International Journal of Engineering, Industrial, Maritime, and Technological Innovation (INJENI) P - ISSN: 3116-3807 E - ISSN: 3116-3815

PRC-CPD Accredited Provider: PTR-2025-749

NBDB Registration Book Publisher (Print & Digital): 0312

DefenDoor: An electromagnetic fingerprint-based access control system with forced-entry detection and SMS notification

Gliann E. Josol*[1], Khryss Andrew L. Lozada[2], Teshaun Louisse S. Mercurio[3], Charlane M. Diasnes[4]
[1, 2, 3, 4] Banga National High School, Barangay Benitez, Banga, South Cotabato, Philippines
*Corresponding Author e-mail: *gliannjosol@gmail.com*

Received: 18 February 2026 **Revised**: 30 March 2026 **Accepted**: 03 April 2026

Available Online: 05 April 2026

Volume 1 (2026), Issue 2, P-ISSN – 3116-3807; E-ISSN - 3116-3815

https://doi.org/10.63498/injeni3

Abstract

Aim: This study aimed to evaluate the performance of the DefenDoor security system, an electromagnetic fingerprint-based access control system with forced-entry detection and SMS notification, in terms of accuracy, response time, and operational reliability.

Methodology: A quantitative experimental research design was employed using prototype-based system testing in a controlled laboratory environment. The system was evaluated through 10 fingerprint authentication trials per authorized user and 10 forced-entry simulations for each sensor configuration. Both authorized and unauthorized fingerprint scans were tested. Response times were measured using a digital oscilloscope, while system accuracy and reliability were recorded using structured observation sheets. Descriptive statistics, one-way analysis of variance (ANOVA), and paired-samples t-tests were applied at the 0.05 level of significance.

Results: The fingerprint recognition system achieved 93.3% accuracy in identifying authorized users and 100% accuracy in rejecting unauthorized attempts, with mean response times ranging from 50 to 53 milliseconds and no significant differences among users. The forced-entry alarm system demonstrated 100% detection accuracy and near-instant response times under both one-contact and two-contact sensor configurations. SMS notifications showed longer response times and achieved a delivery accuracy of 90%. No significant differences were observed between the two sensor configurations.

Conclusion: The DefenDoor system demonstrates reliable performance in biometric access control and forced-entry detection. Local alarm activation provides immediate intrusion alerts, while SMS notifications enable remote monitoring despite network-related transmission delays. The system presents a practical and cost-effective security solution for residential, educational, and small institutional environments.

Keywords: *fingerprint recognition, biometric access control, forced-entry detection, security system, SMS notification*

INTRODUCTION

Burglary is defined as the unlawful entry into a building or structure with the intent to commit a secondary crime, typically theft or another offense (Blurton, 2024). In 2023, approximately 841,924 burglary incidents were reported across the United States, according to the Federal Bureau of Investigation's Uniform Crime Reporting Program (Federal Bureau of Investigation [FBI], 2026). Mid-year analyses of major U.S. cities further indicated fluctuations in burglary trends during the first half of 2025 (Lopez & Boxerman, 2025).

In the Philippines, national surveys showed that a notable percentage of Filipino families reported being victimized by common crimes such as pickpocketing, break-ins, and robbery in late 2024, reflecting ongoing public safety concerns and heightened fear of burglary among the public (Social Weather Stations, 2024). Casilao (2023) reported that property-related crimes such as theft remain among the most prevalent offenses, indicating their continued impact across communities. Traditional security measures such as manual locks and neighborhood watch programs have long been staples of home safety. However, as criminal activities evolve and adapt to modern environments, these measures have increasingly been supplemented with advanced technological solutions such as closed-circuit television (CCTV), intrusion alarms, biometric door locks, and motion-activated lighting. According to Torres-Hernandez et al. (2025), modern smart home security systems integrate surveillance cameras, smart locks, and motion sensors to provide real-time monitoring and control, enhancing overall security and convenience for homeowners.

International Journal of Engineering, Industrial, Maritime, and Technological Innovation (INJENI)
P - ISSN: 3116-3807
E - ISSN: 3116-3815
PRC-CPD Accredited Provider: PTR-2025-749
NBDB Registration Book Publisher (Print & Digital): 0312

Recent advancements in engineering highlight the convergence of biometric authentication, embedded systems, and communication technologies in enhancing modern security solutions. For example, Permana et al. (2024) designed an IoT (Internet of Things) enabled door lock system that integrates fingerprint recognition with real-time data exchange, demonstrating the efficiency of combining hardware and software components. In a similar approach, Kanagamalliga et al. (2025) utilized GSM (Global System for Mobile Communications) technology alongside biometric access control to support remote monitoring and alert functions without relying on constant internet connectivity. These innovations underscore the increasing significance of integrating embedded and communication technologies to improve overall system performance and reliability.

Property-related crimes remain a significant concern, particularly for small and medium establishments that often lack sufficient resources to implement advanced security measures. Empirical evidence suggests that theft and robbery can negatively affect business operations and stability, especially among micro-level enterprises. In the Philippine context, the study of Manansala and Valerio (2024) found that property crimes substantially impact microfirms' performance, as limited access to security infrastructure increases their vulnerability to criminal incidents. These findings highlight the critical need for accessible and effective security solutions to mitigate risks associated with property-related crimes.

Break-ins often occur when occupants are away from home, such as during vacations; however, such incidents may also occur at any time, highlighting the importance of securing homes and businesses year-round. Many burglaries take place when residents are absent, and in some cases, these incidents may escalate into aggressive encounters. The installation of security devices, such as surveillance cameras and alarm systems, plays a vital role in reducing the likelihood of such events. Studies and industry reports have shown that homes equipped with security systems are less likely to be targeted by burglars (Gabriele, 2025).

This study reviewed the role of modern home security technologies in crime prevention, particularly electromagnetic fingerprint access systems, forced-entry alarms, and real-time short message service (SMS) notifications. Technological advancements in security systems have reshaped the landscape of crime prevention. Historically, home security systems were limited to basic alarms and locks, but the rise of smart technologies led to the integration of features such as real-time monitoring, automated access controls, and surveillance enhancements. This transformation in security technology addressed the evolving needs of households and institutions seeking stronger protection against burglary and unauthorized entry.

While many security systems now incorporate biometric features, the DefenDoor system introduced a unique offline-ready security solution by integrating electromagnetic fingerprint access, a forced-entry alarm, and SMS notification that operated without internet connectivity. Unlike many contemporary systems that primarily rely on cloud platforms, mobile applications, or internet-based communication for monitoring and alerts, the DefenDoor system emphasized local detection and GSM-based notification to support use in areas with unstable or limited internet service.

