Public Bike Rack Anti-Theft System

Jhasper U. Corpuz., Axel M. Grageda., Gerald F. Manzano., Cazzandra Joyce C. Sagun., Steve A. Villa., Minerva C. Zoleta

Department of Computer Engineering, Eulogio "Amang" Rodriguez Institute of Science and Technology, Manila, Philippines

DOI: https://doi.org/10.47772/IJRISS.2026.10100278

Received: 21 January 2026; Accepted: 26 January 2026; Published: 03 February 2026

ABSTRACT

Security and access control remain critical concerns in shared storage facilities such as schools, barangays, offices, and public institutions. Traditional locker systems rely on mechanical keys or manual supervision, which are prone to loss, duplication, and unauthorized access. This study presents the design and development of an RFID-based smart locker system integrated with GSM SMS notification using an ESP32 microcontroller.

The system employs an RC522 RFID reader for user authentication, a 4×3 matrix keypad for manual input, solenoid locks controlled through relay modules for physical access control, and limit switches to monitor locker door status. An LCD with I2C interface provides real-time system feedback, while a GSM module (SIM800L) sends SMS alerts upon access events. A DC-to-DC buck converter ensures stable voltage regulation for the GSM module.

Experimental testing demonstrated accurate RFID authentication, reliable locking and unlocking mechanisms, responsive keypad input, and successful SMS notifications. The system offers a secure, low-cost, and scalable solution for smart locker applications, enhancing security, monitoring, and user convenience through embedded system integration.

Keywords: Arduino Uno, Embedded Systems, ESP32, RFID, GSM Module, Smart Locker, Access Control

INTRODUCTION

With the increasing demand for secure storage solutions in educational institutions, barangays, and workplaces, there is a growing need for automated access control systems that reduce reliance on physical keys and manual supervision. Conventional lockers are vulnerable to unauthorized access, key duplication, and lack of real-time monitoring.

Recent advancements in embedded systems and wireless communication technologies have enabled the development of smart access control systems that provide improved security, traceability, and user convenience. Technologies such as Radio Frequency Identification (RFID), keypad-based authentication, and Global System for Mobile Communications (GSM) have been widely adopted in modern security applications.

This study proposes an RFID-based smart locker system using an ESP32-WROOM-32 microcontroller. The system authenticates users through RFID cards and keypad input, controls solenoid locks through relay modules, monitors locker door status via limit switches, and sends SMS notifications using a GSM module. An LCD interface provides immediate feedback to users.

Inspired by prior research on embedded safety and automation systems, this project applies similar design principles—sensor integration, wireless communication, and real-time feedback—to a security-oriented application. The proposed system aims to improve locker security while maintaining affordability and ease of implementation.

Review of Related Literature RFID Technology

RFID systems use radio frequency communication to identify authorized users without physical contact. Compared to traditional keys, RFID cards are more secure, faster to authenticate, and easier to manage.

GSM Based Notification Systems

GSM modules enable remote monitoring by sending SMS alerts for security-related events. This feature enhances accountability and allows system administrators to receive real-time access notifications.

