INTERNATIONAL SCIENTIFIC JOURNAL OF ENGINEERING AND MANAGEMENT (ISJEM) ISSN: 2583-6129
CONFERENCE PROCEEDINGS: VOLUME: 05 ACME – 2026 DOI: 10.55041/ISJEM.ACME139
AN INTERNATIONAL SCHOLARLY || MULTIDISCIPLINARY || OPEN ACCESS || INDEXING IN ALL MAJOR DATABASE & METADATA

IOT Smart Door System with Motion Sensing and Facial Recognition

Ms.S.Bhavani
Assistant Professor
Department of Electronics and Communication Engineering
Annamacharya Institute of Technology and Sciences
Tirupati, India.
bhavanisangadala433@gmail.com

Dande Venkata Naga Likhit Royal
UG Student
Department of Electronics and Communication Engineering
Annamacharya Institute of Technology and Sciences
Tirupati, India.
likhithroyaldande@gmail.com

Koneti Yashwitha Reddy
UG Student
Department of Electronics and Communication Engineering
Annamacharya Institute of Technology and Sciences
Tirupati, India.
yashwithareddy028@gmail.com

Nadimicherla Mahesh
UG Student
Department of Electronics and Communication Engineering
Annamacharya Institute of Technology and Sciences
Tirupati, India.
msm1432657@gmail.com

Gundumani Pavan
UG Student
Department of Electronics and Communication Engineering
Annamacharya Institute of Technology and Sciences
Tirupati, India.
pavangundumani@gmail.com

***Abstract*—**The increasing demand for intelligent home security solutions has led to the adoption of Internet of Things (IoT) technologies in access control systems. The project proposes an IoT smart door system that integrates motion detection, facial recognition, and RFID authentication to enhance safety and automation. A PIR sensor is used to detect human movement near the door, after which a camera module captures the facial image of the individual. Facial authentication is performed using cloud-based recognition techniques. In addition, an RFID module is incorporated as an alternative and supplementary authentication method, allowing authorized users to gain access through registered RFID tags or cards. Access is granted only when valid credentials are verified through either facial recognition or RFID authentication, while unauthorized attempts are restricted and instant alerts are generated. The system is implemented using an Arduino Uno, providing a cost-effective, reliable, and scalable security solution for modern residential environments.

Keywords— IoT, Smart Door System, PIR Motion Sensor, Arduino Uno, Facial Recognition, RFID Authentication, Cloud Service.

I. INTRODUCTION

Smart security has become an essential requirement due to increasing safety concerns and advancements in digital technology. Conventional door locking systems based on mechanical keys often fail to provide adequate protection because of risks such as key loss, duplication, and lack of monitoring. To address these limitations, IoT- enabled access control systems are being widely adopted in modern.

The proposed IoT-based smart door system is developed to offer a secure and automated solution for controlling entry access. The system works by continuously monitoring the area near the door using a PIR motion sensor. Whenever someone approaches, the sensor detects movement and immediately triggers the camera module. The camera then captures the person's facial image, which is further processed for identity verification. This approach ensures that the system remains energy efficient while providing real-time monitoring and enhanced security. The captured image is processed using cloud-based facial recognition to verify user authorization. And also uses RFID authentication, Authorized individuals are allowed entry automatically, while unauthorized access attempts are denied and alerted. This approach enhances security while reducing manual intervention.

II. LITERATURE SURVEY

The foundation of modern access control has shifted significantly toward Internet of Things (IoT) frameworks

and remote connectivity. Early research, such as the studies by Sujita et al. [1] and Gupta et al. [2], proved that low-power microcontrollers like the NodeMCU are highly effective for managing entry points via mobile apps. These researchers demonstrated how linking physical locks to digital interfaces allows for real-time monitoring without needing expensive infrastructure. Building on this, Aswini et al. [4] explored the transition from traditional mechanical keys to cloud-based credentials, which is a vital step for deploying flexible security solutions in diverse professional or industrial settings.

To make these systems more reliable, recent literature has moved away from single-point entry toward multi-layered verification and sensor fusion. Simatupang and Tambunan [5] developed a robust approach that combines RFID, fingerprint scanning, and physical keypads to minimize the chances of unauthorized access. This concept is reinforced by Ahmed et al. [3], who argued that dual-factor authentication is essential for protecting "critical zones." By requiring a physical token alongside a secondary credential, these systems provide much higher integrity than basic methods, making them ideal for high-security installations where verifying identity is the top priority.