The research gap identified in previous studies involved the limited evaluation of fully integrated, cost-effective security systems that combined (1) biometric access control, (2) forced-entry detection, and (3) SMS-based emergency alerting in a single offline-capable design. Although previous works commonly examined fingerprint locks, IoT-based door systems, or remote alert mechanisms independently, fewer studies evaluated these components as one coordinated system with measurable performance indicators under forced-entry conditions. In addition, prior works often reported general performance outcomes but did not consistently provide instrument-based response-time measurements such as millisecond-level timing using an oscilloscope across users and sensor configurations. This study addressed these limitations by developing and experimentally evaluating an integrated system under controlled trials, measuring both accuracy and response-time performance for access control and forced-entry response.

The present study contributes to security technology research by providing empirical performance evidence for an integrated, offline-capable biometric security system. Beyond technical evaluation, the study offered practical value for homes, schools, and small businesses by presenting an approach designed for local environments where rapid on-site alerts and reliable remote notification may be needed despite network constraints. By combining biometric authentication, forced-entry alarm activation, and SMS notification into a cohesive and cost-effective solution, the DefenDoor system supported quicker response initiation and strengthened protective measures against unauthorized access.

Review of Related Literature and Studies

The development of IoT-based smart door lock systems has significantly enhanced home security by integrating advanced biometric and communication technologies. Permana et al. (2024) introduced an IoT-based smart door lock system that combines fingerprint authentication and a keypad, using Firebase for real-time communication and remote control via Android applications. The system demonstrated a 100% success rate during black-box testing, highlighting its

International Journal of Engineering, Industrial, Maritime, and Technological Innovation (INJENI)
P - ISSN: 3116-3807
E - ISSN: 3116-3815
PRC-CPD Accredited Provider: PTR-2025-749
NBDB Registration Book Publisher (Print & Digital): 0312

effectiveness for both residential and commercial security applications. This integration of biometric authentication and remote control exemplifies the growing trend of using smart technologies to improve security. However, the system relied on internet-based communication and cloud infrastructure, which may limit its functionality in areas with unstable connectivity.

Similarly, Sutikno et al. (2024) developed a wireless fingerprint-based door lock system that utilizes Arduino and smartphone integration. The system showed reliable performance, with fast response times for authentication and data transmission, making it a promising solution for enhancing residential security. The use of Bluetooth communication eliminates the need for additional infrastructure, offering an efficient solution for smaller homes or remote areas. These studies reflect the ongoing trend of combining biometric systems with wireless technologies to improve both accessibility and security. Nevertheless, the study focused primarily on authentication mechanisms and did not integrate forced-entry detection or emergency notification systems into a single offline-capable platform.

Further innovations focus on multi-modal authentication to enhance security by integrating fingerprint recognition with other biometric methods, such as facial recognition. Barfield et al. (2025) designed an advanced IoT-based smart lock system that combines facial recognition and fingerprint authentication. The system offers real-time notifications and role-based access control, utilizing a cloud-based interface to enable remote door management, access logging, and differentiated user permissions. Initial testing confirmed accurate biometric recognition, reliable remote access, and effective alert mechanisms, making this system a promising solution for smart home security. Despite its advanced features, the system depended on cloud-based infrastructure and continuous internet access, which may not be suitable for low-resource or connectivity-limited environments.

Despite advancements, security vulnerabilities in IoT-based smart home systems remain a significant challenge. Vardakis et al. (2024) examined security risks in IoT-enabled smart homes, focusing on devices such as home assistants, smart TVs, locks, and sensors. The study highlighted threats like unauthorized access, data breaches, and device tampering, which can undermine the effectiveness of modern security systems. The authors emphasize the importance of encryption, authentication, and intrusion detection mechanisms to safeguard smart home systems, and stress the need for user awareness in mitigating these risks. This highlights the need for security systems that minimize external network dependence while maintaining reliable local detection and alert capabilities.

In response to these vulnerabilities, multi-factor authentication (MFA) has become a key feature in modern security systems. Suneetha et al. (2025) developed an IoT-enabled biometric door lock system that combines fingerprint and facial recognition for dual authentication. This system enables real-time monitoring through email notifications, and LCD displays provide status updates and alerts for unauthorized access. By combining multi-factor authentication with IoT-based monitoring, the system enhances both security and user convenience, addressing the increasing demand for multi-layered security solutions in smart homes. However, as this work was disseminated as a preprint and relied on internet-based monitoring and email alerts, further empirical validation of offline-integrated systems remains necessary.

As affordability remains a concern for many, particularly in developing countries, researchers have explored creating low-cost security solutions. Emetere et al. (2023) focused on affordable security technologies tailored to low-income households. Their systems balance cost-effectiveness with user convenience, proposing unmonitored, low-cost systems that could significantly reduce crime rates in vulnerable communities. These studies emphasize the importance of creating scalable solutions that make home security accessible to a wide range of socioeconomic groups.

The use of Arduino and various sensors for creating customizable home automation systems has become central to improving both security and home convenience. Porje et al. (2025) presented an IoT-based home automation system using Arduino and integrated sensors for improved security and flexibility. The system supports both online and offline operation via smartphones and web interfaces, allowing users to manage multiple devices simultaneously. By combining password protection and remote access, the system offers a cost-effective solution for home automation, demonstrating the practical integration of IoT in modern homes.

Finally, Burglary incidents are more likely to occur when opportunities arise due to reduced surveillance, such as when occupants are absent. Preventive measures, including home security systems and monitoring devices, are designed to increase the risk of detection and discourage potential offenders from committing crimes. These deterrent mechanisms significantly influence criminal decision-making by making targeted properties less attractive and more difficult to access (Bankiewicz & Papadouka, 2024).

The reviewed studies highlighted significant advancements in biometric-based security systems, including fingerprint authentication, multi-modal biometrics, and remote alert mechanisms. However, most prior works examined these components independently or relied heavily on internet-dependent infrastructure. A GSM communication module enables wireless data transmission over cellular networks, allowing embedded systems to send SMS notifications. The SMS

International Journal of Engineering, Industrial, Maritime, and Technological Innovation (INJENI) P - ISSN: 3116-3807 E - ISSN: 3116-3815

PRC-CPD Accredited Provider: PTR-2025-749

NBDB Registration Book Publisher (Print & Digital): 0312

transmission mechanism involves encoding and transmitting text messages through the GSM network to a designated mobile number. A clear gap remained in the integration of (1) biometric fingerprint-based access control, (2) forced-entry detection through contact sensors, and (3) GSM-based short message service (SMS) notification operating independently of internet connectivity within a single cohesive and experimentally evaluated system. Furthermore, few studies reported precise instrument-based response-time measurements under controlled forced-entry simulations. This study addressed these gaps by developing and experimentally evaluating an integrated, offline-capable security system designed for cost-effective deployment in residential, educational, and small-business settings.

Theoretical and Technical Frameworks

This study is grounded primarily in engineering and system design principles to align with the technical nature of the proposed biometric security system. It uses Systems Engineering Architecture, Embedded Systems Design, Control Systems Theory, and Reliability Engineering Models as its main technical foundations.

