International Journal of Science, Technology, Engineering and Mathematics
Volume 5 Issue 4 December 2025
DOI: https://doi.org/10.53378/ijstem.353275

Enhancing efficiency and security: A study of automated visitors monitoring system in the Bureau of Jail Management and Penology

Leoncio O. Limyoco Jr.

Abstract

This study aimed to design, develop, and evaluate an Automated Visitors Monitoring System (AVMS) using fingerprint biometric technology to enhance visitor management efficiency and security in the Bureau of Jail Management and Penology (BJMP). A mixed methods approach was employed, integrating quantitative data from user surveys with qualitative insights from interviews and focus group discussions. Pilot testing at the Quezon District Jail in Pagbilao, Quezon involved 20 personnel and 200 visitors, with biometric accuracy evaluated through 918 fingerprint entries. The AVMS achieved 100% accuracy, with high user satisfaction (WAM = 4.88), confirming its reliability and institutional relevance. The AVMS achieved 100% accuracy with zero false acceptance or rejection rates. Users rated the system as "very satisfactory" (WAM = 4.88) and reliability "very reliable" (WAM = 4.88). Respondents noted faster processing times, improved record accuracy, and enhanced security. Suggestions for system refinement included visitor restriction tagging, service provider monitoring, alert notifications, and data recovery functions. The study was limited to a single facility and focused exclusively on fingerprint biometrics, which may affect its applicability in other settings. Future research involving multiple facilities and incorporating other biometric modalities is recommended to strengthen the findings. Nonetheless, the results provide strong evidence of the AVMS's feasibility and highlight its potential for wider institutional adoption.

Keywords: *automated visitor monitoring system, fingerprint recognition, jail security, BJMP, visitor management, correctional facilities*

Article History:

***Received**: July 29, 2025* ***Revised**: October 15, 2025*
***Accepted**: October 16, 2025* ***Published online**: October 31, 2025*

Suggested Citation:
Limyoco, L.O. (2025). Enhancing efficiency and security: A study of automated visitors monitoring system in the Bureau of Jail Management and Penology. *International Journal of Science, Technology, Engineering and Mathematics*, 5(4), 44-63. https://doi.org/10.53378/ijstem.353275

About the author:
PhD in Criminology at Philippine College of Criminology. Jail Officer, BJMP. limyocoleoncio@gmail.com

1. Introduction

Correctional facilities play an important role in maintaining law and order, not only through the detention of Persons Deprived of Liberty (PDLs), but also by ensuring that operational protocols promote both institutional security and humane treatment. One such operational component that remains a persistent challenge is visitor management. The Bureau of Jail Management and Penology (BJMP), as the frontline agency in the Philippines tasked with the safekeeping of PDLs, continues to rely on manual visitor logging systems across its jail facilities. This conventional approach is prone to a host of problems, including inaccuracies in data entry, difficulty in record retrieval, and potential loopholes that compromise security and operational efficiency. Overcrowding in visitor areas, coupled with the absence of real time monitoring, further makes administrative delays and increases the risk of unauthorized access or procedural violations (Department of Justice, 2023).

With the global shift toward digitization and the proven benefits of biometric technologies in security sensitive environments, there is a compelling need for the BJMP to transition toward a more automated and intelligent visitor management system. Studies have shown that automated monitoring systems, particularly those using biometric features such as fingerprint scanning, significantly enhance accuracy, minimize fraud, and improve institutional control (Jain et al., 2023; Yang et al., 2019; Yu et al., 2023). However, despite the availability of such technologies, their adoption within the Philippine jail management system remains limited. Previous modernization efforts in the BJMP have mainly focused on improving infrastructure and manual processes, but there is little to no record of any attempt to create a fully automated visitor monitoring system. Current practices still rely on paper logbooks or standalone digital tools that do not include biometric verification or centralized recordkeeping. This makes the present study unique, as it is the first to design, develop, and pilot test a fingerprint-based Automated Visitor Monitoring System (AVMS) made specifically for BJMP operations.

Specifically, the objectives of the study are as follows: (1) to evaluate user satisfaction with the features of the AVMS; (2) to determine the system's biometric accuracy and reliability through performance testing; (3) to assess the operational impact of the AVMS on jail management practices; and (4) to gather user feedback for future system enhancements. By fulfilling these objectives, this research seeks to establish a foundation for digital innovation within the BJMP and contribute to the broader body of knowledge on technology adoption in

correctional environments. The findings will not only inform policy and investment decisions within the BJMP but also serve as a model for other government agencies facing similar operational challenges.

The significance of this research lies in its practical application and potential contribution to the modernization of jail management in the Philippines. Unlike previous studies that primarily focused on theoretical models or general technological adoption in public institutions, this study provides an empirically validated system that directly addresses operational shortcomings in jail visitor management. Moreover, the proposed system emphasizes data privacy, accountability, and institutional control key principles that are essential in high security settings.

