STM JOURNALS

Journal of
Mechatronics and Automation

ISSN: 2455-1988
Volume 12, Issue 2, 2025
May–August
DOI (Journal): 10.37591/JoMA

https://journals.stmjournals.com/joma

Review JoMA

AI-Powered Smart Door Lock System with IoT Integration for Enhanced Home Security

M. Banu Priya*

Abstract

An AI-Powered Smart Door Lock System with IoT Integration for Enhanced Home Security system is an advanced security solution that utilizes sensors, microcontrollers, and authentication mechanisms to control access efficiently. This system is designed to enhance security and convenience by eliminating the need for traditional keys, reducing the risks associated with lost or duplicated keys. It operates using various authentication technologies such as RFID (Radio Frequency Identification), fingerprint recognition, and password-based entry systems, ensuring that only authorized individuals can access a secured area. The system functions by detecting an authorized user through one of these authentication methods and granting access accordingly. Once the person has entered, the door automatically locks after a predetermined period or immediately upon detecting unauthorized attempts to gain entry. Some advanced models integrate with motion sensors, facial recognition systems, or mobile applications, further improving security and ease of use. AI-Powered Smart Door Lock System with IoT Integration for Enhanced Home Security system are widely implemented in residential buildings, commercial establishments, and vehicles to enhance safety, streamline access control, and improve user experience. In homes, these systems provide homeowners with peace of mind, allowing them to control entry remotely or through biometric authentication. In offices and corporate buildings, they help regulate access to restricted areas, ensuring that only authorized personnel can enter specific locations. In automobiles, automatic central locking enhances passenger safety by locking doors once the vehicle starts moving or when it detects unauthorized access attempts. Additionally, some modern systems are integrated with smart home automation and Internet of Things (IoT) technologies, enabling remote monitoring and control via smartphones or computers. These systems can also be programmed to send real-time notifications in case of a security breach, making them a crucial component of modern security infrastructure. Overall, the automatic door locking system is an essential technology that boosts security, prevents unauthorized access, and offers unparalleled convenience for homes, businesses, and vehicles.

Keywords: Real-time security monitoring, remote access control, motion sensor security system, smart home integration, wireless door lock system, embedded security systems, cyber-physical security

INTRODUCTION

An AI-Powered Smart Door Lock System with IoT Integration for Enhanced Home Security system is a smart security solution that automates door access using ultrasonic sensors, a servo motor, and an Arduino board. It enhances safety, convenience, and efficiency by eliminating manual locking and reducing the risk of unauthorized entry. This system ensures that doors automatically lock and unlock based on predefined conditions, such as user authentication, motion detection, or time-based settings. These systems are highly customizable and can include multi-factor authentication, emergency overrides, and time-based locking for enhanced security. Authentication methods such as RFID,

***Author for Correspondence**
M. Banu Priya
E-mail: banuchandru146@gmail.com

Assistant Professor, Department of Computer Applications, Nilgiri College of Arts and Science, Thaloor, Nilgiris, Tamil Nadu

Received Date: May 20, 2025
Accepted Date: June 26, 2025
Published Date: July 15, 2025

Citation: M. Banu Priya. AI-Powered Smart Door Lock System with IoT Integration for Enhanced Home Security. Journal of Mechatronics and Automation. 2025; 12(2): 34–38p.

fingerprint scanning, and password entry ensure that only authorized individuals can access the premises. Additionally, motion sensors can trigger automatic unlocking for authorized users while preventing unauthorized access. With the integration of IoT and smart home technology, modern automatic door locking systems allow remote control via mobile apps, enabling real-time monitoring and security alerts. These features make them ideal for homes, offices, and industrial facilities, where security and convenience are top priorities. By offering a seamless, secure, and efficient access control solution, automatic door locking systems improve safety, accessibility, and user experience, making them an essential component of modern security infrastructure.

EXISTING SYSTEM

The existing system for door locking primarily relies on manual locks, traditional key-based mechanisms, or basic electronic locks with limited automation. These systems often lack remote access, real-time monitoring, and advanced security features, making them less efficient and prone to security risks. Additionally, lost keys, unauthorized duplication, and human errors can compromise safety and convenience.

DRAWBACKS OF AUTOMATIC DOOR LOCKING SYSTEMS

Automatic door locking systems offer advanced security and convenience, but they come with certain challenges. One major concern is power dependency, as most systems require a continuous power supply or backup battery to function, making them vulnerable during outages. Additionally, the high initial cost of installation, including sensors, microcontrollers, and smart authentication devices, can be a barrier for some users. Another significant issue is cybersecurity risks, as smart locking systems connected to Wi-Fi or IoT platforms can be susceptible to hacking or unauthorized access. Despite these challenges, proper security measures, backups, and encryption can enhance reliability and safety in automated locking systems.

