Design and Development of an RFID-Based Anti-Theft Bicycle Lock With Alarm, SMS Notification, and Tile Tracking System

Dwight Baines F. Camposano., Lawrence Airan V. Fajardo., Kenneth George L. Malejana., Mark Reagan Fhae D. Reyes., Chenesa A. Tiboso., Minerva C. Zoleta

Computer Engineering Department, Eulogio "Amang" Rodriguez Institute of Science and Technology, Nagtahan, Sampaloc, Manila, 1016 Philippines

DOI: https://doi.org/10.51244/IJRSI.2026.13010072

Received: 14 January 2026; Accepted: 19 January 2026; Published: 31 January 2026

ABSTRACT

Bicycle theft remains a significant concern in urban and academic environments, creating a demand for reliable and intelligent security solutions. This study presents the design and development of an RFID-Based Anti-Theft Bicycle Lock system that integrates electronic authentication, motion and vibration detection, alarm mechanisms, SMS notification, and Tile-based tracking. The system is built around an Arduino Nano microcontroller, utilizing an RFID RC522 module for secure access verification, an MPU-6050 sensor for detecting unauthorized movement, and a solenoid lock for physical locking control. Visual and audible alerts are provided through an RGB LED and an active buzzer, while real-time SMS notifications are delivered to the bicycle owner using a SIM800L GSM module. In the event of unauthorized access or suspicious movement, the Tile tracker allows the bicycle to be located through a smartphone application.

The prototype was evaluated through controlled testing scenarios to assess authentication accuracy, motion detection reliability, alert responsiveness, and power management performance. Test results indicate that the system consistently permits access only to authorized RFID credentials and promptly activates security responses during unauthorized access attempts or abnormal motion events. The inclusion of a backup power source ensures continued operation during main power interruptions, enhancing system dependability. The results demonstrate that the developed system offers a practical, low-cost, and multi-layered approach to bicycle security, providing improved theft prevention and user awareness suitable for real-world application.

Keywords: Anti-Theft Bicycle Lock, RFID, Arduino Nano, Tile Tracking, GSM-Based SMS Alert

INTRODUCTION

Bicycle theft remains a widespread problem, particularly in urban areas and school communities where bicycles are commonly used for daily transportation. Conventional bicycle locks, such as chains and mechanical padlocks, are often vulnerable to cutting, forced removal, and unauthorized manipulation. These weaknesses lead to frequent theft incidents, financial loss, and reduced confidence among bicycle owners.

Traditional bicycle locking mechanisms rely solely on physical protection and user vigilance. Without electronic authentication, motion detection, or alert mechanisms, these systems are unable to respond to unauthorized access in real time. The absence of alarms, visual indicators, and remote notifications allows theft attempts to go unnoticed, emphasizing the need for an intelligent and responsive bicycle security system.

Advancements in embedded systems have enabled the integration of access control, sensing, and wireless communication into compact devices. RFID technology provides secure user authentication, while motion and vibration sensors enable real-time detection of tampering. However, many existing solutions lack a comprehensive approach that combines theft detection, immediate alerting, post-theft tracking, and reliable power continuity.

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue I January 2026

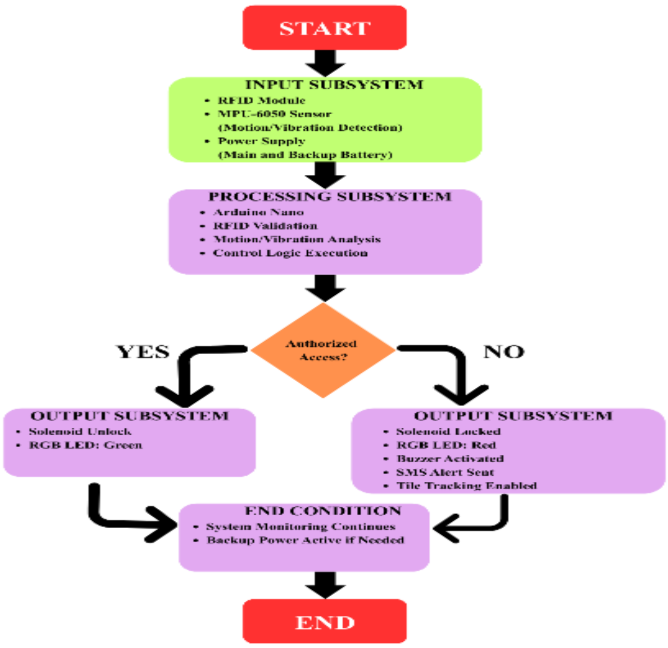
This study presents the design and development of an RFID-Based Anti-Theft Bicycle Lock with Alarm, SMS Notification, and Tile Tracking System. The prototype utilizes an Arduino Nano, RFID authentication, an MPU-6050 motion sensor, buzzer, RGB LED indicators, and a solenoid lock to prevent unauthorized access. When a security threat is detected, the system activates an alarm, sends an SMS alert through a GSM module, and provides visual warnings. If the lock is compromised, a Tile tracker allows the bicycle to be located after theft. In addition, the system incorporates a rechargeable backup power supply that operates alongside the main battery, ensuring continuous functionality and allowing the bicycle to be safely unlocked even in the event of main power loss. This multi-layered prototype demonstrates a practical and low-cost approach to improving bicycle security.