The current state-of-the-art in autonomous identification involves using computer vision and machine learning for a "touchless" experience. Wati and Abadianto [6] and Zhu and Cheng [7] showed how OpenCV and attitude-tracking algorithms can make face recognition more accurate, even in unpredictable environments. By merging these visual capabilities with IoT and machine learning as seen in the work of Pawar et al. [8] and Kumar and Rekha [9] modern systems can now achieve high-precision monitoring. These advancements offer a sophisticated layer of security that can be easily adapted for a wide variety of multi-purpose applications, from corporate offices to automated facilities.

III. METHODOLOGY

The methodology adopted for Fig.1.developing the IoT-based smart door system with motion detection and facial recognition is outlined as follows:

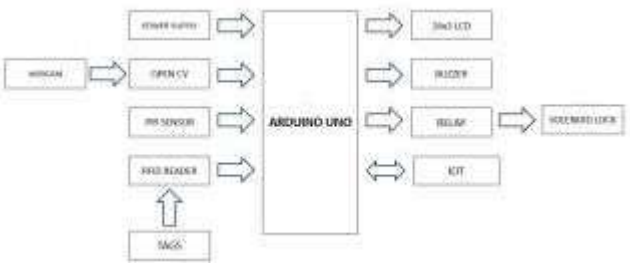


Fig.1.Block diagram of the proposed methodology

A. Power Supply

The system is powered by a reliable power source that feeds the Arduino Uno and all connected peripherals.

B. Input Components:

- **OpenCV:** The facial recognition software runs on a connected device (Opens the camera and use Haar Cascades to find a face. Uses the LBPH Recognizer to compare the face against your "Authorized" database. With external processing) using OpenCV for image processing and recognition.
- **PIR Sensor:** Detects motion near the door, triggering the system to activate facial recognition or RFID scanning.
- **RFID Reader&Tags:** Provides an alternative authentication method using RFID tags for access control.

C. Processing Unit (Arduino Uno):

The Arduino acts as the central controller, managing inputs from sensors and RFID, processing facial recognition data (or interfacing with a secondary processor for OpenCV), and making access decisions.

D. Output Components:

- **16x2 LCD:** Displays system status, access messages, or user information.
- **Buzzer:** Gives alerts for access granted/denied or system notifications.
- **Relay & Solenoid Lock:** Controls the door lock; the relay activates the solenoid to unlock the door upon successful authentication.

- **IoT:** Enables remote monitoring and control via internet connectivity, sending logs or receiving commands for smart management, Although the IoT module supports bidirectional communication its primary function is data transmission to cloud services.

E. Operation Flow:

- Motion is detected by the PIR sensor, prompting the system to activate facial recognition (OpenCV) or wait for RFID input.
- Facial recognition verifies the user's identity; if recognized, the Arduino triggers the relay to unlock the door.
- Alternatively, an RFID tag is scanned for access.
- The LCD displays status, and the buzzer sounds for feedback.
- All events are logged or transmitted via IoT for remote access and monitoring.

IV. SYSTEM WORK FLOW

The overall workflow of the proposed method is illustrated through a sequential operational process. The system integrates motion detection, biometric authentication, alternative RFID access, and IoT-based monitoring to ensure secure and automated door control. Fig.2.Represents the model representation.

Step 1: System Initialization

- When the power supply is switched ON, the Arduino Uno initializes all connected peripherals including the PIR sensor, camera module, RFID reader, ESP8266 Wi-Fi module, LCD display, buzzer, and relay-controlled solenoid lock. The system enters standby monitoring mode.

Step 2: Motion Detection

- The PIR (Passive Infrared) sensor continuously monitors the area near the door.
- When the motion sensor detects movement near the entrance, it immediately sends a signal to the Arduino Uno controller.
- Upon receiving this signal, the system activates the camera module to capture an image of the person approaching the door.