At the core of the study is Systems Engineering Architecture, which provides a structured approach to the design, development, and integration of complex systems. According to Kossiakoff et al. (2011), systems engineering defines the relationships among components, subsystems, inputs, processes, and outputs to ensure reliable and efficient system operation. In this study, it guides the overall design of the offline biometric fingerprint access system, particularly the interaction among the fingerprint scanner, microcontroller, alarm module, GSM module, and locking mechanism.

Supporting this is Embedded Systems Design, which focuses on integrating hardware and software to perform dedicated functions under real-time and resource constraints. Embedded systems are designed for efficiency, timing, and reliability, with microcontrollers interfacing with sensors, actuators, and communication components to support responsive and application-specific control (Lambert, 2017). In this study, this framework explains how the fingerprint sensor, GSM module, forced-entry detection mechanism, and microcontroller are integrated to provide secure and responsive access control.

The study also incorporates Control Systems Theory, which explains how system inputs, outputs, and feedback mechanisms are coordinated to achieve stable and desired performance in engineered systems (Zywno, 2023). In this study, Control Systems Theory is relevant in explaining how the biometric sensor, contact sensors, alarm system, GSM module, and locking mechanism function as a coordinated control process, ensuring accurate and consistent system responses to authentication inputs and forced-entry events.

To further strengthen the technical basis, the study adopts Reliability Engineering Models, which emphasize the consistent and dependable operation of system components over time under specified conditions (BCcampus Open Education, 2018). In this study, reliability engineering supports the evaluation of the fingerprint sensor, GSM module, alarm system, and locking mechanism in terms of stability, accuracy, and dependable performance under repeated testing conditions.

Overall, this framework guided the design of the system architecture, the integration of hardware and software, the regulation of system response, and the evaluation of system performance. Through this engineering-centered approach, the study is positioned as a practical, dependable, and effective embedded biometric security solution.

Conceptual Framework

The conceptual framework for this study illustrates the relationships among key concepts in the biometric fingerprint-based door security system. The system setup served as the independent variable (IV), specifically defined by two levels: (1) one-contact sensor configuration and (2) two-contact sensor configuration integrated with the fingerprint recognition system. The dependent variables (DV) were the measurable performance indicators of the system, namely: (a) fingerprint recognition accuracy expressed as percentage of correct identification, (b) response time measured in milliseconds (ms) for fingerprint authentication, alarm activation, and SMS transmission, (c) alarm detection accuracy expressed as percentage of successful forced-entry detection, and (d) SMS notification delivery rate expressed as percentage of successful message transmission to the designated authority. This relationship was examined by comparing system performance across the two sensor configurations to determine whether significant differences existed in accuracy and response-time metrics.

International Journal of Engineering, Industrial, Maritime, and Technological Innovation (INJENI)
P - ISSN: 3116-3807
E - ISSN: 3116-3815
PRC-CPD Accredited Provider: PTR-2025-749
NBDB Registration Book Publisher (Print & Digital): 0312

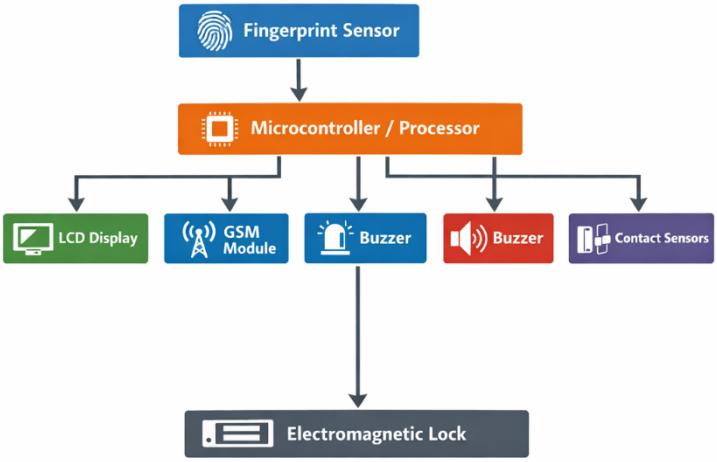

Figure 1. Block Diagram

Statement of the Problem

Unauthorized access and burglary remain persistent security concerns in residential, commercial, and institutional environments. Traditional security measures such as mechanical locks and neighborhood watch programs provide only limited protection and are increasingly insufficient in addressing modern intrusion threats. As security risks evolve, there is a growing need for integrated technological systems capable of providing reliable authentication, intrusion detection, and rapid alert mechanisms.

Advances in biometric authentication and automated monitoring technologies have enabled the development of intelligent security systems that enhance access control and incident detection. However, many existing smart security solutions rely heavily on internet connectivity and cloud-based infrastructures, which may limit their effectiveness in areas with unstable or unavailable network access. Furthermore, previous studies have often evaluated biometric authentication, intrusion detection, and remote notification systems independently rather than as a fully integrated security platform.

In response to these technological limitations, this study focuses on the development and evaluation of an electromagnetic fingerprint-based door access control system integrated with a forced-entry detection mechanism and SMS notification capability. The proposed system combines biometric authentication, sensor-based intrusion detection, and GSM-based communication to provide both local and remote security alerts.

This study evaluates the performance of the system in terms of authentication accuracy, detection reliability, response time, and SMS notification effectiveness. In addition, the study investigates whether different sensor configurations (one-contact and two-contact sensors) influence the performance of the security system. Through experimental testing and statistical analysis, the research aims to determine the effectiveness and reliability of the proposed system as a cost-effective security solution for environments with limited internet connectivity.

Research Objectives

General Objective

To design, develop, and evaluate the performance of an electromagnetic fingerprint-based door access control system with forced-entry detection and SMS notification for enhancing security through reliable biometric authentication and automated intrusion alerting.

Specific Objectives

1. To determine the accuracy of the fingerprint recognition system in identifying authorized and unauthorized users.
2. To measure the response time of the fingerprint recognition system in activating the electromagnetic door lock mechanism.

International Journal of Engineering, Industrial, Maritime, and Technological Innovation (INJENI) P - ISSN: 3116-3807 E - ISSN: 3116-3815
PRC-CPD Accredited Provider: PTR-2025-749
NBDB Registration Book Publisher (Print & Digital): 0312

3. To evaluate the accuracy of the forced-entry alarm system and SMS notification under one-contact and two-contact sensor configurations.
4. To determine the response time of the alarm system and SMS notification during forced-entry detection under one-contact and two-contact sensor configurations.
5. To assess the reliability of SMS notification delivery from forced-entry detection to transmission to the designated authority.
6. To determine whether there is a significant difference in fingerprint recognition response time among different users.
7. To determine whether there is a significant difference in the response times of the alarm system and SMS notification between one-contact and two-contact sensor configurations.

