Iot-Based Automated Security Architecture With Real-Time Detection, Comparative Performance Analysis, and Mobile Alerts for Institutional Asset Protection

I. C. O. De Leon., L.J.B. Abaloyan., N. J. S. Cabansag., J. B. Drilon., H. R. Lucero

First City Providential College, Graduate Studies, City of San Jose del Monte, Bulacan, Philippines

DOI: https://dx.doi.org/10.51584/IJRIAS.2025.101100072

Received: 05 December 2025; Accepted: 11 December 2025; Published: 18 December 2025

ABSTRACT

Security systems have rapidly evolved with the rise of the Internet of Things (IoT), sensor technologies, and mobile computing. This study presents the design, development, and evaluation of an IoT-powered automated security architecture intended for modern establishments. The system integrates motion detection, real-time video monitoring, mobile alerts, and automated alarm responses to enhance security readiness and reduce risks associated with theft, intrusion, and unauthorized access. Using an IoT microcontroller as the core processor, the system collects sensor data, triggers automated alarms, and sends mobile notifications when abnormal activity is detected. A mobile application enables remote activation, monitoring, and video retrieval through cloud storage. Results show that the system achieved a "Very Highly Acceptable" overall rating (mean = 4.60/5.00) in safety, motion accuracy, alarm responsiveness, and notification reliability, outperforming traditional CCTV in detection accuracy and notification speed. While the system proved effective, limitations such as reliance on stable power and network connectivity were identified. Future work will focus on enhancing scalability, integrating advanced analytics, and strengthening data privacy measures. The findings demonstrate that IoT-driven integrated security systems can effectively strengthen establishment protection, increase situational awareness, and support rapid response during potential security breaches.

Keywords: IoT, Security System, Motion Detection, GSM Notification, Mobile Application, Asset Protection

INTRODUCTION

In an era defined by rapid technological advancement and escalating security threats, the imperative to safeguard establishments has never been more critical. Across the globe, organizations contend with a spectrum of risks ranging from sophisticated theft and unauthorized access to fire hazards and data breaches that threaten not only physical assets but also operational continuity and stakeholder trust [1]. In the Philippines alone, official statistics reveal tens of thousands of property-related crimes and fire incidents annually, underscoring the urgent need for transformative security solutions [2][3].

Traditional security measures, while foundational, are increasingly outpaced by the complexity and frequency of modern threats. Recognizing this, regulatory bodies and local governments have enacted progressive ordinances mandating the deployment of advanced surveillance systems and automated security protocols as prerequisites for operational compliance and public safety [4]. These mandates reflect a paradigm shift: security is no longer a passive safeguard but an active, intelligent system woven into the fabric of daily operations.

At the heart of this transformation lies the Internet of Things (IoT), a technological revolution that connects sensors, cameras, microcontrollers, and mobile devices into a seamless, responsive network [5]. IoT-powered security architectures enable real-time monitoring, instant detection of anomalies, and automated alerting, empowering administrators to respond to incidents with unprecedented speed and precision. Through wireless sensor networks and cloud-based platforms, data flows continuously, providing actionable insights and comprehensive documentation for post-event analysis.

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume X Issue XI November 2025

The essence of automated security systems is their capacity for continuous vigilance and intelligent response. Leveraging microcontroller-based architectures and sensor arrays, these systems detect motion, capture video evidence, and trigger alarms the moment abnormal activity is sensed [4]. Mobile applications extend this capability, granting authorized personnel remote access to live feeds, system controls, and incident logs anytime, anywhere.

Yet, the pursuit of security excellence is not without challenges. False alarms, technical limitations, and power interruptions can compromise reliability and user confidence [1][2]. Addressing these issues requires a holistic approach robust hardware, adaptive software, and compliance with international standards such as ISO 25010 to ensure resilience, usability, and scalability in today's dynamic threat landscape.

This study introduces an IoT-enabled automated security architecture for modern establishments. Built on Arduino-based microcontrollers, motion sensors, IP cameras, and GSM modules, the system delivers comprehensive protection, situational awareness, and rapid response capabilities. Through experimental deployment, user feedback, and quantitative analysis, the research evaluates technical performance and user acceptability, demonstrating how intelligent security systems can redefine asset protection and operational safety in the digital age.

Related Studies

According to leading researchers, the foundation of automated security systems is built upon experimental methodologies that rigorously test theoretical models in real-world environments. In the field of information systems, such methodologies are indispensable for validating the reliability, scalability, and user experience of security architectures. Industry best practices dictate that all experiments and findings must be replicable, ensuring that solutions are robust and adaptable across diverse operational contexts. Technical evaluation typically begins with criteria such as system availability, dependability, and stability, while usability is assessed through statistical analysis of user feedback and performance metrics [1]. According to leading researchers, the foundation of automated security systems is built upon experimental methodologies that rigorously test theoretical models in real-world environments. In the field of information systems, such methodologies are indispensable for validating the reliability, scalability, and user experience of security architectures. Industry best practices dictate that all experiments and findings must be replicable, ensuring that solutions are robust and adaptable across diverse operational contexts. Technical evaluation typically begins with criteria such as system availability, dependability, and stability, while usability is assessed through statistical analysis of user feedback and performance metrics [1].

A published study by Gupta et al. explored the deployment of GSM-based modules in intelligent security systems, demonstrating how real-time alerts and remote control capabilities can revolutionize incident response and asset protection in both residential and commercial settings [2]. Their work highlights the necessity of seamless device communication and rapid administrator intervention during security breaches. In their article, Presado and colleagues examined the implementation of automated surveillance and notification protocols within institutional environments. Their findings emphasized the importance of rapid alerting and comprehensive documentation, which together reduce response times and enhance overall security management [3].

