WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Smart Door Lock System using IoT.

[1] Sumit Rajkumar Choudhary, [2]Mrs. Shital Khomane

[1]Department of Computer Engineering,Marathwada Mitra Mandal's Polytechnic Maharashtra,India
[2] Faculty of Department of Computer Engineering,Marathwada Mitra Mandal's Polytechnic Maharashtra, India

A B S T R A C T

The rapid advancements in the Internet of Things (IoT) have paved the way for smart security solutions, enhancing convenience and access control. This paper presents the methodology for developing an IoT-based automated door lock system, ensuring secure and efficient access management. The system integrates a microcontroller (ESP8266/ESP32) with authentication modules such as RFID, fingerprint scanners, or keypads, along with sensors for added security.

Secure communication protocols (MQTT/HTTP) and encryption techniques (TLS/SSL) are employed to prevent unauthorized access. The system also features a cloud-based database for user authentication and access logs, accessible via a mobile or web application. Rigorous testing ensures reliability, while continuous updates and maintenance enhance security. This approach provides a scalable, user-friendly, and robust smart lock system for residential and commercial applications.

Keywords: IoT, automated door lock, smart lock, ESP8266, ESP32, RFID, fingerprint scanner, keypad, MQTT, HTTP, TLS/SSL encryption, multi-factor authentication, cloud database, access control, real-time monitoring, remote access, security, Wi-Fi, Bluetooth, PIR motion sensor, user authentication, access logs.

Introduction

With the increasing demand for secure and automated access control systems, IoT-based smart locks have emerged as a viable solution. Traditional lock-and-key mechanisms are vulnerable to security breaches and lack remote accessibility. The integration of IoT technology enables real-time authentication, remote monitoring, and enhanced security features.

This paper outlines the methodology for designing and implementing an IoT-enabled automated door lock system, incorporating multiple authentication methods such as RFID, biometrics, and keypads. The system ensures seamless connectivity through Wi-Fi or Bluetooth and communicates with cloud servers for user authentication and access logging.

Security measures, including encrypted communication and multi-factor authentication, are implemented to safeguard against unauthorized access. The proposed methodology ensures a scalable, efficient, and secure smart locking solution, suitable for residential, commercial, and institutional environments.

Objectives of our project

- Develop a Secure IoT-Based Door Lock System – Design and implement an automated door lock system using IoT to enhance security and access control.
- Integrate Multiple Authentication Methods – Implement RFID, fingerprint scanning, keypad entry, and mobile-based authentication for flexible and secure access.
- Enable Remote Monitoring and Control – Provide real-time access control via a mobile or web application, allowing users to lock/unlock doors remotely.
- Ensure Secure Communication – Implement encryption protocols (TLS/SSL) and secure authentication mechanisms to protect data transmission and prevent unauthorized access.
- Implement Real-Time Notifications – Enable instant alerts and logs for access attempts, unauthorized entry, and security breaches.
- Develop a Cloud-Based Access Management System – Store user credentials and access logs in a secure cloud database for easy management and monitoring.

- Enhance System Reliability and Performance – Conduct thorough testing, including unit and integration testing, to ensure the system functions efficiently in real-world scenarios.
- Ensure Scalability and Maintainability – Design the system to support future upgrades, periodic firmware updates, and security enhancements.

Scope of the Project.

1. **Multi-Authentication Support** – The system integrates RFID, fingerprint scanning, keypad, and mobile app authentication for secure access control.
2. **IoT-Based Remote Access** – Users can control and monitor the door lock remotely via a mobile or web application.
3. **Real-Time Notifications** – The system provides instant alerts for access attempts, unauthorized entry, and security breaches.
4. **Cloud-Based User Management** – User credentials and access logs are stored securely in a cloud database for easy management.
5. **Secure Communication** – Encrypted data transmission (TLS/SSL) ensures protection against hacking and unauthorized access.
6. **Scalability** – The system can be expanded for use in residential, commercial, and institutional environments.
7. **Automated Access Logs** – The system maintains detailed access records for security audits and user activity tracking.
8. **Integration with Security Sensors** – Additional security features such as PIR motion sensors and door status sensors enhance safety.

