IoT Based Electronic Door Opener

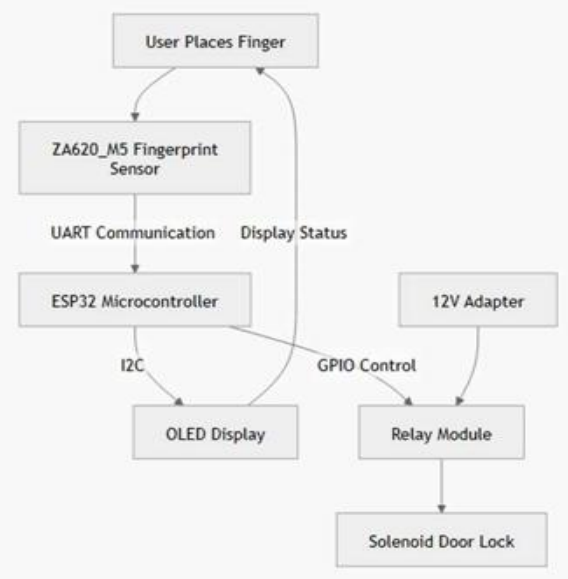
Manoj S. Chittawar[1], Kartik P. Handekar[2], Chirag D. Chaudhari[3], Tushar K. Khanke[4] Yash S. Jathade[5] Nakul R. Ambatkar[6]
[1]*Guide, Professor, Department of CSE RCERT, Chandrapur, Maharashtra, India*
[2,3,4,5,6]*Department of CSE RCERT, Chandrapur, Maharashtra, India*

***Abstract*—The IoT-Based Electronic Door Opener is a smart security system designed to provide secure, convenient, and remote-controlled access to homes, offices, and other restricted areas. The system uses Internet of Things (IoT) technology to allow users to control and monitor door access through smartphones or other smart devices. It replaces traditional locking mechanisms with an automated electronic system that enhances security and reduces manual effort. The project consists of a microcontroller, electronic locking mechanism, wireless communication module. Authorized users can unlock or lock the door remotely using an internet connection. The system can also provide real-time notifications, access logs, and authentication features to improve safety and monitoring.**

I. INTRODUCTION

The IoT-Based Electronic Door Opener is a smart automation system designed to provide secure and efficient access control through electronic and internet enabled technologies. The system allows users to lock or unlock doors remotely using smartphones or other smart devices. By integrating a microcontroller, electronic locking mechanism, sensors, and wireless communication modules, the project enhances both security and user convenience.

The main objective of this project is to develop a low cost, reliable, and user-friendly smart door opening system that reduces manual effort and improves safety. The system can also include advanced authentication methods such as password verification, RFID cards, or fingerprint recognition for enhanced protection. Real-time monitoring and notification features further increase the effectiveness of the system. This project demonstrates the practical application of IoT in home automation and security systems. It provides a modern solution for access management and contributes to the growing field of smart technology by offering improved control, flexibility, and efficiency in everyday life.



II. METHODOLOGY

The methodology of the IoT-Based Electronic Door Opener involves designing and implementing a smart access control system using IoT technology, electronic components, and wireless communication. The complete process is divided into several stages to ensure proper functioning, security, and reliability of the system.

1. Requirement Analysis The first step involves identifying the requirements of the system such as secure access control, remote operation, real-time monitoring, and user convenience. The necessary hardware and software components are selected based on system requirements and project objectives.

2. System Design
A system architecture is designed to integrate all components including the microcontroller, electronic lock, sensors, Wi-Fi module, and mobile application. The design ensures smooth communication between the hardware and the user interface.

