International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 10 Issue: 11 | Nov - 2026 SJIF Rating: 8.659 ISSN: 2582-3930

Design and Development of a Smartphone-Controlled Bluetooth Smart Door Lock System

Under the guidance **Professor. Shruthi M.K**
Department of Electronics and Communication Engineering Aditya College of Engineering and Technology Bangalore, India

Archana L
Department of Electronics and Communication Engineering Aditya College of Engineering and Technology Bangalore, India

Abstract

This paper describes the development of a smartphone-operated door locking arrangement based on Bluetooth communication and an embedded controller. The proposed prototype brings together a mobile application, a Bluetooth interface, a microcontroller, a driver stage, and an electronic locking unit. Through the application, a user can issue commands to lock or unlock the door without making a direct wired connection to the controller. After a command reaches the controller, the embedded program interprets the received data and produces the output needed to operate the locking device through an appropriate driver circuit.

The work is intended to provide a straightforward and economical alternative to a conventional key-operated arrangement for small access-controlled spaces. The mobile phone acts as the command interface, while the controller coordinates communication and lock operation. The hardware arrangement can be implemented with an ESP32 board or another suitable controller paired with a compatible Bluetooth interface. The final selection of the electronic lock and driver depends on their electrical ratings and the requirements of the prototype.

The paper outlines the system structure, component requirements, software approach, communication sequence, and method used to evaluate the prototype. Particular attention is given to pairing the phone with the controller, receiving and interpreting commands, and producing a consistent response from the locking mechanism. Factors such as usable communication distance, supply stability, interface compatibility, and response behaviour are relevant when assessing the design.

The prototype may be examined through functional checks that include device pairing, command delivery, connection continuity, and correct lock and unlock responses. Since Bluetooth is a short-range technology, its practical performance depends on the selected interface and the surrounding environment. Access protection must also be considered: pairing alone should not be treated as complete security, and the design should accept only recognised commands. The proposed arrangement demonstrates the use of embedded control and local wireless communication for convenient electronic access management.

KEY WORDS

Bluetooth communication, smart door lock, wireless access control, microcontroller, smartphone application, electronic security system.

I. INTRODUCTION

Security is a basic requirement in homes, workplaces, educational institutions, and other buildings where people or equipment must be protected from unauthorised entry. A door is an important part of this protection because it separates an accessible area from a restricted one. For many years, mechanical locks and physical keys have been the usual means of controlling entry. Although familiar and easy to use, this approach can cause practical difficulties when keys are lost, misplaced, copied without permission, or forgotten.

These limitations have encouraged the use of electronic access systems. Such systems can use a password, an identification card, a biometric feature, or a wireless command to control a locking device. Embedded controllers make it possible to receive an input, evaluate it according to programmed rules, and operate an electronic output. When wireless communication is added, the user can interact with the control unit without a direct cable connection.

Smartphones are widely available and can provide a convenient interface for controlling nearby electronic equipment. A Bluetooth-enabled phone can exchange data with a compatible embedded device over a local wireless link. This makes Bluetooth a practical option for a small door-access prototype that does not require an internet connection for its basic operation.

Bluetooth-Based Access Concept

The proposed project applies this idea to a door lock. A mobile application is used to send a lock or unlock request to a controller. The Bluetooth interface receives the transmitted information and passes it to the microcontroller. The controller checks the command and, when it is recognised, drives the connected locking mechanism through a suitable interface circuit. The arrangement is intended to reduce dependence on a conventional key for normal operation while keeping the overall design understandable and suitable for an academic prototype.

The controller is the main decision-making unit in the system. It manages the communication interface, identifies the incoming instruction, and controls the output stage. The lock itself performs the physical locking action. Depending on the electrical characteristics of the selected lock, a relay or another driver circuit may be required so that the controller is not directly exposed to a load beyond its output capability.

Bluetooth is selected because it is supported by many smartphones and embedded platforms and is appropriate for local communication. Unlike an internet-dependent arrangement, a basic Bluetooth implementation can work within its supported radio range without a router or cloud service. Its range is nevertheless limited and can be affected by walls, interference, device orientation, and the particular Bluetooth hardware used.

Project Scope and Design Considerations

The proposed arrangement is aimed at locations such as a residential room, office, laboratory, or small controlled area where nearby wireless operation is sufficient. It is not presented as a replacement for certified commercial access-control equipment. The actual capability of the prototype depends on the controller, Bluetooth interface, application, power source, driver stage, and lock selected for implementation.

