International Journal of Sustainability and Advanced Integrated Research
Volume 2, Issue 1 (January-March 2026) | ISSN: 3107-7854
DOI: https://doi.org/10.65339/ijsair.V2.I1.05

An Android Based Anti-Intrusion Device Using A Motion Sensor with Short Message Service Notification

Rommel V. Romero [1 *], Dr. Ma. Eugenia M. Yangco [2], Aljon Peter L. Temporal [3]

[1] *Information Technology Officer, Maritime Industry Authority, Manila City, Philippine*
[2] *Professor, Rizal Technological University, College of Engineering and Architecture, Mandaluyong City*
[3] *Assistant Professor, Our Lady of Fatima University, Antipolo City, Philippines*

Publication history: Received: December 22, 2025; Revised: January 8, 2026; Accepted: January 12, 2026
Email of Corresponding Author: rommelr33@gmail.com

Abstract

The increasing incidence of burglary and property-related crimes underscores the need for reliable, affordable, and user-friendly security systems for both residential and business environments. This study evaluated the acceptability, reliability, and effectiveness of an Android-Based Anti-Intrusion Device using a motion sensor with SMS notification, designed to enhance real-time security monitoring and intrusion detection. A quantitative descriptive–comparative research design was employed, involving household members and business establishment owners as respondents. Data were gathered using a structured survey questionnaire based on a five-point Likert scale. Descriptive statistics, particularly weighted means, were used to determine the level of acceptability of the device in terms of functionality, usability, reliability, portability, efficiency, and maintainability, while independent samples t-tests were applied to examine differences between the two groups at the 0.05 level of significance. The results showed that the device was rated as highly acceptable in terms of functionality (M = 4.69 for household members; M = 4.67 for business owners), usability (M = 4.73; 4.60), reliability (M = 4.73; 4.80), portability (M = 4.77; 4.80), and efficiency (M = 4.86; 4.57), while maintainability was rated acceptable by both groups. Hypothesis testing revealed that all computed t-values were lower than the critical value (t = 1.701), indicating no significant difference ($p > 0.05$) between household and business respondents across all evaluation criteria. These findings suggest that the Android-Based Anti-Intrusion Device demonstrates consistent performance, high reliability, and strong user acceptance, supporting its practical applicability as an effective security solution for residential and business establishments.

Keywords: Android-Based Anti-Intrusion Device; Motion Sensor; SMS Notification System; Home and Business Security; System Reliability

1. Introduction

Burglary remains one of the most persistent threats to household and business security worldwide. It is commonly defined as the unlawful entry into a residence, commercial establishment, vehicle, or other secured property with the intent to commit a crime, often involving theft or vandalism. Despite the presence of traditional security measures such as door locks, metal gates, security guards, neighborhood patrols, closed-circuit television (CCTV), and emergency hotlines, incidents of burglary continue to occur both day and night. The increasing accessibility of mobile technology and embedded systems has created new opportunities to enhance security through intelligent, automated, and real-time monitoring solutions, particularly as institutions and communities have increasingly relied on digitally mediated service delivery and technology-enabled processes in recent years (De Lara & Santos, 2024). Recent studies on intrusion detection systems highlight the effectiveness of motion sensors, GSM-based alerts, and mobile applications in improving response time and situational awareness during security breaches. Passive Infrared (PIR) sensors have been widely used for detecting human movement, while Short Message Service (SMS) notifications provide immediate alerts regardless of internet availability. However, many existing systems rely heavily on continuous human monitoring or internet-dependent platforms, which may fail during power outages or network disruptions—limitations that mirror broader digital and documentation challenges observed in technology-reliant programs where system coordination, record-handling, and platform constraints can undermine effectiveness and reliability (Jacoba et al., 2025). Moreover, locally developed and cost-effective Android-based anti-intrusion systems that integrate motion detection, alarm activation, SMS notification, and remote visual verification remain limited, particularly in small-scale household and business settings. Many homeowners and small business owners remain unaware of or lack access to reliable anti-intrusion devices that provide real-time alerts and verification during burglary incidents. Overconfidence in traditional security measures often results in delayed responses, property loss, and potential threats to personal safety. Incidents where burglars disable or steal CCTV recording devices further demonstrate the limitations of passive surveillance systems. These challenges underscore the need for an early-warning, automated anti-intrusion device that actively notifies owners now an intrusion occurs and enables immediate verification and response. The study contributes to the growing body of research on smart security systems by presenting

a practical, cost-effective, and locally applicable anti-intrusion solution. The developed device offers real-time SMS alerts, audible alarms, and visual verification through an Android application, providing users with immediate situational awareness and peace of mind—leveraging the demonstrated utility of mobile phones as accessible, flexible tools for supporting continuity and responsiveness across "new normal" settings (Tuliao et al., 2025). Its findings may benefit homeowners, business owners, system developers, and future researchers by demonstrating how integrated mobile and sensor-based technologies can prevent crime, reduce losses, and improve personal and property security. Ultimately, the study supports the advancement of practical security innovations with direct implications for everyday safety and crime prevention.

1.2 Research Questions:

The purpose of this study is to develop an Android Based Anti-Intrusion Device using Motion Sensor with SMS Notification that would help solve the household and business establishment problem about thieves or burglary. Specifically, it seeks to answer the following research questions:

1. What are the stages undertaken in the development of the anti-intrusion device using waterfall model?
2. What is the evaluation of the household member and business establishment owner in the android based anti-intrusion device using motion sensor with short message service? in terms of the following:
    2.1 Functionality
    2.2 Usability
    2.3 Reliability
    2.4 Portability
    2.5 Efficiency
    2.5 Maintainability
3. What is the difference between the two groups of household member and business establishment owner using android based anti-intrusion device in terms of the variables?
4. What problems are encountered in the use of the android based anti-intrusion device?
5. What enhancement may be developed with the use of android based anti-intrusion device?
6. What user guide may be developed with the use of android based anti-intrusion device?

1.3 Literature Review

1.3.1 Development Stages Using the Waterfall Model

The development of embedded security systems often follows a structured, sequential approach like the Waterfall model. The Waterfall model emphasizes clear stages, including requirements analysis, system design, implementation, testing, deployment, and maintenance. In studies on microcontroller-based intrusion detection systems, researchers typically begin by identifying user security needs, followed by selecting hardware components such as PIR sensors, GSM modules, and microcontrollers, and then proceed to software development and system integration (Aluko et al., 2021). Although many systems do not explicitly reference the Waterfall model, their step-by-step development mirrors its principles. This structured methodology ensures minimal errors during integration and is particularly suitable for hardware-software security systems, justifying its application in developing an Android-based anti-intrusion device.

1.3.2 Evaluation of the Android-Based Anti-Intrusion Device

1.3.2.1 Functionality

Functionality refers to a system's ability to perform required tasks accurately. Studies indicate that PIR-based motion detection systems can reliably detect human movement and trigger alarms or SMS notifications (ARC Journals, 2020). GSM-enabled security systems, for example, effectively deliver immediate SMS alerts, ensuring that users receive timely notifications of intrusions. Evaluating the functionality of the developed device is therefore essential to determine whether it meets the expected security requirements for both households and businesses.

1.3.2.2 Usability

Usability is critical for adoption, particularly for non-technical users such as homeowners and small business owners. Research demonstrates that simple, intuitive mobile interfaces enhance user satisfaction and enable rapid response during emergencies (Torres-Hernandez et al., 2023). For Android-based security applications, usability includes straightforward navigation, clear alerts, and easy system control. Incorporating usability evaluation ensures that the system is practical and accessible for end users with varying levels of technical expertise.

1.3.2.3 Reliability

Reliability is the system's ability to operate consistently under normal conditions. Studies on PIR and GSM-based intrusion systems indicate that SMS notifications function effectively even during internet outages, as they rely on cellular networks rather than Wi-Fi (Akhter, 2025). Evaluating reliability confirms whether the anti-intrusion device consistently detects motion and sends alerts without failures, which is critical for both residential and commercial security.