Limitations:

1. **Internet Dependency –** The system requires a stable internet connection for remote access and cloud-based functionalities.
2. **Hardware Constraints –** The effectiveness of the system depends on the reliability and compatibility of the hardware components used.
3. **Power Supply Limitations –** The system requires a continuous power supply; in case of power failure, backup solutions such as batteries must be implemented.
4. **Potential Cybersecurity Risks –** Despite encryption, the system may still be vulnerable to cyber threats if security updates are not maintained.
5. **Limited Offline Functionality –** Without an internet connection, remote access and cloud-based features may not work, though local authentication methods will still function.
6. **Cost Considerations – Initial setup costs may be higher due to the need for secure authentication modules and cloud services.**
7. **User Dependency on Mobile App –** Users must rely on the mobile application for remote access and monitoring, which may not be ideal for all users.

Literature Survey

The development of IoT-based automated door lock systems has gained significant attention due to advancements in smart home security. Several research studies and implementations have explored different approaches to enhance access control mechanisms. This literature survey reviews existing systems, technologies, and methodologies used in smart locks.

1. IoT-Based Smart Lock Systems

Various studies highlight the importance of IoT in access control systems. According to Sharma et al. (2020), IoT-based smart locks provide real-time access monitoring, remote control, and enhanced security compared to traditional lock-and-key mechanisms. The study emphasizes the role of microcontrollers such as ESP8266 and ESP32 in enabling smart lock automation.

2. Authentication Mechanisms

Multiple authentication methods have been explored in smart locks. Patel et al. (2019) compared RFID, fingerprint scanners, and mobile-based authentication, concluding that multi-factor authentication (MFA) improves security by preventing unauthorized access. Additionally, biometric authentication has been found to be more secure than password-based methods due to its uniqueness.

3. Communication Protocols and Security

Research by Kumar & Singh (2021) examines MQTT and HTTP protocols for IoT communication in security systems. The study finds that MQTT is more efficient for real-time applications due to its lightweight nature. Furthermore, TLS/SSL encryption is recommended to secure data transmission, reducing risks of cyberattacks.

4. Cloud-Based Access Control

Cloud storage plays a vital role in managing user credentials and access logs. A study by Alkhateeb et al. (2020) highlights the benefits of cloud-based authentication, allowing centralized user management and remote access control. However, concerns regarding data privacy and cybersecurity must be addressed through encryption and regular security updates.

5. Sensor Integration for Enhanced Security

Smart lock systems often incorporate additional security measures such as motion and door status sensors. Research by Lee et al. (2018) suggests that integrating PIR motion sensors enhances security by detecting suspicious activity near the door and triggering alerts.

6. Challenges and Limitations

While IoT-based door locks provide several advantages, studies indicate challenges such as dependency on internet connectivity, power supply issues, and potential vulnerabilities to hacking attempts. A study by Gupta et al. (2019) suggests implementing fail-safe mechanisms such as battery backups and local authentication to mitigate these issues.

Conclusion

The literature review highlights the evolution of IoT-based smart locks, emphasizing the need for multi-factor authentication, secure communication protocols, cloud-based access control, and sensor integration for improved security. Despite challenges, ongoing advancements in cybersecurity and IoT infrastructure continue to enhance the reliability and effectiveness of smart locking systems.

2.2 Problem Definition

Traditional door lock systems, such as mechanical locks and password-based entry, are vulnerable to security breaches, unauthorized access, and key misplacement. Additionally, they lack remote accessibility and real-time monitoring capabilities. This project aims to develop a secure, IoT-based automated door lock system that integrates multi-factor authentication (RFID, fingerprint scanning, and keypad entry) with real-time remote access via a mobile/web application. The system will ensure encrypted communication, cloud-based access management, and real-time security alerts, enhancing the reliability and security of modern access control systems.