REVIEW OF RELEVANT THEORY, STUDIES, AND LITERATURE

Theoretical Framework

The theoretical framework establishes the scientific and engineering principles that guide the design, operation, and evaluation of the RFID-Based Anti-Theft Bicycle Lock with Alarm, SMS Notification, and Tile Tracking System. The system integrates radio frequency identification for access control, inertial sensing for motion and vibration detection using the MPU-6050 sensor, microcontroller-based processing through the Arduino Nano, wireless GSM communication for SMS alerts, electromechanical locking using a solenoid, and a dual power supply with a rechargeable backup battery to ensure continuous operation and enhanced bicycle security.

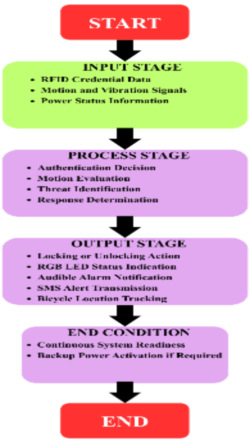
Figure 1. System Theory



Systems Theory explains that a system functions through the interaction of interconnected components working together to achieve a common goal. In the RFID-Based Anti-Theft Bicycle Lock with Alarm, SMS Notification, and Tile Tracking System, the system is composed of multiple subsystems including the RFID module, MPU-6050 sensor, Arduino Nano microcontroller, solenoid lock, buzzer, RGB LED indicator, SIM800L GSM module, Tile tracker, and a main and backup power supply. Each component performs a specific function, but effective bicycle theft prevention is achieved only when all subsystems operate cohesively. The RFID module and motion sensor serve as input sources, the Arduino Nano processes authentication and motion data, and the output components execute locking actions, alarms, visual indicators, SMS notifications, and tracking functions. This theory supports the system architecture by emphasizing the coordination of inputs, processes, and outputs to ensure reliable and secure bicycle operation.

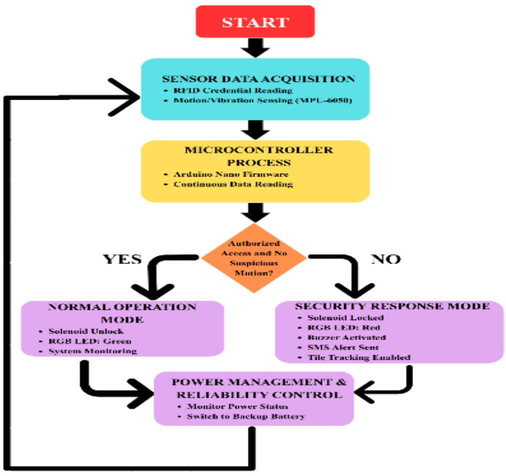
ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue I January 2026

Figure 2. Input–Process–Output (IPO) Model



The Input–Process–Output (IPO) model illustrates how information flows through the RFID-Based Anti-Theft Bicycle Lock system to perform its security functions. In the input stage, the system collects data from the RFID module for user authentication, motion and vibration signals from the MPU-6050 sensor for tamper detection, and power status information from both the main and backup power sources. During the process stage, the Arduino Nano analyzes the received data, verifies access credentials, evaluates motion conditions, and decides whether a security response is required. In the output stage, the system controls the solenoid lock, displays system status through the RGB LED, activates the buzzer during unauthorized access, transmits SMS alerts to the owner, and supports bicycle tracking through the Tile tracker. This model demonstrates how the system delivers timely and reliable responses to potential theft scenarios while maintaining continuous operation.

