IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Smart Door Access System Using Iot

Hybrid authentication based security solution

Meena Kumari[1], Vrinda Yadav[2], Vaishnawi Kumari[3], Saumya Bansal[4]

[1] Assistant Professor, [2]Student, [3]Student, [4]Student

Department of Computer Science and Engineering (IoT), ABES Institute of Technology, Ghaziabad, India

Abstract: Old methods like RFIDs, PIN codes, key security mechanisms are showing their weakness. These Old methods have the danger of manipulation like keys being stolen or copied. These methods can be easily tampered on a keypad PIN as a backup option. Additionally, the system also has a mobile application that allows authorised users to remotely lock or unlock the door with just a tap. By using multiple modes of authentication, the system focuses on convenience and removes single points of failure. In essence, this project can be considered as a step towards a safer and smarter access with security, which aligns with the technology driven world of today.

Index Terms — Smart Door Lock, IoT, ESP32-CAM, Hybrid Authentication, Face Recognition, Security System, Mobile App Access.

I. INTRODUCTION

Progress in IOT and embedded systems has affected change in how modern security systems are designed. Old door locks like keys, pins, or RFID cards, have hown that there is a risk of misuse, so there is an increase in demand for systems that are intelligent and automated such that the reliability and security can be increased.

A hybrid smart door lock system is a feasible solution for this, by using ESP32-CAM which allows real-time monitoring and gives remote access to users. Even if this fails, there are backups in place that can be used, this enhances the overall functionality of the model. This project focuses on providing a cost-effective, scalable, and secure solution that might be suitable for our homes.

1.1 Motivation

There is an increase in need for a secure and affordable access control system which is the motivation behind the development of this hybrid system. Conventional locks as well as modern locks are dependent upon a single authentication method which has risk of failure, unauthorised access and high installation costs along with issues of complexity which decrease its use among consumers. The aim of this project is to make an integrated system that has face recognition along with keypad-based authentication and simple application interface so that the system becomes reliable, user friendly and is a low cost security solution that aligns with the vision of a secure and smart environment such that the gap between affordability and technology can be decreased.

1.2 Objective

The goal of this project is to design and implement a system that uses facial recognition and PIN authentication using an IoT-based hybrid smart door lock system using the ESP32-CAM module in order to provide user convenience, better access control and improved reliability.

1. Multi- Authentication

There is multiple layers of security in the system so that even if one authentication method fails the other can be used, like if facial recognition fails then PIN based verification can be used as a backup.

2. Intelligent Recognition

A lightweight MTCNN model is used in the ESP32-CAM so that there is quick and accurate facial detection. This approach ensures that the hardware and overall cost are low along with increasing recognition efficiency.

3. Cost- Effective and Easy to Deploy

The design ensures that the project focuses on affordability and simplicity. The components being used are easily available. It also requires only minimal technical expertise that makes it suitable for both household and small-scale commercial use.

4. Scalable and Adaptable

The system is flexible and can be scaled up and used with the existing smart home technologies. The design ensures that it can be effectively used in various environments, including homes, offices, or educational institutions.

1.3 Problem Statement

As the technology is advancing, traditional security measures such as the use of keys, RFID tags, and PINs are losing their reliability as they are prone to theft, duplication, or brute force attacks. Even modern methods like facial recognition and fingerprint can be misused using photo spoofing or face difficulties in low light and high implementation costs. That is why there is a need for a cost effective, scalable, and robust solution for practical implementation.

