Indonesian Journal of Electronics, Electromedical Engineering, and Medical Informatics e-ISSN: 2656-8624
Homepage: https://ijeeemi.org/; Vol. 7, No. 4, pp. 619-629, November 2025

RESEARCH PAPER **OPEN ACCES**

An IoT-Enabled Bicycle Access and Monitoring System with Geo-Fence-Based Location Restriction

Hans Christian, Yohanes Gunawan Yusuf, and Rafina Destiarti Ainul

Department of Electrical Engineering, University of Surabaya, Surabaya, Indonesia

Abstract

Managing shared bicycle usage within a university campus can be challenging, especially when relying on manual systems that are slow, difficult to track, and offer limited security. This paper proposes the development of an IoT-based Bicycle Access and Monitoring System designed to make borrowing bikes easier for users and more manageable for campus administrators. The system allows users to borrow bicycles independently through a mobile application developed for Android devices. Each bicycle is equipped with a QR code, which users scan to initiate the borrowing process. After scanning, the application generates a One-Time Password (OTP), which is entered into a keypad embedded on the bicycle. After successful verification, the electronic lock on the bicycle is automatically unlocked. To ensure bicycles remain within the designated campus boundaries, the system includes a geo-fencing feature that continuously monitors the bicycle's GPS coordinates. If a bicycle crosses the predefined boundary, the system triggers an alert and logs the event to a cloud-based database. All borrowing data, including time, user ID, and location, is recorded in real-time and accessible to campus administrators via a web interface. According to the experimental results show that the system functions reliably, with successful access control, accurate event logging, and an average GPS horizontal error of 1.48 meters under both Line of Sight (LOS) and Non Line of Sight (NLOS) conditions. The proposed system provides a scalable, secure, and user-friendly platform that integrates IoT communication, location monitoring, and also improves the bicycle sharing system in university areas, enhancing both operational efficiency and student convenience.

Paper History
Received July 10, 2025
Revised Sept. 20, 2025
Accepted Oct 6, 2025
Published Oct 10, 2025

Keywords
IoT;
Bicycle Access & Monitoring;
Geo-Fence;
Campus Mobility;
OTP Authentication

Author Email
indetail.hans@gmail.com
yohanesgunawan@staff.ubaya.ac.id
rafina@staff.ubaya.ac.id

I. Introduction

In recent years, bicycles have gained widespread attention as a practical and sustainable solution for urban mobility. The development of bicycle-friendly cities has been widely associated with the implementation of well-structured cycling infrastructure and interconnected bicycle networks, as demonstrated in various theoretical models and empirical studies [1]. The integration of Internet of Things (IoT) technologies into bike-sharing systems has emerged as a global trend, such as in the Bicipuma delivery system at UNAM-Mexico [2]. IoT also supports cycling safety through smart devices that monitor biking conditions [3] and intelligent locking systems using multi-sensor configurations [4]. IoT-based bike-sharing systems have been deployed in numerous cities [5], with innovations such as cloud-connected traffic signals to support urban planning [6] and motorcycle monitoring solutions for safety enhancement [7]. IoT applications extend to simulation-based smart city initiatives using bicycles, such as in Bogotá [8], and rental systems like GlideX that utilize IoT for operational control [9]. Smart city transportation is increasingly supported by IoT-enabled bicycle services [10] and remote security systems for electric bikes [11]. Community-based e-bike transportation models have also been proposed to enhance shared mobility [12], with university-based implementations such as the E-WheelShare prototype [13]. In addition to monitoring, prediction models like Recurrent Neural Networks are used for rental forecasting [14][15], and intelligent scheduling has been developed based on spatiotemporal data [16]. Further studies propose shared cycle monitoring systems and energy-optimized bike-sharing frameworks that improve resource efficiency and localization accuracy [17][18][19][20]. Assessments of cycling infrastructure using portable sensor-based lights have also been introduced [21]. However, one of the major challenges in these systems is preventing bikes from being taken outside of predefined usage zones, leading to potential misuse or theft. Geo-fencing technology has been proposed as a solution to define virtual boundaries and restrict movements based on geographic location. This has been applied in mobile attendance systems [22][23][24], speed-limiting mechanisms for vehicles based on zone detection [25], and anti-theft systems utilizing GPS tracking and alert mechanisms [26]. Additionally, geo-fencing has found uses in COVID-19 hotspot alerts [27], religious area management [28], smart route condition alerts for cyclists [29], and open-source urban mobility services [30].

Corresponding author: Rafina Destiarti Ainul, rafina@staff.ubaya.ac.id, Department of Electrical Engineering, Universitas Surabaya, Jl. Raya Kalirungkut, 60293, Surabaya, Indonesia.
Digital Object Identifier (DOI): https://doi.org/10.35882/ijeeemi.v7i4.123

Despite extensive developments in IoT-based bike-sharing systems and geo-fencing technologies, very few studies have combined these two approaches into an integrated solution that is applied to university environments. At Universitas Surabaya (UBAYA), the current manual bike-borrowing system relies on paper logs, which are inefficient, prone to data loss, and challenging to manage, especially given the dynamic nature of campus mobility. Manual bicycle management systems often suffer from several limitations, such as inadequate security mechanisms, inefficient tracking of usage, and a lack of automated control. These issues can lead to unauthorized access, difficulties in monitoring user activity, and operational inefficiencies, particularly in large-scale deployments. Addressing these challenges requires a secure, scalable, and automated solution that not only improves accessibility but also ensures data integrity and user accountability in environments such as university campuses.

Therefore, this paper proposes an IoT-Enabled Bicycle Access and Monitoring System with Geo-Fence-Based Location Restriction. The system integrates a mobile application for Android, QR code-based bike identification, OTP (One-Time Password) access control, and real-time geo-fencing. Users initiate the borrowing process by scanning a QR code on the bike, after which an OTP is generated and entered into a keypad on the bicycle to unlock it. A geo-fencing mechanism monitors the GPS location of each bike, and an audible buzzer alarm is triggered if the bicycle is taken outside the allowed zone, providing both physical and digital deterrents to misuse. All activity is logged in real time to a cloud database and can be monitored by campus administrators via a web dashboard.

The main contributions of this papers are: (1) the design of an integrated and user-friendly IoT-based bike-sharing system specifically adapted for university settings, (2) the implementation of a geo-fencing mechanism combined with a physical buzzer for immediate feedback when bikes exit permitted zones, and (3) a complete backend infrastructure enabling secure access, real-time monitoring, and data transparency for administrative oversight. The remainder of this paper is structured as follows: Section 2 details the materials and methods used to design and implement the system, including the hardware components mounted on the bicycle, such as the microcontroller, GPS module, buzzer, keypad, and locking mechanism, as well as the development of the Android application and cloud infrastructure. Section 3 presents the experimental results, evaluating system performance in real campus scenarios, including access accuracy, GPS tracking precision, and user interaction flow. Finally, Section 4 concludes the paper by summarizing the key findings and discussing future enhancements for scalability and user experience.

II. Materials And Methods

This section presents the design of an IoT-based Bicycle Access and Monitoring System consisting of three primary components: (1) the electrical and hardware design, which utilizes an ESP32 microcontrollerintegrated with a GPS module, keypad, buzzer, and electronic lock, all mounted securely on the bike and docking stand; (2) the geo-fencing security system, which defines restricted usage areas and activates an audible buzzer alarm if the bicycle exits the permitted zone; and (3) the software infrastructure, comprising an Android-based mobile application that enables QR code scanning and OTP-based bike unlocking, and a cloud-based backend using Firebase for real-time data synchronization, logging, and system monitoring. These integrated components ensure a secure, efficient, and fully automated bicycle borrowing process intended for campus environments, as illustrated in the system overview shown in Fig.1. In addition, the system employs UART communication for GPS data transmission to the ESP32. At the same time, Wi-Fi with HTTPS protocol is utilized for secure synchronization with the Firebase cloud backend, ensuring reliable and transparent data flow across all components.