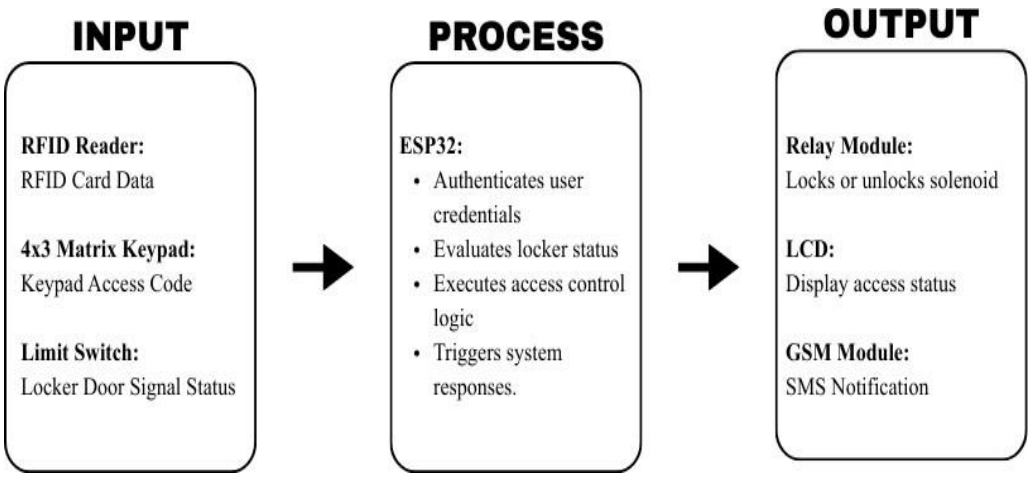
Related Studies

Previous studies have demonstrated the effectiveness of RFID-based access control, GSM-enabled alert systems, and ESP32-based automation platforms. However, many systems focus on single-factor authentication or lack real-time notification. This study integrates multiple authentication inputs and SMS alerts in a unified smart locker system.

Theoretical Framework

This Input-Process-Output (IPO) model illustrates the functional workflow of an automated bike rack or locker system controlled by an ESP32 microcontroller. It outlines how the system gathers data, handles decision-making, and executes physical actions to secure a bicycle.

Figure 1. Input-Process-Output (IPO) Model



The system begins with the Input block, which serves as the interface for data acquisition. It utilizes three primary components to collect necessary information: an RFID Reader that scans card data for user identification, a 4x3 Matrix Keypad where users can manually enter access codes, and a Limit Switch. This switch is crucial for physical feedback, as it monitors the locker door's status to determine if it is currently open or closed. Together, these inputs provide the raw data required for the system to understand who is attempting access and what the current physical state of the locker is.

The Process block acts as the "brain" of the operation, powered by the ESP32 microcontroller. Once the input data is received, the ESP32 performs several logical operations: it authenticates the user's credentials against its database, evaluates whether the locker is currently available or occupied (based on the limit switch data), and executes the specific access control logic programmed into it. This stage is where the system decides whether to grant or deny access, essentially translating digital inputs into actionable commands.

Finally, the Output block carries out the physical and digital responses triggered by the processing stage. To secure or release the bike, the Relay Module activates to lock or unlock a solenoid bolt. Simultaneously, the system provides feedback to the user via an LCD, which displays the current access status (such as "Access

Granted" or "Locker Locked"). For added security and remote monitoring, a GSM Module is used to send an SMS notification to the user or administrator, confirming that the locker has been accessed or secured.

This IPO model ensures systematic handling of user access requests and real-time feedback.