II. LITERATURE REVIEW

1. In Ref [1], Jakia Sultana Sonamoni et al. (2024) proposed an IoT-based smart remote door lock and monitoring system using an Android application. Their design integrated mobile app control and real-time feedback, demonstrating reliable remote access and monitoring capabilities.
2. In Ref [2], Dick Daz Delgado et al. (2025) developed an IoT-enabled smart lock using YOLOv5-based real-time person detection and mobile app integration. The system, implemented on a LilyGo ESP32-S3 microcontroller, achieved 96% detection accuracy with low power consumption.
3. In Ref [3], Chukwuemeka Obasi and Kasim Mohammed Tahir (2025) introduced a real-time smart door access control system using Haar Cascade classifiers and embedded vision. Implemented on ESP32-CAM, it achieved 97% accuracy with 151 ms average detection time, suitable for low-power IoT applications.
4. In Ref [4], M. Marimuthu et al. (2025) presented a facial recognition–enabled smart security lock system using machine learning. Their multimodal approach combines ESP32-CAM and Arduino for facial and fingerprint authentication, offering high biometric accuracy and enhanced security.
5. In Ref [5], Rizky A. Susilo et al. (2024) designed and built a smart door lock using face recognition with Telegram-based security monitoring. The ESP32-CAM module performed efficiently within 30–90 cm, while Telegram alerts ensured real-time surveillance and improved safety.
6. In Ref [6], Sato et al. (2024) proposed adversarial defense mechanisms in face-based access control. By implementing spoof-prevention techniques and adversarial training on ESP32-CAM, they improved system reliability and resistance to spoofing attacks.
7. In Ref [7], Shivraj Patil, Sangram Gade, and Indrajeet Holkar (2024) developed an IoT-based smart door lock system using Arduino Uno, NodeMCU (ESP32), and a keypad interface. The prototype demonstrated reliable performance, low energy usage, and easy integration into smart home environments.
8. In Ref [8], Dimas Ricky Saputra and Adi Winarno (2024) created a home door security system combining face recognition and keypad-based access. Using ESP32-CAM, Arduino Uno, and Telegram alerts, it performed effectively across the 25–50 cm range under various lighting conditions.

III. METHODOLOGY

The methodology of the project Smart door lock system using IOT and ML proposes on designing low-cost, scalable hybrid authentication system which is scalable and reliable. The approach combines face recognition, keypad pin and a use of IR sensor for anti-spoofing. ESP32-CAM is used as the microcontroller for the project which works on a light weight Convolutional Neural Network (CNN) for quick and accurate facial recognition.

3.1. System Design

The system constitutes of three modules:

- **Authentication Module** - Performs the biometric facial recognition using ESP32-CAM and the keypad based PIN entry.
- **Control module** - In this a relay and solenoid lock are used for physical actuation of the door.
- **IoT Monitoring Module** - It is responsible for data logging , and alert message via mobile application.
- The proposed design ensures flexibility, scalability, cost effectiveness and reliability.

3.2. Hardware Integration

- **ESP32-CAM** : Micro controller with camera and wi-fi support system used for facial recognition and communication.
- **Arduino UNO :** It is a open source microcontroller board based on ATmega328P microcontroller.
- **4 x 4 Keypad** : It provides the pin entry and acts as the mechanism for dual authentic mode.
- **Solenoid lock** : Its controls the physical locking and unlocking mechanism.
- **IR Proximity Sensor** : It validates 3D presence to avoid photo spoofing.
- Power Supply : 5V/12V adapter for ESP32- CAM and solenoid lock.

3.3. Software Implementation

The software workflow is implemented on the Arduino IDE using ESP32 libraries:

- **Face Recognition**: Lightweight CNN-based algorithm on ESP32-CAM to detect and match stored faces.
- **PIN Verification**: Input from the keypad is compared against a stored database of authorized PINs.
- **Hybrid Authentication Logic**: Supports three modes – Face only, PIN only, or Face + PIN.
- **Relay Control**: Relay is triggered by ESP32 to unlock the solenoid lock when authentication is successful.
- **Anti-Spoofing**: IR sensor confirms live presence before authentication proceeds.
- **IoT Communication**: Telegram Bot API enables remote lock/unlock, access log retrieval, and photo alerts for failed attempts.

3.4. Testing Plan

- The system is tested across:
- Lighting Conditions (low, medium, bright).
- Spoofing Attempts (printed photos)
- Internet Variability
- Mode Switching (face, pin, hybrid)
- Performance is measured using accuracy, false acceptance, false rejection and system response time.