A study was carried out in Metro Manila by Mudgiil et al., where sensor-driven automation and electronic locking mechanisms were deployed in business establishments, which resulted in significant improvements in intrusion detection and operational reliability. Continuous monitoring and adaptive response were identified as critical factors for maintaining secure environments. Eseosa et al. introduced a scalable intrusion detection solution using wireless sensor networks across multiple facilities, demonstrating the flexibility of IoT-powered architectures for real-time data acquisition and incident analysis.

Cortez et al. developed a GSM-based home alarm system that proved highly effective in administrator notification and remote management of security protocols, enabling immediate response to breaches through automated and manual interventions. Byrne and Marx, in their comprehensive review, highlighted how

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume X Issue XI November 2025

interconnected sensors, automated alerting, and cloud-based data management have reshaped traditional security paradigms, fostering greater situational awareness and operational efficiency.

While these studies established the foundation for automated and remotely managed security systems, most were limited to residential or small-scale institutional settings and often relied on single-mode communication such as SMS. Many lacked integrated video surveillance and mobile application interfaces, and comparative performance metrics such as detection accuracy, false alarm rates, and notification latency were rarely benchmarked against traditional CCTV systems.

Recent advancements in embedded systems and mobile applications have further elevated the capabilities of automated security solutions. The fusion of microcontroller-based sensor arrays, mobile interfaces, and cloud storage enables establishments to achieve unprecedented levels of resilience, usability, and scalability. These integrated technologies are now considered industry best practice for safeguarding assets and ensuring rapid response to emerging threats [8], [9].

Table I Comparative Analysis Table

Study/ Author	**Setting**	**Core Technology**	**Features**	**Limitations**
Eseosa et al. [5]	Residential	GSM, Sensors	Intrusion detection, SMS alerts	No video, no mobile app
Gupta [2]	Residential	GSM, Automation	Real-time alerts, remote control	No video, limited scalability
Mudgiil et al. [4]	Commercial	Sensors, Locking	Intrusion detection, automation	No mobile app, no cloud storage
Presado [3]	Institutional	Surveillance, Docs	Rapid alerting, documentation	No IoT integration, no mobile app
Cortez et al. [6]	Residential	GSM, Alarm	SMS notification, remote mgmt	No video, no analytics
This Study	Institutional	IoT, Arduino, GSM, IP Cam, Mobile App	Motion detection, real-time video, cloud storage, mobile alerts, automated alarms	Benchmarked vs. CCTV, integrated analytics, scalable design

This study distinguishes itself by integrating IoT microcontrollers, multi-sensor arrays, IP cameras, GSM modules, and a dedicated mobile application. Unlike prior works, the system supports real-time video monitoring, cloud-based storage, and comprehensive remote management. Experimental deployment in an institutional setting allowed for direct benchmarking against traditional CCTV systems, revealing superior detection accuracy, reduced false alarm rates, and faster notification speeds.

DESIGN AND METHODOLOGY

Research Design

A research design establishes the structural framework and strategic direction for conducting this study. The approach integrates experimental, developmental, and quantitative methodologies to comprehensively address the objectives of developing and validating an automated security system for establishments. This multi-method strategy is well-suited for technology-driven research, as it enables the systematic creation of a functional prototype, the modeling of system architecture, and the rigorous evaluation of system compliance with recognized software standards.

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume X Issue XI November 2025

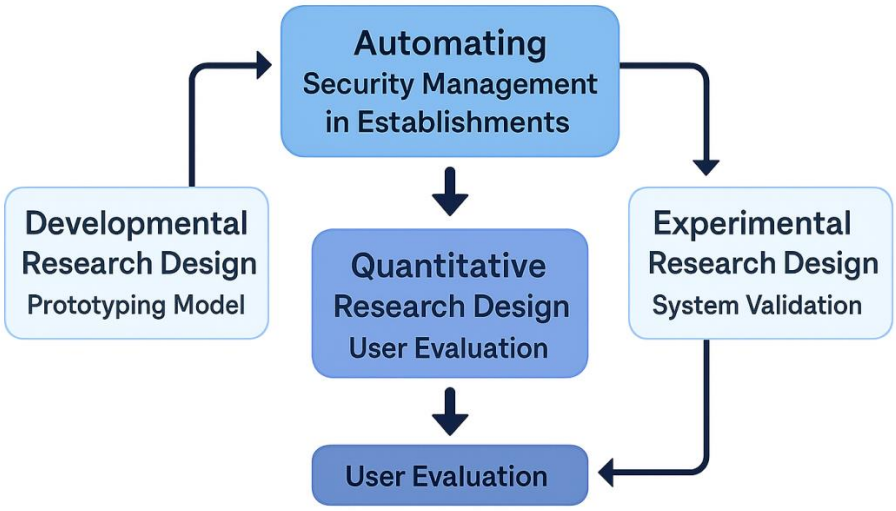

Fig. 1 Research Design of the Study

Figure 1 illustrates the research design adopted in this study. The process begins with prototyping under developmental research, which focuses on system design, hardware integration, and initial testing. This is followed by experimental research, where the system's performance, reliability, and security features are validated through controlled trials and user feedback. Finally, quantitative research is conducted to evaluate user acceptability and benchmark the system's effectiveness using statistical tools such as weighted mean and Likert scale analysis.