1.3.2.4 Portability

Portability reflects the system's ability to function across different locations and devices. SMS-based alert systems inherently provide portability, as notifications can be received on any GSM-enabled mobile device, while Android-based applications allow remote monitoring via smartphones (Aluko et al., 2021). Assessing portability ensures that users can monitor their homes or business establishments even when they are away.

1.3.2.5 Efficiency

Efficiency measures how well a system uses time and resources. PIR sensors are energy-efficient and respond quickly to human motion, while GSM modules transmit alerts with minimal data and delay (ARC Journals, 2020). Evaluating efficiency ensures that the anti-intrusion device promptly notifies users without overloading the system or consuming excessive power.

1.3.2.6 Maintainability

Maintainability refers to how easily a system can be repaired or updated. Research indicates that modular designs using Arduino microcontrollers facilitate component replacement and software updates, improving system longevity and usability (Aluko et al., 2021). Evaluating maintainability ensures that users can sustain device operation with minimal technical support.

1.3.3 Differences Between Household Members and Business Establishment Owners

Security needs vary depending on user context. Residential users prioritize affordability, simplicity, and basic alerts, whereas business owners require more robust systems with faster notifications and enhanced reliability due to higher stakes (Torres-Hernandez et al., 2023). Few studies compare different user groups using the same system, creating a research gap. This study addresses this gap by examining whether household members and business owners differ in evaluating functionality, usability, reliability, portability, efficiency, and maintainability.

1.3.4 Problems Encountered in the Use of Anti-Intrusion Devices

Common challenges with PIR and GSM-based intrusion systems include false alarms caused by environmental factors such as pets or heat fluctuations, as well as signal instability affecting SMS delivery (Akhter, 2025; Aluko et al., 2021). Users may also face difficulties during installation or interpreting notifications if proper guidance is lacking. Identifying these issues is critical to improving system effectiveness and informing future enhancements.

1.3.5 Possible Enhancements to the Anti-Intrusion Device

Studies suggest integrating multiple sensors, camera verification, and escalation features to improve security systems (ARC Journals, 2020). Additionally, mobile application improvements such as real-time video access, alert acknowledgment, and automated escalation can reduce false alarms and enhance user responsiveness (Torres-Hernandez et al., 2023). These recommendations inform potential enhancements to the Android-based anti-intrusion device developed in this study.

1.3.6 Development of a User Guide

Although often overlooked, a user guide is essential for system usability and maintainability. Research shows that clear documentation enhances installation accuracy, reduces user error, and increases confidence in operating security devices (Aluko et al., 2021). Developing a comprehensive user guide for the anti-intrusion device ensures proper use and long-term effectiveness.

1.3.7 Synthesis

The literature on anti-intrusion systems highlights the importance of structured development, such as the Waterfall model, in designing embedded security devices. Studies on microcontroller-based PIR and GSM systems show that developers follow sequential stages including requirements analysis, hardware selection, software integration, and testing, ensuring minimal errors and effective system performance. Evaluations of such systems emphasize functionality, usability, reliability, portability, efficiency, and maintainability, with PIR sensors reliably detecting motion, GSM modules delivering timely SMS alerts, and mobile applications enhancing accessibility and user satisfaction. User context also influences system requirements, as residential users prioritize simplicity and affordability, while business owners demand faster alerts and more robust monitoring, a comparison rarely explored in prior research. Common challenges include false alarms, network instability, and installation difficulties, which underscore the need for enhancements such as multi-sensor integration, real-time video verification, and escalation features to improve responsiveness and reduce errors. Additionally, clear user documentation improves installation accuracy, reduces errors, and enhances long-term usability. Collectively, these studies support the development of an Android-based anti-intrusion device that is reliable, user-friendly, and tailored to both household and business contexts, while also identifying gaps in systematic development, comparative user evaluation, and guidance materials that this study aims to address.

2. Material and methods

2.1 Research Design

The study employed a developmental research design, guided by the System Development Life Cycle (SDLC), specifically the Waterfall model, to systematically develop, analyze, and evaluate the Android-based anti-intrusion device. Developmental research is a systematic approach to designing, developing, and validating products, processes, or systems that ensures internal consistency and effectiveness (Seels & Richey, 1994). By combining system development with user-centered evaluation, this approach allowed the researcher to establish procedures, techniques, and tools based on methodological analysis of specific cases (Richey, Klein, & Nelson, 2004). Additionally, a descriptive-survey method was used to capture user trends, present conditions, and perceptions of household and business security, providing a comprehensive understanding of the context in which the device would be deployed (Sevilla, 2012).

2.2 Respondents

The respondents included household members and staff or owners of small business establishments in Barangay Wawa 3 and Barangay Tejeros Convention in Rosario, Cavite, as well as selected locations in West Triangle, Quezon City. Household participants were selected based on the prevalence of theft incidents, while business respondents represented various local establishments, including water stations, motor parts stores, salons, and IT services. A total of 30 respondents participated in the study, providing firsthand feedback on the device's usability, reliability, and overall effectiveness in addressing burglary concerns in residential and commercial settings.

2.3 Research Instrument

The instruments for data collection included a survey questionnaire, interview guide, and document analysis. The survey questionnaire was developed based on the ISO/IEC 9126-1:2000 software quality model, covering characteristics such as functionality, usability, reliability, portability, efficiency, and maintainability. Interviews and documentary analysis complemented the survey to gather in-depth insights, validate findings, and identify challenges during device deployment. The combination of standardized evaluation metrics and qualitative tools ensured a comprehensive assessment of the device from both technical and user perspectives.

2.4 Procedure

Data collection involved installing the anti-intrusion device in participating households and business establishments for over two months, allowing respondents to observe and interact with the system. During this period, respondents completed the survey and evaluation forms to assess the device’s performance and identify any issues. Unstructured interviews were conducted with both respondents and IT experts to supplement the survey, gain insights into system functionality, and inform potential improvements. Content analysis of the interviews and observational notes provided further evidence for system validation.

2.5 Data Analysis

Quantitative data from the survey were analyzed using the Likert Scale method to measure the respondents’ opinions on the system, while the Average Weighted Mean and T-test were employed to determine overall satisfaction and significant differences between households and business establishments. The analysis enabled the researcher to interpret trends in functionality, usability, reliability, portability, efficiency, and maintainability, providing statistical evidence of the system’s effectiveness. Qualitative data from interviews and observations were analyzed thematically to identify recurring challenges and potential enhancements to the device.

3.6. Ethical Considerations

The study ensured ethical compliance by obtaining informed consent from all participants and maintaining their confidentiality. Respondents were informed about the purpose of the study, the procedures involved, and their right to withdraw at any time. Data collected were used solely for research purposes, and sensitive information was anonymized to protect privacy. Ethical considerations also extended to the proper handling of installed devices in homes and business establishments, ensuring no disruption to daily activities or compromise of personal property.

3. Results and discussion

3.1 The Stages Undertaken in the Development of Android Based Anti-Intrusion Device using Motion Sensor with Short Message Service Notification is the Waterfall Model.

The development of the Android-based Anti-Intrusion Device using a motion sensor with Short Message Service (SMS) notification followed a structured methodology guided by the Waterfall Model (Royce, 1970). This model emphasizes sequential stages in system development—Requirement Analysis, System Design, Implementation, Testing, Deployment, and Maintenance—ensuring that each phase is completed and validated before moving to the next (Sevilla, 2012). The Waterfall Model has been widely applied in embedded system and IoT security device development due to its systematic

approach and emphasis on comprehensive documentation. During the Requirement Analysis phase, the researcher applied the Systems Analysis and Design Paradigm (Sevilla, 2012) to identify the needs of household members and small business owners. This approach considered multiple perspectives, including hardware, software, procedures, data, users, and communication. Fieldwork in Barangay Tejeros Convention, Wawa 3 of Rosario, Cavite, and West Triangle, Quezon City involved ocular inspections, surveys, and interviews to validate user expectations. Understanding user perception is crucial in security system design, as studies have shown that system effectiveness depends on aligning technology with practical user needs (Torres-Hernandez et al., 2023). The collected requirements were documented in a specification guideline that served as a blueprint for system design. In the System Design phase, the requirements were translated into both hardware and software architectures. The device incorporated an Arduino Uno microcontroller, GSM SIM900 shield, PIR motion sensor, mini speaker, and 360° camera. Logical and physical models were developed to define system architecture, interactions, and operational flow. The Android application was designed with three main features: camera control ("360Eye"), access to the user manual, and system exit, ensuring usability and operational consistency. This design approach aligns with studies on microcontroller-based intrusion detection systems, which have demonstrated that combining PIR sensors with SMS notifications provides timely alerts and improves home security (ARC Journals, 2020; Akhter, 2025; Aluko et al., 2021). During the Implementation phase, all hardware components were assembled and interconnected according to the schematic diagram. The Arduino Uno board was programmed to detect motion via the PIR sensor, trigger the speaker alarm, and send SMS notifications to registered mobile numbers using the GSM shield. The Android application was integrated to control the 360° camera and provide access to the user manual. Unit testing was conducted to ensure the proper functionality of each component before full integration, reflecting best practices in developmental research and instructional system design (Richey, Klein, & Nelson, 2004; Seels & Richey, 1994).