Figure 3. Embedded Systems Theory

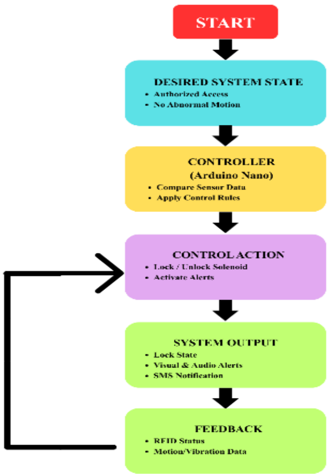


Embedded Systems Theory explains that microcontroller-based systems are designed to carry out specific functions through continuous sensing, real-time processing, and direct control of hardware components. In the RFID-Based Anti-Theft Bicycle Lock system, the Arduino Nano serves as the embedded controller that constantly monitors RFID authentication data and motion or vibration signals from the MPU-6050 sensor, and executes security control logic accordingly. The microcontroller operates in a continuous loop, enabling immediate detection of unauthorized access or abnormal movement and allowing rapid activation of locking,

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue I January 2026

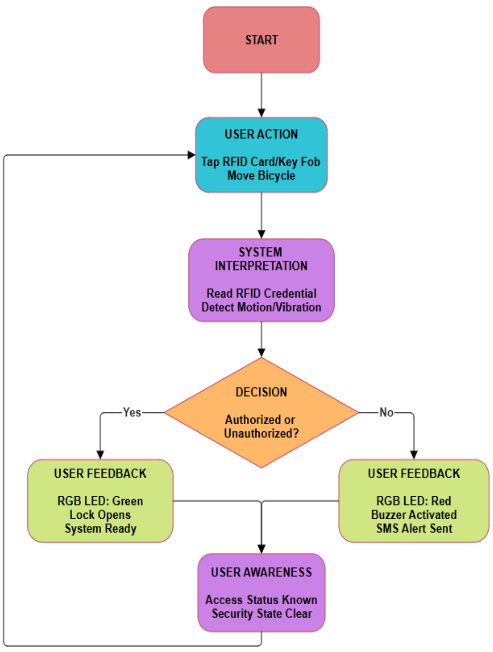
alert, and notification mechanisms. This theory emphasizes the system's ability to provide timely security responses, autonomous operation, and reliable performance through the close integration of software routines and hardware components.

Figure 4. Control Systems Theory



Control Systems Theory explains how systems regulate their behavior by continuously comparing actual conditions with a desired state and applying corrective actions through feedback mechanisms. In the RFID-Based Anti-Theft Bicycle Lock system, the desired system state is defined as authorized access with no abnormal motion detected. The Arduino Nano functions as the controller that evaluates RFID authentication results and motion or vibration data against predefined control conditions and applies appropriate control rules. Based on this evaluation, the system executes control actions such as locking or unlocking the solenoid and activating visual, audio, and notification alerts. The resulting system outputs, including lock status and alert responses, are continuously monitored and fed back through updated RFID and motion data. This closed-loop control structure enables automatic correction of system behavior, ensuring timely security responses, stable operation, and reliable control of the bicycle locking mechanism.

Figure 5. Human–Computer Interaction (HCI)



Human–Computer Interaction (HCI) focuses on how users interact with a system and how the system communicates its status in a clear and intuitive manner. In the RFID-Based Anti-Theft Bicycle Lock system, user interaction begins when the user taps an RFID card or key fob or attempts to move the bicycle. The system interprets these actions by reading the RFID credential and detecting motion or vibration, after which a decision is made to determine whether access is authorized or unauthorized. The system then provides immediate feedback to the user through visual, audible, and notification cues. A green RGB LED and unlocked state indicate successful authorization, while a red RGB LED, buzzer activation, SMS alert, and Tile-based tracking notification signal unauthorized access or suspicious activity. This feedback informs user awareness by clearly conveying the current access and security status and enabling the owner to locate the bicycle using the Tile tracker when necessary. By looping user awareness back into user action, the interaction design improves usability, enhances situational awareness, and supports effective response to potential theft incidents.

Framework Summary

The RFID-Based Anti-Theft Bicycle Lock system is grounded in Systems Theory and the Input–Process–Output (IPO) Model to define the overall system structure and functional flow. Embedded Systems Theory supports real-time processing, continuous monitoring, and hardware–software integration through the use of a microcontroller-based design. Control Systems Theory is applied to regulate system behavior using feedback mechanisms that ensure stable operation and timely security responses to unauthorized access or motion. Human–Computer Interaction (HCI) principles guide the design of clear and intuitive user interactions through visual, audible, and notification-based feedback, including RFID access, RGB indicators, alarms, SMS alerts, and Tile-based tracking. Collectively, these theoretical frameworks support the development of a functional, reliable, and user-centered anti-theft bicycle locking system.

RELATED LITERATURE

RFID-Based Bicycle Locking Systems

Research conducted by Han et al. (2017) demonstrated the effectiveness of RFID technology for securing bicycles through electronic locking mechanisms. Their study showed that RFID-based authentication enables reliable control of locking and unlocking actions while reducing dependence on traditional mechanical locks. The integration of alarm functionality during forced tampering further enhanced system security. These findings support the use of RFID authentication as a core component in bicycle anti-theft systems to improve access control and theft deterrence.

