SmartGate ACC: A Proposed QR-Based Attendance and Entry Management Framework for PSU - ACC

Leizel R. Tresenio[1], Jurlyn Jeanne V. Fruto[2], Carl Anthony N. Supetran[3], Marino B. Bartolome Jr.[4]

Department of Information Technology, Pangasinan State University-Alaminos City Campus

DOI: https://doi.org/10.47772/IJRISS.2026.100700280

Received: 12 July 2026; Accepted: 17 July 2026; Published: 30 July 2026

ABSTRACT

Institutional management is undergoing an extensive digital shift driven by Industry 4.0, making real-time data acquisition essential for administrative accountability. For educational institutions like Pangasinan State University – Alaminos City Campus (PSU-ACC), maintaining precise attendance logs for its 88 personnel (60 faculty and 28 non-teaching staff) is critical, since minor tracking delays carry direct institutional sanctions. While Quick Response (QR) code tracking systems offer an affordable, contactless mechanism for automated logs, standard configurations remain heavily dependent on continuous internet connectivity. Network disruptions frequently break automated workflows, forcing security personnel to revert to manual paper sign-in sheets, introducing administrative redundancies, reporting delays, and vulnerability to proxy attendance. To address these gaps, this study aims to design and develop SmartGate ACC, a proposed IoT-integrated entry management system featuring dual-layer authentication—combining QR code scanning and biometric facial recognition—alongside an engineered offline-first synchronization architecture. Following an Agile Software Development Life Cycle (SDLC) framework structured across seven phases (Plan, Design, Develop, Test, Deploy, Review, and Launch), the system will integrate a Flutter mobile application, Google ML Kit for localized biometric matching, an embedded SQLite local cache database, a Laravel back-end web dashboard, and a central MySQL database. System usability and quality will be evaluated by 50 purposively sampled respondents using a modified questionnaire based on the ISO/IEC 25010 standard, covering functional suitability, reliability, performance efficiency, usability, and security. The proposed system framework aims to establish a secure, network-resilient blueprint capable of executing identity verification locally on the edge terminal during network outages and triggering an automated Store-and-Forward background process to synchronize data with the cloud server upon reconnection. By eliminating manual logbook redundancies and preventing credential fraud, this study aims to demonstrate how localized edge computing and automated cloud synchronization can secure administrative workflows in resource-constrained academic environments.

Keywords: Quick Response (QR) technology, Biometric Face Recognition, Edge Computing, Offline-First Architecture

INTRODUCTION

The global landscape of institutional management is currently undergoing a radical transformation driven by the Fourth Industrial Revolution, commonly referred to as Industry 4.0. Across the globe, organizations are moving away from isolated, manual administrative tasks toward integrated ecosystems powered by the Internet of Things (IoT) (Raut et al., 2023). In an era where data is considered a primary institutional asset, the ability to capture and process it in real time is a fundamental requirement for operational success and organizational discipline. The integration of smart technologies allows for a more fluid exchange of information between different levels of management, ensuring that decision-making processes are based on accurate, up-to-the-minute data rather than delayed or potentially altered paper-based records. Within educational institutions, this shift is characterized by the need for high-speed data acquisition, where physical actions are converted into digital intelligence to maintain high standards of institutional accountability. Central to this digital evolution is the widespread adoption of Quick Response (QR) technology as a primary interface for data exchange. Originally developed for industrial manufacturing, QR codes have evolved into a global standard for tracking due to their high data capacity, contactless identification, and real-time cost-effectiveness (Setiawan & Rahayu, 2022). This scanning speed advantage has been shown to significantly optimize operational processing time in high-traffic identification settings (Stupina et al., 2021). Unlike traditional biometric systems that require specialized, high-maintenance hardware, QR-based solutions leverage existing mobile technology to create a seamless bridge between physical presence and digital records. In the Philippine educational landscape, the Commission on Higher Education (CHED) has actively promoted digitalization as a core pillar for administrative and academic success through its ACHIEVE 2030 Strategic Agenda. This national mandate encourages State Universities and Colleges (SUCs) to adopt decentralized, real-time innovations that can be seamlessly integrated into daily operations, establishing a clear benchmark for administrative maturity and technological readiness.

