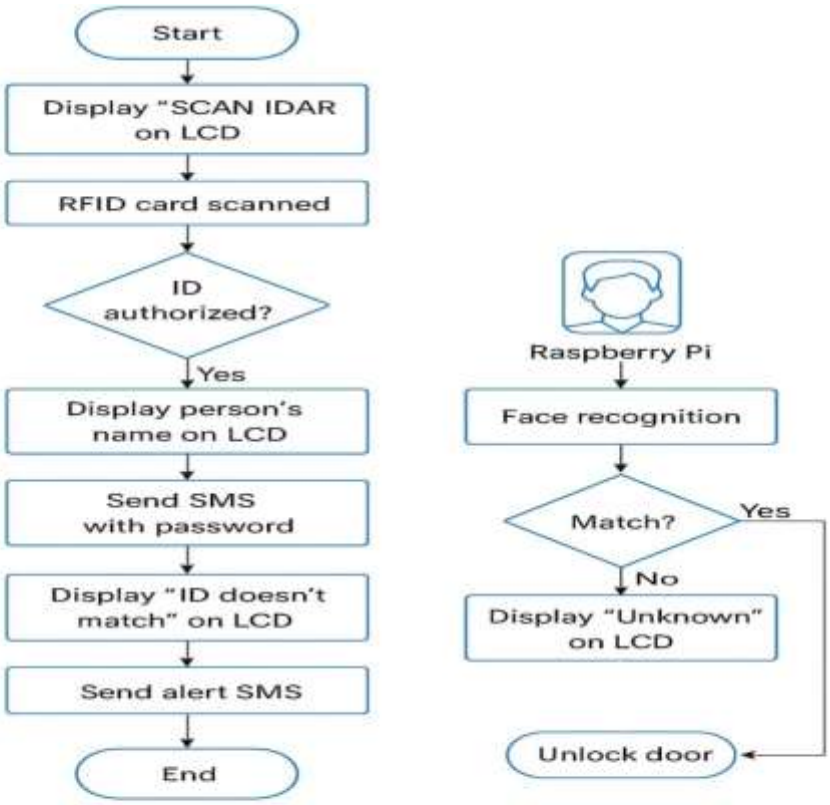
Problem Statement:

In today's world, ensuring security and restricted access to sensitive area such as offices, laboratories, and residentials buildings has become increasingly important. Traditional lock-and-key mechanisms or standalone RFID system often fall short in offering comprehensive protection due to vulnerabilities like card duplication, theft, or unauthorized sharing of credentials. Moreover, many existing access control systems lack real-time monitoring, remote communication, and adaptive verification capabilities, making them inefficient for handling modern security challenges. There is a growing demand for intelligent systems that can provide multi-layer authentication, instant alerts, and real-time user verification. To address these concerns, there is a need for an integrated and scalable solution that not only verifies identity using RFID-based authentication but also incorporates biometric verification, such as facial recognition, for added security. Additionally, the system must ensure real-time communication through GSM modules to notify users of any unauthorized attempts, while

maintaining a user-friendly interface for legitimate access. The core problem lies in combining these diverse technologies-RFID, GSM, and facial recognition-into a synchronized into cost-effective access control system that can operate seamlessly using microcontrollers like Arduino and computing platform such as the Raspberry Pi.

Flow Chart:

The flowchart begins with the system prompting the user to scan their RFID card. If the RFID is valid, an SMS with a unique password is sent, and face recognition is initiated. The face is matched with stored data using the Raspberry Pi. If both verifications succeed, access is granted; otherwise, an alert is triggered.



RFID and IoT-based access system

Working:

The RFID and IoT-Based personalized access system combines key hardware components like an RFID reader, GSM module, LCD display, microcontroller, Raspberry Pi, camera module, and external storage. The RFID reader and microcontroller handle ID authentication and SMS alerts, while the Raspberry Pi with camera performs facial recognition using python and OpenCV. An external storage device supports the storage of facial data. Software tools like Arduino IDE and Python scripts coordinate hardware operations, ensuring smooth integration of RFID and biometric verification for enhanced security.