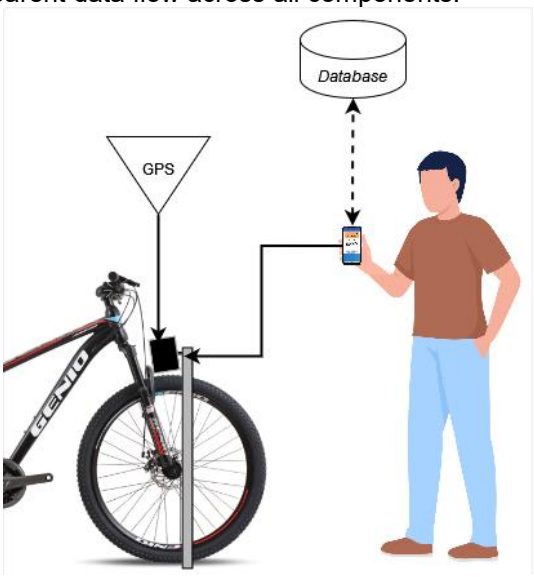


Fig. 1. An Overview of Bicycle Access and Monitoring System

A. The Electrical and Hardware Design of Bicycle Access and Monitoring System

The electrical system of the bicycle access and monitoring system is centered around the ESP32 microcontroller, integrating several key components: a 4×4 matrix keypad for OTP input, a solenoid lock for securing the bicycle, a GPS module (Neo-6M) for geo-fencing, red and green LEDs for visual indicators, and a buzzer for audible alerts, as shown at Fig. 2. To ensure reliable system performance, the ESP32 microcontroller was selected because it integrates Wi-Fi and Bluetooth connectivity within a low-cost, low-power platform, offering better efficiency compared to alternatives such as Arduino Mega or Raspberry Pi for continuous IoT communication. Similarly, the Neo-6M GPS module was chosen due to its high accuracy, fast satellite acquisition, and affordable cost, which makes it more practical than other GPS modules like SIM808 or Ublox NEO-M8 when applied to mobile bicycle monitoring systems. These selections balance performance, energy efficiency, and cost-effectiveness, making them well-suited for this proposed system.

Corresponding author: Rafina Destiarti Ainul, rafina@staff.ubaya.ac.id, Department of Electrical Engineering, Universitas Surabaya, Jl. Raya Kalirungkut, 60293, Surabaya, Indonesia.
Digital Object Identifier (DOI): https://doi.org/10.35882/ijeeemi.v7i4.123

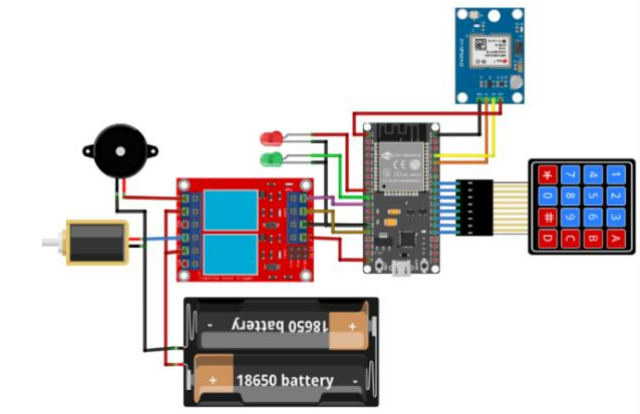


Fig. 2. The electrical wiring configuration of the bicycle access and monitoring system

The ESP32 is powered by two 18650 batteries connected in series. Since the total voltage from the batteries can reach up to 10V, a DC-DC step-down converter module (LM2569) is employed to regulate the input down to a stable 5V, thus preventing overheating of the ESP32's internal voltage regulator. The use of two 18650 batteries is essential, as the solenoid lock requires a voltage of 7–12V to function correctly. At voltages below 7V, the solenoid is unable to retract the plunger mechanism that disengages the lock. Similarly, due to outdoor operation requirements, the buzzer is also driven at approximately 8V to ensure adequate sound volume. Both the solenoid lock and buzzer operate at voltages higher than the ESP32's GPIO levels; therefore, they are controlled through a 2-channel relay module. The relays receive 5V from the ESP32 and are driven by GPIO pins 13 and 27 for the solenoid and buzzer, respectively. The positive wires of the solenoid and buzzer are connected to the normally open (NO) terminals of the relays. In contrast, the common (COM) terminals are linked to the positive output of the battery pack. The negative terminals of both the buzzer and solenoid are directly connected to the battery's ground.

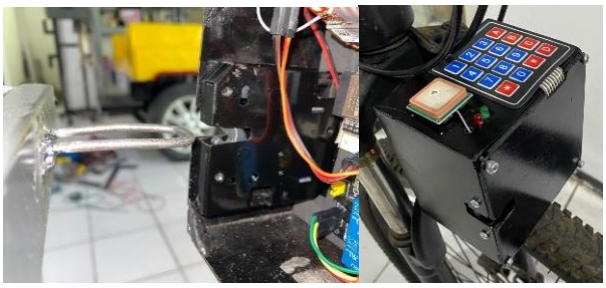


Fig. 3. The locking setup of the bicycle access and monitoring system

The 4×4 matrix keypad consists of 8 pins, 4 for rows and 4 for columns, which are interfaced with the ESP32 through GPIO pins 19, 18, 5, and 17 (rows), and 16, 4, 0, and 2 (columns). These pins are sequentially assigned to simplify the routing on the PCB layout. For user feedback, two LEDs serve as visual indicators: a red LED connected to GPIO 25 indicates error or rejection, and a green LED connected to GPIO 26 indicates successful authentication. The locking system employs a robust 12V 2A metal solenoid lock with a holding force of up to 150 kg, providing secure physical immobilization of the bicycle when docked. This solenoid is triggered via a relay controlled by the ESP32 and is directly powered by the battery pack to ensure sufficient current delivery during operation. The solenoid is mounted securely on the left side of the control module casing using bolts, with the locking hook aligned precisely to engage with a fixed anchor point on the stand. A visual depiction of the locking setup is shown in Fig. 3.

Fig. 4. The holder stand of the bicycle access and monitoring system

To complement the electronic locking system, a custom-designed bicycle stand has been fabricated using 4×2 cm hollow steel tubing. The stand features a secure anchoring point for the solenoid plunger, welded at a fixed offset to accommodate the lateral placement of the locking module. Although implemented as a prototype, the stand is stabilized using a concrete base formed via wooden formwork to simulate permanent ground installation. The physical structure and placement details of the stand are presented in Fig. 4.

B. The Geo-Fencing security system

A geo-fencing mechanism is integrated into the bicycle system to restrict its operational area based on GPS coordinates. This security system operates using the Neo-6M GPS module, which continuously transmits latitude and longitude data to the ESP32 microcontroller via its RX and TX pins, powered at 3.3V. The ESP32 performs real-time calculations to determine the distance between the bicycle's current location and a predefined central point. If the computed distance exceeds a set threshold, the onboard buzzer is activated to alert the user and enforce the boundary limit. This approach aligns with recent implementations of GPS-based area monitoring in mobility systems [22], [25], [28].