Pangasinan State University (PSU) has consistently aligned itself with these national standards of administrative innovation, seeking to automate core processes to enhance service delivery. At the Alaminos City Campus (PSU-ACC), there is an existing effort to utilize a QR-attendance system co-developed by the Alaminos and San Carlos campuses to automate logs and prevent manual time manipulation, recognizing that even a minor delay counts toward institutional sanctions for tardiness. The campus manages a total population of 88 employees, consisting of 60 faculty members and 28 non-teaching staff, with verification workflows coordinated between campus security and the Human Resources (HR) department. However, despite these technological strides, the campus still faces significant hurdles in achieving a fully seamless and secure real-time environment, as the current system remains heavily dependent on stable internet connectivity. When the campus Wi-Fi signal drops or network disruptions occur, the attendance process for all 88 employees completely reverts to traditional manual logbooks and physical signatures, a pattern consistent with documented cases of network instability and data latency disrupting cloud-dependent campus information frameworks (Nugroho et al., 2023).

The primary goal of this study is to design and develop SmartGate ACC, an IoT-integrated entry management and real-time monitoring system with dual-layer authentication for PSU Alaminos City Campus, to automate attendance tracking and enhance campus-wide transparency. This study aims to: [1] analyze and improve the existing entry management processes of PSU-ACC, particularly the recurring gaps in the current hybrid manual-digital logging system; [2] address the recurring problems and difficulties encountered in the current system, such as failed scans due to weak connectivity, delayed manual reporting to HR, and vulnerability to proxy attendance; [3] develop SmartGate ACC, an improved system featuring dual-layer authentication—combining QR code scanning and biometric facial recognition—supported by an offline-first synchronization architecture with edge-based verification during network outages; and [4] determine the acceptance level of the system based on functional suitability, reliability, performance efficiency, usability, and security, following the ISO/IEC 25010 evaluation standard.

METHODOLOGY

Software Development Life Cycle (Agile SDLC Phases)

This study utilizes a developmental and descriptive research design to engineer and evaluate the proposed entry management platform. The development of the SmartGate ACC software infrastructure will follow the Agile Software Development Life Cycle (SDLC) framework, which is characterized by its iterative, flexible, and incremental progression. The development life cycle is systematically broken down into seven sequential phases: Plan, Design, Develop, Test, Deploy, Review, and Launch.

Figure 1. Agile Methodology

ISSN No. 2454-6186 | DOI: 10.47772/IJRISS | Volume X Issue VII July 2026

During the initial planning stage, the exact functional parameters will be mapped alongside user experience expectations gathered from campus administrative departments. The design phase establishes the entity-relationship schemas for the local and cloud databases, alongside mobile layout mockups. The development environment consists of active sprint programming blocks using cross-platform compilation frameworks to build out the terminal application. In the testing phase, the system will undergo simulated stressful computing exceptions, focusing on intentional hardware network disconnection routines to verify data persistence stability within the isolated storage drivers. The deployment phase involves field setup of physical terminal monitors at target entryways. The review phase handles active documentation of validation feedback metrics, while the launch phase transfers operational custody to the institution.

Population and Locale

The structural boundary of this research is situated at Pangasinan State University – Alaminos City Campus (PSU-ACC), located within Barangay Bolaney, Alaminos City, Pangasinan. The target institutional population encompasses the entire current campus employee directory, totaling 88 active personnel. This baseline framework includes 60 designated academic faculty members and 28 non-teaching administrative support staff who routinely traverse the university perimeter daily. To systematically isolate qualified system evaluators from this broader ecosystem, a non- probability purposive sampling technique will be applied. This sampling logic targets specific sub-strata of professionals whose day-to-day administrative obligations or technical skill sets directly correspond with the system's backend monitoring applications, front-facing hardware gate operation, or underlying system infrastructure. Through this selective approach, a representative sample size of 50 distinct respondents will be integrated into the evaluation stage, ensuring a robust user acceptance evaluation. The selected respondent panel of 50 evaluators is organized across specific administrative and operational profiles to test every structural layer of the entry management platform. To ensure complete clarity regarding who will evaluate the application interfaces, the distribution matrix is categorized as follows:

Table 1. Respondents of the Study

Respondents (by Field)	Number of Respondents
ICTMO Coordinator	1
IT Experts	3
Human Resources	1
Security Guards	3
Faculty and Staff	42
Total	50

As shown in Table 1, the 50-respondent panel is deliberately weighted toward Faculty and Staff (42 respondents), who represent the primary daily users of the entry checkpoint, while the remaining eight respondents are distributed across ICTMO, IT Experts, Human Resources, and Security Guards. This distribution is intended to ensure that evaluation feedback reflects the perspective of the system's heaviest users while still capturing the specialized concerns of the technical and administrative staff who will manage the backend infrastructure and daily operational reporting. Including Security Guards and the ICTMO Coordinator as separate respondent categories is also intended to directly evaluate the two roles most affected by the current system's reliance on manual logbooks and technical troubleshooting during outages.

Data Instrumentation and Planned Evaluation

The central quantitative collection instrument will be a modified survey questionnaire structured closely around the globally recognized ISO/IEC 25010 software quality evaluation standard. This validation instrument maps user interaction quality through five distinct criteria: Functional Suitability, Reliability, Performance Efficiency, Usability, and Security. Each category targets a precise metric: Functional Suitability evaluates feature

ISSN No. 2454-6186 | DOI: 10.47772/IJRISS | Volume X Issue VII July 2026

completeness against requirements; Reliability tests data persistence during outages; Performance Efficiency records scanning processing speeds; Usability grades layout simplicity; and Security measures biometric accuracy.

To accurately analyze the gathered quantitative datasets, mathematical compilation will compute the exact Weighted Mean for every software attribute. Individual ratings will be calculated, stored, and then interpreted through a standardized 5-Point Likert Scale matrix framework:

Table 2. Scale of Measurement

Scale	Range	Verbal Interpretation
5	4.21-5.00	Highly Acceptable
4	3.41-4.20	Acceptable
3	2.61-3.40	Moderately Acceptable
2	1.81-2.60	Slightly Acceptable
1	1.00-1.80	Not Acceptable

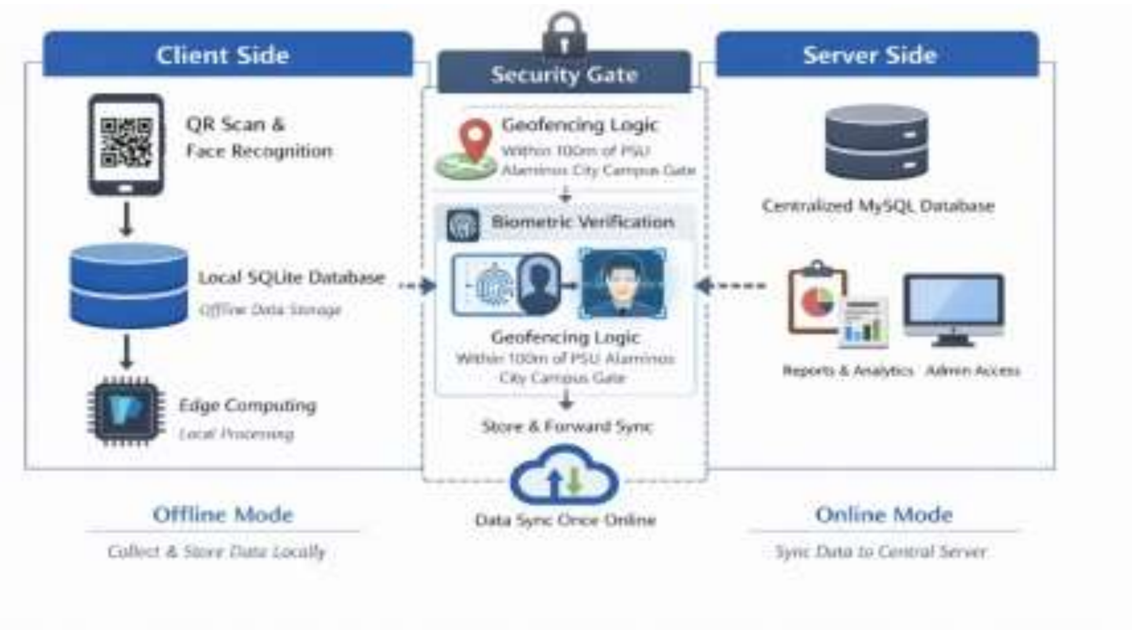
Table 2 defines the five-point Likert interpretation scale that will be applied to convert respondents' raw ratings into standardized verbal judgments, ranging from "Not Acceptable" to "Highly Acceptable." This scale is intended to give a consistent, replicable basis for interpreting the Weighted Mean computed for each ISO/IEC 25010 criterion (Functional Suitability, Reliability, Performance Efficiency, Usability, and Security), rather than relying on raw numerical averages that would be difficult for non-technical stakeholders, such as HR and campus administrators, to interpret directly. Establishing this scale in advance is also intended to support the study's objective of determining the system's acceptance level in a measurable, standardized way.