3. Hardware Implementation The hardware components are assembled and connected according to the circuit design. The main components include: Microcontroller for processing and control

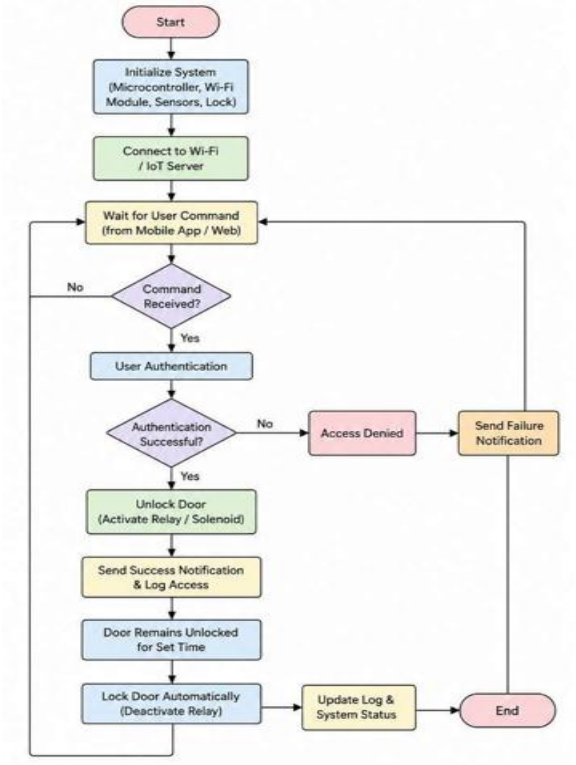
- Electronic door lock mechanism
- Wi-Fi or Bluetooth communication module
- Power supply unit
- Sensors or authentication modules

(RFID/Fingerprint/Password keypad) The electronic lock is connected to the microcontroller, which controls door opening and closing operations based on user authentication. 4. Software Development Programming is carried out using embedded programming languages to control the microcontroller and communication modules. A mobile application or web interface is developed to allow users to operate the door remotely. Authentication and access control logic are implemented to improve security.

5. IoT Integration
The system is connected to the internet using a wireless communication module. This enables users to control and monitor the door from remote locations through smartphones or smart devices. Real-time notifications and access logs can also be generated.

6. Testing and Verification The complete system is tested under different conditions to verify proper operation, response time, connectivity, and security performance. Any hardware or software errors identified during testing are corrected to improve system reliability.

7. Final Deployment
After successful testing, the system is installed and demonstrated in a real-time environment. The final implementation ensures secure, efficient, and convenient door access management.



FLOW CHART

III. IMPLEMENTATION DESIGN

Implementation Design
The implementation design of the IoT-Based Electronic Door Opener focuses on integrating hardware and software components to create a secure and automated door access system. The system is designed to provide remote access, authentication, and real-time monitoring using IoT technology.

1. Hardware Design
The hardware section consists of the following main components:
a) Microcontroller
The microcontroller acts as the central processing unit of the system. It controls all operations such as receiving commands, processing authentication, and activating the electronic lock. b) Wi-Fi Module
The Wi-Fi module enables internet connectivity between the door opener system and the user's smartphone or web application. It allows remote communication and control. c) Electronic Door Lock
An electronic lock or solenoid lock is used to physically lock and unlock the door. The lock is

controlled through relay signals generated by the microcontroller.

d) Relay Module
The relay module acts as a switching device between the microcontroller and the electronic lock. It helps control high-voltage components safely. e) Authentication Unit
The authentication unit may include:
- Password keypad
- RFID reader
- Fingerprint sensor

These components verify the identity of authorized users before granting access. f) Power Supply
A regulated power supply is used to provide stable voltage to all electronic components in the system.

2. Software Design
The software implementation includes embedded programming and IoT communication protocols.
a) Embedded Programming
The microcontroller is programmed using embedded C/C++ or Arduino IDE to:
- Read user inputs
- Process authentication
- Control door locking mechanism
- Communicate with IoT servers

b) Mobile Application / Web Interface
A mobile app or web dashboard is developed to:
- Send lock/unlock commands
- Monitor door status
- Receive notifications
- View access logs

c) IoT Cloud Integration
Cloud services are used to store user data, access history, and notifications. The cloud platform enables remote monitoring and real-time communication.

