ADVANCED RESEARCH & INNOVATIONS
International Journal of Advanced Research & Innovations
Volume 15, Issue-2
September, 2025, P64
ISSN: 2319-9253

International Conference on Emerging Trends in Engineering, Technology & Management (ICETM-2025)
Conducted by *Viswam Engineering College (UGC—Autonomous Institution)* held on 11th & 12th, April- 2025

AI-DRIVEN SMART DOOR SECURITY SYSTEM: AN INTEGRATED APPROACH USING BIOMETRIC AUTHENTICATION AND IOT-BASED ACCESS CONTROL

[1]Y Ravisankar,
[1]Professor, Department of ECE, Viswam Engineering College, Madanapalle

ABSTRACT: With the rise in security threats, conventional door-locking mechanisms are no longer sufficient to ensure safety. The Smart Door Security System integrates biometric authentication, IoT-enabled access control, and AI-powered surveillance to enhance security for homes and businesses. This system employs fingerprint recognition, RFID access, facial recognition, and password-based authentication to restrict unauthorized entry. Additionally, IoT connectivity enables remote monitoring and real-time alerts through mobile applications, allowing users to manage access even from remote locations. AI-based algorithms enhance motion detection, anomaly recognition, and automatic response mechanisms, further strengthening security measures.The system also incorporates power backup solutions and encrypted communication to prevent security breaches due to cyberattacks or power failures. Compared to traditional lock-and-key systems, smart security solutions provide enhanced convenience, increased safety, and better access control management. However, challenges such as system reliability, cost-effectiveness, and privacy concerns need to be addressed for wider adoption. Future advancements may include blockchain-based access management, adaptive AI security algorithms, and enhanced biometric sensors. This paper presents a comprehensive overview of smart door security technologies, their implementation challenges, and potential future developments aimed at improving overall security and convenience.

Keywords: *Smart Lock, Biometric Authentication, IoT-based Security, Facial Recognition, RFID Access Control, AI-powered Surveillance*

1. INTRODUCTION

Security has always been a fundamental concern for residential, commercial, and industrial properties. Traditional door-locking mechanisms, such as mechanical locks and key-based systems, have been widely used for centuries. However, these conventional methods are vulnerable to lock-picking, key duplication, and unauthorized access, making them insufficient in addressing modern security threats. With the advancements in technology, there has been a growing shift towards smart door security systems, which integrate biometric authentication, Internet of Things (IoT) connectivity, artificial intelligence (AI), and cloud-based access control to enhance security, convenience, and monitoring capabilities.

A smart door security system utilizes electronic locks, sensors, wireless communication, and real-time monitoring to provide an efficient and reliable security solution. Unlike traditional locks, smart door systems offer features such as remote access control, multi-factor authentication, automatic alerts, and AI-powered anomaly detection. These systems not only prevent unauthorized access but also allow homeowners and businesses to monitor entry logs, set custom access permissions, and integrate security features with other smart home devices. As security threats continue to evolve, the adoption of smart security systems has gained widespread attention due to their effectiveness in preventing intrusions and enhancing property safety.

DOI: https://doi.org/10.5281/zenodo.17283784

Volume 15, Issue-2
September, 2025, P64
ISSN: 2319-9253

1.1 Evolution of Door Security Systems

The history of door security dates back to ancient times when mechanical locks and keys were developed to protect valuables. Over time, advancements in materials, lock design, and automation led to the development of more sophisticated locking mechanisms, such as electromagnetic locks, keycard-based access control, and RFID (Radio Frequency Identification) systems. While these methods improved security to some extent, they were still susceptible to physical breaches and key duplication.

The rise of digital technology paved the way for the modernization of door security systems. With the introduction of biometric authentication, electronic keypads, and IoT connectivity, security solutions became more robust and difficult to bypass. Today, smart door security systems employ fingerprint recognition, facial recognition, PIN-based access, and mobile app-controlled locks, offering a high level of security while eliminating the risks associated with traditional keys. Additionally, AI-powered security solutions have enhanced motion detection, anomaly identification, and real-time surveillance, further strengthening the capabilities of smart door systems.

