International Journal of Science and Technology (IJST) | ISSN(O):2049-7318 | 2(4):57-60, 2026 | DOI:10.5281/zenodo.21406303

IoT Based Smart Bike Security System and Fingerprint Ignition

Mr. G. Venu Babu, G. V. Venkateswara, S. Shakeer, O. Narendra, K. Uday Kumar

Department of Computer Science and Engineering, Aditya College of Engineering, Madanapalle

Abstract: The smart bike security system is an IoT-based solution designed to improve vehicle safety, access control, and emergency response. The proposed system replaces conventional key-only operation with fingerprint-based ignition, remote engine control through a Telegram bot, and a manual key for backup use. ESP32 and ESP8266 modules provide the communication layer for sensor processing, wireless connectivity, and user interaction. The system also integrates a Neo-6M GPS module for real-time location tracking and a flame sensor with buzzer and LED alerting for fire detection. During testing, the system authenticated authorized users, denied unauthorized access, responded to remote control commands, and transmitted security and emergency alerts with location details. The overall design provides a cost-effective and reliable solution for two-wheeler security using biometric authentication and IoT monitoring.

Index Terms: biometric authentication, ESP32, GPS tracking, IoT, smart bike security, Telegram bot.

INTRODUCTION

Vehicle theft and unauthorized access remain major concerns for two-wheeler owners. Conventional bike security systems depend mainly on mechanical keys, which can be duplicated, misplaced, or misused. The project titled "IoT-Based Smart Bike Security System and Fingerprint Ignition" addresses this limitation by combining biometric authentication with IoT-based monitoring and control. The system allows only authorized users to start the bike through fingerprint verification while also supporting remote engine control and security alerts.

ESP32 acts as the main controller for fingerprint processing and relay control, while ESP8266 supports internet communication for Telegram-based interaction. A Neo-6M GPS module provides real-time location information, and a flame sensor detects fire hazards and triggers buzzer, LED, and message alerts. Together, these modules improve security, monitoring, and emergency response.

PROBLEM STATEMENT

Traditional engine systems rely primarily on physical key-based operation. Such systems are vulnerable to theft and unauthorized misuse, do not provide remote monitoring, and cannot send instant alerts during critical situations. Existing setups also lack real-time location sharing during emergencies and do not offer an integrated solution that combines biometric security, remote control, backup manual operation, and hazard detection.

LITERATURE REVIEW

Recent studies on smart bike security, anti-theft monitoring, and fingerprint ignition emphasize multi-layer authentication and IoT-assisted monitoring. The following related works influenced the design of the proposed system and show why secure ignition, tracking, and alerting should be integrated into one connected platform.

RFID and Fingerprint-Based Smart Bike Ignition System (2025)

This study reported that hybrid RFID and fingerprint authentication improves ignition security reliability. The work shows that multi-factor access control is effective in reducing unauthorized vehicle starts, but it does not focus on emergency alerting or real-time remote owner interaction.

Biometric-Based Bike Ignition System Using IoT (2024)

O. Mhaske highlighted that biometric verification integrated with IoT improves bike safety and enables remote monitoring. The study supports network-assisted access control, but its scope is limited in terms of fire detection, backup control, and integrated tracking.

Bike Anti-theft System using IoT (2023)

This work emphasized GPS tracking and alert notification for real-time theft detection. It proved that IoT connectivity helps the owner locate and monitor the vehicle remotely, though the system does not center on fingerprint-based ignition.

Design, Implementation, and Evaluation of a Fingerprint-Based Ignition Key for Motorcycles (2020)

Heru Supriyono et al. showed that fingerprint ignition can replace traditional mechanical keys and improve motorcycle security. The work strongly supports biometric access control, although it does not integrate complete IoT-based remote monitoring and emergency messaging.

BiSafe: An IoT-Based Smart Bike Security System (2025)

J. Suganya et al. proposed an IoT-enabled bike protection framework that combines monitoring and security functions for two-wheelers. Their results support the value of connected vehicle protection and instant owner notification.

