© APR 2026 | IRE Journals | Volume 9 Issue 10 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV9I10-1716218

Design And Implementation of A Password-Based Smart Door Lock System With GSM-Based Alert and Surveillance.

OBIANKE F. I[1], OBIANKE E. C[2], OBIANKE G. U[3]
[1]*Department of Electrical & Electronics Engineering, Delta State Polytechnic, Otefe-Oghara, Delta State, Nigeria.*
[2]*Evertech Packaging Solutions Nigeria. Ltd, Agbor, Delta State, Nigeria*
[3]*Atlantic Exhibition Nigeria Limited, Magboro, Ogunstate, Nigeria*

Abstract- ***This study describes the development of a secure and affordable password-based smart door lock system built using an Arduino microcontroller. The system combines a keypad for user input, a camera module for monitoring, GSM communication for alerts, and a servo motor to control the locking mechanism. Access is granted when a user enters the correct password through the keypad, after which the servo motor automatically unlocks the door. To enhance security, the system sends real-time notifications via GSM and provides local surveillance through the camera module. It is designed to operate independently without relying on a constant Internet connection, making it suitable for areas with limited network availability. The embedded real-time control logic ensures fast response and smooth standalone operation. Experimental results demonstrate that the system is reliable, efficient, and cost-effective, making it a practical solution for improving security in residential and office environments.***

Keywords: Arduino Microcontroller, GSM Alerts, Servo Motor, Smart Lock, Surveillance.

I. INTRODUCTION

With the growing need for stronger and more reliable access control, embedded electronic systems are steadily replacing conventional mechanical locks because of their improved security and automation features. Traditional keys can be easily lost, stolen, or duplicated, creating security risks that have encouraged the shift toward electronic authentication methods.

The password-authenticated smart door lock system combines microcontroller technology, digital authentication, surveillance capability, and GSM communication to deliver a more intelligent and responsive security solution. It is designed to meet the needs of homes, offices, and other secure facilities.

Recent research in this field has focused on developing smart lock systems that integrate microcontrollers, sensors, and communication modules to ensure dependable and autonomous operation. Unlike traditional mechanical locks, an Arduino-based smart door lock operates through a keypad password system. This approach allows users to set customized passwords while maintaining secure, non-invasive control over the door's locking and unlocking functions (Vadakkane et al., 2021). Because these systems do not rely on cloud connectivity, they deliver fast response times and maintain reliable operation even without Internet access.

Its functionality is based on the concept of a digital combination lock, supported by a stable multivibrator circuit that activates a relay for a few seconds once the correct code is entered. In another mode of operation, the system can act like an ON/OFF switch, toggling the relay state each time a valid code is correctly inputted.

The password mechanism works by entering a specific sequence of two or more digits (0–9) to unlock the door (Vinodhini et al., 2024). These digits are entered through push buttons that trigger a stable multivibrator circuit arranged in a cascaded configuration. When the correct password is entered completely and in the proper sequence, the logic circuit goes high, generating a pulse signal. This pulse energizes a relay, which then drives the actuator responsible for opening or closing the door.

© APR 2026 | IRE Journals | Volume 9 Issue 10 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV9I10-1716218

Conventional lock-and-key systems are vulnerable to problems such as key loss, theft, duplication, and misplacement of keys, and they do not provide real-time intrusion alerts or remote monitoring. On the other hand, many existing smart lock solutions are costly and depend heavily on continuous Internet connectivity to function effectively.

There is therefore a clear need for a secure, affordable, and standalone smart locking system that offers automated access control and real-time notifications without relying extensively on network infrastructure. This study focuses on the design and implementation of a password-authenticated smart door lock system integrated with surveillance features and GSM-based alert functionality.

Objectives of the Study

- To design a keypad-based password authentication system.
- To interface an Arduino microcontroller for system control.
- To implement a servo motor-based automatic locking mechanism.
- To integrate a camera module for surveillance.
- To implement GSM-based real-time alert notifications.

Security has become a major concern in many parts of the world, where weaknesses in existing security structures have contributed to increasing cases of unauthorized access and theft. In this context, reliable and affordable security solutions are no longer optional—they are essential.

The proposed password-authenticated smart door lock system is designed to strengthen security in homes and offices by providing low-cost automation, reducing dependence on constant Internet connectivity, and delivering real-time intrusion alerts.

Beyond residential and office use, password activation systems have broad applications. In vehicles, password-based mechanisms can help immobilize or track cars, reducing theft and enhancing recovery chances. In GSM systems, password protection secures communication networks from unauthorized access. Banking systems, such as Automated Teller Machines (ATMs), also rely on password authentication to safeguard customers' accounts.

Because of its effectiveness in protecting sensitive information and physical assets, password activation remains a vital security measure across domestic, industrial, commercial, and transportation sectors. It plays an important role in protecting lives, property, and economic well-being.

However, many existing smart lock systems depend on continuous Internet access or complex hardware designs, increasing both cost and installation difficulty. This research addresses these challenges by integrating password authentication, embedded control, surveillance capability, and GSM-based alert mechanisms into a standalone architecture. The proposed system is suitable for homes, warehouses, and office environments, offering a practical, reliable, and cost-effective security solution.

II. LITERATURE REVIEW

A password-activated lock is a type of combination lock that opens when the correct sequence of numbers or codes is entered. Instead of using a traditional key, it relies on a specific arrangement (permutation) of digits to grant access.

The earliest known combination lock was discovered in a Roman-period tomb at Koromikos in Athens. It was attached to a small box and featured several rotating dials rather than keyholes.

In 1206, the Muslim engineer Al-Jazari described a combination lock in his famous *Book of Knowledge of Ingenious Mechanical Devices*. His work documented many advanced mechanical inventions of his time (Vallely, 2015). Later, in 1878, Joseph Loch, a German inventor based in New York City, developed what is considered the modern combination lock. By the early 1900s, several improvements were made to enhance the design, security, and functionality of permutation locks leading to the reliable systems we use today (Loch,1878).