Research Questions

1. What is the accuracy of the fingerprint recognition system in identifying:
   a. authorized fingerprints;
   b. unauthorized fingerprints?
2. What is the response time of the fingerprint recognition system in activating the electromagnetic door lock mechanism?
3. What is the accuracy of the alarm system and SMS notification during forced-entry detection under the following configurations:
   a. one-contact sensor;
   b. two-contact sensor?
4. What is the response time of the alarm system and SMS notification during forced-entry detection under the following configurations:
   a. one-contact sensor;
   b. two-contact sensor?
5. What is the accuracy of SMS notification delivery from forced-entry detection to transmission to the designated authority?
6. Is there a significant difference in fingerprint recognition response time among different users?
7. Is there a significant difference in the response times of the alarm system and SMS notification between one-contact and two-contact sensor configurations?

Hypotheses

Hypothesis 1 (Fingerprint Response Time Across Users)
Null Hypothesis (H_0):
There is no significant difference in fingerprint recognition response time among different users.
Alternative Hypothesis (H_1):
There is a significant difference in fingerprint recognition response time among different users.

Hypothesis 2 (Sensor Configuration Response Time)
Null Hypothesis (H_0):
There is no significant difference in the response times of the alarm system and SMS notification between one-contact and two-contact sensor configurations.
Alternative Hypothesis (H_1):
There is a significant difference in the response times of the alarm system and SMS notification between one-contact and two-contact sensor configurations.

International Journal of Engineering, Industrial, Maritime, and Technological Innovation (INJENI)
P - ISSN: 3116-3807
E - ISSN: 3116-3815
PRC-CPD Accredited Provider: PTR-2025-749
NBDB Registration Book Publisher (Print & Digital): 0312

METHODS

Research Design

This study employed a quantitative experimental research design to evaluate the performance of the DefenDoor security system. The design utilized prototype development, controlled system testing, and performance evaluation, which are common approaches in engineering research. It enabled the researchers to manipulate the independent variable, specifically the sensor configuration (one-contact and two-contact sensor setups), and measure its effects on the dependent variables, namely fingerprint recognition accuracy, response time, alarm activation, and SMS notification reliability**.** Quantitative data were collected in numerical form to allow objective measurement and statistical analysis of system performance. This design was appropriate because it allowed precise comparison of system behavior across configurations and users, providing measurable evidence of the effectiveness of the proposed security system.

Materials, Systems or Components

The DefenDoor security system is centered on the Arduino Nano microcontroller, which functions as the main control and processing unit. The system integrates multiple input, output, communication, and power components to perform biometric authentication, intrusion detection, and remote notification. The power supply subsystem consists of a 7.4 V lithium-ion battery pack (18650 cells) connected to a 2S battery charging module for safe charging and protection. A 5 V DC buck converter regulates the battery output to provide a stable voltage required by the Arduino and other electronic components. A manual power switch is included for system control. For input sensing, the system uses a fingerprint sensor connected to the Arduino via serial communication for user authentication. A magnetic contact sensor, which detects door status by sensing the separation of magnetic contacts, was used to monitor door opening and closing events. The processing unit, Arduino Nano, receives and processes signals from these input devices and controls all output operations. Based on authentication and sensor inputs, it triggers appropriate responses. The output and actuation components include a relay module that controls the solenoid lock, allowing or restricting door access. A buzzer provides audible alerts during unauthorized access or system events. Additionally, visual indicators such as LEDs (with current-limiting resistors) are used to display system status. For user feedback, an I2C LCD display (LCM1602/20x4) is connected to the Arduino to show real-time system messages such as access granted/denied and system alerts. The communication subsystem consists of a SIM800L GSM module, which is interfaced with the Arduino via UART communication. This module enables the system to send SMS notifications to a designated user in case of intrusion or security events. All components are interconnected using appropriate signal interfaces, including serial, UART, and I2C protocols, ensuring coordinated operation of the system. Through this integrated architecture, the DefenDoor system achieves secure biometric access control, real-time monitoring, and remote alert functionality.

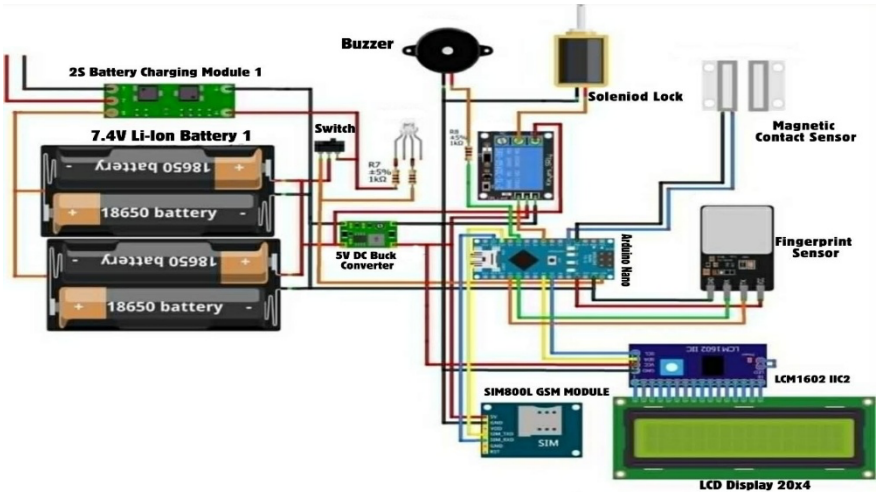

Figure 2. System Architecture

Instruments or Engineering Tools

A digital oscilloscope (FNIRSI-1014D) was used as the primary measurement instrument to evaluate system performance. The oscilloscope has a bandwidth of 100 MHz and a maximum sampling rate of 1 GSa/s, enabling accurate

International Journal of Engineering, Industrial, Maritime, and Technological Innovation (INJENI)
P - ISSN: 3116-3807
E - ISSN: 3116-3815
PRC-CPD Accredited Provider: PTR-2025-749
NBDB Registration Book Publisher (Print & Digital): 0312

capture of fast signal transitions in embedded systems. It was used to measure the signal initiation from the fingerprint sensor, activation signals of the electromagnetic lock, alarm triggering signals, and the timing of SMS notification activation. The oscilloscope provided millisecond-level precision, which was appropriate for response-time analysis.

Data Collection and Testing Procedures

Data were collected through prototype-based testing of the DefenDoor system conducted in a controlled laboratory environment. Testing commenced after the complete assembly and calibration of the system. During each testing session, authorized and unauthorized fingerprints were repeatedly scanned using the fingerprint sensor to assess recognition accuracy. Forced-entry scenarios were simulated under one-contact and two-contact sensor configurations to evaluate alarm activation and SMS notification performance. For each trial, system responses, including successful access, access denial, alarm triggering, and SMS transmission, were observed and recorded. Response times were measured in milliseconds using the digital oscilloscope and system-generated logs. During the experiments, the oscilloscope probe channels were connected to the relevant output pins of the Arduino Nano and associated modules. A sampling setting of 5 kS/s (5000 samples per second) was used during measurements to capture system-level response timing events. This setup enabled accurate monitoring of signal transitions corresponding to authentication, alarm activation, and communication processes. To ensure measurement reliability, oscilloscope readings were cross-validated with system-generated logs, particularly for SMS transmission events. All observations were immediately documented using structured data recording sheets and later compiled into tables for statistical analysis.