Arduino-Based Bicycle Security Applications

Studies on Arduino-controlled bicycle security systems highlight the practicality of microcontroller-based designs for managing access control and security logic. Patil et al. (2018) emphasized that Arduino platforms offer low-cost implementation, ease of integration, and flexibility for incorporating RFID authentication and alert mechanisms. Their work demonstrated that microcontroller-based systems are well-suited for prototype-level bicycle security applications, validating the use of an Arduino Nano for processing RFID credentials and coordinating system responses.

Advanced RFID Security with Alarm Integration

Recent work by Raj et al. (2024) emphasized the importance of combining RFID authentication with alarm mechanisms in bicycle security systems. Their findings revealed that immediate audio and visual alerts significantly improve theft prevention by drawing attention to unauthorized access attempts. This supports the integration of buzzer alarms and RGB LED indicators as essential feedback components in RFID-based bicycle locks.

Motion and Vibration-Based Theft Detection

Kor et al. (2023) explored the use of motion and vibration sensing in bicycle anti-theft systems through IoT-based implementations. Their research demonstrated that abnormal movement detection is effective in identifying theft attempts even when physical locking mechanisms are compromised. The study supports the use of motion and vibration sensors, such as inertial measurement units, to enable real-time detection of tampering and unauthorized bicycle movement.

Tracking and Backup Power in Bicycle Anti-Theft Systems

Sawant et al. (2019) highlighted the importance of tracking and power redundancy in enhancing bicycle anti-theft solutions. Their system employed wireless communication technologies to monitor bicycle movement and notify users of unauthorized access. The inclusion of a backup power source ensured continuous system operation during power interruptions. These findings support the integration of tracking solutions and rechargeable backup batteries to improve system reliability and post-theft recovery in bicycle security systems.

Table 1. Comparison Matrix of Related Studies and Current Research

Study	Sensor(s) Used	Platform / Technology	Key Feature(s)	Gap Addressed by This Study
Han et al. (2017)	RFID reader	Microcontroller-based system	Electronic bicycle lock using RFID authentication	Does not include motion or vibration sensing, SMS alert, or tracking capability
Patil et al. (2018)	RFID reader	Arduino-based system	Smart bicycle security with RFID access control	Lacks motion or vibration detection and remote user notification
Sawant et al. (2019)	GPS module, vibration sensor	Arduino + IoT + GSM	Real-time bicycle tracking and theft alert system	Does not integrate RFID-based access authentication
Kor et al. (2023)	Accelerometer-based motion sensor	IoT-based platform	Motion-based theft detection and alerting	No electronic locking mechanism or user access control
Raj et al. (2024)	RFID reader	Arduino-based system	RFID-based security with alarm activation	No backup power source or location tracking integration
Current Study (RFID-Based Anti-Theft Bicycle Lock System)	RFID module, MPU-6050 (accelerometer & gyroscope)	Arduino Nano + GSM + Tile tracker	RFID access control, motion/vibration detection, alarm, SMS alert, tracking, backup power	Integrates access control, motion sensing, alerting, tracking, and power redundancy in one system

METHODOLOGY

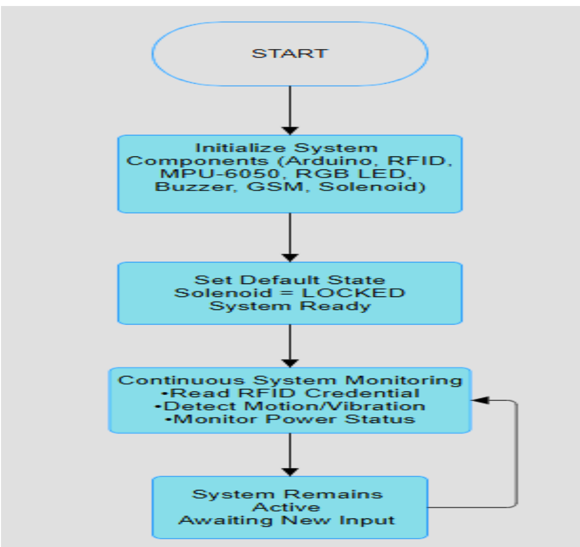
This study employed a developmental and experimental research design to design, implement, and evaluate an RFID-Based Anti-Theft Bicycle Lock system with alarm, notification, and tracking features. The prototype was developed using an Arduino Nano microcontroller as the main control unit, integrating an RFID module for access authentication, an MPU-6050 sensor for motion and vibration detection, a solenoid lock for physical locking, and alert components including a buzzer and RGB LED for system status indication. A SIM800L GSM module was incorporated to enable SMS notifications, while a Tile tracker was embedded to support post-theft bicycle location tracking. The system was powered by a primary power source with an additional rechargeable backup battery to ensure continued operation during power interruptions.