This RFID and IoT-based personalized access system is structured around a two step authentication process that combines RFID verification and facial recognition to ensure secure access. The system begins by prompting the user through an LCD interface to scan their RFID card or tag. The RFID reader captures the card's unique

identification number and sends it to the Arduino Uno, which compares the ID with a preloaded database stored in its memory. If the Id is found in the database, the corresponding user's name is displayed on the LCD screen, and the Arduino sends a signal to the GSM module to deliver an SMS to the registered mobile number. This SMS contains a unique pre-assigned password for an added layer of verification. The user is then required to input this password through a numeric keypad connected to a second Arduino Uno. If the entered password matches the stored one, the process continues. Simultaneously, the Raspberry Pi with a connected camera module captures the user's face and compares it with the stored facial data in its database. If a match is detected, the Raspberry Pi signals the system to unlock the door and display the user's name. It the facial data does match, the system remains locked and the user is labeled as "Unknown". In the case of unrecognized RFID card scan, the system immediately display a warning message on the LCD and the GSM module send an alert SMS to all authorized users, indicating a potential unauthorized access attempt. The Raspberry Pi also stores the captured unknown face data for future reference

Result:

- Accurate RFID Authentication: The system successfully identifies and authenticates authorized users through RFID cards, displaying their names and sending secure passwords via GSM.
- Effective Intrusion Alerts: Unauthorized RFID scans trigger real-time alert messages to all authorized users, enhancing the system's responsiveness to potential security breaches.
- Reliable Face Recognition: The Raspberry Pi-based face recognition accurately verifies authorized users and ensures the door unlocks only upon a successful match.
- Secure Dual-Layer Access: The integration of both RFID and facial recognition creates a robust, two-factor authentication process, significantly improving overall access control security.
- Efficient Data Management: External storage with the Raspberry Pi allows effective handling of facial recognition data without performance issues, supporting multiple user profiles.

Fig 1.1 Model

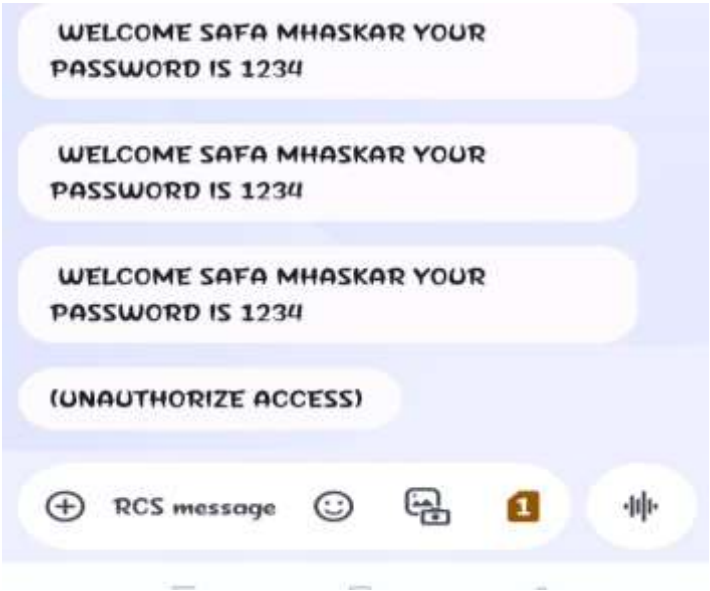


Fig 1.2 SMS Receiving

Conclusion and Future Scope:

The RFID and IoT based personalized access system is highly secure and efficient authentication solution that leverages RFID technology, GSM communication, and face recognition using a Raspberry Pi. This system provides a multi-layered security mechanism that not only verifies users based on RFID credentials but also ensures an additional level of authentication through biometric face recognition. The combination of these two technologies significantly enhances security, Reducing the risk of authorized access and improving overall access control management. By implementing RFID authentication, the system ensures that only users with registered RFID cards can initiate the authentication process. If an authorized RFID card is detected, an SMS containing a unique password is sent to user's registered mobile number via GSM, adding an additional layer of security. Unauthorized RFID attempts trigger an alert notification to all registered users, thereby keeping the system administrators informed about potential security breaches. Incorporating face recognition with a Raspberry Pi further enhances the security framework by ensuring the pre-registered individuals can successfully complete the authentication process. The system captures and processes facial images, comparing them with stored biometric data. If a match is found, access is granted, and the door unlocks. If no match is found, access is denied, and the individual is labeled as "Unknown". Since biometric verification requires additional storage, an external storage device is integrated with the Raspberry Pi, enabling efficient management of facial data.