Data Analysis

Quantitative statistical methods were used to analyze the collected data. Descriptive statistics were used to answer Research Questions 1 to 5 by computing accuracy percentages, mean response times, and standard deviations**.** A one-way analysis of variance (ANOVA) was used to address Research Question 6 by comparing fingerprint recognition response times across users. Paired-samples t-tests were conducted to address Research Question 7 by comparing trial-by-trial response times between one-contact and two-contact sensor configurations for both the alarm system and SMS notification. The pairing was performed by matching corresponding forced-entry trials under the one-contact and two-contact configurations to ensure equivalent comparison conditions. All response time measurements were derived from oscilloscope readings to ensure precision. The results were tabulated and interpreted to assess the efficiency and reliability of the DefenDoor system. For inferential statistical tests, a significance level of $\alpha = 0.05$ was used as the decision threshold for accepting or rejecting the null hypothesis.

Ethical and Safety Considerations

The study was conducted in accordance with established ethical standards to ensure safety, privacy, and responsible system use. Ethical approval was obtained from the administration of Banga National High School prior to data collection. All participants provided informed consent before fingerprint enrollment and testing. Participants were informed about the purpose of the study, the voluntary nature of participation, and their right to withdraw at any time. No personally identifiable biometric data were stored beyond the testing period. Permission was also secured for the use of the testing venue and communication facilities required for SMS notification. Fingerprints used during testing were registered solely for evaluation purposes, and all collected data were securely stored to prevent unauthorized access. SMS notifications were transmitted only to pre-approved recipients to avoid privacy violations or unintended alarms. All procedures were carried out with appropriate safety measures to ensure that system testing posed no risk to individuals or property.

International Journal of Engineering, Industrial, Maritime, and Technological Innovation (INJENI)
P - ISSN: 3116-3807
E - ISSN: 3116-3815
PRC-CPD Accredited Provider: PTR-2025-749
NBDB Registration Book Publisher (Print & Digital): 0312

RESULTS and DISCUSSION

This section presents the results and discussion of the study, including the analysis and interpretation of the data collected from the experimental evaluation of the system's performance in terms of accuracy, response time, and reliability.

Table 1. Accuracy of the Fingerprint Recognition

No. of Trials	Authorized Fingerprint			No. of Trials	Unauthorized Fingerprint		
	User 1	User 2	User 3		User 1	User 2	User 3
1	1	1	1	1	0	0	0
2	1	1	1	2	0	0	0
3	1	1	1	3	0	0	0
4	1	1	1	4	0	0	0
5	1	1	1	5	0	0	0
6	1	1	1	6	0	0	0
7	1	1	1	7	0	0	0
8	0	1	1	8	0	0	0
9	1	1	1	9	0	0	0
10	1	1	0	10	0	0	0
Error (X)	1	0	1	**Error (✓)**	0	0	0
Correct (✓)	9	10	9	**Correct(X)**	10	10	10

Table 1 presents the accuracy of the fingerprint recognition system in identifying authorized and unauthorized users across three participants. For authorized fingerprints, the system correctly recognized 9 out of 10 trials for User 1, 10 out of 10 trials for User 2, and 9 out of 10 trials for User 3, corresponding to an overall accuracy of 93.3%. A total of two false rejections occurred for authorized users (one for User 1 and one for User 3). For unauthorized fingerprints, the system correctly rejected all attempts for all users, resulting in 100% accuracy with no false acceptances. These results indicate that the fingerprint recognition system is highly reliable in distinguishing authorized users from unauthorized individuals, with minimal false rejections among legitimate users.

This finding is supported by the study of Jaafa et al. (2021), which reported that fingerprint-based biometric systems demonstrate high reliability, characterized by very low false rejection rates for authorized users and zero or near-zero false acceptance rates for unauthorized attempts, reinforcing the effectiveness of fingerprint recognition technologies in access control and identity verification applications.

Table 2. Fingerprint Recognition Response Time

No. of Trials	Fingerprint Recognition Response Time (ms)		
	User 1	User 2	User 3
1	50 ms	50 ms	50 ms
2	50 ms	50 ms	50 ms
3	50 ms	60 ms	50 ms
4	56 ms	50 ms	50 ms
5	50 ms	60 ms	50 ms
6	50 ms	50 ms	56 ms
7	60 ms	50 ms	50 ms
8	50 ms	56 ms	50 ms
9	50 ms	50 ms	56 ms
10	56 ms	56 ms	50 ms
Total	**522 ms**	**532 ms**	**512 ms**
Mean	**52.2 ms**	**53.2 ms**	**51.2 ms**

Table 2 presents the response times of the fingerprint recognition system in unlocking the door for three users across ten trials. The mean response times were 52.2 ms for User 1, 53.2 ms for User 2, and 51.2 ms for User 3, indicating consistently fast system performance. Response times across trials ranged from 50 ms to 60 ms, showing minimal variability and demonstrating the system's reliability in processing authorized fingerprints. Overall, these results suggest that the fingerprint recognition system is capable of unlocking the door almost instantaneously, with stable performance across

International Journal of Engineering, Industrial, Maritime, and Technological Innovation (INJENI)
P - ISSN: 3116-3807
E - ISSN: 3116-3815
PRC-CPD Accredited Provider: PTR-2025-749
NBDB Registration Book Publisher (Print & Digital): 0312

different users. This finding aligns with the study of Padmaja Devi et al. (2025) in biometric systems, where fingerprint-based recognition and identification have been demonstrated to complete the authentication process in under two seconds, showcasing that fingerprint biometrics can deliver both speed and efficiency in real-time applications.