METHODOLOGY

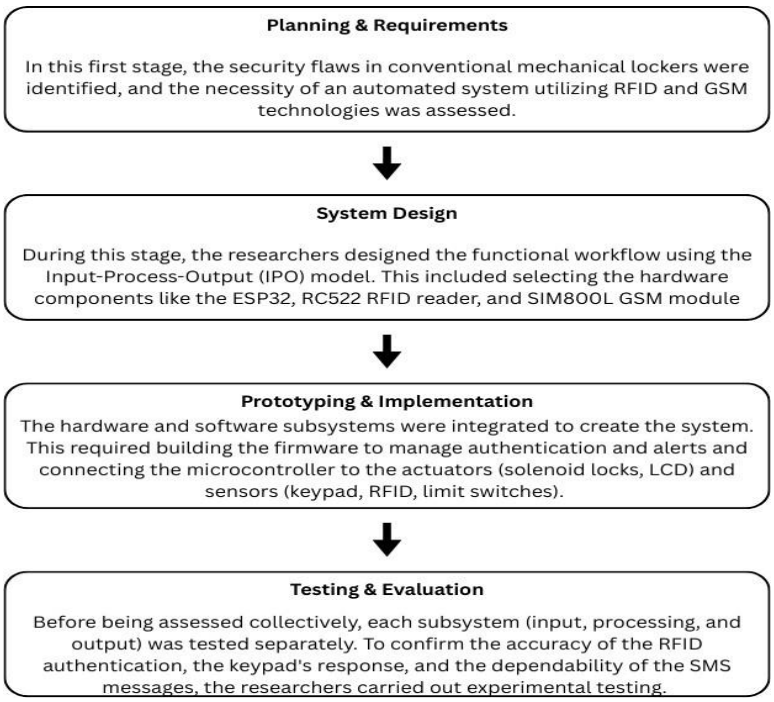
Research Design

This study employed a developmental and experimental research methodology focused on the design, implementation, and evaluation of an RFID-Based Smart Locker System with GSM SMS Notification. The primary goal of the methodology was to ensure that the proposed system is reliable, secure, and practical for use in shared facilities such as schools, barangays, offices, and public institutions. The study integrates embedded system development, hardware–software integration, wireless communication, and functional testing. The system was developed through iterative stages of planning, prototyping, implementation, and evaluation. Each subsystem (input, processing, and output) was tested independently and then as an integrated whole to ensure accuracy, responsiveness, and stability under real-world conditions. The research process followed a structured approach to ensure systematic development and validation of the system. This approach enabled the researchers to evaluate not only the functionality of individual components but also the overall performance of the smart locker in terms of security, usability, and monitoring capability.

System Overview

The Public Bike Rack Anti-Theft System overview outlines a complete security solution intended for public spaces like schools. The device, which is based on the ESP32 microcontroller, uses a 4x3 matrix keypad for manual code entry and an RFID reader for contactless identification in place of conventional mechanical keys. Limit switches are integrated to give real-time feedback on whether the locker door is physically open or closed, and the microcontroller regulates solenoid locks via relay modules to control physical access. A GSM module that is backed by a DC-to-DC buck converter for voltage stability sends SMS messages to users or administrators upon access events, and an LCD provides instantaneous system status for user interaction.

Figure 2. Waterfall Model



The system was developed based on this waterfall model, which is defined by a linear and sequential evolution through four distinct phases. The process starts with Planning & Requirements, when researchers determine the

requirement for an automated solution utilizing RFID and GSM technologies and pinpoint the security flaws in conventional mechanical lockers. This immediately leads to the stage of System Design, which is devoted to choosing certain hardware, such as the SIM800L module and ESP32 microcontroller, and mapping out the functional workflow using an Input-Process-Output (IPO) architecture. Following the completion of the blueprint, the project proceeds to Prototyping & Implementation, where bespoke firmware is coupled with the physical hardware to control mechanical actuators, sensor data, and authentication. The cycle ends with Testing & Evaluation, a demanding stage in which each subsystem such as RFID response and SMS dependability is checked for accuracy before the integrated system as a whole is evaluated to make sure it satisfies the original project objectives.

Hardware and Software Implementation

The hardware architecture for the anti-theft bike rack is centered on a high-performance ESP32 Microcontroller, which serves as the primary processing hub for security logic, user authentication, and communication. To provide a seamless user experience, the system integrates a 16x2 LCD Display for real-time visual feedback and a 4x3 Matrix Keypad for manual PIN-based access. These components work alongside an MFRC522 RFID Module, allowing for a flexible, multi-modal authentication system. When a valid RFID tag or the correct PIN is detected, the ESP32 activates a 5V Relay Module, which acts as an electronic switch to engage a 12V Solenoid Door Lock. This solenoid provides the physical resistance necessary to deadbolt the bicycle frame securely to the rack.

For proactive theft deterrence, the system incorporates Limit Switches to detect unauthorized physical tampering. If the rack is tampered with while the system is armed, the ESP32 triggers an emergency protocol that displays an alarm status on the LCD and dispatches an immediate SMS notification to the owner's mobile device via the SIM800L GSM Module. The system utilizes a dual-input power strategy to maintain operation: a high-capacity 12V source is dedicated exclusively to the solenoid's mechanical requirements, while a separate, regulated 5V DC source is used to power the ESP32, sensors, keypad, and LCD logic. This separation ensures that high-torque mechanical loads do not cause voltage drops that could disrupt the sensitive electronic controllers.