2. Literature Review

2.1. Theoretical Framework

The research on automated visitor monitoring systems in the BJMP is grounded in several Philippine laws and established management theories. The legal foundation supports enhancing public safety, ensuring security in detention facilities, and promoting data privacy and technological innovation. It aligns with mandates from the Philippine Constitution, which emphasizes maintaining peace, order, and general welfare while protecting individual rights, including privacy (1987). Specific laws, such as the Department of the Interior and Local Government Act (R.A. No. 6975), assign the BJMP the responsibility to maintain effective jail management, supporting technology upgrades. The Data Privacy Act (R.A. No. 10173) mandates that any automated system collecting sensitive information must ensure data is stored securely and is accessible only to authorized personnel. Furthermore, the Electronic Commerce Act (R.A. No. 8792) and the Ease of Doing Business Act (R.A. No. 11032) promote the use of electronic records for efficiency and transparency. These national laws are complemented by the BJMP's own Comprehensive Operations Manual, which sets visitor protocols and security standards, and by policies from the DILG encouraging technological adoption.

The legal framework is supported by relevant theoretical foundations. Systems Theory views organizations as complex systems where changes in one part, such as improved visitor monitoring, can positively impact the entire organization's performance, including security and administrative operations (Besio & Tacke, 2024). This approach suggests that a well-integrated system can optimize resource use and reduce staff workload. High Reliability Organization

(HRO) principles emphasize operational consistency and institutional mindfulness as crucial for maintaining security in sensitive environments (Weick et al., 1999). An automated visitor monitoring system acts as a "capable guardian," reducing security vulnerabilities by ensuring consistent verification and alert mechanisms. Finally, the Technology Acceptance Model (TAM) explains that user acceptance of a new system is largely driven by its perceived usefulness and ease of use (Venkatesh & Bala, 2008). In the BJMP context, the system's effectiveness and reliability are key to gaining acceptance from both personnel and visitors.

Routine Activity Theory explains that security threats arise when motivated offenders encounter suitable targets without capable guardians. In a jail setting, this theory underscores the importance of visitor verification and monitoring to deter potential risks, such as unauthorized access or contraband smuggling. An automated visitor monitoring system with biometric verification and real time alerts acts as a "capable guardian," reducing security vulnerabilities. This aligns with High Reliability Organization principles, which emphasize operational consistency and institutional mindfulness as critical to maintaining security and user trust in complex, sensitive environments (Weick et al., 1999).

2.2. The Growing Role of Automated Visitor Management Systems (AVMS) in Security Operations

AVMS have gained global recognition for their ability to improve operational security and efficiency in high-risk environments, particularly correctional institutions. The core benefit of AVMS lies in its capacity to streamline visitor verification processes, minimize manual entry errors, and reinforce institutional security protocols. These systems automate tasks that were once reliant on error-prone manual processes, making them essential in facilities that demand strict identity control.

Biometric authentication technologies have become indispensable in sectors demanding high-level security, such as law enforcement, immigration, and healthcare (Zhou et al., 2024). Among the various biometric modalities, fingerprint recognition is widely regarded as the most effective due to its accuracy, cost-efficiency, and ease of integration into existing infrastructures (Alrawili et al., 2024; Jain et al., 2023). Unlike access cards or passwords, fingerprints are unique, tamper-resistant, and less susceptible to duplication or fraud, making them a feasible model for correctional institutions such as the BJMP.

Fingerprint-based AVMS thus address long-standing security gaps inherent in manual systems while enhancing accountability and reliability (M2SYS Technology).

Other biometric modalities, such as facial recognition, have been increasingly adopted in industries requiring fast and contactless verification. While facial recognition provides convenience and speed, studies continue to show that its accuracy can be more susceptible to environmental factors like lighting and pose compared to the highly stable patterns of the fingerprint and iris. Iris recognition, in particular, is often cited as offering the highest levels of accuracy and security due to the extreme uniqueness and permanence of its patterns, which are nearly impossible to replicate (Zakaria, 2025). Nevertheless, Baig et al. (2022) demonstrated that face recognition systems can effectively support attendance and monitoring processes, suggesting their potential for broader applications in institutional visitor management where speed is prioritized over precision.

Beyond biometrics, Radio-Frequency Identification (RFID) systems have also been explored for automated attendance and access control. Arulogun et al. (2013) highlighted how RFID technology improved efficiency in environments plagued by administrative delays, particularly in developing countries. Similarly, Awotunde et al. (2023) found that contactless RFID systems reduced human error in student monitoring, while Siddiqui et al. (2024) advanced this approach through an IoT-based RFID model that stored attendance data in real time on cloud servers. Despite these benefits, RFID systems remain less secure than biometrics due to vulnerabilities such as data duplication, dependency on internet connectivity, and lower accuracy in identity verification. Hence, in security-critical environments like correctional facilities, biometric solutions remain the preferred standard.

2.3. The Need for Biometric AVMS in Developing-Country Contexts

Most existing literature on AVMS implementation focuses on technologically advanced or well-resourced environments. However, research in developing-country contexts remains limited, despite the pressing need for efficient and secure systems. This study addresses that gap by testing the feasibility and effectiveness of a fingerprint-based AVMS in the resource-constrained environment of Philippine jails under the BJMP. Local findings further underscore the urgency of modernization, as manual logbook-based visitor management continues to expose facilities to administrative inefficiencies and security risks.