The boundary enforcement is defined using a circular geo-fence model centered at a reference location. Distance calculation is performed using the Haversine formula, which accounts for the Earth's curvature and

Corresponding author: Rafina Destiarti Ainul, rafina@staff.ubaya.ac.id, Department of Electrical Engineering, Universitas Surabaya, Jl. Raya Kalirungkut, 60293, Surabaya, Indonesia.
Digital Object Identifier (DOI): https://doi.org/10.35882/ijeeemi.v7i4.123

provides high accuracy for geospatial computations. The formula is given by (Eq. (1) and Eq. (2)):

$$d = 2r.arcsin\left(\sqrt{sin^2\left(\frac{\Delta\phi}{2}\right) + \cos(\phi_1).cos(\phi_2).sin^2\left(\frac{\Delta\lambda}{2}\right)}\right) \quad (1)$$

$$d = (P, P_c);\ \Delta\phi = \phi - \phi_c;\ \Delta\lambda = \lambda - \lambda_c \quad (2)$$

where ϕ and λ are the respective latitudes and longitudes, and r is the Earth's radius. When the computed distance d exceeds the allowed limit, the system triggers an audible buzzer, serving as a passive alert mechanism for location violations. An overview of the implemented geo-fencing concept, including the allowable circular boundary and system behavior upon zone exit, is presented in Fig. 5.

Fig. 5. Geo-Fencing radius implementation for bicycle access and monitoring system

The decision of whether a bicycle is located inside or outside the defined geo-fence region is formulated mathematically as a binary classification problem. The system first computes the distance between GPS position P = (ϕ, λ) and the geo-fence center P_C = (ϕ_c, λ_c) using the haversine formula in Eqs. (1), (2). Based on the computed distance, the decision rule is expressed as (Eq. (3)):

$$Inside\ (P) = \begin{cases} 1, & d(P, P_c) \le R \\ 0, & d(P, P_c) \ge R \end{cases} \quad (3)$$

where R denotes the geo-fence radius. A value of Inside(P)=1 indicates that the bicycle is located within the permissible boundary, while Inside(P)=0 denotes that the bicycle has moved outside the geo-fence area. This decision rule provides a simple yet rigorous mathematical criterion that is computationally efficient for real-time implementation in resource-constrained IoT devices.

Furthermore, by employing the Haversine formula, the distance between the bicycle's current GPS coordinates (latitude and longitude) and the predefined central point of the geo-fence can be accurately calculated. If the computed distance is less than the defined geo-fence radius, the system remains in a normal state and the alarm remains inactive. Conversely, if the bicycle moves beyond the allowable boundary, i.e., the calculated distance exceeds the geo-fence, radius an audible alarm is triggered to notify the user of a location limit area. Nevertheless, the accuracy of this decision rule is highly dependent on the precision of the GPS measurements, which are inherently affected by environmental noise and multipath effects. To mitigate these inaccuracies, an error tolerance factor ε is introduced into the distance calculation, such that the effective distance can be modeled as (Eq. (4)):

$$d_{eff} = d(P, P_c) \pm \varepsilon \quad (4)$$

where ε represents the average deviation obtained from experimental observations. The value of ε is not arbitrarily chosen but derived from the standard deviation of positioning error obtained during measurement under different conditions. Specifically, for LOS environments, ε is set equal to the observed standard deviation of GPS error in open areas, while for NLOS environments, ε corresponds to the standard deviation measured in obstructed areas. This adaptive tolerance setting reduces the probability of false boundary violations while accounting for environmental variations in GPS accuracy. This adjustment ensures that the geo-fence mechanism remains robust against minor fluctuations in GPS readings, thereby reducing false alarms and improving overall system reliability.

C. Android-Based Mobile Application System

An Android-based mobile application was developed using Kodular as the front-end interface to facilitate the bicycle borrowing process securely and efficiently. The application features three main user interfaces: (1) a login page where users authenticate using their institutional Google accounts; (2) an instruction page providing usage guidelines and important notices for borrowers; and (3) a main dashboard where users can scan a QR code attached to the bike stand to request a one-time password (OTP) for unlocking. Upon a successful scan, the system returns the OTP, bike number, and borrowing timestamp. To prevent misuse, the application enforces a 120-second cooldown between OTP requests and disables scanning for 30 seconds if an invalid QR code is detected. The main dashboard also displays available bike station locations on an interactive map, allowing users to select the preferred terminal visually.

On the login page, as shown in Fig. 6, users are required to authenticate using their institutional Google email accounts (e.g., students and staff). The system utilizes Firebase Authentication to enable seamless login through the existing Google account on the user's smartphone. This method ensures both convenience and verification of valid email credentials. However, its implementation involves additional steps, such as uploading the google-services.json file into the assets directory in Kodular and registering the SHA-1 certificate fingerprint from Kodular into Firebase using tools like Keystore Explorer. The second screen displayed after a successful login is the usage instruction page. This page is designed to help first-time users understand how to access and operate the bicycle system properly. It provides a step-by-step guide along with important notes users should be aware of during the borrowing process. As illustrated in Fig. 7, the inclusion of diagrams and images enhances user understanding and reduces the likelihood of operational errors.

Corresponding author: Rafina Destiarti Ainul, rafina@staff.ubaya.ac.id, Department of Electrical Engineering, Universitas Surabaya, Jl. Raya Kalirungkut, 60293, Surabaya, Indonesia.
Digital Object Identifier (DOI): https://doi.org/10.35882/ijeeemi.v7i4.123

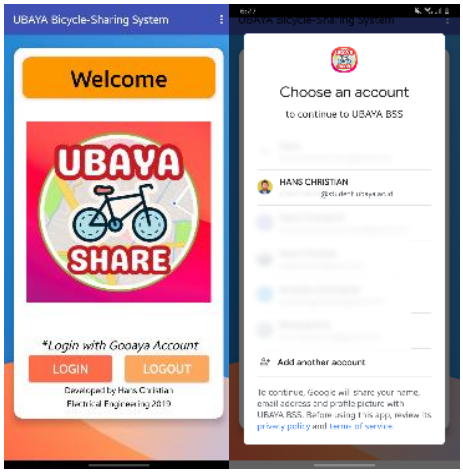


Fig. 6. Login page using institutional Google accounts

Placing this page immediately after login ensures that every user is informed of the correct procedures before accessing the system. This approach improves system usability and supports a smoother user experience, especially for new or unfamiliar users.

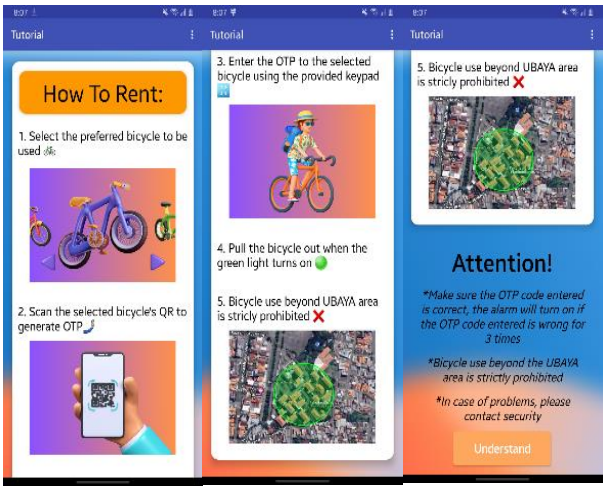


Fig. 7. Instruction page of Android Application

On the main interface, users initiate the bicycle borrowing process by scanning a QR code attached to the bicycle, as illustrated in Fig. 8. Upon successful scanning, the application generates a One-Time Password (OTP) and displays relevant information, including the OTP code, bicycle ID, and the current date and time. To prevent abuse and ensure proper data management, the system enforces a 120-second cooldown period before another OTP can be requested. If the user scans an incorrect QR code, the system imposes a 30-second delay to reduce repeated invalid attempts.