Figure 3. Block Diagram

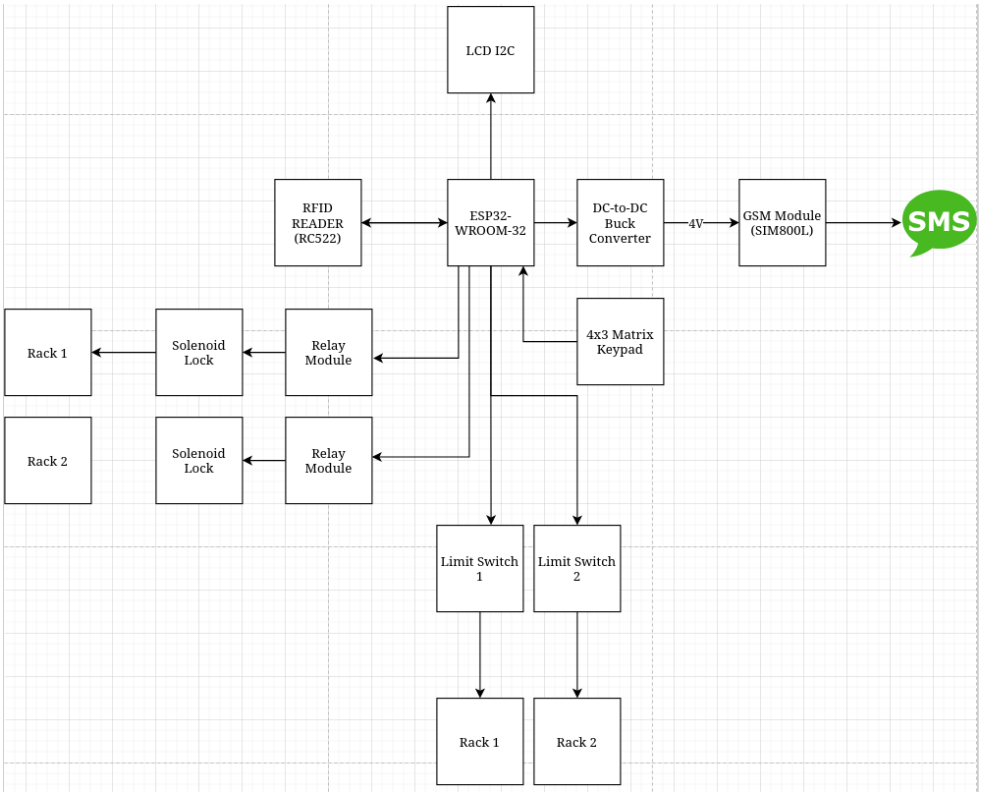
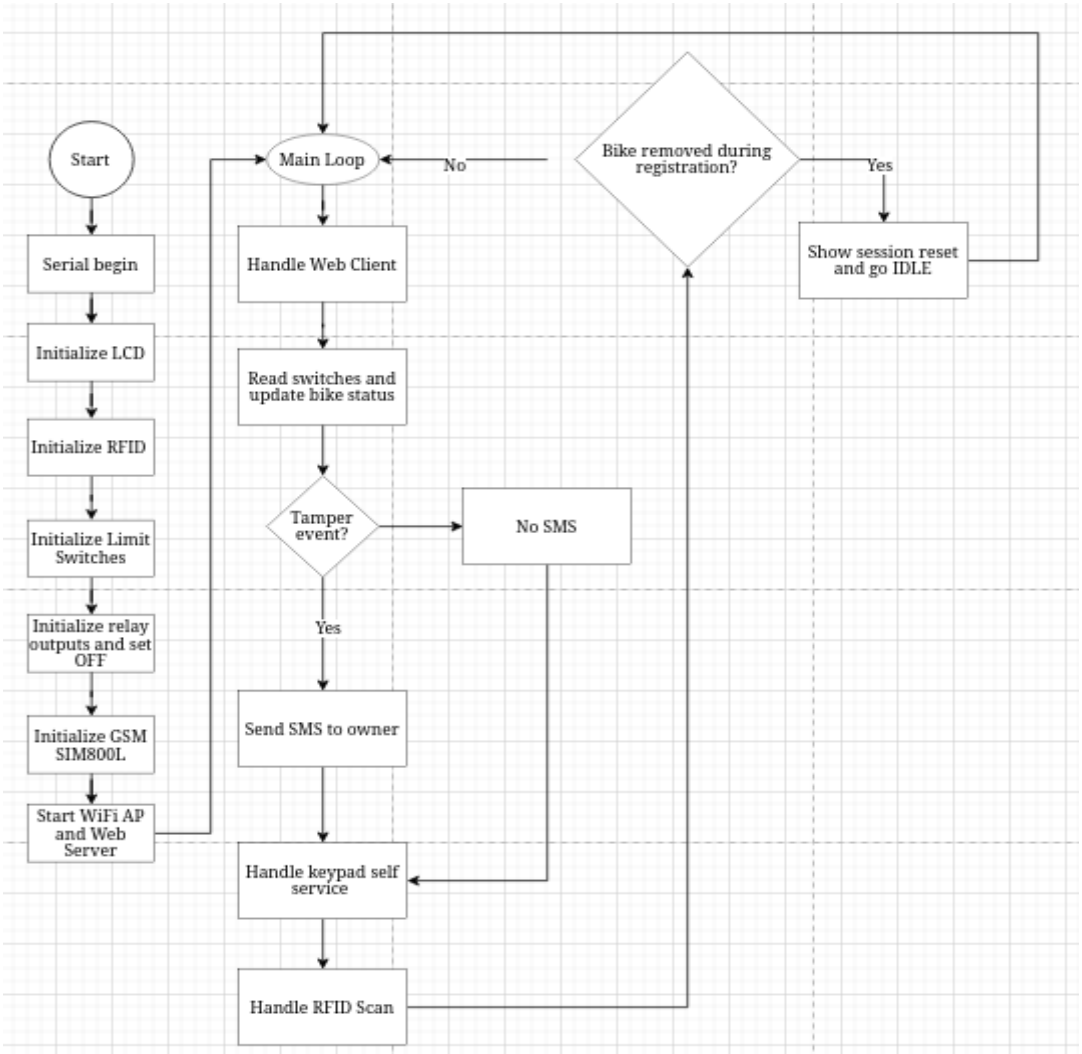


