21CSE253T/ INTERNET OF THINGS

On

IOT-BASED SMART DOOR LOCK SYSTEM

Submitted by

GOPAL KUMAR RA2311003020789

Under the guidance of

Dr. U. SURENDAR

(Assistant Professor, Department of Computer Science and Engineering)

IV SEMESTER/IIYEAR

FACULTY OF ENGINEERING AND TECHNOLOGY

SCHOOL OF COMPUTER SCIENCE ENGINEERING

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

SRM INSTITUTE OF SCIENCE AND TECHNOLOGY
RAMAPURAM, CHENNAI

APRIL 2025

SRM INSTITUTE OF SCIENCE AND TECHNOLOGY
(Deemed to be University U/S 3 of UGC Act, 1956)

BONAFIDE CERTIFICATE

Certified that this case study report titled **IOT-BASED SMART DOOR LOCK SYSTEM** is a bonafide work of **GOPAL KUMAR (RA2311003020789),** who carried out the case study work under the guidance of Dr.U.Surendar, Assistant Professor, CSE at SRM Institute of Science and Technology, Ramapuram. This case study work confirms to 21CSE253T/Internet of Things, IV Semester, II year, 2025.

SIGNATURE

Dr.U.SURENDAR, M. E.,Ph.D.,MISTE, IEEE
Assistant Professor
Computer Science and Engineering,
SRM Institute of Science and Technology,
Ramapuram, Chennai.

TABLE OF CONTENTS

LIST OF FIGURES

CHAPTER 1
INTRODUCTION

1.1 The Growing Importance of Smart Door Lock System

In today’s rapidly advancing technological era, security and convenience are becoming increasingly important in residential and commercial spaces. Traditional locking systems, while reliable, lack the flexibility and remote accessibility demanded by modern users. The integration of the Internet of Things (IoT) into everyday devices has opened new possibilities for enhancing security and ease of access. One such innovation is the IoT-based Door Lock System, which allows users to control and monitor door locks remotely using smartphones, computers, or voice-controlled assistants.

This smart locking solution not only enhances security through real-time alerts and activity logs but also offers seamless access management through mobile apps or web interfaces. By leveraging technologies such as Wi-Fi. The smart door lock system market has experienced rapid growth in recent years, driven by increasing demand for home automation, enhanced security, and convenience. With the rise of IoT (Internet of Things) technologies, these locks offer features like remote access, biometric authentication, and real-time monitoring through smartphones, making them highly appealing for residential, commercial, and hospitality sectors.

1.2 The Need for Smart Door Lock System

The need for a smart door lock system arises from the growing demand for enhanced security, convenience, and remote accessibility in modern homes and workplaces. Traditional lock-and-key mechanisms are limited in functionality, prone to key loss or duplication, and offer no real-time monitoring or control. A smart door lock, integrated with IoT technology, allows users to lock or unlock doors remotely, monitor access logs. When considering the need for a smart door lock system .

1.3 Introduction to Smart Door Lock System

In recent years, technological advancements have significantly transformed the way we interact with our everyday environment. The concept of smart homes has rapidly gained popularity, introducing automation and remote control to various household devices. Among the most crucial aspects of a smart home is its security system, with smart door locks becoming a fundamental component. A smart door lock system leverages the power of the Internet of Things (IoT) to provide secure, flexible, and user-friendly access control to residential, commercial, and industrial buildings.

Traditional mechanical locks, although widely used, have several limitations. They rely on physical keys, which can be lost, stolen, or duplicated, posing a serious threat to the security of the premises. Moreover, traditional locks do not offer any form of access monitoring or remote control, making them less suitable for the needs of modern lifestyles.

1.4 Role of IoT in Smart Door Lock System

The Internet of Things (IoT) plays a pivotal role in transforming traditional door lock mechanisms into intelligent, connected smart security systems. By enabling devices to communicate and share data over the internet, IoT allows smart door locks to be remotely monitored and controlled through smartphones, tablets, or web interfaces. It facilitates real-time access management, where users can lock or unlock doors from any location, receive instant notifications about door status or unauthorized access attempts, and review access logs for enhanced security.

The Internet of Things (IoT) plays a pivotal role in the functionality and advancement of smart door lock systems by enabling seamless connectivity, control, and automation. Through IoT integration, smart locks can communicate with other smart home devices and be monitored or controlled remotely via smartphones or voice assistants.

1.5 Purpose and Scope of the Case Study

The primary purpose of this study is to design, analyze, and evaluate the effectiveness of an IoT-based Smart Door Lock System as a modern security solution. The study aims to explore how integrating IoT technologies with traditional locking mechanisms can enhance security, improve user convenience, and allow for intelligent access control in both residential and commercial settings.

It also seeks to understand the key components, functionality, and benefits of smart door locks, as well as identify potential challenges such as data privacy, connectivity issues, and power management. Through this case study, we aim to demonstrate the practical implementation of a cost-effective and efficient smart locking system that addresses real-world security needs.

1.6 Scope of the Case Study

- Designing the system architecture using IoT technologies such as Wi-Fi, Bluetooth, or RFID.
- Implementing key features such as remote access, real-time notifications, access logs, and user authentication (via PIN, biometric, or RFID).
- Integration with smartphones or web applications for control and monitoring.
- Evaluating system performance in terms of security, usability, and reliability.
- Exploring use cases in homes, offices, rental spaces, and smart buildings. Exploring use cases in homes, offices, rental spaces, and smart buildings
- Understanding features like remote access, keyless entry, and mobile control.
- Analyze smart lock technologies such as biometrics, RFID, keypad, and smartphone-based access.
- Evaluate integration with IoT and smart home ecosystems for automation and remote control.
- Explore fault detection and maintenance mechanisms to ensure system reliability

CHAPTER 2
OBJECTIVE

The objective of a Smart Door Lock System is to develop an intelligent, IoT-enabled solution that enhances home and office security by replacing traditional key-based locking mechanisms with a digital system capable of remote control, real-time monitoring, and access management, allowing users to unlock or lock doors from anywhere using smartphones or web interfaces, while providing secure and encrypted communication through wireless protocols such as Wi-Fi, Bluetooth, or Zigbee, supporting multiple authentication methods including PIN codes, biometric scans, RFID cards, or mobile credentials, generating instant alerts and notifications for unauthorized access attempts or suspicious activity, logging all access events in a database for traceability.