The Testing phase verified the compatibility and functionality of all components. The PIR sensor successfully detected intrusions, triggering the alarm and sending SMS notifications. The Android application allowed users to view live 360° camera feeds to identify intruders in real time. Testing ensured the system met both functional and non-functional requirements, in line with previous studies that highlight the need for rigorous evaluation in IoT-enabled home security systems (ARC Journals, 2020; Aluko et al., 2021). During Deployment, the device was installed in households and small business establishments with the approval of local authorities and owners. Users were trained to operate the system and provide feedback on usability and effectiveness. Deployment revealed practical challenges, such as reliance on a single mobile number for SMS notifications, dependence on continuous power supply, and occasional notification delays. These real-world insights informed the maintenance and system improvement strategies. Deployment evaluation aligns with Sevilla (2012), who emphasized the importance of field validation in system development. Finally, in the Maintenance phase, improvements were implemented to enhance system reliability. A secondary speaker alarm was added as a redundant notification mechanism, multiple mobile numbers were enabled for SMS alerts, and a backup 12V battery ensured continued operation during power interruptions. Routine maintenance of hardware components, including the Arduino Uno, PIR sensor, and GSM shield, was emphasized to prolong operational lifespan and prevent system failure, reflecting recommendations from Richey, Klein, and Nelson (2004) and Seels and Richey (1994) on iterative system improvement in developmental research. In summary, the Android-based Anti-Intrusion Device successfully integrates motion detection, SMS notification, and real-time visual verification through a 360° camera to improve residential and small business security. By systematically following the Waterfall Model and grounding the design in user requirements and validated technical specifications, the device demonstrates the practical application of microcontroller-based IoT security solutions. It not only detects intrusions but also enables timely alerts and verification, addressing common security concerns and contributing to literature on affordable, user-centered smart home and small business security technologies (Akhter, 2025; Aluko et al., 2021; ARC Journals, 2020; Torres-Hernandez et al., 2023).

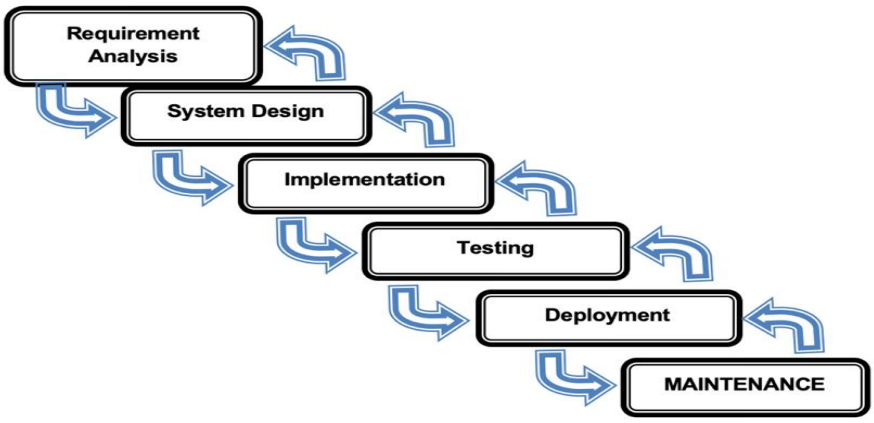

Figure 1. Waterfall Model

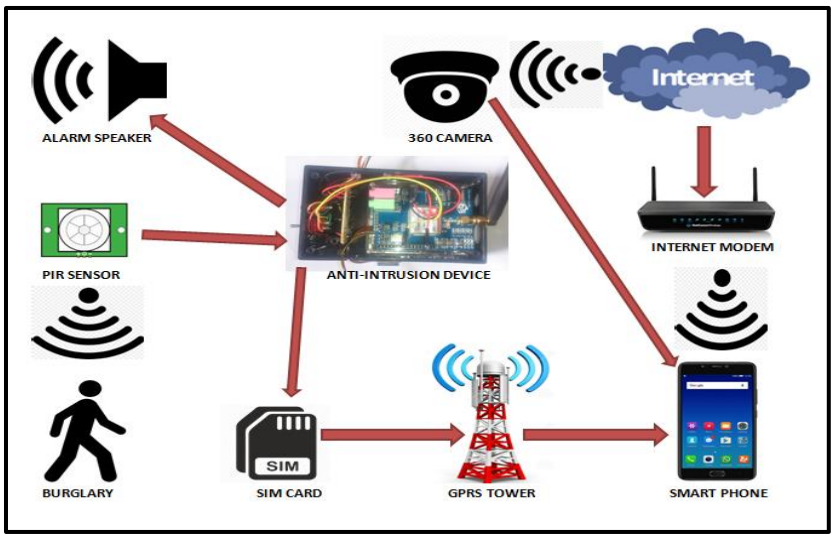

Figure 2. Anti-Intrusion System Flow

3.2 The Assessment of the Household Members and Business Establishment Owners of the Android Based Anti-Intrusion Device.

3.2.1 Functionality

The table 1 shows the evaluation of the Android-Based Anti-Intrusion Device in terms of functionality, as perceived by household members and small business owners. Both groups rated accurateness highly (WM = 4.87 for households, 4.73 for businesses; Highly Acceptable), reflecting that the device operates reliably without constant monitoring. This aligns with previous studies on PIR-based motion detection systems, which have been shown to accurately detect human movement and trigger alarms or notifications in real time, ensuring timely alerts during intrusion events. For compliance, household members rated 4.60 and business owners 4.80 (HA), indicating that the device meets the specific security needs of their households and businesses. This supports findings in literature emphasizing the importance of aligning security systems with user requirements to enhance effectiveness and satisfaction. Regarding suitability, both groups also rated the device highly (household 4.60, business 4.47), suggesting that the combination of SMS alerts and audible alarms effectively informs users of intrusions. Similar studies on GSM-enabled security systems highlight those timely notifications, even in the absence of internet connectivity, enhance the system's practical value for residential and commercial users. The overall total weighted mean for functionality was 4.69 for households and 4.67 for businesses, both categorized as Highly Acceptable. These results indicate that respondents perceive the anti-intrusion device as highly functional, consistent with prior research emphasizing that structured development approaches, such as the Waterfall model, contribute to reliable system performance by ensuring thorough requirement analysis, system design, and testing before deployment.