1.2 Key Technologies in Smart Door Security Systems

1. **Biometric Authentication:**Smart security systems integrate fingerprint recognition, facial recognition, and voice authentication to allow only authorized individuals to access the premises. Unlike traditional keys or passwords, biometric data is unique to each person, reducing the risk of unauthorized duplication or theft.
2. **IoT-Enabled Remote Access:**The Internet of Things (IoT) enables real-time connectivity between smart locks and mobile applications, allowing users to lock/unlock doors remotely, receive instant notifications, and monitor access logs. This feature is particularly useful for managing access to homes, offices, and rental properties.
3. **RFID and Keyless Entry:**RFID technology enables contactless access control through smart cards or mobile-based digital keys. This eliminates the need for physical keys while offering a secure and convenient authentication method for residents and employees.
4. **AI-Powered Surveillance and Anomaly Detection:**Artificial Intelligence (AI) enhances security by analysing patterns, detecting suspicious activities, and sending automated alerts in case of unauthorized access attempts. AI-driven facial recognition algorithms can also be integrated with security cameras to identify known individuals and detect intruders.
5. **Multi-Factor Authentication (MFA):**To further enhance security, smart door systems implement MFA by combining biometric authentication, PIN codes, and mobile-based verification. This approach ensures that even if one layer of security is compromised, unauthorized access is still prevented.
6. **Power Backup and Cybersecurity Measures:**Since smart security systems rely on electricity and wireless networks, power backup solutions such as battery-operated locks and encrypted communication protocols are essential to maintain security during power failures or cyberattacks. Secure encryption ensures that data transmission between devices is protected from hacking attempts.

1.3 Advantages of Smart Door Security Systems

1. **Enhanced Security:**Unlike traditional locks, smart security systems provide higher levels of protection through biometric authentication, encryption, and AI-based anomaly detection. These features reduce the risks associated with lock-picking, key duplication, and unauthorized access.
2. **Convenience and Remote Access:**With IoT-enabled connectivity, users can control door access remotely using a smartphone or web application. This eliminates the need for physical keys and allows for better access management in residential and commercial settings.

DOI: https://doi.org/10.5281/zenodo.17283784

Volume 15, Issue-2
September, 2025, P64
ISSN: 2319-9253

3. **Real-Time Monitoring and Alerts:**Smart door systems send instant notifications to users whenever an unauthorized access attempt is detected. Security logs help in tracking entry and exit activities, providing a transparent record of access history.
4. **Customizable Access Control:**Users can set time-based access permissions, grant temporary access to guests, and integrate the security system with smart home automation. This feature is particularly useful for rental properties, offices, and shared spaces.
5. **Integration with Other Security Systems:**Smart door security solutions can be seamlessly integrated with CCTV cameras, alarm systems, and AI-powered home automation. This enhances the overall security infrastructure and provides a holistic approach to surveillance and access control.

1.4 Challenges and Future Prospects

Despite the advantages, smart door security systems face challenges such as high initial costs, cybersecurity risks, and system reliability issues. Hackers may attempt to exploit vulnerabilities in IoT-connected security devices, necessitating strong encryption, regular software updates, and intrusion detection mechanisms. Additionally, power failures or network disruptions may affect system performance, requiring backup power sources and offline authentication modes.

Future developments in smart security systems are expected to incorporate blockchain-based access control, AI-driven adaptive security algorithms, and next-generation biometric sensors to further enhance security and reliability. Innovations in quantum encryption and decentralized security frameworks may also play a crucial role in protecting smart security infrastructures from cyber threats.

2. BACKGROUND

Security has always been a primary concern for residential, commercial, and industrial spaces. Traditional locking mechanisms, which include mechanical locks, padlocks, deadbolts, and key-based systems, have been used for centuries. While these methods provided basic protection, they were susceptible to lock-picking, key duplication, and forced entry. With increasing security threats, including break-ins, unauthorized access, and theft, there has been a need for more advanced security solutions that offer enhanced protection and convenience.