3. Working Process
1. The system starts and connects to the Wi-Fi network.
2. The user sends a command through the mobile application or authentication device.
3. The microcontroller verifies the user credentials.
4. If authentication is successful, the relay activates the electronic lock to open the door.
5. Access details are stored in the cloud database.
6. After a predefined time, the system automatically locks the door again.
7. If authentication fails, access is denied and a notification may be sent to the user.

4. Security Features
- Password or biometric authentication
- Remote monitoring
- Access logging
- Automatic locking system
- Unauthorized access alerts

5. Advantages of the Design
- Improved security and safety
- Remote accessibility
- Reduced manual operation
- Real-time monitoring
- Easy integration with smart home systems The implementation design ensures that the system operates efficiently, securely, and reliably while providing modern smart access control functionality.

IV. LITERATURE SURVE

I. Literature Survey
The rapid advancement of Internet of Things (IoT) technology has significantly improved the field of home automation and smart security systems. Traditional locking mechanisms are gradually being replaced by intelligent electronic access systems that provide better security, remote accessibility, and user convenience. Several researchers and developers have proposed different smart door lock systems using wireless communication and embedded technologies.
Many existing systems use microcontrollers such as Arduino, Raspberry Pi, and NodeMCU to control electronic door locks. These systems commonly integrate Wi-Fi, Bluetooth, RFID, fingerprint sensors, and mobile applications to provide secure authentication and remote monitoring features. IoTbased door security systems are widely appreciated for their ability to enhance safety while reducing manual effort.
Research studies have shown that RFID-based door access systems are effective in providing fast and reliable authentication. However, RFID cards may be lost or duplicated, which creates security concerns. To overcome these limitations, biometric authentication systems such as fingerprint recognition have been introduced. Fingerprint-based systems provide higher

security because biometric data is unique for each user. Several smart door lock systems also use mobile applications connected through cloud platforms. These systems allow users to lock or unlock doors remotely, receive real-time notifications, and maintain access logs. Cloud integration improves monitoring and management but requires stable internet connectivity for efficient operation.

Recent developments in IoT security systems focus on combining multiple authentication methods such as password verification, OTPs, fingerprint scanning, and facial recognition to increase reliability and prevent unauthorized access. Researchers have also emphasized the importance of encryption and secure communication protocols to protect user data from cyber threats.

Based on the literature survey, it is observed that IoTbased electronic door opener systems provide an efficient, secure, and user-friendly solution for modern access control. The proposed system aims to combine remote accessibility, automation, and secure authentication into a low-cost and reliable smart door opener solution suitable for homes, offices, and smart environments.

In recent years many implementations add cloud storage (Firebase, custom cloud DBs, or commercial SaaS) to enable centralized access, scalability, remote monitoring, and integration with payroll/HR systems.

Cloud integration also enables multi-site deployments and real-time dashboards for administrators.

1. Sensor & edge-hardware choices. Many prototypes use low-cost optical/ capacitive fingerprint modules (R305, GT-511, ZAseries) paired with microcontrollers (ESP8266/ESP32, Arduino) to capture templates and transmit events via Wi-Fi/ MQTT/HTTP. Edge choices balance cost, latency, and template extraction capabilities.
2. Template storage vs. raw images. Standard practice stores fingerprint templates (feature descriptors) rather than raw images to reduce storage and privacy risk; enrolment and matching may be done locally (on device) or in the cloud. Hybrid approaches buffer events locally and sync templates/records to the cloud.
3. Cloud backends & real-time sync. Google Firebase is a common choice in prototypes for its realtime DB and auth; commercial deployments use dedicated cloud HR platforms with secure APIs. Offline caching + eventual synchronization is a common design to handle intermittent connectivity. SSRN+1
4. Security & privacy controls. Literature stresses encryption-in-transit, secure storage, access control, and consent/notice for employee biometrics. Recent regulatory and watchdog actions highlight legal risk when biometric data is collected without adequate safeguards.