After the OTP is generated, user credentials such as the username and email address are uploaded to the database along with the bicycle number and the borrowing timestamp. Additionally, users can select their desired terminal location through an interactive map interface when a terminal such as the Engineering Building is selected, a marker appears on the map to visually indicate its position. This feature enhances navigation and helps users locate the intended terminal more efficiently. The combination of OTP-based security and real-time location selection contributes to a secure and user-friendly access system. In the proposed system, once an OTP is issued, the associated user credentials, including username, email address, bicycle number, and borrowing timestamp, are securely stored in the database. Simultaneously, the user is provided with an interactive interface to select the desired terminal location, where a visual marker is displayed on the map for enhanced navigation. To ensure that only authorized users can proceed, an OTP based access control mechanism is employed. The mathematical formulation of this mechanism is presented in Eq. (4), where the exact character string matching between the user-provided code and the server generatedserver-generated code determines OTP validity.

$$OTP_{Valid} = \begin{cases} 1, & OTP_{user} = OTP_{server} \\ 0, & OTP_{user} \neq OTP_{server} \end{cases} \quad (5)$$

The backend system integrates Firebase Realtime Database and Firebase Authentication to handle data storage and user verification. Firebase Authentication restricts access to approved institutional email accounts, allowing the administrator to manage login permissions manually. Once a user is authenticated, borrowing data such as username, email, time, and bike number is stored

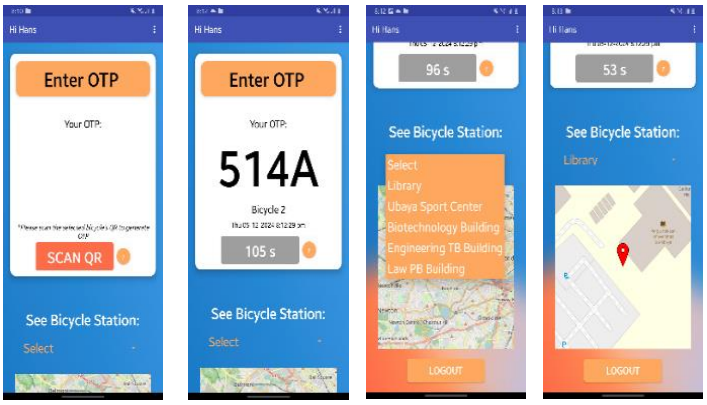


Fig. 8. Scan QR code page and enter OTP for unlocking bicycle.

in the database under unique identifiers. Each successful transaction is logged with an OTP and metadata, while invalid attempts are marked with a “WARNING!” tag to distinguish them from valid records. Firebase also allows the administrator to add, remove, or deactivate user accounts as needed.

III. Results

In this paper, three main tests were conducted to evaluate the system's performance: GPS accuracy, geo-fencing security, and OTP authentication functionality. The GPS accuracy test involved comparing the distance readings obtained from the Neo-6M GPS module with ground truth measurements taken using a digital wheel meter. The geo-fencing security test was performed by intentionally moving the bicycle outside the predefined safety boundary to observe the system’s response. Finally, the OTP authentication test was carried out by inputting both valid and random OTP codes to evaluate the system’s

Corresponding author: Rafina Destiarti Ainul, rafina@staff.ubaya.ac.id, Department of Electrical Engineering, Universitas Surabaya, Jl. Raya Kalirungkut, 60293, Surabaya, Indonesia.
Digital Object Identifier (DOI): https://doi.org/10.35882/ijeeemi.v7i4.123

ability to accept correct inputs while rejecting unauthorized access attempts.

A. GPS Accuracy

The accuracy of the GPS module was measured by comparing its positional readings with actual distance measurements obtained using a digital wheel meter. This evaluation was carried out under both Line-of-Sight (LOS) and Non-Line-of-Sight (NLOS) conditions to determine the module's performance in varied environments. Distance sampling was conducted at intervals ranging from 1 meter to 60 meters from the geo fence center. GPS coordinates were obtained via the Arduino IDE serial monitor, while ground truth distances were measured simultaneously using the digital wheel meter. This method provided a reliable basis for quantifying GPS accuracy under realistic operational scenarios. The measured discrepancies between the GPS result and ground truth, as the real distances are summarized in Table 1, illustrate the accuracy of the GPS module under LOS and NLOS scenarios.

To assess the reliability of the geo-fencing feature, a series of tests was carried out to evaluate the accuracy of GPS readings under both LOS and NLOS conditions. The goal was to determine how precisely the GPS module can detect the bicycle's location relative to the defined boundary. Under LOS conditions, measurements taken at 1 m and 2 m distances showed shifts exceeding 1 m, attributed to the inherent horizontal accuracy limitations of the Neo-6M GPS module. However, at distances ranging from 3 m to 60 m, the GPS readings were considerably more stable, with an average positional deviation of approximately 1.4 m, which is acceptable for most outdoor monitoring applications.

Table 1. Distance Measurement at LOS and NLOS Scenarios

NO	LOS Scenarios		NLOS Scenarios	
	Real Distance (meters)	GPS Distance (meters)	Real Distance (meters)	GPS Distance (meters)
1	1	2.1	1	3.1
2	2	3.16	2	3.44
3	3	3.6	3	5.68
4	5	5.68	5	9.13
5	10	8.85	10	12.4
6	20	21.97	20	21.97
7	30	33.35	30	33.35
8	40	45.5	40	45.5
9	50	49.89	50	49.89
10	60	61.74	60	61.74

In contrast, under NLOS conditions, the GPS data became highly unstable. At distances below 5 m, the positional error increased significantly, reaching deviations of up to 2 m. Beyond 5 m, the average shift was recorded at around 2.52 m. As shown in Fig. 9, the statistical analysis confirms that GPS positioning is generally more reliable under LOS conditions, where the mean error was 1.74 m with a standard deviation of 1.6 m. In contrast, NLOS conditions produced a larger mean error of 2.54 m, indicating reduced accuracy even though the variability was of similar magnitude (standard deviation of 1.5 m). This demonstrates that obstructions in the environment significantly degrade GPS performance, making LOS preferable for applications requiring precise localization. These results also revealed the presence of blind spots within the UBAYA campus, where GPS signals were inconsistent or degraded. This level of inaccuracy may pose challenges when deploying the system in areas with narrow geo-fence margins or near obstacles such as trees, canopies, or high buildings, all of which can interfere with satellite signal reception.