RESULTS AND DISCUSSION

Proposed Operational System Architecture

The core logic driving the gate application depends on a Client-Server Architecture with Offline-First Capability. This integration bridges the physical entry checkpoint with the administrative layer.

Figure 2. SmartGate ACC System Architecture

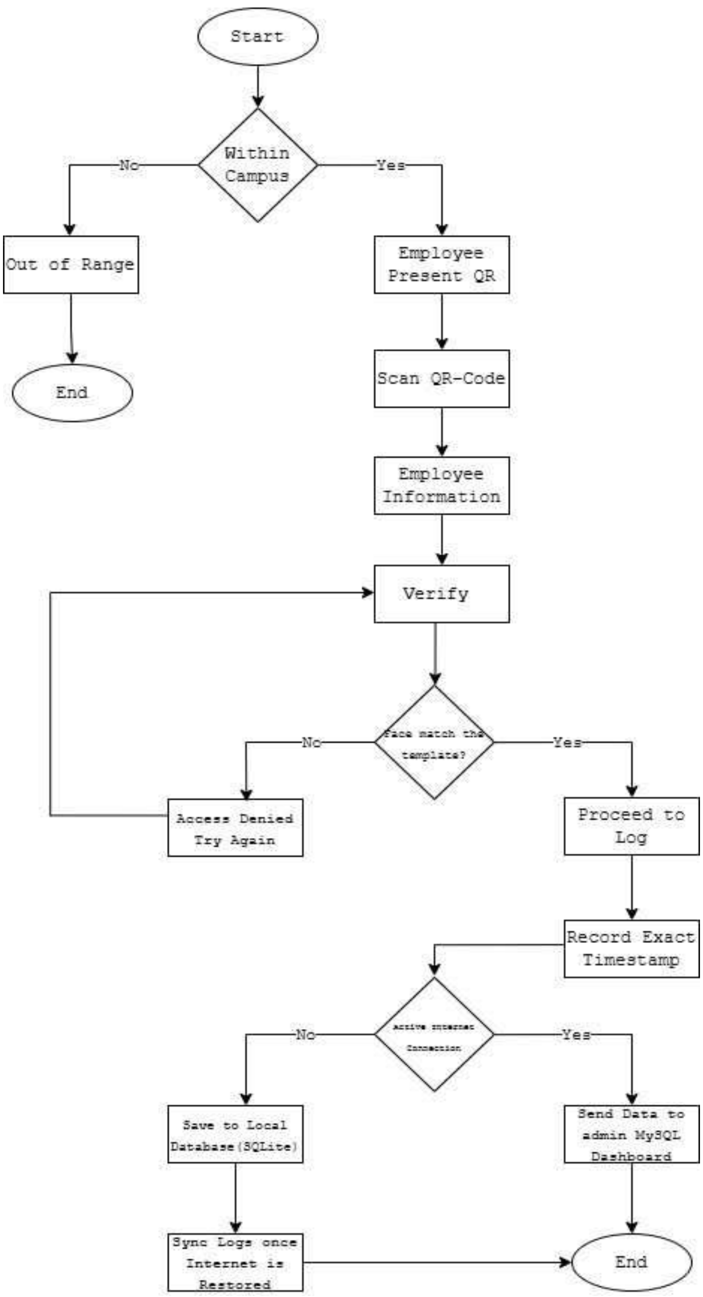


INTERNATIONAL JOURNAL OF RESEARCH AND INNOVATION IN SOCIAL SCIENCE (IJRISS)
ISSN No. 2454-6186 | DOI: 10.47772/IJRISS | Volume X Issue VII July 2026

This figure illustrates the proposed Client-Server Architecture with Offline-First Capability that will underlie SmartGate ACC, showing how the Edge Mobile Gate Client and the Web Administrative Dashboard are designed to interact across both connected and disconnected states. Unlike conventional attendance systems that treat the mobile client as a thin interface fully dependent on a live server connection, this proposed architecture positions the gate terminal as a self-sufficient node capable of independently authenticating and logging entries. This structural design directly addresses the core problem identified in the Introduction — that the current system reverts entirely to manual logbooks whenever connectivity drops — by ensuring that authentication and logging logic will reside locally at the edge rather than solely on the central server. This architecture is intended to form the technical foundation for the study's objective of developing a network-resilient entry management system, drawing on established design principles for centralized, real-time synchronization architectures in entry management terminals (Perin, 2024).

The step-by-step programmatic logic to be executed by the system during high-traffic gate hours will follow a strict execution path. When an employee approaches the gate station and scans their unique QR code, the system is designed to immediately process the frame. Rather than sending the data to a cloud API, the mobile gate hardware will natively decrypt the QR payload using Flutter and Google ML Kit. The system will then capture a camera frame to run a biometric face match, confirming user identity directly on the edge.

Figure 3. Flowchart



ISSN No. 2454-6186 | DOI: 10.47772/IJRISS | Volume X Issue VII July 2026