The system was assembled and programmed to continuously monitor RFID credentials and motion data from the MPU-6050 sensor. When a valid RFID credential was detected, the system granted access by unlocking the solenoid and activating a green LED indicator. If an invalid RFID credential or abnormal motion or vibration was detected, the system initiated a security response by keeping the lock engaged, activating the buzzer, switching the RGB LED to red, and sending an SMS alert to the bicycle owner. Testing was conducted under controlled conditions to evaluate authentication accuracy, motion detection sensitivity, alert responsiveness, and power reliability. This methodology enabled systematic assessment of the system's effectiveness in preventing unauthorized access, providing timely alerts, and enhancing overall bicycle security.

Figure 6. Waterfall Model

A sequential development methodology was used in this study to guide the systematic creation and evaluation of the RFID-Based Anti-Theft Bicycle Lock system. The process began with identifying essential system requirements, including secure RFID authentication, detection of unauthorized motion or vibration, alert generation, SMS notification, tracking support, and reliable power management. Based on these requirements, the system architecture and operational logic were designed to coordinate the Arduino Nano with the RFID module, MPU-6050 sensor, solenoid lock, alert devices, and communication modules. The implementation stage involved assembling the hardware components and developing firmware to manage access control, motion analysis, alert responses, and power switching. The final stage focused on controlled testing to evaluate system functionality, responsiveness, and reliability, ensuring that the prototype performed effectively as an anti-theft bicycle security system.

Figure 7. Flow Chart



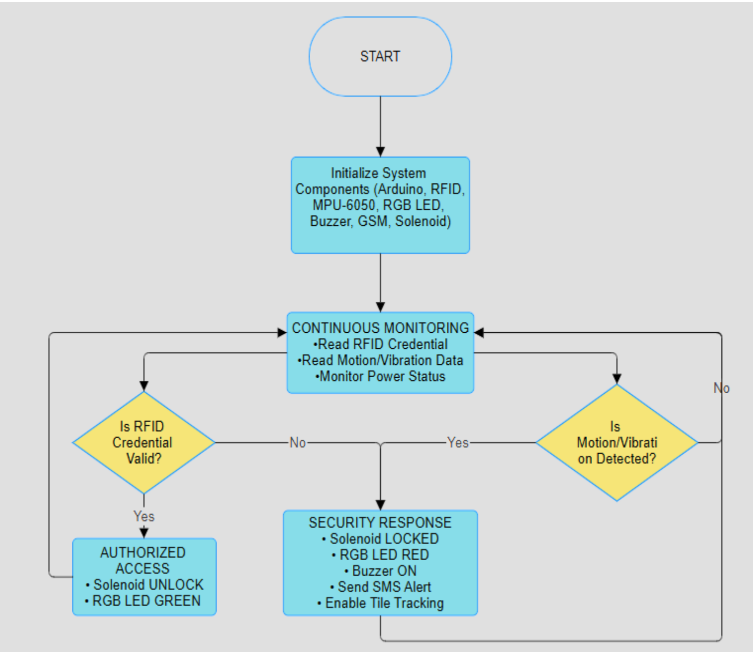
It presents the overall operational flow of the RFID-Based Anti-Theft Bicycle Lock system, illustrating how the system processes user interaction and sensor data to maintain bicycle security. The flow begins with system initialization, where the Arduino Nano activates the RFID module, MPU-6050 motion and vibration sensor,

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue I January 2026

solenoid lock, RGB LED, buzzer, GSM module, and power supply. After initialization, the system enters a continuous monitoring state in which it repeatedly checks for RFID authentication attempts, detects motion or vibration, and monitors power availability.

When a valid RFID credential is detected and no abnormal motion is sensed, the system grants authorized access by unlocking the solenoid and illuminating the RGB LED in green. If an invalid RFID credential is detected or if motion or vibration is identified, the system immediately initiates a security response by keeping the lock engaged, activating the buzzer, switching the RGB LED to red, and sending an SMS alert to the bicycle owner, while enabling tracking support. This operational flow runs continuously without termination, ensuring real-time monitoring, rapid response to unauthorized access, and consistent protection of the bicycle.