Smart Vehicle Security Authentication Based System using Fingerprint (2025)

P. Sai Keerthana, V. Shavali, and L. Rangaswamy focused on fingerprint-driven vehicle security authentication. Their findings strengthen the case for biometric ignition by showing that fingerprint verification can minimize key misuse and unauthorized access.

Anti-Theft Protection of Vehicle by GSM GPS with Fingerprint Verification (2018)

N. Bala Sundara Ganapathy et al. combined GPS location sharing, GSM communication, and fingerprint verification for vehicle protection. This work indicates that effective anti-theft systems are those that fuse identity verification with real-time location transmission and user alerts.

PROJECT OBJECTIVES

- To enhance bike security using IoT-based monitoring and protection against unauthorized access.
- To allow only authorized users to start the bike through fingerprint authentication.
- To enable remote engine lock and unlock through Telegram-based control.
- To provide real-time GPS tracking and instant alert notification during theft or emergency situations.
- To include fire detection and backup manual control for improved reliability and user safety.

EXISTING METHODOLOGY AND LIMITATIONS

Existing bike security setups rely mainly on mechanical keys. Such systems do not provide biometric authentication, remote engine control through mobile or internet connectivity, or integrated fire detection and alerting. In practical use, this creates a single-point access mechanism that is vulnerable to theft, duplication, and delayed response during emergencies.

The major limitations identified from the project review documents are high risk of engine theft, lack of real-time monitoring, delayed response during fire accidents, no GPS-based emergency location sharing, and poor operational flexibility. These limitations motivated the design of an integrated system that combines fingerprint ignition, Telegram-based control, GPS tracking, fire alerts, and manual backup control.

PROPOSED METHODOLOGY

The proposed system integrates fingerprint authentication, Telegram-based remote control, GPS tracking, fire detection, and manual backup operation. The user first interacts with a fingerprint-enabled mobile application. If the scanned fingerprint matches a registered template, the ESP32 activates the relay module and allows engine ignition. If the fingerprint does not match, access is denied.

For remote operation, the owner can issue commands through a Telegram bot. ESP8266 receives these commands over the internet and supports lock or unlock actions. A flame sensor continuously monitors for fire or abnormal heat conditions. When a hazard is detected, the system activates a buzzer and LED and sends an alert with GPS coordinates obtained from the Neo-6M module. A manual key switch is also included as a backup path when IoT services are unavailable.

Figure 1. System architecture of the proposed smart bike security system.

SYSTEM MODULES

A. Fingerprint Authentication Module

This module uses a fingerprint sensor, ESP32, and a mobile application. The user scans a fingerprint, the template is verified, and the engine is turned on only when a valid match is found. The module prevents unauthorized engine access.

B. Remote Engine Control Module

This module uses ESP8266, a Telegram bot, and internet connectivity. The owner sends commands through Telegram, the ESP8266 receives the command, and the engine is locked or unlocked remotely.

C. GPS Tracking and Alert Module

The GPS module acquires latitude and longitude and forwards the location to the user. It is especially useful during theft, tampering, or emergency events.

D. Fire Detection and Backup Control

The flame sensor continuously detects fire hazards. On detection, the system activates the buzzer and LED and sends

an alert notification.

E. Manual Key Control Module

This module uses a key switch and relay path to provide direct control when internet service is unavailable or when the owner prefers manual operation. It improves system reliability by ensuring that the bike can still be operated safely even if remote services fail.

DESIGN CONSIDERATIONS

Security is the primary design concern of the proposed system. Fingerprint authentication is used as the first level of access control so that only registered users can activate the ignition path. Remote commands are limited to the authorized owner through the Telegram interface, which adds monitoring flexibility without removing access restrictions.

Reliability and real-time response are also important. The prototype uses dedicated sensing and control modules so that fire alerts, GPS location updates, and ignition actions are performed without significant delay. Manual key control is retained as a backup path to avoid singlepoint failure when remote services are unavailable.

Power efficiency and maintainability were also considered during design. Since the system is intended for a two-wheeler platform, the selected microcontrollers and sensors must operate with moderate power usage while remaining easy to program, test, and replace during maintenance.