One of the simplest types of combination locks is commonly found on low-security bicycle locks and in briefcases. This type of lock uses several rotating discs

with notches cut into them. The lock is secured by a pin with multiple teeth that engage with the rotating discs (Afroz, 2022). When the notches on all the discs align correctly with the teeth of the pin, the lock can be opened.

Combination padlocks and safes often use a simple dial mechanism that interacts with a set of internal discs or cams arranged in parallel. To unlock this type of system, the user typically rotates the dial clockwise to the first number, then counterclockwise to the second number, and continues alternating directions until the final number in the sequence is reached. Each cam contains a notch, and when the correct combination is entered, all the notches align. This alignment allows a locking bar or fence to drop into place, releasing the locking mechanism and opening the lock. If testing a combination does not alter the internal state of the lock, different combinations can be tried sequentially. This can significantly reduce the time required for a brute-force attack.

Earlier combination padlocks manufactured by Master Lock had a vulnerability. By applying tension to the shackle while slowly rotating the dial, it was sometimes possible to detect stopping points that revealed the numbers in the combination.

More recent 40-position dial models from Master Lock were found to have a mechanical weakness. In some cases, the final number of the combination could be determined through manipulation, and the first two numbers had a predictable mathematical relationship with the last number. This flaw reduced the number of possible combinations from 64,000 to only about 100, which could be tested in a very short time.

In 1978, a combination lock that users could set to their own chosen number sequence was invented by Andrew Elliott Rae. Around the same period, electronic keypads were also emerging. However, Rae was unable to secure manufacturing support for his mechanical resettable lock design for use in lockers, luggage, or briefcases. Early silicon chip-based locks also failed to gain widespread popularity because they required constant battery power to maintain stored data. When Rae's patent eventually expired, manufacturers quickly adopted and mass-produced the original mechanical design. It became widely used around the world, particularly in luggage, lockers, and hotel safes. Today, resettable combination locks are a standard feature on most travel luggage used by travellers.

In 1886, Charles Sanders Peirce demonstrated that logical operations could be performed using electrical switching circuits (Peirce, 1976). This marked an important step toward modern digital logic systems. Later, in 1898, Nikola Tesla filed patents describing devices that incorporated electromechanical logic gate circuits. Initially, relays were used to implement logical operations. However, vacuum tubes later replaced relays due to their faster switching capabilities. In 1907, Lee De Forest improved the Fleming valve, making it suitable for use as an AND logic gate.

A major breakthrough came in 1937 when Claude E. Shannon introduced the application of Boolean algebra to the analysis and design of switching circuits. His work laid the foundation for modern digital circuit design. Earlier, in 1924, Walther Bothe developed the coincidence circuit, considered one of the first modern electric AND gates. Bothe later received part of the Nobel Prize in Physics for related contributions (Thomas, 2024).

Since the 1990s, most logic gates have been implemented using CMOS (Complementary Metal-Oxide-Semiconductor) transistor technology due to its low power consumption and high efficiency. Over time, several logic families have been developed, each with unique characteristics. These include Resistor-Transistor Logic (RTL), Diode-Transistor Logic (DTL), Transistor-Transistor Logic (TTL), and Complementary Metal-Oxide-Semiconductor (CMOS). Logic gates serve as the fundamental building blocks of combinational logic circuits. When multiple logic gates are interconnected to produce a specified output based solely on present input combinations without memory storage, the resulting system is called a combinational logic circuit. In such circuits, the output at any given time depends entirely on the current input values.

Non-electronic implementations of logic gates have also been explored, although they are less common in practical applications. Early electromechanical

computers, such as the Harvard Mark I, were built using relay-based logic circuits. Logic systems have also been implemented using pneumatic devices and mechanical switching mechanisms. More recently, researchers have developed DNA-based logic gates capable of performing computational functions in molecular computing systems, including experimental biological computers such as MAYA (Brown et al., 2012).

Electronic combination locks are an advanced variation of the traditional dial-based mechanical lock. In these systems, the secret access code is programmed into an electronic microcontroller rather than being purely mechanical. They are widely used in safes and vault doors, especially in environments where traditional dial locks are preferred over key-based systems. One major advantage of electronic combination locks is that they can support multiple valid access codes, one for each authorized user. This means that if access needs to be revoked for a particular user, only that individual's code is changed without affecting others.

Many modern electronic locks also include auditing features. These systems record which access code was used and the exact time the lock was opened, thereby enhancing accountability and security monitoring. Power for the locks is typically supplied by an internal battery or a small dedicated power source.

There are different types of combination locks. Multiple-dial locks are commonly seen on low-security devices such as bicycle locks. Single-dial locks are frequently used on padlocks and traditional safes. More advanced designs include keypad-based systems that require a numeric sequence to grant access, as well as fully electronic combination locks used in high-security vault doors. Early manufacturers of combination locks include ABUS, Master Lock, Sargent & Greenleaf, Wordlock, Dudley, and Conair, which contributed significantly to the development and commercialization of these systems.

Password-based door locks are particularly common in office environments. Instead of issuing physical keys to every employee, management can simply distribute a shared access code. This eliminates the logistical challenges associated with key duplication and replacement. However, if the code becomes known to an unauthorized individual, it may compromise security. This vulnerability is not unique to password systems; it also exists in keyed and mechanical combination locks when proper management procedures are not followed (Hlaing & Lwin, 2019).

Compared to manual key-based systems, electronic password locks offer several advantages. They reduce physical stress and time spent searching for keys, eliminate the risk of lost keys, and ensure that access credentials remain confidential among authorized users. In addition, electronic systems can be integrated with circuit protection mechanisms to ensure reliability and safety.

Circuit protection is essential in electronic lock systems to safeguard components against power failures, voltage spikes, lightning strikes, overloaded circuits, and sudden electrical surges. Such abnormal conditions can damage sensitive electronic components or even create fire hazards. Protective devices automatically interrupt excessive current flow to prevent damage before it occurs.

