ANDROID-BASED GUARD MONITORING AND SITE SURVEILLANCE SYSTEM

Mariel U. Ondos[1*], Domingo V. Origines Jr.[2]
Davao Del sur State College[1, 2]
*Correspondence Email : m_ondos@dssc.edu.ph1 , dvorigines@gmail.com2

ABSTRACT

The System is designed to enhance security operations and ensure accountability among security personnel by integrating mobile technology with real-time data collection, the system improves the efficiency, transparency, and reliability of monitoring activities across designated locations. Developed using the Agile Development Model, the system incorporates key features such as monitoring via QR codes and a timestamp camera that enables guards to take and submit pictures. The software also makes it easier for guards to report incidents, enabling them to document any anomalies they come across while on patrol. Evaluation of the system was conducted using the ISO 25010 Software Quality Framework, with fourteen (14) evaluators including administrators, advisory committee members, and IT experts. The results indicated strong performance: the QR code generation feature scored 4.7, while the user module for real-time incident capture and visited site reporting earned 4.8. Overall, the system achieved a 4.5 rating for functional suitability, 4.3 for both performance efficiency and compatibility, and 4.2 for usability and reliability. Aligned with Sustainable Development Goal (SDG) 9: Industry, Innovation, and Infrastructure, the system promotes innovation in security management and strengthens institutional infrastructure. Upon implementation at the Davao del Sur State College General Services Office (GSO), it is expected to significantly improve patrol compliance, incident documentation, and overall operational performance.

KEYWORDS Surveillance System, Security Guards, Security Operations, Guard Monitoring,

INTRODUCTION

Security is a critical aspect of any institution, as it ensures the safety of people, property, and valuable resources. For academic institutions like Davao del Sur State College, maintaining an effective security system is essential not only for protecting infrastructure but also for creating a safe learning and working environment. However, the efficiency and reliability of security operations often face challenges, particularly when they rely solely on manual patrol methods. In many cases, security guards are assigned to conduct routine patrols across different areas, yet these patrols are not always completed as intended. Some guards, especially those working alone, may remain in one area for extended periods, skip certain checkpoints, or avoid difficult-to-reach locations altogether. Such lapses can be caused by poor weather conditions, fatigue, or the physical difficulty of accessing certain areas, such as upper floors requiring multiple flights of stairs. These gaps in monitoring leave critical areas vulnerable and weaken the overall security framework of the institution.

The integration of technology into security operations offers a promising solution to these challenges. As Lee (2024) notes, adopting modern tools and digital platforms can greatly enhance the efficiency, accountability, and coordination of security personnel. Mobile applications, in particular, have emerged as a cost-effective and practical approach to streamlining security operations. Somavanshi et al. (2024) showcased the effectiveness of Android-based applications using QR code technology in restricted environments such as factories, warehouses, and educational institutions. Their system allowed authorized personnel to scan unique QR codes at designated checkpoints, automatically validating entries against a centralized database. This process not only confirmed that the correct personnel were present but also maintained a secure, tamper-proof digital record of all patrol activities.

Despite the existence of various guard monitoring systems in the market, common operational issues remain prevalent. Three critical challenges often observed in both traditional and modern setups are: **tampering**, where checkpoint verification is bypassed; **missing patrols**, where guards fail to follow their designated routes; and **lack of centralized control**, where monitoring data is fragmented and inaccessible for real-time decision-making. Addressing these issues requires a system that not only verifies guard presence but also ensures route completion, centralizes monitoring data, and produces actionable reports for administrators.

In response to these needs, this study developed an **Android-Based Guard Monitoring and Site Surveillance System** specifically tailored for the General Services Office of Davao del Sur State College. The system employed QR code technology ensured that all patrol checkpoints—especially those in remote, difficult-to-access, or less frequently visited areas—are monitored consistently. QR codes was strategically placed across campus facilities, and security guards used smartphones to scan each code during patrols. Each scan accompanied by a timestamped image capture, which served as visual proof of guard presence. Additionally, guards had the capability to record real-time incidents, enabling immediate documentation of security concerns or irregularities encountered during patrols.

The data collected was stored in a centralized database, accessible to administrators for oversight and evaluation. From this database, comprehensive reports can be generated, including the list of active general services personnel, daily patrol timestamps, captured images, incident logs by location, and records of visited or missed checkpoints. Such a system improved transparency, enforce patrol compliance, and discourage negligence

among security personnel. It was also allow administrators to make informed decisions regarding security measures, resource allocation, and personnel performance.

Moreover, the development of this system supports **Sustainable Development Goal (SDG) 9: Industry, Innovation, and Infrastructure**, which promotes the adoption of innovative technologies, the improvement of institutional infrastructure, and the creation of sustainable systems for public safety. By integrating mobile technology with a systematic guard monitoring process, the institution not only strengthens its security operations but also sets a foundation for technological advancement in campus management. Ultimately, the proposed Android-Based Guard Monitoring and Site Surveillance System aims to create a safer, more secure environment that protects lives, property, and resources while fostering trust and reliability in institutional security.

CONCEPT OF THE STUDY

The conceptual framework for the System illustrates the interaction between system users, core functionalities, and administrative processes. The framework begins with the **security guard**, who is required to register by creating an account and entering personal information. Once registered, the guard can access the system to update or remove personal data, scan QR codes at designated checkpoints, capture timestamped images, and report incidents in real time during patrols. These actions ensure accurate location verification and documentation of on-duty activities.

The **administrator** plays a supervisory and management role in the system. Administrators are responsible for generating unique QR codes for specific site areas, assigning and monitoring patrol routes, and tracking the real-time status of personnel. They maintain control over system operations by managing user accounts, validating reported incidents, and producing detailed reports on patrol activities, visited sites, and incident locations. The administrator's interface also provides tools for system oversight and performance evaluation, ensuring that operations remain transparent and well-documented.

The diagram presented in Figure 1 visually represents these processes, with the administrator's functions positioned on the right side and the guard's interactions on the left. The central features of the system—QR code scanning, timestamp-based monitoring, and real-time incident reporting—serve as the link between guards and administrators, ensuring seamless communication and data exchange. By streamlining these processes, the framework demonstrates how the system enhances accountability, improves patrol efficiency, and strengthens the overall security infrastructure of the institution.

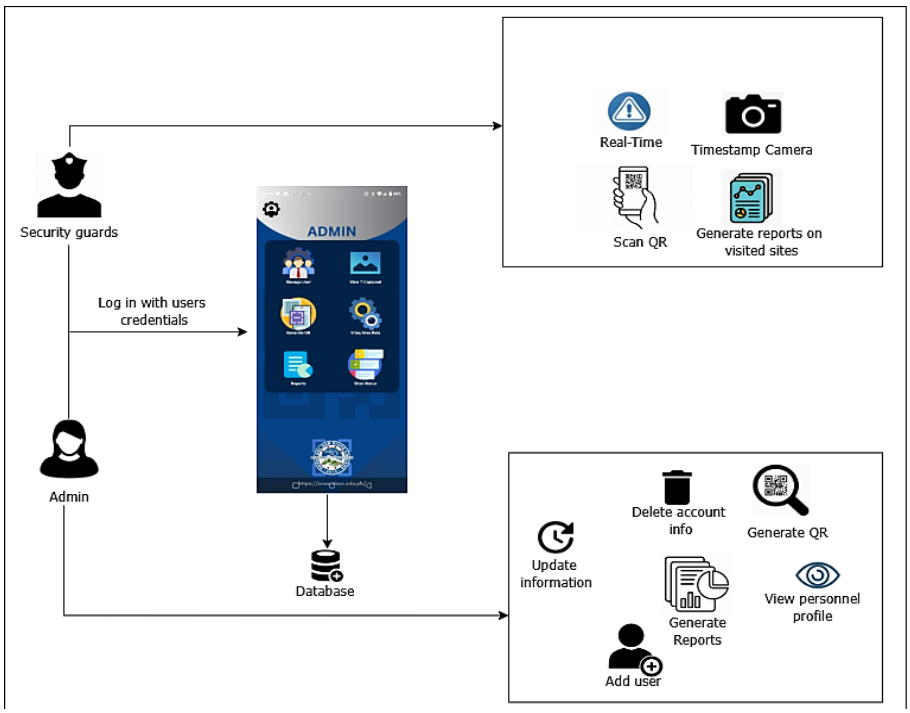

Figure 1. Conceptual Framework of the Study

RESEARCH METHOD

Research Design of the Study

This study adopted the Agile Development Methodology, a flexible and iterative approach to software development. Agile delivers the system in small, manageable units called *sprints*, allowing for continuous testing, feedback, and improvement. Unlike the traditional waterfall method, Agile prioritizes adaptability, active stakeholder involvement, and rapid response to changes—qualities essential for developing a security monitoring application that requires accuracy, efficiency, and user-centered design.