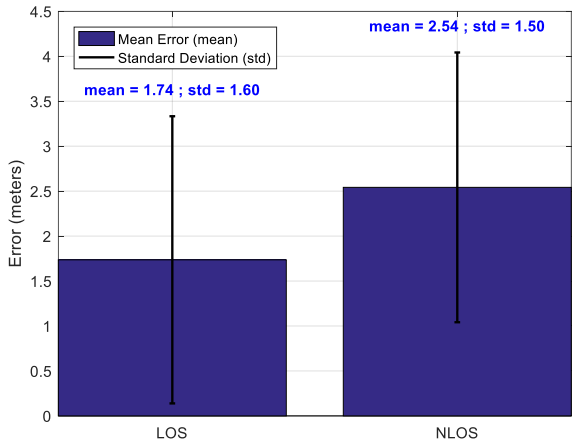


Fig. 9. Statistical Analysis of GPS Error Performance in LOS and NLOS Conditions

B. Geo-Fencing Security

This evaluation focused on determining the consistency and responsiveness of the implemented geo-fence security mechanism. Two separate tests were conducted: the first examined the system's ability to detect when the bicycle exceeded the designated safe zone reliably and to activate the onboard alarm; the second assessed the response delay of the bicycle access and monitoring module. For the reliability test, the bicycle was moved beyond the boundary in 10 different locations, each tested twice, to observe whether the alarm was triggered. For the response time test, the bicycle was placed approximately 2 meters outside the geo-fence for a duration of 3 seconds at each of the same 10 locations (repeated twice). The response delay was measured from the last known position inside the safe zone to the moment the system recognized the out-of-bounds status and activated the buzzer, as monitored via the serial console. The results of these tests are presented in Table 2. Then, to enhance the reliability of the geo-fencing mechanism under GPS measurement uncertainty, the buffer margin (m) was derived using a probabilistic formulation based on the Rayleigh error distribution of horizontal GPS positioning. In this context, the positional error magnitude (E) of a GPS

Corresponding author: Rafina Destiarti Ainul, rafina@staff.ubaya.ac.id, Department of Electrical Engineering, Universitas Surabaya, Jl. Raya Kalirungkut, 60293, Surabaya, Indonesia.
Digital Object Identifier (DOI): https://doi.org/10.35882/ijeeemi.v7i4.123

receiver affected by isotropic Gaussian noise in the horizontal plane follows a Rayleigh distribution with scale parameter (σ).

Table 2. Geo-fence system reliability and response time test results.

Testing Number	Result Number Active (V), Non-Active (X)		Time (s)
	Result-1	Result-2	
Test-1	V	V	1.408
Test-2	V	V	2.043
Test-3	V	V	2.050
Test-4	V	V	1.498
Test-5	V	V	1.577
Test-6	V	V	2.057
Test-7	V	V	3.024
Test-8	V	V	2.067
Test-9	V	V	2.036
Test-10	V	V	1.534

The probability operator, denoted by Pr(·), represents the likelihood of an event occurring. Thus, the probability that the GPS error exceeds the buffer margin can be expressed as:

$$P_r(E > m) = \exp\left(-\frac{m^2}{2\sigma^2}\right) \quad (6)$$

For a specified target false-alarm probability (α), the acceptable probability that GPS error alone will produce a spurious geo-fence violation, the required buffer margin is:

$$m = \sigma\sqrt{2\ln\left(\frac{1}{\alpha}\right)} \quad (7)$$

In practice, σ is estimated from empirical positional-error statistics obtained by comparing GPS coordinates with simultaneous ground truth distances recorded by a digital wheel meter. Under LOS conditions, the measured mean positional deviation was $E_{LOS} = 1.74\ m$ while under NLOS conditions, the mean deviation increased to $E_{NLOS} = 2.54\ m$ For a Rayleigh-distributed magnitude, the relationship between the mean error and the Rayleigh scale parameter is:

$$\bar{E}[E] = \sigma\sqrt{\frac{\pi}{2}} \rightarrow \sigma = \frac{\bar{E}[E]}{\sqrt{\pi/2}} \quad (8)$$

Using the measured means yields $\sigma_{LOS} = 1.6\ m$ and $\sigma_{NLOS} = 1.5\ m$ substituting these values into the buffer equation produced required margins of 3.92 m, 4.83 m, and 5.93 m for LOS with false-alarm probabilities of 5%, 1%, and 0.1%, respectively, while the corresponding NLOS margins were 3.68 m, 4.53 m, and 5.55 m. These results illustrate that NLOS conditions require substantially larger buffer margins to achieve the same false-alarm probability, consistent with the increased mean error (2.54 m) and the presence of blind spots observed on campus. Practically, we used selecting m according to deployment priorities: choose a smaller α(larger m) where false alarms are costly, or accept a larger α (smaller m) if tighter geo-fence margins are mandatory. Additionally, temporal smoothing strategies (e.g., N out of M voting) and hysteresis should be implemented to mitigate transient GPS spikes and reduce the operational impact of brief outliers, particularly under NLOS conditions.

C. OTP authentication functionality

OTP verification reliability was tested by entering incorrect codes and monitoring the system's ability to reject unauthorized access attempts. a total of 15 access attempts were conducted using randomly generated alphanumeric codes, each consisting of three numeric digits followed by one uppercase letter (e.g., 123A). These codes were entered into the Bicycle Access and Monitoring System to assess its rejection accuracy. The results showed that 13 out of 15 invalid OTP entries were correctly rejected, with the locking mechanism remaining engaged and the buzzer activated after every three failed attempts. However, in two cases, the system erroneously accepted the incorrect codes and unlocked the bike. This was attributed to the coincidental match between the randomly generated codes and preprogrammed valid OTPs stored in the ESP32 module. These results highlight the overall reliability of the OTP validation process, while also emphasizing the need for enhanced code randomization or dynamic key generation to prevent unintended matches.

D. Battery Lifetime Evaluation

To evaluate the battery lifetime of this proposed IoT-enabled bicycle access and monitoring system with geo-fence-based location restriction, a series of tests was conducted by continuously operating the module until complete power depletion, with timestamps recorded from activation to shutdown using the serial monitor. During testing, the system remained stationary within the safe zone to ensure consistent power consumption. Under ideal conditions, the 18650 lithium-ion battery has a nominal capacity of 1200 mAh, while the system draws an average current of 190 mA during idle operation and up to 2.1 A momentarily when actuating the solenoid lock. Since the current spike is transient, it isn't very important for lifetime calculations. Using the following theoretical formula:

$$Time = \frac{Battery\ Capacity\ (mAH)}{Average\ Current\ (mA)} \quad (9)$$

According to the theoretical calculation, the battery endurance is estimated to be approximately 6 hours and 31 minutes. However, experimental testing revealed shorter operational durations, with the first trial lasting 161 minutes, the second 153 minutes, and the third 157 minutes. These results indicate an average lifetime of approximately 157 minutes (≈2 hours and 37 minutes). The discrepancy between theoretical and measured outcomes is primarily due to battery degradation caused by repeated charge-discharge cycles, which reduce the effective capacity below its nominal rating. This observation emphasizes the critical role of energy management in maintaining the reliability of the IoT-

Corresponding author: Rafina Destiarti Ainul, rafina@staff.ubaya.ac.id, Department of Electrical Engineering, Universitas Surabaya, Jl. Raya Kalirungkut, 60293, Surabaya, Indonesia.
Digital Object Identifier (DOI): https://doi.org/10.35882/ijeeemi.v7i4.123

enabled bicycle system under real-world operating conditions.

IV. Discussion

The evaluation of GPS accuracy under both LOS and NLOS conditions reveals significant implications for the reliability of the geo-fence-based area restriction system. As illustrated in Fig. 10, the measurement error under LOS conditions remains relatively low, typically below 3 meters, supporting the use of GPS as a viable positioning method for enforcing spatial boundaries. In contrast, NLOS scenarios result in higher positional deviations, especially within short distances (1–10 meters) due to signal obstruction, which may affect the precision of geo fence detection and lead to potential misclassification of in-zone or out-of-zone locations.