The Philippine experience with biometrics in various institutional settings reinforces their reliability and practicality. In education, for instance, a study at Cebu Technological University reported a "very satisfactory" rating for a fingerprint-based attendance system in terms of timeliness and accuracy (Perez et al., 2022) while in recent findings from Don Honorio Ventura State University observed similarly positive results, with the attendance system proving exceptionally effective and efficient in practice (Frigillana et al., 2023). In local government offices, pilot initiatives have explored the adoption of biometric attendance systems (Villaroman et al., 2018), though challenges remain regarding funding, infrastructure, and staff readiness (BARS Philippines, n.d.; Villaroman et al., 2018). In correctional settings, Castillo et al. (2025) documented the successful implementation of a QR code–based visitor management and monitoring system in a BJMP facility in Baliwag, which led to enhanced security and reduced administrative errors. These localized examples highlight both the promise and practical challenges of adopting automated and biometric systems within Philippine institutions.

3. Methodology

3.1 Research Design

This study employed a convergent parallel mixed methods design, where quantitative and qualitative approaches were implemented simultaneously, analyzed separately, and then integrated (Creswell & Creswell, 2018).

The quantitative approach involved structured survey questionnaires administered to 200 visitors, along with biometric accuracy tests using 918 fingerprint scans (459 registered visitor entries and 459 simulated unauthorized entries). These provided measurable data on user satisfaction, efficiency, and system reliability.

The qualitative approach engaged 20 BJMP personnel through semi-structured interviews and focus group discussions, supported by observational field notes during pilot testing. This allowed for deeper insights into system usability, operational challenges, and recommendations for improvement.

By integrating both approaches, the study achieved triangulation, combining numerical results with contextual perspectives to comprehensively evaluate the AVMS in a correctional setting.

3.2 System Development

In the design phase, the study began with a systematic analysis of existing visitor management workflows in BJMP facilities. System requirements were identified through consultations with jail administrators and IT personnel to ensure that the AVMS would address real operational problems such as delays in processing, data inconsistencies, and security vulnerabilities. A user centered design approach was adopted to make the interface intuitive for both staff and visitors.

The development phase involved translating these requirements into a working prototype that integrated fingerprint biometric authentication with a secure database for visitor records. Core modules included visitor registration, identity verification, check-in/check-out logging, and automated reporting. Additional safeguards were developed to comply with data privacy standards and ensure reliability in a high-security environment.

Pilot testing and system evaluation were then conducted to assess user satisfaction, system performance, and the impact of the AVMS on operational efficiency. Questionnaires distributed to jail personnel and visitors were used to gather qualitative and quantitative data to validate the system's usability and effectiveness.

3.3 Participants of the Study

The study involved 200 visitors for the quantitative approach and 20 BJMP personnel for the qualitative approach. Visitors were randomly selected during the pilot implementation to answer structured survey questionnaires and participate in biometric testing, which recorded 918 fingerprint scans (459 registered visitor entries and 459 simulated unauthorized entries).

BJMP personnel were chosen through purposive sampling based on their roles in visitor management, administration, and IT support, with at least one year of service experience. They participated in interviews and focus group discussions to provide operational insights. This distribution ensured that the quantitative approach captured visitor satisfaction and system accuracy, while the qualitative approach highlighted staff perspectives on implementation and security.

3.4 Instrumentation and Data Gathering Process

The primary instruments were structured survey questionnaires, interview guides, observation checklists, and the AVMS prototype itself. Each tool was carefully prepared and subjected to procedures that ensured both validity and reliability.

Surveys measured visitor satisfaction, perceived system reliability, and the impact of the AVMS on jail operations. To establish content validity, the questionnaire was reviewed and validated by a panel of six experts' three practitioners in jail management, two faculty members from academe, and one information technology (IT) specialist. Their collective expertise ensured that the items were clear, relevant, and aligned with the study objectives. Following expert validation, a pilot test was conducted with a small group of respondents representing both BJMP personnel and visitors. The pilot exercise assessed the clarity of wording, response format, and the adequacy of the Likert scale.

Interviews and focus group discussions with BJMP personnel provided qualitative data. To enhance credibility and trustworthiness, interview and FGD guides were aligned with the study's objectives, and open-ended questions encouraged detailed responses. Triangulation with survey and observation results further validated the consistency of findings.

Observational checklists were used to document changes in visitor processing before and after AVMS implementation. Reliability was reinforced by using standardized checklists applied consistently across both baseline and pilot phases, minimizing researcher bias.

The AVMS prototype itself served as an experimental instrument, generating biometric performance data such as False Rejection Rate (FRR) and False Acceptance Rate (FAR). Reliability was ensured by conducting repeated tests (918 scans total, with 459 registered visitor entries and 459 simulated unauthorized entries) under controlled conditions.

Data collection occurred in two phases: Baseline data collection under the manual visitor logging system; and Pilot testing and full deployment of the AVMS. Through validation, pilot testing, standardized procedures, and triangulation of results, the study ensured that the instruments and processes used were both valid and reliable, thereby strengthening the credibility of the findings.