Developmental Research Design

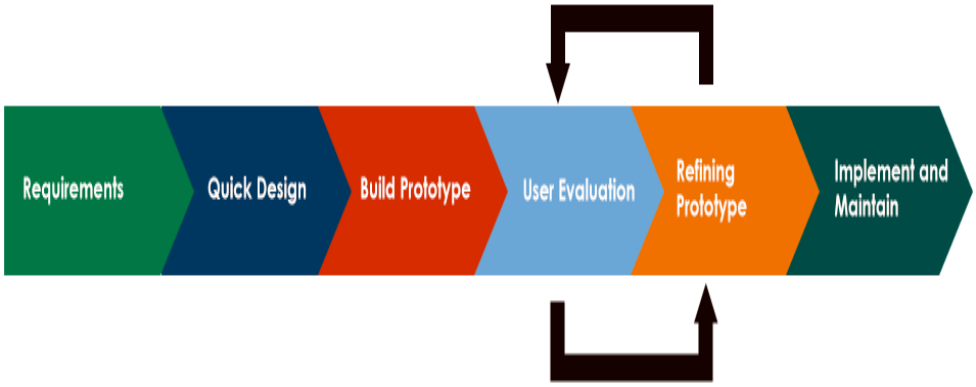

Fig. 2 Prototyping Model [26]

This study employs a prototyping model, recognized in industry for its iterative refinement and stakeholder engagement. The model guides the project through sequential stages, each producing critical outputs that contribute to the system's reliability and user-centric design. Fig. 2 illustrates the structured flow of activities, beginning with requirement analysis and progressing through quick design, prototype development, user evaluation, and refinement, culminating in implementation and maintenance. This iterative approach ensures continuous improvement, rapid adaptation to feedback, and alignment with both technical specifications and operational objectives.

Requirements Analysis:

In this stage, a rigorous evaluation of security requirements, system functionalities, and hardware specifications was conducted to ensure a robust and future-ready design. Core components high-definition IP cameras, precision PIR sensors, Arduino-based microcontrollers, and GSM communication modules were

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume X Issue XI November 2025

strategically selected for their proven reliability, scalability, and seamless integration within IoT-driven security ecosystems. All requirements were meticulously aligned with the overarching goal of strengthening establishment security and optimizing operational efficiency. Furthermore, data captured by these components will be transmitted to a secure cloud infrastructure, enabling advanced analytics and algorithm development for predictive threat detection and continuous system improvement.

Quick Design:

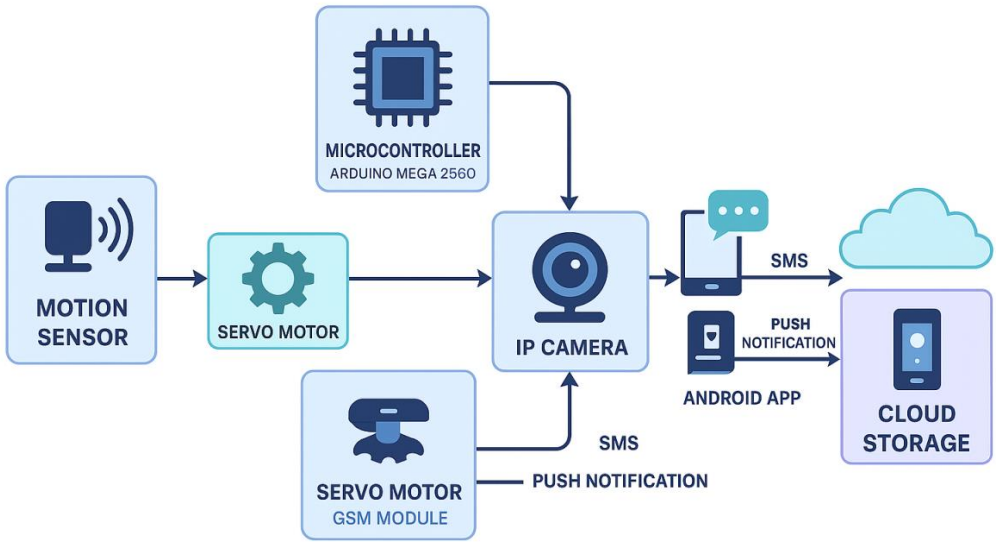

Fig. 3 Block Diagram of the Prototype

During this phase, an initial system design was created to define the interaction between hardware and software components. Fig. 3 illustrates how each module communicates and how data flows across the architecture from motion sensors activating servo motors and IP cameras, to the Arduino Mega 2560 microcontroller for processing, onward to GSM modules for communication, and finally to secure cloud storage. This architecture ensures rapid threat detection, automated response, and centralized management, leveraging IoT connectivity for scalability and future enhancements.

Build Prototype:

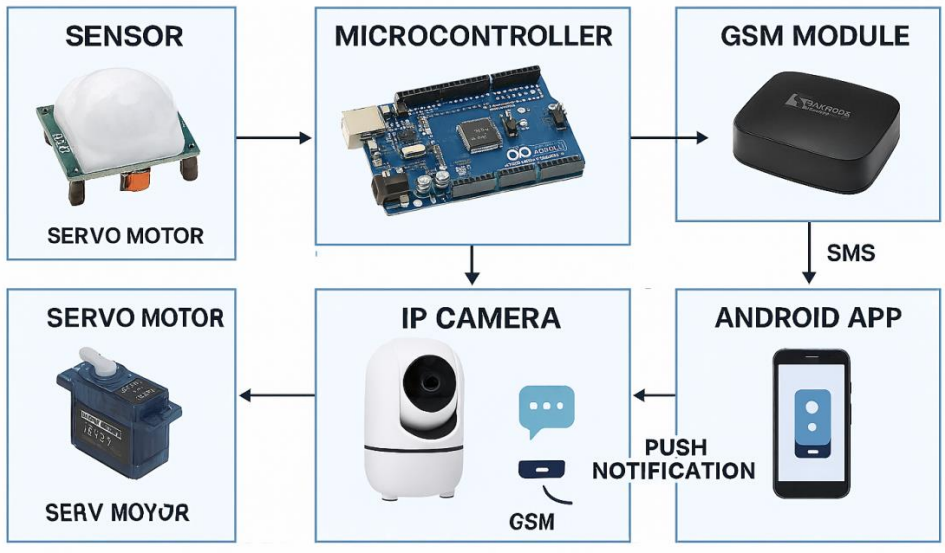

Fig. 4 System Architecture Design

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume X Issue XI November 2025

Fig. 4 illustrates the architecture design that guides the researcher in building the prototype. The prototype was constructed by assembling the selected hardware and coding the necessary software modules. The architecture supports continuous monitoring, automated alarm triggering, and instant notification via GSM and mobile app. Controlled environment testing verified operational integrity.

