Arjun M, 2026, 14:1
ISSN (Online): 2348-4098
ISSN (Print): 2395-4752

International Journal of Science, Engineering and Technology
An Open Access Journal

MotoGuard: Smart IoT-Based Two-Wheeler Anti-Theft Detection System

Arjun M, Ammu K Reji, Akhil Shaji, Meenu M R, Dr.Rani Saritha R
Department Of Computer Application Saintgits College Of Engineering Kottayam, Kerala,India

Abstract - In this work, MotoGuard, a smart IoT-based two-wheeler anti-theft detection system, is designed and evaluated to provide real-time monitoring and instant alerts. The system uses an ESP-32 microcontroller integrated with SW-420 and MPU6050 sensors to detect unauthorized movement, shock, or tampering. Detected events are transmitted to Firebase cloud services, and alerts are delivered to an Android application developed using Kotlin and Jetpack Compose. Experimental results show reliable detection with minimal false alerts after threshold tuning, and alert delivery latency within one to two seconds. The results indicate that MotoGuard is a low-cost, effective, and scalable solution for improving two-wheeler security through real-time alerting and continuous monitoring.

Keywords - IoT, Anti-Theft System, ESP32, Firebase, Vibration Sensor, Android App, Real-Time Alerts.

I. INTRODUCTION

Two-wheeler theft remains a persistent security issue due to the widespread use of inadequate protection mechanisms. Mechanical locks and basic alarm systems provide only localized security and fail to notify owners remotely. GPS- based tracking systems, although effective, introduce recurring subscription costs and may suffer from signal unavailability in certain environments.

With the advancement of Internet of Things (IoT) technology, smart security systems have gained significant attention. MotoGuard addresses these limitations by introducing an IoT-enabled anti- theft system capable of detecting unauthorized vibration or movement and notifying the owner instantly through a mobile application. The system integrates sensor-based detection, cloud communication, and mobile visualization to provide continuous monitoring with minimal cost and complexity.

Proposed System

The MotoGuard system is designed to detect unauthorized movement of a two-wheeler and notify the owner instantly. The system consists of hardware, cloud, and mobile application components. The ESP-32 microcontroller continuously monitors vibration and motion data from the SW-420 and MPU6050 sensors. When abnormal movement is detected beyond predefined thresholds, the system triggers an alert event.

The detected data are transmitted to Firebase cloud services using Wi-Fi connectivity. An Android application receives these alerts in real time and displays relevant information such as alert time, movement intensity, and approximate location. The system also stores historical data for future reference and analysis. The stored data enable users to review past security events and identify recurring patterns of suspicious activity. This improves situational awareness and supports better decision-making for enhancing vehicle security

System Architecture

The system architecture is composed of three integrated modules that work together to ensure effective theft detection and user notification. The sensor module includes vibration and motion sensors that continuously monitor the vehicle for shocks, tilting, or unauthorized movement. Data collected from these sensors are processed by the ESP-32 microcontroller in the processing and alert module, where sensor values are compared against predefined threshold levels to identify suspicious activity. When abnormal movement is detected, alert information is transmitted to the cloud in real time. The user module consists of an Android application that provides a user-friendly interface for displaying real-time alerts, alert history, and overall system status, enabling vehicle owners to monitor security events efficiently

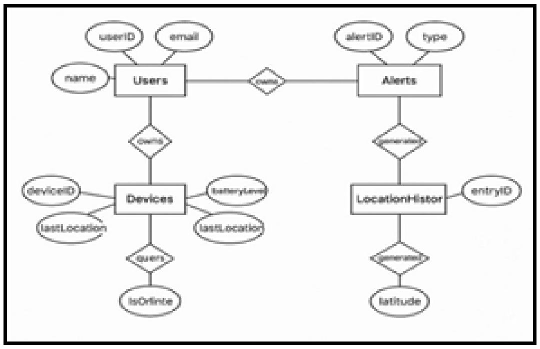

Figure 1: System Architecture

Result and Discussion

The system was tested under different vibration conditions to evaluate detection accuracy and response time. Results indicate that the MotoGuard system effectively detects unauthorized movement with minimal false alerts after proper threshold tuning. The average alert delivery time ranged between one and two seconds. The mobile application performed efficiently across different Android devices, providing smooth navigation and real-time updates.

Limitations

Despite its effectiveness, the system has certain limitations. The use of Wi-Fi-based location tracking provides only approximate location accuracy. High-vibration environments may occasionally trigger false alerts. Additionally, continuous Wi-Fi connectivity is required for real- time alert transmission.

Future Enhancement

Future improvements include the integration of a GPS module for precise location tracking, GSM/LTE connectivity for improved network coverage, and geofencing features for enhanced security. Machine learning techniques can also be applied to distinguish between normal and suspicious movements, reducing false alerts.

II. CONCLUSION

Future improvements include the integration of a GPS module for precise location tracking, GSM/LTE connectivity for improved network coverage, and geofencing features for enhanced security. Machine learning techniques can also be applied to distinguish between normal and suspicious movements, reducing false alerts.

REFERENCES

1. S. Napitu, “IoT-Based Visitor Monitoring Tool for Reading Rooms,” IJACSA, 2021.
2. A. Kishor et al., “Smart Bi-Directional Visitor Counter System Using IoT,” IJERT, 2020.
3. X. Zhao et al., “Cloud–Edge Collaborative Computing,” IEEE Access, 2020.
4. Espressif Systems, “ESP32 Technical Reference Manual,” 2022.
5. P. Prabhulkar, S. Gupta, and R. Kumar, “Automated Vehicle Security System Using IoT and Mobile Application,” International Journal of Scientific Research in Computer Science, vol. 9, no. 2, pp. 44–49, 2021.
6. R. Singh and A. Kumar, “Smart Vehicle Monitoring and Theft Detection System Using IoT,” International Journal of Emerging Trends in Engineering Research, vol. 8, no. 5, pp. 1650–1655, 2020.