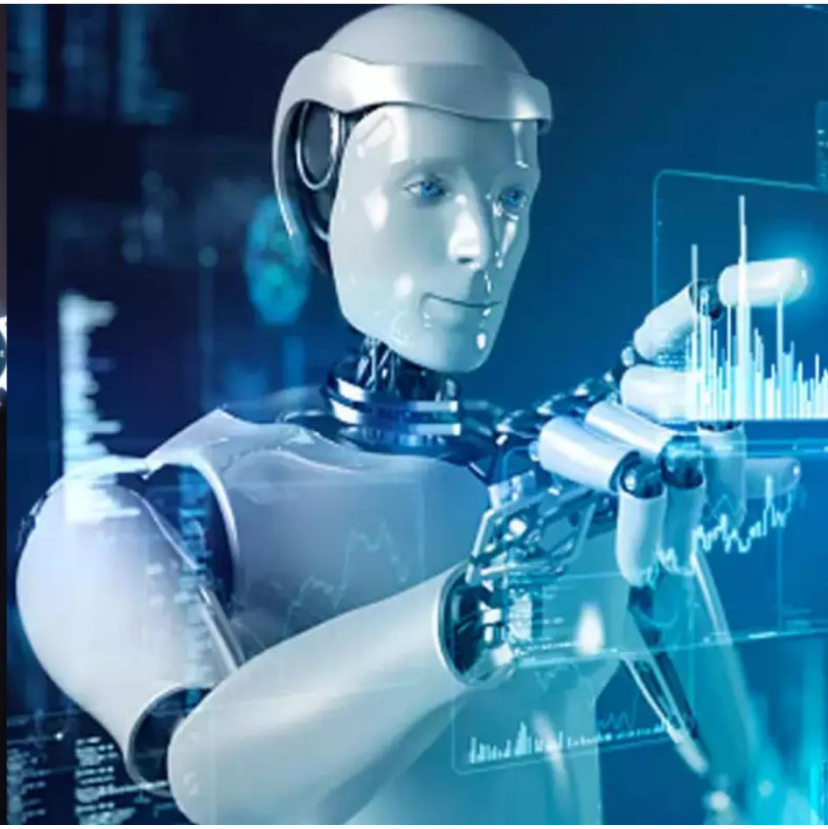
IJIRSET
International Journal of Innovative Research in Science | Engineering | Technology

ISSN(O): 2319-8753
ISSN(P): 2347-6710

International Journal of Innovative Research in Science Engineering and Technology (IJIRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.699

Volume 14, Issue 4, April 2025

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 4, April 2025

|DOI: 10.15680/IJIRSET.2025.1404530|

IoT Operated Door Control System

Prof. Pravin Thosare[1], Kalyani Bhaskar[2], Om Kokate[3], Rohini Yeole[4], Pravish Sadafale[5]

Department of Electronics & Telecommunication Engineering, Prof. Ram Meghe Institute of Technology and Research, Maharashtra, India[1-5]

ABSTRACT: This research presents the development of a cost-efficient, programmable smart door access and home security system. The system utilizes ESP32-CAM, fingerprint sensor, 4x3 keypad, HC-SR501 motion sensor, solenoid latch, and a 16x2 LCD display for seamless security management. Integrated with Arduino IDE, the ESP32-CAM captures intruder images and communicates real-time alerts to smartphones via the Telegram app using a Wi-Fi module. The inclusion of a buzzer and servo motor enhances system functionality by providing audible alarms and automated locking mechanisms. Unified Modelling Language (UML) models the system workflow, while a battery with USB-C BMS ensures consistent power supply. Comprehensive testing validated system efficiency, image recognition accuracy, and operational reliability.

KEYWORDS: ESP32-CAM, fingerprint sensor, motion sensor, solenoid latch, Wi-Fi module, Arduino IDE, Telegram, smart security.

I. INTRODUCTION

Security has been a fundamental concern for humanity since ancient times. Early door locks, dating back to 4000 B.C. in Egypt, Greece, and Iraq, used basic pin mechanisms to restrict access unless a matching key was used. Over time, traditional deadlock systems became common, requiring people to carry physical keys. However, this approach posed challenges such as lost keys, broken locks, and the inconvenience of carrying keys constantly. With advancements in technology, smarter and more reliable solutions have emerged to enhance security.