The earliest form of circuit protection is the fuse. A fuse contains a thin filament designed to melt when excessive current flows through it, thereby breaking the circuit. While effective, fuses must be replaced after they blow. To overcome this limitation, modern systems commonly use circuit breakers. A circuit breaker functions similarly to a fuse but can be reset after tripping. When abnormal current is detected, the breaker disconnects the circuit and can later be restored by switching it off and back on.

Another important protective device used in modern installations is the Ground Fault Interrupter (GFI). This device is particularly useful in environments where water may come into contact with electrical outlets. The GFI detects small differences in current between the live and neutral conductors, indicating that current is leaking to ground, and immediately disconnects the circuit to prevent electric shock.

Additionally, surge protectors are widely used to protect sensitive electronic equipment from voltage spikes and lightning-induced surges. These devices

often incorporate transient voltage suppressors, such as gas-filled diodes, which respond extremely quickly to abnormal voltage conditions and divert excess energy away from critical components.

Overall, electronic combination locks integrate digital control, multiple-user access management, auditing capability, and advanced circuit protection mechanisms, making them significantly more versatile and secure than traditional mechanical locking systems.

Previous research and implementations of electronic door lock systems have incorporated a wide range of technologies, including RFID, biometric authentication, and mobile application-based access control. While these solutions provide high levels of security and convenience, they often require expensive hardware components and complex infrastructure, making them less suitable for cost-sensitive environments.

Arduino-based systems, however, provide a practical balance between simplicity, effectiveness, and affordability. According to Harishini et al. (2024), Arduino platforms such as the Uno and Nano are widely adopted for embedded security applications due to their flexibility and ease of integration. In many related projects, the Arduino board serves as the local processing unit, while peripherals such as keypads, LCDs, and servo motors manage user interaction and physical lock actuation. Some advanced implementations extend functionality by incorporating SMS notifications through GSM modules or wireless control via Bluetooth connectivity.

The present project focuses on the design and development of a password-based smart door lock system enhanced with a camera module and GSM technology. The objective is to improve safety, real-time monitoring, and remote communication capabilities while maintaining cost-effectiveness and system simplicity.

Earlier foundational work by Goswami et al. (2017) introduced an automated password-protected door lock system, establishing the basic principles of password-based access control mechanisms. Motwani et al. (2021) conducted a comprehensive review of multi-factor door locking systems, emphasizing the importance of integrating multiple authentication methods to strengthen security. Rane (2015) explored the integration of GSM technology into password-based locking systems, highlighting the benefits of remote access, status notification, and control. Similarly, Ray (2022) provided detailed insights into the design considerations and implementation challenges associated with password-based door lock systems.

Beyond keypad-based approaches, Sia et al. (2022) developed a voice-activated storage locker specifically designed for visually impaired individuals, demonstrating innovative alternatives to traditional input methods. Vadakkan et al. (2021) examined the practical implementation of an Arduino Uno-based keypad door locking system, emphasizing the hardware configuration and system performance optimization.

Biometric approaches have also been widely studied. Vamsi et al. (2019) investigated face recognition-based door unlocking systems using Raspberry Pi, presenting an alternative biometric solution for access control. Similarly, Hassan et al. (2012) explored microcontroller-based facial recognition systems, illustrating advancements in biometric authentication techniques.

Additionally, Verma and Tripathi (2010) presented a digital security system integrating RFID technology for door lock systems, offering insights into contactless identification methods for door lock applications.

Recent studies have shown that the integration of Internet of Things (IoT) technology can significantly enhance security monitoring and remote accessibility, as demonstrated by Nalayini et al. (2022). IoT-enabled systems provide real-time data transmission, remote authentication, and cloud-based monitoring features, further strengthening security architecture.

By synthesizing insights from these diverse studies, the proposed work aims to develop a robust and secure password-based smart door lock system that integrates Arduino, a keypad membrane, servo motor actuation, a camera module, and GSM communication

© APR 2026 | IRE Journals | Volume 9 Issue 10 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV9I10-1716218

technology. This integrated approach enhances authentication, monitoring, and remote notification capabilities while maintaining affordability and implementation simplicity. The project contributes to the advancement of access control solutions suitable for residential, office, and institutional environments, with future work aimed at incorporating IoT-based enhancements for improved scalability and connectivity.