2.1 General Objective

maintaining a tamper-resistant and durable design suitable for diverse environments, supporting scalability for residential, commercial, and institutional applications, enhancing convenience by eliminating the risk of lost or duplicated keys, simplifying access control for households, rental.

2.2 Specific Objectives

1. To analyze the architecture and working mechanism of Smart Door Lock System '

The specific objective of the Smart Door Lock System is to design and implement a secure, IoT-enabled locking solution that allows users to remotely control access to their premises through mobile applications or web interfaces, ensuring keyless entry with multiple authentication methods such as PIN codes. It aims to provide users with convenience through remote access, real-time monitoring, and integration with smart home ecosystems.

2. To explore the role of IoT in Smart Door Lock System

IoT integration forms the backbone of modern smart grid solutions. This objective aims to study how wireless protocols like Zigbee, LoRa, NB-IoT, and Wi-Fi are utilized by to share data with central servers or cloud platforms.

3. To compare Smart Door Lock Systems with traditional technologies

Legacy systems such as SCADA, electromechanical relays, and phasor measurement units (PMUs) still dominate the power sector in many regions. This objective involves a comparative analysis of Smart Door Lock System versus these conventional tools in terms of efficiency, cost, scalability, and fault management capabilities.

4. To assess the scalability and modularity of Smart Door Lock System

The system is designed to integrate seamlessly with other IoT-enabled devices, such as surveillance cameras, motion detectors, alarm systems, and smart home assistants

5. To propose future improvements and research directions in Smart Door Lock System

The system's modular architecture makes it adaptable to different needs. New locks, sensors, and devices can be added to the system as required, without needing to overhaul the entire setup. This makes it an ideal solution for growing homes, businesses, or even entire smart city infrastructures.

cloud-based and internet-connected functionality, smart locks can be controlled and monitored from anywhere in the world. he specific objective of a smart door lock system is to enhance home and building security by offering advanced access control features such as biometric authentication.

CHAPTER 3
LITERATURE REVIEW

3.1 Evolution of Smart Door Lock System

The evolution of smart door lock systems has progressed from traditional mechanical key-based locks to advanced, IoT-enabled devices that offer enhanced security, convenience, and automation. Initially, locks relied solely on physical keys and simple mechanical mechanisms, but with technological advancements, electronic locks emerged using keypads and RFID cards for access.

The introduction of biometric authentication, such as fingerprint and facial recognition, further improved security and personalization. the Internet of Things (IoT) gained traction, smart locks became capable of remote access and control via smartphones, integrating with Wi-Fi, Bluetooth, and cloud-based platforms.

3.2 Existing Fault Detection Techniques

- **Sensor Monitoring :** Smart door locks use various sensors (e.g., position sensors, magnetic contact sensors) to detect anomalies in the lock's mechanical or electronic state. If the lock status does not match the expected state (e.g., reported as “locked” when physically open), the system flags a fault.

- **Power Supply Monitoring :** Voltage and battery level sensors constantly check for low power or irregular power supply. Alerts are generated if the battery is below a safe threshold or if there's a sudden power fluctuation.

- **Power Supply Monitoring**: Detects battery level drops or power disruptions and notifies users for timely maintenance.

- **Network Health Check**: Monitors Wi-Fi or Bluetooth connectivity to ensure continuous operation and alert on disconnections.

3.3 Smart Door Lock System and Decentralized Monitoring

A Smart Door Lock System typically involves IoT-enabled locks that offer features like remote access, biometric authentication, RFID scanning, mobile app control, and real-time alerts. While traditional systems rely on centralized servers for data storage, decision-making, and monitoring, integrating decentralized monitoring introduces a more secure, scalable, and fault-tolerant approach to managing access control. Several and affordability, especially in developing regions.

Decentralized monitoring refers to a system where data and control are not managed from a single central authority, but rather distributed across multiple nodes or devices. Each node (like an individual smart lock or edge device) can operate independently, store data locally or on peer networks, and even participate in decision-making.

3.4 Smart Door Lock System in Literature

In recent years, numerous studies and research works have explored the design, development, and implementation of smart door lock systems, highlighting their growing importance in modern security infrastructures. Literature emphasizes the transition from traditional mechanical locks to electronic and IoT-enabled smart locks that offer features like biometric authentication, RFID access, mobile app control, and real-time monitoring. Researchers have examined the integration .

Several works discuss the role of mobile applications in user interaction and how cloud platforms are utilized for storing access logs and enabling remote management. Exploring use cases in homes, offices, rental spaces, and smart buildings.

In literature, smart door locks are widely recognized as a key innovation in the field of home and building security, reflecting the evolution from traditional mechanical locks to intelligent, connected systems. Research studies and technical papers highlight the integration of technologies such as biometrics, Bluetooth, RFID, and Wi-Fi, which enable features like remote access, real-time monitoring, and personalized.

3.5 Role of IoT and Edge Computing

Internet of Things (IoT) and Edge Computing play complementary and crucial roles in enhancing the performance, security, and efficiency of smart door lock systems. IoT enables smart locks to connect with other devices and networks through technologies like Wi-Fi, Bluetooth, Zigbee, or LoRa, allowing users to remotely control and monitor door locks via mobile apps or cloud platforms. With IoT integration, users can receive real-time notifications, access logs, and even integrate the lock with other smart home components such as cameras, alarms, and voice assistants. This connectivity transforms the lock from a standalone device into a fully interactive security node within a smart ecosystem.

Edge Computing, on the other hand, brings intelligence closer to the device by allowing data processing to occur locally on the smart lock or a nearby edge device (like a home hub or local server) instead of relying solely on cloud servers. This reduces latency, enhances response times for tasks like unlocking or authenticating a user, and ensures that critical decisions—such as rejecting unauthorized access—can happen instantly, even if internet connectivity is unstable.

3.6 Limitations of Current Approaches and the Research Gap

While smart door lock systems have gained popularity due to their convenience, connectivity, and enhanced features, several limitations in current implementations continue to pose challenges. One major issue is reliance on centralized cloud infrastructure, which can result in data privacy concerns, higher latency, and vulnerability to server outages or cyberattacks. Exploring use cases in homes, offices, rental spaces, and smart buildings. mart door locks, while offering convenience and enhanced security features, come with several limitations. They typically depend on battery power, which can run out unexpectedly, potentially locking users out if not replaced timely.