A reliable design must ensure that the phone and controller can establish a connection and that the received data is interpreted consistently. The firmware should distinguish the expected lock and unlock instructions from unknown input. An unrecognised command should not cause the lock output to change. Power requirements must be checked for both the controller and the locking device, since the load may require a separate supply or driver stage.

The project includes component selection, circuit interfacing, embedded program development, Bluetooth setup, mobile application configuration, and functional testing. During evaluation, the developer can record whether pairing succeeds, whether commands arrive correctly, how quickly the controller responds, and whether the locking mechanism completes the requested action. Testing under more than one operating condition helps identify practical limitations.

Wireless access introduces security considerations in addition to ordinary electrical design. The system should use suitable pairing and command validation, and should be arranged to avoid unintended activation. More advanced features, such as a password layer, door-position sensing, event records, or remote notifications, are possible extensions. They should be described as future additions unless they have actually been implemented and tested in the present prototype.

The project therefore serves as a compact demonstration of the relationship between mobile communication and embedded control. It shows how a smartphone can act as a local user interface and how a microcontroller can translate a received instruction into a physical output. The design also provides a starting point for further study of smart-home devices and electronic access systems.

II. LITERATURE SURVEY

Smart locking arrangements have developed alongside progress in microcontrollers, identification technologies, short-range radio communication, and mobile software. Traditional mechanical locks remain common, but the inconvenience associated with carrying and managing keys has led to a range of electronic alternatives. The following review groups the main approaches relevant to the proposed prototype.

A. Conventional Electronic Door-Locking Systems

Earlier electronic locking products commonly used numeric keypads, RFID cards, or other digital identification methods. In these designs, an electronic input is supplied by the user and processed by a controller. If the submitted information meets the programmed condition, the controller activates the locking unit. These systems reduce reliance on a metal key, but may require a separate keypad, card, tag, or reader. Their convenience depends on how the user credential is issued and managed.

B. Wireless Communication-Based Access Control

Wireless links have expanded the ways in which an access-control unit can receive a request. Bluetooth supports data exchange between compatible devices over a relatively short distance and is therefore suitable for local control. Bluetooth Classic and Bluetooth Low Energy provide different communication and energy-use characteristics. The appropriate option depends on the hardware and application requirements. A local Bluetooth link can provide control without relying on an internet connection, although its coverage is limited by radio conditions.

C. Microcontroller-Based Smart-Lock Systems

A microcontroller is commonly used as the central element of an embedded lock because it can read incoming information, execute programmed checks, and control an output interface. The ESP32 family is relevant to this type of work because selected devices provide integrated wireless capabilities, including Bluetooth. Other controller boards can also be used when an external Bluetooth module is connected and supported by the firmware. The selected platform must have compatible logic levels, sufficient input/output resources, and an appropriate development environment.

D. Smartphone-Controlled Door-Locking Systems

In a smartphone-operated design, a mobile application provides the control screen through which the user chooses an operation. The phone sends a data message to the embedded unit over a wireless connection. The controller interprets the received message and changes the state of the lock through an output circuit. This arrangement can avoid the need for a dedicated keypad or card reader at the door, although the phone and controller must be compatible and correctly paired.

E. Research Gap and Proposed Approach

The approaches reviewed above show that electronic access can be implemented through several different types of user input and communication. Some solutions rely on dedicated credentials, additional readers, internet access, or more extensive infrastructure. For a small-scale demonstration, a direct local connection between a smartphone and a microcontroller offers a comparatively simple route. The present work focuses on this arrangement and combines a mobile command interface with Bluetooth communication and an electronic locking unit.

The proposed design gives priority to straightforward operation, readily available components, and clear interaction between the main functional blocks. It also recognises that reliable communication, correct command interpretation, and user authorisation are necessary for meaningful access control. The prototype is therefore evaluated not only by whether the lock moves, but also by whether the connection and command sequence behave as intended.

III. METHODOLOGY

The method adopted for the Bluetooth-based smart door lock comprises hardware planning, circuit interfacing, software preparation, wireless-link configuration, mobile application setup, and prototype evaluation. The objective is to establish a local communication path from the smartphone to the embedded controller and to use the controller output to operate the door-locking unit.