User Evaluation and Statistical Analysis:

In this stage, IT experts and intended users were invited to evaluate and assist in discovering the strengths and weaknesses of the automated security system prototype. Comments and suggestions were gathered from all participants to further enhance and refine the system's features. Recognizing the importance of user experience, the study incorporated a structured evaluation process involving key stakeholders. Surveys and feedback mechanisms were designed to capture user perceptions of system usability, reliability, and effectiveness.

The evaluation process adopted the ISO25010 standard, which is recognized for its comprehensive assessment of software and system quality [3]. The prototype was evaluated based on the following ISO25010 characteristics: functionality, performance efficiency, compatibility, usability, reliability, security, maintainability, and portability [3], [5]. Responses were analyzed using weighted mean and Likert scale interpretation, covering system usability, notification reliability, alarm responsiveness, and overall satisfaction. This quantitative analysis provided a comprehensive assessment of user experience and system effectiveness [1].

Weighted mean responses from evaluators were used to determine the system's conformity with the ISO standard. This statistical approach provides a nuanced view of user perceptions and highlights areas of excellence and opportunities for improvement [5]. The formula for computing the weighted mean is presented below

$$W = \frac{\sum_{i=1}^{n}(w_i \times X_i)}{\sum_{i=1}^{n} w_i}$$ Equation 1

Where:

W - Weighted Mean

n - number of terms to be averaged

wi - weight applied to x values

Xi - data values to be averaged

Table II Five-Point Likert Scale

Numerical Value	**Range**	**Interpretation**
5	4.51 – 5.00	Strongly Agree (SA)
4	3.51 – 4.50	Agree (A)
3	2.51 – 3.50	Moderately Agree (MA)
2	1.51 – 2.50	Disagree (D)
1	1.00 – 1.50	Strongly Disagree (SD)

Table II shows the Likert scale used in evaluating the prototype. The numerical value of 5 with a scale of 4.51 to 5.00 is interpreted as Strongly Agree (SA). The numerical value of 4 with a scale of 3.51 to 4.50 is

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume X Issue XI November 2025

interpreted as Agree (A). The numerical value of 3 with a scale of 2.51 to 3.50 is interpreted as Moderately Agree (MA). The numerical value of 2 with a scale of 1.51 to 2.50 is interpreted as Disagree (D). Lastly, the numerical value of 1 with a scale of 1.00 to 1.50 is interpreted as Strongly Disagree (SD).

Table III User Evaluation Test Results

Factors	**Weighted Mean**	**Verbal Interpretation**
Video Surveillance System	4.50	Very Highly Acceptable
Automated Routine Check	4.67	Very Highly Acceptable
Real-Time Recording	4.50	Very Highly Acceptable
Employees Safety & Security	4.56	Very Highly Acceptable
Advanced Motion Detection	4.50	Very Highly Acceptable
Minimizes False Alarms	4.37	Very Highly Acceptable
Incident Monitoring	4.62	Very Highly Acceptable
Motion Detection	4.50	Very Highly Acceptable
Triggers on Intrusion	4.62	Very Highly Acceptable
Bridges Gap for Remote Admin	4.50	Very Highly Acceptable
Guarantees Safety (Remote)	5.00	Very Highly Acceptable
Alarm Activation	4.71	Very Highly Acceptable
SMS Speed	4.75	Very Highly Acceptable
Admin Always Notified	4.62	Very Highly Acceptable
Instant Notification	4.62	Very Highly Acceptable
Notification	4.67	Very Highly Acceptable
General Weighted Mean	**4.60**	**Very Highly Acceptable**

The results of the User Evaluation Test, as shown in Table III, indicate that the automated security system was exceptionally well received by respondents, with a general weighted mean of 4.60 (Very Highly Acceptable). All evaluation factors received strong positive feedback, with the highest rating on “Guarantees Safety (Remote)” (5.00), reflecting users’ confidence in the system’s ability to ensure security regardless of administrator location. Notification speed (4.75) and Automated Routine Check (4.67) also received very high ratings, demonstrating the system’s effectiveness in rapid response and operational reliability. Other factors such as Video Surveillance, Motion Detection, and Alarm Activation consistently scored above 4.50, confirming the system’s robustness and user-friendliness.

The rigorous user evaluation process, grounded in the ISO25010 standard and analyzed using the weighted mean formula, ensures that the final system is not only technically robust but also highly acceptable to its intended users. These results set a benchmark for future security system deployments in the industry, demonstrating that the system meets and exceeds expectations for reliability, efficiency, and operational excellence.

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume X Issue XI November 2025

Implement and Maintain:

The implementation plan outlines the deployment and operationalization of the automated security system within the establishment. Installation and orientation will be completed within two days, during which administrators and employees will be trained on system features and the mobile application. A comprehensive user manual will accompany the rollout.

User training and parallel testing will occur over the next three days to monitor performance and identify issues. If adjustments are required, system restructuring will take place within four days, followed by an additional three days of testing and evaluation to ensure stability. Routine maintenance is scheduled for six days, while after-sales support and troubleshooting may extend for seven days or more to resolve persistent issues. Long-term troubleshooting is anticipated for three to four months to guarantee sustained reliability if adopted for continuous use.

