Smart Security Door System Using Raspberry PI And HMI

Pooja Chaudhary[1], Vrushali Mali[2], Diya Chaudhari[3], Sunil Mahajan[4]
[1,2,3,4]*Department of Electronic Science, MAEER's MIT Arts, Commerce & Science College, Alandi, Pune, Maharashtra, India*
doi.org/10.64643/ijirt.208517-459

***Abstract*—Security and efficient access management have become essential requirements in residential, commercial, and industrial settings. This paper proposes a Smart Security Door System developed using a Raspberry Pi and a Human–Machine Interface (HMI) to provide automated and controlled access. The system combines a Passive Infrared (PIR) sensor, touchscreen-based HMI, password authentication mechanism, servo motor, and buzzer within an integrated embedded platform. When the PIR sensor detects the presence of a person, the HMI is activated to allow password entry. The Raspberry Pi processes and verifies the authentication credentials, and upon successful verification, the door is unlocked through the operation of a servo motor. If multiple incorrect password attempts are made, the system activates a buzzer to alert users about a potential unauthorized access attempt. The developed prototype was tested under various operating conditions to evaluate its overall performance. Experimental observations showed dependable motion sensing, quick authentication, and effective door control while maintaining a relatively low implementation cost. The proposed system offers a practical, user-friendly, and scalable approach for applications such as smart homes, offices, laboratories, and other areas requiring controlled access. It also demonstrates the potential of Raspberry Pi-based embedded systems in developing intelligent and reliable security solutions.**

***Index Terms*—IoT, Raspberry Pi, Smart Security, HMI, PIR Sensor, Access Control, Embedded Systems.**

I. INTRODUCTION

The growing need for secure and automated access management has increased the use of intelligent security systems across residential, commercial, and industrial sectors. Traditional door-locking mechanisms that depend on physical keys have several limitations, including the risk of keys being lost, copied, or misused for unauthorized entry. As a result, conventional locking methods may not adequately satisfy the security expectations of modern environments.

Advancements in the Internet of Things (IoT) and embedded technologies have made it possible to develop smart security systems that integrate detection, authentication, and automated operation into a unified system. The Raspberry Pi is widely used as an embedded computing platform because of its affordability, flexibility, and ability to interface with different sensors, actuators, and communication devices. These features make it a suitable platform for implementing intelligent access control solutions.

This research focuses on the design and development of a Smart Security Door System based on a Raspberry Pi and a Human–Machine Interface (HMI). The proposed system uses a Passive Infrared (PIR) sensor to detect human movement and activates an HMI touchscreen for password-based user authentication. A servo motor performs the door locking and unlocking operation, while a buzzer generates an alert when unauthorized access attempts are detected. The developed prototype is intended to deliver a dependable, economical, and easy-to-use access control solution for applications such as smart homes, offices, laboratories, and other locations where entry needs to be restricted.

II. LITERATURE REVIEW

Recent developments in embedded technology have contributed significantly to the advancement of automated security and access-control systems. Various studies have investigated the use of embedded controllers, motion-detection sensors, electronic authentication methods, and automated locking

mechanisms to improve security. Among the available embedded platforms, Raspberry Pi has gained considerable attention because of its processing capability and flexibility in interfacing with sensors and actuators. One study combined a Raspberry Pi, PIR sensor, and object-recognition techniques to develop a smart-home security system [1]. The results demonstrated that PIR-based detection can effectively initiate security-related operations; however, the use of image processing increased the overall complexity of the system.

Several researchers have investigated security and monitoring applications based on Raspberry Pi and PIR sensors [2], [3], [4]. These systems were developed for purposes such as smart-home door security, visitor monitoring, motion detection, and security notification. The findings indicate that PIR sensors provide a simple and effective method for detecting human movement. However, most of these approaches focus mainly on intrusion monitoring and notification rather than integrating motion detection with local password-based door access.

Password authentication has also been widely applied in electronic door-security systems because it provides a simple and economical method of restricting access. Previous studies have demonstrated password-controlled door locks using Arduino-based controllers, servo motors, and conventional keypad interfaces [5][7], [8]. These systems successfully verified user credentials and controlled the locking mechanism after authentication. Although the results demonstrate the practicality of password-based access control, most of the existing designs use conventional keypads and Arduino platforms instead of combining an HMI touchscreen with a Raspberry Pi.