A. System Architecture

The functional arrangement contains a smartphone application, Bluetooth communication interface, microcontroller, driver circuit, electronic lock, and power source. The phone is the user-facing control device. The Bluetooth interface carries the command to the controller, which acts as the processing unit. The driver stage connects the controller output to the locking device where electrical isolation or additional drive capability is needed.

B. Hardware Requirements

The principal hardware elements considered for the prototype are listed below. The exact parts should be selected to match the implemented circuit and the electrical ratings of the lock.

Hardware Components

1. Microcontroller: An ESP32 or another compatible controller is used to receive the wireless instruction, process it, and generate the control output.

2. Bluetooth Interface: Provides the radio link between the smartphone and the controller. Bluetooth may be built into the selected controller or supplied by a separate module.

3. Electronic Locking Mechanism: Carries out the physical locking and unlocking action in response to the controller output.

4. Driver or Relay Circuit: Interfaces the controller with the lock when the load requires a switching stage or electrical drive beyond the controller

output capability.

5. Power Supply: Delivers suitable power to the controller and the locking unit. Voltage and current ratings must be chosen according to the selected components.

6. Connecting Wires and Supporting Parts: Provide the electrical connections and mechanical integration needed to assemble the prototype.

C. Software Requirements

The software work consists of preparing the controller firmware and configuring the mobile application. A suitable environment, such as the Arduino IDE, may be used according to the selected board. Firmware can be written in the supported C/C++ environment and should initialise the Bluetooth interface, receive data, recognise the requested action, and control the output. The mobile application provides the controls used to send the lock and unlock messages.

D. Hardware Design and Interfacing

During assembly, the Bluetooth interface is connected to the microcontroller either internally or through the required external pins. The controller output is connected to the driver circuit, and the driver is connected to the electronic lock. The supply arrangement must meet the needs of each part. Before operation, the developer should verify the pin assignments, voltage compatibility, common reference requirements where applicable, and the current capacity of the selected driver.

E. Bluetooth Communication

The smartphone and the embedded unit first establish a Bluetooth connection. Once the connection is available, the user selects the required action in the mobile application. The application sends the associated data message, and the controller receives it through the configured interface. The communication method—Bluetooth Classic or Bluetooth Low Energy—must match the selected hardware and application implementation.

F. Programming and Command Processing

The firmware begins by configuring the controller pins and starting the Bluetooth service. It then waits for incoming data from the paired smartphone. When a message arrives, the program compares it with the commands defined for the project. A recognised lock or unlock instruction causes the corresponding output state to be selected. Data that does not match an accepted command should be ignored so that unknown input cannot directly operate the locking mechanism.

The output stage is then used to control the electronic lock. The control logic must take account of the operating requirements of the chosen lock and driver. The program should also maintain a predictable state when the connection is interrupted or the controller is restarted. These behaviours should be checked during prototype testing rather than assumed.

G. Working Principle

The normal operating sequence is as follows:

1. Power is applied to the controller and the associated circuit.
2. The Bluetooth interface is initialised.
3. The smartphone is paired or connected with the controller.
4. The user chooses the lock or unlock command in the application.
5. The application transmits the selected command wirelessly.
6. The controller receives the data and checks its meaning.
7. A recognised command causes the relevant output to be generated.
8. The driver stage operates the electronic locking mechanism.
9. The controller returns to a ready state for the next request.

H. System Testing and Evaluation

After the hardware and firmware have been integrated, the prototype should be tested in a controlled manner. Initial checks confirm that the power supply is stable and that the controller starts correctly. Bluetooth pairing is then examined, followed by the transmission of each supported command. The observer records whether the controller receives the correct message and whether the locking unit responds as expected.

Useful evaluation points include successful pairing, continuity of the connection, correct command recognition, response time, and successful completion of lock and unlock operations. Communication distance may also be recorded at different positions, provided the test conditions are clearly stated. Results should be reported from actual observations; performance values should not be inserted unless they have been measured.

I. Security Considerations

Because the system controls physical access through a wireless link, pairing and command handling require attention. The design should restrict operation to an authorised device and reject unknown or malformed messages. The application and controller should be configured so that accidental input does not trigger a lock-state change. Further protection, such as an additional user verification step or event logging, may be introduced if it forms part of the implementation.