3.5 Data Analysis

Quantitative data from the surveys were analyzed using descriptive statistics such as frequency, percentage, and Weighted Average Mean (WAM) to determine satisfaction levels and perceived system effectiveness. The accuracy test used the following formulas:

FRR (False Rejection Rate) = False Rejections / Total Registered Attempts

FAR (False Acceptance Rate) = False Acceptances / Total Intruder Attempts

CI (95% Confidence Interval) = $p + z(\sqrt{(p(1-p)/n)})$ where $z = 1.96$

Qualitative responses were analyzed using thematic analysis to identify common themes and insights regarding system usability and implementation experiences.

3.6 Research Ethics

The study adhered to established ethical standards in conducting research involving research participants and sensitive biometric data. Ethical clearance was secured from the Research Ethics Committee of the Philippine College of Criminology and was accepted and approved dated 22 July 2025. This approval confirmed that the study met the requirements for protecting the rights, safety, and welfare of all participants.

Informed consent was obtained from every participant prior to their involvement. Participation was strictly voluntary, and respondents were assured that they could withdraw at any time without penalty. Confidentiality was maintained by anonymizing survey responses, interview transcripts, and system-generated records.

The collection and storage of biometric data were restricted to academic purposes only and safeguarded by encryption and limited access protocols. Data management complied with the Philippine Data Privacy Act of 2012 (Republic Act No. 10173) and adhered to international guidelines that emphasize the important need for strong privacy safeguards, data minimization, and purpose limitation in the handling of biometric information in law enforcement contexts (Privacy International, 2020).

4. Findings and Discussion

The primary outcome of this study is the development and pilot implementation of an enhanced AVMS, a biometric based software application designed specifically for the BJMP. The AVMS stands as the central product of the research, resulting from a systematic process of needs assessment, user interface design, system development, and multi-phase evaluation. It directly addresses the long standing challenges associated with manual visitor logbooks by introducing a secure, accurate, and efficient tool tailored to the operational demands of correctional facilities.

The system incorporates essential features such as biometric fingerprint authentication, visitor registration and banning, PDL management, service provider tracking, automated alerts for overstaying visitors, and detailed log reporting. It also includes user activity logs and data recovery capabilities, all of which are grounded in the feedback from jail personnel and aligned

with institutional security requirements. The AVMS has been developed not only as a proof-of-concept but as a functional and scalable system ready for deployment in actual correctional settings.

Tested during a live environment at the Quezon District Jail, the system achieved 100% biometric accuracy, with zero false acceptance and false rejection rates across 918 fingerprint entries. These results validate its technical robustness and suitability for secure visitor verification. Furthermore, survey results among 20 BJMP personnel and 200 visitors revealed high user satisfaction, operational benefits, and strong institutional acceptance, confirming that the system is usable, practical, and effective. The qualitative findings, drawn from interviews and focus group discussions with 20 BJMP personnel, complemented these results by highlighting practical experiences with the system. Staff confirmed that the AVMS reduced manual workload, minimized recordkeeping errors, and improved overall security. However, they also identified challenges such as equipment limitations, technical support needs, and resistance to change among some staff and visitors.

When integrated, both sets of findings reinforce each other: the quantitative results confirm the system's technical accuracy and user satisfaction, while the qualitative findings explain why these results were achieved and identify areas for further improvement. For example, the very high reliability ratings in surveys were supported by staff testimonies describing the system's effectiveness in detecting unauthorized visitors. Conversely, the qualitative reports of infrastructure and training challenges contextualize the slightly lower survey scores on processing speed, suggesting that technical performance was strong but dependent on adequate resources and user readiness. Together, these integrated findings provide a comprehensive understanding of how the AVMS performs in a real-world correctional setting, validating its feasibility while also pointing to necessary refinements for broader implementation.

Table 1 shows the overall satisfaction with the AVMS. The overall weighted mean was 4.88, indicating a descriptive rating of Very Satisfied. This suggests that users had highly favorable perceptions of the system's design, performance, and ease of use. The results are consistent with recent usability frameworks, which stress that biometric systems gain traction when they are perceived as both accessible and efficient (Basaligheh & Kothawade, 2025).

Table 1

User satisfaction with the features of the automated visitors monitoring system

Indicators	Weighted Mean	Descriptive Meaning
Ease of learning and using the biometric system	4.93	Very Satisfied
Ability to handle the registration of both first-time and repeat visitors	4.92	Very Satisfied
Reliability in detecting and preventing unauthorized access	4.89	Very Satisfied
Accuracy and reliability of the fingerprint scanner in verifying visitors	4.91	Very Satisfied
Speed of the check-in and check-out process	4.74	Very Satisfied
Weighted Average Mean	**4.88**	**Very Satisfied**

The highest mean score was 4.93, corresponding to the ease of learning and using the biometric system. This implies a high level of intuitiveness and user friendliness, even for users with minimal technical expertise. Fallahi et al. (2025) emphasized that ease of use is a critical determinant in user trust and long-term system adoption. In addition, the system's ability to handle registration of both first-time and repeat visitors indicates seamless and efficient enrollment processes, which are crucial in correctional environments with continuous visitor flow (El-Abed et al., 2010). Similarly, the accuracy and reliability of the fingerprint scanner underscores the significance of precise biometric identification, as fingerprint recognition accuracy is vital for maintaining system credibility and usability in secure settings (Meiramkhanov & Tleubayeva, 2024; Jain et al., 2023). The system's reliability in detecting and preventing unauthorized access, reflecting user trust in its security features, an essential factor since system reliability and threat mitigation foster institutional trust in biometric technologies (Basaligheh & Kothawade, 2025). Although the lowest score, 4.74, was recorded for the speed of the check-in and check-out process, it still indicates high satisfaction while highlighting room for further optimization, as response time remains a key determinant of user satisfaction in high-volume biometric systems (Fallahi et al., 2025).

