International Scientific Journal of Engineering and Management (ISJEM) ISSN: 2583-6129
Volume: 04 Issue: 03 | March – 2025 DOI: 10.55041/ISJEM02279
An International Scholarly || Multidisciplinary || Open Access || Indexing in all major Database & Metadata

Advanced Smart Lock Systems

Balaji Shivram R U
UG Student, Dept. of CSE
Jain (Deemed-to-be) University
Erode, Tamil Nadu
balajishivramru@gmail.com

Giri Prasath
UG Student, Dept. of CSE
Jain (Deemed-to-be) University
Hosur, Tamil Nadu
giriprasath714@gmail.com

Gowreesh J K
UG Student, Dept. of CSE
Jain (Deemed-to-be) University
Erode, Tamil Nadu
gowreesh.jk03@gmail.com

Kavya Sri
UG Student, Dept. of CSE
Jain (Deemed-to-be) University
Coimbatore, Tamil Nadu
kavyakeyan@gmail.com

Sindhanur Jahnavi
UG Student, Dept. of CSE
Jain (Deemed-to-be) University
Hospet, Karnataka
jahnavisindanur28@gmail.com

Dr. P. Srinivasa Rao
Professor, Dept. of CSE
Jain (Deemed-to-be) University
Andhra Pradesh
srinivasa.p@jainuniversity.ac.in

Abstract— This paper introduces a smart lock system that integrates IoT, artificial intelligence, and computer vision to enhance security and accessibility. The system is built on an Arduino platform, incorporating an NFC reader, keypad, PIR sensor, ultrasonic sensor, Bluetooth module, and servo motor, along with an ESP32-CAM module for facial recognition and real-time object detection. By leveraging motion sensors and a YOLO-based deep learning model, the system detects the number of individuals present, analyzes body build, and identifies outfit colors, generating audio descriptions to assist visually impaired users. Authentication is conducted through NFC tags, a keypad, and Bluetooth communication, with SHA-256 encryption ensuring secure access. Successful authentication triggers the servo motor to unlock the door, while unsuccessful attempts activate an alert system and log access attempts for security monitoring. Additionally, IoT-enabled remote access and real-time notifications improve control over entry points in residential and commercial settings. Performance evaluations indicate high accuracy in person detection and outfit recognition, demonstrating the system's effectiveness. Future developments aim to integrate cloud-based authentication, mobile applications, and AI-driven behavioral analysis for further enhancements.

Keywords—Smart Locks, Smart Automation, Assistive Technology, Smart home integration, Internet of Things (IoT), AI-based Authentication

I. INTRODUCTION

Smart buildings are now integral to the Internet of Things (IoT) landscape. Connecting devices within homes boosts internet use, enhancing convenience, security, and comfort. The suggested method handles the door lock mechanism, a security feature of smart home technology. By enabling the building owner to keep an eye on the structures using the door lock system is an Arduino UNO-powered smartphone-controlled, Bluetooth-enabled solution determines the security. It is critical to secure confidential items, properties, and lives. To prevent needless harm to these items, we should give them the attention they require. The microcontroller-based door lock system is one of the greatest security measures available in society, however there are many more systems in place. Overall, the statement underscores the role of smart buildings and IoT in improving security, comfort, and convenience in living spaces. The suggested method of utilizing a Smartphone-controlled, Bluetooth-connected door lock system using Arduino UNO showcases the potential of smart home technology to enhance security measures effectively.

II. LITERATURE SURVEY

Multiple door control systems were examined, each with its distinct features. In one system, emphasis was placed on utilizing PIR and Ultrasonic sensors, along with a servo motor, all connected to an Arduino and Bluetooth app. The Bluetooth module facilitated door control through a dedicated mobile application, while the Arduino UNO continuously processed data from the sensors, such as intensity and distance. However, this particular system lacked intrusion detection.