In today's world, securing homes and properties is crucial, given the increasing complexity of threats. While various techniques and systems exist, many fail to balance user convenience with robust security. IoT-based systems have revolutionized this domain by offering remote control and real-time monitoring capabilities. However, some existing systems, particularly those relying solely on mobile apps, are vulnerable to misuse and security breaches.

Motivated by these challenges, this research aims to design a smart door access system that integrates biometric authentication, motion detection, and cloud-based security features to create a reliable and efficient solution. The system utilizes a combination of IoT devices, including ESP32-CAM, fingerprint sensors, a 4x4 keypad, solenoid latch and Wi-Fi connectivity, to ensure only authorized users gain access. Additionally, the system enhances security by employing mobile-specific IMEI verification alongside biometric authentication to mitigate vulnerabilities associated with app-only systems.

This paper introduces a Wi-Fi-enabled door access system that captures intruder images, sends real-time notifications via the Telegram app, and integrates seamless automation features. Section II reviews related works, Section III outlines the system architecture, and Sections IV and V focus on implementation, evaluation, and security considerations. Finally, Section VI concludes the study with insights into future developments.

II. LITERATURE REVIEW

In Internet of Things: Principles and Paradigms, Rajkumar Buyya and Amir Vahid Dastjerdi provide a comprehensive overview of IoT technologies, architectures, and applications, covering essential aspects such as cloud and edge computing integration, security challenges, data analytics, and real-world IoT deployments. The authors emphasize the role of IoT in smart cities, healthcare, and industrial automation, presenting a multidisciplinary approach to the field. With contributions from experts, the book serves as a valuable resource for researchers, professionals, and students looking to understand IoT's evolving landscape and its future potential.[1]

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 4, April 2025

|DOI: 10.15680/IJIRSET.2025.1404530|

In "Door Automation System Using Bluetooth-Based Android for Mobile Phone," L. Kamelia, A. Noorhassan S.R, M. Sanjaya, and W. Mulyana present a smart door automation system that utilizes Bluetooth communication via an Android mobile phone. The study explores the design and implementation of a secure and efficient access control system, eliminating the need for traditional keys. The authors highlight the system's effectiveness in enhancing security, ease of use, and automation, making it a practical solution for residential and commercial applications. Published in the ARPN Journal of Engineering and Applied Sciences, the research contributes to the growing field of smart home technology.[2]

In "A Sixth Sense Door using Internet of Things," J. Britto, V. Chaudhari, D. Mehta, A. Kale, and J. Ramteke present an advanced smart door system that leverages IoT technology to enhance security and automation. The study discusses the integration of sensors, cloud computing, and real-time monitoring to enable seamless and intelligent access control. The authors emphasize the system's ability to detect and authenticate users, providing a hands-free and secure entry mechanism. Published in the International Conference on Computer Networks and Communication Technologies Lecture Notes on Data Engineering and Communications Technologies, this research contributes to the evolution of smart home and security systems.[3]

C. G. Sarika, A. B. Malakreddy, and H. N. Harinath (2018) discuss an IoT-based smart login system utilizing biometrics for enhanced security. Their study explores how biometric authentication, integrated with IoT, improves access control by offering a secure and efficient login mechanism. The paper highlights advantages such as reduced reliance on passwords and increased protection against unauthorized access, while also addressing challenges like data security and system reliability. This research contributes to the growing field of biometric-based smart security solutions.[4]

K. Loong Pang and H. Seng Teh (2019) present a mobile-based access control system that leverages smartphones for secure authentication. Their study emphasizes the convenience and security of mobile access, reducing the need for physical keys or cards. The paper highlights key features such as remote access, real-time monitoring, and encrypted authentication while addressing potential challenges like connectivity issues and cybersecurity threats. This research contributes to the advancement of mobile-driven security solutions in modern access control systems.[5]