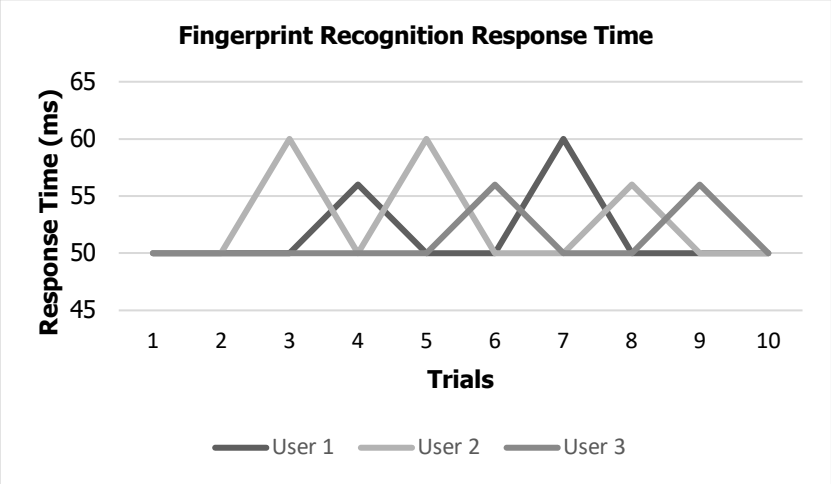

Figure 3. Fingerprint Recognition Response Time Across Users

Figure 3 illustrates the response time of the fingerprint recognition system across ten trials for three users. The graph shows that response times remain consistently within the range of 50 ms to 60 ms, with minimal variation between users. This visual representation supports the findings in Table 2, confirming that the system provides stable and fast authentication performance across different users.

Table 3. Accuracy of the Alarm System and SMS Notification for Forced-Entry

No. of Trials	Alarm System		SMS Notification	
	One Contact Sensor	Two Contact Sensor	One Contact Sensor	Two Contact Sensor
1	✓	✓	✓	✓
2	✓	✓	✓	✓
3	✓	✓	✓	✓
4	✓	✓	✓	✓
5	✓	✓	✓	✓
6	✓	✓	✓	✓
7	✓	✓	✓	✓
8	✓	✓	✓	X
9	✓	✓	✓	✓
10	✓	✓	✓	✓
Error(X)	**0**	**0**	**0**	**1**
Correct	**10**	**10**	**10**	**9**

Table 3 presents the accuracy of the alarm system and SMS notification in detecting forced-entry events under one- and two-contact sensor setups. The alarm system achieved 100% accuracy in both sensor setups, correctly detecting all ten forced-entry trials with no errors. The SMS notification system also performed with high accuracy, correctly identifying all 10 trials under the one-contact sensor setup and 9 out of 10 trials under the two-contact sensor setup, with only a single error recorded in one trial under the two-contact sensor condition. Overall, these results indicate that both the alarm system and SMS notifications are highly effective in detecting forced-entry events, with the alarm system demonstrating perfect reliability and SMS notifications showing minimal errors. This result is consistent with the findings of Feng et al. (2021), who reported that sensor-based security systems utilizing magnetic or contact-based detection mechanisms achieve high accuracy and reliability, particularly due to their resistance to environmental interference such as dust and oil.

International Journal of Engineering, Industrial, Maritime, and Technological Innovation (INJENI)
P - ISSN: 3116-3807
E - ISSN: 3116-3815
PRC-CPD Accredited Provider: PTR-2025-749
NBDB Registration Book Publisher (Print & Digital): 0312

Table 4. Response Time of the Alarm System and SMS Notification for Forced-Entry

No. of Trials	Alarm System Response Time (ms)		SMS Notification Response Time (ms)	
	One Contact Sensor	Two Contact Sensor	One Contact Sensor	Two Contact Sensor
1	100 ms	100 ms	1700 ms	1700 ms
2	100 ms	108 ms	1800 ms	1880 ms
3	108 ms	100 ms	1700 ms	1700 ms
4	100 ms	100 ms	1700 ms	1700 ms
5	116 ms	108 ms	1900 ms	1800 ms
6	100 ms	100 ms	1800 ms	1900 ms
7	100 ms	116 ms	1700 ms	1700 ms
8	100 ms	100 ms	1880 ms	1700 ms
9	108 ms	116 ms	1700 ms	1900 ms
10	100 ms	100 ms	1800 ms	1700 ms
Total	**1032 ms**	**1048 ms**	**17680 ms**	**17680 ms**
Mean	**103.2 ms**	**104.8 ms**	**1768.0 ms**	**1768.0 ms**

Table 4 presents the response times of the alarm system and SMS notifications for forced-entry detection under one- and two-contact sensor setups. The alarm system demonstrated significantly lower latency compared to SMS notifications, with mean response times of 103.2 ms for one-contact sensors and 104.8 ms for two-contact sensors. In contrast, SMS notifications had substantially longer mean response times of 1768.0 ms for both sensor setups. The alarm system also showed low variability, with most trials ranging from 100 to 116 ms, whereas SMS notifications demonstrated greater variability, with response times ranging from 1700 to 1900 ms. These results indicate that the alarm system provides near-instant alerts suitable for immediate response, while SMS notifications, although functional, are significantly slower and less consistent, highlighting the difference in timeliness between the two notification methods.

These findings are consistent with the framework proposed by De (2025), which emphasized that local alert mechanisms in intelligent perimeter security systems achieve significantly lower latency compared to remote notification channels due to reduced dependence on network transmission and external communication delays.

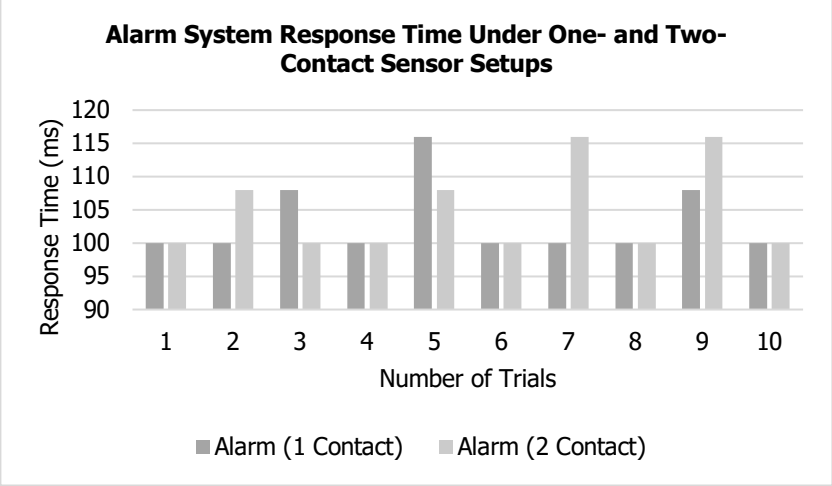

Figure 4. Alarm System Response Time Under One- and Two-Contact Sensor Setups

Figure 4 shows the response time of the alarm system under one- and two-contact sensor configurations. The results indicate that the system maintains low and consistent response times ranging from 100 ms to 116 ms, demonstrating fast and reliable detection of forced-entry events.

