ISSN : 2350-0743

International Journal of Recent Advances in Multidisciplinary Research

Vol. 12, Issue 06, pp.11336-11339, June, 2025

RESEARCH ARTICLE

SMART ACCESS: AN RFID-BASED CAMPUS SYSTEM FOR SECURE GATE ENTRY AND EXIT VERIFICATION

***Joseph Jaymel S. Morpos, Nathalie Grace Poticar, John Mark Cuyos and John Carlo Tijas**

EVSU-Ormoc Campus, Philippines

ARTICLE INFO

Article History

Received 20th March, 2025
Received in revised form
17th April, 2025
Accepted 16th May, 2025
Published online 28th June, 2025

Keywords:

Test Identification parade – Relevancy of evidence- u/s. 7 of BSA- Guidelines issued by the Govt. of Kerala-Identity of person/things-probative value of evidence.

****Corresponding author: Dr. Aliyar M.E.***

ABSTRACT

This study presents the design, development, and implementation of an RFID-based Verification System for managing gate entry and exit at Eastern Visayas State University – Ormoc Campus (EVSU-OC). Addressing the limitations of manual identity verification processes, the system was developed using agile methodology, integrating stakeholder feedback across iterative cycles to enhance usability and functionality. The solution includes RFID-embedded ID cards for students, employees, and temporary cards for vendors and visitors, supported by a web-based interface and centralized database for real-time monitoring. A five-day test implementation was conducted, capturing quantitative and qualitative data from system logs, user interactions, and performance feedback. The system achieved an accuracy rate of 85.56% in verifying identities, with observed delays primarily attributed to internet connectivity issues. Technical refinements such as cooldown mechanisms, loading indicators, and bcrypt encryption were incorporated to improve reliability and security. Despite minor challenges, the system demonstrated effectiveness and adaptability, highlighting its potential as a scalable solution for campus access control.

Citation: Joseph Jaymel S. Morpos, Nathalie Grace Poticar, John Mark Cuyos and John Carlo Tijas. 2025. "Smart Access: An RFID-Based Campus System for Secure Gate Entry and Exit Verification". *International Journal of Recent Advances in Multidisciplinary Research,* 12, (06), 11336-11339.

INTRODUCTION

The manual verification process at Eastern Visayas State University Ormoc Campus is prone to security risks such as campus security breaches and the like, according to Vacca (2007, "both public and private sectors are looking for reliable, accurate, and practical methods for automated verification of identity" (p. 15).). Currently, the verification process at the campus gate is managed by two security personnel out of four security guards on duty. The job of the security personnel includes checking the IDs of students and employees and issuing unique IDs to visitors. As for the canteen, vendors are also provided with a unique ID with vehicle passes. The Head of Security and Public Safety, who falls under the Administrative and Finance Services, manages the school's Security personnel. Maintenance issues, like unplugged appliances, will be reported to the Campus Director. However, regardless of these procedures, there is no digital tool to manage individuals' entry and exit on campus effectively. Since the school is releasing RFID-embedded Identification cards for students and employees, a system that can automatically verify the identities of people entering and exiting the campus premises is needed. RFID technology can provide rapid and accurate identity verification. A manual verification process at EVSU-OC is inefficient, time-consuming, and vulnerable to potential security risks. To minimize these, we proposed developing and implementing an RFID verification system at the entry and exit of EVSU-OC to help improve the overall security of the campus.