A. Kassem, S. E. Murr, G. Jamous, E. Saad, and M. Geagea (2016) introduce a smart lock system utilizing Wi-Fi security for enhanced access control. Their study focuses on integrating Wi-Fi technology with smart locks to enable remote operation and monitoring, improving security and user convenience. The paper discusses the benefits of wireless connectivity, such as ease of installation and real-time updates, while addressing potential concerns regarding network security and reliability. This research contributes to the development of Wi-Fi-enabled smart lock systems for modern security applications.[6]

M. S. Hadis, E. Palantei, A. A. Ilham, and A. Hendra (2018) present a design for a smart lock system for doors utilizing Bluetooth technology. Their study emphasizes the integration of Bluetooth for secure, wireless access control, providing features such as keyless entry and user authentication through mobile devices. The paper highlights advantages like low energy consumption, ease of use, and seamless connectivity, while also discussing potential challenges such as range limitations and security concerns. This research contributes to the development of Bluetooth-based solutions in smart lock technology.[7]

III. PROBLEM STATEMENT

1. Security Concerns in Traditional Locks
- Physical keys can be lost, stolen, or duplicated.
- Mechanical locks are prone to wear and tear, leading to security risks.

2. Limitations of Existing IoT-Based Solutions
- Many rely solely on mobile apps, making them vulnerable to hacking and unauthorized access.
- Lack of multi-layer authentication increases the risk of breaches.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 4, April 2025

|DOI: 10.15680/IJIRSET.2025.1404530|

3. User Inconvenience
- Remembering and managing passwords or PINs can be difficult.
- Dependence on mobile apps alone may pose accessibility challenges if the phone is lost or battery-depleted.

4. Lack of Real-Time Monitoring & Alerts
- Many systems do not provide immediate notifications or visual evidence of intrusions.
- No integration with cloud-based storage for security logs and alerts.

5. Proposed Solution
Biometric Authentication: Ensures only authorized users can access the door.
- Motion Detection & ESP32-CAM: Captures intruder images and enhances security.
- Telegram App Integration: Sends instant notifications and captured images to users for immediate action.

IV. SYSTEM MODEL AND ASSUMPTIONS

1. Hardware Components
ESP32-CAM: A low-power, Wi-Fi-enabled microcontroller that supports camera functionality. It captures images of users or intruders and sends them via the Telegram bot for monitoring.
Arduino Microcontroller: Acts as the central control unit, handling authentication processes, processing user input, and triggering the door lock mechanism. It interfaces with the keypad, fingerprint sensor, and solenoid lock.

1.2 Sensors
Fingerprint Sensor: This biometric sensor captures and verifies fingerprints. It ensures that only registered users can gain access, adding an extra layer of security beyond PIN or mobile app access.

1.3 Locking Mechanism
Solenoid Lock: This electronic locking device controls the door's locking and unlocking. It operates on 12V DC and gets activated when the system validates the user's credentials.

1.4 Connectivity Module
Wi-Fi Module (Built-in ESP32-CAM): Enables communication between the system and the Telegram bot, allowing remote access and real-time notifications.

1.5 Power Supply
Battery (9V or 12V): Provides power to the system, ensuring functionality even during power outages.
Voltage Regulators: Convert the power supply into appropriate voltage levels (e.g., 5V for microcontrollers and 12V for the solenoid lock) to prevent damage to components.

1.6 Keypad
4x4 Keypad: A tactile input device used for password authentication. Users enter a predefined PIN to unlock the door, serving as an alternative to fingerprint or mobile access.

2. Software Components
2.1 Mobile Application & Web Interface
The system integrates a Telegram Bot to allow users to control the door remotely.
Features of the Telegram Bot:
Start & Stop Function: Activates or deactivates the camera.
Flash Control: Turns the ESP32-CAM's flashlight ON/OFF for better image capture.
Live Image Capture: Sends images of the person at the door to the owner for verification.