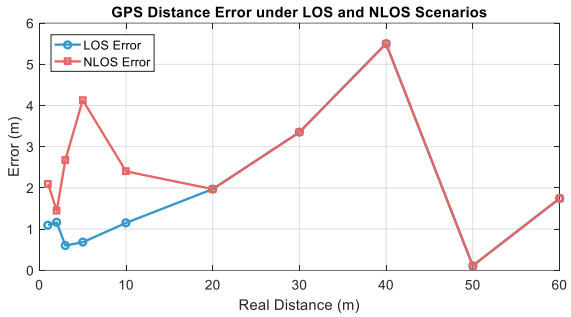


Fig. 10 GPS Error Analysis for Geo-Fence Accuracy in LOS and NLOS Conditions

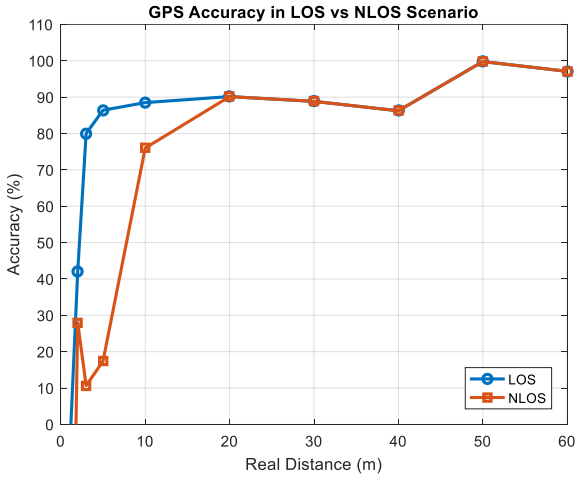


Fig. 11 Accuracy of GPS-Based Distance Measurements at LOS and NLOS Scenarios

Fig. 11 further supports this finding by showing that GPS accuracy during LOS scenarios consistently exceeds 90%, while under NLOS it drops as low as 69% at 1 meter and only stabilizes beyond 20 meters. These deviations are critical, as the geo-fence system relies on accurate location input to activate or deactivate access control mechanisms. Therefore, geo-fence boundaries should ideally be implemented in open environments with minimal obstruction, or coupled with dynamic buffer zones to account for signal noise and urban interference.

In addition to location accuracy, the responsiveness of the geo-fence system plays a crucial role in ensuring effective security enforcement. As shown in Table 2, the average response time between detecting an out-of-bounds location and triggering the alarm was 1.893 seconds across 10 different trial locations. This response latency includes both GPS signal processing and communication delays to the bicycle access and monitoring system module. While the system consistently activated the alarm in all trials (100% reliability), minimizing the response time remains essential, especially in scenarios where rapid unauthorized movement outside of geo-fenced areas must be promptly mitigated. A response time below 2 seconds is considered acceptable for real-time applications, but future improvements could involve optimizing the polling frequency or employing edge-based GPS preprocessing to reduce furtherto reduce latency further.

Moreover, the system's OTP authentication mechanism plays a vital role in ensuring secure bicycle access. The test results show that the module correctly rejected 13 out of 15 incorrect OTP entries and triggered an alarm after three consecutive failed attempts, demonstrating strong access control functionality. However, two unauthorized codes unintentionally matched pre-programmed valid codes, leading to unauthorized unlocking. This highlights a potential vulnerability in the static storage of OTP codes, indicating a need for dynamic OTP generation and server-side validation in future iterations.

The proposed system, an IoT-Enabled Bicycle Access and Monitoring System with Geo-Fence Based Location Restriction, is designed specifically for outdoor environments, particularly under LOS and NLOS conditions. In this system, users can independently borrow bicycles through a mobile application equipped with an OTP feature to unlock the bicycle. While the current OTP implementation is limited to a simple four-character combination, future improvements will consider more advanced data security schemes. Furthermore, the monitoring subsystem integrates a geo-fencing mechanism based on GPS to enforce area restrictions. Although a delay of up to 2 seconds in alarm activation was observed when the bicycle moved outside the designated area, this limitation will be addressed in future work by incorporating alternative wireless localization technologies such as LoRA. Despite these current constraints, the proposed system demonstrates several advantages over related works, as summarized in Table 3. As summarized in Table 3, prior works have explored IoT-enabled bicycle or vehicle sharing with features such as location monitoring, smart locks, and anti-theft mechanisms. However, most do not incorporate a geo-fencing restriction mechanism integrated with IoT, or are limited to specific hardware implementations. For instance, [5] provides LoRaWAN-based bicycle tracking without usage restriction, while GlideX [9] offers IoT-based rentals with multiple sensors but no geo-fencing capability. Similarly, [17] focuses on availability monitoring without access control, and [19] emphasizes accelerometer-based theft detection rather than location restriction. The study in [26] introduces geo-fencing with Arduino and GSM, yet remains hardware-specific and vehicle-oriented rather than IoT-integrated. In contrast, the proposed system uniquely combines GPS tracking,

Corresponding author: Rafina Destiarti Ainul, rafina@staff.ubaya.ac.id, Department of Electrical Engineering, Universitas Surabaya, Jl. Raya Kalirungkut, 60293, Surabaya, Indonesia.
Digital Object Identifier (DOI): https://doi.org/10.35882/ijeeemi.v7i4.123

Table 3. Comparison of Related Works and the Proposed System

Reference	Main Features	Limitation	Comparison with Proposed System
[5] J. L. M. Puyol, et All., "Bicycle Sharing System Using an IoT Network".	Bicycle sharing with LoRaWAN tracking	Location monitoring only; no restriction area	Proposed system introduces geo-fencing restriction for usage control
[9] L. Boppana, et. All., "GlideX: An IoT Based Bicycle Rental System".	GlideX: IoT-based rental with sensors (orientation, odometer, lock)	No geo-fencing; GPS + IoT only	Adds restriction area enforcement for enhanced security
[17] L. Alluri, et. All., "Shared Cycle and Vehicle Sharing and Monitoring System".	IoT cycle sharing with GPS monitoring in smart city	Focus on availability; no access control	Ensures controlled access with OTP and geo-fencing alarms
[19] S. S. Mahmoud, et. All., "Smart IoT-Based Shared Bike System".	Smart bike with GPS, accelerometer, smart lock, anti-theft	Security via accelerometer; no geo-fencing restriction	Combines OTP + geo-fencing for theft prevention and access control
[26] S. R. Gantenapalli, et.All., "Securing Vehicles with Arduino: Implementing Geo-Fencing Technology for Theft Prevention".	Vehicle theft prevention using Arduino, GPS, GSM with geo-fencing	Limited to Arduino; not IoT-integrated; vehicle-focused	IoT-enabled system tailored for bicycle sharing in campus context

OTP authentication, and geo-fencing enforcement, thereby enhancing both security and practical applicability for campus-based bicycle sharing scenarios.