METHODOLOGY

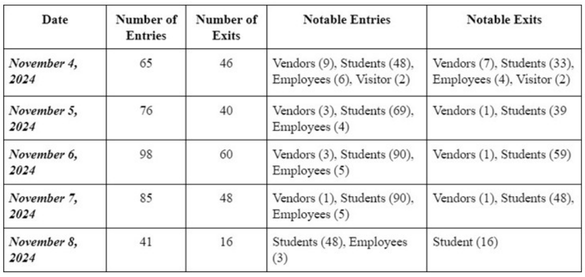
This project was conducted using an action research design due to the nature of how the project was developed. The research was intended to address issues such as the need for a digital verification system at the campus gate to authenticate the identities of individuals entering and exiting the premises. Throughout the project's development, regular meetings were held with department heads and administrators to gather feedback, which was then used to adjust and improve the system accordingly. Ward (2022) stated, "A good maximum sample size is usually around 10% of the population, as long as it does not exceed 1000." In line with this principle, a 10% sample of the 568 students from the Computer Studies Department was selected for the initial testing phase. This decision was made considering the supply office's schedule, prioritizing the distribution of IDs to the said department. A smaller population was targeted to test the system during its early stages effectively. To ensure the timely completion of the system, an Agile methodology was employed for the development process. Regular meetings with system users were conducted throughout the iterative process, and the system was refined after each iteration. These practices collectively produced a high-quality, adaptable, and value-driven final product. The web-based system was developed using PHP, Bootstrap, custom CSS, JavaScript, and integrated libraries such as PHPMailer and Cropper.js. MySQL was utilized as the database platform to store user information securely. An Admin LTE pre-built template was adopted to accelerate development. Additionally, GitHub was used for version control, allowing efficient code backup and update staging. These programming tools were utilized to ensure the system's successful development. Their combined functionalities enabled a reliable, well-designed web application tailored to user needs. Several challenges, however, were encountered during the development phase, including incompatible RFID scanners with newly issued IDs, the absence of suffix fields in the registration module, duplicate entries, and issues with profile image uploads. Upon identification, the programmer immediately addressed these issues to enhance system efficiency. During data collection, informed consent was secured from selected participants through consent letters endorsed by the adviser, noted by the department head, and approved by the Campus Director. Once documentation was completed, participants obtained permission to collect their personal and demographic data for system registration.

Following consent, participant information was encoded into the system. After registration, further approval was obtained for their active participation in the system’s dry run. Before this, the system and required hardware were set up at the guardhouse. Participants were allocated one week to swipe their IDs through the system as part of the testing phase. Participant entry and exit data were recorded during the test implementation using the RFID system. System performance, including reliability and response time under varying internet conditions, was observed. Challenges that arose during the dry run were documented and analyzed. Upon the conclusion of the testing phase, end users' feedback was gathered through interviews. The feedback was analyzed to identify opportunities for system enhancement and improvement.

RESULTS AND DISCUSSION

This chapter presents the data gathered during the system's development and test implementation phases. Quantitative and qualitative findings were derived from system logs, user interactions, and stakeholder feedback. The collected data have been systematically organized into tables and charts to provide a clear and structured understanding of the system’s performance and the outcomes of the RFID-based verification system implementation.

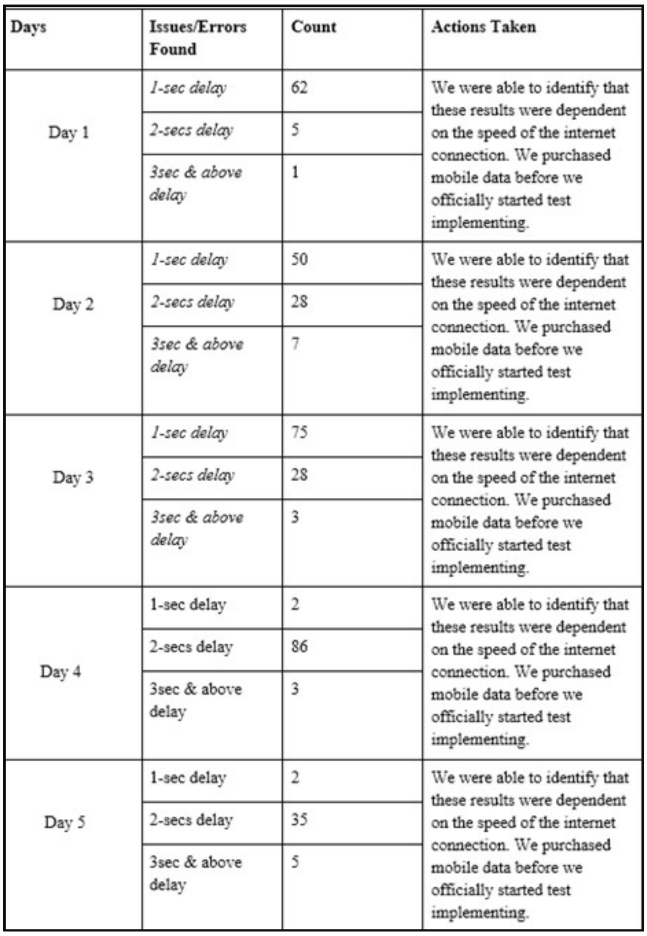
Table 1. Daily Summary of RFID-Based Verification System Logs for Entries and Exits at the Campus Gate