International Journal of Engineering, Industrial, Maritime, and Technological Innovation (INJENI)
P - ISSN: 3116-3807
E - ISSN: 3116-3815
PRC-CPD Accredited Provider: PTR-2025-749
NBDB Registration Book Publisher (Print & Digital): 0312

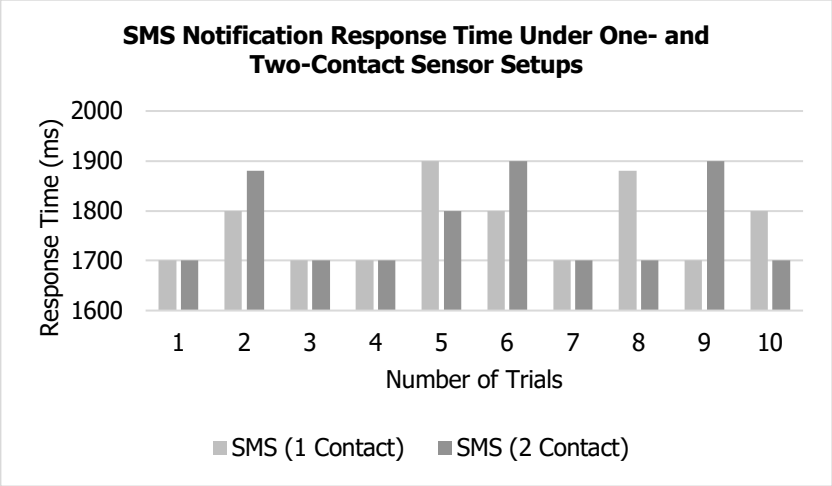

Figure 5. SMS Notification Response Time Under One- and Two-Contact Sensor Setups

Figure 5 shows the response time of SMS notifications under one- and two-contact sensor configurations. The results indicate that SMS response times range from 1700 ms to 1900 ms, demonstrating significantly higher latency compared to the alarm system due to network-dependent communication delays.

Table 5. Accuracy of the SMS Notification from Forced-Entry to Sending to the Authority

No. of Trials	SMS Notification to Authorities
1	1
2	1
3	1
4	1
5	1
6	1
7	1
8	0
9	1
10	1
Error (x)	**1**
Correct (✓)	**9**

Table 5 presents the accuracy of SMS notification delivery from forced-entry detection to transmission to the authorities. Out of ten trials, the SMS notification system successfully transmitted nine messages, resulting in an overall accuracy of 90%, with only one failed delivery. These results indicate that the SMS notification system is generally reliable in transmitting alerts to the authorities, although occasional transmission errors may occur, highlighting a minor limitation in dependability for real-time forced-entry notifications.

Similar observations were reported by Nasir et al. (2025), who demonstrated that GSM-based SMS alert systems remain viable for critical event notifications despite experiencing transmission delays and occasional reliability constraints. Their findings support the present study's conclusion that SMS notifications are effective for remote alerting, although they are inherently subject to network-related limitations.

International Journal of Engineering, Industrial, Maritime, and Technological Innovation (INJENI) P - ISSN: 3116-3807 E - ISSN: 3116-3815

PRC-CPD Accredited Provider: PTR-2025-749

NBDB Registration Book Publisher (Print & Digital): 0312

Table 6. ANOVA Results of Fingerprint Recognition Response Times Across Users

ANOVA

Response Time

	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	20.000	2	10.000	.770	.473
Within Groups	350.800	27	12.993		
Total	370.800	29			

Table 6 presents the results of a one-way ANOVA conducted to compare fingerprint recognition response times across three groups. The analysis revealed no significant differences between groups, F (2, 27) = 0.770, p = 0.473, indicating that the mean response times did not differ statistically. The between-group variance (SS = 20.000) was small relative to the within-group variance (SS = 350.800), suggesting that most variability in response time is attributable to individual differences rather than group membership. These results imply that the fingerprint recognition system performs consistently across the tested groups.

Table 7. Paired-Samples t-Test Results of Alarm System and SMS Notification Response Times Across Sensor Setups

System Type	Sensor Type	N	Minimum (ms)	Maximum (ms)	Mean (ms)	Std. Deviation (ms)
Alarm System	One Contact	10	100	116	103.2	5.59
Alarm System	Two Contact	10	100	116	104.8	6.75
SMS Notification	One Contact	10	1700	1900	1768.0	78.99
SMS Notification	Two Contact	10	1700	1900	1768.0	91.99

Table 7 shows the descriptive statistics of response times for the alarm system and SMS notifications under one- and two-contact sensor setups. The alarm system responded much faster than SMS notifications, with mean response times of 103.2 ms (one sensor) and 104.8 ms (two sensors), compared to 1768.0 ms for both SMS conditions. The alarm system also demonstrated low variability (SD = 5.59–6.75 ms), indicating consistent performance, whereas SMS notifications exhibited higher variability, particularly with two sensors (SD = 91.99 ms). Differences between one- and two-contact sensors were minimal within each system, suggesting that sensor quantity has little impact on response speed. Overall, these results indicate that the alarm system provides near-instant alerts suitable for immediate forced-entry detection, while SMS notifications, though useful for remote alerts, are slower and less consistent, making them less effective for time-critical responses.

Conclusions

The study demonstrates that the DefenDoor security system provides reliable performance in biometric access control and forced-entry detection through the integration of fingerprint authentication, contact sensor monitoring, and GSM-based notification. The fingerprint recognition subsystem achieved high identification accuracy while maintaining rapid response times, indicating efficient biometric processing suitable for real-time access control applications. The forced-entry detection mechanism exhibited perfect alarm activation accuracy under both sensor configurations, demonstrating the effectiveness of contact sensors for intrusion detection. However, the SMS notification subsystem showed longer response times and occasional transmission failure, reflecting the inherent limitations of network-dependent communication channels. Statistical analysis further confirmed that system performance remained consistent across users and sensor configurations. These findings indicate that the proposed system offers a practical and reliable security solution for residential, educational, and small institutional environments, particularly in locations with limited internet connectivity.

Recommendations

The existing recommendations already follow engineering standards. Minor wording improvements can strengthen technical clarity:

1. System operators may require multiple fingerprint samples during enrollment and conduct periodic re-enrollment to reduce the occurrence of false rejections observed among authorized users.

International Journal of Engineering, Industrial, Maritime, and Technological Innovation (INJENI)
P - ISSN: 3116-3807
E - ISSN: 3116-3815
PRC-CPD Accredited Provider: PTR-2025-749
NBDB Registration Book Publisher (Print & Digital): 0312

2. Developers may optimize the sensor polling interval and processing thresholds to maintain authentication latency below 60 milliseconds and ensure stable system performance.
3. Installers may ensure proper physical alignment and secure mounting of contact sensors to maintain high detection accuracy during forced-entry events.
4. The system may be configured so that local alarm activation operates independently from SMS transmission to ensure immediate on-site alerts.
5. Developers may implement automatic SMS retry mechanisms and delivery-status verification to improve notification reliability during network interruptions.
6. Future system testing may involve users with varied fingerprint conditions such as dry, wet, or worn fingerprints to evaluate system robustness under realistic operating conditions.
7. System designers may select a one-contact sensor configuration for cost-efficient installations or a two-contact configuration for redundancy depending on the operational environment.