This figure presents the proposed step-by-step programmatic logic to be executed from the moment an employee scans their QR code to the final synchronization of the attendance log. The flowchart outlines two possible paths after a local timestamp is generated and saved to the SQLite database: an online path, where the log will be immediately pushed to the MySQL server via REST API, and an offline path, where the log will be retained locally until the Store-and-Forward synchronization logic detects a restored connection. This branching logic is designed to operationalize the offline-first design principle described in the study's objectives, demonstrating how data integrity and accurate timestamping are intended to be preserved regardless of network status. By mapping out this proposed decision path, the flowchart also clarifies how the system is expected to prevent data loss and reconcile offline records without requiring manual intervention from HR or security personnel — directly addressing the administrative redundancy and reporting delays identified as recurring problems in the current system.

If confirmed, the system will verify the device geofencing bounds to ensure the scan occurs within the authorized campus perimeter. Upon validation, a local system timestamp will be generated, and the log will be instantaneously saved to the local SQLite database, providing immediate visual and audio confirmation feedback to the user. The terminal will check the internet network status; if online, it will push the log via REST API to synchronize with the centralized MySQL server and update the HR dashboard. If offline, the log will be securely retained inside the local SQLite database, waiting for network restoration to trigger the automated store-and-forward synchronization logic.

Proposed System Prototype Framework

The proposed SmartGate ACC system prototype is designed to split its operations cleanly between two specialized software environments. The Edge Mobile Gate Client (to be developed using Flutter and Android Studio) will operate at the campus security gate checkpoint. Utilizing Google ML Kit, it is designed to handle high-speed frames from the device camera to perform local facial landmark detection. When the campus Wi-Fi signal drops, the software is designed to switch seamlessly to Offline Mode, routing all time-in and time-out logs into the embedded SQLite engine, which is intended to prevent data loss during internet blackouts.