Date	Number of Entries	Number of Exits	Notable Entries	Notable Exits
November 4, 2024	65	46	Vendors (9), Students (48), Employees (6), Visitor (2)	Vendors (7), Students (33), Employees (4), Visitor (2)
November 5, 2024	76	40	Vendors (3), Students (69), Employees (4)	Vendors (1), Students (39
November 6, 2024	98	60	Vendors (3), Students (90), Employees (5)	Vendors (1), Students (59)
November 7, 2024	85	48	Vendors (1), Students (90), Employees (5)	Vendors (1), Students (48),
November 8, 2024	41	16	Students (48), Employees (3)	Student (16)

During the five-day test implementation of the Verification System for campus entry and exit using RFID technology, the system's capability to verify the identities of individuals entering and exiting the campus was demonstrated. Entry and exit logs were generated, showing varying patterns due to data collection being conducted daily from 5:00 AM to 5:00 PM. System accuracy was evaluated by dividing the number of successful verifications by the total number of verification attempts, then multiplying the result by 100.

Table 2. Summary of Identified System Delays and Corresponding Actions Taken During the 5-Day Test Implementation of the RFID- Based Verification System



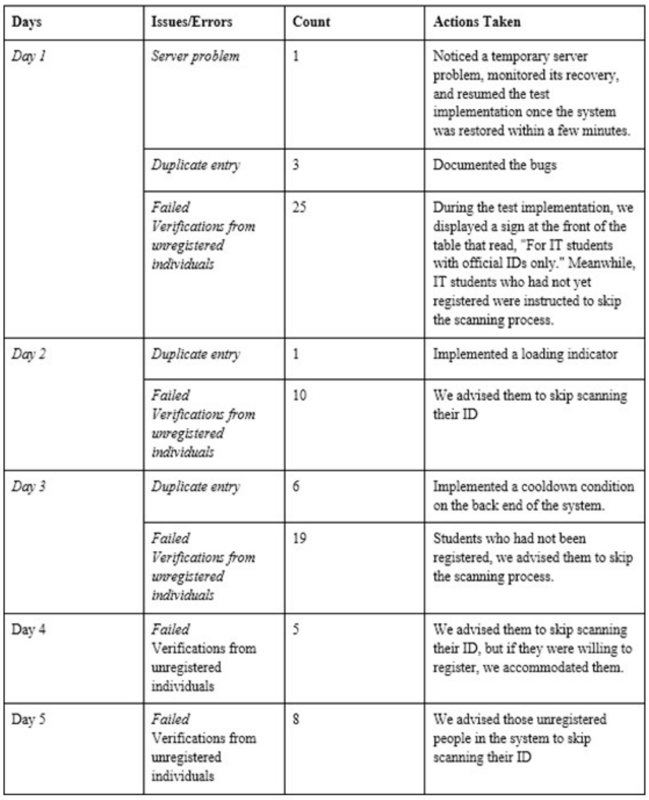
Days	Issues/Errors Found	Count	Actions Taken
Day 1	*1-sec delay*	62	We were able to identify that these results were dependent on the speed of the internet connection. We purchased mobile data before we officially started test implementing.
	2-secs delay	5	
	3sec & above delay	1	
Day 2	*1-sec delay*	50	We were able to identify that these results were dependent on the speed of the internet connection. We purchased mobile data before we officially started test implementing.
	2-secs delay	28	
	3sec & above delay	7	
Day 3	*1-sec delay*	75	We were able to identify that these results were dependent on the speed of the internet connection. We purchased mobile data before we officially started test implementing.
	2-secs delay	28	
	3sec & above delay	3	
Day 4	1-sec delay	2	We were able to identify that these results were dependent on the speed of the internet connection. We purchased mobile data before we officially started test implementing.
	2-secs delay	86	
	3sec & above delay	3	
Day 5	1-sec delay	2	We were able to identify that these results were dependent on the speed of the internet connection. We purchased mobile data before we officially started test implementing.
	2-secs delay	35	
	3sec & above delay	5	

Based on this computation, an accuracy rate of 85.56% was achieved, indicating a generally reliable system performance. However, it was observed that the system's responsiveness was affected by internet connectivity. Specifically, the average response time was recorded at approximately three seconds under a slow connection. To mitigate this issue temporarily, a mobile data backup was provided to support system performance. To address the issue of duplicate entries, a cooldown mechanism and a loading indicator were implemented on the monitor to prevent multiple swipes by the same individual within a short time interval. Additionally, user credentials were encrypted using bcrypt in adherence to industry best practices for data security. Overall, the five-day test implementation validated the system’s effectiveness in verifying identities at campus entry and exit points. The system is expected to enhance campus security with further improvements.