III. DESIGN ARCHITECTURE OF THE SYSTEM

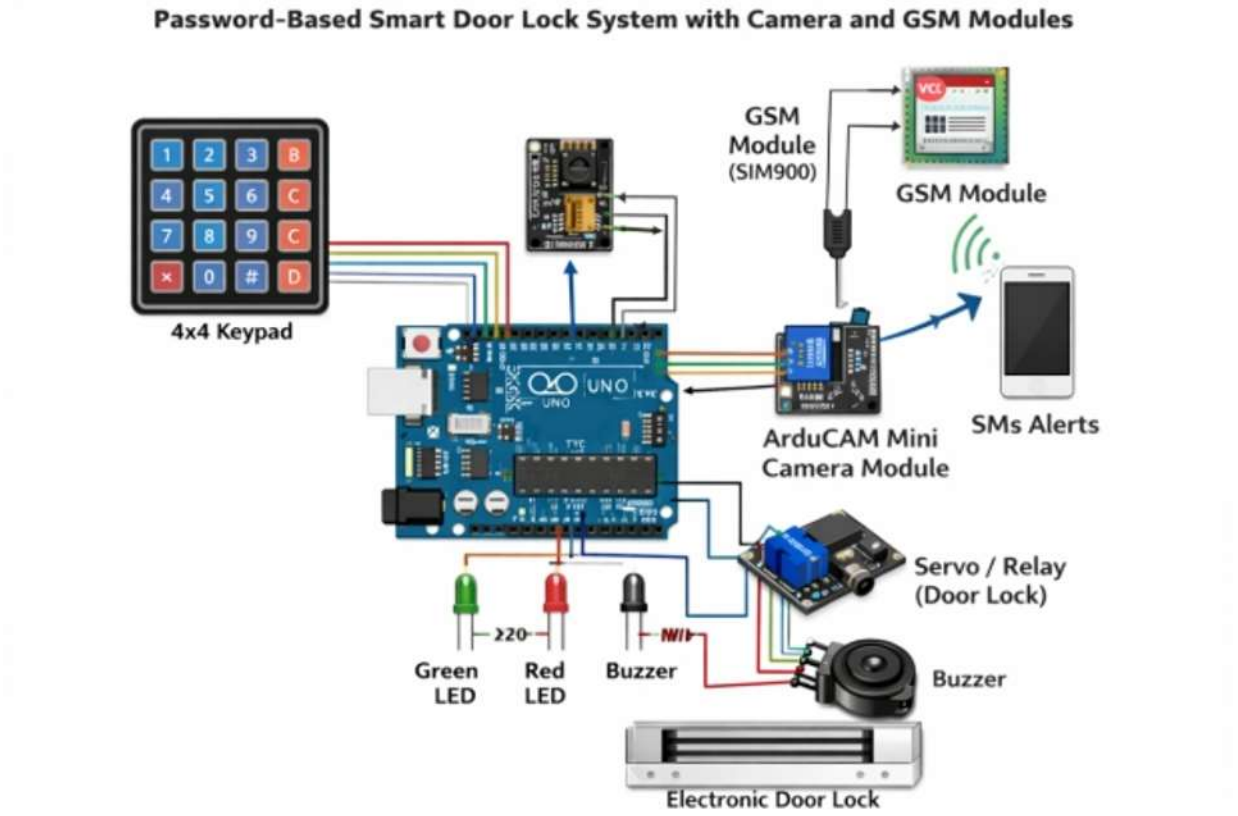

Figure 1 illustrates the circuit architecture of the Arduino-authenticated smart door lock system integrated with camera and GSM modules.

This section describes the major hardware components and interfaces used in the proposed system. The system consists of the following electrical and electronic components:

a. Arduino Uno/Nano
b. 4×4 Matrix Keypad
c. Servo Motor (for door latch actuation)
d. LCD Display (optional)
e. Buzzer
f. Power Supply
g. Camera and GSM Modules

The proposed password-based smart door lock system integrates an Arduino Uno, a servo motor, a keypad membrane, a camera module, and a GSM communication module to create a secure, reliable, and user-friendly access control solution. The primary objective of the system is to provide a convenient and dependable method for controlling access to doors and other restricted areas.

At the core of the system is the Arduino Uno, which functions as the central control unit. It receives input signals from the keypad membrane, processes the password entered by the user, and determines whether access should be granted or denied. Upon successful

© APR 2026 | IRE Journals | Volume 9 Issue 10 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV9I10-1716218

password verification, the Arduino sends a control signal to the servo motor, which actuates the locking mechanism to unlock the door. If an incorrect password is entered, the system initiates predefined security responses, including activating the buzzer, capturing an image using the camera module, and transmitting an alert through the GSM module.

The keypad membrane serves as the primary user interface, allowing authorized users to enter their passwords. Its simple and intuitive design ensures ease of use while maintaining system reliability.

The servo motor is responsible for the physical locking and unlocking mechanism. Depending on the authentication result, it rotates to either unlock or lock the door, ensuring smooth and reliable operation.

To enhance security, the system incorporates a camera module that captures images of individuals attempting to access the door, particularly during unauthorized access attempts. These images can be used for surveillance, monitoring, and evidence collection.

The GSM module further strengthens the security system by enabling real-time communication. It sends SMS alert notifications to the property owner whenever unauthorized access attempts occur and can also receive remote commands when required. This remote notification capability significantly improves security monitoring and allows prompt response to potential threats.

Overall, the proposed system is designed to be a robust, cost-effective, and versatile password-based smart door lock solution using readily available hardware components and open-source technologies. The system provides enhanced security, ease of operation, and real-time monitoring, making it suitable for residential, office, and institutional environments. Furthermore, its modular architecture allows future expansion through integration with advanced technologies such as IoT, cloud-based monitoring, and biometric authentication.

IV. DESIGN ANALYSIS AND IMPLEMENTATION

The design, setup, and implementation of the proposed smart door lock system were carried out in clearly defined stages to ensure proper integration and functionality. These stages are outlined below:

A. Circuit Design

The hardware design phase involved establishing proper electrical connections between all system components and the Arduino Uno microcontroller. The rows and columns of the keypad membrane were connected to the digital input/output (I/O) pins of the Arduino to enable password entry detection.

The servo motor was interfaced with one of the Arduino's Pulse Width Modulation (PWM) pins to allow precise angular control for locking operations. The camera module was integrated to enable image capture during unauthorized access attempts. An LCD display was connected to provide real-time user feedback, such as password prompts or access status messages.

Additionally, the GSM module was interfaced using serial communication pins to facilitate SMS-based alerts, while a buzzer was incorporated to generate audible warnings during incorrect password attempts or security breaches.

B. Software Logic Configuration

The system firmware was developed to manage authentication and security operations efficiently. Passwords were either hard-coded into the program or securely stored in the Arduino's EEPROM memory to allow persistent storage even after power loss.

To improve reliability, software debouncing techniques were implemented to eliminate false key-press readings from the keypad. Password masking was also incorporated to prevent visible display of entered digits, thereby enhancing user privacy.

The system allows multiple password retry attempts; however, after three consecutive incorrect entries, a delay-based lockout mechanism is activated. This temporary lockout enhances protection against brute-force attacks and unauthorized access attempts.

C. Prototype Assembly

During the prototyping phase, a breadboard was used to establish temporary electrical connections and verify circuit functionality before final assembly. Once testing confirmed proper operation, all components were arranged and packaged into a compact housing to create a neat, portable, and practical system enclosure suitable for real-world installation.

D. Testing and Validation

Comprehensive testing was conducted to ensure system reliability and performance. The system response to both correct and incorrect password entries was verified to confirm accurate authentication behaviour.