Conversely, the Web Administrative Dashboard (to be constructed using Laravel, PHP, and MySQL) is designed to serve as the central repository and hosted "source of truth" on the internal institutional servers. Using asynchronous JavaScript and styled CSS, it is intended to present human resource personnel with real-time monitoring streams, live error alerts, and automated monthly summaries. The system is designed to store employee identification data, attendance timestamps, QR token identifiers, and facial landmark reference data necessary for authentication and synchronization. When network connectivity is restored, the client's automated Store-and-Forward Synchronization Logic is designed to detect the connection and push the offline logs to the MySQL backend via lightweight JSON REST APIs, reconciling administrative records across all departments without human intervention.

Figure 4. QR Code Scanning Interface

This figure presents the proposed initial checkpoint of the SmartGate ACC authentication process, where the employee will scan a unique QR code to initiate the clock-in or clock-out procedure. The interface, to be built

ISSN No. 2454-6186 | DOI: 10.47772/IJRISS | Volume X Issue VII July 2026

using Flutter on the Edge Mobile Gate Client, was designed with a minimal layout to reduce scanning time and cognitive load for both guards and faculty during peak entry hours. The planned real-time scan status indicator ("Waiting for QR scan...") is intended to reflect the system's responsiveness, allowing users to immediately recognize whether the device is actively reading the code. This first-layer authentication is designed to address the study's objective of automating attendance tracking, as it is expected to eliminate the need for guards to manually record entries in paper logbooks, directly resolving the structural discrepancies identified in the current hybrid manual-digital system, a bookkeeping inefficiency well documented in public institutional settings (Okon, 2025).

Figure 5. Employee Information Confirmation

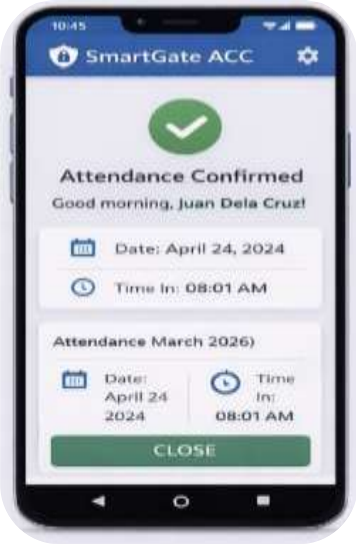
After a successful QR scan, the system is designed to retrieve and display the employee's stored identification details — including name, department, and employee ID — for user verification before proceeding to biometric authentication. This confirmation step is intended to function as a safeguard against QR token misuse, as it will require the scanned individual to manually confirm ("VERIFY" or "CANCEL") that the retrieved information matches their identity before advancing to facial recognition. This design choice directly supports the study's objective of preventing proxy attendance, since a mismatched or unauthorized scan can be immediately flagged and cancelled at this stage, rather than being processed as a valid entry.

Figure 6. Facial Recognition Verification

This figure illustrates the proposed second authentication layer, wherein the system is designed to use Google ML Kit to perform local facial landmark detection directly on the mobile device. Because facial verification is intended to be processed on-device rather than through a cloud-dependent service, the system is expected to maintain authentication capability even during network outages — a design decision that reflects the study's edge computing architecture. The proposed dual-layer authentication (QR code followed by facial recognition) is expected to significantly strengthen the system's resistance to credential fraud, as it will require both a valid digital token and a live biometric match, addressing the vulnerability to proxy attendance identified as a key problem in the current system, consistent with documented risks of open-access identification keys in institutional tracking systems (Chen & Li, 2022).

