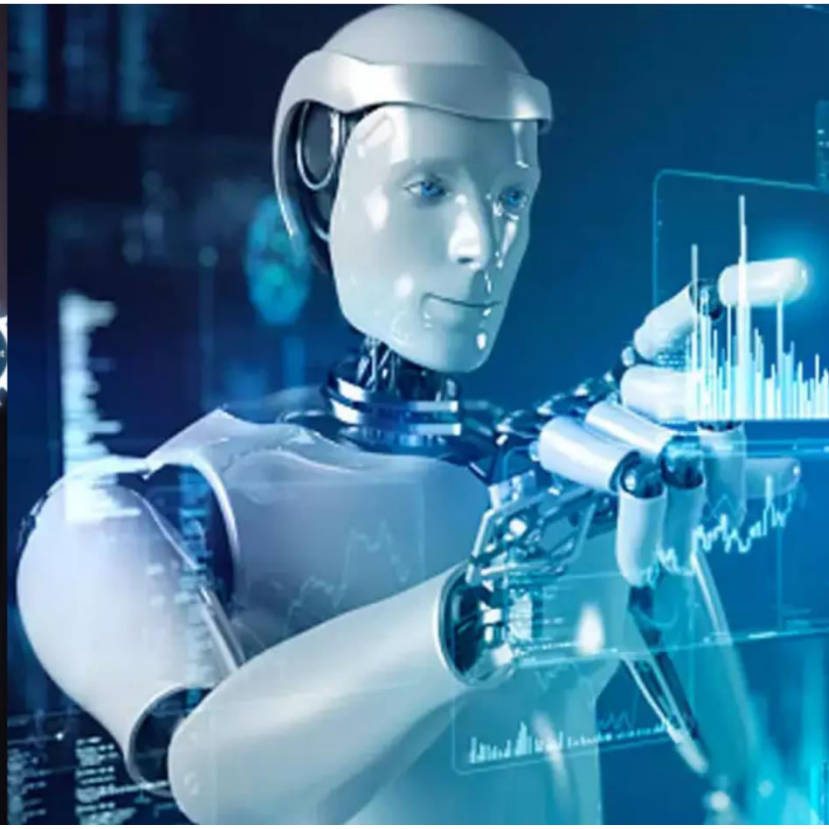
IJIRSET
International Journal of Innovative Research in Science | Engineering | Technology

ISSN(O): 2319-8753
ISSN(P): 2347-6710

International Journal of Innovative Research in Science Engineering and Technology (IJIRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.699

Volume 14, Issue 12, December 2025

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 12, December 2025

|DOI: 10.15680/IJIRSET.2025.1412100|

App-Controlled Smart Door Lock System for Home and Office Security

Manjunatha B[1], Aishwarya A P[2], Darshan C[2], Deekshitha P[2], Giridhar K S[2]

Assistant Professor, Department of Electrical and Electronics Engineering, Vidya Vikas Institute of Engineering and Technology, Mysuru, Karnataka, India[1]

Student, Department of Electrical and Electronics Engineering, Vidya Vikas Institute of Engineering and Technology, Mysuru, Karnataka, India[2]

ABSTRACT: An app controlled smart door lock system for home and office security is an low-cost, IoT-based smart door lock system using an ESP8266 microcontroller and a Flutter-based mobile application. The proposed system provides multiple authentication methods such as password, fingerprint, and one-time entry password (OTEP) while maintaining affordability, security, and ease of use. Unlike traditional digital locks, the system supports contactless unlocking and offers offline operation through Wi-Fi communication without cloud dependency. The prototype demonstrates reliable operation, efficient power management using TP4056 and MT3608 modules, and robust performance in both residential and industrial settings.

I. INTRODUCTION

Digital locks are modern security devices that utilize electronic mechanisms to provide access control. They offer various methods of authentication, such as: Password/PIN-based Access: Users enter a numeric code to unlock. Biometric Authentication: Uses fingerprints, facial recognition or other unique physical traits. RFID/Smart Card Access: Users swipe a card or tag. Bluetooth/Wi-Fi-based Access: Operate through smart phone apps or other connected devices. These locks are often used in residential, commercial and industrial applications, providing convenience, enhanced security and additional features like remote monitoring.