V. RESULTS AND DISCUSSIONS

Results and Discussions

The IoT-Based Electronic Door Opener system was successfully designed and implemented to provide secure and automated door access control. The system was tested under different operating conditions to evaluate its performance, reliability, and security features.

1. System Performance

The implemented system was able to successfully perform the following operations:

- Connect to the Wi-Fi network and IoT platform
- Receive lock and unlock commands from the mobile application
- Authenticate users through the selected security method
- Control the electronic door lock accurately
- Automatically lock the door after a predefined time
- Send notifications and maintain access logs The response time of the system was fast and reliable, providing smooth communication between the hardware and the mobile application.

2. Authentication Accuracy

The authentication mechanism effectively prevented unauthorized access. Authorized users were able to access the system successfully, while invalid credentials resulted in access denial. The use of IoT technology improved security by enabling real-time monitoring and user verification.

3. Remote Access Functionality

The remote access feature allowed users to control the door from different locations using internet connectivity. This increased convenience and flexibility compared to traditional locking systems. Notifications regarding successful and failed access attempts were also received in real time.

4. Security Analysis

The implemented system provided enhanced security through:

- User authentication
- Automatic locking mechanism
- Real-time monitoring
- Access logging
- Unauthorized access alerts

The combination of electronic locking and IoT communication reduced the risk of manual security failures.

5. Discussion

The developed smart door opener system demonstrated that IoT technology can be effectively used in modern security and home automation applications. The project achieved its objective of creating a low-cost, efficient, and user-friendly access control system. However, the system depends on internet connectivity for remote operations. Network interruptions may affect communication between the user and the device.

Future improvements can include:

- Facial recognition authentication
- Voice control integration
- Backup power supply
- Enhanced cloud security
- Mobile application improvements Overall, the project successfully improved door security, convenience, and automation while demonstrating the practical implementation of IoT in smart access systems.

VI. CONCLUSION

The IoT-Based Electronic Door Opener system was successfully designed and implemented to provide a smart, secure, and automated access control solution. The project demonstrated the effective use of IoT technology in improving home and office security through remote monitoring and electronic door control.

The system was capable of performing secure authentication, remote lock and unlock operations, automatic door locking, and real-time notification services. The integration of hardware components such as the microcontroller, electronic lock, relay module, and wireless communication module ensured smooth and reliable system performance.

The project achieved its main objectives of enhancing security, reducing manual effort, and increasing user convenience. Compared to traditional locking systems, the proposed smart door opener provides better flexibility, automation, and remote accessibility. The system also supports future expansion with advanced technologies such as facial recognition, voice assistants, and cloud-based security features.

Although the system depends on internet connectivity for remote operations, it still provides an efficient and cost-effective solution for modern smart security applications. Overall, the project proves that IoT-based automation can play an important role in developing intelligent, reliable, and user-friendly security systems for smart homes and organizations.

REFERENCE

References Books

[1] Raj Kamal, Embedded Systems: Architecture, Programming and Design, Tata McGraw-Hill Education.

[2] Muhammad Ali Mazidi, Janice Gillispie Mazidi, and Rolin D. McKinlay, The 8051 Microcontroller and Embedded Systems, Pearson Education.

Websites

[1] Arduino Official Website – https://www.arduino.cc

[2] Electronics For You – https://www.electronicsforu.com

[3] Instructables – https://www.instructables.com

Journals / Research Articles

[1] IEEE Research Papers on Smart Door Lock Systems and Home Automation.

[2] Research Articles on IoT-Based Security and Access Control Systems.

[3] International Journal of Advanced Research in Computer Science and Software

[4] Engineering (IJARCSSE) – Articles related to IoT security applications.

[5] International Journal of Engineering Research & Technology (IJERT) – Research papers on smart door opener systems and embedded security solutions.

[6] IEEE Internet of Things Journal – Articles on IoT-enabled smart home security systems.