The consistently high satisfaction ratings across all five dimensions demonstrate the AVMS's success in meeting user expectations. The findings reinforce the system's practical applicability and potential scalability for wider use in other BJMP facilities. Moreover, the results affirm the system's alignment with usability and biometric security standards, validating its readiness for institutional adoption.

Table 2 presents the findings on the reliability of the biometric-based AVMS implemented in the BJMP. Reliability in this context refers to the system's ability to perform

its intended functions consistently under various conditions, including accurately verifying visitor identities, minimizing errors, and maintaining secure operations. Based on user responses, the overall weighted mean score for system reliability was 4.88, which corresponds to a descriptive interpretation of Very Reliable. This high rating suggests that the system met or exceeded user expectations across all measured performance indicators. This high level indicates that the AVMS consistently met user expectations across all measured indicators.

Table 2

Accuracy and reliability of the automated tool for jail visitors monitoring

Indicators	Weighted Mean	Descriptive Meaning
Accurately verifying visitor identity	4.89	Very Reliable
Minimizing errors during visitor verification	4.90	Very Reliable
Security and performance	4.90	Very Reliable
Performing its intended functions	4.88	Very Reliable
Overall accuracy (e.g., no errors, consistent operation)	4.86	Very Reliable
Weighted Average Mean	**4.88**	**Very Reliable**

The AVMS achieved consistently high reliability ratings, with the highest-rated indicators, each with a weighted mean of 4.90, being the system's ability to minimize errors during visitor verification and its reliability in maintaining secure and consistent operations. These results indicate strong user confidence in the system's precision and dependability, aligning with Jain et al. (2023) and Alrawili et al. (2024). The system's reliability in verifying visitor identities followed closely with a mean of 4.89, underscoring its effectiveness in accurate identification, consistent with Jain et al. (2023). Meanwhile, the ability to perform under varying operational conditions scored 4.88, reflecting user confidence in the system's adaptability, echoing Alrawili et al. (2024). The lowest-rated indicator, overall system accuracy, still earned a strong 4.86, suggesting minimal variability in performance. As per Jain et al. (2023), reducing verification errors is key to fostering long-term trust and adoption in high-security contexts.

The consistently high ratings across all reliability indicators reinforce the system's strong operational foundation. The results align with TAM, which suggests that perceived reliability and functionality are significant predictors of user acceptance (Venkatesh & Bala,

2008). The AVMS demonstrates these attributes, making it suitable for institutional deployment in the BJMP, where secure and efficient visitor monitoring is essential.

Table 3 evaluates the overall impact of the biometric-based AVMS on operational efficiency, security, and user experience within the BJMP. Five key impact areas were assessed: security enhancement, efficiency improvements, visitor processing time, operational effectiveness, and the general impact on BJMP operations.

Table 3

Perceived impact of the developed automated tool on the efficiency and security of jail visitor monitoring

Indicators	Weighted Mean	Descriptive Meaning
Security of visitor management	4.90	Significant Positive Impact
Operational efficiency	4.79	Significant Positive Impact
Visitor processing time	4.85	Significant Positive Impact
Operational effectiveness	4.88	Significant Positive Impact
Impact on the operations of BJMP	4.75	Significant Positive Impact
Weighted Average Mean	**4.83**	**Significant Positive Impact**

The overall weighted mean across all five indicators was 4.83, interpreted as a Significant Positive Impact. This result suggests that the biometric system was well-received by both staff and visitors, offering substantial operational benefits. These findings align with the Diffusion of Innovation Theory, which posits that technological innovations are more likely to be adopted when they demonstrate clear advantages over previous methods (Rogers, 2003).

The AVMS received high ratings across all performance indicators, with the highest-rated aspect being its contribution to improving security (M = 4.90), reflecting enhanced visitor identification, tracking, and prevention of unauthorized access. This outcome is consistent with findings that biometric systems offer significant security enhancements over traditional methods like ID cards or passwords, primarily because unique physical traits are virtually impossible to forge or replicate (Jain et al., 2022). Operational effectiveness followed with a mean of 4.88, as respondents noted workflow optimization through automated verification and reduced manual encoding, supporting Jain et al. (2023) findings that biometrics lessen administrative burdens and enhance reliability. The system's impact on visitor processing time (M = 4.85) showed that biometric identification expedited check-ins and check-outs. Similarly, general operational efficiency (M = 4.79) was strengthened through improved data accuracy

and staff productivity, aligning with the Biometrics Institute's view that system efficacy and data accuracy are crucial for effective implementation and continuous improvement of biometric technology (Biometrics Institute, 2019). Lastly, the overall impact on BJMP operations received the lowest yet still strong mean of 4.75, with respondents recognizing positive outcomes while emphasizing the need for continued system refinement and user training. Gupta (2024) stressed that ongoing technical support and capacity building are essential for the sustainable adoption of biometric systems.