A smart door lock that is based on the confirmation that the identified subject is a person is offered in another study. The associated trajectory indicates that the subject intends to pass. The owner is notified when the picture is taken and can then determine whether or not to open the door. In order to facilitate the process of carrying out the whole operations, we have created an Android application and lighting system for IoT-enabled smart homes. This system allowed users to remotely control door access. However, a limitation of this system was the reliance on relays for operating the door lock and , which

International Scientific Journal of Engineering and Management (ISJEM) ISSN: 2583-6129
Volume: 04 Issue: 03 | March – 2025 DOI: 10.55041/ISJEM02279
An International Scholarly || Multidisciplinary || Open Access || Indexing in all major Database & Metadata

typically required more resources than what the microcontroller could provide at minimal cost. These studies highlight different strategies for remote control and intrusion detection, though some systems rely on relays, which increase costs and complexity.

III. OVERVIEW

This smart lock system combines IoT, AI, and computer vision to provide secure and accessible entry management. Built on an Arduino platform, it integrates an NFC reader, keypad, PIR sensor, ultrasonic sensor, Bluetooth module, servo motor, and an ESP32-CAM for facial recognition and real-time detection. When motion is detected, the system activates the camera and AI model to identify individuals, count the number of people, and analyze outfit colors. This information is then converted into audio descriptions to assist visually impaired users. Authentication is handled through NFC, a keypad, or Bluetooth, with SHA-256 encryption ensuring security. Upon successful verification, the lock opens; otherwise, an alert is triggered. The system also supports remote monitoring via IoT connectivity. Designed for homes and commercial spaces, it enhances security while promoting accessibility. Future improvements include cloud authentication, AI-driven behavioral analysis, and mobile app integration for enhanced functionality.

A. *Existing Systems*

The research paper examines a variety of current smart locks, each offering features like keyless entry, remote control, and compatibility with virtual voice assistants, utilizing authentication methods such as proximity sensing with smartphones and biometrics. For instance, the Schlage Encode Smart Wi-Fi Deadbolt connects directly to Wi-Fi without requiring a bridge, supports multiple user codes, and includes built-in alarm sensors. The Yale Assure Lock SL provides a keyless, streamlined design that integrates with popular home automation systems and includes tamper detection. Meanwhile, the Kwikset Kevo Smart Lock employs Bluetooth, enabling touch-to-open access and convenient control via smartphone. Each of these locks brings unique benefits, such as easy installation, compatibility with older systems, appealing design, and temporary access options. However, some models may face challenges like the need for additional modules, occasional connectivity disruptions, or compatibility limitations with certain door types or automation systems. A thorough analysis of these features, benefits, and constraints is essential to understanding how these locks contribute to the study's objectives.

B. *Aim*

IoT products are blooming all over the globe at this time. It is becoming a need to build a connected space for most of the people. We'll build the connected space starting with smart doors and locks.

The goal of this study is to create a smart lock system that addresses the shortcomings of current options and gives homeowners a safe, dependable, and easy-to-use access control system.. The proposed system should offer advanced security features, such as biometric authentication, tamper detection, and real-time monitoring, while also providing convenient access methods, including remote control via smartphones, keyless entry options, and integration with existing home automation systems.

C. *Proposed system*

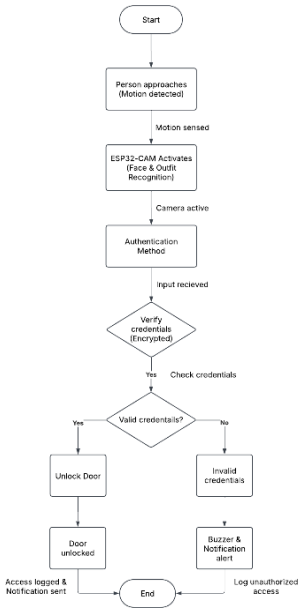

Fig. 1. Proposed flowchart

D. *Limitations*

- Fault on recognition devices.
- Requires a standardized communication protocol for interoperability between different vehicles and infrastructure.
- Reliability issues in areas with limited network coverage.