Figure 8. System Logic Flow Chart



It illustrates the detailed decision-making logic implemented in the RFID-Based Anti-Theft Bicycle Lock system to regulate access and security responses based on real-time authentication and motion data. After initialization, the Arduino Nano continuously monitors RFID credentials and motion or vibration readings from the MPU-6050 sensor to determine whether access should be granted or restricted. When a valid RFID credential is detected and no abnormal motion is present, the system unlocks the solenoid and activates the green RGB LED to indicate authorized access.

If an invalid RFID credential is detected or if motion or vibration is sensed without authorization, the system immediately enters a security state. In this state, the solenoid remains locked, the RGB LED switches to red, the buzzer is activated, and an SMS alert is sent to the bicycle owner, while tracking support is enabled. This structured logic ensures that the bicycle can only be unlocked under authorized conditions and that unauthorized movement is promptly detected and addressed. The continuous monitoring loop allows the system to respond instantly to changes in system conditions, enhancing overall reliability and user safety.

Figure 9. Schematic Diagram

RESULTS & DISCUSSION

The RFID-Based Anti-Theft Bicycle Lock system successfully processed RFID authentication and motion or vibration data in real time during testing. The RFID module consistently read credentials and transmitted the data to the Arduino Nano, enabling immediate system decisions. When a valid RFID credential was detected, the solenoid lock disengaged and the RGB LED illuminated green, indicating authorized access. This behavior was observed consistently across repeated test trials.

During unauthorized access attempts or when motion or vibration was detected by the MPU-6050 sensor without valid authentication, the system maintained the locked state of the solenoid and activated its security mechanisms. The RGB LED switched to red, the buzzer generated an audible alert, and an SMS notification was successfully sent to the bicycle owner. In addition, the Tile tracker embedded in the bicycle enabled location tracking through the Tile mobile application installed on the user's smartphone. This allowed the user to view the bicycle's last known location and initiate tracking when a security event occurred. These responses were triggered promptly and consistently during testing, demonstrating effective coordination between access control, alert mechanisms, and user-accessible tracking for enhanced bicycle security.

Requirements

The functional requirements of the RFID-Based Anti-Theft Bicycle Lock system focus on its security and access control capabilities. The system continuously monitors RFID credentials and motion or vibration data using the RFID module and MPU-6050 sensor to detect authorized access and potential theft attempts in real time. Unlocking of the bicycle is permitted only when a valid RFID card or key fob is detected and no abnormal motion is present. When unauthorized access or suspicious movement is identified, the system automatically maintains the locked state of the solenoid, activates the buzzer, switches the RGB LED to red, sends an SMS alert to the bicycle owner, and enables Tile-based tracking for location monitoring through the user's smartphone. Visual feedback is provided through RGB LED indicators, with green indicating authorized access and red signaling a security alert. All system logic and decision-making processes are implemented using microcontroller-based programming to ensure structured and reliable operation.

The non-functional requirements define the performance, reliability, and usability characteristics of the system. The bicycle lock is designed to operate with real-time responsiveness, ensuring immediate reaction to authentication attempts and motion detection events. System safety is prioritized by enforcing automatic lock control and alert activation without requiring user intervention during unauthorized access. The system provides stable and consistent feedback through visual, audible, and notification mechanisms without noticeable delay. Power reliability is supported through continuous power status monitoring and the use of a rechargeable backup battery to maintain functionality during main power loss. Measurement and detection accuracy are ensured by consistent sensor readings, while system components operate reliably under programmed conditions to maintain effective and dependable bicycle security.

Table 2. Variables and Conditions of RFID-Based Anti-Theft Bicycle Lock System

Variable / Component	Type (Input / Output)	Parameter Measured / Controlled	Condition or Range	System Response / Action
Arduino Nano (ATmega328P)	Microcontroller	System logic and control execution	Operates at 5 V, continuous loop	Reads inputs, evaluates conditions, controls solenoid, LEDs, buzzer, GSM, and power switching
RFID Module (RC522)	Input	RFID credential data	Valid / Invalid UID	Grants or denies access based on authentication result
RFID Card / Key Fob (MIFARE)	Input	Unique identification code	Authorized / Unauthorized	Triggers access decision in microcontroller
MPU-6050 Sensor	Input	Motion and vibration data	Motion detected / No motion	Activates security response when abnormal movement is detected