II. PROBLEM STATEMENT

Digital locks offer significant advantages in terms of security, convenience and modern features, but their drawbacks must be addressed to improve reliability and accessibility for a broader user base.
The main drawbacks of Digital Locks are Power Dependence, Vulnerability to Hacking, Cost, Complex Installation and Maintenance, Dependence on Digital Systems, Environmental Sensitivity, Limited Lifespan of Components, Privacy Concerns, Compatibility Issues, Physical Override Issues and Dependency on Connectivity.
These are the main drawbacks of the digital locks that must be resolved in order to gain more usability and more features. Resolving these issues my result in more durable and improved version of the digital locks.

III. OBJECTIVES

A digital smart lock represents a significant evolution in security technology, replacing traditional mechanical keys with electronic or digital systems. These locks leverage advanced technologies to provide enhanced security, convenience and flexibility, addressing modern security challenges in various domains.

Historically, mechanical locks have been the cornerstone of physical security, but they come with inherent limitations, such as vulnerability to picking, difficulty in managing multiple keys, and lack of scalability. Digital smart locks emerged to address these shortcomings by incorporating electronic authentication methods and remote access capabilities.

These locks are ideal for residential, commercial, and industrial applications. For instance, in residential settings, they enable homeowners to grant temporary access to visitors without sharing physical keys. In commercial applications,

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 12, December 2025

|DOI: 10.15680/IJIRSET.2025.1412100|

they streamline access management for employees and contractors, while in industrial settings, they enhance the security of restricted areas.

The main objective of the proposed system is,

- To design a circuit with more power efficient, power back up options and reduced system failures and durable for environmental conditions.
- To create a user-friendly application with more accessibility and for to set up the lock with features and verification methods.
- To create a system that only allows authorized people access to a location that is secure, practical and user-friendly. With cutting-edge features like remote access, biometric authentication and real-time monitoring capabilities, the system should offer an alternative to conventional lock-and-key systems and digital locks.

IV. METHODOLOGY

The system architecture comprises an ESP8266 microcontroller, a servo motor, and power management modules (TP4056, MT3608). The microcontroller handles authentication logic and communicates with the mobile app through Wi-Fi. The Flutter app allows users to enter credentials, manage access modes, and trigger lock/unlock actions. All user credentials are stored locally in the ESP8266 for enhanced security. A buzzer provides feedback for lock status, and emergency backup power ensures uninterrupted operation.

V. BLOCK DIAGRAM

The methodology outlines the systematic approach used to design, develop, and implement the Flutter-based app for secure, contactless unlocking systems using Bluetooth and NodeMCU. This section provides a step-by-step breakdown of the process, ensuring clarity and repeatability.

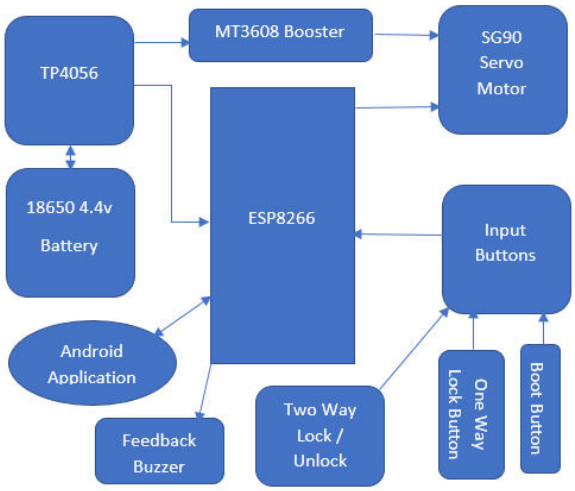


Fig 5: Block Diagram of the proposed system

VI. CIRCUIT DIAGRAM

The below diagram shows the circuit connections of digital smart lock and shows the list of components which have been used in this project. The circuit operates and demonstrate as shown in the figure to achieve its goal and aim.

The TP4056 powers the whole circuit, it charges the battery and simultaneously powers the other components like MT3608, ESP8266, LED, Buzzer. The MT3608 steps up the voltage up to 12v and powers the servo with about 5v. the

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 12, December 2025

|DOI: 10.15680/IJIRSET.2025.1412100|

inbuilt potentiometer typically helps to regulate voltage between 12v. as the esp8266 can't power the servo alone as the servo requires more voltage and current under load it requires more current drawing to much current from the esp8266 can result in improper function of esp8266 and damage of esp8266. A switch is also included to turn on or turn off the supply. 3 buttons each has its own operations like boot button initializes the esp8266 or resets, one way button typically reads the servo if it is locked or unlocked if unlocked can be locked and does nothing the other button works both ways from inside.