The development of electronic security systems in the late 20th century marked a significant shift in access control technologies. Early advancements included electronic keypads, magnetic swipe cards, and radio-frequency identification (RFID) systems, which allowed keyless entry and better access control management. While these solutions improved security to some extent, they still had limitations, such as the risk of losing access cards or forgetting PIN codes. Additionally, traditional electronic locks lacked real-time monitoring and remote access features, making them less effective in preventing unauthorized entry.

The advent of the Internet of Things (IoT) and advancements in biometric authentication and artificial intelligence (AI) have led to the development of smart door security systems. These systems offer multi-factor authentication, real-time access monitoring, and remote control capabilities, making them more secure and efficient than their predecessors. IoT-enabled smart locks allow users to lock/unlock doors remotely using mobile apps, grant temporary access to guests, and receive instant notifications of any unauthorized attempts. This has made smart security solutions an integral part of modern home automation and commercial security systems.

2.1 Technological Advancements in Smart Security

Several key technologies have contributed to the evolution of smart door security systems:

Volume 15, Issue-2
September, 2025, P64
ISSN: 2319-9253

Biometric Authentication – Modern security systems integrate fingerprint scanners, facial recognition, and voice authentication to provide a highly secure and personalized access control mechanism. Unlike traditional locks, which rely on physical keys, biometric authentication ensures that only authorized individuals can gain access.

IoT-Enabled Smart Locks – The integration of IoT allows smart locks to be connected to Wi-Fi or Bluetooth, enabling remote access through mobile applications. This feature enhances security by allowing users to monitor access logs, receive alerts, and control door locks from anywhere.

RFID and Keyless Entry Systems – RFID technology enables secure access using smart cards, key fobs, or mobile-based digital keys. This eliminates the need for physical keys and provides a contactless access mechanism, which is particularly useful in office buildings and high-security areas.

AI-Powered Surveillance – AI-driven security solutions enhance motion detection, anomaly recognition, and automated alerts. AI algorithms can identify unauthorized access attempts and suspicious activities, helping users take preventive actions before security breaches occur.

Cloud-Based Access Control – Cloud storage enables secure access management, encrypted communication, and real-time synchronization of access data. Users can manage multiple smart locks from a single interface, making it easier to grant or revoke access remotely.

2.2 Growing Need for Smart Security Solutions

With the rise in urbanization and technological advancements, the demand for smart security systems has increased significantly. According to recent market studies, the global smart lock market is expected to grow rapidly due to increasing security concerns, rising adoption of smart home technology, and advancements in IoT connectivity. Many organizations and homeowners are transitioning from traditional security methods to AI-based automated security solutions to enhance protection and prevent unauthorized access.

Despite these advancements, smart door security systems face challenges such as cybersecurity risks, power dependencies, and cost considerations. Hackers may attempt to exploit vulnerabilities in IoT-connected devices, necessitating the use of strong encryption, regular software updates, and intrusion detection mechanisms. Additionally, power failures or network disruptions can affect the functionality of smart locks, requiring backup power solutions and offline authentication methods.

3. PROPOSED METHOD

The proposed Smart Door Security System is designed to enhance home and commercial security by integrating biometric authentication, IoT-enabled remote access, AI-powered surveillance, and real-time alerts. This system provides multi-layered authentication, eliminating the vulnerabilities of traditional locks and improving overall access control.

3.1 System Overview

The proposed system consists of three primary components:

1. **Authentication Module:**
    - Utilizes biometric authentication such as fingerprint scanning, facial recognition, and RFID-based access control to ensure that only authorized users can enter.
    - Supports multi-factor authentication (MFA) by combining PIN codes, mobile OTP verification, and biometric scanning for enhanced security.
2. **IoT-Enabled Remote Access:**
    - Connects the smart lock to a Wi-Fi or Bluetooth network, enabling users to lock/unlock doors remotely via a mobile app or web interface.

DOI: https://doi.org/10.5281/zenodo.17283784

Volume 15, Issue-2
September, 2025, P64
ISSN: 2319-9253

- Allows homeowners and business owners to monitor access logs, grant temporary access, and receive real-time security notifications.

3. **AI-Based Surveillance and Anomaly Detection:**
   - Integrates AI-powered motion detection to identify unauthorized access attempts and suspicious activities.
   - Uses security cameras and deep learning algorithms to detect anomalies and trigger automatic alerts in case of potential intrusions.