2.2 Authentication Methods
The system supports three authentication techniques to enhance security:
Telegram Access – Users can unlock the door remotely via the Telegram bot.
Keypad Access – Users enter a predefined PIN on the 4x4 keypad for authentication.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 4, April 2025

|DOI: 10.15680/IJIRSET.2025.1404530|

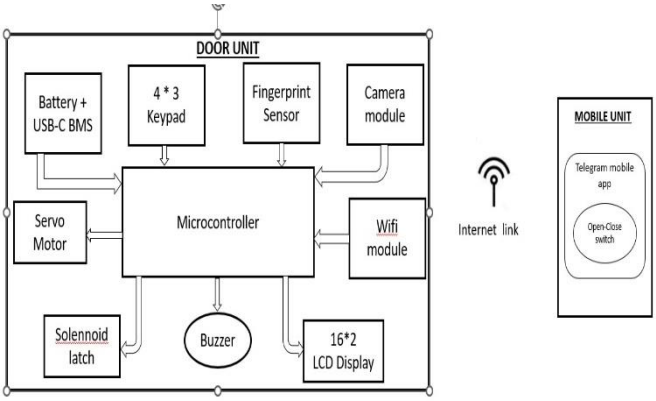


Figure. 1.1 Block Diagram

Fingerprint Access – Users scan their fingerprint, which is verified against stored data before granting access.

Working :

The IoT-based smart door access system is designed to provide secure and convenient entry using multiple authentication methods, including password-based, fingerprint-based, and Telegram-based access. The system integrates various hardware components such as the ESP32-CAM, ATMega 328P, fingerprint sensor R307S, solenoid lock, and a 4x4 keypad. The software component leverages a Telegram bot to facilitate remote control and real-time monitoring.

1. System Design and Power Distribution

The circuit operates on a 9V battery, which powers different components of the system.

Voltage regulators are used to supply 5V for logic circuits and 12V for the solenoid lock to ensure stable operation.

2. Authentication Methods

The system offers three authentication mechanisms to enhance security and usability:

A. Keypad and Password-Based Access

A 4x4 matrix keypad is used for password input.

The keypad is connected to the ATMega 328P microcontroller, which detects the sequence of key presses.

If the entered password matches the predefined password stored in the microcontroller, it triggers a relay, which activates the solenoid lock to unlock the door.

B. Fingerprint-Based Access

The system includes a R307S fingerprint sensor, which has an embedded STM32 microcontroller for storing and processing fingerprint data.

The fingerprint sensor communicates with the ATMega 328P to verify whether the scanned fingerprint matches the stored database.

If a match is found, the system triggers the relay, unlocking the solenoid lock and allowing access.

C. Camera and Telegram-Based Access

The ESP32-CAM module connects to a Wi-fi network and interacts with a Telegram bot for remote access control.

When a door access request is received via Telegram, the ESP32-CAM captures a photo of the individual attempting to open the door.

The captured image is transmitted via Telegram to the owner for verification.

Based on the owner's response, the ESP32 processes the command to open or close the door remotely.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 4, April 2025

|DOI: 10.15680/IJIRSET.2025.1404530|

3. Validation and Access Control
The system continuously monitors user input from the keypad, fingerprint sensor, and Telegram bot.
If a valid authentication method is detected, the relay module is activated to unlock the solenoid latch.
If an incorrect password or unregistered fingerprint is detected, access is denied, and the system remains locked.

4. Security Features and Intrusion Detection
The fingerprint sensor provides biometric security, reducing unauthorized access risks.
The ESP32-CAM module enhances security by capturing images of unauthorized individuals attempting access.
The system enables real-time monitoring via Telegram, allowing the owner to control the door remotely.

5. Implementation and Integration
The entire system is programmed using Embedded C for microcontroller operations.
The ESP32-CAM is programmed to interact with Telegram API for real-time notifications.
The fingerprint sensor and keypad are calibrated to store and retrieve authentication data efficiently.
This methodology ensures a secure, convenient, and remotely accessible smart door system that integrates multiple authentication techniques to enhance security and user convenience.