The consistently high mean scores across all evaluated areas affirm the AVMS's effectiveness in addressing long-standing challenges in jail visitor management. It significantly enhances security, operational efficiency, and staff performance, supporting its potential for broader deployment across correctional facilities. As recommended, BJMP may benefit from establishing ongoing feedback mechanisms, implementing regular staff training, and conducting scalability assessments to ensure sustained success.

Table 4

Challenges encountered in using the system and the necessary improvements needed

Participant ID	Responses	Code
Challenges encountered in using the system		
RG 1 RG 2 RG 3	Integration with the automated system, such as the encoding of visitor information. However, encoding the details of Persons Deprived of Liberty (PDL) is not an issue because data can be conveniently imported from existing Excel files.	Data Encoding
	System Adoption and Training Maintenance and Technical Support	Technical Support
	Purchasing the necessary computers and equipment	equipment
	Resistance to change among staff or visitors who are accustomed to manual processes	Resistance to change
Additional features or improvements suggested		
RG 1 RG 2 RG 3	Enhance the system, such as restrictions for banned visitors or Persons Deprived of Liberty (PDL)	Restricted visitors
	Visitor monitoring for service providers like lawyers, court personnel, priests, pastors, and others	Service provider monitoring
	Automated Alerts: Send alerts for unusual activities, such as: Visitor staying beyond allowed time	Overstaying visitors
	The Data Restore feature allows administrators to recover accidentally deleted visitor records	Archive
	System log-in, record all data deletion and restoration activities for accountability of user	System log-in activities

As shown in Table 4, qualitative data were collected from twenty (20) BJMP personnel through open-ended survey questions. Using a thematic analysis approach, responses were categorized into two main themes: suggested enhancements for AVMS and the challenges encountered during its implementation. This allowed for a deeper understanding of how the system performs in a real-world correctional setting beyond what was revealed through quantitative metrics.

Challenges experienced during system use were thematically analyzed. One of the most common issues identified was difficulty in encoding visitor data, particularly for first-time users. However, this challenge was partially mitigated by the system's ability to import PDL information from pre-existing Excel spreadsheets, which improved the speed and ease of data entry. Another significant concern was the lack of immediate technical support and system maintenance. Respondents noted that the absence of accessible technical assistance could delay problem resolution and negatively impact operational efficiency, suggesting the need for a dedicated support mechanism (Akingbade & Adaramola, 2025).

The study also revealed that limited equipment availability, including computers and biometric scanners, posed logistical challenges during the initial deployment of the system. This underscores the need for adequate infrastructure to support technology-based initiatives. The resistance to technological change emerged as a barrier among some staff and visitors who were more comfortable with manual procedures. This finding highlights the importance of sustained user training, institutional orientation programs, and effective change management strategies to encourage user adoption, consistent with related studies on biometric-based systems that demonstrate the role of technological enhancements in ensuring effectiveness and user acceptance (Francisco et al., 2025).

Regarding suggested enhancements, respondents proposed several improvements focused on increasing system functionality, security, and administrative efficiency. A frequently mentioned recommendation was the integration of a restricted visitor access feature that would automatically identify and prevent entry for blacklisted individuals or those with prior violations. This feature was viewed as essential for maintaining strict security protocols in managing visits to PDLs. Moreover, many participants expressed the need for specialized monitoring of regular service providers such as lawyers, court officials, and religious workers who require differentiated levels of access. The use of biometric systems to provide customized access and tracking for regular service providers raises ethical concerns related to data privacy

and accountability (Cieslik et al., 2022). Implementing such a system would require robust data protection protocols to maintain user trust and enhance institutional control.

Another widely suggested enhancement was the inclusion of automated alerts for overstaying visitors. This feature would generate real-time notifications if a visitor exceeds their authorized time, allowing prompt administrative action and reinforcing compliance with jail visitation policies. Respondents also advocated for a data restore function to recover accidentally deleted records, which would help preserve data integrity and prevent operational setbacks. These needs align with research that highlights effective data management and the need for robust system support mechanisms in biometric implementation (Akingbade & Adaramola, 2025). Additionally, participants emphasized the importance of a system activity log to track user actions such as login times and data modifications. This feature would reinforce accountability and support internal audits. These suggestions highlight the importance of integrating administrative tools, security protocols, and oversight features to further optimize the AVMS.

The qualitative results indicate that while the AVMS is generally well received, its long-term success depends on addressing technical and institutional challenges. The suggestions for enhancement reflect user needs for greater control, transparency, and operational flexibility, while the reported obstacles point to areas requiring administrative attention and support. Incorporating these insights into future system updates will not only improve the AVMS's functionality but also increase its scalability and sustainability within other correctional facilities nationwide.