Table 1. Hardware Components

Component	Function	Technical Contribution
ESP32	Main Processor	Coordinates logic between authentication, sensors, and remote alerts.
16x2 LCD	User Interface	Provides real-time visual status and instructions to the user.
MFRC522 RFID	Identity Gateway	Enables secure, contactless authentication using RFID tags.
12V Solenoid	Physical Barrier	Acts as a mechanical deadbolt to lock the bike to the rack.
SIM800L GSM	Remote Link	Sends cellular SMS alerts to the owner during security breaches.
5V Relay Module	Power Switching	Safely triggers the high-voltage solenoid using low-voltage logic.
4x3 Matrix Keypad	Manual PIN Entry	Allows for numeric passcode input as a secondary access method.
Limit Switches	Tamper Detection	Monitors the physical state of the lock to detect forced entry.

Figure 4. Flowchart



This flowchart outlines the operational logic of an automated bike security and management system, beginning with a comprehensive initialization sequence. Upon startup, the system sequentially configures its hardware components, including the serial communication, LCD display, RFID reader, limit switches, and relay outputs.

It then establishes external communication by initializing a GSM SIM800L module for cellular alerts and launching a local WiFi Access Point and web server for user interaction. Once the setup is complete, the system enters a continuous Main Loop that serves as the core processing hub for all real-time events.