Servo motor actuation time and rotation accuracy were measured to evaluate mechanical performance. Additionally, the functionality of the reset feature and the delay-based lockout mechanism was validated to ensure that security protocols operated as intended under repeated failed attempts.

The methodology and configuration adopted in realizing this design are based on sound electronic principles and embedded control logic. The system applies a combination of multivibrator concepts configured in an astable mode (for timing and signal generation where applicable) and digital communication logic for decision-making processes. The overall design approach is guided by its primary objective: to address prevailing security challenges through an intelligent and automated access control system.

At the core of the implementation is the Arduino Uno, which serves as the prototyping and control platform. The Arduino Uno is a microcontroller-based development board that enables seamless integration of hardware components and software programming. It is programmed using the Arduino Integrated Development Environment (IDE), an open-source platform that allows users to write, compile, and upload code to the microcontroller.

The Arduino IDE is based on a simplified version of C++, making programming accessible while still powerful enough for embedded applications. Once the program is written, it is uploaded to the Arduino board via a USB connection using a built-in bootloader. Unlike many earlier programmable systems, the Arduino does not require an external hardware programmer to upload code. The USB interface handles both communication and power supply during development.

The Arduino board can receive both digital and analog input signals from various sensors and input devices. It processes these inputs according to the programmed logic and generates appropriate output signals to control actuators such as motors, buzzers, LEDs, and communication modules. This capability makes it suitable for applications involving automation, signal processing, and intelligent decision-making systems.

Although there are different versions of Arduino boards, they all share compatibility with the Arduino IDE. The major differences among them include the number of input/output pins, clock speed, memory capacity, physical size (form factor), and operating voltage levels. While others can run at lower voltages such as 3.3 V, the Arduino Uno remains one of the most widely used boards due to its balance between functionality, simplicity, and cost-effectiveness.

In this password-based smart door lock system, the Arduino Uno coordinates the interaction between the keypad, servo motor, camera module, GSM module, and display interface, ensuring synchronized and reliable operation.

The servo motor used in this system is designed for precise control of position and movement. Unlike conventional DC motors that rotate continuously, a servo motor operates using a closed-loop control mechanism. This means that its position is constantly monitored and adjusted based on feedback from an internal position sensor.

A typical servo motor consists of a rotor enclosed within a stator. When electrical current is applied, a magnetic field is generated within the stator, causing the rotor to rotate. The internal position sensor continuously measures the shaft position and sends feedback to the control circuit. The controller then compares the actual position with the desired position

and makes necessary adjustments to minimize any error.

This closed-loop feedback system ensures high accuracy, stability, and repeatability. Servo motors are therefore widely used in applications that require precise positioning, such as robotics, CNC machines, aerospace systems, industrial automation, and intelligent access control systems.

In the context of the proposed smart door lock, the servo motor is programmed to rotate to a specific angle when a correct password is entered, thereby unlocking the door. After a defined time interval, it returns to its original position to re-engage the locking mechanism. This controlled motion ensures reliable mechanical operation and enhances overall system security.

Hardware Components and System Description
Jumper wires are essential components in electronics hardware development and prototyping. They are insulated electrical wires fitted with connectors on both ends. These connectors may be male-to-male, male-to-female, female-to-female, or header-type connectors, allowing easy and secure connections between electronic components such as breadboards, microcontrollers, sensors, and peripheral modules.

The primary function of jumper wires is to transmit electrical signals and power between components. When properly inserted into compatible pins or terminals, they establish electrical continuity, enabling signals and current to flow through the circuit. Their flexibility and ease of use make them highly suitable for rapid prototyping and circuit testing, as they allow temporary connections without soldering. Jumper wires are available in various lengths, colours, and thicknesses to accommodate different circuit designs and user preferences, making them a convenient and efficient solution for wiring electronic systems.

The password-based smart door lock system is built around the Arduino Uno microcontroller to enhance access control and security. One of the key input devices used in the system is the 4×4 membrane keypad. The 4×4 keypad membrane switch is an input device commonly used in embedded systems to allow users to enter numeric or alphanumeric data. It consists of a thin, flexible membrane layer with conductive traces arranged in a matrix of four rows and four columns. Each intersection of a row and a column represents a key position.

At each key position, a dome-shaped conductive pad is placed beneath the surface. When a key is pressed, the dome collapses and connects the corresponding row and column traces, thereby closing the circuit. This change in electrical conductivity is detected by the microcontroller, which identifies the pressed key by scanning the row and column signals. The tactile feedback provided by the dome structure gives the user a physical response during operation.

This type of keypad is compact, cost-effective, durable, and widely used in electronic devices such as calculators, remote controls, and security systems.

In this door lock system, a camera module is installed at the entrance. Once the microcontroller detects a predefined trigger condition such as repeated incorrect password attempts, it activates the camera to capture an image of the person at the door.

Simultaneously, the GSM module receives a signal from the microcontroller and sends an alert message to the authorized user or security personnel. This real-time notification enhances the overall security of the system by enabling remote monitoring and rapid response to unauthorized access attempts.

The circuit diagram of the password-based smart door lock system illustrates the hardware connections between the Arduino Uno and the peripheral components, including the servo motor, keypad, camera module, GSM module, and power supply.

The servo motor was connected to the Arduino Uno using its three interface wires. The red wire was connected to the 5 V pin to supply power, the brown wire was connected to the GND pin to complete the circuit, and the orange (signal) wire was connected to digital pin 11 of the Arduino board.

In the Arduino program, the Servo library was used to control the motor's position and movement. By specifying particular angular positions in the code, the servo was programmed to rotate 90 degrees in one

© APR 2026 | IRE Journals | Volume 9 Issue 10 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV9I10-1716218

direction to unlock the door and 90 degrees in the opposite direction to lock it.

After writing the control program, the code was uploaded to the Arduino board using a USB cable through the Arduino IDE. Once powered, the servo motor responded according to the programmed angles, demonstrating proper actuation of the locking mechanism.