ISSN No. 2454-6186 | DOI: 10.47772/IJRISS | Volume X Issue VII July 2026

Figure 7. Attendance Record Confirmation



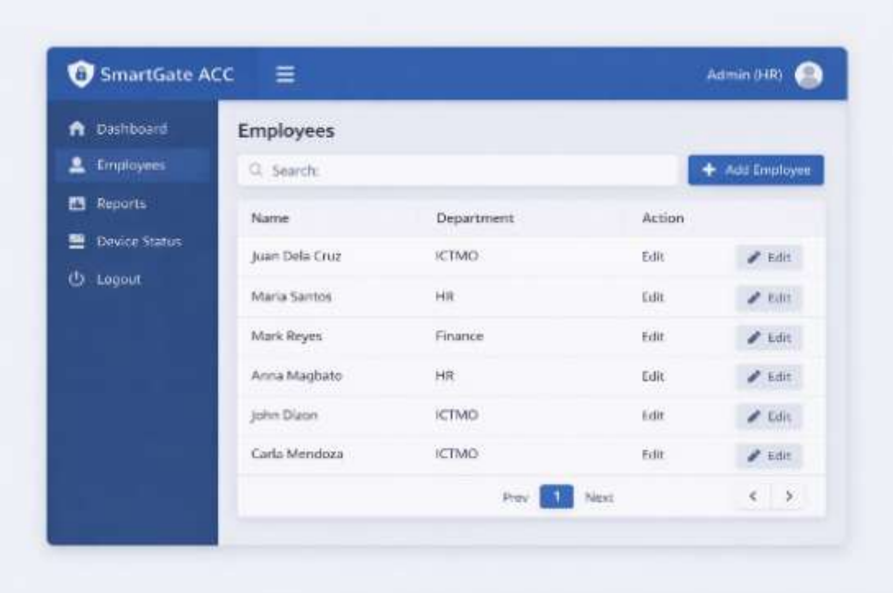
Upon successful facial verification, the system is designed to generate a confirmation screen displaying the employee's name, date, and exact time-in, providing immediate feedback that the attendance entry has been successfully logged. This real-time confirmation is intended to reduce ambiguity for the employee, ensuring they leave the checkpoint with certainty that their attendance was recorded. More critically, this entry is designed to be logged using the device's internal system clock, meaning the timestamp is expected to remain accurate even if the transaction occurs during a connectivity outage, and will be stored locally in the embedded SQLite engine. This is intended to resolve the recurring problem of inaccurate manual timestamps and reinforces the offline-first design objective of the study.

Figure 8. Real-Time Attendance Monitoring Dashboard

This figure presents the proposed Web Administrative Dashboard, to be built using Laravel, PHP, and MySQL, which is designed to serve as the centralized "source of truth" for institutional attendance data. The dashboard is intended to provide HR personnel with an at-a-glance summary of total employees, present, late, and absent counts, updated in real time as synchronized data arrives from the gate client. This is expected to address the study's objective of enhancing campus-wide transparency, as administrators would no longer need to manually consolidate paper logs and digital records to obtain an accurate daily headcount — a task previously prone to delay and discrepancy under the old hybrid system.

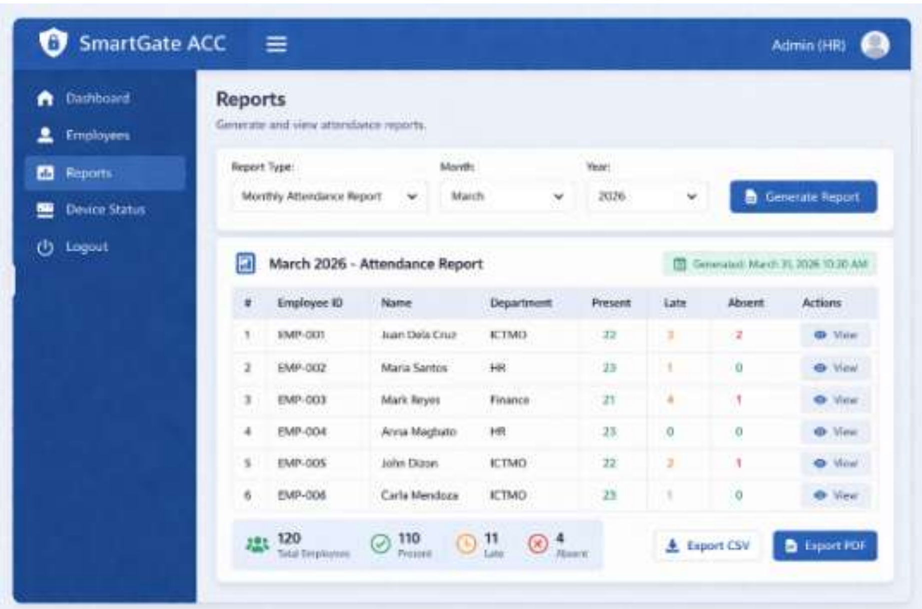
ISSN No. 2454-6186 | DOI: 10.47772/IJRISS | Volume X Issue VII July 2026