3.5. Hardware Tools

ESP32-CAM, 4x4 Keypad, Arduino Lock, Solenoid Lock, IR Sensor, LCD, Voltage Regulator.

a. Arduino Uno

Figure 3.5.a Arduino Uno R3 (source: SparkFun Electronics, Wikimedia Commons, CC BY 2.0).

Parameter	Specification
Digital I/O pins	14 (6 pins for PWM)
Memory	32KB of flash, 2KB SRAM, 1KB EEPROM
Operating Voltage	5Volts
Input Voltage Limit	7-20 Volts
Power Source	DC Power jack and USB port

b. ESP32-CAM

Figure 3.5.b. ESP32-CAM Module (source: Instructables).

Parameter	Description
Module	ESP32 CAM
SPI Flash	32 Mbit
Wi-Fi	802.11 b/g/n
I/O Pins	9
Antenna	Onboard PCB antenna (2 dBi)
Voltage	5 Volts

c. 4X4 Matrix Keypad

Figure 3.5.c. 4×4 Matrix Keypad (source: Amazon product image, REES52 Keypad listing).

Parameter	Specification
Numberof Keys	16 (4 rows × 4 columns)
Operating Voltage	3.3V – 5V DC
Interface	8-pin (4 rows + 4 columns)

d. IR Sensor

Figure 3.5.d. IR Receiver Module (source: SunFounder Wiki, “IR Receiver Module” page)

Parameter	Specification
Operating Voltage	5V DC
Relay Type	Single Pole Double Throw (SPDT)
Control Signal Voltage	3.3V – 5V DC
Indicator LEDs	Power and Status indicators

3.6. Workflow Summary

1. User approaches → IR sensor detects presence.
ESP32-CAM captures face → matches with database.
2. If fails, user enters PIN on keypad.
3. Relay activates lock if authentication succeeds if not an alert is sent.
4. Logs and alerts are sent via mobile application.
5. Unauthorized attempts trigger instant photo capture and alert.

The methodology ensures a reliable, cost-effective, scalable door lock system. By building a hybrid authentication system implying face recognition and keypad as backup, IR based anti-spoofing and mobile application for logins and alerts, the project is a well-designed system and delivers a practical lock solution.

The diagram below shows the integrated flow chart diagram:

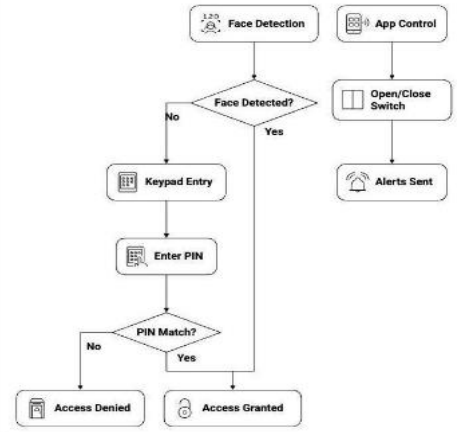

figure 3.6 Flowchart for smart door

IV. RESULTS AND DISCUSSION

The proposed Smart Door Access System involves the use of the microcontroller ESP32-CAM, which comprises Machine Learning algorithms for face recognition and IoT-based remote monitoring . The proposed system architecture consists of three major modules: the Authentication Module, the Control Module, and the IoT Monitoring Module.

The Authentication Module presents user verification through a lightweight CNN model deployed on the ESP32-CAM, which performs real-time face detection and recognition. On failure due to poor lighting conditions or occlusion, authentication via a PIN is allowed using the Keypad Module. Further, an IR proximity sensor provides liveness detection in order to avoid spoofing through photo or video inputs. The Control Module, coupled with a microcontroller, interfaces to a relay and a solenoid lock that are triggered in case of successful authentication. It operates on 5V DC, hence low power consumption, to be in line with compact embedded systems. All of the processing described is managed with Arduino IDE: the authentication logic, image processing, and relay control functions are coded and deployed onto the ESP32-CAM.