Phased Agile Workflow

The development process followed four key phases as shown in Figure 2 aligned with the Agile framework: **Planning**, **Development**, **Testing**, and **Deployment**.

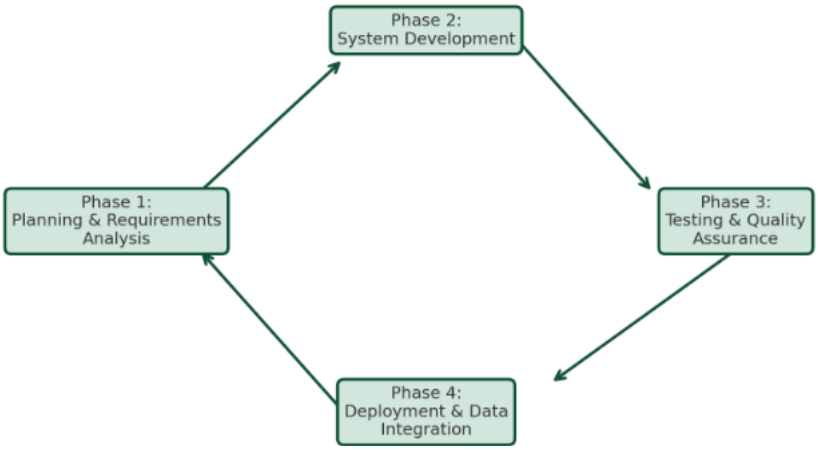

Figure 2. Agile Model Framework of the Study

Phase 1: Planning and Requirements Analysis

This phase focused on gathering, defining, and analyzing user requirements through consultations with **security guards** and the **General Services Office (GSO) head**. The goal was to determine operational needs, define the project scope, and identify technical specifications.

Key Activities:

1. Conducted interviews and requirement-gathering sessions with end-users.
2. Defined system features such as QR code checkpoint scanning, timestamp-enabled image capture, and real-time incident reporting.
3. Analyzed resource needs, including hardware and software specifications, to ensure smooth system operation.

For hardware requirements, a laptop serves as the primary development and administrative machine. It must operate on Windows 10 and have a processor speed of at least 1.8 GHz (with a quad-core or higher recommended for better performance). A minimum of 4 GB RAM is required, though 8 GB is preferable for faster processing during coding, testing, and deployment tasks. Storage should be an SSD with at least 800 MB free space, but 20–50 GB is recommended to accommodate application files, development tools, and backup data. An Android phone is also necessary for testing and actual use of the application. It should have a processor speed of at least 2 GHz, 32 GB ROM, 3 GB RAM, and run on Android OS 9 or higher to ensure compatibility with the developed features and smooth execution of the application.

For software requirements, the system relies on Windows 10 as the operating environment for development. Android Studio is the primary programming tool for building and debugging the application, offering the necessary libraries, SDKs, and emulator support for Android development. For backend services and data storage, Firebase is used as the Database Management System (DBMS), enabling real-time synchronization, secure authentication, and efficient storage of user data, incident reports, and images. Overall, these hardware and software specifications were chosen to guarantee the reliability, compatibility, and responsiveness of the system during both development and deployment, ensuring that the application performs well in real-world security monitoring operations.

Phase 2: System Development

Using the Agile model (Figure 2), the system was developed in iterative cycles. Each sprint involved coding, integrating features, and reviewing progress with stakeholders for feedback and improvements.

Key Development Components:

1. **QR Code Module:** Generates unique QR codes for designated site locations.
2. **Timestamp Camera Module:** Captures images with date and time as proof of guard presence.
3. **Incident Reporting Module:** Enables guards to document irregularities during patrols.
4. **Admin Dashboard:** Allows administrators to create QR codes, manage user accounts, monitor patrol activity, and generate reports.

Phase 3: Testing and Quality Assurance

This phase ensured that the application met the functional, performance, and compatibility requirements. Testing was conducted according to the **ISO 25010 Software Quality Framework**, with fourteen (14) evaluators including administrators, advisory committee members, and IT experts.

Phase 4: Deployment and Data Integration

After successful testing, the system was deployed for use by the Davao del Sur State College General Services Office. The deployment included setting up Firebase for data storage, configuring QR codes at patrol checkpoints, and registering system users.

Data Sources:

User Dataset (Figure 3): Includes unique IDs, roles, emails, names, birthdates, and gender, enabling role-based access control.

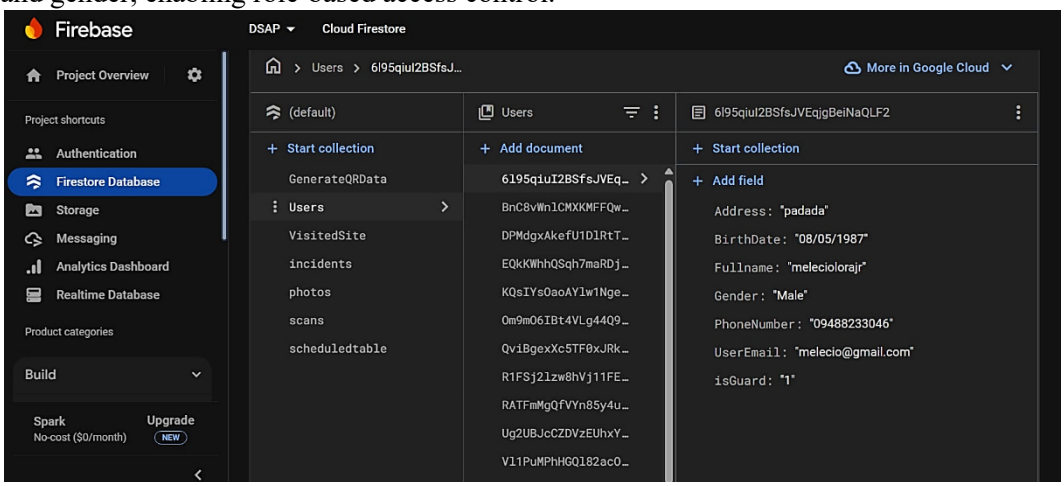

Figure 3. Dataset for users

Image Dataset (Figure 4): Stores timestamped photographs of guards at checkpoints, providing visual proof of patrol completion. Metadata such as file name, size, and creation date further enhances accountability.