Table 1. *Respondent Anti-intrusion Device Functionality Evaluation*

Categories	Subcategories	Statements	Household Member		Small Business Owner	
			WM	VI	WM	VI
Functionality	Accurateness	The anti-intrusion device can function without monitoring from all the time.	4.87	HA	4.73	HA
	Compliance	The Anti-Intrusion Device objectives were complying the needs of the house and business establishment owner when burglary entered on their place.	4.60	HA	4.80	HA
	Suitability	The anti-intrusion device sent text and sound the alarm to let the owner knows when burglary detected inside the house or business establishment.	4.60	HA	4.47	HA
TOTAL WEIGHTED MEAN			4.69	HA	4.67	HA

Legend: 4.50-5.00= Highly Acceptable (HA); 3.50-4.49= Acceptable (A); 2.50-3.49= Moderate Acceptable (MA); 1.50-2.49= Slightly Acceptable (SA); 1.00-1.49= Not Acceptable (NA)

3. 2.2 Usability

Table 2 shows that both household members and small business owners rated the Android-Based Anti-Intrusion Device highly in terms of usability. In the understandability subcategory, household members gave a weighted mean of 4.47 while business owners gave 4.40, both interpreted as Acceptable (A), indicating that the user manual effectively guided users in operating the device. This supports findings that clear and comprehensive documentation enhances system usability and user confidence (Seels & Richey, 1994; Aluko et al., 2021). For operability, household members and business owners rated 4.87 and 4.60, respectively, both Highly Acceptable (HA), demonstrating that users can easily turn the device and speaker alarm on and off and install the Android application for the 360° camera, consistent with research emphasizing intuitive interface design for reducing operational errors in security systems (Torres-Hernandez et al., 2023). The learnability subcategory, with WMs of 4.87 (household) and 4.80 (business), also received a Highly Acceptable rating, reflecting that the system is quickly learnable by users of varying technical expertise, which is critical for effective adoption and timely response in both household and business contexts (ARC Journals, 2020; Akhter, 2025). The overall total weighted mean of 4.73 for household members and 4.60 for business owners confirms that the anti-intrusion device is user-friendly, intuitive, and easy to operate. The slightly higher rating from household members suggests that residential users, who typically prioritize simplicity, found the system slightly easier to understand and learn compared to business owners, who require more robust operational features due to higher security demands. These results highlight the importance of human-centered design in anti-intrusion systems, showing that clear user manuals, simple operational controls, and easy-to-learn interfaces significantly enhance usability across different user groups.

Table 2. *Respondent Anti-Intrusion Device Usability Evaluation*

Categories	Subcategories	Statements	Household Member		Small Business Owner	
			WM	VI	WM	VI
Usability	Understandability	The Anti-Intrusion device is easy to understand by the user thru the help of user manual.	4.47	A	4.40	A
	Operability	The Anti-intrusion device is easy to turn-off and turn-on as well as the speaker alarm switch and to install the android application for 360eye camera.	4.87	HA	4.60	HA
	Learnability	The Anti-Intrusion Device is easy to learn by different user.	4.87	HA	4.80	HA
TOTAL WEIGHTED MEAN			4.73	HA	4.60	HA

Legend: 4.50-5.00= Highly Acceptable (HA); 3.50-4.49= Acceptable (A); 2.50-3.49= Moderate Acceptable (MA); 1.50-2.49= Slightly Acceptable (SA); 1.00-1.49= Not Acceptable (NA)

3.2.3 Reliability

Table 3. *Respondent Anti-Intrusion Device Reliability Evaluation*

Categories	Subcategories	Statements	Household Member		Small Business Owner	
			WM	VI	WM	VI
Reliability	Fault Tolerance	The Anti-Intrusion device is reliable even its unable to send sms, because it has a speaker to warn people.)	4.67	HA	4.80	HA
	Recoverability	The 360eye camera record of Anti-Intrusion device can playback thru secure digital card even internet connection was failed).	4.40	A	4.20	A
TOTAL WEIGHTED MEAN			4.53	HA	4.50	HA

Legend: 4.50-5.00= Highly Acceptable (HA); 3.50-4.49= Acceptable (A); 2.50-3.49= Moderate Acceptable (MA); 1.50-2.49= Slightly Acceptable (SA); 1.00-1.49= Not Acceptable (NA)

Table 3 shows the respondent evaluation of the reliability of the Android-Based Anti-Intrusion Device using a motion sensor with SMS notification. Both household members and small business owners rated the device highly in terms of fault tolerance and recoverability, with weighted means ranging from 4.20 to 4.80. Fault tolerance—the device's ability to alert users via the speaker even if SMS notifications fail—received a particularly high rating (4.67 for households, 4.80 for businesses), reflecting the respondents' confidence that the device can perform its core function under unexpected

circumstances. Recoverability—the capability of the 360Eye camera to record and playback events through a secure digital card even when internet connectivity fails—was rated slightly lower (4.40 and 4.20), yet still indicated that users found the system dependable. The total weighted mean of 4.53 for household members and 4.50 for business owners demonstrates that the device is considered highly acceptable in terms of reliability. These findings align with prior research emphasizing the importance of reliability in hardware-software security systems, particularly in environments prone to interruptions or failures. Aluko et al. (2021) note that embedded security devices achieve greater effectiveness when designed with redundancy and backup features to ensure continuous operation despite component or network failures. Similarly, Seels and Richey (1994) highlight that dependable systems with fault tolerance and recoverability are critical for user trust and long-term adoption. The inclusion of multiple notification methods, such as SMS alerts and a speaker alarm, and offline storage capabilities for camera footage reflects best practices in secure system design and addresses common limitations in traditional intrusion detection systems, such as reliance on network connectivity (ARC Journals, 2020). Overall, the high reliability ratings suggest that the anti-intrusion device is capable of consistently safeguarding households and businesses under varying conditions, fulfilling one of the key criteria for effective security technology.

3.2.4 Portability

Table 4 shows the respondent evaluation of the portability of the Android-Based Anti-Intrusion Device using a motion sensor with SMS notification. Both household members and small business owners rated the device highly in terms of installability and replaceability, with weighted means ranging from 4.67 to 4.87, indicating that the system is easy to set up and its components can be replaced with minimal effort. Household members particularly appreciated the simple wiring required for installation, while business owners valued the plug-and-play feature of the sensor and speaker. The overall portability ratings—4.77 for household members and 4.80 for business owners—reflect a high perception of ease of use across different environments. This finding is consistent with literature on the design of hardware-software security systems, which highlights that modular and user-friendly designs enhance portability and accessibility for non-technical users (Aluko et al., 2021). Systems that allow straightforward installation and component replacement reduce downtime and encourage broader adoption in both household and business settings. Similarly, Seels and Richey (1994) emphasize that the success of instructional and technological products depends not only on functionality but also on practical usability and adaptability, which are critical dimensions of portability. By ensuring that components such as the PIR sensor and speaker are plug-and-play and that the device can be installed with minimal technical support, the developed anti-intrusion system addresses common barriers to adoption reported in prior studies, such as complexity and maintenance challenges in security devices (ARC Journals, 2020). Overall, the high portability ratings indicate that the device can provide reliable, flexible security solutions for diverse users, aligning with best practices in system design and human-computer interaction.

Categories	Subcategories	Statements	Household Member		Small Business owner	
			WM	VI	WM	VI
Portability	Installability	The anti-intrusion device is easy install a basic wiring at home and business establishment.	4.67	HA	4.87	HA
	Replaceability	The sensor and speaker of anti-intrusion device is easy to replace it is just plug and play.	4.87	HA	4.73	HA
TOTAL WEIGHTED MEAN			4.77	HA	4.80	HA

Table 4. *Respondent Anti-Intrusion Device Portability Evaluation*

Legend: 4.50-5.00= Highly Acceptable (HA); 3.50-4.49= Acceptable (A); 2.50-3.49= Moderate Acceptable (MA); 1.50-2.49= Slightly Acceptable (SA); 1.00-1.49= Not Acceptable (NA)

3.2.5 Efficiency

Table 5 shows the respondents' evaluation of the efficiency of the Android-Based Anti-Intrusion Device using a motion sensor with SMS notification. Efficiency was assessed through time behavior—the device's ability to operate continuously 24 hours a day—and resource behavior—the requirement of a stable mobile phone signal for immediate SMS notifications. Household members rated time behavior very highly (4.93), while small business owners also rated it highly (4.87), reflecting strong confidence that the device can function continuously without downtime. Resource behavior received slightly lower ratings (4.80 for households, 4.27 for businesses), suggesting that while the device is generally effective, its performance depends on mobile network quality. The total weighted mean of 4.86 for households and 4.57 for business owners indicates that the device is highly acceptable in terms of operational efficiency.