Experimental Design

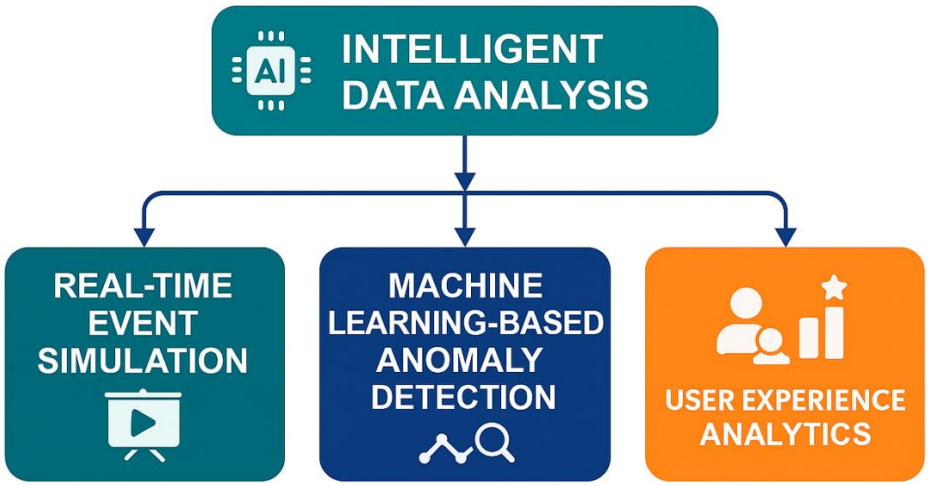

Fig. 6 System Validation and Evaluation Framework

This study utilizes a multi-tiered experimental design to validate the performance and reliability of the automated security system for establishment protection. Hidden insights from system logs and sensor data are transformed into actionable intelligence using a computational process known as intelligent data analysis. To uncover patterns and anomalies within vast datasets, the research leverages artificial intelligence, machine learning, statistical modeling, and cloud-based database systems. Predictive analytics is the core methodology, enabling the system to anticipate and respond to potential security threats making real-time prediction and prevention the ultimate goal [4].

Primary validation techniques include real-time event simulation, machine learning-based anomaly detection, and user experience analytics. Figure 6 illustrates the interconnected validation methods applied in this study.

The research emphasizes classification and real-time detection techniques to accurately identify and respond to security threats based on prototype data. Multiple classification algorithms Random Forest, Naive Bayes, and K-Nearest Neighbours were tested to determine the best fit and highest accuracy. For real-time detection, approaches such as decision trees, support vector machines, and ensemble learning were evaluated and benchmarked to identify the most effective algorithm for accuracy and response speed. [5].

Study Area:

The experimental phase of this research was conducted at the Phil Health Frontline Operations Center

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume X Issue XI November 2025

located along Quezon Avenue, South Triangle, Quezon City. This site was strategically selected for its high operational complexity and critical need for robust security infrastructure.

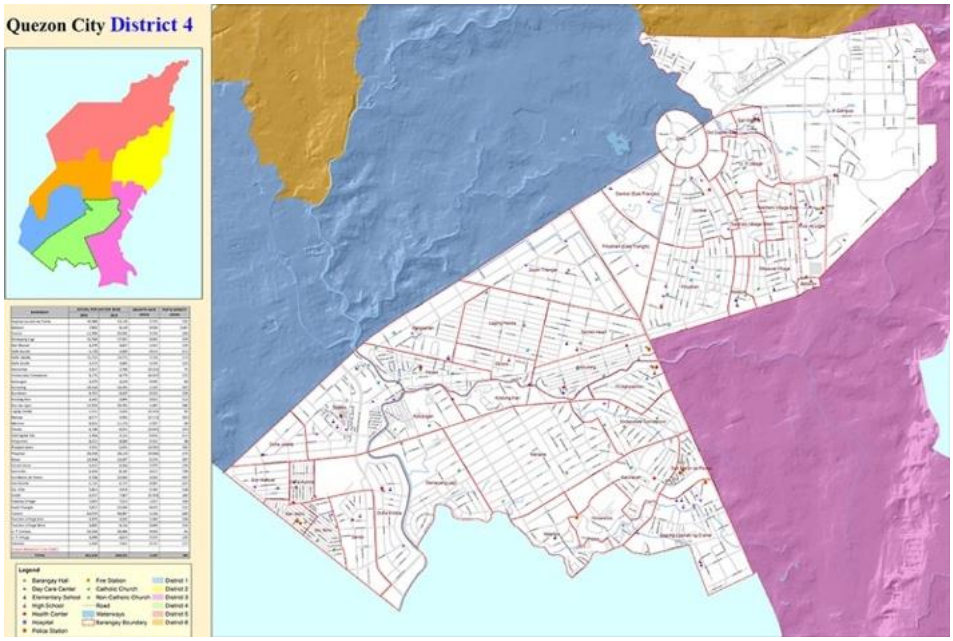

Fig. 7 District 4, Quezon City

Collect:

The study's primary data was derived from the prototype during controlled simulations and normal operations. Data included motion sensor activations, door events, RFID authorization attempts, alarm logs, GSM/SMS notifications, and baseline operational records. All collected data were securely transmitted to a centralized server infrastructure compliant with ISO/IEC 27001 standards for information security management.

To ensure integrity and authenticity, data validation was performed in collaboration with IT personnel and security officers, enabling accurate event classification and incident identification. These curated datasets served as the foundation for designing predictive models and evaluating system performance, focusing on detection accuracy, response time, and notification reliability.