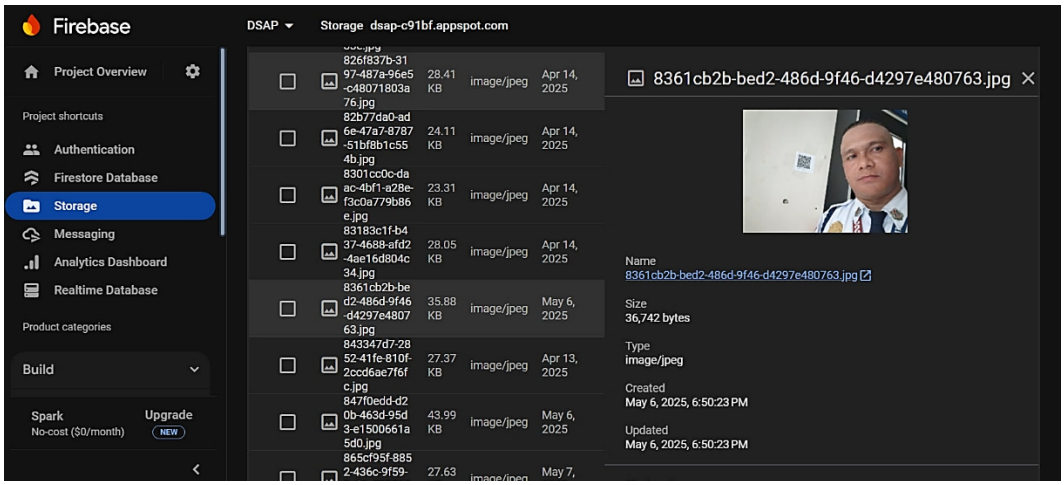

Figure 4. Datasets for images

Flowchart of the System

The flowchart, shown in Figure 5, provides a clear visual representation of the System's workflow. By using standard symbols such as ovals, diamonds, and arrows, it illustrates the sequential flow of actions, inputs, and outputs within the system. This visual approach simplifies the understanding of the system's operations for both technical and non-technical stakeholders, enabling easier analysis, better communication, and more effective collaboration. It also serves as a reference for future development, ensuring that the system can be maintained, enhanced, and scaled with minimal difficulty.

The process begins with both **administrators** and **guards** logging in to access their respective dashboards. From the guard's side, the system prompts them to scan a location-specific QR code, which verifies their presence at a designated site. After scanning, they are directed to a timestamp-enabled camera to capture an image, which can be saved or submitted immediately. In case of an incident, guards can file a **real-time report** by entering the incident location and details, capturing supporting images, and submitting them through the application.

On the administrator's side, successful login grants access to various management functions. Administrators can **add, edit, or remove user accounts**, generate new QR codes for monitoring points, and oversee security staff activity. They can also generate comprehensive reports that include user lists, timestamps by location, daily image captures, and incident records. These reports enhance oversight and provide a reliable basis for evaluating security operations. Additionally, administrators can view detailed personnel profiles to monitor performance and ensure accountability.

Overall, the flowchart encapsulates the system's core processes, from authentication to data management, demonstrating how the application streamlines guard monitoring and site surveillance through structured, real-time operations.

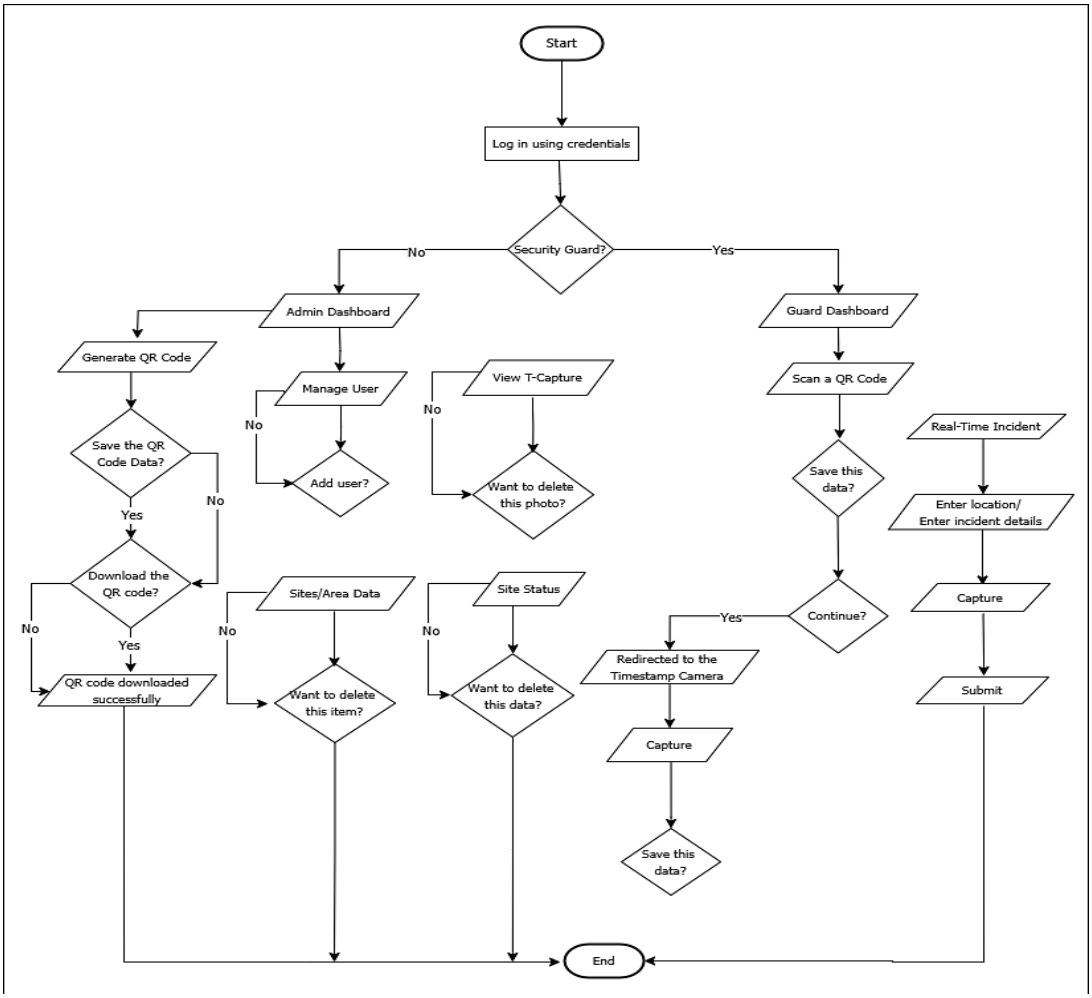

Figure 5. Flowchart of the System

Likert Scale of Measurement for Functional Suitability, Performance Efficiency, Reliability, Usability, and Compatibility

To assess the overall quality and effectiveness of the proposed system, this study employed a five-point Likert scale to gather respondents' perceptions and feedback. The Likert scale provided a structured way of quantifying qualitative opinions by offering five response options per question, with ratings ranging from 1 (lowest) to 5 (highest). This method allowed for consistent evaluation across multiple quality attributes, specifically functional suitability, performance efficiency, reliability, usability, and compatibility.

The evaluation framework was guided by the work of Ariyani et al. (2021) and Hasanah et al. (2020), who applied the **ISO 25010 Software Product Quality Standards** to measure software reliability and effectiveness. This internationally recognized standard ensured that the assessment criteria were comprehensive and aligned with best practices in software evaluation.

Table 5. Likert Scale of Measurement for functional suitability, performance efficiency, reliability, usability and compatibility.

Mean Range	Descriptive Equivalent	Verbal Interpretation
4.51—5.00	Strongly Agree	This measure indicates, participants are completely certain that the goals have been met and that every facet of the system's functional suitability, performance efficiency, dependability, usability, and compatibility has been successfully handled without any issues.
3.51-4.50	Agree	This measure indicates that respondents acknowledge the results, even though the functional suitability, performance efficiency, reliability, usability and compatibility have not been entirely achieved and minor issues such as bugs, malfunctions, or unexpected outcomes may exist.
2.51-3.50	Fairly Agree	This measure indicates that participants recognize the outcomes and assume that the functional suitability, performance efficiency, reliability, usability and compatibility objectives have been partially achieved. However, certain features may not be completely satisfactory for the respondents.
1.51-2.50	Disagree	This metric shows that the majority of participants believed the results fell short of their expectations.
1.00-1.50	Strongly Disagree	This metric shows that participants lacked confidence in the system's capacity to achieve the goals.

This measurement approach was instrumental in identifying which aspects of the system successfully met user expectations and which required further improvement. It also facilitated a simplified yet precise analysis of responses, enabling the researchers to draw clear and evidence-based conclusions about the system's quality and user satisfaction. By applying a standardized scale and interpretation, the study ensured objectivity, comparability of results, and a well-structured basis for system refinement.