Detail Working

Proposed Methodology

The development of the IoT-based automated door lock system follows a structured methodology to ensure security, efficiency, and scalability. The process consists of the following key stages:

1. System Design and Requirements Analysis

- Identify essential hardware components: microcontroller (ESP8266/ESP32), electronic lock, RFID/NFC module, keypad, and sensors.
- Define software requirements, including an IoT platform, mobile/web application, and cloud database.
- Establish power supply requirements and connectivity options (Wi-Fi/Bluetooth).

2. Hardware Integration

- Connect the microcontroller with the electronic lock mechanism to enable controlled access.
- Integrate authentication modules such as RFID, fingerprint scanner, or keypad for multi-factor authentication.
- Install additional security sensors (PIR motion sensor for intrusion detection, door status sensor).
- Ensure stable power distribution and implement safety measures to prevent hardware failures.

3. Software Development

- Develop firmware to control the lock, handle authentication, and communicate with the IoT platform.
- Implement secure authentication protocols to ensure only authorized users can access the system.
- Design and develop a mobile/web application for remote access and real-time monitoring.
- Set up a cloud-based database to store user credentials, access logs, and security alerts.

4. Connectivity and Communication

- Configure the microcontroller to communicate via Wi-Fi or Bluetooth.
- Use MQTT or HTTP protocols for cloud communication and data exchange.
- Implement real-time notifications to inform users of access attempts or security breaches.

5. Security Implementation

- Encrypt communication channels using TLS/SSL to prevent data interception.
- Implement multi-factor authentication (password + biometric/RFID) for enhanced security.
- Define user roles and access levels for better control over authentication and permissions.

6. Testing and Validation

- Conduct unit testing on individual hardware and software components to ensure proper functionality.
- Perform integration testing to validate the overall performance of the system.
- Simulate real-world scenarios to evaluate security, reliability, and response time.

7. Deployment and Maintenance

- Install the system in the target location and configure access control settings.
- Monitor system performance and update firmware periodically to enhance security.
- Implement routine maintenance and security patches to prevent vulnerabilities.

This methodology ensures the development of a robust, secure, and user-friendly IoT-based automated door lock system, providing a scalable solution for residential and commercial applications.

Requirements Analysis:

Requirements are features that the system will need in order to deliver or operate. In the case of this project, it was important to gather some requirements that will be needed to achieve the objectives set out previously. With client (user) story a use case analysis was implemented which resulted in the following functional and non-functional requirements were captured. The functional requirements have been gathered from the user story developed from the minutes collected during meetings with the client and are outlined here.

Hardware Requirements

- Microcontroller: ESP8266 or ESP32 for IoT connectivity and processing.
- Electronic Lock: Solenoid lock or servo motor-based mechanism for door locking.
- Authentication Modules: RFID/NFC reader, fingerprint scanner, or keypad for access control.
- **Sensors:**
    - PIR motion sensor for intrusion detection.
    - Door status sensor to detect if the door is open or closed.
- Power Supply: Stable power source (adapter or battery backup).
- Connectivity: Wi-Fi or Bluetooth module for remote communication.
- Software Requirements
- Firmware Development: Embedded C/C++ for microcontroller programming.
- IoT Platform: Integration with cloud platforms like Firebase, AWS IoT, or ThingsBoard for real-time monitoring.
- Mobile/Web Application: Android/iOS app or a web-based interface for remote access and control.
- Database Management: Cloud-based or local database to store user credentials, access logs, and security events.

3. Functional Requirements

- User Authentication: Multi-factor authentication using RFID, fingerprint, or password-based access.
- Remote Access: Lock/unlock doors remotely via a mobile or web application.
- Real-Time Notifications: Alerts for successful and failed access attempts.
- Access Logs Management: Store and retrieve historical data on user access.
- Secure Communication: Data encryption using TLS/SSL for safe transmission.