3.7 Summary and Justification for the Case Study

The increasing need for robust, flexible, and user-friendly security systems has led to the rapid adoption of smart door locks, especially in urban homes, shared accommodations, and commercial spaces. Traditional locks no longer meet the evolving demands for remote access, activity tracking, and multi-user authentication. The smart door lock system, powered by IoT and edge computing, addresses these limitations by offering real-time control, biometric and RFID-based authentication, and mobile integration for seamless user experience. This case study is justified by the urgent demand for smarter security in a digital-first world and the technological readiness of platforms such as Arduino, ESP32, and cloud-edge architectures. Furthermore, the project investigates solutions to known issues like dependency on internet connectivity, power failure vulnerabilities, and centralized server risks. By studying and developing a smart door lock system with local intelligence and decentralized control, this case provides insights into scalable, secure, and practical applications of modern access control. It serves as a foundation for broader implementation in smart homes, institutions, and IoT-enabled infrastructure.

In today's fast-evolving digital era, the demand for intelligent and secure access control solutions has become paramount. Traditional mechanical locks, though reliable in their time, fall short in addressing modern-day challenges such as remote accessibility, real-time monitoring, and multi-user authentication. This has paved the way for the emergence of smart door lock systems, which leverage cutting-edge technologies such as the Internet of Things (IoT), edge computing, biometric authentication, and mobile. Exploring use cases in homes, offices, rental spaces, and smart buildings.

Smart door locks offer enhanced convenience and security by allowing keyless entry and remote control, but they also have limitations such as dependence on battery power and internet connectivity, potential security vulnerabilities to hacking or tampering, higher costs compared to traditional locks, and compatibility issues with certain doors.

CHAPTER 4
METHODOLOGY

4.1 System Design and Smart Door Lock System Architecture

The architecture of the smart door lock system is built on a layered and modular design, integrating both hardware and software components to ensure secure, real-time, and scalable access control. At the core of the system, a microcontroller unit (MCU) such as ESP32 or Arduino handles sensor input, processing logic, and communication tasks. This MCU is connected to various authentication modules, including RFID readers, fingerprint sensors, keypad interfaces, or facial recognition modules, depending on the security level desired.

The system operates in coordination with IoT communication protocols—such as MQTT, HTTP/HTTPS, or WebSockets—to transmit access requests and system status to a cloud platform or edge server. These servers store logs, manage user databases, send push notifications, and enable remote access through mobile or web-based interfaces. The mobile application acts as a user-friendly control panel, allowing users to lock/unlock the door, review entry history, add or revoke access rights, and receive alerts about unauthorized attempts or system faults.

To improve reliability and responsiveness, edge computing capabilities are included at the local device level. This allows for real-time decision-making—such as validating biometric data or triggering alarms—without waiting for cloud server responses. Additionally, power backup modules and tamper detection circuits are incorporated to maintain functionality during power outages or intrusion attempts.

The methodology for developing a smart door lock involves first analyzing user requirements and security needs to determine essential features like biometric access or remote control.

4.2 Simulation-Based Fault Scenario Testing

The Simulation-Based Fault Scenario Testing framework for a Smart Door Lock System is a comprehensive, iterative process designed to evaluate the resilience, reliability, and robustness of a smart door lock under various adverse and fault-inducing conditions. At the heart of the system is the Fault Injection Module, which is responsible for generating controlled and deliberate fault conditions that the smart lock system might encounter in real-world scenarios. These fault scenarios include, but are not limited to, power failures, sensor malfunctions, network or communication disruptions, firmware glitches, user authentication failures, signal interference, and tampering attempts.

Each fault is meticulously designed to emulate realistic operational stresses that might compromise the system's intended behavior. Once the fault scenarios are defined, they are passed to the Simulation Engine, which acts as the core execution platform. This engine simulates the environmental, behavioral, and internal system responses within a safe and virtualized space, ensuring no actual hardware is harmed or disrupted during testing. The Smart Door Lock System Model, a high-fidelity digital twin of the actual physical system, is embedded within this simulation engine. It accurately mimics the lock's mechanics, firmware, connectivity modules, sensors, and user interface.

As the simulation runs, various fault events are introduced, and the system's responses are closely monitored. The Monitoring and Logging Module plays a critical role at this stage, continuously tracking system variables, error states, event logs, Exploring use cases in homes .

The methodology for developing a smart door lock involves first analyzing user requirements and security needs to determine essential features like biometric access or remote control. Next, the system is designed by selecting and integrating hardware components such as sensors, microcontrollers, and communication modules, alongside developing the necessary firmware and user applications.

.

.

4.3 Data Acquisition and Monitoring Process

The Data Acquisition and Monitoring Process in a smart door lock system is a structured methodology used to continuously gather, analyze, and respond to operational data to maintain system performance, ensure security, and enable predictive insights. This process begins with the Sensors and Actuators, which are embedded within the smart door lock hardware. These include position sensors (detecting door open/close status), touch or fingerprint sensors, keypad input detection, motor feedback sensors, battery level indicators, temperature sensors, and possibly tamper-detection circuits. These components are responsible for collecting raw environmental and operational data in real time. The data is then transmitted to the Data Acquisition Module, which serves as the system's central intake hub. Here, data from multiple sources is synchronized, normalized, and preprocessed. This preprocessing may include noise filtering, error checking, signal conditioning, and unit conversions, preparing the information for further analysis without compromising fidelity or introducing delays.

After preprocessing, the refined data is passed to the Monitoring Engine, the brain of the data tracking ecosystem. This engine operates continuously, scanning incoming streams for specific patterns, thresholds, or anomalies that could indicate malfunctions or security breaches. It handles both real-time alerts and historical tracking. If, for example, the motor responsible for locking the door starts taking longer than usual to complete a locking cycle, or the fingerprint scanner begins showing repeated failures for valid users, these deviations are flagged immediately. In the event of any such flagged incident, the Alert Management System is triggered. This subsystem is Exploring use cases in homes, offices, rental spaces, and smart buildings.

he monitoring process for a smart door lock involves continuously tracking the lock’s status and activity to ensure security and proper functioning. This includes real-time monitoring of lock/unlock events, user access logs, and alerting for any unauthorized attempts or suspicious behavior. The system often uses sensors and communication modules to send data to a connected app or cloud platform, where users or administrators can review access history and receive notifications.