RESULT AND DISCUSSION

Graphical User Interface of the System

The Graphical User Interface (GUI) of the System is designed with a strong emphasis on usability, clarity, and efficiency. It incorporates intuitive graphical elements such as icons, buttons, dropdown menus, and interactive features, ensuring that both administrators and guards can navigate the system with ease. The design prioritizes a clean layout, consistent color schemes, and clear labeling, making the system accessible even to users with minimal technical expertise. Figures 12 and 13 present the dashboards for

administrators and guards, respectively, each tailored to their specific roles and responsibilities within the security workflow.

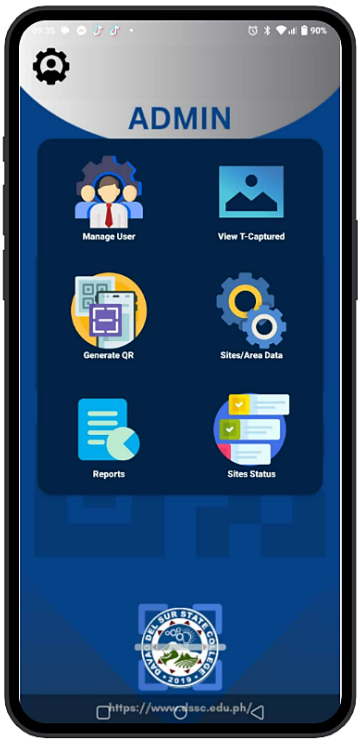

Figure 6. Dashboard for Admin

For **administrators** (Figure 6), the dashboard serves as the central control hub for the entire system. It provides quick access to essential functions such as managing user accounts (add, delete, update, and view), viewing timestamped captured images from guard patrols, creating QR codes for specific sites or areas, generating detailed activity reports, and managing stored site or area data. The interface uses a gradient blue background, visually enhancing the workspace while maintaining a professional aesthetic. Icons are accompanied by clear text labels, ensuring straightforward navigation and reducing the likelihood of errors.

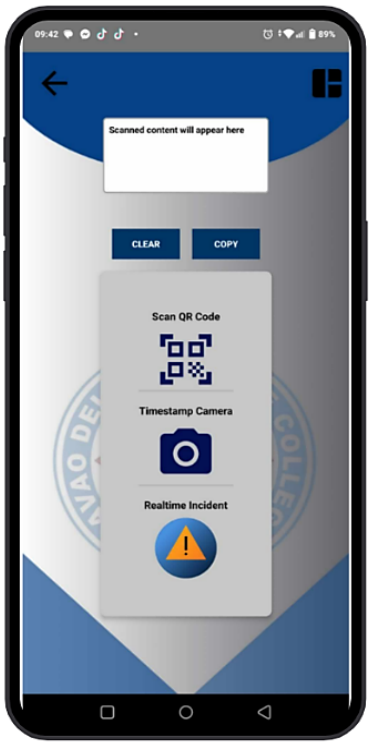

Figure 7. Dashboard for Users

For **guards** (Figure 7), the dashboard is streamlined to focus on operational tasks. It features essential tools such as the QR code scanner for verifying patrol locations, a timestamp-enabled camera for documenting site visits, and a real-time incident reporting function that allows guards to capture images, record incident details, and submit the location instantly. Navigation tools such as the back arrow and quick actions like "CLEAR" and "COPY" are also available for convenience. The guard interface follows a blue-and-white color scheme with organized grid layouts, presenting a neat and uncluttered appearance suitable for field use.

Overall, the GUI is not only functional but also user-centered, providing each type of user with the specific tools they need to perform their duties efficiently. The combination of clear visual elements, organized layouts, and role-based dashboards ensures smooth interaction, faster task completion, and improved accuracy in data recording and reporting.

Admin Module for Managing Users (Add, Delete, and Update Information)

The **Admin Module** serves as the central control hub for managing user accounts, particularly those of the security guard personnel under general services. Through the admin panel—illustrated in Figure 16—administrators are granted the capability to add, delete, and update user information efficiently. This feature ensures that records remain accurate, up-to-date, and reflective of the current security staff roster.

In addition to basic account management, the admin panel provides real-time oversight of security operations. Administrators can monitor which guards are currently on duty or actively patrolling specific locations. The **"View T-Captured"** feature further enhances monitoring by displaying timestamped photographs captured during patrols, enabling verification of personnel activity and compliance.

Figure 8. GUI for Admin Module that Manage User

As shown in Figure 8, the admin dashboard is equipped with multiple core functions:

1. **Manage User Accounts** – Add, delete, update, and view security guard information.
2. **View T-Captured** – Access and review timestamped photos or data collected during patrols.
3. **Generate QR Codes** – Create QR codes assigned to specific sites or rooms for patrol verification.
4. **Manage Site/Area Data** – Organize and update information about monitored sites or locations.
5. **Reports** – Access and generate detailed reports on guard activities, patrol logs, and incidents.
6. **Site Status** – View real-time status updates of various monitored locations.

This centralized interface streamlines administrative tasks, improves data organization, and enhances operational oversight. By providing quick access to essential tools, the Admin Module helps ensure accountability, efficient deployment of personnel, and informed decision-making in security operations.

Viewing Account Information for General Services Personnel Profile

The **"View Account Information"** feature allows authorized users—such as managers and administrators—to quickly and securely access critical details about each general services personnel stored in the system. This includes the employee's full name, contact information, role or position, work location, and other relevant data. By consolidating this information into one centralized platform, administrators can efficiently review staff assignments, verify employee records, and ensure that all data remains accurate

and up-to-date. This functionality not only streamlines personnel management but also reduces administrative errors, saves time, and enhances overall operational efficiency.

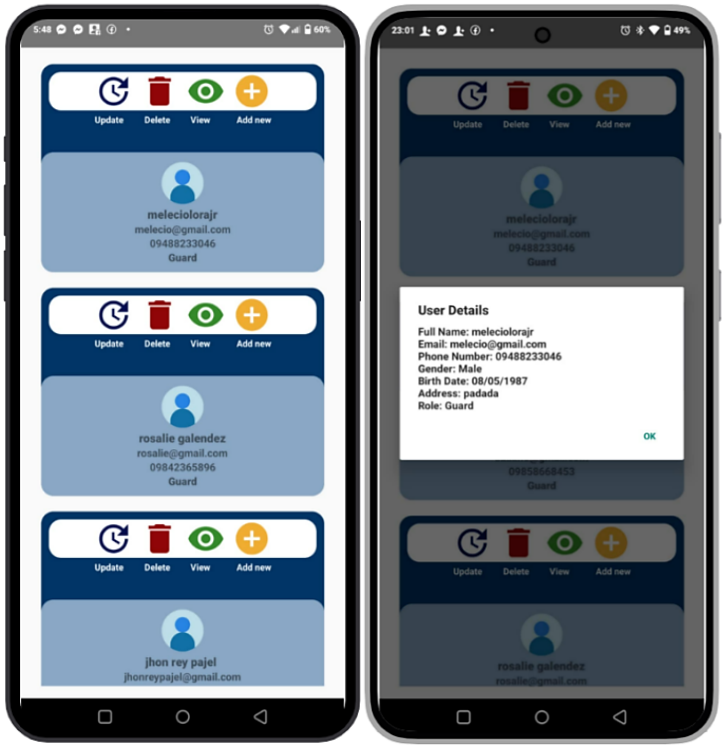

Figure 9. GUI for Viewing Account Info for Personnel Profile

As shown in Figure 9, the system provides a clear and well-structured display of personnel information. On **Screen 1**, administrators can view comprehensive details for each staff member, including full name, phone number, email address, gender, role, job status, and other relevant profile data. **Screen 2** offers a more concise, organized layout for quick reference, allowing easy verification of user roles and employment status.

This feature is particularly valuable in environments such as security operations, where maintaining accurate personnel documentation is essential. By enabling quick access to complete staff profiles, the system supports effective monitoring, better decision-making, and stronger accountability in managing the general services workforce.