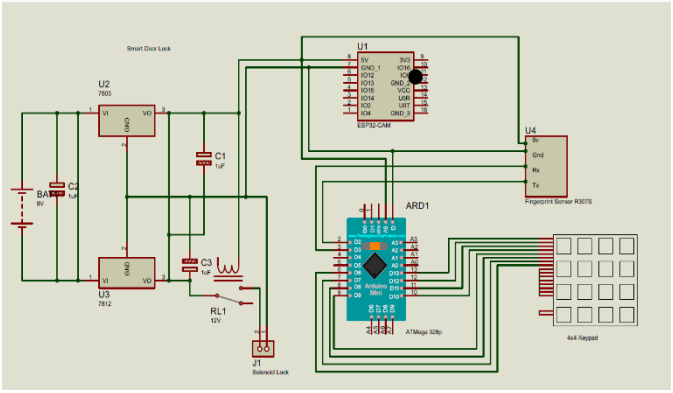


Figure. 1.2 Circuit Diagram

V. EXPECTED OUTCOMES

Bluetooth Action	Fingerprint Status	Motion Sensor	Door Condition	LCD Notification
Open	Verified	No Motion	Door Opens	"Access Granted. Door is Unlocked."
Open	Not Recognized	No Motion	Stays Closed	"Access Denied. Try Again!"
Open	Verified	Motion Detected	Door Opens	"Access Granted. Door is Unlocked."
Close	X	X	Door Closes	"Door is Now Locked."
X	X	Motion Detected	Stays Closed	"Alert: Unauthorized Movement!"
Open	Verified	X	Door Opens	"Access Granted. Door is Unlocked."
Close	X	No Motion	Door Closes	"Door Locked. No Activity Detected."

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 4, April 2025

|DOI: 10.15680/IJIRSET.2025.1404530|

Bluetooth Action:
Represents the command given via Bluetooth to either open or close the door.
If no Bluetooth command is given, it is marked as "X" (No action).

Fingerprint Status:Identifies whether the scanned fingerprint is valid (recognized) or invalid (not recognized).
If fingerprint authentication is not required in certain cases, it is marked as "X".

Motion Sensor:
Detects movement near the door.
If motion is detected, security measures may prevent unauthorized access.
If motion sensing is not relevant for a particular action, it is marked as "X".

Door Condition:
Describes whether the door opens or remains closed based on the input conditions.
If a close command is received, the door locks.

LCD Notification:
Displays appropriate messages on the LCD based on different conditions.
Messages include:
"Access Granted. Door is Unlocked." – When authentication is successful.
"Access Denied. Try Again!" – When an unrecognized fingerprint is scanned.
"Door is Now Locked." – When the door is successfully closed.
"Alert: Unauthorized Movement!" – When movement is detected without proper access credentials.
"Door Locked. No Activity Detected." – When the door is closed and no motion is present.

VI. ADVANTAGES AND DISADVANTAGES

Advantages

1. **Remote Access:**
   - The system allows users to control the door lock from anywhere using their smartphone or a connected platform like Telegram.
   - Users can lock/unlock the door without being physically present, improving convenience for deliveries, visitors, or emergencies.
2. **Fingerprint Access:**
   - Enhances security by requiring biometric authentication.
   - A fingerprint sensor ensures that only authorized individuals can gain access, making it more secure than traditional locks.
3. **Password Access:**
   - Provides an additional or alternative method for accessing the system via a keypad.
   - Useful for situations where fingerprint access is unavailable or in case of multiple users who do not share fingerprints.
4. **Low Cost:**
   - The system is built using affordable and readily available components like the Arduino Mini, ESP32-CAM, and R307 fingerprint sensor.
   - This makes it an economical alternative to commercial smart locks.
5. **Integration with Telegram:**
   - The system can send notifications or alerts via Telegram, a widely-used messaging app.
   - Allows the owner to monitor access events in real-time, such as when the lock is opened or tampered with.
6. **Customizable:**
   - The system's modular design allows users to add or modify features.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 4, April 2025

|DOI: 10.15680/IJIRSET.2025.1404530|

7. **User-Friendly**

Disadvantages

1. **Wi-Fi Dependency:**
   - Requires a stable Wi-Fi connection for features like remote access, Telegram notifications, or ESP32-CAM functionalities.
   - If the internet is down, remote monitoring and control features will not work.
2. **Telegram Bot Security Risks:**
   Malicious users could gain access or manipulate the system through the bot.
3. **Fingerprint Sensor Limitations:**
   - The R307 fingerprint sensor might face issues such as:
     - Difficulty recognizing wet or dirty fingerprints.
     - A limited number of fingerprints that can be stored.
4. **Complexity in Setup:**
   - The installation and configuration of the system can be challenging for non-technical users.
   - Involves wiring multiple components (e.g., relays, fingerprint sensor, keypad) and programming the microcontroller, requiring expertise in electronics and coding