5. Conclusion and Implications

The study results strongly validate the potential of biometric-based AVMS to modernize visitor management in correctional and jail facilities like BJMP. The findings confirmed the system's success in addressing key operational challenges in visitor management, such as inefficiency, manual errors, and security vulnerabilities. Through a combination of software development, pilot testing, and user evaluation, the AVMS was proven to be not only functional but also highly satisfactory to its users. The AVMS met all four research objectives by demonstrating high user satisfaction, biometric accuracy, significant improvements in efficiency and security, and valuable insights for enhancement.

These outcomes confirm the system's viability as a secure and effective visitor monitoring solution, while also highlighting areas for refinement and expansion.

Future research is encouraged to expand testing across multiple facilities, compare alternative biometric modalities, and evaluate long term cost effectiveness and integration with national databases. Despite these limitations, the study demonstrates the feasibility and value of digital transformation in correctional administration. The AVMS not only strengthens security and efficiency within the BJMP but also provides a model for broader institutional reform and innovation in correctional management in the Philippines and beyond.

The results of this study carry direct implications for correctional management and public sector digital transformation. For the BJMP, the AVMS offers a scalable solution that can be gradually deployed across facilities to standardize visitor management processes, reduce security risks, and enhance transparency. For policymakers, the findings provide evidence to support investments in digital infrastructure, capacity building programs, and institutional policies that promote biometric based automation in correctional facilities. Furthermore, the study highlights the importance of pairing technology adoption with staff training, technical support, and change management strategies to ensure smooth integration. By addressing these areas, the AVMS can serve as a practical and sustainable tool for strengthening jail operations and supporting broader government efforts toward efficiency, accountability, and secure public service delivery.

Disclosure statement

No potential conflict of interest was reported by the author.

Funding

This work was not supported by any funding.

Institutional Review Board Statement

This study was conducted in accordance with the ethical guidelines set by the Philippine College of Criminology (PCCR) and Bureau of Jail Management and Penology (BJMP). The conduct of this study has been approved and granted ethical clearance by the Philippine College of Criminology Research Ethics Committee.

AI Declaration

The author declares the use of Artificial Intelligence (AI) in writing this paper. In particular, the author used Google Scholar assisted AI tools for searching appropriate literature, identifying relevant references, and summarizing key points. The author takes full responsibility for reviewing, validating, and editing all AI assisted content.

References

Akingbade, L. O., & Adaramola, O. J. (2025). The impacts, benefits and challenges of finger biometrics attendance for students and staff of higher institutions. *International Journal of Research Publication and Reviews, 6*(5), 7858–7862. https://ijrpr.com/uploads/V6ISSUE5/IJRPR45700.pdf

Alrawili, R., AlQahtani, A. A. S., & Khan, M. K. (2024). Comprehensive survey: Biometric user authentication application, evaluation, and discussion. *Computers and Electrical Engineering, 114*, 109485. https://doi.org/10.1016/j.compeleceng.2024.109485

Arulogun, O. T., Olatunbosun, A., Fakolujo, O. A., & Olaniyi, O. M. (2013). RFID-based students attendance management system. *International Journal of Scientific & Engineering Research, 4*(2).

Awotunde, J.B., Sur, S.N., Aderinto, M.T., Gaber, T. (2023). RFID-Based Student Identification Card Attendance Monitoring System. In: Dhar, S., Do, DT., Sur, S.N., Liu, CM. (eds) *Advances in Communication, Devices and Networking. ICCDN 2022. Lecture Notes in Electrical Engineering*, vol 1037. Springer, Singapore. https://doi.org/10.1007/978-981-99-1983-3_4

Baig, S., Geetadhari, K., Noor, M. A., & Sonkar, A. (2022). Face recognition based attendance management system by using machine learning. *International Journal of Multidisciplinary Research and Growth Evaluation, 3*(3), 1–4.

BARS Philippines. (n.d.). *BARS – Barangay automated records solutions.* https://www.bars.com.ph/

Basaligheh, P., & Kothawade, S. (2025). Biometric authentication systems: Advances in security and usability. *International Journal of Recent Advances in Engineering and Technology, 13*(1), 16–19.

Besio, C., & Tacke, V. (2024). Old and new organizational forms in a complex society: A systems theoretical perspective. *Current Sociology Monographs, 72*(1), 143–161. https://doi.org/10.1177/08969205231189472

Biometrics Institute. (2019). *Biometrics and privacy: Issues and challenges.* https://ovic.vic.gov.au/privacy/resources-for-organisations/biometrics-and-privacy-issues-and-challenges/

Castillo, J., Aniag, J., Orbeso, M., & Evale, R. (2025). SDG-driven visitor management and monitoring system for BJMP Baliwag municipal: Enhancing security and efficiency in jail governance. *Journal of Lifestyle and SDGs Review, 5*(3), 1–14. https://doi.org/10.47172/2965-730X.SDGsReview.v5.n03.pe04722

Cieslik, M., Obrecht, A., Sarnowski, J., & Sieber, F. (2022). Digital technology and accountability. *Centre for Humanitarian Action (CHA).* https://www.chaberlin.org/en/publications/digital-technology-and-accountability

Creswell, J. W., & Creswell, J. D. (2018). *Research design: Qualitative, quantitative, and mixed methods approaches* (5th ed.). SAGE Publications.