Generate QR Code for Site Names by Offices and Rooms

The **Generate QR Code** feature assigns each office or room a unique digital identifier, allowing for quick and efficient access to location-specific information. By scanning the generated QR code using a mobile device, users can instantly retrieve details such as the equipment present in the area, assigned personnel, and the room's designated

function. This capability enhances site management by reducing the need for manual record searches, improving security, streamlining navigation, and ensuring accurate documentation.

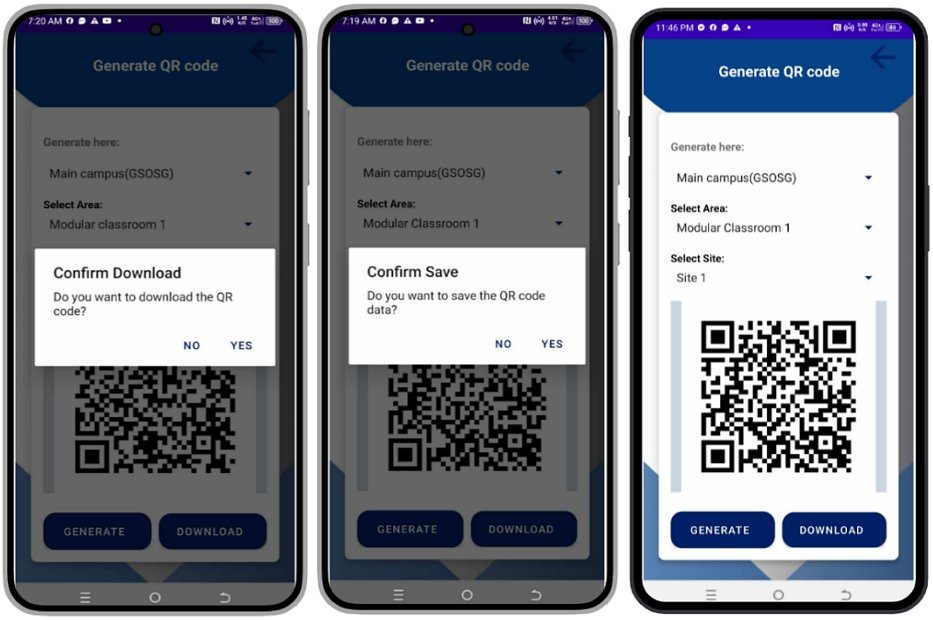

Figure 10. Graphical User Interface (GUI) for Generating QR Codes

As shown in Figure 10, the interface enables administrators to generate QR codes for specific sites or areas. From a dropdown menu, the administrator can select the designated region, such as **Utility (GSOPA)**, **Ground Maintenance (GSOP)**, **Facilities (GSOPA)**, or **Main Campus (GSOSG)**. After selecting the region, the specific office or room name is entered. Once the information is provided, clicking the **"Generate QR"** button automatically creates a unique QR code for that location.

The system also allows the generated QR code to be downloaded instantly, with the image automatically saved to the gallery for future reference. This streamlined process ensures that every room and office has a readily accessible, scannable code, supporting efficient tracking, monitoring, and management of facilities.

Timestamp for Location Report

This feature plays a critical role in monitoring field operations by recording the exact time and location of activities. It ensures accurate documentation, supports transparency in service delivery, and provides verifiable records for operational audits. Furthermore, it helps identify patterns in photo captures, determine peak activity periods, and detect areas that may be under-monitored, enabling administrators to address gaps in coverage effectively.

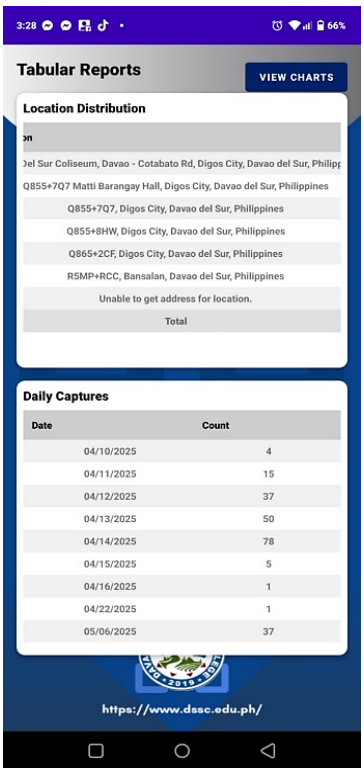

Figure 11. GUI for Timestamp for Location Report

Figure 11 displays two key data tables: **Daily Captures** and **Location Distribution**. The Location Distribution table lists various recorded locations, including multiple addresses in Digos City, Davao del Sur, Philippines, along with one entry where the address could not be retrieved. The Daily Captures table presents the number of captures logged each day, spanning from April 10, 2025, to April 16, 2025, along with corresponding tallies. This structured reporting format enables quick analysis of operational coverage, activity frequency, and geographic distribution of captured data.

Incident by Location Report

The *Incident by Location Report* feature serves as a central tool for systematically documenting, organizing, and presenting incident data according to the specific location of each occurrence. This function plays a critical role in helping organizations maintain a safe, secure, and well-managed environment by enabling quick identification of high-risk areas, facilitating targeted preventive measures, and supporting strategic resource allocation for incident response.

By integrating with the system's **QR Code Generation** and **Timestamp for Location** modules, each incident record can be linked to a unique site identifier and an exact date-time capture. This ensures that every reported event is verifiable, location-specific, and traceable, reducing the risk of data loss or misreporting. For example, QR codes assigned to offices or rooms make it possible for personnel to quickly log incidents using their mobile devices, while timestamped entries confirm when and where the events occurred.

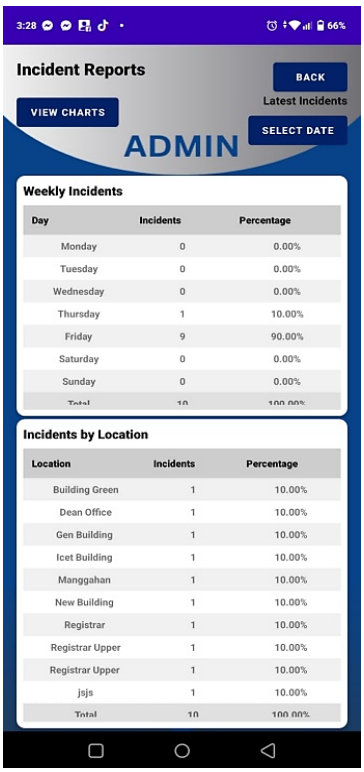

Figure 12. Incident by Location Report

Figure 12 showcases the *Incident Reports* interface, which visually presents both weekly incident statistics and their corresponding locations. The design includes **BACK** and **VIEW CHARTS** buttons for easy navigation, with the title *Incident Reports* positioned at the top left. A **SELECT DATE** button highlights the *Latest Incidents* section, allowing users to filter and focus on specific reporting periods. The interface is divided into two primary tables: **Weekly Incidents** and **Incidents by Location**. The *Weekly Incidents* table provides a detailed breakdown of occurrences for each day of the week, showing both the total number of incidents and their percentage distribution. The *Incidents by Location* table lists the exact places where these events occurred, offering a location-based perspective that is crucial for pattern recognition and decision-making. Through this integrated reporting approach, administrators can not only see the "what" and "when" of incidents but also the "where" with precise, verifiable data. This enhances transparency, improves accountability, and allows management to focus preventive actions on the areas that need them most.

QR Code Integration for Site Management

The QR Code feature set within the system provides a complete workflow for location identification, tracking, and reporting. This process begins with the **Generate QR Code** module, where administrators assign a unique digital identifier to each site—whether it is an office, room, or designated operational area. These codes store vital site details such as location name, purpose, and assigned personnel. By generating and distributing these codes, the system ensures that every site can be quickly identified and monitored without relying on manual recordkeeping.