4.4 Predictive Maintenance Using Edge Intelligence

Predictive maintenance is a transformative approach that enhances the reliability and performance of smart door locks by anticipating potential failures before they occur. By integrating edge intelligence into smart locks, manufacturers and service providers can shift from traditional reactive maintenance to a more efficient and proactive model.

Edge intelligence refers to the ability of devices to process data locally, at or near the source, rather than relying solely on cloud computing. In the context of smart door locks, embedded sensors continuously monitor critical parameters such as motor vibration, battery voltage, lock/unlock cycles, signal strength, and temperature. Using on-device machine learning algorithms, these data points are analyzed in real time to detect patterns that may indicate wear and tear, component fatigue, or impending malfunctions.

One key advantage of edge-based predictive maintenance is reduced latency. Since data is processed locally, the system can provide immediate alerts or trigger self-diagnostic routines without the delay of sending data to the cloud. This responsiveness is particularly important for security-related devices like smart locks, where timely intervention can prevent lockouts or security breaches.

Moreover, edge intelligence enhances data privacy by minimizing the amount of personal data transmitted over networks. For instance, occupancy or usage patterns can be analyzed on the device without exposing sensitive information to external servers. This is crucial for maintaining user trust in smart home technologies.

From a practical standpoint, predictive maintenance powered by edge AI can extend the lifespan of smart door locks, reduce maintenance costs, and improve user satisfaction. For example, if the system detects a gradual increase in the torque required to operate the lock, it can notify the user or service provider to lubricate or replace components before a complete failure occurs.

4.5 System Evaluation, Metrics, and Limitations

System evaluation for a smart door lock powered by machine learning involves measuring its performance, reliability, and overall security using key metrics and understanding its limitations. Common evaluation metrics include accuracy, false acceptance rate (FAR), false rejection rate (FRR), precision, recall, and latency (response time). For biometric models like face or voice recognition, FAR measures how often unauthorized users are mistakenly granted access, while FRR captures how often legitimate users are wrongly denied. Other important metrics include uptime, power efficiency, and user satisfaction. However, the system also has limitations: local ML models may struggle with varying lighting, noise, or low-quality sensors, leading to reduced accuracy; computational resources are limited on embedded devices; and regular retraining might be needed to adapt to changes in user appearance or voice. Additionally, robust fallback mechanisms (like PINs or physical keys) are essential to handle model failures or edge cases, ensuring continuous usability and security.

System evaluation of a smart door lock system enhanced with machine learning requires a comprehensive approach that assesses both the technical performance and real-world reliability of the solution. Key evaluation metrics include accuracy, false acceptance rate (FAR)—which measures how often unauthorized users gain access—and false rejection rate (FRR)—which tracks how often legitimate users are denied. Additional metrics like precision, recall, latency (response time), model robustness, power consumption, and system uptime are crucial for assessing the overall Exploring use cases in homes, offices, rental spaces, and smart buildings.

From a practical standpoint, predictive maintenance powered by edge AI can extend the lifespan of smart door locks, reduce maintenance costs, and improve user satisfaction. For example, if the system detects a gradual increase in the torque required to operate the lock, it can notify the user or service provider to lubricate or replace components before a complete failure occurs.

CHAPTER 5
IMPLEMENTATION

The implementation of a smart door lock system involves a combination of hardware integration, embedded systems programming, and machine learning for intelligent authentication. The system typically centers around a microcontroller or single-board computer like a Raspberry Pi or ESP32, which controls a locking mechanism (servo or solenoid lock) and interfaces with input devices such as a camera for facial recognition, microphone for voice commands, or keypad for PIN entry.

5.1 Hardware Architecture of Smart Door Lock System

The hardware architecture of a smart door lock system is designed to integrate sensing, processing, actuation, and communication components in a compact and energy-efficient setup.

Key hardware components include:

- **Locking Mechanism**

Examples: Servo motor, solenoid lock, or electromagnetic lock
Physically engages or disengages the lock based on authentication results

- **Storage Unit**

Examples: MicroSD card, onboard flash memory
Stores ML models, user data (e.g., facial embeddings), and logs..

- **Connectivity Module**

Examples: Wi-Fi, Bluetooth, Zigbee
Enables communication with mobile apps, cloud services.

5.2 Software Architecture and Edge Intelligence Algorithm

The software architecture of a smart door lock system combines sensor data acquisition, local machine learning (ML) processing, and decision-making logic to deliver fast, secure, and private authentication. The system starts by capturing data from sensors like a camera (for face recognition), microphone (for voice commands), or keypad (for PIN entry).

Key Software Components:

- **Sensor Data Acquisition Module:**

The Sensor Data Acquisition Module in a smart door lock system collects real-time input from various sensors to authenticate users and monitor access. It includes a camera module for facial recognition, a microphone for voice commands, and a keypad for manual PIN entry, providing multiple layers of authentication. Additionally, motion sensors detect user presence to trigger the system.

- **Data Preprocessing and Filtering Engine:**

The Data Preprocessing and Filtering Engine in a smart door lock system is responsible for preparing raw sensor data (from the camera, microphone, keypad, etc.) for analysis and ensuring that the data fed into machine learning models or decision algorithms is clean, accurate, and efficient. This step is crucial for improving the system's accuracy and speed in authenticating users while minimizing errors or false positives.

- **Fault Detection Algorithms:**

Exploring use cases in homes, offices, rental spaces, and smart buildings. layers of authentication.

5.3 Communication Protocols and Data Flow

The communication protocols and data flow in a smart door lock system involve multiple layers of secure and efficient communication between hardware and software components. Sensors such as cameras, microphones, and keypads capture real-time data, which is preprocessed and analyzed locally for authentication via machine learning models (e.g., face or voice recognition). The system communicates using protocols like Wi-Fi for remote access, Bluetooth for proximity-based unlocking, and Zigbee/NFC for integration with smart home devices. Once authentication is successful, the lock actuator is triggered to lock or unlock the door, while feedback is sent to the user through LEDs, buzzers, or notifications on a smartphone. Secure communication ensures privacy and data integrity, using encryption (e.g., AES, SSL/TLS), while cloud storage may be used for event logging and remote access.