Department of Justice. (2023, November 6). *Justice sector coordinating council to hold national summit on jail decongestion*. https://www.doj.gov.ph/news_article.html?newsid=dadJmMGnuhvDDDbvqSmmNdcLHunys9hEfIlF9XDGLj0

El-Abed, M., Giot, R., Hemery, B., & Rosenberger, C. (2010). A study of users' acceptance and satisfaction of biometric systems. In *2010 44th Annual IEEE International Carnahan Conference on Security Technology* (pp. 170–178). IEEE. https://doi.org/10.1109/CCST.2010.5678678

Fallahi, M., Ramesh, R., Ramasamy, P. P., Cabarcos, P. A., Strufe, T., & Terhörst, P. (2025). On the reliability of biometric datasets: How much test data ensures reliability? *arXiv:2501.06504*. https://doi.org/10.48550/arXiv.2501.06504

Francisco, A. E., Seraspi, A. L., Guialil, J., & Mata, K. (2025). An enhancement of the Eigenface algorithm using Weber local descriptor applied in attendance management system. *International Student Research Review, 2*(1). https://doi.org/10.53378/isrr.164

Frigillana, K. G., Jocson, J. C., Muldong, R. M. C., Natividad, L. O., & Tiongson, H. T. (2023). The effects of reimplementing a biometric attendance monitoring system in the electronics engineering department at Don Honorio Ventura State University. *Everant Journal, 1*(1), 58–69. https://everant.org/index.php/etj/article/view/1100

Gupta, D. (2024). *Biometrics: Enhancing security in organizations.* IBM Center for The Business of Government. https://www.businessofgovernment.org/sites/default/files/GuptaReport.pdf

Jain, A. K., Ross, A. A., & Flynn, P. J. (2022). *Handbook of biometrics.* Springer. https://content.e-bookshelf.de/media/reading/L-1927-957d45a798.pdf

Jain, A. K., Ross, A., & Nandakumar, K. (2023). *Introduction to biometrics* (2nd ed.). Springer. https://doi.org/10.1007/978-3-031-10911-2

M2SYS Technology. (n.d.). *Biometric case studies: U.S. jails and correctional facilities.* https://www.m2sys.com/case-studies/

Meiramkhanov, T., & Tleubayeva, A. (2024). Enhancing fingerprint recognition systems: Comparative analysis of biometric authentication algorithms and techniques for improved accuracy and reliability. *arXiv*. https://doi.org/10.48550/arXiv.2412.14404

Murthy, M. N., & Katyal, M. (2024). The role of change management in large-scale technology adoption. *International Journal of Research Publication and Reviews, 5*(12), 5934–5942. https://doi.org/10.55248/gengpi.5.1224.0251

Perez, L. P., Palle, R. V., & Adornado, V. V. (2022). The performance of biometric attendance system (BAS): CTU-Tuburan Campus as case study. *International Journal of Scientific and Research Publications (IJSRP),* 12(7). http://dx.doi.org/10.29322/IJSRP.12.07.2022.p12748

Privacy International. (2020). *Responsible use and sharing of biometric data in counter-terrorism.* https://privacyinternational.org/sites/default/files/2020-07/Responsible%20use%20and%20sharing%20of%20biometric%20data%20in%20counter-terrorism.pdf

Rogers, E. M. (2003). *Diffusion of innovations* (5th ed.). Free Press.

Siddiqui, M. M., Valsalan, P., Shajanah, H. A., Baraami, M. S. A., & Baraami, H. S. A. (2024). IoT-based RFID attendance system. In *2024 International Conference on Signal Processing and Advance Research in Computing (SPARC)* (pp. 1–5). IEEE. https://doi.org/10.1109/SPARC61891.2024.10829042

Venkatesh, V., & Bala, H. (2020). Technology acceptance model 3 and a research agenda on interventions. *Decision Sciences, 39*(2), 273–315. https://doi.org/10.1111/j.1540-5915.2008.00192.x

Villaroman, G., San Pedro, A., Bacani, K., Clerigo, E., & Hipos, A. (2018). The use of biometric attendance recording system (BARS) and its impact on the work performance of Cabanatuan City government employees. *Open Access Library Journal*, *5*, 1–10. https://doi.org/10.4236/oalib.1104273

Weick, K. E., Sutcliffe, K. M., & Obstfeld, D. (1999). Organizing for high reliability: Processes of collective mindfulness. In R. I. Sutton & B. M. Staw (Eds.), *Research in organizational behavior* (Vol. 21, pp. 81–123). Elsevier Science/JAI Press.

Yang, W., Wang, S., Hu, J., Zheng, G., & Valli, C. (2019). Security and Accuracy of Fingerprint-Based Biometrics: A Review. *Symmetry*, *11*(2), 141. https://doi.org/10.3390/sym11020141

Yu, Y., Niu, Q., Li, X., Xue, J., Liu, W., & Lin, D. (2023). A review of fingerprint sensors: Mechanism, characteristics, and applications. *Micromachines, 14*(6), 1253. https://doi.org/10.3390/mi14061253

Zakaria, Z. (2025). Face recognition technology: Benefits, applications, and challenges in the modern era. *International Journal of Scientific Research and Management, 13*(03), 2096–2102.