Once QR codes are deployed on-site, the **Scan QR Code by Site Location** module enables personnel to verify and retrieve site details in real-time. Using a mobile device, users simply scan the administrator-issued QR code to instantly display key information such as the site name, identification number, date, time, and operational status. This step ensures that all site interactions—whether inspections, maintenance, or incident

responses—are tied to an authenticated location record, minimizing errors and ensuring data accuracy.

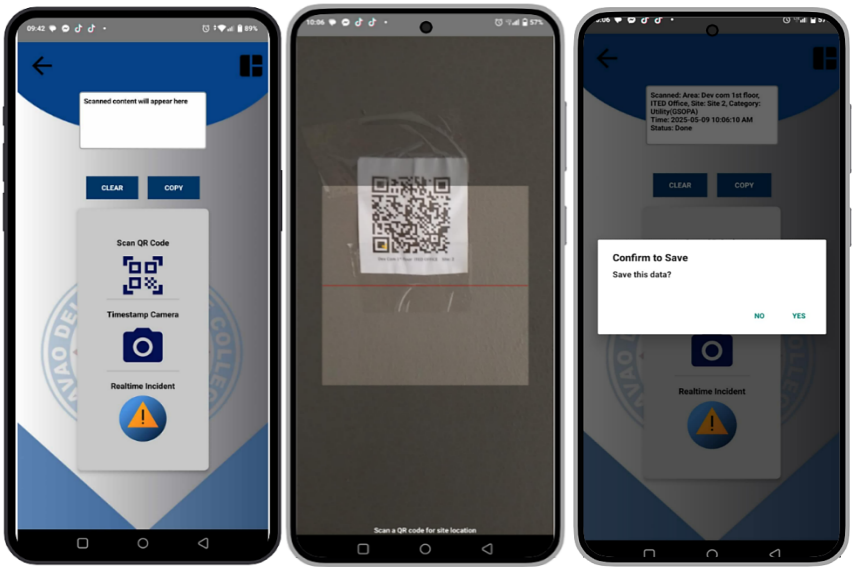

Figure 13. GUI for Scan a QR Code for site location

Finally, location-specific activities and occurrences are recorded and organized through the **Incident by Location Report** module. Incidents captured from the field are automatically linked to their corresponding QR-verified location. This allows administrators to view, sort, and analyze data based on exact site coordinates and usage history. Weekly incident summaries and detailed breakdowns by location help management identify high-risk areas, allocate resources more effectively, and maintain a safe, well-managed environment. By integrating QR code generation, scanning, and location-based reporting, the system creates a seamless loop of **site identification → verification → performance and incident monitoring**, significantly enhancing operational efficiency, security, and data reliability.

Capture with Timestamp Camera Module

The **Capture with Timestamp Camera Module** allows users to accurately document incidents, site visits, or field activities by taking photos with the application's built-in camera. Each captured image is automatically embedded with the exact date, time, and location, ensuring that all records are both verifiable and time-specific. This feature is particularly valuable for operational monitoring, incident reporting, and maintaining reliable proof of presence at designated sites. **Figure 14** illustrates the module's user interface, which is divided into three key screens.

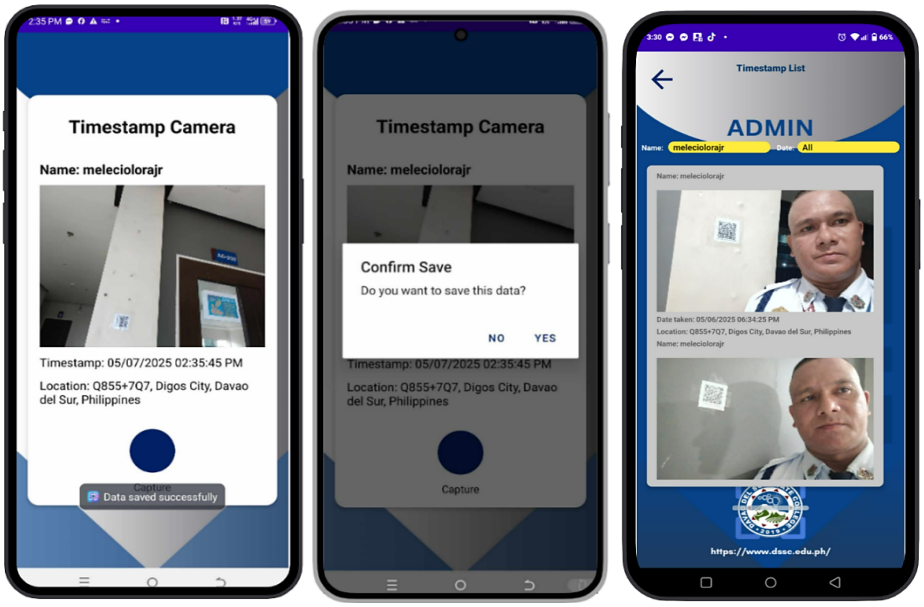

Figure 14. GUI for Timestamp Camera Module

- **Screen 1** displays a confirmation prompt asking the user whether to save the recently captured image, with **YES** and **NO** options. The lower section shows the embedded location (0855-F07, Digos City, Davao del Sur, Philippines) and timestamp (05/07/25 02:25 PM).
- **Screen 2** presents the camera interface, including the user's name (melecio loro jr.), a preview of the captured image, and the automatically generated timestamp (05/07/25 02:35:45 PM) along with the location details.
- **Screen 3** shows the **ADMIN** view, which lists all timestamped photos submitted by security personnel. This log provides visual proof of their presence and activities at specific sites, with each entry linked to a verified date, time, and location. The **Davao del Sur State College** logo appears at the bottom of the interface for official branding.

By integrating timestamped geolocation data directly into photos, this module ensures accuracy, accountability, and transparency in field operations.

Capture with Real-Time Incident by Location Module

The **Capture with Real-Time Incident by Location Module** is designed to streamline the process of recording and tracking incidents as they happen, with precise geolocation tagging. This feature allows users to log incidents instantly, capturing essential details such as the type of incident, its severity, exact time of occurrence, description, and any supporting images. By providing comprehensive and timely information—including incident category, severity level, date and time, summary, and optional photo evidence—the module ensures accurate documentation and reliable recordkeeping. This real-time capability significantly enhances situational awareness, enabling decision-makers to respond promptly and effectively. In emergency or time-sensitive scenarios, it supports faster command chain reactions, minimizes communication delays, and reduces errors common in manual reporting.

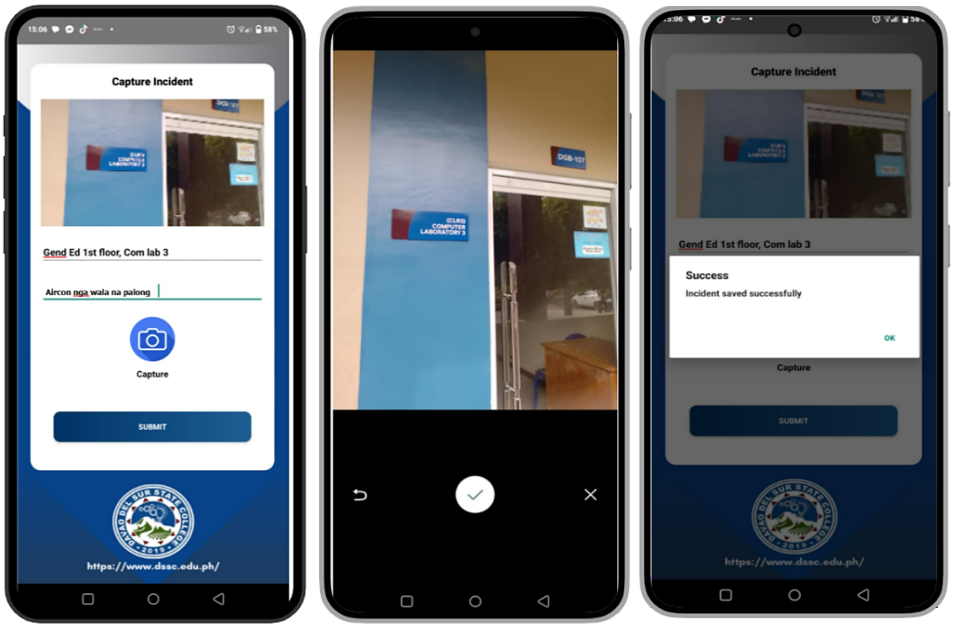

Figure 15.GUI for Capture Incident Report

Figure 15 shows the **Capture Incident Report** interface, where users can complete a structured incident report form by entering the location and relevant details. Once submitted, the system logs the incident, ensuring it is properly documented and traceable. This function not only promotes operational efficiency but also strengthens accountability and safety by allowing immediate, on-site reporting of critical events.