Table 1 presents observed patterns of campus activity, revealing notable discrepancies between recorded entries and exits. On November 4, 2024, 65 entries and 46 exits were recorded, with students comprising the majority of the entries (48). Canteen vendors accounted for nine (9) recorded entries and seven (7) exits in the system's database. Similarly, on November 7, 2024, 85 entries and 48 exits were documented, again showing inconsistencies, particularly among student and vendor records.

The lowest activity was observed on November 8, 2024, with only 41 entries and 16 exits, most of which were attributed to students. These findings indicate that several individuals who entered the campus were not registered as having exited by the 5:00 PM cutoff time for data collection. All data reflected in the table were collected between 5:00 AM and 5:00 PM during each day of the five-day test implementation period.

Table 3. Summary of Verification Attempts, Successful and Failed Verifications, and System Accuracy During Test Implementation

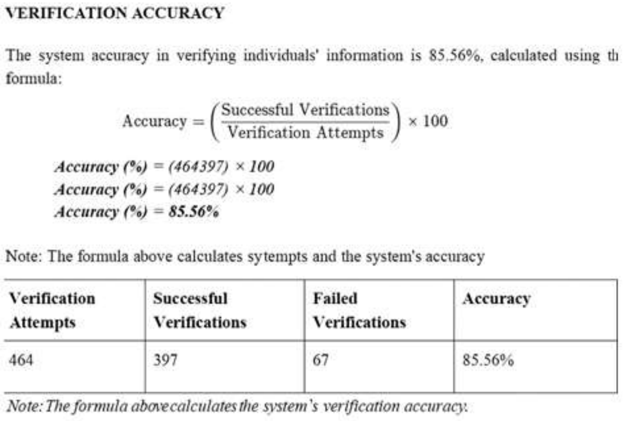


Days	Issues/Errors	Count	Actions Taken
Day 1	*Server problem*	1	Noticed a temporary server problem, monitored its recovery, and resumed the test implementation once the system was restored within a few minutes.
	Duplicate entry	3	Documented the bugs
	Failed Verifications from unregistered individuals	25	During the test implementation, we displayed a sign at the front of the table that read, "For IT students with official IDs only." Meanwhile, IT students who had not yet registered were instructed to skip the scanning process.
Day 2	*Duplicate entry*	1	Implemented a loading indicator
	Failed Verifications from unregistered individuals	10	We advised them to skip scanning their ID
Day 3	*Duplicate entry*	6	Implemented a cooldown condition on the back end of the system.
	Failed Verifications from unregistered individuals	19	Students who had not been registered, we advised them to skip the scanning process.
Day 4	*Failed* Verifications from unregistered individuals	5	We advised them to skip scanning their ID, but if they were willing to register, we accommodated them.
Day 5	*Failed* Verifications from unregistered individuals	8	We advised those unregistered people in the system to skip scanning their ID

Table 2 illustrates the variations in system delays observed over the five-day testing period. Among the recorded delays, 1-second delays were the most prevalent, with the highest occurrence noted on Day 3, where 75 instances were documented. These delays were primarily attributed to fluctuations in internet speed, prompting the acquisition of mobile data as a temporary measure to stabilize system performance.

A notable increase in 2-second delays was observed on Day 4, with 86 instances recorded, while delays of 3 seconds or longer remained relatively infrequent across all testing days. The analysis confirms that the system's response time depended heavily on network conditions. Consequently, it is recommended that further optimization efforts be undertaken to enhance the system's performance and reduce its reliance on internet connectivity.

Table 4. Summary of System Issues Encountered and Corresponding Actions Taken During the 5-Day Test Implementation of the RFID Verification System



VERIFICATION ACCURACY

The system accuracy in verifying individuals' information is 85.56%, calculated using th formula:

$$\text{Accuracy} = \left(\frac{\text{Successful Verifications}}{\text{Verification Attempts}}\right) \times 100$$

Accuracy (%) = (464397) × 100
Accuracy (%) = (464397) × 100
Accuracy (%) = 85.56%

Note: The formula above calculates sytempts and the system's accuracy

Verification Attempts	Successful Verifications	Failed Verifications	Accuracy
464	397	67	85.56%

Note: The formula abovecalculates the system's verification accuracy.