IV. EXISTING SYSTEM

Conventional door security generally relies on a mechanical key and a corresponding lock. This method is straightforward and does not depend on an electrical supply, but the user must possess the correct key to enter. A lost or misplaced key can prevent access, while an unauthorised duplicate can weaken the intended protection. Carrying and managing physical keys can also be inconvenient when several doors or users are involved.

Electronic alternatives have been introduced to address some of these issues. Password-based locks accept a predefined code through a keypad. RFID arrangements identify a card or tag presented to a reader. Biometric systems compare a personal characteristic with stored information before granting access. Each method has its own requirements for input devices, credential management, controller hardware, and maintenance.

Although electronic methods provide alternatives to ordinary keys, they may require dedicated readers, cards, keypads, or other components. Some advanced products also use wired networks or internet-based services. Their installation and operating costs depend on the selected features and infrastructure. A network-dependent solution may additionally be affected by the availability of the network or service.

The main limitations considered in this project are dependence on a physical key or separate credential, the possibility of key loss or duplication, the need for additional devices in some electronic systems, and the installation effort associated with more complex access-control arrangements. These points motivate a compact local wireless design for a limited-use prototype.

Limitations of the Existing Approach

1. Entry may depend on carrying a physical key or a separate identification token.
2. A key can be lost, misplaced, or copied without the owner's permission.
3. Keypad, RFID, or biometric arrangements require their own input and identification hardware.
4. More advanced electronic systems can involve additional installation and maintenance work.
5. Conventional locks do not provide smartphone-based wireless operation.
6. Network-connected solutions may rely on external communication infrastructure.

A simple and economical access arrangement that can be operated locally from a commonly available mobile device is therefore worth investigating.

V. PROPOSED SYSTEM

The proposed Bluetooth-based smart door lock is intended to provide local wireless control of a door through a smartphone. It combines a Bluetooth

communication link, a microcontroller, and an electronic locking mechanism. A mobile application is used to submit the required operation, while the embedded controller processes the received instruction and controls the lock through a suitable driver circuit.

When the user selects a command in the application, the smartphone sends the corresponding data over Bluetooth. The controller receives and interprets the message. If the message is recognised as a valid lock or unlock request, the controller activates the relevant output and the driver stage operates the locking unit. This arrangement provides an alternative to using a conventional key for the supported operations.

The proposed design is based on commonly available embedded components and is intended to keep the system structure compact. Its key functions are wireless operation, application-based control, microcontroller processing, and electronic actuation. Optional features such as access history or remote monitoring are not assumed to be present unless they are added to the actual prototype.

Main Features of the Proposed System

1. Wireless operation: Lock and unlock requests are sent through a Bluetooth connection.
2. Smartphone interface: A mobile application provides the controls used by the operator.
3. Embedded processing: The microcontroller checks received data and selects the required output.
4. Electronic actuation: A suitable driver operates the connected locking mechanism.
5. Economical construction: The design can be assembled from commonly available embedded components.
6. Compact arrangement: The functional blocks can be integrated into a relatively small control unit.
7. Scope for extension: Additional authentication, door monitoring, or notification functions may be considered in later development.

The system may be used as a learning prototype for a room, office, laboratory, or other small area where short-range access control is adequate. Its suitability depends on the selected lock, the reliability of the power source, the Bluetooth environment, and the security measures implemented. The design should not be treated as a certified security product without further engineering and validation.

Evaluation of the proposed arrangement should include connection establishment, message delivery, command interpretation, and physical lock response. Measuring these aspects provides a clearer indication of the prototype's practical operation than describing the design only in terms of its intended features.

VI. SYSTEM ARCHITECTURE

The architecture explains how the smartphone, Bluetooth interface, microcontroller, driver circuit, and electronic lock cooperate. The smartphone is the point from which the user issues a command. The Bluetooth link carries the data to the controller, which processes the instruction and determines the required output. The driver circuit then interfaces the controller with the electronic locking device.

The controller may be an ESP32 or another suitable platform. Where Bluetooth is integrated into the selected board, an external module may not be necessary. If a separate module is used, its communication interface and logic levels must be compatible with the controller. A relay or other driver is included when required by the electrical characteristics of the lock. The power arrangement must supply the controller and lock within their specified operating limits.

Main Functional Blocks

1. Smartphone: Runs the mobile application and provides the lock and unlock controls.
2. Bluetooth Communication: Carries the command between the phone and the embedded controller.
3. Microcontroller (ESP32): Receives the message, checks the command, and generates the control output.
4. Relay/Driver Circuit: Provides the required switching interface for the electronic lock, when

needed.