The 4×4 membrane keypad was interfaced with the Arduino using a matrix configuration. The row pins of the keypad (8, 7, 6, 5) were connected to Arduino digital pins (2, 3, 4, 5), while the column pins (4, 3, 2, 1) were connected to Arduino digital pins (9, 6, 7, 8) using jumper wires.
This matrix arrangement allows multiple keys to be read efficiently using fewer input pins. The Keypad library in the Arduino IDE was used to manage row-column scanning and detect key presses accurately.

After uploading the program, the Arduino interpreted user inputs from the keypad and executed the appropriate actions, such as password validation, door unlocking, or triggering security alerts.

The mechanical lock was physically coupled to the shaft of the servo motor. Proper alignment and firm mounting were ensured to maintain stability and reliable operation.

The rotational motion of the servo motor directly controlled the locking mechanism. When programmed to rotate to a specific angle, the servo either engaged or disengaged the lock, thereby providing controlled and secure access to the protected area.

The complete system consisted of the following interconnected components: an Arduino Uno (control unit), servo motor (actuation unit), 4×4 membrane keypad (input unit), camera module (surveillance unit), GSM module (alert unit), and 9 V power supply. All components were connected according to the designed circuit diagram. The integrated program, which included control codes for the servo motor, keypad, camera, and GSM module, was written and uploaded to the Arduino board using a USB cable via the Arduino IDE. After successful upload, the USB cable was disconnected, and the system operated independently using the external power supply. The system was then tested to verify proper functionality.
If modifications to the program were required, the Arduino board was reset, and the updated code was re-uploaded using the Arduino IDE. This allowed for iterative improvements and debugging during system development.

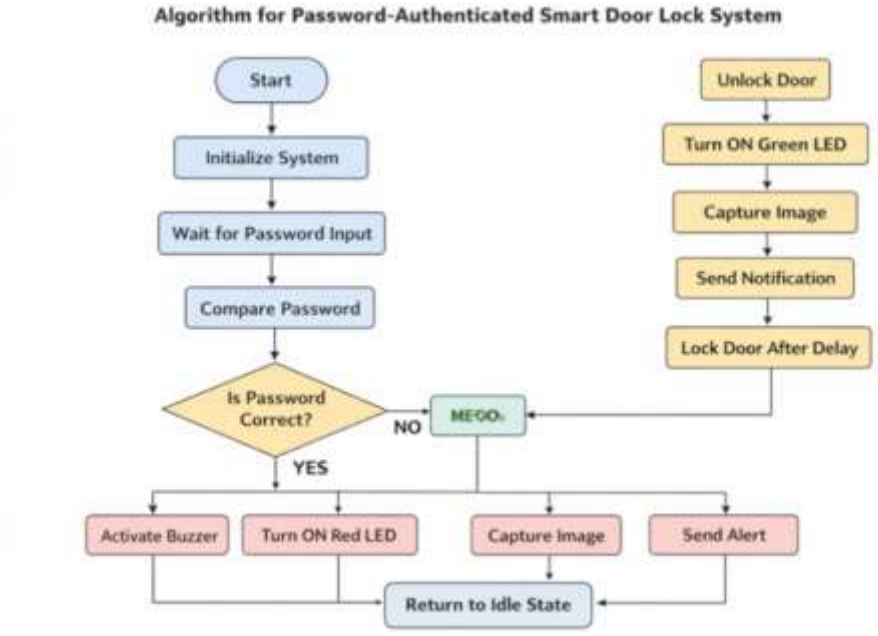

Fig. 2 illustrating the flow chart of the Arduino smart-based door lock system.

Architecture Overview / System Flow
(i) User inputs password via keypad.
(ii) Arduino verifies the password.
(iii) If correct, the servo rotates to unlock; otherwise, the buzzer sounds (alarm).
(iv) The system resets after each attempt.

V. RESULTS AND DISCUSSION

The Arduino Uno is programmed to control the servo motor, interface with the 4×4 membrane keypad, and manage the system password. When a user approaches the entrance, they are prompted to enter their password using the keypad.

As soon as the password is entered, the Arduino reads the input from the keypad and processes it within the system. After the user completes the entry, the Arduino compares the typed password with the one stored in its memory. If the password is correct, the Arduino sends a control signal to the servo motor. The servo motor then rotates to a preset angle, pulling the door latch and allowing the door to open.

However, if the password entered is incorrect, no signal is sent to the servo motor. As a result, the motor remains stationary and the door stays locked. This ensures that only authorized users can gain access. The system offers a secure and efficient method of unlocking the door through password authentication.

To further enhance security, the owner receives real-time updates whenever the door is locked or unlocked. Notifications are sent via SMS and video footage directly to the owner's smartphone through a GSM module. If three incorrect password attempts are made, the system automatically locks and displays "NO MORE TRIALS, ACCESS DENIED". At this point, no additional password entries can be made through the keypad. Only the owner can reset or unlock the system using the master password.

This research demonstrates a successful integration of hardware and software in developing a smart security system. Its major advantages include improved security compared to traditional mechanical locks, instant user feedback, compatibility with IoT-based remote monitoring, low cost, and scalability.

System testing was carried out to validate the functionality, reliability, and security of the smart door lock. The tests covered password authentication, motion detection, camera activation, GSM alert transmission, and system recovery after power failure. GSM-based alert mechanisms are well supported in the literature (Lee et al., 2014), and recent IoT-based smart lock studies also highlight the importance of strong authentication methods (Ahsan & Pathan, 2025). Overall, the system proved to be responsive, dependable, and highly effective in preventing unauthorized access.

Table 5.1 Test performance of implementation setup.