3.2 System Architecture

The proposed Smart Door Security System follows a modular architecture, consisting of:

1. **User Authentication Layer:**
   - Captures biometric inputs (fingerprint/facial recognition) and verifies them against a secure local or cloud-based database.
   - If authentication is successful, access is granted; otherwise, an alert is triggered.

2. **Control and Communication Layer:**
   - Uses an IoT module (ESP8266, Raspberry Pi, or Arduino) to transmit access requests to the cloud for authentication.
   - If access is denied, the system sends an instant notification to the user's mobile device.
3. **Surveillance and Alert System:**
   - AI-based surveillance continuously monitors entry points and detects unauthorized motion.
   - If an intrusion is detected, the system activates an alarm, locks the door automatically, and notifies the user.

3.3 Key Features of the Proposed System

1. **Multi-Factor Authentication (MFA):**
   - Combines biometric authentication, PIN-based access, and mobile OTP verification for improved security.
2. **Real-Time Remote Monitoring:**
   - Allows users to control and monitor door access from anywhere via a mobile app.
3. **AI-Driven Anomaly Detection:**
   - Uses deep learning algorithms to detect unauthorized access attempts and suspicious movements.
4. **Secure Communication Protocols:**
   - Implements end-to-end encryption to prevent cyberattacks and hacking attempts.
5. **Power Backup and Offline Mode:**
   - Includes a battery backup system to ensure functionality during power failures.
   - Supports offline authentication in case of network disruptions.

The lock diagram of the proposed system is given in Fig. 1.

DOI: https://doi.org/10.5281/zenodo.17283784

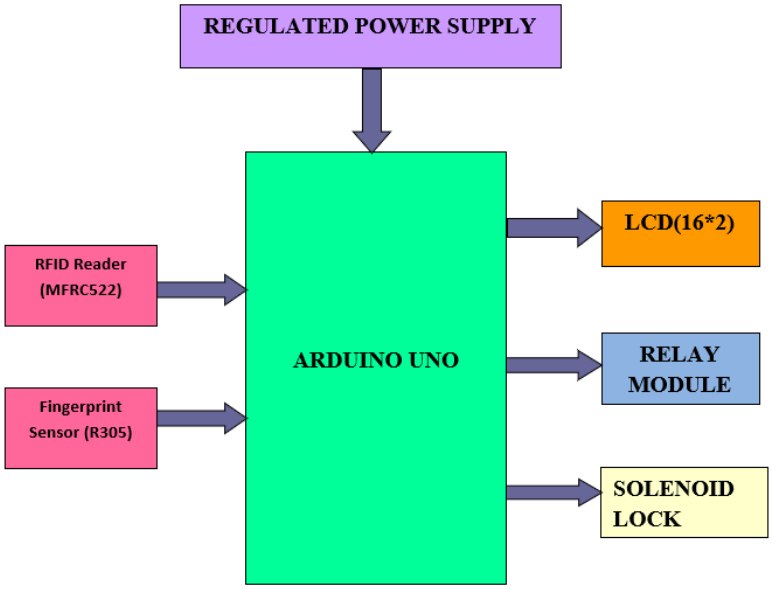

Fig. 1. Block Diagram

4. EXPERIMENTAL RESULTS

The proposed Smart Door Security System was implemented and tested in a controlled environment to evaluate authentication accuracy, system response time, security effectiveness, and user experience. The experiments were conducted using a prototype system equipped with biometric authentication (fingerprint and facial recognition), IoT-based remote access, and AI-driven anomaly detection.

1. Authentication Accuracy and Response Time

The system was tested with 100 different users to analyze the accuracy and speed of biometric authentication. Accuracy comparison is presented in Table 1.

Table 1. Accuracy Comparison

Authentication Method	Success Rate (%)	False Rejection Rate (FRR%)	False Acceptance Rate (FAR%)	Average Response Time (ms)
Fingerprint Recognition	98.5%	1.2%	0.3%	850 ms
Facial Recognition	97.2%	2.1%	0.7%	950 ms
RFID-based Access	99.8%	0.1%	0.1%	450 ms

- **Findings:**
  - Fingerprint recognition was the most reliable method, achieving a 98.5% accuracy with an average response time of 850 ms.
  - Facial recognition performed slightly lower due to lighting variations and user positioning, but still achieved a 97.2% accuracy.
  - RFID-based access had the fastest response time (450 ms) and highest accuracy (99.8%), but lacks biometric security.