Servo motors are commonly used in automated door-locking mechanisms because they provide controlled angular movement for locking and unlocking operations. Several password-based doors-lock systems have successfully used servo motors to control physical access [5], [6], [8]. Raspberry Pi-based contactless door-opening and locking mechanisms have also been investigated [9], [10]. These studies demonstrate the ability of embedded controllers to generate the required signals for automated locking mechanisms. In the proposed system, the servo motor is controlled after successful password authentication and returns to the locked position after a predefined time interval.

Security-alert mechanisms are another important component of electronic access-control systems. Earlier PIR-based security applications have incorporated alarms and notification mechanisms to indicate suspicious activity or human presence [1], [3], [4]. Similarly, password-protected door systems have used audible or visual feedback to indicate authentication results [7], [8]. Raspberry Pi has also been used for surveillance, alert generation, and IoT-based home-security applications [11], [12]. These studies highlight the importance of providing an immediate warning when potentially unauthorized activity is detected. In the proposed system, a buzzer is activated after three consecutive incorrect password attempts to provide a local audible alert.

Researchers have also explored advanced authentication techniques to improve access-control security. Facial recognition has been investigated as a low-cost biometric approach for door-access systems [13], while dual-factor authentication has been proposed to provide an additional level of protection [14]. Although these techniques can offer stronger authentication, they may require additional hardware, higher processing capability, or greater implementation complexity. Therefore, the proposed system uses password-based authentication to maintain a balance between security, simplicity, and implementation cost.

Raspberry Pi has further been applied in IoT and smart-home security systems for monitoring, automation, and connected access control [12], [15], [16], [17]. Some of these approaches incorporate cloud platforms, remote monitoring, or communication infrastructure to extend system functionality. However, such additional services may increase system complexity and create a dependency on network connectivity. The proposed prototype is designed to perform its primary security functions locally without requiring cloud services or continuous internet access.

Overall, previous research confirms the usefulness of PIR sensors for human-motion detection [1], [3], [4], Raspberry Pi for security monitoring and automation [2], [12], [15], [16], [17], password authentication for access control [5][7], [8], and servo motors for automated door-locking applications [5], [6], [8]–[10].

Advanced methods, such as facial recognition and multifactor authentication, have also been explored to improve security [13], [14]. However, many existing systems concentrate on individual functions, remote monitoring, or more complex authentication mechanisms. The proposed system integrates a Raspberry Pi, PIR sensor, HMI touchscreen, password-authentication mechanism, servo motor, and buzzer into a unified platform. The PIR sensor detects human presence and initiates the authentication process by activating the HMI. The user then enters a password, which is verified by the Raspberry Pi. Successful authentication operates the servo-based door lock, whereas repeated invalid attempts trigger the buzzer. This integrated design aims to provide a low-cost, automated, and user-friendly security solution for small-scale residential, commercial, laboratory, and other restricted-access applications.

III. METHODOLOGY

The proposed Smart Security Door System integrates a Raspberry Pi, PIR sensor, HMI touchscreen, servo motor, buzzer, power supply, and connecting wires into a single automated security platform. The Raspberry Pi acts as the central processing and control unit, coordinating the sensor input, password authentication, door-lock operation, and security alert mechanism.

The PIR sensor is positioned near the entrance to detect the presence or movement of a person and initiate the authentication process. Once motion is detected, the Raspberry Pi activates the HMI display, which provides an interactive interface for password entry and displays the system status.
The entered password is received through the HMI and verified by the Raspberry Pi against the stored credentials. If the entered password is correct, the system considers the user authorized and sends a control signal to the servo motor.

The servo motor then unlocks the door for a predefined period, after which it automatically returns to the locked position. This provides automated access control without requiring manual operation of the door lock.

If an incorrect password is entered, the system denies access and allows the user to retry. When multiple invalid attempts occur, the Raspberry Pi identifies the activity as a potential unauthorized access attempt and activates the buzzer. The buzzer provides an audible warning to alert nearby personnel. The HMI can simultaneously display the corresponding authentication or security status.
The complete system is powered through a stable and regulated power supply to ensure reliable operation of the Raspberry Pi, HMI, PIR sensor, servo motor, and buzzer. Connecting wires are used for electrical interconnections, while a mounting frame provides secure physical installation of the components.

Operating Process

The proposed Smart Security Door System functions in two main operating modes: Authorized Access Mode and Security Alert Mode.