Inside this main loop, the system multi-tasks by managing web client requests, reading physical switches to update bike status, and monitoring for security breaches. If a tamper event is detected, the system triggers an immediate SMS notification to the owner; otherwise, it bypasses this step and proceeds to handle manual keypad inputs and RFID scans. A critical safety check is integrated at the end of the cycle to determine if a bike was prematurely removed during the registration process. If a removal is detected, the system displays a session reset notification and reverts to an idle state; if not, it seamlessly returns to the start of the loop to maintain continuous monitoring and service availability.

RESULTS AND DISCUSSION

Table 2. Test Results

Test Condition	Expected Output	Actual Output	Status
Authorized RFID scanned	Locker unlocks	Locker unlocks	Passed
Unauthorized RFID scanned	Access denied	Access denied	Passed
Correct keypad code entered	Locker unlocks	Locker unlocks	Passed
Incorrect keypad code entered	Access denied	Access denied	Passed
Door opened	Limit switch detected	Limit switch detected	Passed
GSM SMS triggered	Message sent	Message sent	Passed
Power fluctuation	System stable	System stable	Passed

The experimental data, as summarized in the testing matrix, confirms that the system achieved a 100% success rate across all primary test conditions. Specifically, the authentication layer demonstrated high precision; the system distinguishes between authorized and unauthorized inputs with total accuracy, ensuring the 12V Solenoid only retracts when valid RFID tags or correct keypad codes are processed by the ESP32. This binary success in "Access Denied" and "Locker Unlocks" states proves the reliability of the dual-modal credential verification system. Beyond user access, the study investigated the system's reactive security protocols through physical and environmental stress tests. The integration of Limit Switches proved effective for tamper detection, as the "Actual Output" consistently matched the "Expected Output" when the door was opened without prior authorization. Furthermore, the SIM800L GSM Module maintained a stable remote link, successfully dispatching SMS alerts during triggered breach events. Crucially, the system remained resilient under power fluctuations, indicating that the dual-rail power distribution strategy provides the necessary stability for both high-torque mechanical loads and sensitive logic circuits. These findings suggest that the hardware architecture is robust enough for deployment in real-world scenarios where security and reliability are paramount.

CONCLUSION

The anti-theft bike rack's development and testing show that a multi-layered hardware design controlled by an ESP32 Microcontroller offers a very dependable bicycle security solution. The study's conclusions verify that combining manual 4x3 Matrix Keypad inputs with contactless MFRC522 RFID offers a strong dual-authentication gateway that successfully blocks unwanted access while preserving user convenience. The rack was successfully converted from a passive storage unit to an active security system thanks to the 12V solenoid's

mechanical integrity and the Limit Switches' real-time monitoring. Additionally, regardless of distance, owners are guaranteed to stay connected to their property thanks to the SIM800L GSM Module's reliable performance in sending SMS notifications. In the end, the system's "Passed" rating under every test condition, including power stability and breach detection, confirms that it is technically sound and prepared for real-world deployment in busy metropolitan settings.

REFERENCES

1. Sankhe, P., & Rodrigues, E. (2018). Smart Backpack. 2018 3rd International Conference for Convergence in Technology (I2CT), Pune, India. https://doi.org/10.1109/I2CT.2018.8529333
2. Tai, N. C., & Hu, S. C. (2017). Development of a natural user interface-based cyclist signaling vest. International Journal of Automation and Smart Technology, 7(4), 157–162. https://doi.org/10.5875/ausmt.v7i4.1342
3. Tsai, P. S., Hu, N. T., Wu, T. F., Chen, J. Y., & Chao, T. H. (2021). Multifunctional Bicycle Helmet Using Internet of Things Technology. Sensors & Materials, 33. https://doi.org/10.18494/SAM.2021.3169
4. Usha, S., Karthik, M., Lalitha, R., Jothibasu, M., & Krishnamoorthy, T. (2021). Automatic turning ON/OFF bike indicator using offline GPS navigation system. IOP Conference Series: Materials Science and Engineering. https://doi.org/10.1088/1757-899X/1055/1/012032
5. Wood, J., Tyrrell, R., Marszalek, R., Lacherez, P., Carberry, T., Chu, B., & King, M. (2010). Cyclist visibility at night: Perceptions of visibility do not necessarily match reality. Journal of the Australasian College of Road Safety, 21(3), 56– https://www.researchgate.net/publication/257927233_Cyclist_visibility_at_night_Perceptions_of_visibility_don't_necessarily_match_reality