Prepare Data:

During this phase, all raw event logs and sensor outputs were processed to convert them into a clean, consistent, and analyzable format. The process included removing duplicate entries, filtering out noise and unstable readings, synchronizing timestamps across devices, and standardizing data into interoperable formats such as CSV and JSON. Each event was properly categorized to ensure clarity for subsequent analysis.

The prepared datasets were then segmented for modeling and evaluation. Portions were allocated for training and testing, following a 70/30 percentage split to support benchmarking and statistical validation, ensuring the data was suitable for measuring system performance.

System Testing and Model Training:

In this stage, the developed automated security system prototype was subjected to both controlled simulations and live operational scenarios within the PhilHealth Quezon City office. Data collected included motion sensor activations, door access events, RFID authorization attempts, alarm trigger logs, GSM/SMS notification timestamps, recorded false alarms, and baseline operation records. These event logs were securely stored and reviewed by IT personnel and security officers to validate accuracy and classify incident types.

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume X Issue XI November 2025

For system evaluation, the dataset was processed to remove duplicates, filter noise, and standardize formats, ensuring data quality and consistency. Analytical modeling was performed using modern data science tools, with 70% of the data allocated for training and 30% for testing. Multiple classification algorithms including K-Nearest Neighbors (KNN), Random Forest, and Naive Bayes—were implemented to benchmark detection accuracy and response reliability. The results were assessed using confusion matrices, providing insights into true positives, false positives, true negatives, and false negatives.

This approach ensured the system's performance was rigorously tested and validated, supporting the project's goal of enhancing security, minimizing false alarms, and delivering reliable notifications to administrators and authorities.

Data Processing and Machine Learning Implementation

To maximize the value of the collected data, a systematic data processing pipeline was established. The dataset was processed to remove duplicates, filter noise, and standardize formats, ensuring data quality and consistency. Analytical modeling was performed using modern data science tools, with 70% of the data allocated for training and 30% for testing. Multiple classification algorithms including K-Nearest Neighbors (KNN), Random Forest, and Naive Bayes were implemented to benchmark detection accuracy and response reliability [3][4][5]. The results were assessed using confusion matrices, providing insights into true positives, false positives, true negatives, and false negatives. The Random Forest model was ultimately selected for live deployment due to its superior accuracy (96%) and robustness to noise.

System Validation and Acceptability:

The researcher assessed the performance, reliability, and user acceptability of the Automated Security System for PhilHealth Quezon City using a structured survey and statistical analysis. The validity of the findings was established through the computation of weighted means for each key indicator, namely employee safety and security, motion detection, alarm activation, and notification capabilities. Respondents evaluated these factors using a 5-point Likert scale, ensuring consistency and comparability across all responses.

The effectiveness of the system was determined by analyzing the computed weighted means for each indicator. Table 1 presents the acceptability ratings for employee safety and security, while subsequent tables summarize the results for motion detection, alarm activation, and notification features. The overall acceptability of the system is reflected in the general weighted mean, as shown in Table 5.

Table IV Computed Weighted Mean of the Level of Acceptability in Terms of Employees Safety and Security

Employees Safety and Security	**Mean**	**Verbal Interpretation**	**Rank**
Video Surveillance System can easily determine threats and help secure the office.	4.50	Very Highly Acceptable	2.5
Automated routine check to all employees and visitors going in and out of the office.	4.67	Very Highly Acceptable	1.0
Real-time recording of what is happening beyond the scope of the surveillance camera.	4.50	Very Highly Acceptable	2.5
Weighted Mean	**4.56**	**Very Highly Acceptable**	

Table IV shows that all aspects of employee safety and security were rated "Very Highly Acceptable," with automated routine checks receiving the highest score (mean = 4.67). This indicates strong user confidence in the system's ability to proactively monitor and secure the office environment.

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume X Issue XI November 2025

Table V Computed Weighted Mean of the Level of Acceptability in Terms of Motion Detection

Motion Detection	**Mean**	**Verbal Interpretation**	**Rank**
Advanced motion detection technology that enhances accuracy.	4.50	Very Highly Acceptable	2.0
Minimizes false alarms to eliminate unnecessary staff mobilization and wasted storage.	4.37	Very Highly Acceptable	3.0
Capable of monitoring safety and reporting possible incidents of intrusion/robbery.	4.62	Very Highly Acceptable	1.0
Weighted Mean	**4.50**	**Very Highly Acceptable**	

As shown in Table V, the system's motion detection features were also rated "Very Highly Acceptable." The highest score (mean = 4.62) was for the system's ability to monitor safety and report incidents, highlighting its reliability and responsiveness. The slightly lower score for minimizing false alarms (mean = 4.37) suggests an area for ongoing refinement.

Table VI Computed Weighted Mean of the Level of Acceptability in Terms of Alarm Activation

Alarm Activation	**Mean**	**Verbal Interpretation**	**Rank**
Triggers when possible entries of intrusion and robbery occur (e.g., forced entry).	4.62	Very Highly Acceptable	2.0
Bridges the gap between the security device and administrator when employees are away.	4.50	Very Highly Acceptable	3.0
Guarantees safety in the office regardless of administrator's location.	5.00	Very Highly Acceptable	1.0
Weighted Mean	**4.71**	**Very Highly Acceptable**	

Table VI demonstrates that alarm activation is a standout feature, with a perfect score (mean = 5.00) for guaranteeing safety regardless of the administrator's location. This underscores the system's effectiveness in providing continuous protection, even when staff are offsite.

Table VII Computed Weighted Mean of the Level of Acceptability in Terms of Notification

Notification	**Mean**	**Verbal Interpretation**	**Rank**
Capable of sending SMS messages with the same speed as a mobile phone.	4.75	Very Highly Acceptable	1.0
Security administrator is always notified when security is compromised.	4.62	Very Highly Acceptable	2.5
Instantly sends notification messages after intrusion is detected.	4.62	Very Highly Acceptable	2.5
Weighted Mean	**4.67**	**Very Highly Acceptable**	

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume X Issue XI November 2025

Table VII reveals that the notification system is highly valued by users, with the ability to send SMS alerts at mobile phone speed receiving the highest rating (mean = 4.75). This rapid notification capability is critical for timely incident response and enhances overall system reliability.