In Authorized Access Mode, the PIR sensor first detects the presence or movement of a person near the door. Once detection occurs, the HMI is activated and requests the user to enter the password. The entered credentials are transmitted to the Raspberry Pi for verification. If the password is valid, the Raspberry Pi sends a control signal to the servo motor to unlock the door. After a specified time, interval, the servo automatically returns the locking mechanism to its original locked position.

In Security Alert Mode, access is denied when an incorrect password is entered. The system monitors repeated unsuccessful authentication attempts, and when the permitted limit is exceeded, the Raspberry Pi activates the buzzer to produce an audible warning. This mechanism helps indicate a potential unauthorized attempt to gain access.

Therefore, the overall system integrates motion detection, user authentication, automated locking, and security alert generation within a single platform.
PIR Sensor Detection → HMI Activation → Password Input → Raspberry Pi Authentication → Authorized Access / Access Denied → Servo Motor Operation / Buzzer Alert

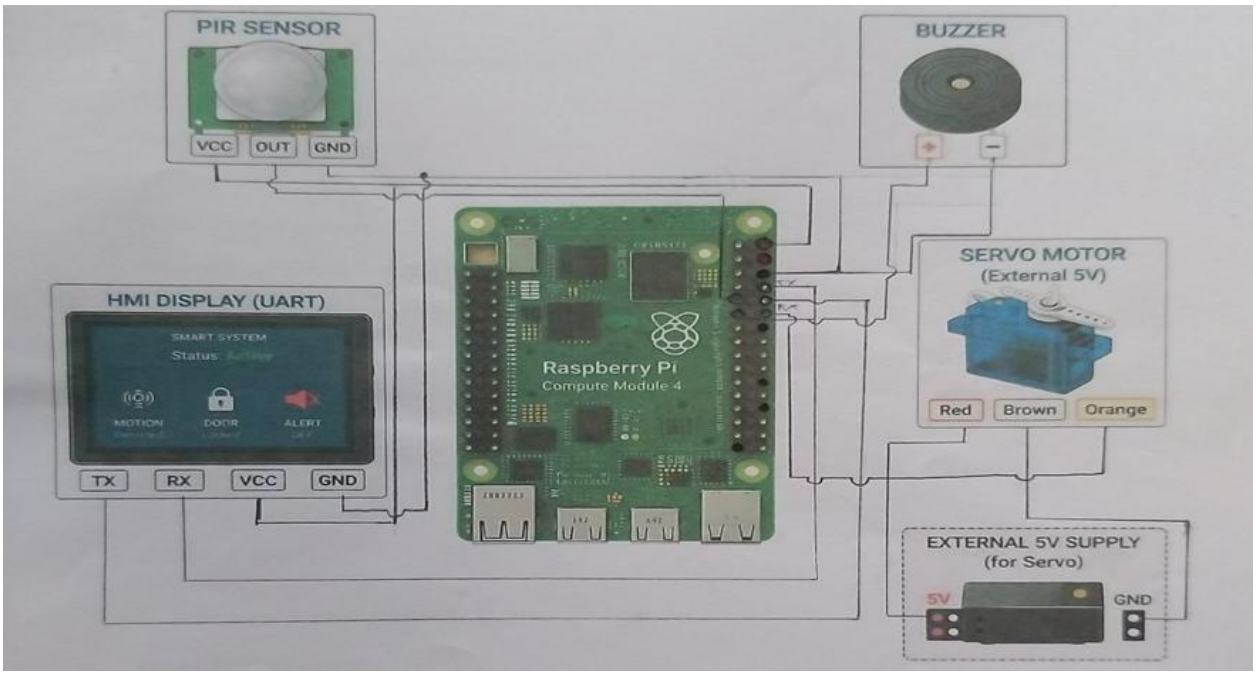

Fig. 1. Circuit Connection Diagram of the Proposed Smart Security Door System

IV. WORKING PRINCIPLE

- The PIR sensor continuously observes the area near the entrance to detect human presence or movement.
- When motion is detected, the sensor transmits a signal to the Raspberry Pi.
- Based on this signal, the Raspberry Pi activates the Human–Machine Interface (HMI) to begin the authentication process.
- The HMI then presents a password input screen to the user.
- The password entered by the user is checked against the credentials stored in the system.
- If the entered password matches the stored password, the Raspberry Pi controls the servo motor to unlock the door for a specified period.
- After the predefined time has elapsed, the servo motor returns the locking mechanism to its secured position.
- If an invalid password is entered, the system denies access and keeps the door locked.
- When three consecutive incorrect password attempts are detected, the Raspberry Pi activates the buzzer to provide an audible warning of a possible unauthorized access attempt.
- By combining motion sensing, password verification, automated locking, and alert generation, the proposed system provides an integrated approach to secure and automated door access control.