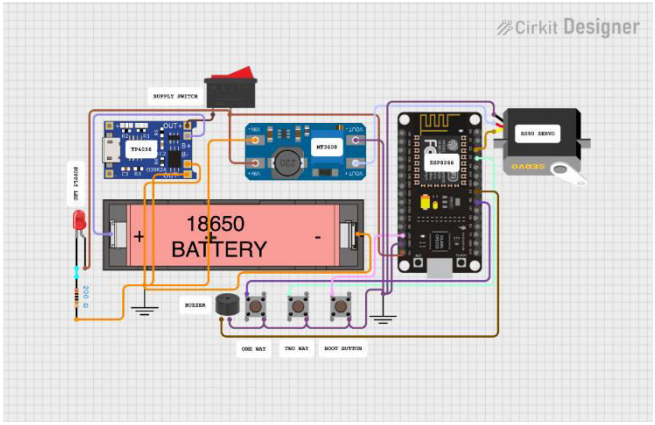


Fig 6: Circuit Diagram of the proposed system

VII. WORKING OF THE PROPOSED SYSTEM

The TP4056 is used for to charge the battery and switch between two power sources such as battery and main power. The project runs with the main power and charges the battery as well in case there is no main power it will switch from main to backup.

In this project we have used a servo motor. This servo motor consumes more voltage and power that ESP8266 or ESP32 can't provide so we have used MT3608 boost the voltage specially for the servo motor to operate.

The ESP8266 is the brain of our project which handles majority all the components connected to it. It is programmed in a way that it can communicate with the app that we have developed seamlessly. The ESP8266 can store, operate and clear the passwords and pin codes. And can be operated via mobile phone via the Digital smart lock app.

The sg 90 is a servo motor which serves as a locking actuator to our lock design. Which moves between 0 to 180 degree for both lock and unlock conditions.

A 18650 is lithium ion battery which can be recharged for reusability, we have included this in our project to serve as a 2nd power options or as a backup power options.

We have used a buzzer for feedback upon booting up, feedback upon user made changes or to give feedback when tampered detected.

We have used 3 of this 1 serves for booting up to esp8266, 2 serves for one way Locking and another serves for both two-way lock/unlock.

The application offers setting up digital smart lock with proper inputs such as password, pin code, Fingerprints and Face ID. Which can be used to unlock or lock the digital smart lock. It offers a setup of OTEP (one-time entry password or pin code) feature. It requires an additional detail like the devices IP, SSID and SSID password for Contactless unlocking or locking capabilities. Very thing which can stetted up can be cleared or reset any time individually via the app at any time or from anywhere by authorized or registered device.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 12, December 2025

|DOI: 10.15680/IJIRSET.2025.1412100|

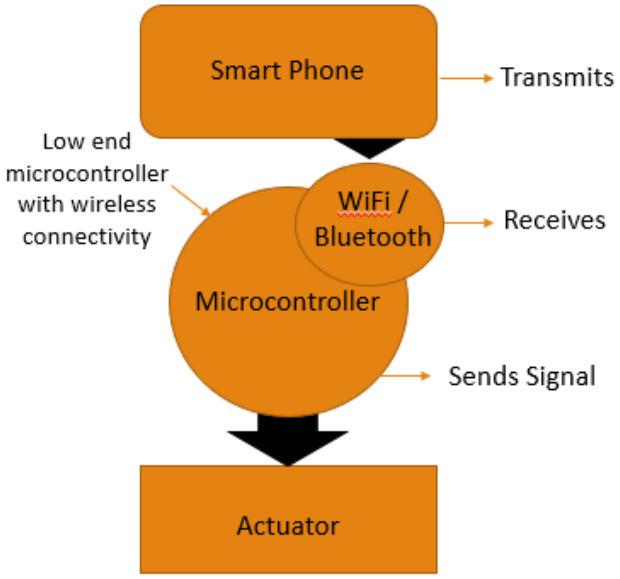


Fig 7: Flow chart of the Proposed system

VIII. HARDWARE IMPLEMENTATION

The proper operation of the project is heavily influenced by the selection and design of hardware components, which are depicted in the block diagram. Each component's selection and design play a crucial role in ensuring the project functions correctly. Therefore, careful consideration and planning are essential to guarantee the project's success and effectiveness. The block diagram serves as a visual representation of how these components interact to achieve the project's objectives.