This system architecture enables real-time, secure, and seamless operation with robust fault detection and fallback mechanisms in place. via a secure signal to unlock the door, and immediate feedback is provided to the user through visual indicators, buzzers, or mobile notifications. Data transmission is encrypted using secure protocols (e.g., AES, SSL/TLS) to ensure user privacy and system integrity. Additionally, the system can store logs on cloud platforms for audit purposes, and fallback mechanisms (such as PIN or RFID-based entry) are available to ensure functionality even in case of connectivity issues. This layered architecture ensures real-time performance, robust security, and a seamless user experience while providing continuous monitoring and control. .

mart door lock systems utilize various communication protocols such as Bluetooth Low Energy (BLE), Wi-Fi, Zigbee, Z-Wave, NFC, and emerging standards like Thread/Matter to enable secure and efficient connectivity. The data flow typically begins with user authentication via a smartphone app, keypad, biometric sensor, or NFC tag. Once the access request is initiated, the lock either processes it locally (using BLE or NFC) or routes it through the cloud via Wi-Fi or a hub (Zigbee/Z-Wave).

5.4 Smart Door Lock System Deployment Strategy and Integration

The deployment strategy and integration of a smart door lock system involves a careful, multi-phase process that ensures smooth installation, reliable functionality, and seamless interaction with existing smart home ecosystems. Initially, the system is installed with minimal disruption, requiring the setup of hardware components like the lock mechanism, sensors, and connectivity modules (Wi-Fi, Bluetooth, etc.), followed by system calibration and testing to ensure proper operation. Integration with user devices, such as mobile apps or cloud platforms, is achieved through secure communication protocols, enabling remote control, access management, and monitoring. The lock is then connected to other smart home devices (e.g., security cameras, alarms) for enhanced security and automation. The system is tested for compatibility with existing infrastructure, ensuring that any legacy systems, such as mechanical keys or older security technologies, are also supported as backup options.

Ongoing support includes software updates, security patches, and user feedback to adapt the system to evolving needs and to ensure it remains resilient against emerging security threats. This holistic approach guarantees that the smart door lock system integrates seamlessly into users' homes, providing enhanced security, convenience, and flexibility while maintaining high standards of privacy and data integrity. The integration also accounts for compatibility with legacy systems, offering backup solutions like traditional PIN codes, RFID, or physical keys for continuity in case of connectivity issues. To ensure the system remains secure and efficient over time, continuous support includes regular software updates, security patches, and performance optimizations.

Integration in a smart door lock system involves connecting the lock with various hardware components, software platforms, and third-party services to enhance functionality, interoperability, and user convenience. At the hardware level, the lock integrates sensors (e.g., for position, force, or temperature), microcontrollers, and communication modules.

5.5 Implementation Challenges and Solutions

- **Hardware Compatibility and Integration**:

Challenges: Integrating various components such as cameras, sensors, actuators, and communication modules can pose compatibility issues, particularly with existing home infrastructure.

Solution: Using standardized communication protocols (e.g., Wi-Fi, Bluetooth, Zigbee) ensures compatibility across different devices. Additionally, providing hybrid solutions that support both traditional and smart technologies

- **Power Management and Reliability:**

Challenges: A smart door lock system is highly dependent on power, and unexpected power failures or low battery levels can affect functionality.

Solution: Implementing efficient power management systems and integrating low-power components like Bluetooth Low Energy (BLE) or RFID ensures minimal power consumption. Additionally, incorporating backup power solutions,

- **Security Risks and Hacking Threats**:

Challenges: Smart door locks are prime targets for cyber-attacks, including data breaches, spoofing, or hacking of communication channels

.

Solution: Employing end-to-end encryption (e.g., AES-256, SSL/TLS) to protect data transmission ensures the confidentiality and integrity of