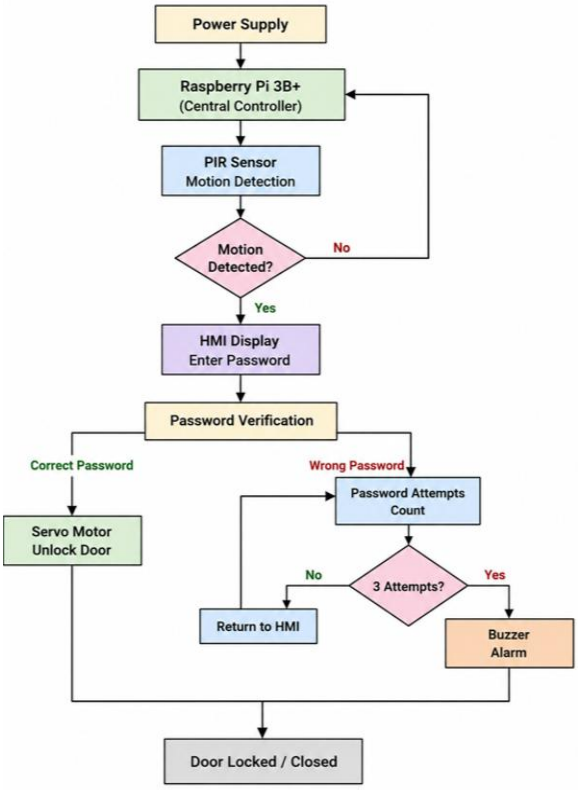

Fig. 2. Flowchart of the Working Principle of the Proposed System

V. IMPLEMENTATION

The developed Smart Security Door System prototype was tested under controlled laboratory conditions to examine its functionality and overall performance.

Several key parameters were considered during the evaluation of the system:

1. PIR Sensor Performance The ability of the PIR sensor to detect human movement or presence near the entrance was examined.
2. Password Authentication Performance The authentication process was tested using both valid and invalid passwords to verify the accuracy of access authorization.
3. Servo Motor Response The response of the servo motor was evaluated by observing the time required to unlock the door following successful authentication and to return the locking mechanism to its original position.
4. Buzzer Alert Functionality The alert mechanism was tested to confirm that the buzzer was triggered after three consecutive unsuccessful password attempts.
5. Overall System Reliability The stability of the integrated hardware and software components was evaluated during continuous system operation.
6. Access Scenario Testing Multiple authorized and unauthorized access attempts were performed under different operating conditions to assess the effectiveness of the proposed security mechanism.

The implementation and testing process confirmed the coordinated operation of the PIR sensor, HMI, Raspberry Pi, servo motor, and buzzer, demonstrating the practical feasibility of the proposed Smart Security Door System.

VI. RESULTS AND DISCUSSION

The performance of the developed Smart Security Door System was assessed under different operating conditions. Experimental testing demonstrated dependable motion sensing, accurate password verification, and effective automated control of the door-locking mechanism.

The experimental evaluation of the Smart Security Door System demonstrated satisfactory performance under different operating conditions.

Table 1. Authentication Performance

Parameter	Result
Motion detection Accuracy	98 %
Password Detection Accuracy	100 %
Door Unlock Response Time	1.5 s
Alarm Activation Time	0.5 s

Table 2. Unauthorized Access Detection

Attempt Number	System Response
1	Warning Message Displayed
2	Warning Message Displayed
3	Buzzer Alarm Activated

The PIR sensor successfully detected human presence during laboratory testing, while the password authentication mechanism correctly validated authorized credentials. For successful authentication, the servo motor responded quickly, unlocking the door with an average response time of approximately 1.5 seconds. In addition, the buzzer was activated successfully after three consecutive incorrect password attempts, providing an audible indication of a possible unauthorized access attempt. These findings demonstrate that the proposed system can provide reliable operation, quick response, and effective access management for applications such as smart homes, offices, laboratories, and other restricted-entry areas.