Step 3: Image Capture and Facial Recognition

- The captured facial image is then analyzed using OpenCV-based recognition techniques, which can be performed either on a local processing unit or through a cloud-enabled IoT platform, depending on the system configuration.
- The facial features are extracted and compared with the stored authorized user database.
- The system determines whether the person is authorized or unauthorized.

Step 4: Authentication Decision

Case 1: Authorized Face Detected

- If the face matches stored data, access is granted. Arduino activates the relay module The solenoid lock opens the door. LCD

displays: “Access Granted” via Face ID. Entry log is sent to the IoT cloud.

Case 2: Unauthorized Face Detected

- If the face does not match the database, access is denied. Door remains locked. Entry log is sent to the IoT cloud.

Step 5: RFID-Based Alternative Authentication

- If facial recognition fails or if an authorized user prefers RFID access:

- The RFID reader scans Arduino verifies the tag ID with stored authorized IDs. If valid → Door unlocks. If invalid → Access denied and alert triggered.

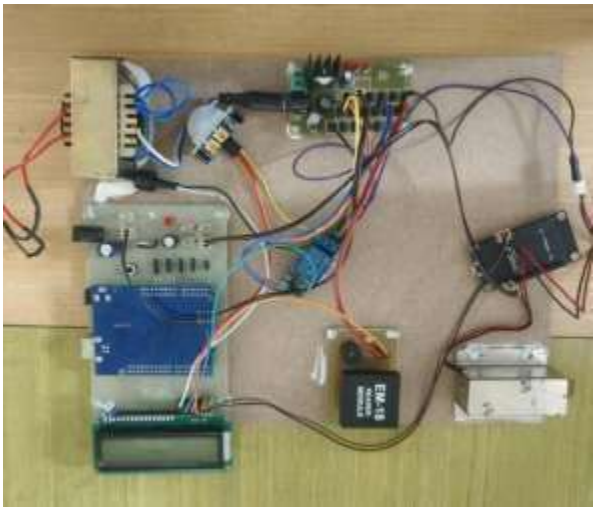


Fig.2.Model Representation.

Step 6: IoT Monitoring and Logging

All authentication events (authorized, unauthorized) are: Logged in the system database. Transmitted to the cloud via Wi-Fi module.

Displayed in the IoT cloud for real-time monitoring.

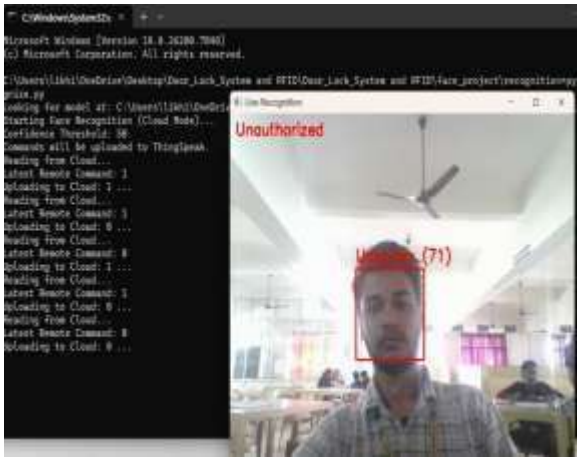
Step 7: System Reset

After a predefined delay the door automatically locks again. The system returns to motion detection standby mode.

V. RESULTS & DISCUSSION

A. Test with authorized face

When an authorized person enters the detection area, the smart door system automatically verifies their identity



using facial recognition. Fig.3.Represents the Authorized Person. Once the captured face matches the stored authorized data, the system grants access by unlocking the door instantly. This ensures secure and seamless entry for permitted users while preventing unauthorized access, thereby enhancing overall safety and convenience. Fig.4.Represents the access granted via face

ID,Fig.5.shows the door unlocks.