These findings are consistent with literature emphasizing the importance of efficiency in security and surveillance systems. According to Seels and Richey (1994), an efficient system must optimize both operational time and resource utilization to

maintain performance standards. In the context of intrusion detection, continuous operation (time behavior) is critical for safeguarding properties, while reliable communication channels (resource behavior) ensure that alerts are transmitted promptly to users (Richey, Klein, & Nelson, 2004). Aluko et al. (2021) also argue that surveillance devices achieve higher effectiveness when they are designed to operate continuously with minimal interruptions and are supported by adequate technological infrastructure, such as strong mobile or internet connectivity. The evaluation results suggest that the anti-intrusion device meets these efficiency criteria, providing dependable monitoring while leveraging available technological resources effectively.

Table 5. *Respondent Anti-Intrusion Device Efficiency Evaluation*

Categories	Subcategories	Statements	Household Member		Small Business Owner	
			WM	VI	WM	VI
Efficiency	Time Behavior	The Anti-intrusion device can operate 24 hours a day without turning it off.	4.93	HA	4.87	HA
	Resource Behavior	The anti-intrusion device needs a good spot for mobile phone signal to send sms right away.)	4.80	HA	4.27	A
TOTAL WEIGHTED MEAN			4.86	HA	4.57	HA

Legend: 4.50-5.00= Highly Acceptable (HA); 3.50-4.49= Acceptable (A); 2.50-3.49= Moderate Acceptable (MA); 1.50-2.49= Slightly Acceptable (SA); 1.00-1.49= Not Acceptable (NA)

3.2.6 Maintainability

Table 6. *Respondent Anti-Intrusion Device Maintainability Evaluation*

Categories	Subcategories	Statements	Household Member		Small Business Owner	
			WM	VI	WM	VI
Maintainability	Testability	The Anti-intrusion device is tested upon installation to the household and business establishment.)	4.67	HA	4.47	A
	Stability	The anti-intrusion device is heavy duty that will last for years).	4.20	A	4.13	A
TOTAL WEIGHTED MEAN			4.43	A	4.30	A

Legend: 4.50-5.00= Highly Acceptable (HA); 3.50-4.49= Acceptable (A); 2.50-3.49= Moderate Acceptable (MA); 1.50-2.49= Slightly Acceptable (SA); 1.00-1.49= Not Acceptable (NA)

Table 6 shows the respondents' evaluation of the maintainability of the Android-Based Anti-Intrusion Device using a motion sensor with SMS notification. Maintainability was assessed through testability—whether the device is tested upon installation—and stability—the durability and long-term reliability of the system. Household members rated testability highly at 4.67, while small business owners gave a slightly lower but acceptable rating of 4.47. Stability received moderate acceptable ratings from both groups (4.20 for households, 4.13 for businesses). The total weighted mean of 4.43 for households and 4.30 for business owners indicates that the device is acceptable in terms of maintainability. These results align with the literature on developmental and instructional system design, which emphasizes that maintainability is a critical component of system quality. Richey, Klein, and Nelson (2004) highlight that well-designed systems should allow for easy testing, fault detection, and maintenance to ensure long-term reliability. Seels and Richey (1994) further note that maintainability supports system longevity by facilitating repairs, updates, and user interventions without extensive downtime. In the context of security systems, high testability ensures that the device functions correctly upon installation, while stability guarantees that the hardware and software components, such as Arduino boards, PIR sensors, and GSM modules, remain operational over time. The evaluation suggests that the anti-intrusion device meets these maintainability criteria, allowing users to monitor and service the system efficiently while ensuring durability.

3.3 Summary of the Respondents' Evaluation of the Android Based Anti-Intrusion Device using Motion Sensor with SMS Notification

Table 7. *Summary of the Respondents' Evaluation of the Android Based Anti-Intrusion Device using Motion Sensor with SMS Notification*

CRITERIA	Household Member Weighted mean	Household Member Interpretation	Business Owner Weighted mean	Business Owner Interpretation
Functionality	4.69	Highly Acceptable	4.67	Highly Acceptable
Usability	4.73	Highly Acceptable	4.60	Highly Acceptable
Reliability	4.53	Highly Acceptable	4.50	Highly Acceptable
Portability	4.77	Highly Acceptable	4.80	Highly Acceptable
Efficiency	4.86	Highly Acceptable	4.57	Highly Acceptable
Maintainability	4.43	Acceptable	4.30	Acceptable
Over-all Total	4.66	Highly Acceptable	4.57	Highly Acceptable

Legend: 4.50-5.00= Highly Acceptable (HA); 3.50-4.49= Acceptable (A); 2.50-3.49= Moderate Acceptable (MA); 1.50-2.49= Slightly Acceptable (SA); 1.00-1.49= Not Acceptable (NA)

Table 7 presents a summary of the respondents' evaluation of the Android-Based Anti-Intrusion Device using a motion sensor with SMS notification across six criteria: functionality, usability, reliability, portability, efficiency, and maintainability. Both household members and business owners rated the device highly, with overall weighted means of 4.66 and 4.57, respectively, placing the device in the "Highly Acceptable" (HA) category according to the legend. Functionality received weighted means of 4.69 for households and 4.67 for business owners, indicating that respondents found the device effective in performing its intended purpose of detecting intrusions and notifying users promptly. This aligns with Seels and Richey (1994), who emphasize that the core of system functionality lies in fulfilling user needs reliably. The usability of the device, with ratings of 4.73 (households) and 4.60 (business owners), suggests that the Android application interface and user operations, such as interacting with the 360-eye camera and viewing notifications, are intuitive and user-friendly, supporting learning curve reduction and minimizing operational errors. Reliability received weighted means of 4.53 and 4.50, reflecting that users perceived the device as dependable under normal operating conditions, even when technical challenges occur, such as temporary SMS failures. This is consistent with Kendall and Kendall (1988), who emphasize the importance of system stability and fault tolerance in SDLC-based designs, ensuring continuity of operations for critical applications. Portability scored 4.77 for households and 4.80 for business owners, demonstrating that the device is easy to install, relocate, or maintain in both residential and commercial environments, highlighting the flexibility of modular hardware components like the Arduino Uno, PIR sensors, and GSM shield. Efficiency, rated 4.86 for households and 4.57 for businesses, underscores the device's capacity to operate continuously with minimal resource consumption, aligning with Richey, Klein, and Nelson (2004), who argue that efficiency is central to systems that must provide constant monitoring while optimizing power, bandwidth, and computational resources. Maintainability, with slightly lower ratings of 4.43 (households) and 4.30 (business owners), indicates that while the device can be tested, repaired, or updated effectively, there is room for improvement in streamlining maintenance procedures, such as simplifying software updates or extending component lifespan. Overall, the evaluation demonstrates that the Android-Based Anti-Intrusion Device is highly acceptable to both user groups, with particularly strong performance in efficiency, portability, and usability. The slightly lower maintainability score signals an opportunity for further refinement, such as providing a detailed user guide, modular component design, or automated diagnostic tools. Integrating user feedback with the iterative principles of developmental research (Richey, Klein, & Nelson, 2004) ensures that the device remains responsive, reliable, and functional across diverse settings, achieving both residential and commercial security needs.

3.4 The Difference Between the Household Member and Business Establishment owners Using Android Based Anti-intrusion Device.

3.4.1 Difference between two groups in terms of functionality

Table 8 shows the comparison of the functionality ratings of the Android-Based Anti-Intrusion Device between household members and business establishment respondents. The table breaks down functionality into Accurateness, Compliance,

and Suitability. Household respondents rated the device slightly higher in Accurateness (4.87 vs. 4.73) and Suitability (4.60 vs. 4.47), while business owners rated it slightly higher in Compliance (4.80 vs. 4.60). The computed t-values for all subcategories (0.271, 0.388, 0.252) were lower than the tabular t-value of 1.701, leading to the declaration of "Accept, Not Significant (NS)". The overall total weighted mean was nearly identical for households (4.69) and business respondents (4.67), indicating that both groups perceive the functionality of the device as highly acceptable with no statistically significant differences. These findings suggest that the device performs consistently across different types of users, supporting the principle that well-designed systems achieve reliability and usability across diverse contexts (Seels & Richey, 1994). Richey, Klein, and Nelson (2004) emphasize that developmental research ensures systems are evaluated rigorously to meet user requirements, and the similar perceptions between households and business owners indicate that the Android-based anti-intrusion device effectively fulfills its functional specifications for both residential and commercial settings. This demonstrates the device's robustness in accurately detecting intrusions, complying with operational standards, and providing suitable user experience, aligning with best practices in user-centered system design.