Solenoid Lock	Output	Locking mechanism state	Locked / Unlocked	Unlocks for authorized access, remains locked during security events
Relay Module	Output	High-voltage switching control	ON / OFF (5 V control)	Controls 12 V supply to solenoid lock
RGB LED (Common Cathode)	Output	Visual status indication	Green / Red	Displays system status (access granted or alert condition)
Active Buzzer	Output	Audible alert signal	ON / OFF	Sounds alarm during unauthorized access or motion detection
GSM Module (SIM800L)	Output	SMS alert transmission	Network available	Sends alert notification to bicycle owner
Tile Tracker	Output (Tracking)	Bicycle location data	Bluetooth range / Last known location	Allows user to track bicycle location using smartphone application
Main Battery Pack	Power Source	Primary system power	16 V supply	Powers the entire system during normal operation
Backup Battery	Power Source	Emergency power supply	9 V supply	Maintains system operation during main power loss
Buck Converter (16 V → 12 V)	Power Regulation	Voltage conversion	12 V output	Supplies regulated power to solenoid lock
Buck Converter (16 V → 5 V)	Power Regulation	Voltage conversion	5 V output	Powers microcontroller, relay, LED, and buzzer
Buck Converter (5 V → 4 V)	Power Regulation	Voltage conversion	~4 V output	Supplies stable voltage to GSM module

Table 3. Variables and Conditions of RFID-Based Anti-Theft Bicycle Lock System

Test #	Input Condition	Observed Output	Expected Output	Pass / Fail	Remarks / Behavior Explanation
1	No RFID presented, no motion detected	Solenoid remains locked, RGB LED OFF, buzzer OFF	System remains in monitoring state	Pass	System correctly waits for valid input
2	Valid RFID credential presented	Solenoid unlocks, RGB LED turns GREEN	Authorized access granted	Pass	Authentication functions correctly
3	Invalid RFID credential presented	Solenoid remains locked, RGB LED turns RED, buzzer ON	Security response activated	Pass	Unauthorized access detected

4	Motion/vibration detected without valid RFID	Solenoid locked, buzzer ON, RGB LED RED	Theft alert triggered	Pass	Motion detection works as intended
5	Invalid RFID + motion detected	Solenoid locked, buzzer ON, SMS alert sent	Full security response activated	Pass	Combined threat handled correctly
6	SMS network available during alert	SMS successfully sent to owner	Owner notified	Pass	GSM module operates reliably
7	Security event triggered	Tile tracker accessible via smartphone app	Bicycle location available	Pass	Tracking function supports recovery
8	Valid RFID after alert	Solenoid unlocks, RGB LED GREEN	System returns to normal state	Pass	Recovery from alert works correctly
9	Main power disconnected	System switches to backup battery	Continued operation maintained	Pass	Backup power functions correctly
10	Power restored	System resumes normal operation	Safe restart behavior	Pass	System stability confirmed

The results demonstrate that the RFID-Based Anti-Theft Bicycle Lock system effectively enforces security rules by prioritizing authentication and motion-based decision logic over unauthorized user actions. The consistent unlocking of the solenoid only when a valid RFID credential is detected, combined with immediate locking and alert activation during unauthorized access or suspicious movement, reflects correct implementation of the system logic. This behavior confirms that access control and theft detection mechanisms operate as intended under defined conditions.

The rapid response of the RGB LED indicators, buzzer, SMS notifications, and Tile-based tracking aligns with control and embedded systems principles, where continuous monitoring and timely feedback are essential for system stability and reliability. The system successfully informs the user through visual, audible, and mobile-based alerts, improving awareness and enabling location tracking through a smartphone during security events. These outcomes are consistent with findings in related studies on sensor-based security and microcontroller-driven access control systems.

Furthermore, the structured program logic and modular hardware design contribute to system reliability and ease of implementation. The integration of authentication, motion detection, alert generation, and tracking demonstrates that low-cost embedded components can be combined to produce a practical and responsive bicycle security solution. The results confirm the feasibility of the prototype for real-world application and provide a strong foundation for further enhancement and deployment.

CONCLUSION AND RECOMMENDATIONS

The RFID-Based Anti-Theft Bicycle Lock system successfully achieved its primary objective of enhancing bicycle security through electronic access control, motion detection, and real-time alert mechanisms. The integration of RFID authentication, MPU-6050 motion sensing, solenoid locking, visual and audible indicators, SMS notifications, and Tile-based tracking enabled the system to reliably distinguish between authorized access and potential theft attempts. The consistent system response observed during testing demonstrates that the control logic effectively enforces security rules and provides immediate feedback to the user.

The system exhibited reliable performance in detecting unauthorized access and abnormal motion, with timely activation of alarms, notifications, and tracking features. The use of layered security mechanisms improved user awareness and strengthened protection against theft. The inclusion of a backup power source further enhanced system reliability by ensuring continued operation during main power interruptions. These results confirm that the prototype is functional, practical, and suitable for real-world bicycle security applications.