Future Scope:

In the future, the system can be extended by incorporating cloud storage for centralized facial data management, enabling remote access and real-time monitoring. Integration with mobile applications can enhance users control and flexibility. Ai-based facial recognition can improve accuracy under different lighting and environment conditions. Additionally, expanding the system for multi-location use, attendance tracking, and analytics and benefit corporate offices, educational institutions, and secure facilities. Voice recognition and fingerprint authentication can also be added for even stronger multi-factor security.

References:

1. Thejaswini S, Rashmi N, Mamatha K R, Dr. Seema Singh, & Dr. Girish H. (2024). Intelligent Access Control Using RFID and IoT Blynk Interface. Educational Administration: Theory and Practice, 30(1), 4603–4610. (kuey.net)
2. Oluwasola S. Maitanmi, Akinniran O. Oke, Ayorinde Peters Oduroye, Adesoji Adedeji Adegbola, Olubukola D. Adekola, Ajao Joseph Oluwtosin, Kikelomo Ibiwumi Okesola, Michael Agbaje, Funmilayo A. Sanusi, Akintoye A. Onamade, Olusegun Gbenga Lala. (2024). Design and Implementation of a Door Card Access System Using Internet of Things Technology. International Journal of Intelligent Systems and Applications in Engineering, 12(23s), 600–605. (ijisae.org)
3. J. Selvin Paul Peter, Mehul Singh, Sarthak Verma. (2020). IoT Based Security System Using RFID Tags. International Journal of Advanced Science and Technology, 29(06), 2486–2490. (sersc.org)
4. Agbotiname Lucky Imoize, Olusegun Babatunde Alabi. (2021). Implementation of a User-Friendly Radio Frequency Identification and Password-Enabled Security Access System. Journal of Telecommunication, Electronic and Computer Engineering (JTEC), 13(2), 23–30. (jtec.utem.edu.my)
5. Soheb Khamaysah, Mahmoud Hijjeh, Muhammad Odeh. (2024). IoT-Based Attendance System Using RFID and Fingerprint. Graduation Project, College of Information Technology and Computer Engineering. (scholar.ppu.edu)
6. Preeti Soni, Mohammad S. Obaidat, Arup Kumar Pal, SK Hafizul Islam. (2022). RFID-Based Authentication Scheme for Secure Access of Medical Data in IoT-Enabled Health Environments. In

Advances in Distributed Computing and Machine Learning (pp. 59–69). Springer, Singapore. (link.springer.com)
7. Puhshadapu Paparao, Ch. Lakshmi Prasad. (2018). RFID Based Advanced Technology for Security in Small Homes Using IoT. International Journal of Research, 5(12), 2305–2310. (journals.pen2print.org)
8. Umar Farooq, Mahmood ul Hasan, Muhammad Amar, Athar Hanif, Muhammad Usman Asad. (2015). RFID Based Security and Access Control System. International Journal of Engineering and Technology, 6(4), 309–314.
9. K. S. T. Kumar, S. S. Kumar, R. S. Shaji. (2016). IoT Based Access Control Mechanism Using RFID Technology. Asian Journal of Computer Science and Technology, 5(S1), 45–48.
10. S. S. Kulkarni, P. S. Kulkarni. (2017). Face Recognition using Raspberry Pi. International Journal of Advanced Research in Computer and Communication Engineering, 6(4), 632–636.
11. Muhammad Naveed Aman, Kee Chaing Chua, Biplab Sikdar. (2017). Securing IoT-Based RFID Systems: A Robust Authentication Protocol. IEEE Transactions on Industrial Informatics, 13(3), 1466–1474.
12. Piotr Porwik, Bartosz Mrozek, Adam Lis, Andrzej Lis. (2020). Personal Identification Using Embedded Raspberry Pi-Based Face Recognition System. Applied Sciences, 10(14), 4825.