The HMI-based interface provided a simple and convenient method for entering the password. After receiving the user input, the Raspberry Pi compared the entered credentials with the stored password and completed the authentication process with minimal delay. This enabled authorized users to obtain access quickly while ensuring that invalid credentials were rejected. The proposed security mechanism was able to monitor unsuccessful authentication attempts effectively. When three consecutive incorrect passwords were entered, the system immediately triggered the buzzer to generate an audible warning. This feature provides a local indication of a potential unauthorized attempt and improves the overall security response of the system.

During the experimental testing, the Raspberry Pi-based prototype operated consistently without major interruptions or significant performance problems. Communication and coordination among the PIR sensor, HMI, servo motor, and buzzer remained stable throughout the evaluation.

These observations indicate that the integrated system is capable of supporting continuous operation in small-scale smart security applications.

- Combines human-motion detection, password-based authentication, automated door operation, and security alert generation within a unified embedded system.
- Utilizes a Raspberry Pi and commonly available hardware components to develop an economical access-control solution.
- Provides a rapid response to both successful and unsuccessful authentication attempts.
- Allows future expansion and modification for use in smart homes, offices, laboratories, and other controlled-access environments.
- Demonstrates the practical integration of sensing, authentication, and actuator control for automated security applications.

The experimental results demonstrate the successful integration of PIR-based human detection, HMI-based password entry, Raspberry Pi authentication and control, servo-operated door locking, and buzzer-based security alerts. The prototype showed consistent operation, rapid authentication, and effective control of authorized and unauthorized access attempts. Owing to its relatively simple design and use of readily available components, the proposed system represents a practical and economical approach for implementing automated access control in various smart security environments.

VII. CONCLUSION AND FUTURE SCOPE

This research presented the design and development of a low-cost Smart Security Door System based on a Raspberry Pi, PIR sensor, HMI touchscreen, password authentication mechanism, servo motor, and buzzer. The implemented prototype demonstrated the ability to detect human presence, verify user credentials, operate the door-locking mechanism automatically, and generate an audible warning after repeated unsuccessful password attempts. The combination of these components resulted in a compact, straightforward, and user-friendly solution for electronic access control.

Laboratory testing showed that the system achieved a 98% accuracy in PIR-based detection and 100% accuracy in password authentication. The average time required for the door mechanism to respond after successful authentication was approximately 1.5 seconds, while the buzzer alert was activated within approximately 0.5 seconds after the specified security condition was met. These results indicate that the proposed system can provide dependable access control with a relatively fast response to both authorized users and potential unauthorized access attempts. Furthermore, the use of a Raspberry Pi and easily available electronic components makes the system a practical option for small-scale residential, educational, and commercial environments.

Although the developed prototype provides the required basic security functions, several improvements can be considered in future work. Possible enhancements include the integration of biometric authentication, RFID-based identification, remote monitoring capabilities, support for multiple users, improved HMI functionality, event and access logging, battery backup, and AI-based anomaly detection. Further optimization of the hardware and software could also improve reliability, reduce system response time, and support deployment in larger or more demanding security environments. The inclusion of additional authentication and protection mechanisms could further extend the applicability of the system for advanced residential and commercial access-control applications.

ACKNOWLEDGEMENT

The successful completion of this project was made possible through the support and facilities provided by various individuals and the institution. We sincerely express our gratitude to MAEER's MIT Arts, Commerce & Science College, Pune, for providing the necessary laboratory facilities, infrastructure, and resources required for the development and experimental testing of this project. We also extend our appreciation to everyone who provided guidance, encouragement, and support throughout the completion of this work.

REFERENCES

[1] N. Surantha and W. R. Wicaksono, “Design of smart home security system using object recognition and PIR sensor,” *Procedia Computer Science*, vol. 135, pp. 465–472, 2018, doi: 10.1016/j.procs.2018.08.198.

[2] Z. Muslimin, M. A. Wicaksono, M. F. Fadlurachman, and I. Ramli, "Rancang bangun sistem keamanan dan pemantau tamu pada pintu rumah pintar berbasis Raspberry Pi dan Chat Bot Telegram," Jurnal Penelitian Enjiniring, 2019, doi: 10.25042/jpe.112019.05.

[3] P. K. Prayogo, L. P. Pratama, and D. Junesco, "Home security system based on Raspberry Pi and PIR sensor using WhatsApp Messenger," Journal of Global Engineering Research and Science, vol. 4, no. 1, 2025, doi: 10.56904/j-gers.v4i1.134.