PROPOSED SYSTEM

The proposed system for an automatic door locking system enhances security by integrating smart authentication methods such as Arduino IDE, Arduino UNO board, Ultrasonic sensors, etc. It ensures real-time monitoring, remote access, and automated locking/unlocking based on predefined conditions. The system includes backup power solutions to prevent failures and encryption protocols for secure communication. By leveraging IoT and automation, it offers a reliable, user-friendly, and efficient security solution for homes and businesses.

LITERATURE SURVEY

The progression of access control technologies reflects the broader evolution of security paradigms from mechanical reliability to intelligent adaptability. While early developments in electronic locks introduced foundational digital mechanisms, such as numeric keypads and magnetic stripe readers, their security frameworks remained largely static and vulnerable to predictable intrusion patterns. The incorporation of wireless connectivity, notably Wi-Fi and Bluetooth Low Energy (BLE), marked a pivotal transition towards remotely operable systems. As outlined by Kim *et al.*, these early implementations expanded the functional scope of door locks but failed to address real-time adaptability and user-specific context awareness [1]. Recent advancements in embedded system architectures now facilitate dynamic integration with IoT ecosystems, thereby enabling live control, conditional automation, and location-aware responses [2]. This integration is central to transforming a door lock from a reactive mechanism to a proactive security node within a larger smart environment.

Artificial Intelligence introduces a vital layer of decision-making and predictive analysis within smart access systems. Unlike traditional access control systems that rely solely on deterministic inputs (e.g., password match), AI-powered locks can learn and adjust based on user-specific behavioral trends and biometric features. Deep learning algorithms, particularly convolutional models such as FaceNet, have demonstrated superior accuracy in identity verification under non-ideal conditions [3]. These systems

outperform earlier pattern-matching techniques by generating feature embeddings that generalize across lighting, angle, and facial expressions. Furthermore, by deploying such models locally on edge devices using frameworks like TensorFlow Lite, researchers like Warden and Situnayake have shown that it is possible to perform biometric inference in real time without relying on cloud connectivity, preserving both latency and privacy [4]. Beyond facial recognition, the field has explored hybrid modalities, including voice signature authentication and keystroke dynamics, offering an additional resilience layer against spoofing and unauthorized physical access [5].

However, the expansion of connectivity and intelligence inevitably introduces new vulnerability surfaces. While smart locks provide operational convenience, they also become targets for remote interception, firmware exploitation, and unauthorized relay attacks. Roman *et al*. highlighted systemic challenges in IoT security, especially where devices interact in loosely coupled, heterogeneous environments [6]. Proposed solutions include lightweight cryptographic protocols and device-authenticated trust layers, yet these require optimization for energy-constrained hardware. More recently, the implementation of blockchain-inspired ledgers for access logging has gained traction, offering tamper-evident data records and decentralized policy enforcement [7, 8]. Nevertheless, these technologies remain experimental in embedded security applications due to their overhead and integration complexity.

SYSTEM DESIGN AND DEVELOPMENT

System design and development for an automatic door locking system involves creating a secure, efficient, and user-friendly mechanism using hardware components like microcontrollers, sensors, and locking mechanisms. The development process includes software programming, IoT connectivity, and security protocols to ensure seamless operation, remote access, and protection against unauthorized entry. An Automatic Door Lock System is designed to enhance security and convenience by allowing automated access control. The system can be used in residential, commercial, and industrial settings to restrict unauthorized access and enable seamless entry using various authentication methods. The system consists of hardware and software components that work together to control door access. Users can unlock doors via keycards, PIN codes, biometric authentication, or mobile applications [9].

Input Design

The input design of an automatic door locking system includes authentication methods like RFID, biometrics, keypads, and mobile apps for secure access. Sensors detect motion, proximity, and door status for automatic operation (Figure 1). Remote access via IoT apps allows users to control the lock from anywhere. Emergency access is ensured through manual overrides, while power monitoring detects failures. Some systems also support voice commands and multi-factor authentication for enhanced security [10].

Output Design

The output design of an automatic door locking system focuses on providing clear, reliable, and secure responses to user inputs. The primary output is the activation of the locking mechanism, either locking or

Figure 1. Object detection triggering door unlocking.

Figure 2. Door closure triggered by absence of nearby object.

unlocking the door based on authentication. Visual indicators like LED lights or an LCD screen display access status, error messages, or power alerts. Audio outputs, such as buzzers or alarms, notify users of successful access, unauthorized attempts, or system malfunctions (Figure 2). Remote notifications via mobile apps or IoT platforms inform users about door status and security alerts. Some systems also provide real-time logs or access history for monitoring and security purposes [11].