5. Electronic Door Lock: Performs the physical locking or unlocking action.

6. Power Supply: Provides suitable electrical power to the control and locking sections.

i. Architecture Flow

The signal path begins with the user action in the smartphone application. The command is transmitted through Bluetooth and received by the controller. After checking the data, the controller activates the relevant driver output. The electronic lock then changes to the requested state. If feedback has been implemented, the application may also display the reported status of the system.

Figure 1: Architecture Flow of the Bluetooth-Based Smart Door Lock System.

VI. SYSTEM ARCHITECTURE

The architecture of the Bluetooth-operated lock illustrates the sequence through which a mobile command is converted into a physical locking action. The phone provides the user interface, Bluetooth carries the request, and the microcontroller performs the command-processing task. The output stage links the controller to the electronic lock.

An authorised operator uses the mobile application to select the required action. The Bluetooth interface receives the transmitted data and forwards it to the embedded controller. The controller interprets the message and controls the locking device according to the programmed operation.

Main Blocks of the System

1. Smartphone: Provides the application used to issue lock and unlock requests.

2. Bluetooth Link: Establishes local wireless communication between the phone and controller.

3. ESP32 Controller: Receives and processes the incoming command.

4. Driver Circuit: Switches the electronic lock when the chosen device requires a separate drive stage.

5. Electronic Lock: Carries out the requested locking or unlocking operation.

6. Power Supply: Feeds the controller and lock circuit with appropriate power.

i. Architecture Flow

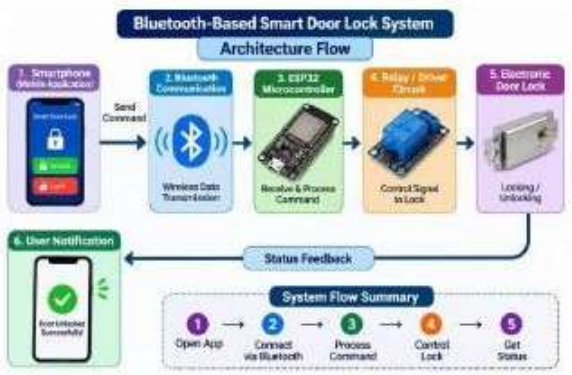


Figure 1: Architecture Flow of the Bluetooth-Based Smart Door Lock System.

ii. Working of System Architecture

The normal sequence of operation is described below:

1. The user opens the door-lock application on the smartphone.

2. The phone establishes a Bluetooth connection with the ESP32 controller.

3. The user selects the required lock or unlock option.

4. The application sends the selected command through the wireless link.

5. The ESP32 receives the message and checks the command.

6. The controller activates the corresponding lock-control output.

7. The driver circuit operates the electronic locking mechanism.

8. If feedback is supported by the prototype, the

application displays the available status information.

Communication and Control Sequence

The phone-to-controller link carries the user request, while the controller-to-lock path carries the electrical control signal. Keeping these functions separate helps explain the role of each block. Correct operation depends on compatible communication settings, suitable output interfacing, and a power supply capable of supporting the load.

ii. Hardware and Software Requirements

Hardware Requirements: The proposed arrangement uses an ESP32 controller or a compatible microcontroller with Bluetooth support, a smartphone, an electronic door lock, a relay or driver module where required, a suitable power supply, and connecting components. The final selection must follow the electrical specifications of the actual prototype.

Software Requirements: Firmware can be developed in the Arduino IDE or another environment supported by the selected controller. The program may use Embedded C/C++ and the relevant Bluetooth libraries. A mobile application is required to send the lock and unlock commands. The phone application and controller firmware must use matching communication settings and command definitions.

Together, these hardware and software elements provide the local wireless control path. Correct interfacing and testing are necessary to confirm that the complete system operates as intended.

iv. Summary

The Bluetooth-based smart door lock is an embedded access-control prototype designed to operate a door through a smartphone. Its central objective is to offer a convenient local alternative to a conventional key for the locking operations supported by the system. The design combines a mobile application, Bluetooth communication, a microcontroller, and an electronic locking mechanism.

An ESP32 may be used as the main controller because it supports Bluetooth communication. The phone sends a lock or unlock instruction through the application. The controller receives and interprets the data, then operates the electronic lock through a suitable driver or relay circuit. This enables the requested action to be performed without a direct wired command from the phone.