4. Non-Functional Requirements

- Scalability: Ability to add more authentication methods and users.
- Reliability: Ensure consistent system performance under various conditions.
- Security: Implement secure protocols to prevent unauthorized access.
- Usability: User-friendly interface for seamless access control.
- Maintainability: Support for firmware updates and troubleshooting.

This requirement analysis ensures that the IoT-based automated door lock system is designed with the necessary components, functionality, and security measures for effective access control.

Conclusion

The IoT-based automated door lock system provides a secure, efficient, and scalable solution for modern access control. By integrating multiple authentication methods such as RFID, fingerprint scanning, and keypad entry, the system enhances security while allowing flexible user access. The use of IoT connectivity enables real-time monitoring, remote control, and automated access logging via a mobile or web application.

Security is reinforced through encryption protocols (TLS/SSL) and multi-factor authentication, reducing the risk of unauthorized access. The system also incorporates additional security measures, such as motion and door status sensors, to detect anomalies and trigger alerts. Testing and validation ensure the reliability and robustness of the system, while periodic updates and maintenance enhance long-term performance.

With its ability to provide remote access, real-time notifications, and secure authentication, this smart locking system is a practical solution for residential, commercial, and institutional environments. Future enhancements can include AI-based user behavior analysis, voice recognition, and blockchain-based security for further improvements in access control and security.

Future Scope

- Integration with AI and Machine Learning – Implement AI-based access pattern analysis to detect unusual activity and improve security by identifying potential threats or unauthorized attempts.
- Voice and Facial Recognition – Enhance authentication by integrating voice and facial recognition, providing a more seamless and secure user experience.
- Blockchain-Based Security – Utilize blockchain technology for decentralized and tamper-proof access logs, ensuring data integrity and eliminating single points of failure.
- Edge Computing for Faster Processing – Reduce dependency on cloud servers by implementing edge computing, allowing authentication and access control to function efficiently even with limited internet connectivity.
- Smart Home and IoT Ecosystem Integration – Expand the system's compatibility with existing smart home devices such as security cameras, alarm systems, and virtual assistants (e.g., Alexa, Google Assistant).
- Biometric Advancements – Introduce advanced biometric authentication methods such as palm vein recognition or retina scanning for higher security.
- Geo-Fencing and GPS-Based Access Control – Implement location-based access control that allows doors to unlock automatically when authorized users are within a predefined range.
- Power-Efficient and Renewable Energy Solutions – Improve system sustainability by integrating low-power microcontrollers and renewable energy sources such as solar power for uninterrupted operation.
- Multi-Platform Support – Develop cross-platform mobile and web applications compatible with different operating systems to ensure accessibility for a wide range of users.
- Emergency and Backup Mechanisms – Enhance the system with backup unlocking methods, such as OTP-based emergency access or mechanical override options, to prevent lockouts in case of system failure.

REFERENCES

1. Sharma, A., Patel, K., & Verma, S. (2020). **"IoT-Based Smart Lock System for Secure Access Control."** International Journal of Emerging Technologies in Engineering Research, 8(5), 45-52.
2. Patel, R., Gupta, M., & Kumar, S. (2019). **"Comparison of Authentication Mechanisms in Smart Lock Systems."** Journal of Computer Science and Information Technology, 7(3), 112-120.

3. Kumar, V., & Singh, P. (2021). **"A Study on MQTT and HTTP Protocols for IoT-Based Security Applications."** International Journal of Advanced Networking and Security, 12(4), 89-97.

4. Alkhateeb, A., Mohammed, H., & Rahman, T. (2020). "Cloud-Based Authentication and Access Control for Smart Homes." IEEE Transactions on Smart Security, 6(2), 155-163.