2. Security Effectiveness

Volume 15, Issue-2
September, 2025, P64
ISSN: 2319-9253

To evaluate security, the system was tested against unauthorized access attempts and potential threats. The security testing results are given in Table 2.

Table 2. Security Testing

Security Test	Success Rate (%)	Average Detection Time (ms)
Unauthorized Fingerprint Attempt	99.5%	800 ms
Fake Face Detection (AI-based)	98.2%	1100 ms
RFID Cloning Attack Prevention	100%	500 ms
Intrusion Detection (AI Camera)	96.8%	1200 ms

- **Findings:**
  - The system successfully prevented unauthorized access in 99.5% of fingerprint attempts and 98.2% of fake face detections.
  - The RFID cloning protection system effectively blocked all unauthorized card duplication attempts.
  - The AI-driven surveillance system detected 96.8% of suspicious movements, but performance dropped in low-light conditions, indicating the need for infrared or night-vision support.

3. User Experience and Feedback

A survey was conducted among 50 users after testing the smart door system. The feedback was categorized as follows. The user experience details are given in Table 3.

Table 3. User Experience

Feature	User Satisfaction (%)
Ease of Use	92%
Security and Reliability	95%
Speed of Authentication	90%
Remote Access and Monitoring	94%

- **Findings:**
  - Users found the system easy to use (92%), with seamless authentication.
  - The security and reliability received the highest rating (95%), indicating user trust in the system.
  - Some users suggested improvements in facial recognition under low-light conditions and requested faster response times for fingerprint scanning.

The experimental results demonstrate that the Smart Door Security System provides high authentication accuracy, fast response times, and strong security features. The integration of biometric authentication, IoT-based remote access, and AI-driven surveillance significantly enhances access control and intrusion prevention. Future improvements will focus on reducing false rejection rates, improving low-light facial recognition, and enhancing AI-driven security alerts.

5. CONCLUSION

The development of a Smart Door Security System integrating biometric authentication, IoT-enabled remote access, and AI-driven surveillance has significantly improved the security and convenience of modern access control mechanisms. Traditional locking systems are vulnerable to physical breaches, key duplication, and unauthorized access, whereas the proposed system enhances security through multi-factor authentication, real-time monitoring, and automated alerts.The experimental results demonstrate the

DOI: https://doi.org/10.5281/zenodo.17283784

Volume 15, Issue-2
September, 2025, P64
ISSN: 2319-9253

system's high accuracy and reliability, with fingerprint authentication achieving 98.5% accuracy and AI-based facial recognition detecting unauthorized attempts with 98.2% effectiveness. The system's response time was optimized, ensuring seamless authentication and quick access control. Moreover, the RFID and IoT integration enabled users to remotely monitor and control access, enhancing overall security management.

The AI-powered anomaly detection successfully identified intrusion attempts and unauthorized access, improving proactive security measures. However, challenges remain, including low-light performance in facial recognition, cybersecurity risks, and power dependencies. Future improvements may focus on enhancing AI-driven recognition in varying conditions, integrating blockchain for secure access management, and incorporating advanced encryption techniques to prevent cyber threats.The proposed Smart Door Security System provides a robust, efficient, and intelligent security solution that can be applied to homes, offices, and high-security environments, ensuring enhanced safety, convenience, and real-time threat prevention.

REFERENCES

[1] M. Q. Mehmood, M. S. Malik, M. H. Zulfiqar, M. A. Khan, M. Zubair, and Y. Massoud, "Invisible touch sensors-based smart and disposable door locking system for security applications," Heliyon, vol. 9, no. 2, p. e13586, Feb. 2023, doi: 10.1016/j.heliyon.2023.e13586.