IV. ARCHITECTURE

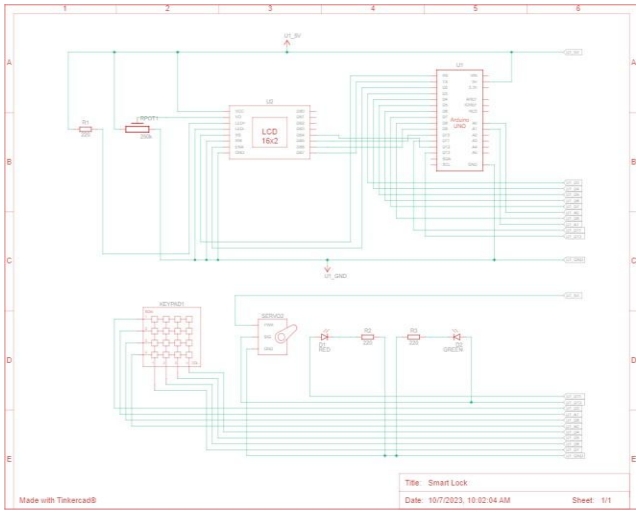

Fig. 2. System architecture

This smart lock system integrates a variety of components to enhance security and control access. A Passive

Infrared Sensor (PIR) detects any movement around the door, while an Ultrasonic sensor gauges the distance of approaching individuals to alert the system of nearby presence. For convenient, contactless entry, an NFC module allows users to unlock the door with authorized devices. Additionally, the ESP32 Cam provides live video feed and captures images upon detecting motion, enabling real-time monitoring. An optional keypad offers another access method through code entry. Together, these components coordinate with the electronic lock mechanism to provide adaptable and secure access for both residential and commercial applications

V. EXPECTED OUTCOMES

The smart lock system is expected to deliver enhanced security, accessibility, and automation through the integration of IoT, AI, and computer vision. It will accurately detect motion and human presence, continuously monitor individuals at the door, and identify body build and outfit colors to provide audio descriptions for visually impaired users. The authentication process using NFC, a keypad, and Bluetooth, secured by SHA-256 encryption, will ensure that only authorized users gain access. Successful authentication will trigger the servo motor to unlock the door, while failed attempts will activate alerts and logging mechanisms for security monitoring. Additionally, the system will support remote access and real-time notifications via IoT connectivity, allowing users to monitor and control access from a distance. The project is expected to improve safety, convenience, and inclusivity, with future expansions incorporating cloud-based authentication, AI-powered behavior analysis, and mobile app integration for a more advanced and user-friendly system.

VI. MARKET ANALYSIS

A. *Marketing Analysis*

The smart home automation market is rapidly growing, with leading technology companies such as Godrej, Amazon, and Samsung driving advancements. The increasing demand for secure and connected living spaces, especially in regions with strong networking infrastructure, is fueling market expansion.

1) *Market Size and Growth:*

The global market for smart locks and home automation is witnessing continuous growth, driven by the increasing need for enhanced security solutions and smart connectivity. The market is expected to expand significantly in the coming years due to the rising adoption of IoT-enabled devices and the emphasis on modern security infrastructure.

2) *Key Players:*

Several established companies are actively investing in the development and deployment of smart home technologies. Notable industry leaders include Godrej, Google, Amazon, Philips, Samsung, and Honeywell Home, all of whom are advancing automation technologies to improve security and convenience.

3) *Competitive Landscape:*

The smart automation sector is highly competitive, with both well-established brands and emerging startups striving to offer innovative and secure solutions. Companies are allocating substantial resources toward research and development to enhance the efficiency, reliability, and cybersecurity of smart automation systems.

4) *Regional Analysis:*

Smart home automation is experiencing significant growth in regions such as North America, Europe, and Asia-Pacific. Developed economies with high-speed internet access and widespread adoption of IoT devices are at the forefront of implementing advanced smart home solutions, making these regions key markets for further expansion.

B. *Comparsion Analysis*

Smart locks offer a significant upgrade over traditional locks in terms of security, convenience, access control, integration, and user experience. Traditional locks provide basic security but are vulnerable to picking, unauthorized key duplication, and forced entry. In contrast, smart locks incorporate advanced security features such as encryption, tamper detection, and real-time monitoring to offer enhanced protection against physical attacks. Moreover, smart locks eliminate the need for physical keys and offer keyless entry methods like smartphone apps, PIN codes, or biometrics, providing a more convenient and hassle-free experience. They also allow for flexible access control, enabling users to remotely manage access permissions, grant temporary access, and monitor door activity through mobile apps. Additionally, smart locks can integrate with home automation systems, virtual voice assistants, and other smart devices, allowing users to control and monitor their locks remotely, automate locking and unlocking, and integrate access control with other smart home functionalities. With their seamless user experience, compatibility with standard door preparations, and ease of installation, smart locks provide a comprehensive solution that significantly improves security and convenience for residential applications.