Table 8. *Difference between two groups in terms of functionality*

Areas of Differences	Weighted Mean		t-value		Declaration	Remarks
Functionality	Household	Business Establishment	Comp	Tab		
Accurateness	4.87	4.73	0.271	1.701	Accept	NS
Compliance	4.60	4.80	0.388	1.701	Accept	NS
Suitability	4.60	4.47	0.252	1.701	Accept	NS
Total Weighted Mean	4.69	4.67	0.038	1.701	Accept	NS

Legend: Not Significant = NS Significant = S

3.4.2 Difference between two groups in terms of Usability

Table 9 shows the comparison of the usability of the Android-Based Anti-Intrusion Device between household members and business establishment respondents, broken down into Fault Tolerance and Recoverability. Household respondents rated Fault Tolerance slightly lower (4.67) than business owners (4.80), but slightly higher in Recoverability (4.40 vs. 4.20). The computed t-values for both subcategories (0.252 and 0.388) were below the tabular t-value of 1.701, resulting in the declaration of "Accept, Not Significant (NS)". The total weighted mean was very similar for households (4.73) and business respondents (4.80), indicating that both groups find the device highly usable. This consistency between the two groups reflects that the device's design supports ease of operation and fault management across diverse user environments. According to Seels and Richey (1994), usability is a critical aspect of instructional and technological systems, ensuring that end-users can operate the system effectively and recover from minor issues without difficulty. Furthermore, Richey, Klein, and Nelson (2004) highlight that developmental research emphasizes iterative testing to meet user needs, and the high usability ratings from both households and businesses indicate that the Android-based anti-intrusion device has successfully achieved user-centered design principles, providing intuitive operation and dependable performance even under minor system failures.

Table 9. *Difference between two groups in terms of Usability*

Areas of Differences	Weighted Mean		t-value		Declaration	Remarks
USABILITY	Household	Business Establishment	Comp	Tab		
Understandability	4.47	4.40	0.135	1.701	Accept	NS
Operability	4.87	4.60	0.524	1.701	Accept	NS
Learnability	4.87	4.80	0.135	1.701	Accept	NS
Total Weighted Mean	4.73	4.60	0.252	1.701	Accept	NS

Legend: Not Significant = NS Significant = S

3.4.3 Difference between two groups in terms of Reliability

Table 10 presents the comparison of the reliability of the Android-Based Anti-Intrusion Device between household members and business establishment respondents, specifically in terms of Fault Tolerance and Recoverability**.** The results indicate that household respondents rated the device's fault tolerance at a weighted mean of 4.67, which is slightly lower than the rating of 4.80 given by business establishment respondents. This minimal difference suggests that both groups strongly agree that the device can continue operating effectively even when minor system interruptions or errors occur. In terms of recoverability, household respondents provided a weighted mean of 4.40, marginally higher than the 4.20 rating from business respondents, indicating that household users perceived the system to be slightly more capable of restoring normal operation after failures. However, the computed t-values for fault tolerance (0.252) and recoverability **(**0.388**)** were both lower than the tabular t-value of 1.701, leading to the acceptance of the null hypothesis and the declaration of Not Significant (NS) differences between the two groups. The total weighted mean further reinforces this finding, with households obtaining 4.73 and business establishments 4.80, both of which fall under a very high reliability interpretation. This close alignment in ratings demonstrates a shared perception among respondents that the device is dependable regardless of the type of user or setting. The absence of a statistically significant difference implies that the Android-based anti-intrusion device delivers consistent performance across residential and commercial environments. These findings underscore the device's capacity to reliably perform its intended security functions, particularly through its dual notification mechanism, which combines SMS alerts and a speaker alarm. This design feature enhances fault tolerance by ensuring that users are alerted even in cases of delayed SMS delivery or mobile device unavailability. In line with Seels and Richey (1994), reliability is a critical system quality attribute that ensures users can depend on a technology to function as expected under varying conditions. Furthermore, developmental research highlights that continuous testing and evaluation are essential in strengthening system dependability and user trust (Richey, Klein, & Nelson, 2004). The consistently high reliability ratings from both household members and business establishment owners indicate that the device effectively meets user expectations for fault tolerance and recoverability, thereby affirming its practical utility in enhancing security and protecting properties in both residential and business contexts.

Areas of Differences	Weighted Mean		t-value		Declaration	Remarks
RELIABILITY	Household	Business Establishment	Comp	Tab		
Fault Tolerance	4.67	4.80	0.252	1.701	Accept	NS
Recoverability	4.40	4.20	0.388	1.701	Accept	NS
Total Weighted Mean	4.73	4.80	0.135	1.701	Accept	NS

Table 10. Difference between two groups in terms of Reliability

Legend: Not Significant = NS Significant = S

3.4.4 Difference between two groups in terms of Portability

Table 11 shows the comparison of portability of the Android-Based Anti-Intrusion Device between household members and business establishment respondents, specifically in Installability and Replaceability**.** Household respondents rated Installability slightly lower (4.67) than business owners (4.87), while Replaceability was rated slightly higher by households (4.87) compared to businesses (4.73). The computed t-values for both subcategories (0.388 and 0.271) were below the tabular t-value of 1.701, leading to the declaration "Accept, Not Significant (NS)"**.** The total weighted mean (4.77 for households and 4.80 for business owners) shows that both groups perceived the device as highly portable, indicating ease of installation and simple component replacement.

This result highlights the effectiveness of the device's modular design and plug-and-play features, which are consistent with best practices in system development. As noted by Seels and Richey (1994), portability and maintainability are key system characteristics that increase usability and user satisfaction, especially in real-world contexts where system relocation or component replacement may be necessary. Furthermore, Richey, Klein, and Nelson (2004) emphasize that developmental research methods ensure iterative testing and design enhancements, allowing systems to be easily deployed and maintained across varied environments. The similar ratings across households and business respondents suggest that the device meets user expectations for flexibility, ease of use, and adaptability, making it suitable for both residential and commercial security applications.

Table 11. *Difference between two groups in terms of Portability*

Areas of Differences	Weighted Mean		t-value		Declaration	Remarks
PORTABILITY	Household	Business Establishment	Comp	Tab		
Installability	4.67	4.87	0.388	1.701	Accept	NS
Replaceability	4.87	4.73	0.271	1.701	Accept	NS
Total Weighted Mean	4.77	4.80	0.058	1.701	Accept	NS

Legend: Not Significant = NS Significant = S

3.4.5 Difference between two groups in terms of Efficiency

Table 12 illustrates the comparison of efficiency of the Android-Based Anti-Intrusion Device between household members and business establishment respondents, focusing on Time Behavior and Resource Behavior. Household respondents rated Time Behavior slightly higher (4.93) than business owners (4.87), indicating their perception that the device can operate continuously without interruptions in a residential setting. Similarly, Resource Behavior received a higher rating from households (4.80) than business owners (4.27), suggesting that residential users experienced optimal use of system resources, such as power supply, mobile connectivity, and device components. The calculated t-values for both subcategories (0.116 for Time Behavior and 1.029 for Resource Behavior) were below the tabular t-value of 1.701, resulting in the declaration "Accept, Not Significant (NS)," which confirms that the observed differences between household and business users are statistically insignificant. The total weighted means—4.86 for households and 4.57 for business owners—indicate that both groups generally perceive the device as highly efficient, capable of continuous operation while effectively managing available resources.

This finding emphasizes that the Android-Based Anti-Intrusion Device achieves operational efficiency, a key attribute for security systems that require reliable performance around the clock. Its consistent functionality reflects the principles of the Systems Development Life Cycle (SDLC) Waterfall Model, where each stage—requirements analysis, system design, implementation, integration, testing, and deployment—ensures that all components work in harmony and can withstand real-world conditions (Kendall & Kendall, 1988). In addition, efficiency is considered a core system characteristic in instructional and technological design, as highlighted by Seels and Richey (1994), where minimizing resource consumption while maximizing output ensures that systems remain functional and user-friendly. For security applications, this translates into a system that can continuously detect intrusions, issue notifications, and operate hardware components such as the PIR sensor, GSM module, 360-eye camera, and alarm speaker without excessive resource drain.