The arrangement offers wireless operation, ease of access, reduced reliance on physical keys, and a compact implementation using commonly available components. Its practical performance depends on the communication range, connection stability, power arrangement, controller programming, and compatibility of the driver and lock. Features such as fingerprint verification, password protection, facial recognition, Wi-Fi, IoT monitoring, and mobile alerts may be considered as future extensions rather than assumed functions of the basic design.

VII. ADVANTAGES

a. Keyless Access: Reduces the need to use a conventional physical key for supported operations.

b. Wireless Control: Allows the user to send lock and unlock commands over Bluetooth.

c. Ease of Use: Provides a familiar smartphone interface for local access operation.

d. Cost Awareness: Can be implemented with widely available embedded components.

e. Prompt Response: Enables the controller to act after receiving a valid command, subject to the hardware and communication delay.

f. Controlled Operation: Allows the firmware to accept defined commands from a paired device.

g. Flexible Integration: Can be interfaced with a suitable electronic locking mechanism.

h. Efficient Design Potential: The controller and communication interface can be configured for suitable power usage.

i. Compact Construction: The control electronics can be arranged as a small embedded unit.

j. Expandability: Additional authentication, door-state sensing, wireless monitoring, or access

records may be added in future versions.

VIII. CONCLUSIONS

The project presents a smartphone-controlled door-locking arrangement based on Bluetooth communication and embedded control. It demonstrates how a mobile device can send a local command to a microcontroller and how the controller can operate an electronic locking mechanism through an appropriate driver circuit. The design provides an alternative way to request locking and unlocking without relying on a conventional key for each operation.

The proposed system is based on a relatively simple set of functional blocks: a smartphone application, Bluetooth communication interface, microcontroller, driver stage, electronic lock, and power supply. Using commonly available components makes the arrangement suitable for academic demonstration and further experimentation. The ESP32 platform is one possible controller choice because Bluetooth capability is available in the device family, although the exact board and lock must be selected to meet the project requirements.

The practical value of the prototype depends on correct pairing, reliable command reception, proper processing of the received data, and safe operation of the locking unit. Its security is also influenced by how authorised devices are managed and how invalid commands are handled. Bluetooth range, radio interference, power stability, and hardware compatibility are additional factors that affect dependable operation.

The design may be extended by adding stronger user verification, a door-position sensor, event logging, backup power, or notification features. Wi-Fi or Internet of Things connectivity could also be explored where remote monitoring is required. Emergency manual access should be considered in any practical door-lock installation so that the system remains usable if power or communication becomes unavailable.

In summary, the Bluetooth-based smart door lock demonstrates the integration of wireless communication and microcontroller technology in an electronic access-control application. It provides a foundation for further work on smart-home automation and intelligent locking systems, while highlighting the need for appropriate testing and security design.

VIII. ACKNOWLEDGEMENT

We express our sincere appreciation to our respected Principal, the Head of the Department, and our project guide for their guidance, encouragement, and continued assistance during the completion of this project, “Bluetooth-Based Smart Door Lock System.” Their suggestions and academic support helped us organise and carry out the work.

We also thank the faculty members of the Department of Electronics and Communication Engineering for sharing their technical knowledge and for providing the facilities and resources required for the project. Their feedback contributed to the development and preparation of this conference paper.

We are grateful to our parents, friends, and team members for their encouragement, cooperation, and support throughout the work. Finally, we acknowledge everyone who contributed directly or indirectly to the successful completion of the project.

REFERENCES

[1] Espressif Systems, “ESP32 Series Datasheet,” Espressif Systems. Available: ESP32 Datasheet.

[2] Espressif Systems, “ESP32 Arduino Core Documentation.” Available: Arduino ESP32 Documentation.

[3] Espressif Systems, “ESP32 Bluetooth Networking User Guide.” Available: ESP32 Bluetooth Resources.

[4] IEEE, “Modernizing Home Protection: An IoT-Driven Approach with Smart Lock and Android Application,” 2024 IEEE 14th International Conference on Control System, Computing and Engineering, DOI: 10.1109/ICCSCE61582.2024.10696484.

[5] Bluetooth SIG, "Bluetooth Core Specification." Available: Bluetooth Official Specifications.

[6] Arduino, "Arduino Documentation and Programming Environment." Available: Arduino Official Documentation.