TABLE 1. COMPARSION TABLE

Classification	**Physical key**	**Digital Door lock system**	**Smart Door lock system**
Convinience	Central key; requirement of physical keys	No key required	Usage of smartphone
Expandability	NA	NA	USB, Bluetooth, OTP, App support
Security	Duplicate keys	Password leakage	Using secure authentication for reduced risk

VII. CONCLUSION

The development of this AI-powered smart lock system demonstrates the potential of IoT, computer vision, and secure authentication mechanisms in enhancing home and commercial

security. By integrating motion detection, facial recognition, and outfit identification, the system ensures continuous monitoring and improved accessibility for visually impaired users. The authentication process, secured with SHA-256 encryption, provides robust security, preventing unauthorized access while allowing convenient entry for registered users. The system's ability to detect multiple individuals and provide real-time alerts further strengthens its reliability and effectiveness.

Beyond security, the system introduces smart automation and remote accessibility, leveraging IoT technology for real-time notifications and monitoring. The combination of NFC, keypad, and Bluetooth-based authentication offers a versatile and user-friendly experience. Additionally, the implementation of buzzer alerts and access logs enhances overall safety and ensures better tracking of entry attempts.

Future enhancements could include cloud-based authentication, AI-driven behavior analysis, and mobile app integration, further optimizing security and convenience. As smart home automation continues to evolve, this project paves the way for advanced, AI-driven security solutions that prioritize both safety and inclusivity, making homes and businesses more secure and intelligent.

VIII. Future Scope

A rechargeable battery can be incorporated into the system to provide backup power for 3-4 hours in case of an outage. Motion detection will be linked to a light source to ensure sufficient illumination at all times. Additionally, cloud computing can be utilized, enabling users to control the lock remotely from any location. Surveillance capabilities can be enhanced by integrating cameras.

For added security, features such as fingerprint scanning and facial recognition can be included. To prevent unnecessary door openings, voice commands may be implemented, allowing the person outside to interact with the system. Moreover, a fire alarm function can be integrated, serving a dual purpose as both a smart lock and a fire detection system—particularly beneficial in homes where fire alarms are often absent.

This system can be deployed in hotels, banks, motels, and other establishments as an alternative locking mechanism to enhance security. An alert system connected to the cloud can notify the user of any unauthorized entry and automatically contact the authorities if needed.

References

[1] D. Han, H. Kim, and J. Jang, "Blockchain based smart door lock system," unpublished, Sogang University, Seoul 04107, Korea.

[2] J.-I. Jeong, "A study on the IoT based smart door lock system," unpublished.

[3] N. A. Hussein and I. Al Mansoori, "Smart door system for home security using Raspberry Pi3," unpublished, Ferdowsi University of Mashhad, Mashhad, Iran.

[4] F. Aman and A. C., "Motion sensing and image capturing based smart door system on Android platform," unpublished, The National Institute of Engineering, Mysuru, India.

[5] S. M., V. G., and A. R., "IoT enhanced smart door locking system," unpublished.

[6] C. Bapat, G. Baleri, S. Inamdar, and A. V. Nimkar, "Smart-lock security re-engineered using cryptography and steganography," unpublished, Sardar Patel Institute of Technology, University of Mumbai, Mumbai, India.

[7] Y. T. Park, P. Sthapit, and J.-Y. Pyun, "Smart digital door lock for home automation," unpublished, Dept. of Information and Communication Engineering, Chosun University, Gwangju, South Korea.

[8] N. Kumbhar, "Smart door locking system using wireless communication technology," unpublished, Mudhoji College, Phaltan, Aug. 2017.

[9] S. A. Prity, J. Afrose, and M. M. Hasan, "RFID based smart door lock security system," American Journal of Sciences and Engineering Research, vol. 4, no. 3, p. 2348-703X, in press.