REFERENCES

Bankiewicz, U., & Papadouka, M. E. (2024). Factors influencing burglary and home security measures in England and Wales. *European Journal of Criminology, 21*(2), 274–300. https://doi.org/10.1177/14773708231182777

Barfield, F. D. S., Pasag, S. P. E., Delmo, J. S. C., Gaila, D., Agustin, V. A., & Fernandez, R. B. (2025). Advanced smart lock system: Enhancing door security with biometric authentication and advanced technology features. *International Conference on Multidisciplinary Industry and Academic Research: Book of Abstracts, 6*(1). https://iiari.org/conference_abstract/advanced-smart-lock-system-enhancing-door-security-with-biometric-authentication-and-advanced-technology-features/

BCcampus Open Education. (2018). *Reliability engineering*. https://www.opentextbc.ca/oerdiscipline/wp-content/uploads/sites/213/2018/09/Reliability-Engineering.pdf

Blurton, D. (2024). Burglary. In *Research Starters Home*. EBSCO Knowledge Advantage. https://www.ebsco.com/research-starters/law/burglary

Casilao, J. L. (2023, January 9). PNP: Theft, rape, physical injury most prevalent crimes in last 6 months. *GMA News Online*. https://www.gmanetwork.com/news/topstories/nation/856765/pnp-theft-rape-physical-injury-most-prevalent-crimes-in-last-6-months/story/

De, A. (2025). A conceptual framework for multi-sensor human detection in intelligent perimeter security systems. *International Journal for Research in Applied Science and Engineering Technology*. https://doi.org/10.22214/ijraset.2025.72468

Emetere, M. E., Okpala, D. C., Bakeko, M. M., & Afolalu, S. A. (2023). Review on home security system in developing countries: Affordability or comfortability. *Journal of Computer Science, 19*(4), 415–430. https://doi.org/10.3844/jcssp.2023.415.430

Federal Bureau of Investigation. (2026). *Crime data explorer (CDE).* U.S. Department of Justice. https://cde.ucr.cjis.gov/LATEST/webapp/#/pages/home

Feng, T., Chen, W., Qiu, J., & Hao, S. (2021). A new kind of absolute magnetic encoder. *Sensors, 21*(9), Article 3095. https://doi.org/10.3390/s21093095

Gabriele, R. (2025, February 11). Home security statistics and trends. *SafeHome.org*. https://www.safehome.org/data/home-security-statistics/

Jaafa, N. K., Mokaya, B., Savai, S. M., Yeung, A., Siika, A. M., & Were, M. (2021). Implementation of fingerprint technology for unique patient matching and identification at an HIV care and treatment facility in Western Kenya: Cross-sectional study. *Journal of Medical Internet Research, 23*(12), e28958. https://doi.org/10.2196/28958

Kanagamalliga, S., Rajalingam, S., Kannan, A., & Karthikeyan, M. (2025). Biometric and IoT integration for secure and remote door access control using fingerprint recognition and GSM technology. *E3S Web of Conferences, 619*, 03013. https://doi.org/10.1051/e3sconf/202561903013

Kossiakoff, A., Sweet, W. N., Seymour, S. J., & Biemer, S. M. (2011). *Systems engineering principles and practice*. John Wiley & Sons. https://doi.org/10.1002/9781118001028

Lambert, T. R. (2017). *An introduction to microcontrollers and embedded systems*. Auburn University. https://www.eng.auburn.edu/~dbeale/MECH4240-50/Introduction%20to%20Microcontrollers%20and%20Embedded%20Systems.pdf

International Journal of Engineering, Industrial, Maritime, and Technological Innovation (INJENI)
P - ISSN: 3116-3807
E - ISSN: 3116-3815
PRC-CPD Accredited Provider: PTR-2025-749
NBDB Registration Book Publisher (Print & Digital): 0312

Lopez, E., & Boxerman, B. (2025). *Crime trends in U.S. cities: Mid-year 2025 update*. Council on Criminal Justice. https://councilоncj.org/crime-trends-in-u-s-cities-mid-year-2025-update/

Manansala, L. D., & Valerio, A. T. (2024). Impact of violent and property crimes on microfirms' performance: The Philippine experience. *Ho Chi Minh City Open University Journal of Science, 14*(3). https://doi.org/10.46223/HCMCOUJS.econ.en.14.3.2822.2024

Nasir, F. F. M., Ren, E. T. W., Rahman, K. A. A., & Noor, A. Z. M. (2025). Autonomous Blazebot: A real-time fire detection and SMS alert system using AI and GSM technology. *Jurnal Kejuruteraan, 37*(6), 3063–3074. https://doi.org/10.17576/jkukm-2025-37(6)-40

Padmaja Devi, K., Krishna, P. H., Bhuvanesh, M., & Trilok Sai, M. (2025). Fingerprint biometric-based attendance system. *International Journal of Innovative Research in Technology, 11*(12), 4000–4003. https://ijirt.org/publishedpaper/IJIRT178240_PAPER.pdf

Permana, K. A. K., Piarsa, I. N., & Cahyawan, A. (2024). IoT-based smart door lock system with fingerprint and keypad access. *Journal of Information Systems and Informatics, 6*(3), 2086–2098. https://doi.org/10.51519/journalisi.v6i3.844

Porje, S. D., Pisolkar, Y. S., Pisolkar, M. R., Porje, O. S., & Jagtap, G. R. (2025). Anti-theft door lock system using IoT for home security. *International Journal of Advanced Research in Science, Communication and Technology, 5*(4), 452–458. https://doi.org/10.48175/IJARSCT-24100

Social Weather Stations. (2024). *National survey on crime victimization: Families victimized by common crimes and cybercrimes (September 14–23, 2024).* https://www.sws.org.ph

Suneetha, K., Surya Teja, K., Jyothi, K., Ravi Kiran, K., & Vianey, E. (2025). *IoT-enabled biometric door lock system with enhanced security features* [Preprint]. SSRN. https://doi.org/10.2139/ssrn.5205290

Sutikno, T., Ubaidillah, M. A. F., Arsadiando, W., & Purnama, H. S. (2024). Fingerprint-based smart door lock system using Arduino and smartphone application. *Computer Science and Information Technologies, 5*(1), 91–98. https://doi.org/10.11591/csit.v5i1.p91-98

Torres-Hernandez, C. M., Garduño-Aparicio, M., & Rodriguez-Resendiz, J. (2025). Smart homes: A meta-study on sense of security and home automation. *Technologies, 13*(8), Article 320. https://doi.org/10.3390/technologies13080320

Vardakis, G., Hatzivasilis, G., Koutsaki, E., & Papadakis, N. (2024). Review of smart-home security using the Internet of Things. *Electronics, 13*(16), Article 3343. https://doi.org/10.3390/electronics13163343

Zywno, M. S. (2023). *Introduction to control systems*. Toronto Metropolitan University. https://pressbooks.library.torontomu.ca/controlsystems/