Generating a Report on Visited Sites

This feature allows users to automatically generate detailed reports of all sites visited within a specified time frame. Each report contains key information such as the site names, along with the exact dates and times of each visit. Maintaining these records makes it easier to verify attendance, review past activities, and ensure that users followed their assigned schedules. This functionality is particularly valuable for monitoring guard patrols, tracking employee field tasks, and ensuring operational compliance. By automating report generation, the system improves accuracy, reduces manual workload, and saves time in compiling visit data.

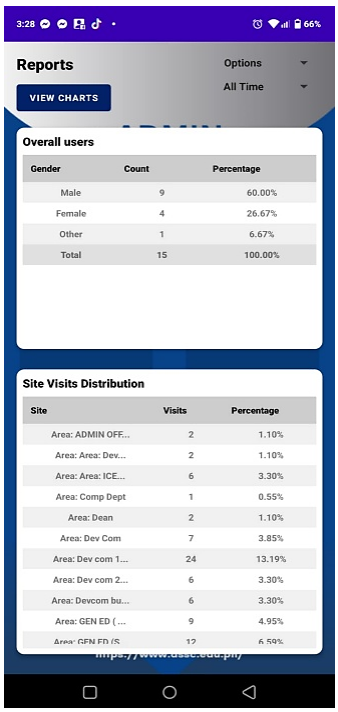

Figure 16. GUI for Generate report on visited sites

Figure 16 presents the **Site Visits Distribution** table, which lists the number and percentage of visits for each location. The table has three columns: *Site*, *Visits*, and *Percentage*. For instance, "Area: Dev com 1" has the highest number of visits—24 visits, or 13.41% of the total—while "Area: Comp Dept" has the fewest, with only one visit (0.56%). Other areas recorded between two and seven visits, indicating relatively low frequency. This data allows administrators to easily identify frequently checked locations versus those with minimal visits, helping determine if certain areas require increased monitoring. Ultimately, this supports improved safety, better resource allocation, and more effective workflow management.

Evaluation Results from the Evaluators based on ISO 25010 Software Quality Framework

The results summarized in **Table 2** reveal a broadly positive evaluation of the System across key quality dimensions defined under the ISO 25010 standard. Each quality attribute—**functional suitability**, **performance efficiency**, **usability**, **reliability**, and **compatibility**—received a mean rating within the "Agree" range, indicating strong user confidence in the system's overall performance.

Table 2. Summary of Respondents Rating based on ISO 25010 Software Quality Framework April, 2025

Quality Characteristics	Mean	Verbal Interpretation
Functional suitability	4.5	Agree
Performance efficiency	4.3	Agree
Usability	4.2	Agree
Reliability	4.2	Agree
Compatibility	4.32	Agree
Consolidated Mean	**4.37**	**Agree**

According to ISO 25010, **functional suitability** reflects the degree to which a system provides functions meeting stated and implied needs under specified conditions ISO 25010 Model. The highest score of **4.50** suggests that users strongly perceive the system to perform its intended tasks—such as accurately managing personnel accounts, generating QR codes for location-based monitoring, and producing detailed site visit reports—with efficiency and correctness.

Performance efficiency, which concerns the system's responsiveness and resource utilization under given conditions ISO 25010 Quality Model, received a mean of **4.30**. This indicates that common operations—such as QR scanning, timestamped captures, and report compilation—execute within acceptable performance thresholds. Such responsiveness is critical for field environments where delays can hinder operational effectiveness.

The **compatibility** dimension earned **4.32**, revealing that users find the system integrates well with existing hardware and workflows. ISO 25010 defines compatibility as a system's ability to function within shared environments without interference ISO 25010 Model. This supports smoother deployment and adoption across diverse operational settings.

Usability and **reliability**, each scoring **4.20**, were the lowest-rated dimensions. ISO 25010 describes usability as the extent to which a product is effective, efficient, and satisfying for specified users ISO 25010 Model, while reliability denotes its ability to perform consistently under required conditions ISO 25010 Model. These results suggest that, although the system is generally user-friendly and dependable, there remains room for improvement—especially in interface design, navigation flow, and stability in varied usage scenarios.

With a **consolidated mean of 4.37**, the system achieves a solid affirmation in software quality under ISO 25010 evaluation. This overall "Agree" rating confirms that the system aligns well with user expectations in terms of operational functionality, efficiency, and integration. The results also highlight specific development areas—namely usability and reliability—where targeted refinements could further enhance user satisfaction and system robustness.

In conclusion, the evaluation demonstrates the system's readiness for real-world deployment, while also offering actionable insights to guide future enhancements. By focusing on interface optimization and reinforcing operational reliability, subsequent versions can achieve even higher levels of user satisfaction and long-term stability.

CONCLUSION

The System meets its objectives as a reliable, efficient, and user-friendly platform for managing personnel and operational surveillance data. Both the admin and user modules performed effectively, with core account management features scoring between **4.4 and 4.6**, and key operational functions—such as **QR code generation (4.77)** and **QR code scanning (4.67)**—earning the highest user approval. Additional features, including timestamped image capture, location tagging, and incident reporting, also received favorable ratings of **4.0 to 4.3**, demonstrating their value in enhancing security monitoring and decision-making. These results validate the system's readiness for real-world deployment, offering a dependable tool that streamlines workflows, ensures accurate reporting, and supports timely, data-driven security operations. Lastly , It is recommended to improve the system's usability through better interface design and navigation, enhance reliability with optimization and stress testing, and upgrade image capture and reporting with higher resolution, offline use, and automated formatting. Expanding compatibility

with other security tools, providing regular personnel training, and implementing continuous feedback with scheduled updates will ensure consistent performance and adaptability to evolving needs.

REFERENCES

Alhudhud, G., Alsaeed, D. H., Al-Baity, H., Al-Humaimeedy, A. S., & Al-Turaiki, I. (2019). iGuard: Mobile security guard system with infrared biosensor and google glass. *Bioscience Biotechnology Research Communications 12*(2), 333-547. https://doi.org/10.21786/BBRC/12.2/16

Ahamed, M. S., & Mustafa, H. A. (2019). A secure QR code system for sharing personal confidential information. In *2019 International Conference on Computer, Communication, Chemical, Materials and Electronic Engineering (IC4ME2)* (pp. 1-4). IEEE. https://doi.org/10.1109/IC4ME247184.2019.9036521

Ariyani, S., Sudarma, M., & Wicaksana, P. A. (2021). Analysis of functional suitability and usability in sales order procedure to determine management information system quality. *INTENSIF Jurnal Ilmiah Penelitian Dan Penerapan Teknologi Sistem Informasi, 5*(2), 234–248. https://doi.org/10.29407/intensif.v5i2.15537

Bao, S., Lin, J. H., Howard, N., & Lee, W. (2023). Development of Janitors' workload calculator. In *Proceedings of the human factors and ergonomics society annual meeting* (Vol. 67, No. 1, pp. 1043-1048). SAGE Publications. https://doi.org/10.1177/21695067231192623

Darie, T., R Aprodu, C. (2024). Aspecte particulare ale politicii de personal în servicii [Particular aspects of staff policy in the services]. *Lucrări ştiinţifice ale Simpozionului Ştiinţific al Tinerilor Cercetători 1*, 174-177. https://doi.org/10.53486/sstc.v1