Test Case	Input	Expected Output	Result
Correct Password	4321	Door unlocks, LCD shows “Access Granted”	Pass
Incorrect Password	1234	Buzzer alerts, LCD shows “Access Denied”	Pass
Multiple Failed Attempts	1234, 2222, 3333	Optional alert after 3 attempts (Camera captures image, SMS sent)	Pass
Auto Lock	Door remains unlocked for 5 s	Door locks automatically	Pass

© APR 2026 | IRE Journals | Volume 9 Issue 10 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV9I10-1716218

Performance Evaluation of the Implementation System

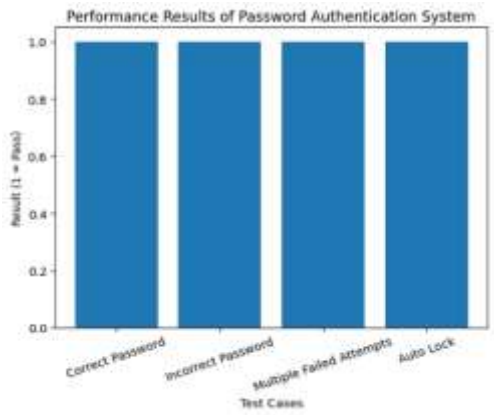

Fig 5.1 illustrating the Performance evaluation barchart.

Performance Evaluation of the Implementation System

The performance of the password-based authentication system was evaluated through a series of test cases to ensure its reliability and effectiveness. All the test cases, including correct password entry, incorrect password entry, multiple failed attempts, and the automatic locking feature, passed successfully, indicating that the system is reliable, secure, and performs as designed under different operating conditions.

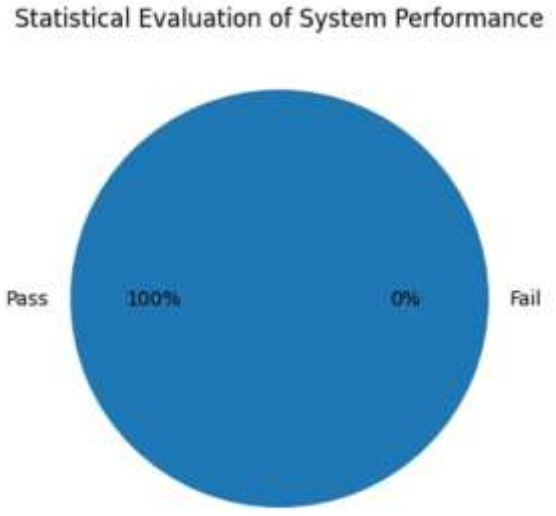

Fig 5.2 illustrating Statistical evaluation piechart.

Statistical Evaluation of System Performance

To quantitatively assess the performance of the password-based authentication system, statistical metrics were computed based on the test results obtained during system evaluation.

Success Rate (SR)

The success rate represents the proportion of test cases that produced the expected outcome.

$$\text{SR} = \frac{\text{Number of Successful Tests}}{\text{Total Number of Tests}} \times 100$$

Substituting the obtained test results:

$$\text{SR} = \frac{4}{4} \times 100 = 100\%$$

The system achieved a 100% success rate, indicating that all functionalities—including correct password authentication, incorrect password detection, multiple failed-attempt handling, and automatic door locking—performed exactly as expected during testing. This result demonstrates the reliability, accuracy, and effectiveness of the proposed smart door lock system under the evaluated operating conditions.

Failure Rate (FR)

The failure rate indicates the proportion of test cases that did not meet expected outcomes.

$$FR = \frac{\text{Number of failed tests}}{\text{Total number of tests}} \times 100$$

$$FR = \frac{0}{4} \times 100 = 0\%$$

A 0% failure rate confirms that no errors were encountered during testing.

Reliability Index (RI)

Reliability measures the consistency of the system in producing correct results.

$$RI = \frac{\text{Successful outcomes}}{\text{Total attempts}}$$

$$RI = \frac{4}{4} = 1.0$$

A reliability index of 1.0 indicates a highly reliable system.

System Efficiency (SE)

Efficiency can be interpreted as the system's ability to perform correctly within defined conditions.

$$SE = \frac{\text{Correct outputs}}{\text{Total inputs}} \times 100$$
$$SE = 100\%$$

The system demonstrates maximum efficiency under the tested scenarios.

Summarily,

- Success Rate = 100% illustrating excellent performance.
- Failure Rate = 0% showing no observed errors.
- Reliability Index = 1.0 indicating complete reliability.
- System Efficiency = 100% confirming that the system operated correctly under all tested conditions.

Therefore, the statistical evaluation confirms that the password-based authentication system is robust, reliable, and efficient, with perfect performance recorded across all test scenarios. This validates the effectiveness of the system design and implementation.

VI. CONCLUSION AND RECOMMENDATION

Password-based smart door lock systems can be upgraded to support multiple user profiles, each with a unique password or biometric credential. This makes it possible to assign different access permissions to different individuals, ensuring controlled and personalized entry management.

Additional security features such as built-in sensors and alarm mechanisms can detect and discourage tampering attempts, including forced entry or interference with the locking mechanism. These protective measures add another layer of safety to the system.

In future improvements, we plan to integrate an LCD display to provide clear and interactive feedback to users. The display will show messages such as "Password is Correct" after successful authentication, "Password is Incorrect" when an incorrect password is entered, and "Please Enter the Correct Password" to prompt the user to try again. This enhancement will improve the user experience by making the system more intuitive and user-friendly.

The implementation of a password-based smart door lock system using the Arduino Uno, servo motor, membrane keypad, camera, and GSM module represents a significant step forward in modern home security technology. By combining microcontroller intelligence with electromechanical components, the system delivers a dependable, flexible, and customizable solution for managing access to residential and commercial environments.

The use of the Arduino Uno as the central controller in this password-based smart door lock system provides great flexibility in programming and future expansion. Because it is easy to configure and modify, additional features can be integrated seamlessly, thereby improving the overall functionality of the system.

The precise control of the servo motor ensures smooth and accurate door unlocking once authentication is successful, offering both security and convenience to authorized users. The inclusion of a DC power supply also guarantees continuous operation, even during power outages, thereby maintaining uninterrupted protection. In addition, the membrane keypad serves as a simple and user-friendly interface for entering passwords, making the system accessible to a wider range of users.

Overall, this smart door lock system strengthens both security and access control. With further improvements and refinement, password-based locking systems have the potential to significantly transform home and office security, contributing to safer and more secure living environments.