ABOUT THE AUTHORS

Jhasper U. Corpuz is a fourth-year Bachelor of Science in Computer Engineering student at the Eulogio "Amang" Rodriguez Institute of Science and Technology (EARIST). He is known for being a hardworking and dedicated student, with academic interests in embedded systems, microcontroller programming, hardware–software integration, and automation technologies. Through his coursework and active participation in system development, he has gained hands-on experience in ESP32-based applications, RFID integration, GSM communication, and electronic circuit implementation, contributing to the successful design, testing, and refinement of the smart locker system.

Andre Axel M. Grageda is a fourth-year Bachelor of Science in Computer Engineering student at the Eulogio "Amang" Rodriguez Institute of Science and Technology (EARIST). He possesses a strong academic interest in system analysis, embedded systems, and the seamless integration of hardware and software. Throughout his collegiate career, he has developed significant expertise in analyzing system behavior, evaluating design logic, and documenting microcontroller-based systems. His contributions have been vital to the project's academic objectives, as he worked to bridge the gap between theoretical computer engineering principles and real-world system functionality through structured analysis and technical documentation.

Gerald F. Manzano is a fourth-year Bachelor of Science in Computer Engineering student at the Eulogio "Amang" Rodriguez Institute of Science and Technology (EARIST). His academic interests include embedded systems, microcontroller programming, hardware–software integration, and automation technologies. Through his coursework and hands-on project development, he has gained practical experience in ESP32-based systems, RFID technology, GSM communication, and electronic circuit design, contributing to the successful development and implementation of the proposed smart locker system.

Cazzandra Joyce C. Sagun is a fourth-year Bachelor of Science in Computer Engineering student at the Eulogio "Amang" Rodriguez Institute of Science and Technology (EARIST). She specializes in technical analysis and documentation, with a strong emphasis on organizing system workflows, methodologies, and performance results. Her role involved reviewing system behavior, refining technical descriptions, and maintaining consistency across project documentation, helping present the system in a clear, logical, and academically sound manner.

Steve A. Villa is a graduating student pursuing a Bachelor of Science in Computer Engineering at the Eulogio "Amang" Rodriguez Institute of Science and Technology (EARIST). He played a major role in the development and implementation of the RFID-Based Smart Locker System with GSM SMS Notification, contributing significantly to the system design, hardware assembly, and firmware development. His academic interests include embedded systems, microcontroller-based system design, access control technologies, and hardware–software integration. Through his coursework and hands-on project development, he has gained practical experience in ESP32 programming, RFID authentication, GSM communication, and automation systems, applying theoretical computer engineering principles to real-world security applications.

Engr. Minerva C. Zoleta, a Professional Computer Engineer, is a dedicated Computer Engineering Professor at the Eulogio "Amang" Rodriguez Institute of Science and Technology in the Philippines, specializing in Embedded Systems, Operating Systems, and Computer Network and Security. With a strong background in academia and industry. She has been instrumental in shaping the next generation of Engineers through innovative teaching methods and hands-on research. Engr. Zoleta holds a Master's degree in Electrical Engineering major in Computer Engineering at Technological University of the Philippines, Manila and is pursuing her doctorate degree in Engineering with specialization in Computer Engineering at Technological Institute of the Philippines. She has presented published research on topics such as Embedded System, IoT applications, and wireless communication international conferences and journals. Passionate about technology-driven solutions, she has led various projects integrating smart systems into real-world applications, contributing to the advancement of local and international engineering communities.