V. Conclusion

The implementation of the IoT-enabled bicycle access and monitoring system successfully facilitates secure and efficient bicycle lending by integrating hardware-based controls, mobile application interfaces, and cloud-based data storage. The system allows real-time uploading of user activity and lending records to a central database, improving management and traceability. Experimental results demonstrate that the Neo-6M GPS module achieves an average accuracy of 1.48 meters under Line-of-Sight (LOS) conditions and 2.52 meters under Non-Line-of-Sight (NLOS) conditions, which is sufficient for outdoor geo-fencing enforcement. However, its performance degrades in indoor or obstructed environments, limiting its reliability in small or enclosed areas. Despite these limitations, the overall system demonstrates effective geo-fence triggering and OTP based access control, validating its functionality in a smart campus deployment. Future development of the IoT-based bicycle access and monitoring system will focus on several key aspects. First, geo-fence accuracy will be enhanced by integrating alternative localization technologies such as Wi-Fi positioning, Ultra Wideband (UWB), or LoRa-based tracking, which can improve robustness in both indoor and outdoor environments and reduce false alarms caused by GPS inaccuracies in LOS and NLOS conditions. Second, the security of the OTP mechanism will be strengthened by replacing the current simple random codes with dynamic approaches such as time-based tokens, one-time cryptographic hashes, or even public-key infrastructure (PKI) schemes, thereby mitigating vulnerabilities to brute-force or replay attacks. Third, system scalability and long-term operation will be explored, including multi-user support, maintenance requirements, and update strategies for sustainable deployment in campus-scale or city-wide implementations. Additionally, mobile application functionalities will be expanded to include real-time alerting, historical route tracking, and tighter integration with institutional IoT frameworks. Finally, hardware robustness and privacy-preserving mechanisms will also be investigated to ensure dependable, secure, and user-centric adoption in future smart mobility and smart city initiatives.

References

[1] G. Reggiani *et al.*, "Bicycle network needs, solutions, and data collection systems: A theoretical framework and case studies," *Case Stud. Transp. Policy*, vol. 10, no. 2, pp. 927–939, 2022, doi: 10.1016/j.cstp.2022.03.006.

[2] A. M. Pérez Silva, V. Olvera Rodríguez, C. García Cerrud, F. I. Soler Anguiano, and I. Flores de la Mota, "Internet of things and industry 4.0 applied in the delivery system for the bicipuma bike-sharing system in UNAM-Mexico," *Procedia Manuf.*, vol. 42, no. 2019, pp. 434–441, 2020, doi: 10.1016/j.promfg.2020.02.052.

[3] G. Kapousizis, M. B. Ulak, K. Geurs, and P. J. M. Havinga, "A review of state-of-the-art bicycle technologies affecting cycling safety: level of smartness and technology readiness," *Transp. Rev.*, vol. 43, no. 3, pp. 430–452, 2023, doi: 10.1080/01441647.2022.2122625.

[4] Z. Xue *et al.*, "A shared bicycle intelligent lock control and management system based on multisensor," *IEEE Internet Things J.*, vol. 7, no. 6, pp. 5426–5433, 2020, doi: 10.1109/JIOT.2020.2979899.

[5] J. L. M. Puyol and V. M. Baeza, "Bicycle Sharing

Corresponding author: Rafina Destiarti Ainul, rafina@staff.ubaya.ac.id, Department of Electrical Engineering, Universitas Surabaya, Jl. Raya Kalirungkut, 60293, Surabaya, Indonesia.
Digital Object Identifier (DOI): https://doi.org/10.35882/ijeeemi.v7i4.123

System Using an IoT Network," *Proc. 2021 Glob. Congr. Electr. Eng. GC-ElecEng 2021*, vol. 2021, no. December, pp. 131–135, 2021, doi: 10.1109/GC-ElecEng52322.2021.9788465.

[6] R. Raman and S. S. Shireshi, "Bicycle-Friendly Urban Planning using IoTConnected Traffic Signals in the Cloud," *2nd Int. Conf. Autom. Comput. Renew. Syst. ICACRS 2023 - Proc.*, pp. 262–267, 2023, doi: 10.1109/ICACRS58579.2023.10404928.

[7] P. Bhottacharjee, A. Saeid, M. R. Jannat, and K. I. Masud, "Developing an IoT-based Motorcycle Safety and Monitoring System: An Efficient Solution," *2024 27th Int. Conf. Comput. Inf. Technol.*, no. December, pp. 1594–1599, 2025, doi: 10.1109/iccit64611.2024.11021958.

[8] S. Garcia-Perez *et al.*, "Alternative mobility system using IoT and smart-cities approaches through the use of the bike for a sector of the city of Bogota within a simulated environment," *2020 Smart Cities Symp. Prague, SCSP 2020*, pp. 4–9, 2020, doi: 10.1109/SCSP49987.2020.9134025.

[9] L. Boppana, S. R. Chodagam, L. J. Mathews, V. M. Krishnan, and I. A. Athawle, "GlideX: An IoT Based Bicycle Rental System," *2024 1st Int. Conf. Robot. Eng. Sci. Technol. RESTCON 2024*, pp. 165–169, 2024, doi: 10.1109/RESTCON60981.2024.10463563.

[10] R. J. Fourie, M. Ndiaye, and G. P. Hancke, "IoT Bicycle Sharing Service for Smart City Transport," *IECON Proc. (Industrial Electron. Conf.*, vol. 2021-Octob, pp. 1–6, 2021, doi: 10.1109/IECON48115.2021.9589463.

[11] A. M. Joy, A. Ravi, J. Roy, G. V. Karthikeyan, and T. P. Rajan, "IoT Enabled Electronic Security & Remote Monitoring Solution for Electric Bikes," *2022 IEEE Int. Power Renew. Energy Conf. IPRECON 2022*, pp. 1–6, 2022, doi: 10.1109/IPRECON55716.2022.10059526.

[12] A. R. Al-Ali *et al.*, "IoT-Based Shared Community Transportation System Using e-Bikes," *5th Int. Conf. Smart Grid Smart Cities, ICSGSC 2021*, pp. 61–65, 2021, doi: 10.1109/ICSGSC52434.2021.9490509.

[13] J. Salimbangon, Leo C. Bermudez, Heubert M, Ferolino, and Leah B. Ybañez, "E-WheelShare: An IoT-Based Bicycle Sharing System Prototype for University of Cebu," *J. Comput. Sci. Technol. Stud.*, vol. 7, no. 3, pp. 1018–2021, 2025, doi: 10.32996/jcsts.2025.7.3.114.

[14] S. Lata, S. T. Gowda, K. P. Spandana, R. A. Srinivasa Reddy, and N. Sumith, "Smart Bike Monitoring System Using IoT," *Proc. - 2023 7th Int. Conf. Des. Innov. 3 Cs Comput. Commun. Control. ICDI3C 2023*, pp. 118–122, 2023, doi: 10.1109/ICDI3C61568.2023.00032.

[15] E. H. C. Lu and Z. Q. Lin, "Rental Prediction in Bicycle-Sharing System Using Recurrent Neural Network," *IEEE Access*, vol. 8, pp. 92262–92274, 2020, doi: 10.1109/ACCESS.2020.2994588.

[16] L. Jiang, "Research on bike-sharing Demand Forecasting and Intelligent Scheduling Method Based on Spatio-temporal Data," *Proc. - 2023 Int. Conf. Mechatronics, IoT Ind. Informatics, ICMIII 2023*, no. Icmiii, pp. 380–384, 2023, doi: 10.1109/ICMIII58949.2023.00079.

[17] L. Alluri and H. J. Magadum, "Shared Cycle and Vehicle Sharing and Monitoring System," *Proc. 2022 11th Int. Conf. Syst. Model. Adv. Res. Trends, SMART 2022*, pp. 243–247, 2022, doi: 10.1109/SMART55829.2022.10047734.

[18] M. A. Mohamed, S. F. Toha, M. D. Ataur Rahman, and M. O. H. Khairudin, "Smart Iot Energy Optimisation and Localisation Monitoring for E-Bike Sharing," *IIUM Eng. J.*, vol. 26, no. 2, pp. 305–325, 2025, doi: 10.31436/iiumej.v26i2.3448.