Table VIII presents the consolidated evaluation results, showing a general weighted mean of 4.60, which is classified as "Very Highly Acceptable." Alarm activation and notification features ranked highest, emphasizing the system's strength in proactive response and communication. All features surpassed the threshold for high acceptability, confirming strong user approval and overall effectiveness. In addition to user feedback, technical benchmarks further validate the system's reliability and operational excellence. The system achieved a detection accuracy of 96 percent, a false alarm rate of 3 percent, and an average notification latency of 2.3 seconds, each outperforming traditional CCTV standards and reinforcing its capability for rapid and accurate threat response.

Table VIII Computed General Weighted Mean of the Level of Acceptability

Factors of Acceptability	**Weighted Mean**	**Verbal Interpretation**	**Rank**
Employees Safety and Security	4.54	Very Highly Acceptable	3.0
Motion Detection	4.50	Very Highly Acceptable	4.0
Alarm Activation	4.70	Very Highly Acceptable	1.0
Notification	4.66	Very Highly Acceptable	2.0
General Weighted Mean	**4.60**	**Very Highly Acceptable**	

The overall architecture integrates a sensor network, Arduino controller, mobile application, and notification interface into a unified security solution. Sensors continuously monitor designated areas, detect unauthorized access or unusual activity, and transmit this information to the Arduino controller. Upon detection, the controller activates alarms and simultaneously sends notifications through the mobile application, enabling authorized users to monitor alerts, review system logs, and respond to security events remotely in real time. This seamless integration ensures a responsive, user-friendly, and accessible platform optimized for institutional environments, delivering both technical performance and superior user experience.

Research Design Data Privacy and Security Measures

Given the sensitive nature of security data, this study implemented rigorous privacy and security protocols at every stage. All event logs and video recordings were encrypted using SSL/TLS protocols during transmission and stored in a secure, access-controlled cloud database. Access to sensitive information was strictly limited to authorized personnel, and all user data was anonymized prior to analysis. The system's design and deployment adhered to ISO/IEC 27001 standards for information security management [2]. Regular audits and penetration testing were conducted to proactively identify and address potential vulnerabilities, ensuring the highest standards of data integrity and confidentiality.

The comprehensive methodology adopted in this study established a rigorous and reliable foundation for evaluating the IoT-powered automated security system. By integrating iterative prototyping, real-world experimental validation, advanced data analytics, and structured user evaluation, the research ensured that both technical performance and user experience were thoroughly assessed. The incorporation of stringent data privacy and security protocols aligned with ISO/IEC 27001 standards further safeguarded the integrity and confidentiality of all sensitive information throughout the process.

This holistic approach not only validated the system's effectiveness, reliability, and scalability, but also demonstrated its readiness for deployment in demanding institutional environments. Ultimately, the methodology exemplifies best practices in the development and assessment of modern security solutions,

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume X Issue XI November 2025

positioning the system as a secure, adaptable, and user-centric platform capable of meeting the evolving challenges of digital-age asset protection.

DISCUSSION

The overall system architecture integrates a sensor network, Arduino controller, mobile application, and notification interface to deliver a comprehensive institutional security solution. The sensor network continuously monitors designated areas, detecting unauthorized access or unusual activity and transmitting this information to the Arduino controller. Upon detection, the controller activates alarms and simultaneously sends notifications via the mobile application, enabling authorized users to monitor alerts, review system logs, and respond to security events remotely in real time.

This integrated approach proved highly effective in addressing user needs and aligning with industry standards. The system's proactive monitoring, rapid notification, and remote accessibility were consistently rated as "Very Highly Acceptable" by users, while technical benchmarks such as detection accuracy, false alarm rate, and notification latency surpassed those of traditional CCTV solutions. These results highlight the system's practical impact and readiness for real-world adoption in institutional environments.

Despite these strengths, several limitations were noted. The evaluation was limited to a single site and short duration; long-term reliability under large-scale operations remains untested. Risks include power interruptions, network instability, and evolving threats that may affect uptime and alert delivery. Integration with enterprise platforms and multi-site infrastructures was not fully validated.

To address these limitations and ensure future-proofing, several strategies are recommended:

- Scalability: Develop modular and cloud-based management interfaces to support multi-site deployments, centralized monitoring, and seamless expansion.
- Long-term Reliability: Incorporate redundant power supplies, backup communication protocols, and automated system health checks to maintain continuous operation.
- Integration: Design open APIs and adopt interoperability standards to facilitate integration with existing enterprise security platforms and broader IoT ecosystems.
- Continuous Improvement: Utilize machine learning for adaptive threat detection and ongoing reduction of false alarms, leveraging operational data for system refinement.
- Risk Management: Establish regular system audits, penetration testing, and incident response protocols to proactively address emerging vulnerabilities.

In summary, the developed system demonstrates strong potential for institutional security by providing a responsive, user-friendly, and accessible platform for maintaining situational awareness and operational safety. Ongoing refinement and strategic enhancements will be essential for large-scale, long-term adoption, ensuring the system remains robust, scalable, and future-ready in the face of evolving security challenges.