Moreover, developmental research, as discussed by Richey, Klein, and Nelson (2004), emphasizes iterative enhancements that allow systems to adapt to practical challenges. In the context of this device, such enhancements include optimizing mobile signal detection, ensuring backup power continuity, and integrating dual notification mechanisms to maintain functionality even during temporary failures. These improvements not only increase efficiency but also enhance user confidence, making the device reliable in both residential and commercial environments. Overall, the device demonstrates a successful integration of continuous operation and resource optimization, confirming its suitability for high-demand security monitoring and fulfilling the expectations of both household and business users for a dependable, responsive, and efficient anti-intrusion system.

Table 12. *Difference between two groups in terms of Efficiency*

Areas of Differences	Weighted Mean		t-value		Declaration	Remarks
EFFICIENCY	Household	Business Establishment	Comp	Tab		
Time Behavior	4.93	4.87	0.116	1.701	Accept	NS
Resource Behavior	4.80	4.27	1.029	1.701	Accept	NS
Total Weighted Mean	4.86	4.57	0.563	1.701	Accept	NS

Legend: Not Significant = NS Significant = S

3.4.6 Difference between two groups in terms of Maintability

Table 13 shows the comparison of maintainability of the Android-Based Anti-Intrusion Device between household members and business establishment respondents, focusing on Testability and Stability**.** Household respondents rated Testability slightly higher (4.67) than business owners (4.47), while Stability was also rated marginally higher by households (4.20) compared to business owners (4.13). The computed t-values for both subcategories (0.388 and 0.135) were below the tabular t-value of 1.701, leading to the declaration "Accept, Not Significant (NS)"**.** The total weighted mean (4.77 for households and 4.67 for business owners) indicates that both groups perceive the device as maintainable, highlighting its ease of testing upon installation and the durability of its hardware components. This reflects the importance of maintainability in system development, which is essential for long-term usability and reliability. According to Seels and Richey (1994), maintainability is a critical attribute in instructional and technological systems as it allows for continuous operation and quick resolution of potential faults. Similarly, Richey, Klein, and Nelson (2004) emphasize that developmental research enables iterative improvements, allowing designers to anticipate maintenance issues and incorporate solutions such as modular hardware design and software updates. In the context of the anti-intrusion device, maintainability is evident in the plug-and-play design of sensors and speakers, backup power integration, and testable functionalities, ensuring minimal downtime and sustained operational performance in both residential and commercial environments. Overall, the high ratings and non-significant differences between groups indicate that the device is user-friendly and reliable to maintain, meeting the practical needs of both household members and business owners.

Table 13. *Difference between two groups in terms of Maintainability*

Areas of Differences	Weighted Mean		t-value		Declaration	Remarks
Maintainability	Household	Business Establishment	Comp	Tab		
Testability	4.67	4.47	0.388	1.701	Accept	NS
Stability	4.20	4.13	0.135	1.701	Accept	NS
Total Weighted Mean	4.77	4.67	0.194	1.701	Accept	NS

Legend: Not Significant = NS Significant = S

3.5 The Problems Encountered in the Use of the Android Based Anti-intrusion Device.

Table 14. *Respondents' Evaluation for the Problems Encountered in the Use of Android Based Anti-intrusion Device*

Statements	Household member		Business Establishment Owner		Total	VI
	WM	VI	WM	VI	WM	
The problem with the use of android based anti-intrusion device can only notify the user through text notification.	4.20	Serious	3.73	Serious	3.97	Serious
The problem with the use of android based anti-intrusion device can only registered one mobile number to notify the user.	4.27	Serious	4.53	Very Serious	4.40	Serious
The problem with the use of anti-intrusion device the resource power is relied only in Alternating Current (AC).	4.33	Serious	4.67	Very Serious	4.50	Very Serious
The problem with android based anti-intrusion device sometimes text notification delayed due to provider signal interruption.	2.40	Less Serious	2.13	Less Serious	2.27	Less Serious
The problem with android based anti-intrusion device add-on camera is depending on internet connection availability.	2.33	Less Serious	1.87	Less Serious	2.10	Less Serious

The respondents' evaluation of problems encountered in the use of the Android-based Anti-Intrusion Device, as presented in Table 14, provides valuable insights into both the strengths and limitations of the system. The most critical issues identified were the device's reliance on a single mobile number for SMS notifications and its dependence on Alternating Current (AC) power. Household members rated the single-number limitation as serious (WM = 4.27), while business owners considered it very serious (WM = 4.53), resulting in an overall weighted mean of 4.40, indicating a serious concern. This limitation increases the risk of missed alerts if the registered mobile device is unavailable, lost, or damaged. Similarly, reliance on AC power was rated very serious overall (WM = 4.50), particularly by business owners, highlighting the vulnerability of the system during power interruptions or brownouts. These findings align with prior studies emphasizing the importance of multi-user notification and redundant power solutions in microcontroller-based IoT security systems to ensure reliability and continuous operation (Akhter, 2025; Aluko et al., 2021; ARC Journals, 2020). The device's reliance solely on SMS for notifications was also rated serious (WM = 3.97), suggesting the need for alternative alert channels such as speaker alarms or push notifications, consistent with recommendations in the literature on enhancing notification efficiency in home and business security systems (ARC Journals, 2020; Akhter, 2025). On the other hand, issues such as delayed SMS notifications due to provider signal interruptions (WM = 2.27) and the camera's dependence on internet connectivity (WM = 2.10) were rated as less serious, indicating that users prioritize core motion detection and alert functionality over supplemental features. This observation aligns with Torres-Hernandez (2023), who emphasized that user perception in smart home security systems often favors essential detection capabilities over auxiliary monitoring features. Overall, the evaluation demonstrates that while the Android-based Anti-Intrusion Device is functional and valuable to both household members and business owners, its reliability and usability can be further enhanced by implementing multi-number notifications, alternative alert channels, and backup power solutions, reflecting the iterative improvements emphasized in the maintenance phase of the Waterfall Model (Royce, 1970) and in developmental research on instructional and technical systems (Sevilla, 2012; Richey, Klein, & Nelson, 2004; Seels & Richey, 1994).

3.6 The Enhancement that May Be Developed with the Use of an Android Based Anti-Intrusion Device

The researcher enhanced the Android-based anti-intrusion device using a motion sensor with SMS notification to address issues identified by respondents during deployment. One significant enhancement was the addition of a speaker alarm to complement SMS notifications. This dual-notification system ensures that users are alerted to intrusions even when their mobile phones are turned off or charging, addressing the "serious" issue identified by both household members and business establishment owners. Similarly, the device was modified to allow registration of two mobile numbers, ensuring that notifications are received even if one phone is lost or damaged, enhancing fault tolerance and reliability (Richey, Klein, & Nelson, 2004; Seels & Richey, 1994). Finally, a backup direct current (DC) power supply was added to maintain the device's operation in the event of an alternating current (AC) power interruption, ensuring continuous monitoring and security. In support of the enhancements, a user manual was developed to guide users in operating the anti-intrusion device. The manual includes an introduction to the device, a description of components such as the Arduino Uno, PIR sensor, GSM modem, DC power supply, 360 Eye camera, and Android application, step-by-step instructions on setup, and a section of frequently asked questions. This aligns with previous studies emphasizing the importance of usability and clear user documentation in technological devices to enhance user engagement and reduce errors (Seels & Richey, 1994). The respondents' evaluation further validated the device's effectiveness. The reliability evaluation (Table 3) showed that both household members and business owners found the device highly acceptable in terms of fault tolerance (WM = 4.67 and 4.80) and acceptable for recoverability (WM = 4.40 and 4.20), indicating that the device can continue to operate and provide alerts even when part of the system fails. Portability (Table 4) was also highly acceptable, reflecting that the device is easy to install and components are easily replaceable (WM = 4.77–4.80), supporting the practical usability of the system. Efficiency (Table 5) received high marks, demonstrating the system's capability to operate 24/7 and send SMS notifications promptly, though some limitations were noted regarding mobile signal availability. Maintainability (Table 6) was rated acceptable, indicating that the system can be tested and maintained effectively, with stability ensured for long-term use. Overall, the combined evaluations (Table 7) showed a highly acceptable rating across functionality, usability, reliability, portability, and efficiency, reinforcing the system's robustness and practical utility. The enhancements introduced by the researcher not only addressed critical issues identified in the study—such as single notification, single registered number, and reliance on AC power—but also reflected the principles of effective instructional design and system development in technology-based interventions (Richey, Klein, & Nelson, 2004). The integration of a dual-notification system, multiple registered numbers, and backup power mirrors recommendations from technology design literature that highlight redundancy, fault tolerance, and user-centered approaches as essential for reliable and sustainable systems (Seels & Richey, 1994). Additionally, the inclusion of a user manual ensures that the end-users are well-informed about the components and operations of the device, enhancing usability and reducing operational errors. In conclusion, the Android-based anti-intrusion device demonstrates a successful application of system development principles, combining reliability, portability, efficiency, maintainability, and usability. The enhancements made by the researcher ensure that the device remains functional under diverse scenarios, providing comprehensive security support to household members and business establishment owners. These findings align with prior studies emphasizing that user-centered design, system fault