[4] A. H. Azhar, M. F. I. Othman, N. Bahaman, M. Z. Mas'ud, and Z. Sa'aya, "Implementation of home security motion detector using Raspberry Pi and PIR sensor," Journal of Advanced Computing Technology and Application, vol. 3, no. 2, pp. 41–50, 2021.

[5] S. Vinodhini, S. Gnanavarshini, S. Eby, and D. P. P. A., "Password based smart doorlock system using Arduino UNO for enhanced security," IRO Journal on Sustainable Wireless Systems, vol. 6, no. 2, pp. 95–109, 2024, doi: 10.36548/jsws.2024.2.002.

[6] V. Kolluru, "Password based door lock system," SSRN Electronic Journal, 2021, doi: 10.2139/ssrn.3918717.

[7] S. Goswami, A. Choudhury, S. Das, T. Banerjee, and S. Ghosh, "Automated password protected door lock system," Advances in Industrial Engineering and Management, vol. 6, no. 1, pp. 48–52, 2017.

[8] H. L. Harishni, S. Srisha, and S. Sandhya, "Design and simulation of an Arduino-based password-protected door locking system," International Journal of Engineering and Advanced Technology, vol. 14, no. 2, 2024, doi: 10.35940/ijeat.B4550.14021224.

[9] P. Tuptewar, C. Rahangdale, S. Patil, and A. Patil, "Contactless door lock system by using Raspberry PI," SSRN Electronic Journal, 2025.

[10] P. Tuptewar, C. Rahangdale, S. Patil, A. Patil, and K. Barje, "Contactless door opening system by using Raspberry PI," SSRN Electronic Journal, 2025.

[11] M. B. Bazezew, "Home surveillance and alert system using Raspberry Pi Zero W and GSM modem with MQTT protocol," Indian Journal of Artificial Intelligence and Neural Networking, 2023, doi: 10.54105/ijainn. D4071.023223.

[12] D. Mangal, A. Tiwari, and S. Singhal, "Pi-Security: An IoT based home security system," International Journal of Advanced Science and Technology, vol. 29, no. 5, pp. 5682–5688, 2020.

[13] G. Orna, D. S. Benitez, and N. Perez, "A low-cost embedded facial recognition system for door access control using deep learning," in Proc. IEEE ANDESCON, 2020, Art. no. 9271984, doi: 10.1109/ANDESCON50619.2020.9271984.

[14] M. S. Ahmed, M. N. Ahmed, M. M. Hussain, and S. O. Farooq, "Smart and secure door lock with dual-factor authentication for critical zones," Mathematical Statistician and Engineering Applications, vol. 72, no. 1, pp. 1491–1501, 2023, doi: 10.17762/msea. v72i1.2373.

[15] I. G. M. N. Desnanjaya and I. N. A. Arsana, "Home security monitoring system with IoT-based Raspberry Pi," Indonesian Journal of Electrical Engineering and Computer Science, vol. 22, no. 3, pp. 1295–1302, 2021, doi: 10.11591/ijeecs.v22.i3. pp1295-1302.

[16] V. S. Parmar, "Home security and automation system: An approach to reduce investment," International Journal of Advanced Research in Computer and Communication Engineering, 2020, doi: 10.17148/IJARCCE.2020.9635.

[17] M. Margapuri, N. Penumajji, and M. Neilsen, "PiBase: An IoT-based security system using Raspberry Pi and Google Firebase," arXiv, 2021.

[18] R. Keerthana and S. Govardhini, "A survey on door access security control system via Raspberry Pi," International Journal of Advance Research, Ideas and Innovations in Technology, vol. 4, no. 5, 2018.

[19] S. Balani, B. Swathi, and N. B. Shrestha, "Survey on home security surveillance system based on Wi-Fi connectivity using Raspberry Pi and IoT module," International Journal of Advanced Research in Computer Science, vol. 9, no. 2, 2018, doi: 10.26483/ijarcs. v9i2.5585.

[20] F. I. Obianke, E. C. Obianke, and G. U. Obianke, "Design and implementation of a password-based smart door lock system with GSM-based alert and surveillance," Iconic Research and Engineering Journals, vol. 9, no. 10, pp. 5038–5052, 2026, doi: 10.64388/IREV9I10-1716218.