[19] S. S. Mahmoud, H. W. Samy, I. R. Mostafa, S. Zakzouk, B. Wasfey, and M. S. Darweesh, "Smart IoT-Based Shared Bike System," *2024 Int. Conf. Futur. Telecommun. Artif. Intell. IC-FTAI 2024 - Proc.*, pp. 1–6, 2024, doi: 10.1109/IC-FTAI62324.2024.10950049.

[20] N. Sehrawat and S. Kaur, "Smart Sharing Bicycle for a Sustainable City: An Application of IoT," *Int. Interdiscip. Humanit. Conf. Sustain. IIHC 2022 - Proc.*, pp. 887–891, 2022, doi: 10.1109/IIHC55949.2022.10060489.

[21] T. Ahmed, A. Pirdavani, D. Janssens, and G. Wets, "Utilizing Intelligent Portable Bicycle Lights to Assess Urban Bicycle Infrastructure Surfaces," *Sustain.*, vol. 15, no. 5, 2023, doi: 10.3390/su15054495.

[22] R. Shinde, A. Nilose, and P. Chandankhede, "Design and Development of Geofencing Based Attendance System for Mobile Application," *Int. Conf. Emerg. Trends Eng. Technol. ICETET*, vol. 2022-April, pp. 1–6, 2022, doi: 10.1109/ICETET-SIP-2254415.2022.9791781.

[23] H. Kang, S. H. Oh, and S. L. Ju, "Study on Device Based Geo-Fencing and Triggering Services for Enhancing Alert Area Accuracy in Cell Broadcast Service," *Int. Conf. ICT Converg.*, pp. 1427–1430, 2023, doi: 10.1109/ICTC58733.2023.10393714.

[24] M. Tamboli, G. Katore, S. Patale, and N. J. Philips, "Attendance Management System Using Geofencing Technology," *1st Int. Conf. Pioneer. Dev. Comput. Sci. Digit. Technol. IC2SDT 2024 - Proc.*, pp. 137–141, 2024, doi: 10.1109/IC2SDT62152.2024.10696345.

[25] M. Upendra, V. Reddy, and M. Safa, "Smart GPS Based Vehicle Speed Limit Controller on zone identification using Geo-Fencing Algorithm," *2024 3rd Int. Conf. Innov. Technol. INOCON 2024*, pp. 1–6, 2024, doi: 10.1109/INOCON60754.2024.10511421.

[26] S. R. Gantenapalli, P. B. Choppala, and P. D. Teal, "Securing Vehicles with Arduino: Implementing Geo-Fencing Technology for Theft Prevention," *2024 IEEE Int. Conf. Inf. Technol. Electron. Intell. Commun. Syst. ICITEICS 2024*, pp. 1–5, 2024, doi: 10.1109/ICITEICS61368.2024.10625496.

Corresponding author: Rafina Destiarti Ainul, rafina@staff.ubaya.ac.id, Department of Electrical Engineering, Universitas Surabaya, Jl. Raya Kalirungkut, 60293, Surabaya, Indonesia.
Digital Object Identifier (DOI): https://doi.org/10.35882/ijeeemi.v7i4.123

[27] D. Diana Josephine, R. Shyam Sunder, S. Sharanesh, C. B. Nithin Ram, and G. Hari Prasath, "COVID Hotspot Alert System using Geo-Fencing Technique," *6th Int. Conf. I-SMAC (IoT Soc. Mobile, Anal. Cloud), I-SMAC 2022 - Proc.*, pp. 819–822, 2022, doi: 10.1109/I-SMAC55078.2022.9987296.

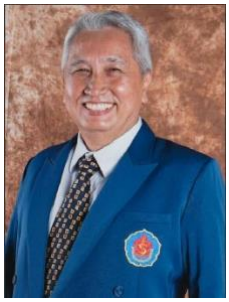
[28] A. Vishnoi, T. Choudhury, J. C. Patni, A. Sar, and H. F. Mahdi, "A Proposed Framework for Smart Geo-Fencing for Religious Places," *ISAS 2023 - 7th Int. Symp. Innov. Approaches Smart Technol. Proc.*, pp. 1–6, 2023, doi: 10.1109/ISAS60782.2023.10391370.

[29] S. Pravin Sawant, D. Yogesh Thakor, D. Kishor Khandelwal, and S. Namdeo Katkar, "Bike Skid Detection and Smart Alert System with Route Condition Assistance," *Proc. 8th Int. Conf. Commun. Electron. Syst. ICCES 2023*, no. Icces, pp. 1640–1643, 2023, doi: 10.1109/ICCES57224.2023.10192876.

[30] A. Eguiluz, U. Hernandez-Jayo, D. Casado-Mansilla, D. Lopez-De-Ipina, and A. E. Moran, "Design and implementation of an open-source urban mobility web service based on environmental quality and bicycle mobility data," *2022 7th Int. Conf. Smart Sustain. Technol. Split. 2022*, 2022, doi: 10.23919/SpliTech55088.2022.9854330.

AUTHOR BIOGRAPHY

Hans Christian received the B.Eng. degree in Electrical Engineering from the University of Surabaya (UBAYA), Indonesia, in 2025. During his undergraduate studies, he was actively involved as a student research assistant in projects related to the Internet of Things (IoT), with a particular focus on mobility systems in campus environments. His interests include IoT-based system development, wireless communication, and smart campus infrastructure. He is currently affiliated with Morning Star Academy, where he continues to apply his engineering skills in educational and technological initiatives. He can be contacted via email at: indetail.hans@gmail.com



Yohanes Gunawan earned his B.Eng. degree in Electrical Engineering from Institut Teknologi Sepuluh Nopember (ITS), Indonesia, in 1961, and received his M.MT. (Magister Manajemen Teknologi) degree in Technology Management from ITS in 2009. He joined the University of Surabaya (UBAYA) as a full-time faculty member in 1987 and is currently serving as an Assistant Professor in the Department of Electrical Engineering. His academic and professional interests are centered around computer networks and electronics, particularly in the implementation and management of network infrastructures. He has extensive experience in teaching and mentoring in the fields of networking and embedded systems. In addition to his academic role, he holds numerous professional certifications in computer networking, particularly from MikroTik. He is also recognized as an internationally certified trainer, actively involved in delivering professional training programs and workshops on computer networks both nationally and internationally. He can be contacted via email at: yohanesgunawan@staff.ubaya.ac.id

Rafina Destiarti Ainul earned her B.Eng. degree in Telecommunication Engineering from Politeknik Elektronika Negeri Surabaya (PENS), Indonesia, in 2015, and received her M.Eng. degree in Electrical Engineering from the same institution in 2017. She joined the University of Surabaya (UBAYA) as a full-time faculty member in 2018 and is currently serving as an Assistant Lecturer in the Department of Electrical Engineering. She is actively involved in the Telecommunication Engineering specialization, where she teaches courses and supervises student projects related to wireless communications and embedded systems. Her primary research interests lie in the development and optimization of Indoor Positioning Systems (IPS), with a particular emphasis on IoT integration, location-aware services, and lightweight network security mechanisms to support smart environments. In addition to her teaching and research, she has participated in various interdisciplinary projects involving real-time positioning, mobile applications, and geofencing technologies for smart campus and smart mobility solutions. She can be contacted via email at: rafina@staff.ubaya.ac.id

Corresponding author: Rafina Destiarti Ainul, rafina@staff.ubaya.ac.id, Department of Electrical Engineering, Universitas Surabaya, Jl. Raya Kalirungkut, 60293, Surabaya, Indonesia.
Digital Object Identifier (DOI): https://doi.org/10.35882/ijeeemi.v7i4.123