Figure 9. Employee Record and Biometric Management



This figure shows the proposed administrative interface for managing employee records, including the ability to edit personal information and associated biometric reference data. Centralizing this function within the Web Administrative Dashboard is intended to ensure that only authorized HR personnel can modify sensitive employee and biometric data, reinforcing data integrity and access control. This module is designed to support the system's long-term scalability, as new employees would be registered and their facial landmark data enrolled directly through the dashboard, ensuring the authentication database remains current without requiring manual coordination between campus security and HR.

Figure 10. Automated Reporting and Analytics



This figure demonstrates the proposed automated report generation feature, which is designed to allow HR to filter attendance records by month and year and export consolidated reports in formats such as CSV or PDF. This function is intended to replace the manual, error-prone process of compiling monthly attendance reports from paper logs and disconnected digital entries, which was identified as a significant source of delay and human error in the current system. This aligns with findings that automated analytics and reporting tools substantially improve the accuracy and usefulness of institutional data compared to manually compiled records (Al Amin et al., 2024). By automating this process, SmartGate ACC is expected to reduce administrative workload while improving the accuracy and consistency of institutional attendance reporting — fulfilling the study's objective of streamlining administrative workflows through automated cloud synchronization.

CONCLUSION

The proposed framework of SmartGate ACC provides a practical, network-resilient solution to traditional attendance monitoring challenges at Pangasinan State University Alaminos City Campus. In line with the study's first and second objectives of analyzing the existing entry management process and addressing its recurring problems, the design directly targets the structural discrepancies, failed scans, and proxy attendance vulnerabilities identified in the current hybrid manual-digital system. Consistent with the third objective of developing an improved system, SmartGate ACC combines QR technology, biometric facial verification, and an offline-first architecture to remove network dependency from the campus entry workflow, effectively eliminating manual logbook redundancies and securing data integrity during internet outages. Finally, addressing the fourth objective, the system's planned evaluation against the ISO/IEC 25010 criteria, functional suitability, reliability, performance efficiency, usability, and security, is intended to determine its acceptance level among faculty, staff, security personnel, and administrators. Taken together, SmartGate ACC establishes a reliable, automated, and secure institutional record infrastructure, optimizing administrative workflows and proving that decentralized edge computing is a viable approach for entry management in localized academic settings.

REFERENCES

1. Al Amin, M., Rahman, M. S., & Islam, R. (2024). Data analytics and visualization trends in modern human resource management systems. Journal of Institutional Intelligence, 12(2), 145-159.
2. Chen, H., & Li, W. (2022). Vulnerabilities and security risks of open-access identification keys in institutional tracking systems. Computers & Security, 114, 102-115.
3. Nugroho, B., Putra, D., & Setiawan, A. (2023). Addressing network instability and data latency in cloud-dependent campus information frameworks. Review of Computer Engineering Studies, 19(4), 210-224.
4. Okon, E. (2025). The cost of paper: Assessing administrative bookkeeping inefficiencies and proxy logging errors in public institutions. Journal of Administrative Automation, 31(3), 88-101.
5. Perin, M. L. (2024). Centralized relational databases and real-time synchronization architectures for entry management terminals. Journal of Software Quality and Systems Architecture, 14(2), 112-126.
6. Raut, S., Joshi, M., & Kulkarni, P. (2023). Ubiquitous mobile scanning: Bridging physical institutional presence with digital university ledger databases. IEEE Transactions on Systems, Man, and Cybernetics, 53(7), 401-412.
7. Setiawan, R., & Rahayu, S. (2022). Matrix data capacity: A comparative study of traditional barcodes and multi-dimensional QR configurations. Journal of Information Systems Technology, 28(3), 190-205
8. Stupina, A., Shaikholder, V., & Kovalev, I. (2021). Optimizing operational processing time lines via high-speed visual identification markers. Academic Research Journal of Engineering, 17(4), 50-63.