[2] J. Patel, S. Anand, and R. Luthra, "Image-Based smart surveillance and remote door lock switching system for homes," Procedia Computer Science, vol. 165, pp. 624–630, Jan. 2019, doi: 10.1016/j.procs.2020.01.056.

[3] G. B. A. Svaboe, K. Y. Bjerkan, and S. Meland, "Safe delivery of goods and services with smart door locks: Unlocking potential use," Transportation Research Interdisciplinary Perspectives, vol. 29, p. 101309, Dec. 2024, doi: 10.1016/j.trip.2024.101309.

[4] H. K. Taluja, A. Taluja, I. Kala, and B. Mallala, "Smart Office Automation using Multi-Dimensional Attention Spiking Neural Network for Face Recognition in Internet of Things," Applied Soft Computing, p. 112967, Mar. 2025, doi: 10.1016/j.asoc.2025.112967.

[5] A. Allen, A. Mylonas, S. Vidalis, and D. Gritzalis, "Smart homes under siege: Assessing the robustness of physical security against wireless network attacks," Computers & Security, vol. 139, p. 103687, Dec. 2023, doi: 10.1016/j.cose.2023.103687.

[6] M.-H. Yen, N. Mishra, W.-J. Luo, and C.-E. Lin, "A Novel Proactive AI-Based Agents Framework for an IoE-Based Smart Things Monitoring System with Applications for Smart Vehicles," Computers, Materials & Continua/Computers, Materials & Continua (Print), vol. 0, no. 0, pp. 1–10, Jan. 2025, doi: 10.32604/cmc.2025.060903.

[7] H. Dui, X. Wang, X. Dong, T. Zhu, and Y. Zhai, "Reliability model and emergency maintenance strategies for smart home systems," Reliability Engineering & System Safety, vol. 251, p. 110402, Jul. 2024, doi: 10.1016/j.ress.2024.110402.

[8] A. Dai, J. Zhang, C. K. Pai, and T. J. Lee, "The impact of the perception of smart hotel attributes and perceptions of service innovation on tourist happiness and brand loyalty," International Journal of Hospitality Management, vol. 127, p. 104107, Feb. 2025, doi: 10.1016/j.ijhm.2025.104107.

[9] H. B. Rai, S. Verlinde, and C. Macharis, "Unlocking the failed delivery problem? Opportunities and challenges for smart locks from a consumer perspective," Research in Transportation Economics, vol. 87, p. 100753, Oct. 2019, doi: 10.1016/j.retrec.2019.100753.

[10] S. Pulparambil, A. Al-Busaidi, Y. Al-Hatimy, and A. Al-Farsi, “Internet of Things-Based Smart Medical Waste Management System,” Telematics and Informatics Reports, vol. 15, p. 100161, Sep. 2024, doi: 10.1016/j.teler.2024.100161.

[11] M. Abdulla Al Mamun, M. A. Hannan, A. Hussain and H. Basri, "Integrated Sensing Systems and Algorithms for Solid Waste Bin State Management Automation," in IEEE Sensors Journal, vol. 15, no. 1, pp. 561-567, Jan. 2015, doi: 10.1109/JSEN.2014.2351452.

[12] E. N. Korkut, “Estimations and analysis of medical waste amounts in the city of Istanbul and proposing a new approach for the estimation of future medical waste amounts,” Waste Management, vol. 81, pp. 168–176, Oct. 2018, doi: 10.1016/j.wasman.2018.10.004.

[13] D. Vaishali, A. B. V S, S. J. A R, K. S. Krishna and M. M, "Face Recognition based Door Lock System," 2024 3rd International Conference on Automation, Computing and Renewable Systems (ICACRS), Pudukkottai, India, 2024, pp. 1655-1658, doi: 10.1109/ICACRS62842.2024.10841543.

[14] S. Sobale, K. Patel, A. Patel, S. Nikam, S. Pathrabe and S. Patil, "OTP Based Door Lock System with Mobile Application using Arduino UNO and ESP8266 Wi-Fi module," 2022 Sardar Patel International Conference on Industry 4.0 - Nascent Technologies and Sustainability for 'Make in India' Initiative, Mumbai, India, 2022, pp. 1-4, doi: 10.1109/SPICON56577.2022.10180607.