Description of Modules

Ultrasonic Sensor Module (HC-SR04)

The Ultrasonic Sensor Module (HC-SR04) enhances the automatic door locking system by detecting objects or movement near the door using ultrasonic waves. It measures the distance of approaching users and triggers automatic door unlocking when a person is detected within a specified range. This enables touchless access control, improving both convenience and hygiene by reducing the need for physical contact. The sensor plays a crucial role in smart security systems, ensuring seamless and efficient door operation while enhancing user safety and accessibility.

Servo Motor Module

The servo motor in an automatic door locking system controls the locking and unlocking mechanism by rotating to a specific angle based on input signals. When authentication via RFID, PIN codes, biometrics, or mobile applications is successful, the servo motor rotates to unlock the door and automatically returns to the locked position after a set time. This ensures precise and efficient door control with minimal power consumption, making it an ideal component for smart security systems. Its ability to provide quick, accurate, and reliable movement enhances both system performance and security, ensuring seamless operation.

Arduino Uno Board

The microcontroller acts as the central processing unit of the automatic door locking system, handling inputs from sensors and authentication devices while controlling components such as the servo motor for locking and unlocking, LED indicators for status display, buzzer alerts for notifications, and remote access modules for IoT connectivity. It processes data efficiently to ensure secure and seamless door operation, responding to authentication inputs in real time. With support for programming via the Arduino IDE, the microcontroller provides a flexible and cost-effective solution for automation projects, making it an essential component in modern smart security systems.

Implementation Steps

The hardware setup of the automatic door locking system involves installing the Arduino board, sensors, servo motor, and power supply within the door system to ensure proper integration. System calibration is then performed by adjusting sensor detection ranges, servo motor angles, and response times for optimal performance. Once the hardware is configured, software deployment follows, where the control program is uploaded and configured on the Arduino board to manage authentication and access control. Finally, monitoring and maintenance include regular updates, troubleshooting, and security checks to ensure long-term reliability and protection against potential failures or security risks.

CONCLUSION

The automatic door locking system enhances security, convenience, and efficiency by integrating smart authentication methods like RFID, biometrics, and IoT-based remote access. It reduces manual effort, prevents unauthorized access, and provides real-time monitoring for improved safety. With proper testing, implementation, and maintenance, the system ensures reliable performance and long-term usability. Overall, it offers a modern, automated solution for secure and hassle-free access control in homes, offices, and industries. The automatic door locking system provides enhanced security and convenience using smart authentication methods like RFID, biometrics, and IoT. It ensures automated access control, prevents unauthorized entry, and offers remote monitoring. With proper implementation and maintenance, it delivers a reliable and efficient security solution.

REFERENCES

1. Kim Y, Lee J, Kim H. A Secure Smart Door Lock System Based on Wi-Fi. Int J Secur Appl. 2014; 8(3): 59–66.
2. Liu J, Xiao Y, Chen CLP. Cyber security and privacy issues in smart homes. IEEE Commun Mag. 2016 Apr; 54(4): 71–77.
3. Schroff F, Kalenichenko D, Philbin J. FaceNet: A unified embedding for face recognition and clustering. In Proc IEEE Conf on Computer Vision and Pattern Recognition (CVPR). 2015; 815–823.
4. Warden P, Situnayake D. TinyML: Machine Learning with TensorFlow Lite on Arduino and Ultra-Low-Power Microcontrollers. Sebastopol, CA: O'Reilly Media; 2019.
5. Jain AK, Ross A. Introduction to Biometrics. Cham: Springer; 2017.
6. Roman R, Zhou J, Lopez J. On the features and challenges of security and privacy in distributed Internet of Things. Comput Netw. 2013 Jul; 57(10): 2266–2279.
7. Novo M. Blockchain meets IoT: An architecture for scalable access management in IoT. IEEE Internet Things J. 2018 Apr; 5(2): 1184–1195.
8. Dorri A, Kanhere SS, Jurdak R. Lightweight blockchain for IoT. J Parallel Distrib Comput. 2019 Jan; 134: 180–197.
9. Xu X, Chen Y, Li X, Blasch E. A Secure Dynamic Edge Resource Federation Architecture for Cross-Domain IoT Systems. arXiv. 2022 Aug 2.
10. Kurniasyah I, Rakhmawati L. Smart Door Lock Innovation Using Integration of Bluetooth Low Energy and MQTT IoT Protocol. Indonesian Journal of Electrical and Electronics Engineering (IJEEE). 2025 Jan; 8(1): 41–46.
11. Jangir S, Sharma BC, Saini S, Soni G, Yadav R. Keyless Lock Based on Internet of Things. Journal of Network Security (JoNS). 2024; 12(2): 18–21.