Fang, C., Song, S., & Mei, Y. (2022). On repairing timestamps for regular interval time series. *Proceedings of the VLDB Endowment 15*(9), 1848-1860. https://doi.org/10.14778/3538598.3538607

Gannapathy, V. R., Narayanamurthy, V., Subramaniam, S. K., Ibrahim, A. F. B. T., Isa, I. S. M., & Rajkumar, S. (2023). A mobile and web-based security guard patrolling, monitoring and reporting system to maintain safe and secure environment at premises. *International Journal of Interactive Mobile Technologies, 17*(11). https://doi.org/10.3991/ijim.v17i11.35483

Goel, N., Sharma, A., & Goswami, S. (2017). A way to secure a QR code: SQR. In *2017 International Conference on Computing, Communication and Automation (ICCCA)* (pp. 494-497). IEEE. https://doi.org/10.1109/CCAA.2017.8229850

Gokasar, I., & Karaman, O. (2023). Integration of personnel services with public transportation modes: A case study of Bogazici University. *Journal of Soft Computing and Decision Analytics, 1*(1), 1-17. https://doi.org/10.31181/jscda1120231

Hasanah, N.A., Atikah, L., & Rochimah, S. (2020). Functional Suitability Measurement Based on ISO/IEC 25010 for e-Commerce Website. In *2020 7th International Conference on Information Technology, Computer, and Electrical Engineering (ICITACEE)* (pp 70-75). IEEE. https://doi.org/10.1109/icitacee50144.2020.9239194

Imanullah, M., & Reswan, Y. (2022). Randomized QR-code scanning for a low-cost secured attendance system. *International Journal of Electrical and Computer Engineering, 12*(4), 3762-3769. https://doi.org/10.26623/transformatika.v17i1.1471

Jung, J. Yoo, S. La, W. G. Lee, D. R., Bae, M. & Kim, H. (2018). Airborne video surveillance system. *Sensors, 18*(6), 1939. https://doi.org/10.3390/s18061939

Kempecova, D., & Kozlovska, M. (2023). Sensing technologies for construction productivity monitoring. *MATEC Web of Conferences 385,* Article 01032. https://doi.org/10.1051/matecconf/202338501032

Kim, J., Ham, Y., Chung, Y., & Chi, S. (2019). Systematic camera placement framework for operation-level visual monitoring on construction jobsites. *Journal of Construction Engineering and Management, 145*(4), 04019019. https://doi.org/10.1061/(ASCE)CO.1943-7862.000163

Lee, J. L. (2024). *Security guard monitoring system* [Doctoral dissertation, university tuknu abdul rahman]. UTAR Institutional Respiratory. http://eprints.utar.edu.my/id/eprint/6650

Llaguno-Munitxa, M. (2023). Site-surveying: Architecture and it's local ecology. *Lieuxdits,* (23), 14-21. https://doi.org/10.14428/ld.vi23.76823

Mulyawan, M. D., Swamardika, I. B. A., & Saputra, K. O. (2021). Analisis Kesesuaian Fungsional Dan Usability Pada Sistem Informasi Karma Simanis Berdasarkan Iso/Iec 25010 [Analysis of functional suitability and usability in the karma simanis information system based on]. *JURTEKSI (Jurnal Teknologi dan Sistem Informasi), 7*(3), 293-302. https://doi.org/10.33330/JURTEKSI.V%VI%I.1139

Ni, J., Zhu, W., Huang, J., Niu, L., & Wang, L. (2019). Fall guard: Fall monitoring application for the elderly based on android platform. In *ACM international conference proceeding series* (pp. 128–135). Association for Computing Machinery. https://doi.org/10.1145/3354031.3354055

Nuakoh, E. B., & Coffie, I. (2018). MonitR: A mobile application for monitoring online accounts' security. In *SoutheastCon 2018* (pp. 1-9). IEEE https://doi.org/10.1109/SECON.2018.8478857

Paudel, N., & Neupane, R. C. (2019). A general architecture for a real-time monitoring system based on the internet of things. In *Proceedings of the 2019 3rd international symposium on computer science and intelligent control* (pp. 1-12). https://doi.org/10.1145/3386164.3387295

Poornima, E. Kumar, R. P. R. Katukam, S. Pericherla, V. V. & Birelli, S. K. (2023). A real-time IoT-based model to detect and alert security guards' drowsiness. *E3S Web of Conferences, 391,* Article 01151. https://doi.org/10.1051/e3sconf/202339101151

Putra, I. G. E. P., Jati, A. N., & Saputra, R. E. (2017). Monitor and control panel of building security system integrated to Android smart phone. In *2017 International Conference on Robotics, Biomimetics, and Intelligent Computational Systems (Robionetics)* (pp. 29-33). IEEE https://doi.org/10.1109/ROBIONETICS.2017.8203432

Rao, A. S., Radanovic, M., Liu, Y., Hu, S., Fang, Y., Khoshelham, K., Palaniswami, M., & Ngo, T. (2022). Real-time monitoring of construction sites: Sensors, methods, and applications. *Automation in Construction, 136,* 104099. https://doi.org/10.1016/j.autcon.2021.104099

Salem, T., Hwang, J., & Padilha, R. (2022*). Timestamp estimation from outdoor scenes*. Embry-Riddle Aeronautical University. https://commons.erau.edu/adfsl

Saidkhodjaev, T., Voas, J.M., Kuhn, R., Defranco, J., & Laplante, P.A. (2020). Aggregating Atomic Clocks for Time-Stamping. In *2020 IEEE International Conference on Service Oriented Systems Engineering (SOSE),* 1-6. https://doi.org/10.1109/SOSE49046.2020.00008

Somavanshi, S. R., Bhand, S. J., Lende, S. D., & Pansare, P. Android Application for: Secure employee track vision. *International Journal of Advanced Research in Science, Communication and Technology, 4*(2). https://doi.org/10.48175/ijarsct-22181

Sapundzhi, F., & Mladenov, M. (2022). An android-based mobile application giving information for weather in real-time [Special issue]. *Bulgarian Chemical Communications, 54,* (B1), 89-91. https://doi.org/10.34049%2Fbcc.54.B1.0455

Setiawan, A. (2019). Evaluasi kinerja karyawan level pelaksana satuan pengamanan pada perguruan tinggi menggunakan metode simple addictive weighting [The method used for performance evaluation the security unit is simple additive weighting*]. Jurnal Transformatika, 17*(1), 26-33. https://doi.org/10.26623/TRANSFORMATIKA.V17I1.1471

Sykes, E. R. (2020). A context-aware system using mobile applications and beacons for on-premise security environments. *Journal of Ambient Intelligence and Humanized Computing, 11*(11), 5487–5511. https://doi.org/10.1007/s12652-020-01906-2

Stone, K., & Horney, J. A. (2018). Methods: Surveillance. In *Disaster epidemiology* (pp. 11-23). Academic Press. https://doi.org/10.1016/B978-0-12-809318-4.00002-2

Triantafyllou, D., & Krinidis, S. (2018). A real-time, multi-space incident detection. *Safety and Security Studies, 8*(2), 266-275. https://doi.org/10.2495/SAFE-V8-N2-266-275

Villaseñor-Ramírez, M.A., Carrillo-Hernández, D., Blanco-Miranda, A.D., & García-Cervantes, H. (2024). Implementation of mobile monitoring technology for industrial safety. *Journal-Economic Development Technological Chance and Growth. 8*(14), 1-18. https://doi.org/10.35429/jedt.2024.8.14.4.8

Wu, Q., Han, Z., Mohiuddin, G., & Ren, Y. (2023). Distributed timestamp mechanism based on verifiable delay functions. *Computer Systems Science & Engineering, 44(*2). https://doi.org/10.32604/csse.2023.030646

Yusuf, I., & Leidiyana, H. (2021). Android based employee attendance app using QR code Scanning and location-based service. *Journal of Informatic and Information Security, 2*(1), 35-44. https://doi.org/10.31599/jiforty.v2i1.569