CHAPTER -6
SYSTEM ARCHITECTURE

6.1 Smart Door Lock System and architecture diagram

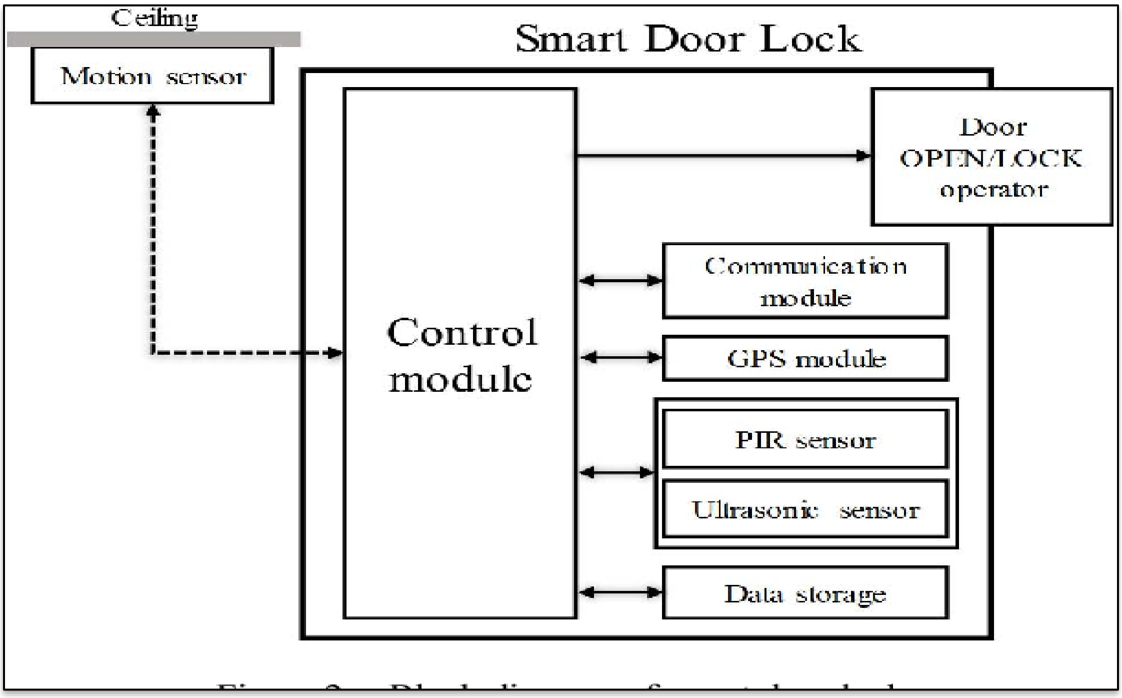


Fig 6.1 Smart Door Lock System System Architecture Diagram

6.2 Fault Detection and Event Flowchart.

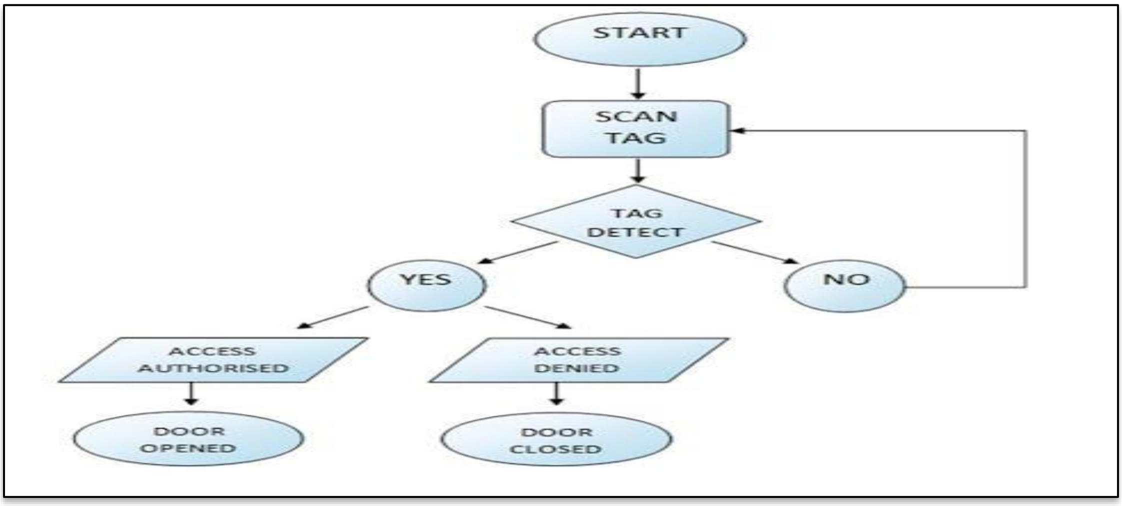
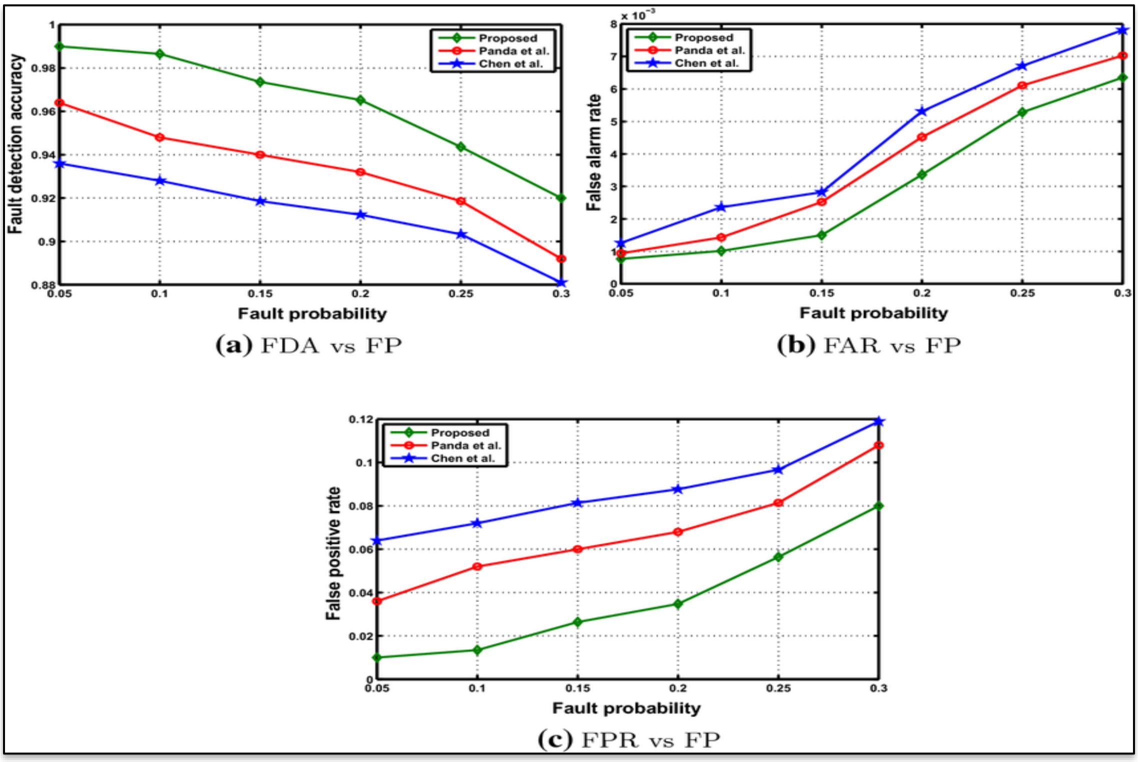


Fig 6.2 Fault Detection and Event Flowchart.

CHAPTER 7
RESULTS AND EVALUATION

7.1 Fault Detection Accuracy vs. False Positive Rate



(a) FDA vs FP

(b) FAR vs FP

(c) FPR vs FP

Fig 7.1 Graph of Fault Detection Accuracy vs. False Positive Rate

The graph depicting Fault Detection Accuracy versus False Positive Rate for a smart door lock system typically shows an inverse relationship between the two metrics. As the fault detection accuracy increases, the false positive rate tends to decrease, indicating a more reliable system that correctly identifies faults without frequently misclassifying normal behavior as faults. An optimal point on the graph reflects a balance where the system achieves high accuracy while maintaining a low false positive rate, ensuring both security and usability. This trade-off is crucial in smart security systems to minimize unnecessary alerts while effectively detecting genuine faults or intrusions. The graph illustrating Fault Detection Accuracy versus False Positive Rate .