tolerance, and proper documentation are critical factors in the success of technology-driven solutions (Richey, Klein, & Nelson, 2004; Seels & Richey, 1994).

Problem 6. A User's Manual Developed with the Use of an Android Based Anti-Intrusion Device

The researcher developed a comprehensive user manual for the Android-Based Anti-Intrusion Device using a motion sensor with SMS notification. This manual provides a clear introduction to the device, highlighting its role in safeguarding individuals' lives and properties from potential burglaries. It serves as a structured guide to help users navigate and utilize the system effectively, addressing the need for usability and accessibility emphasized in instructional design literature (Seels & Richey, 1994). The manual includes detailed descriptions of the device's key components, such as the Arduino Uno microcontroller, PIR sensor, GSM modem, DC power supply, 360-eye camera, and the Android application. Step-by-step instructions are provided for setting up the device, configuring the 360-eye camera, and operating the Android application. These instructions align with best practices in technology-based system design, where clear documentation and user guidance are essential to ensure proper system operation and reduce user errors (Richey, Klein, & Nelson, 2004). Additionally, the manual features a Frequently Asked Questions (FAQ) section, offering troubleshooting tips and solutions to common issues. This feature enhances the device's reliability and maintainability, ensuring that users can address minor problems independently without compromising system performance. By providing comprehensive guidance, the user manual also supports the portability and efficiency of the device, allowing household members and business establishment owners to maximize its functionality in real-world scenarios. Overall, the development of a user manual reflects the integration of user-centered design principles with instructional technology practices. It not only facilitates effective use of the Android-Based Anti-Intrusion Device but also reinforces the importance of structured documentation in enhancing the usability, reliability, and safety of technology-driven security systems (Richey, Klein, & Nelson, 2004; Seels & Richey, 1994).

4. Conclusion

The study successfully designed, developed, and evaluated an Android-based anti-intrusion device using a motion sensor with SMS notification, which was found to be highly acceptable to both household members and business establishment owners in terms of functionality, usability, reliability, portability, efficiency, and maintainability, with no significant difference in their assessments. These findings confirm that the system is a practical, reliable, and cost-effective security solution that can help safeguard lives and properties against intrusion. Based on the results, the following recommendations are proposed: (1) future enhancements should prioritize the integration of multi-channel alert mechanisms such as mobile application notifications, email alerts, and audible alarms to complement SMS notifications and ensure timely warnings; (2) power reliability should be improved through the inclusion of rechargeable battery backups or solar-assisted power systems to maintain continuous operation during power outages; (3) the system should allow multiple mobile numbers to be registered to enable simultaneous notifications to owners, family members, or security personnel; (4) camera functionality may be enhanced by incorporating higher-resolution imaging, night vision, and offline video recording features for improved monitoring; and (5) user support and system adoption can be strengthened by improving the Android application interface and supplementing the user manual with visual, step-by-step guides or video tutorials, while encouraging future studies to conduct extended field testing to evaluate long-term performance and scalability.

Compliance with ethical standards

Statement of ethical approval

The study ensured ethical compliance by obtaining informed consent from all participants and maintaining their confidentiality. Respondents were informed about the purpose of the study, the procedures involved, and their right to withdraw at any time. Data collected were used solely for research purposes, and sensitive information was anonymized to protect privacy. Ethical considerations also extended to the proper handling of installed devices in homes and business establishments, ensuring no disruption to daily activities or compromise of personal property.

REFERENCES

Akhter, M. B. (2025). *Development and analysis of an IoT security alarm system leveraging GSM communication networks*. European Journal of Electrical Engineering and Computer Science. Retrieved from https://eu-opensci.org/index.php/ejece/article/view/19765

Aluko, O. A., et al. (2021). *Development of wireless based home security system using PIR sensor*. https://www.repcomseet.org/journal/ALUKO__et_al__DEVELOPMENT_OF_WIRELESS_BASED_HOME_SECURITY_SYSTEM_USING_PIR_SENSOR1.pdf

ARC Journals. (2020). *Design and construction of a microcontroller-based intrusion detector with SMS alert*. https://www.arcjournals.org/pdfs/ijirec/v7-i4/1.pdf

De Lara, M. G. O., & Santos, A. R. (2024). *Service Delivery and Quality Assurance in Administrative Units of Higher Education Institutions During the Pandemic. Corporate and Business Strategy Review, 5 (1), 494–504*.

Jacoba, E. F. P., Gamit, A. M., Santos, A. R., Alvarez, S. C., Peria, J. N. T., & Claudio, A. E. G. (2025). Exploring Digital and Documentation Issues in State University–LGU Collaborative Programs for Sustainable Quality Education. *International Journal of Learning, Teaching and Educational Research*, *24*(6).

Richey, R. C., Klein, J. D., & Nelson, W. A. (2004). Developmental research: Studies of instructional design and development. Educational Technology Research and Development, 52(3), 51–58. Retrieved from https://www.sciepub.com/reference/105902

Royce, W. W. (1970). *Managing the development of large software systems.* In *Proceedings of IEEE WESCON. Retrieved from https://www.praxisframework.org/files/royce1970.pdf*

Seels, B., & Richey, R. (1994). Instructional technology: The definition and domains of the field. Association for Educational Communications and Technology. Retrieved from https://bibbase.org/network/publication/seels-richey-instructionaltechnologythedefinitionanddomainsofthefield-1994

Sevilla, M. (2012). *Research methods and design in education*. Quezon City, Philippines: Rex Bookstore. Retrieved from https://licbansalan.umindanao.edu.ph/bib/286

Torres-Hernandez, C. M., Garduño-Aparicio, M., & Rodriguez-Resendiz, J. (2023). *Smart home security systems and user perception*. Technologies, 11(4). https://www.mdpi.com

Tuliao, R. C., Santos, A. R., & Ortega, S. A. (2025). The Role of Mobile Phones in Facilitating Business Education During the Transition to New Normal Learning Models. *International Review of Management and Marketing*, *15*(1), 146.

Author's short biography

Rommel V. Romero is an Information Technology Officer at the Maritime Industry Authority, specializing in digital transformation, IT governance, and cybersecurity. He holds a BS in ICT and an MS in IT, with certifications as a Data Privacy Officer and Scientific and Technological Specialist. His expertise covers software development management, systems implementation, cybersecurity and ethical hacking, network infrastructure, and business continuity planning. He is committed to strengthening secure, compliant, and future-ready IT infrastructures.

Dr. Ma. Eugenia M. Yangco is a Full Professor of Technology Education at Rizal Technological University, Mandaluyong City, Philippines. She holds a PhD in T echnology Education.

Aljon Peter L. Temporal is an academic researcher, peer reviewer, and faculty member at Our Lady of Fatima University. He holds a BA in Political Science and an MA in Public Administration, ranked Top 3 in the Certified Public Governance Examination (CPLRTC), and is completing his PhD in Public Administration at Rizal University.