The instant monitoring and verification functions of the RFID system were observed to have performed effectively in confirming and displaying individual information. As shown in Table 3, the system efficiently facilitated rapid identity verification, achieving an accuracy rate of 85.56%, particularly under stable internet conditions. Conversely, reduced internet speed was found to cause delays, with the system taking approximately three seconds or more to display user details. Overall, the system's performance was deemed satisfactory; however, further improvements are recommended to optimize response time across varying network conditions.

Table 4 presents the issues and errors encountered during the five-day test implementation of the system. On Day 1, a temporary server downtime was experienced, slightly affecting system performance. Instances were also noted where students attempted to scan their IDs despite being unregistered in the system. In response, a sign was placed at the verification station stating, "Only students from the Computer Studies Department are advised to scan their IDs before entering the school." Additionally, duplicate entry errors were documented on Day 1 and were addressed before the commencement of testing on Day 2. To improve user interaction, a loading indicator was implemented on Day 2, informing individuals that their data was being processed during ID scanning. As a result of these interventions, the number of unsuccessful verifications and duplicate entries was significantly reduced from Day 3 to Day 5.

CONCLUSION AND RECOMMENDATIONS

The five-day test implementation of the RFID-based Verification System at EVSU–Ormoc Campus demonstrated an 85.56% accuracy rate in verifying campus entries and exits, confirming its effectiveness for access control. Although issues such as internet-dependent delays and duplicate entries arose, they were promptly addressed through system enhancements. To ensure consistent and long-term use, the study recommends providing user training, distributing manuals, conducting regular maintenance, and integrating features like real-time alerts and analytics. These measures aim to improve system reliability, scalability, and institutional value.

REFERENCES

Geethanjali, G., Murthy, A. V., Bhumika, B., & Jagannath. (2023). Dual security-check turnstile using ANPR technology. In 2023 7th International Conference on Design Innovation for 3 Cs Compute Communicate Control (ICDI3C). IEEE.

De la Cruz, J. A., & Diaz, R. A. (2019). Web-based student monitoring system with short message service (SMS)12. International Journal of Advanced Research in Computer Science and Management Studies, 7(6), 8-13.

Vacca, J. R. (2007). Biometric technologies and verification systems. Elsevier Science & Technology.

Simukali, C. M. (2019)Multi factor authentication access control for student and staff based on RFID, barcode and GIS1. University of Zambia. Retrieved from http://dspace.unza.zm/handle/123456789/66232

Vacca, J. R. (2007). Biometric technologies and verification systems. Elsevier Science & Technology.

Smith, R. J. Doe, and A. Johnson, "E-Passport System Using RFID Implants and Microservices Technology to Prevent COVID-19 Spread," in *Proc. 2022 4th Int. Conf. on Cybernetics and Intelligent System (ICORIS)*, Prapat, Indonesia, Oct. 2022, pp. 1-6. IEEE, DOI: 10.1109/ICORIS56080.2022.10031445

Veľas, A., Boroš, M., Kuffa, R., & Lenko, F. (2024). Testing permeability of RFID access control system for the needs of security management. Applied Sciences,14(10),4227. https://doi.org/10.3390/app14104227

Babii, A., & Samila, A. (2023). Dual authentication technique for RFID access control systems with increased level of protection. Systems and Information Security Internet of Things, 1(1). https://doi.org/10.31861/sisiot2023.1.01011

Nanda, I., & De, R. (2022). An integrated campus radio frequency identification system on cloud analysis for improved security. Journal Name, Volume(Issue), Article Number. Available online 23 November 2022

Zare Mehrjerdi, Y. (2011). RFID and its benefits: a multiple case analysis. Assembly Automation, 31(3), 251-262.

Simukali, C. M. (2019)Multi factor authentication access control for student and staff based on RFID, barcode and GIS1. University of Zambia. Retrieved from http://dspace.unza.zm/handle/123456789/6623

Ward, G. (2022, January). “Understanding sample sizes and confidence in predictions. RISC Advisory.” Retrieved from worldoil.com

****