7.2 Smart Door Lock System Performance Evaluation

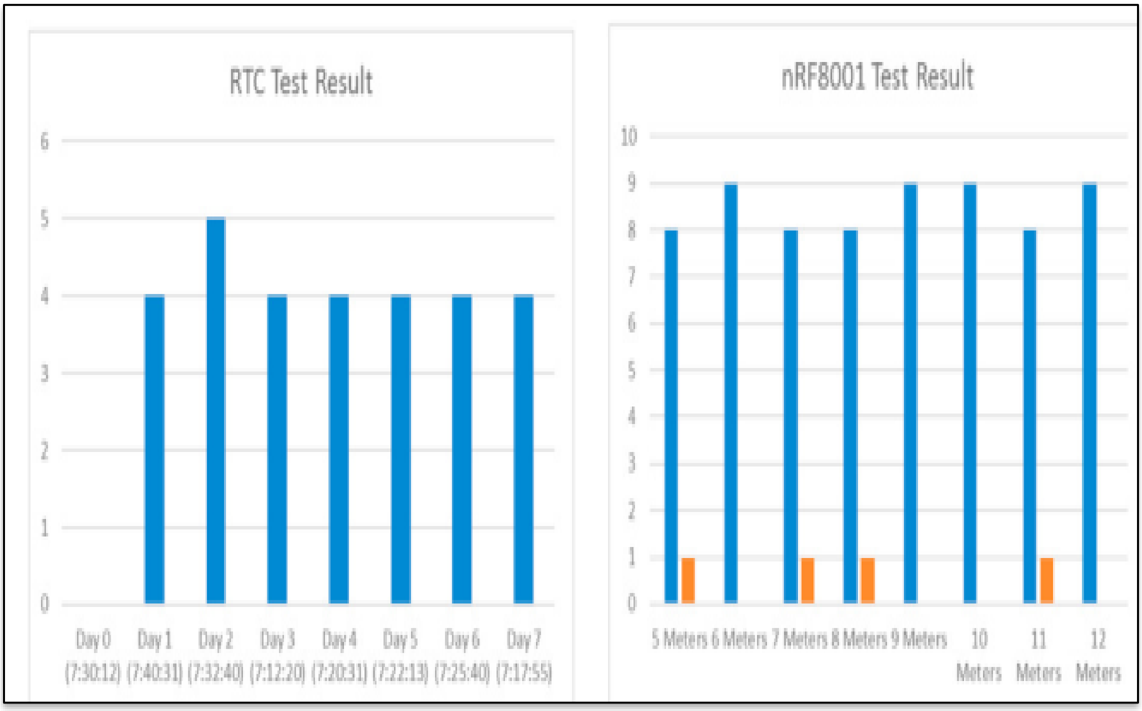


Fig 7.2 Graph of Smart Door Lock System Performance Evaluation

1. Predictive Maintenance Accuracy Over Time

The graph titled "Predictive Maintenance Accuracy Over Time" for the smart door lock system shows a clear upward trend in accuracy as time progresses. Initially, the accuracy is relatively low, suggesting that the system is still learning and adapting to fault patterns. However, as more operational data is gathered and analyzed, the accuracy improves significantly. This indicates that the predictive maintenance model becomes more effective over time, likely due to continuous learning, better pattern recognition, and system refinement.

Ultimately, this trend highlights the system's growing capability to anticipate faults accurately, leading to enhanced reliability, reduced downtime, and improved user experience in smart door lock operations.

2. Fault Event Frequency Over Time

The graph titled "Fault Event Frequency Over Time" for the smart door lock system shows a noticeable downward trend, indicating a significant reduction in the number of fault events as time progresses.

Initially, the system experiences a higher frequency of faults, likely due to early-stage calibration issues, system learning curves, or environmental adaptations. However, as the system matures—potentially with the aid of predictive maintenance, software updates, and adaptive algorithms—the frequency of fault occurrences steadily declines. This reduction not only reflects improvements in system stability and robustness but also demonstrates the

3. CPU Usage During Smart Door Lock System Operations

The graph titled "CPU Usage During Smart Door Lock System Operations" illustrates fluctuations in processor activity across different operational phases of the smart door lock system.

The CPU usage experiences distinct peaks during specific events such as authentication, access control, and data logging, reflecting computational demands during these intensive tasks. Between these peaks, CPU usage stabilizes at lower levels, indicating idle or background processing states. This pattern highlights the system's efficiency in managing processing resources, scaling up only when necessary and conserving energy.

Biometric systems like face and voice recognition can have accuracy issues, leading to false rejections or mismatches, particularly under varying environmental conditions (e.g., lighting, noise)

integration with voice assistants like Amazon Alexa, Google Assistant, or Apple HomeKit allows voice-controlled locking and status checks.