The hardware components include:
• ESP8266 Microcontroller – Core controller handling logic and Wi-Fi communication.
• TP4056 – Lithium-ion charging and protection module.
• MT3608 – Boost converter for servo power.
• SG90 Servo Motor – Controls the physical lock.
• 18650 Battery – Provides backup power.
• Buzzer and Buttons – Used for feedback and manual override.

IX. SOFTWARE IMPLEMENTATION

The Arduino IDE (Integrated Development Environment) is a free, open-source platform used to write, compile, and upload code to Arduino boards. It simplifies microcontroller programming and supports multiple languages, primarily C and C++. Windows, mac OS, and Linux are all supported by the cross-platform Arduino Integrated Development Environment (IDE). Functions in C and C++ are supported. It is used to generate and upload program to boards that are compatible with Arduino as well as other

Vendor development board with the aid of third-party cores. The GNU General Public license, version 2, governs the distribution of the IDE's source code. The Arduino IDE supports the C and C++programming languages using unique code organization techniques. A software library from the Wiring project is available through the Arduino IDE and offers a variety of standard input and output functions. Code Editor: Write and edit programs (called sketches). Library Manager: Easily include libraries to expand functionality (e.g., sensors, displays, or motors). Serial Monitor: Debug and communicate with the Arduino board in real-time. Cross-Platform: Available for Windows, mac OS, and Linux. Board and Port Selection: Allows you to select your Arduino model and USB/serial port.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 12, December 2025

|DOI: 10.15680/IJIRSET.2025.1412100|

Android Studio is an official integrated development environment (IDE) for Android app development, and it also supports Flutter, a framework developed by Google for building cross-platform applications using a single codebase. Flutter apps can run on Android, IOS, web, and desktop platforms. The digital Lock operates with the help of a mobile app that has been specially developed for our project needs. The application fulfills the purpose and goal about what the project meant to be. The mobile application has been developed by software called android studio inside that we have used a plugin for app development such as Flutter. The application consists of API and other Android Packages such as WIFI, Bluetooth and Access point and client protocol. With help of this packages the app successfully communicates with the esp8266. Both the devices communicate with each other in real time making it more responsive and faster. By developing our own app, we were able to establish new features that are not implemented in existing digital locks yet. The main programing language we have used to develop our app is KOTLIN and has been tested on all android platforms up to Android 13.

X. RESULTS AND DISCUSSION

At first the user has to set the password which will be considered as the master password. If the user tries to set password again after setting up it up it doesn't store the password unless the password has been reset or cleared. A snack bar appears which displays the responses form ESP8266 upon performing activities.

If the user wishes to implement any changes or in case of resetting, the user must provide the valid master password in order to do the activities. Then the password or pin code or any of the verification steps can be reset or cleared.

This master password can also be feed in unlock screen to unlock or lock screen to lock the door.

This change can also be done with a new device each time unless and until the user has master password. It is safe to use in different devices because none of the device with the app doesn't store any data inside the smart phone. Making it more secure and hard to breach in. if the user doesn't want to use the password for regular use they can create a Pin code for regular use.

Also, the user can set up face id and finger print which also comes under master password. The setting up of lock and maintenance is so user-friendly and less complicated.

The user can go through the instructions to set up OTEP and also an exclusive feature such as contact less unlocking where the user doesn't need to do anything it automatically verifies and give access upon valid users. In contact less unlocking the user doesn't need to do anything for unlocking the door the user must be near enough and the door opens without any sensors and with security. This will make sure that user is an authorized user and unlocks the door.

The prototype successfully demonstrated all intended features:
• Smooth Wi-Fi-based communication between app and lock.
• Reliable multi-authentication process.
• Low power consumption and stable performance.
• Real-time lock/unlock operation with quick feedback.
The system proved suitable for both residential and industrial environments.

XI. APPLICATIONS

1. Residential Applications:
- Ideal for homeowners seeking secure, keyless entry to their premises.
- Features like temporary access codes or biometric authentication enable flexibility for family members, visitors, or service personnel.

2. Commercial Applications:
- Enhances security for offices, shops, and retail spaces by streamlining access control for employees and contractors.
- Offers the ability to monitor activity logs for better management of business operations.

3. Industrial and Warehouse Applications:
- Ensures restricted access to storage areas, machinery, and sensitive work zones.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 12, December 2025

|DOI: 10.15680/IJIRSET.2025.1412100|

- Robust designs withstand harsh industrial environments and provide reliable performance.