Based on the findings of this study, several improvements are recommended for future development. Implementing a fully enclosed and weather-resistant housing would improve durability for outdoor use. Enhancing mobile integration through a dedicated application could provide more detailed alerts and control options for users. Future work may also explore integrating GPS-based tracking alongside the Tile system to extend tracking range. Overall, the developed system provides a solid foundation for further enhancement and demonstrates the potential of low-cost embedded technologies in improving personal transportation security.

ACKNOWLEDGEMENTS

The researchers would like to express their sincere appreciation to the Department of Computer Engineering of the College of Engineering at the Eulogio “Amang” Rodriguez Institute of Science and Technology, Nagtahan, Manila, for the academic support, guidance, and resources provided throughout the duration of this study. Their contributions played a significant role in the successful development and completion of the project.

Special recognition is extended to the project adviser, Engr. Minerva C. Zoleta, for her valuable insights, technical guidance, and continuous encouragement, which greatly contributed to the direction and quality of this research. Her expertise and mentorship were essential in refining the concepts and implementation of the system.

The researchers are also grateful to their families, classmates, friends, and peers for their unwavering support, motivation, and understanding during the course of this research. Their encouragement served as a source of strength during challenging phases of the study. Furthermore, appreciation is given to all individuals, instructors, and laboratory personnel who, in various ways, contributed to the validation of ideas and improvement of this work. Above all, the researchers give thanks to God Almighty for the wisdom, perseverance, and guidance that made the completion of this research possible.

REFERENCES

1. Han, W., Cao, S., Zhang, Y., OuYang, Y., Chen, X., & Dai, F. (2017). Design and application of the electronic lock for bicycle. Journal of Advanced Control, Automation and Robotics, 2(2), 70–73. https://www.ascspublications.org/wp-content/uploads/woocommerce_uploads/2017/08/JACAR-70-73.pdf
2. Patil, P. R., Alase, M. B., Madival, B. A., Mahamuni, H. S., & Akulwar, P. K. (2018). Smart bike security system. International Journal of Engineering and Technical Research, 6, 1–3. https://ijcrt.org/papers/IJCRT1803275.pdf
3. Raj, A., Sharma, K., Deshmukh, K., Mor, T., & Choudhary, S. (2024). Advance security system for bike. Journal of Emerging Technologies and Innovative Research (JETIR), 11(5), 499–500. https://www.jetir.org/papers/JETIR2405061.pdf
4. Kor, S., Puri, A., Ahire, T., & Balde, K. (2023). Bike anti-theft system using IoT. International Journal of Innovative Research in Multidisciplinary Studies, 11(6). https://www.ijirmps.org/papers/2023/6/230386.pdf
5. Sawant, A., Ashar, S., Baig, A., Choudhary, V., & Haldar, P. (2019). Cloud based bike anti-theft and tracking system (BATS) using Arduino, IoT and Android. International Journal for Scientific Research and Development (IJSRD), 6(12), 53–55. https://www.ijsrd.com/articles/IJSRDV6I120016.pdf

About The Authors

Dwight Baines F. Camposano is an undergraduate student of Computer Engineering at the Eulogio “Amang” Rodriguez Institute of Science and Technology (EARIST). His academic interests include embedded systems,

electronics, and hardware-based solutions. He is actively engaged in developing practical engineering skills and is committed to continuous learning and professional growth in the field of technology.

Lawrence Airan V. Fajardo is an undergraduate Computer Engineering student at Eulogio “Amang” Rodriguez Institute of Science and Technology (EARIST). He has a strong interest in building personal computing devices and exploring hardware technologies. Lawrence is dedicated to improving his technical competencies and strives for excellence in both academic and practical engineering endeavors.

Kenneth George L. Malejana is a Computer Engineering student at the Eulogio “Amang” Rodriguez Institute of Science and Technology (EARIST), skilled in embedded systems and digital logic design. He is passionate about creating practical, innovative technology solutions and applying analytical problem-solving to real-world challenges as he prepares for a professional career in Computer Engineering.

Mark Reagan Fhae D. Reyes is a Computer Engineering student at Eulogio “Amang” Rodriguez Institute of Science and Technology with a growing interest in embedded systems, automation, and hardware integration. He actively participates in hands-on projects involving microcontrollers, sensors, and electronic circuits, focusing on translating theoretical concepts into functional prototypes. Mark is motivated to further develop his technical skills and pursue a career in engineering that emphasizes practical problem-solving and technological innovation.

Chenesa A. Tiboso is a graduating Computer Engineering student at Eulogio “Amang” Rodriguez Institute of Science and Technology. She has a strong interest in robotics and hardware development, focusing on creating innovative and practical engineering solutions. Her career goal is to work in a technology-driven field that aligns with her academic background and personal passion for engineering.

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 in 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.