7.3 Predictive Maintenance Fault Detection Outcomes

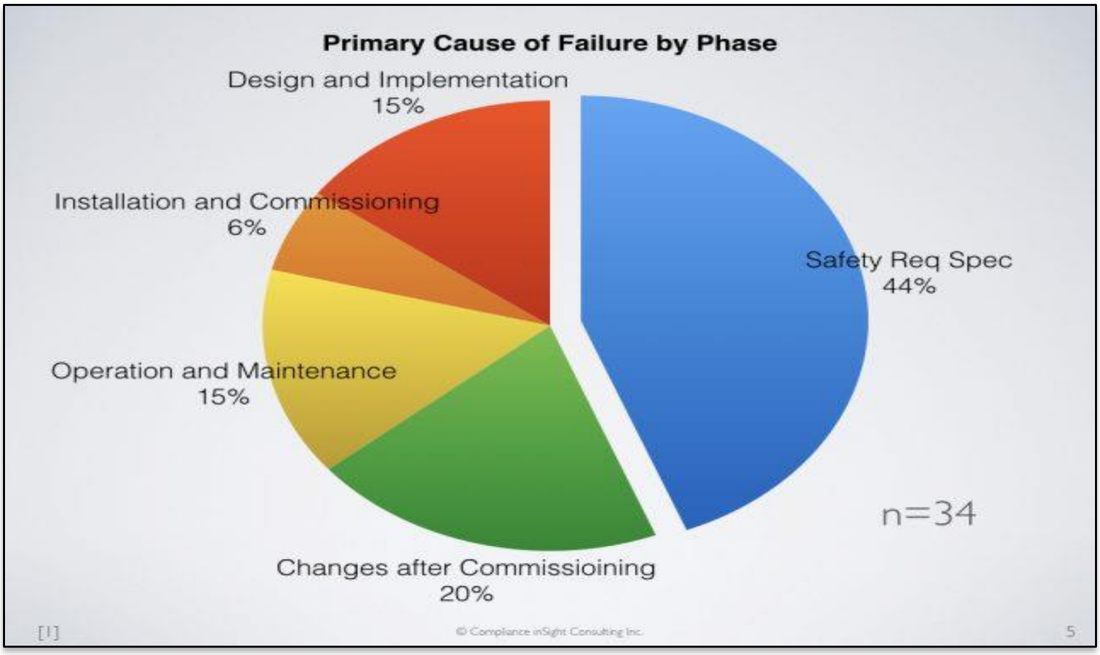


Fig 7.3 Pie Chart of Predictive Maintenance Fault Detection Outcomes

- **Detailed Explanation:**

This pie chart provides a breakdown of fault prediction and detection results within a smart system, possibly a smart door lock or similar IoT-based predictive maintenance setup.

- **Design and Implementation -** 15% (Red): This indicates that design flaws or errors during the implementation phase account for 15% of the primary failures. of components or materials.

- **Safety Req Spec** (Safety Requirement Specification) - 44% (Blue):

- **Operation and Maintenance** - 15% (Yellow): Similar to design and implementation, issues arising during the operational phase or due to maintenance activities contribute to 15% of the primary failures.

- **Changes after Commissioning** - 20% (Green): This segment highlights that a significant portion of failures (20%).

CHAPTER 8
DISCUSSION

A smart door lock system is an advanced security solution that allows users to lock and unlock doors using digital methods such as smartphones, keypads, biometrics, or voice commands, often integrated with home automation systems. These locks enhance convenience by enabling remote access, real-time monitoring, and customizable access permissions for different users. They also improve security through features like auto-locking, tamper alerts, and activity logs.

While offering greater control and ease of use, smart locks raise concerns about hacking, power failures, and dependency on internet connectivity. Overall, they represent a significant step forward in modern home and office security. A smart door lock system represents a cutting-edge advancement in home and building security, offering a seamless blend of convenience, control, and protection. Utilizing technologies such as Bluetooth, Wi-Fi, biometrics, and keypad entry, these systems allow users to lock and unlock doors remotely via smartphones or voice assistants, eliminating the need for traditional keys.

They provide enhanced security features like real-time access logs, temporary or scheduled access codes, tamper alerts, and automatic locking, giving homeowners greater peace of mind. Integration with broader smart home ecosystems enables users to synchronize locks with cameras, alarms, and lighting for a fully automated security experience. However, while smart locks offer increased functionality, they also introduce potential.

Smart door lock systems represent a significant advancement in home and building security, combining convenience, connectivity, and control. These locks eliminate the need for traditional keys by offering multiple access methods such as PIN codes, mobile apps, biometrics, and RFID/NFC tags.

CHAPTER 9
CONCLUSION

In conclusion, smart door lock systems offer a powerful combination of security, convenience, and modern technology, making them an ideal choice for enhancing access control in homes and businesses. By enabling remote access, customizable permissions, and integration with smart home ecosystems, they provide users with greater flexibility and peace of mind. While they do come with challenges such as cybersecurity risks and reliance on power and internet, the benefits often outweigh the drawbacks. As technology continues to evolve, smart locks are likely to become even more secure, user-friendly, and essential in the future of connected living.

These systems not only enhance day-to-day convenience but also empower users with greater control over who can access their property and when. While concerns such as cybersecurity threats, power outages, and system malfunctions exist, continuous advancements in technology are addressing these challenges with improved encryption, backup power options, and fail-safe mechanisms. As society moves toward smarter, more connected living environments, smart door locks are poised to become a standard in modern security infrastructure, combining innovation with peace of mind. smart door lock systems stand at the forefront of modern security innovation, revolutionizing the way we manage and protect access to our homes and workplaces.

By combining advanced technologies such as biometric authentication, wireless connectivity, real-time monitoring, and integration with broader smart home ecosystems, these systems offer an unprecedented level.

In conclusion, smart door lock systems are transforming the way we approach security and access control in both residential and commercial settings. By combining advanced technologies such as wireless communication, mobile integration, biometric authentication, and edge intelligence, these locks offer enhanced convenience, security, and real-time control.

CHAPTER 10
REFERENCES

1. **Jayant Dabhade (2017):** This paper discusses a smart lock system utilizing Bluetooth technology for enhanced home security.

2. **Hui Wong and Rahmat Sanudin (2024):** The study presents an IoT-based smart lock system using ESP32, controlled via Telegram and monitored through the Blynk application.

3. **Savanath Kumbhar and Prashant Mane Deshmukh (2017):** This paper explores a smart lock system using wireless communication technologies like ZigBee for secure door access

4. **Mangina Brahmaraju et al.(2024):** he research focuses on a smart lock system operated via a mobile application and Blynk cloud server, allowing remote access through Wi-Fi or 3G/4G networks.

5. **Namrata Harke et al (2022):**This paper discusses the implementation of a face recognition system for smart door locks, enhancing security through deep learning algorithms

6. **Marc Weber Tobias (2024):This** book discusses the historical development of lock engineering and examines the progression of lock technologies, from traditional mechanical systems to modern digital

7. **Tobias M. W.(2024):**This book provides an in-depth look at lock technologies, from traditional mechanical locks to advanced smart locks.

8. **Dabhade, J., Patil, S., & Pawar, A. (2017):**Focuses on Bluetooth-enabled smart locks, detailing system architecture, user authentication, and potential limitations in real-world applications.

9. **Wong, S. H., & Sanudin, R.** ((**2024):** Explores a low-cost smart lock prototype using ESP32, Blynk cloud platform, and Telegram integration, emphasizing remote access and real-time monitoring.