An Arduino-based smart door lock system provides a reliable and cost-effective solution for secure physical access control. Its simplicity and ability to operate locally without constant Internet dependence make it suitable for residential and office environments. Moreover, the system can be expanded to include advanced features such as Bluetooth access and cloud-based monitoring.

The password-authenticated smart door lock system integrated with a camera and GSM module was

successfully designed and implemented. System testing confirmed that all components functioned as expected. However, further research and enhancements can improve performance and scalability. Suggested improvements include:
(a) Multi-user password management through the addition of EEPROM-based password storage.
(b) Integration of a Real-Time Clock (RTC) to enable time-restricted access control.
(c) Incorporation of biometric authentication or Bluetooth-based mobile unlocking.
(d) Addition of a fail-safe power backup system.
(e) Migration to cloud platforms such as AWS IoT Core for remote monitoring and control.

These future developments would enhance the system's robustness, intelligence, and adaptability to modern smart security demands.

REFERENCES

[1] Vadakkan, A., Babu, A. V. K., Pappachan, C., & Sunny, A. (2021). *Door Locking Using Keypad and Arduino*. International Research Journal of Modernization in Engineering Technology and Science (IRJMETS), 3(11), 780–787.

[2] Vinodhini, S., Gnanavarshini, S., Sheryl, E., & Divya Prapanjani, P. A. (2024). *Password-Based Smart Door Lock System Using Arduino UNO for Enhanced Security*. IRO Journal on Sustainable Wireless Systems, 6(2). Inventive Research Organization.

[3] Vallely, P. (2015). *How Islamic Inventors Changed the World*. New Age Islam.

[4] Loch, J. (1878). *Improvement in Tumblers for Permutation Locks*. U.S. Patent No. 200070.

[5] Afroz, A. (2022). *Digital Smart Door Lock Security System Using Arduino Uno Microcontroller*. Iconic Research and Engineering Journals, 6(1).

[6] Peirce, C. S. (1976). *The New Elements of Mathematics* (Vols. 1–4). The Hague: Mouton. Edited by C. Eisele.

[7] Thomas, F. L. (2024). *Electronic Fundamentals* (7th ed.). Prentice Hall International Inc.

[8] Brown, S. D., Francis, R. J., Rose, J., & Vranesic, Z. G. (1992). *Field-Programmable Gate Arrays*. Boston: Kluwer Academic Publishers. (Reprinted by Springer, 2012).

[9] Hlaing, N. N. S., & Lwin, S. S. (2019). *Electronic Door Lock Using RFID and Password Based on Arduino*. International Journal of Trend in Scientific Research and Development (IJTSRD), 3(3).

[10] Goswami, S., Choudhury, A., Das, S., Banerjee, T., & Ghosh, S. (2017). Automated password-protected door lock system. *Advances in Industrial Engineering and Management*, 6(1), 48–52.

[11] Motwani, Y., Seth, S., Dixit, D., Bagubali, A., & Rajesh, R. (2021). Multi-factor door locking systems: A review. *Materials Today: Proceedings*, 46, 7973–7979.

[12] Rahman, M. M., Ali, M. S., & Akther, M. S. (2018). Password-Protected Electronic Lock System for Smart Home Security. *International Journal of Engineering Research and Technology*, 7(4), 541–544.

[13] Rane, C. (2015). Password-Based Door Locking System Using GSM. *International Journal of Engineering Trends and Applications (IJETA)*, 2(4), 48–53.

[14] Ray, I. (2022). Password-Based Door Lock System. *International Research Journal of Modernization in Engineering Technology and Science*, 4(5), 2405–2413.

[15] Sia, B. J., Wong, W. K., & Min, T. S. (2022). Voice-Activated Storage Locker for Visually Impaired. In *2022 6th International Conference on Trends in Electronics and Informatics (ICOEI)* (pp. 442–447). IEEE.

[16] Vamsi, T. K., Sai, K. C., & Vijayalakshmi, M. (2019). Face Recognition-Based Door Unlocking System Using Raspberry Pi. *International Journal of Advance Research, Ideas and Innovations in Technology*, 5(2), 1320–1324.

[17] Verma, G. K., & Tripathi, P. (2010). A Digital Security System with Door Lock System Using RFID Technology. *International Journal of Computer Applications*, 5(11), 6–8.

[18] Hassan, H., Bakar, R. A., & Mokhtar, A. T. F. (2012). Face Recognition-Based Auto Switching

Magnetic Door Lock System Using Microcontroller. In *International Conference on System Engineering and Technology* (pp. 1–6).

[19] Madhusudhan, M., & Shankaraiah. (2015). Implementation of Automated Door Unlocking and Security System. *International Journal of Computer Applications*, 5–8.

[20] Chowdhury, A. (2011). Revolution in Authentication Process by Using Biometrics. In *International Conference on Recent Trends in Information Systems* (pp. 36–41).

[21] Nalayini, C. M., Sreemathi, P., & Nanditha, B. (2022). Deterrence of Accident Using IoT. *Journal of Trends in Computer Science and Smart Technology*, 4(2), 96–105.

[22] Chen, H., Liu, J., & Yang, C. F. (2016). Design of Intelligent Locks Based on the Triple KeeLoq Algorithm. *Advances in Mechanical Engineering*, 8(4), 1–7.

[23] Lee, S., Tewolde, G., & Kwon, J. (2014). Design and Implementation of Vehicle Tracking System Using GPS/GSM/GPRS Technology. In *IEEE World Forum on Internet of Things* (pp. 353–358).

[24] Ahsan, M. S., & Pathan, A. P. (2025). A Comprehensive Survey on Access Control Models in IoT: Requirements, Applications, and Challenges. *IoT*, 6(1), 9.

[25] Arduino Documentation. (2024). https://www.arduino.cc/reference/en/

[26] Electronic Combination Lock Based on PIC. http://www.elxproject.com/elx/infusions/pro_download_panel/download.php?did=11