VII. FUTURE WORK

- **Integration with Mobile App**
  A dedicated sma rtphone app could replace Telegram for more secure and intuitive control, including logs and push notifications.
- **Access Logging and Analytics**
  Add SD card, EEPROM, or cloud-based logging to track user access, failed attempts, and door usage history.
- **Battery Backup System**
  Include a rechargeable battery or UPS to allow operation during power outages.
- **Facial Recognition Unlock**
  Enhance ESP32-CAM features with face recognition for hands-free and secure access.
- **Voice Assistant Integration**
  Integrate with Google Assistant or Amazon Alexa for voice-controlled door access.
- **RFID or NFC Access Option**
  Add RFID cards or N.FC-based unlocking as another convenient, contactless method.
- **Auto-Learn & Schedule Locking**
  Smart scheduling or AI-based pattern detection could auto-lock/unlock the door based on time or user behavior.
- **Tamper Detection and Alerts**
  Add sensors to detect forceful entry or tampering, and instantly alert the user through Telegram or email.

VIII. CONCLUSION

IoT-operated door lock systems signify a major step forward in modern security solutions, offering an innovative combination of convenience, efficiency, and safety. Features such as remote access, biometric authentication, real-time notifications, and integration with smart home ecosystems make these locks highly practical and appealing for residential and commercial use. They empower users with better control over access to their premises, enhancing peace of mind.

Despite their benefits, challenges like dependence on internet connectivity, potential cybersecurity vulnerabilities, and technical complexities in setup and maintenance must be addressed. With continuous advancements in IoT technology, such as improved encryption, cloud-based storage, and compatibility with other smart systems, these locks will only become more robust and secure.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 4, April 2025

|DOI: 10.15680/IJIRSET.2025.1404530|

IoT-operated door locks are a promising solution for smarter and safer living environments. By addressing current limitations and leveraging emerging technologies, they are set to play a vital role in the future of home and office security systems.

REFERENCES

[1]. Burns et al. has proposed a RFID controlled door lock . where the door lock is controlled with an exterior RFID card input.
[2]. Pang et al. has patented on Bluetooth and Biometric feature based Access Control System. They have proposed that the door will be unlocked using the biometric features as an authentication media and setting a Bluetooth communication link between app and the controller.
[3]. Kassem et al. has proposed a smart door lock providing security via WiFi . The system has been implemented by generating digital keys on user's phone which is used as the authentication method for validating the legitimate user's identity.
[4]. Hadis et al. has proposed a smart door lock system using IoT where the door will be unlocked automatically if the user's phone has reached within the Bluetooth range.
[5]. Thakur et al. has proposed a door lock system which is controlled using biometric or facial recognition via mobile application using WiFi or Bluetooth as the communication link.
[6].Door Lock System Using ESP32-CAM, O. Reddy Raghavendra, B. Dharan
[7].Fingerprint Door Lock Using Arduino, Md. Khayrul Islam, Alimul Rajee
[8]. Fingerprint Door Lock System Using Arduino, Sharmin Yasmin
[9].Door Locking Using Keypad and Arduino, Annmary Vadakkan, Athulya Babu V. K., Christy Pappachan, Prof. Ani Sunny
[10]. IoT-Based Smart Door Lock System Using Arduino, Arnab Debnath, Saswata Samanta, Poulami Das
[11].IoT-Based Smart Door Lock System with Fingerprint and Keypad Access, Ketut Ananta Kevin Permana, I Nyoman Piarsa, Anak Agung Ketut Agung Cahyawan Wiranatha
[12].Smart Door Lock System Using ESP32-CAM (IoT-Based), Yashaswi R., Abdulwahab Ahmed Mohamed Omer, Nikhil Reji, Muhammed Mishal, Nagaraja P. S.
[13]. ESP32-CAM Face Detection Door Lock, Namrata Singh, Dr. Ramveer Singh, Ranjan Kumar, Shivam Paliwal, Shipra Srivastava

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details