Fig.3.Authorized person

Fig.4.Access Grant using Face ID

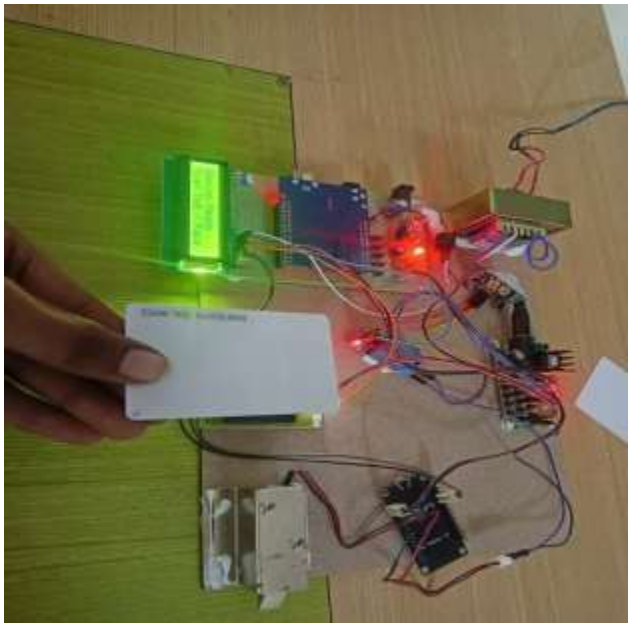


Fig.5.Door Unlocks

B. Test with unauthorized face:

When an unauthorized person enters the detection area, the smart door system successfully identifies that the captured face does not match any stored authorized data. As a result, the door remains securely locked, preventing access and ensuring safety. The system also records the unauthorized attempt and updates the entry log in the IoT cloud for monitoring and tracking

purposes.Fig.6.Represents the Unauthorized person,Fig.7.Shows the Door remains locked.

Fig.6.Unauthorized person

Fig.7.Door Locks

C. *Test with RFID card:*

In addition to facial recognition, RFID cards are used as an alternative authentication method in the smart door system.Fig.8.shows the Authentication of RFID. When an authorized RFID card is scanned, the system verifies the card and unlocks the door successfully. Fig.9.shows the authorized tag, Fig.10.represents the door opens. If an invalid or unauthorized card is detected, the door remains locked and a buzzer is activated to alert nearby users of unauthorized access, while an alert message is displayed on the LCD, ensuring enhanced security and immediate warning.Fig.11.shows the unauthorized tag, Fig.12.represents the door remains locked.

Fig.8.RFID Authentication

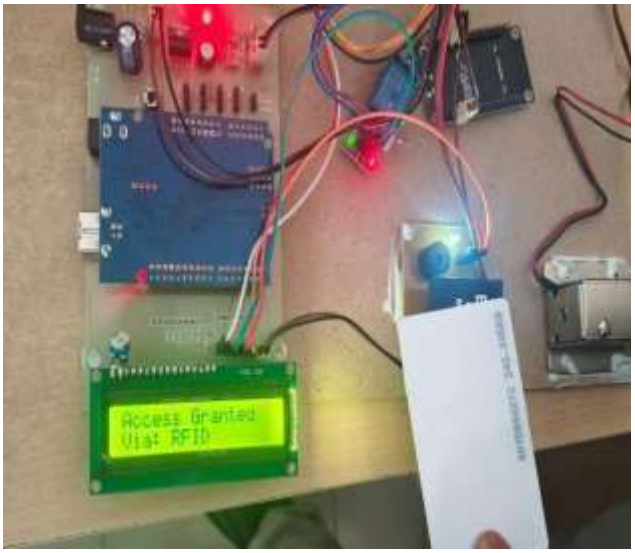


Fig. 9. Authorized Tag

Fig. 10. Door Unlocks

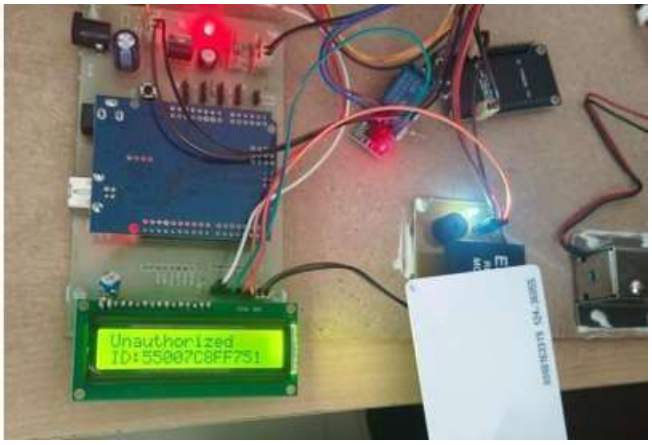


Fig.11.Unauthorized Tag

Fig. 12. Door Locks

VI. CONCLUSION

This project describes the development and implementation of an IoT-based smart door system that integrates motion detection and facial recognition to improve security and access control. The proposed system utilizes a PIR sensor to detect human presence and activates a camera module for facial authentication