4. Healthcare Sector:
- Secures access to medical storage rooms, laboratories, and patient records.
- Biometric authentication ensures that only authorized personnel can access sensitive areas.

5. Educational Institutions:
- Provides secure access to classrooms, libraries, and staff rooms.
- Temporary access codes can be issued to students or visiting lecturers as needed.

6. Public Sector and Government Buildings:
- Ensures security in sensitive locations such as data centers, archives, and administrative offices.
- Offers activity tracking to ensure compliance with security protocols.

7. Emergency and Temporary Applications:
- Useful for securing temporary installations such as event spaces, pop-up stores, or construction sites.
- Easy installation and removal make it suitable for short-term needs.

8. Automobiles and Vehicle Startups:
- Provides keyless entry for vehicles, enhancing user convenience.
- Ideal for modern vehicle fleets or rental services with a focus on digital integration.

XII. FUTURE SCOPE

Future improvements include:
• Child Lock Mode with automatic safety override.
• Broadcast Control for managing multiple locks simultaneously.
• Integration with voice assistants, cloud storage, and AI-based intrusion detection for intelligent monitoring.

XIII. CONCLUSION

The proposed Low-Cost Smart Lock System offers a practical and secure alternative to existing digital locks. By combining embedded systems, IoT, and mobile technology, it delivers a reliable and scalable solution that enhances accessibility, security, and energy efficiency. Its affordability makes it ideal for large-scale adoption in residential, commercial, and institutional applications.

REFERENCES

[1] Mustafa et al. (2018) designed a smart door locking system utilizing a Bluetooth module, keypad and Arduino controller. Their prototype enabled door access through a mobile application, providing users with both convenience and enhanced security. Similarly, Almogren et al. (2019) compared several communication technologies, Bluetooth, Wi-Fi and Z-Wave, for smart door locks. Their analysis showed that Z-Wave offered superior reliability and safety, though it was comparatively more complex to implement

[2] Lee et al. (2018) examined the existing landscape of key management and smart door lock systems. Their study identified interoperability and usability as major challenges. They proposed an NFC-based locking mechanism where users could unlock doors through smartphones. Performance evaluations confirmed the system's practicality and reliability in everyday scenarios.

[3] He et al. (2020) reviewed multiple studies on smart lock security vulnerabilities. They highlighted risks such as Wi-Fi exploitation, Bluetooth attacks, and password cracking. The authors emphasized the need for stronger authentication algorithms and secure data handling to enhance resilience against such threats.

[4] Zhang, Chen, and Lai (2020) analyzed user experiences with smart locks through a survey of 120 participants. Most users reported satisfaction with the convenience and safety features. However, concerns persisted regarding system reliability and the necessity of an emergency manual key in case of malfunction or power failure.

[5] Sharma et al. (2021) implemented a low-cost Wi-Fi-enabled smart door lock using an ESP8266 module and mobile app. Their design prioritized local operation without cloud dependency, improving privacy. Although efficient for residential use, the system faced issues with encryption and scalability for larger networks.

[6] Lee and Park (2022) introduced a hybrid smart lock integrating Bluetooth Low Energy (BLE) with fingerprint authentication. This dual-layer approach improved both access speed and reliability. Despite the benefits, the study noted drawbacks such as increased power consumption and limited Bluetooth coverage in spacious environments.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 12, December 2025

|DOI: 10.15680/IJIRSET.2025.1412100|

[7] Kumar et al. (2022) conducted a detailed vulnerability assessment of commercial smart locks. Their research revealed weaknesses in mobile applications and cloud APIs, exposing systems to replay and spoofing attacks. The authors advocated for stronger encryption, secure key storage and controlled firmware updates to mitigate such risks.

[8] Chen et al. (2023) implemented a camera-based smart lock using the ESP32-CAM module for facial verification. The system authenticated visitors through image recognition before granting access. While this enhanced safety, its dependence on stable internet connectivity made it less effective in low-network or rural areas.

[9] Singh et al. (2023) proposed an NFC-tag-based access system intended for schools and institutional settings. Their results showed the model to be reliable and easy to deploy in limited-user environments, though less adaptable for households requiring multiple dynamic users.

[10] Patel and Desai (2024) explored IoT-integrated smart locks compatible with home automation ecosystems. Their system allowed interaction with virtual assistants such as Google Home and Alexa. Although it enhanced convenience, the research highlighted automation conflicts as potential risks, suggesting implementation of safe default responses to avoid accidental unlocking.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details