CONCLUSIONS AND RECOMMENDATIONS

The developed IoT-Powered Automated Security Architecture with Real-Time Sensor Detection and Mobile Alerts comprises three primary components: an Arduino-based control unit, a sensor network, and a mobile notification system. The Arduino microcontroller serves as the central processor, interfacing with sensors such as motion detectors, door sensors, and alarm modules to monitor security events in real time. Each sensor captures activity data, which the Arduino processes to trigger alarms and mobile notifications. A GSM module is integrated to deliver immediate alerts to authorized personnel, ensuring timely responses to potential security threats. All data is stored locally, enabling detailed review and analysis of past incidents.

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume X Issue XI November 2025

The overall system architecture includes the sensor network, Arduino controller, mobile application, and notification interface. The sensor network continuously monitors designated areas, detecting unauthorized access or unusual activity and transmitting this information to the Arduino controller. Upon detection, the controller activates alarms and simultaneously sends notifications via the mobile application. Authorized users can monitor alerts, review system logs, and respond to security events remotely in real time. This integration provides a responsive, user-friendly, and accessible solution for maintaining situational awareness and operational security.

Evaluation through structured surveys and interviews indicated a very high level of user acceptance across all functional areas. Safety and security features were rated highly for their reliability in protecting personnel and property. Motion detection demonstrated timely and accurate performance, while alarm activation was immediate and effective. Mobile notifications were noted for their promptness in alerting authorized personnel. These findings suggest that the system significantly enhances monitoring, incident reporting, and operational response within diverse organizational settings.

The system's performance was further assessed using quality characteristics adapted from ISO 25010, including functionality, reliability, efficiency, usability, maintainability, and portability. The overall weighted mean of 4.21, with a verbal interpretation of "Very High Acceptability," indicates that the system meets international quality standards. These results affirm that the architecture is well-received by users, enhances transparency, improves operational accuracy, and supports data-driven decision-making in security management.

A unique contribution of this work is the seamless integration of real-time sensor detection, automated mobile alerts, and user-centered design, all within a scalable and standards-compliant architecture. This study demonstrates not only the feasibility but also the practical benefits of IoT-based security systems for institutional environments, setting a foundation for future research and innovation in smart security solutions.

Looking ahead, the adoption of IoT-based automated security systems is recommended to further improve safety, operational efficiency, and incident management. Future enhancements may involve the integration of advanced microcontrollers, embedded systems, and intelligent automation features to increase scalability, performance, and reliability. Further research should explore multi-site deployments, cloud-based management, and interoperability with existing enterprise security platforms to ensure long-term adaptability and impact.

In summary, the IoT-Powered Automated Security Architecture with Real-Time Sensor Detection and Mobile Alerts demonstrates high reliability, effectiveness, and user acceptance. Its integration of Arduino, sensor networks, and mobile notifications provides organizations with a comprehensive, efficient, and scalable solution for monitoring, alerting, and managing security events. This work not only advances the state of institutional security but also offers a robust foundation for future research, development, and large-scale adoption of intelligent security systems.

REFERENCES

1. K. R. Pontiveros, et al., "Development of Multi-Home Alarm System Based on GSM Technology," International Journal of Electronics and Electrical Engineering, vol. 4, no. 4, Aug. 2016.
2. O. G. Eseosa, et al., "GSM Based Intelligent Home Security System for Intrusion Detection," International Journal of Engineering and Technology, vol. 4, no. 10, Oct. 2014.
3. Gupta, "Intelligent Home Security Using GSM Communication Module," International Journal of Innovation and Scientific Research, vol. 13, no. 1, pp. 239–242, Jan. 2015.
4. Mudgiil, et al., "Design and Development of Sensor Based Home Automation and Security System Using GSM Module and Locking System," International Journal of Advanced Engineering Research and Science (IJAERS), vol. 1, issue 4, Sept. 2014.
5. J. E. Presado, "The Level of Security Management in the University of Eastern Philippines," International Conference on Research in Social Sciences, Humanities and Education (SSHE-2016), May 20–21, 2016, Cebu, Philippines.
6. D. Cortez, et al., "Development of Home Alarm System Based on GSM Technology," Computer Department, Centro Escolar University, Manila, Philippines, Aug. 2016.

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume X Issue XI November 2025

7. B. Alb Is, Jr., et al., "A Study On The Effectivity Of The Philippine Prison System," PLJ, vol. 52, no. 1-03, June 2016.
8. Quezon City Ordinance No SP-2139, S-2012, Jan. 13, 2014. [Online]. Available: (Accessed Nov. 22, 2017).
9. Parker, "The Advancement of New Technology. Positive or Negative?" Apr. 12, 2015. [Online]. Available: (Accessed Aug. 31, 2017).
10. R. Fiddis, "Public Safety: The Impact of Technology," Aug. 8, 2016. [Online]. Available: (Accessed Aug. 31, 2017).
11. J. Byrne and G. Marx, "Technological Innovations in Crime Prevention and Policing," Nov. 2013. [Online]. Available: (Accessed Aug. 31, 2017).
12. ISO/IEC 25010:2011, "Systems and software engineering Systems and software Quality Requirements and Evaluation (SQuaRE) System and software quality models."
13. ISO/IEC 27001:2013, "Information technology Security techniques Information security management systems Requirements."
14. L. Breiman, "Random Forests," Machine Learning, vol. 45, no. 1, pp. 5–32, 2001.
15. T. Cover and P. Hart, "Nearest neighbor pattern classification," IEEE Transactions on Information Theory, vol. 13, no. 1, pp. 21–27, 1967.
16. H. Zhang, "The Optimality of Naive Bayes," Proceedings of the Seventeenth International Florida Artificial Intelligence Research Society Conference, 2004.
17. I. C. O. De Leon, R. A. Elandag, D. W. L. Enojo, J. G. Ferrer, and A. I. Lianza, "Developing Automated Security System for PhilHealth Quezon City," Capstone Project, Institute of Computer Studies, Colegio de Montalban, Rodriguez, Rizal, 2018.