using computer vision techniques. Authorized access is granted automatically, while unauthorized attempts are restricted and door remains locked. An RFID-based access method is also integrated to provide an alternative authentication mechanism. The system ensures real-time monitoring, reduced manual intervention, and improved access reliability. The experimental results indicate that the proposed system provides an efficient, reliable, and scalable security solution, making it well-suited for use in homes as well as institutional environments.

ACKNOWLEDGMENT

The authors sincerely thank Annamacharya Institute of Technology & Sciences, Tirupati (Autonomous), for providing the infrastructure, resources, and continuous support that made this work possible. We are especially grateful to Dr. S. Rohini, M.Tech., Ph.D., Associate Professor and Head of the Department of Electronics and Communication Engineering, for her guidance, motivation, and consistent encouragement throughout this work. We also extend our heartfelt appreciation to Ms. S. Bhavani, M.Tech., Assistant Professor, Department of ECE, for her valuable support and financial assistance towards the publication of this research.

REFERENCES

[1] S. A. L. Sujita B. Dabekar, Manasi S. Lunge, Prof. Deepali Yewale, "IOT Based Smart Door Locked System Using Node MCU," Ijraset Journal For Research in Applied Science and Engineering Technology, vol. 10, no. 7, pp. 4384-4388, July 2022 2022, doi: https://doi.org/10.22214/ijraset.2022.45909.

[2] K. Gupta, N. Jiwani, M. H. U. Sharif, M. A. Mohammed, and N. Afreen, "Smart Door Locking System Using IoT," in 2022 International Conference on Advances in Computing, Communication and Materials (ICACCM), 10-11 Nov. 2022 2022, pp. 1-4, doi: 10.1109/ICACCM56405.2022.10009534.

[3] M. N. A. M. M. H. S. O. F. Mohammed Shoaibuddin Ahmed, "Smart and Secure Door Lock with Dual-Factor Authentication for Critical Zones," Mathematical Statistician and Engineering Applications, vol. 72, no. 1, pp. 1491-1501, 01/12 2023, doi: 10.17762/msea.v72i1.2373.

[4] D. Aswini, R. Rohindh, K. S. M. Ragavendhara, and C. S. Mridula, "Smart Door Locking System," in 2021 International Conference on Advancements in Electrical, Electronics, Communication, Computing and Automation (ICAECA), 8-9 Oct.2021,pp.1-5, doi: 10.1109/ICAECA52838.2021.9675590.

[5] J. W. Simatupang and R. W. Tambunan, "Security Door Lock Using Multi-Sensor System Based on RFID, Fingerprint, and Keypad," in 2022 International Conference on Green Energy, Computing and Sustainable Technology (GECOST), 26-28 Oct. 2022 2022, pp. 453-457, doi: 10.1109/GECOST55694.2022.10010367.

[6] D. A. R. Wati and D. Abadianto, "Design of face detection and recognition system for smart home security application," in 2017 2nd International conferences on Information Technology, Information Systems and Electrical Engineering (ICITISEE), 1-2 Nov. 2017 2017, pp. 342-347, doi: 10.1109/ICITISEE.2017.8285524.

[7] Z. Zhu and Y. Cheng, "Application of attitude tracking algorithm for face recognition based on OpenCV in the intelligent door lock," Computer Communications, vol. 154, pp. 390-397, 2020/03/15/ 2020, doi: https://doi.org/10.1016/j.comcom.2020.02.003.

[8] S. Pawar, V. Kithani, S. Ahuja, and S. Sahu, "Smart Home Security Using IoT and Face Recognition," in 2018 Fourth International Conference on Computing Communication.

[9] A. S. Kumar and R. Rekha, "Improving Smart Home Safety with Face Recognition using Machine Learning," in 2023 International Conference on Intelligent Systems for Communication, IoT and Security (ICISCoIS), 9-11 Feb. 2023 2023, pp. 478-482, 10.1109/ICISCoIS56541.2023.10100592.