The IoT monitoring module will be realized with the mobile application, which allows it to send alerts in real-time, access logs, .Using this integration, users will be able to lock or unlock the door from a distance or receive security notifications right on their mobile phones.

The system constituted from ESP32-CAM,4×4 keypad, relay module, IR sensor, and the solenoid lock are interconnected through jumper connections and powered from a regulated 5V DC power. It worked perfectly under different lighting conditions and network variations, which proved that the system is operationally stable with low latency and high recognition accuracy.

The Hybrid Smart Door Access System provides an efficient security solution through its combination of IoT and Machine Learning technologies which offers reliable and cost-effective protection. The ESP32-CAM microcontroller enables face recognition and PIN authentication and IoT-based remote access to provide multi-level security protection. The system includes an IR-based anti-spoofing system which defends against photo attacks and an alert system using a mobile application.

The system demonstrates excellent performance with fast response times and precise results which makes it appropriate for residential and commercial buildings and healthcare facilities. The system has a flexible design.

ACKNOWLEDGMENT

We want to take a moment to genuinely thank everyone who played a part in helping us complete this project.

To begin with, we are thankful to **ABES Institute of Technology, Ghaziabad** for making this project possible in the first place. The college gave us access to the lab, the components we needed like the ESP32-CAM, Arduino, IR sensors, solenoid lock, and keypad, and the space to work through everything at our own pace. Without that kind of institutional backing, a hands-on project like this would have been very difficult to pull off.

A big thank you to our guide **Ms. Meena Kumari** who never made us feel lost even when we were. She gave her time freely, answered our questions without judgment, and always pointed us in the right direction without doing the work for us, which honestly taught us more than we expected.

The **CSE IoT Department** also deserves credit for keeping the lab open and stocked with the tools and equipment we relied on throughout the building and testing phase.

We did not receive any outside or private funding for this work. Everything was done through college resources and our own efforts as a team.

Lastly, we want to acknowledge the researchers whose earlier work we read and learned from. Their papers shaped how we thought about this problem and helped us build something we are proud of.

REFERENCES

1. **Sonamoni, J. S., et al. (2024).** IoT-Based Smart Remote Door Lock and Monitoring System Using an Android Application. — **DOI:** 10.3390/engproc2024076085. Source: MDPI / Eng. Proc. listing. MDPI+1

2. **Díaz-Delgado, D., et al. (2025).** IoT-Based Smart Lock with Real-Time Person Detection Using YOLOv5 and Mobile App Integration. — **DOI:** 10.51252/rcsi.v5i2.1005. Source: Revista Científica de Sistemas e Informática / journal page. revistas.unsm.edu.pe+1

3. **Obasi, C., & Tahir, K. M. (2025).** A Real-Time Smart Door Access Control System Using Haar Cascade Classifier and Embedded Vision. — Sources: IJDIIC listing / ResearchGate. ijdiic.com+1

4. **Marimuthu, M., Mohanraj, G., Akilandeswari, J., & Sathiyapriya, V. (2025).** Facial Recognition Enabled Smart Security Lock System Using Machine Learning Approach. — **DOI:** 10.4108/eetiot.5657. Source: EAI / EUDL record. EUDL

5. **Susilo, R. A., et al. (2024).** Design and Build a Smart Door Lock Using Face Recognition. — Sources: Atlantis Press proceedings PDF. Atlantis Press+1

6. **Sato, T., et al. (2024).** Adversarial Defences in Face-Based Access Control. — Sources: related adversarial FR literature / ResearchGate / arXiv (search hits). ResearchGate+1

7. **Patil, S., Gade, S., & Holkar, I. (2024).** IoT Based Smart Door Lock System. — Source: IJRPR issue listing. IJRPR

8. **Saputra, D. R., & Winarno, A. (2024).** Home Door Security System with Face Recognition Using ESP32-CAM. — **DOI:** 10.36456/best.vol6.no2.9588. Source: Best: Journal of Applied Electrical, Science and Technology (journal page). Jurnal Unipasby+1