ADVANTAGES OF PROPOSED SYSTEM

The proposed system provides high security through biometric authentication and reduces the dependence on mechanical keys alone. It improves user convenience by allowing remote engine control through Telegram, while GPS tracking strengthens theft recovery capability.
The integration of fire detection, buzzer and LED alerts, and location-based emergency notification improves overall rider safety. Because the design combines security, monitoring, backup control, and IoT communication in one platform, it is more practical and reliable than conventional single-function systems.

HARDWARE AND SOFTWARE REQUIREMENTS

The hardware configuration of the proposed prototype includes ESP32, ESP8266, a fingerprint sensor, flame sensor, Neo-6M GPS module, relay module, buzzer, LED indicator, manual key switch, breadboard, jumper wires, power supply, L298N motor driver, and a gear motor used in place of the engine during testing. These components together support authentication, communication, sensing, control, and emergency alert generation.

The software stack includes Arduino IDE, ESP32 and ESP8266 board packages, Telegram bot service support, fingerprint mobile application utilities, and required GPS and IoT libraries. Arduino IDE was used to compile and upload the embedded code, while the serial monitor and mobile interface were used during verification of authentication, tracking, and alert outputs.

RESULTS AND DISCUSSION

Testing showed that the complete system responded correctly to authorized and unauthorized fingerprint attempts, remote engine control requests, GPS tracking operations, and fire alert scenarios. Output testing verified that the mobile application and serial monitor produced meaningful authentication, location, and alert information. User acceptance testing also confirmed that the system successfully prevents unauthorized access and supports secure bike operation.

Figure 2. Representative outputs: fingerprint ignition, telegram engine control, and fire alert notification.

Integration testing was used to verify whether fingerprint authentication, IoT communication, GPS tracking, and relay-based ignition control work correctly when integrated together. System testing confirmed that registered fingerprints start ignition, unauthorized fingerprints deny access, and GPS information is displayed accurately to the user. Validation and user acceptance testing further demonstrated that the prototype satisfies the intended security and monitoring requirements.

CONCLUSION AND FUTURE SCOPE

The IoT Based Smart Bike Security System with Fingerprint Ignition was designed and implemented as a secure and intelligent solution for two-wheeler protection. By combining biometric authentication, remote monitoring, GPS location sharing, and fire detection, the system improves both security and emergency response. The design is cost-effective, user-friendly, and suitable for real-world smart vehicle applications.

Future enhancements suggested in the project documents include multi-level authentication such as face recognition,

cloud storage for tracking history and logs, dedicated mobile application integration, GSM-based alerting, and deeper cloud integration for real-time monitoring and secure data storage.

REFERENCES

1. J. Suganya et al., “BiSafe: An IoT-Based Smart Bike Security System,” Int. J. Eng. Res. Technol., vol. 14, no. 12, 2025.
2. P. S. Keerthana, V. Shavali, and L. Rangaswamy, “Smart Vehicle Security Authentication Based System using Fingerprint,” J. Adv. Electron. Signal Process., 2025. [3] S. Sadhukhan, A. Acharyya, and R. Prasad, “Car Security System using Fingerprint Scanner and IoT,” Indian J. Sci. Technol., vol. 10, no. 40, 2017.
3. B. Saritha et al., “An Intelligent Anti-Theft Vehicle Locking System Using IoT,” Lecture Notes Electr. Eng., Springer, 2022.
4. L. Sreeja et al., “Smart System for Rider Safety and Bike Security,” Int. J. Res. Appl. Sci. Eng. Technol., 2025.
5. N. Bala Sundara Ganapathy, S. Akash, R. Alex Prabhu, T. Kirubakaran, and S. Shyam Kumar, “Anti-Theft
6. Protection of Vehicle by GSM GPS with Fingerprint Verification,” Int. J. Adv. Eng. Manage. Sci., 2018. [7] O. Mhaske, “Biometric Based Bike Ignition System Using IoT,” 2024.