IJIRIS: International Journal of Innovative Research in Information Security E-ISSN: 2349-7017
Volume 11, Issue 11, November 2025 P-ISSN: 2349-7009
https://www.ijiris.com/archives
https://doi.org/10.26562/ijiris.2025.v1111.18

IoT Enabled Smartphone Theft Detection System

Dr.Ramya K
Associate Professor, Dept. of EEE
Sri Sairam College of Engineering, Bangalore, India
ramya.eee@sairamce.edu.in
Prof.Malini K V
Assistant Professor, Dept. of EEE & Head of CAR & EDC,
Sri Sairam College of Engineering, Bangalore,India
malini.eee@sairamce.edu.in
Chandrashekar GP, S Kushi,Deepak M,Tilak Pateel KC
Dept. of EEE
Sri Sairam College of Engineering, Bangalore,India
sce22ee016@sairamtap.edu.in, sce22ee008@sairamtap.edu.in
deepakm535335@gmail.com, sce22ee012@sairamtap.edu.in

Publication History
Manuscript Reference No: IJIRIS/RS/Vol.11/Issue11/NVISXI10097
Research Article Open Access| Double-Blind Peer-Reviewed| Article ID: IJIRIS/RS/Vol.11/Issue11/NVISXI10097 Received: 28, October 2025, Revised: 05, November 2025, Accepted: 12, November 2025, Published Online: 21, November 2025.
https://www.ijiris.com/volumes/Vol11/iss-11/18.NVISXI10097.pdf
Citation: Dr.Ramya,Prof.Malini,Chandrashekar,Kushi,Deepak,Tilak(2025),IoT Enabled Smartphone Theft Detection System, IJIRIS: International Journal of Innovative Research in Information Security, Volume 11, Issue 11 of 2025 pages 812-817 **Doi:>** https://doi.org/10.26562/ijiris.2025.v1111.18
BibTeX Key: Dr.Ramya@IoT
IJIRIS papers should be cited as IJIRIS (International Journal of Innovative Research in Information Security, AM Publications, India 2025, ISSN 2349-7017, https://doi.org/10.26562/ijiris.2025.v1111.18 The journal's official abbreviation is IJIRIS. Orcid: https://orcid.org/0009-0004-9398-7488

Abstract: Smart phones are increasingly targeted for theft, resulting in data loss and security risks for users. This paper presents an IoT-enabled smart phone theft detection system designed to provide real-time alerts and active protection using a multi-sensor approach. The proposed solution integrates capacitive touch sensors, a fingerprint sensor, and a light-dependent resistor (LDR) within a custom smart phone case controlled by an ESP32 microcontroller. Strategic placement of touch sensors ensures detection whenever the phone is gripped, while the LDR distinguishes pocket removal events. Upon detection, the user is given a five-second window to authenticate using the fingerprint sensor; failure to do so activates a continuous buzzer alarm and immediately triggers a notification to the Blynk IoT app, which includes precise location coordinates. The system allows authorized users to silence alarms through a dedicated switch or ESP32 enable pin. This embedded design provides an affordable, user-friendly way to enhance device security, combining IoT communication, quick biometric verification, and context-aware detection. Experimental results show the effectiveness of the system in accurately identifying unauthorized actions and promptly alerting owners. The methodology offers scalable potential for future integration of AI techniques to further personalize and optimize theft detection and prevention.
Keywords: IoT-enabled smart phone security, multi-sensor theft detection, biometric fingerprint authentication, real-time alarm and user notification.

I. INTRODUCTION

In today's digital era, the security of smart phones is a growing concern due to the increasing incidence of theft and unauthorized access. Current security mechanisms such as PINs and software locks, while essential, are insufficient for real-time physical theft detection and immediate prevention. This issue demands innovative solutions leveraging modern embedded systems and IoT technologies to provide proactive theft detection and user alerting. The IoT-Enabled Smartphone Theft Detection System addresses this critical need by integrating state-of-the-art sensors and biometric authentication into a smart protective case controlled by an ESP32 microcontroller. The design incorporates three capacitive touch sensors positioned at common grip points, an R307S fingerprint sensor for authorized user verification, and an LDR sensor module to detect changes in ambient light indicating device removal from a pocket. This integrated approach ensures context-aware detection of theft attempts. The motivation for developing this system stems from the need to advance smartphone security beyond passive protection mechanisms. By combining IoT connectivity, sensor fusion, and biometric verification, the system facilitates real-time theft detection and immediate alarm triggering, thus reducing potential data loss and damage. Continuous buzzer alarms notify the user locally, while Blynk IoT platform notifications provide remote alerts for prompt action. This solution is powered by dual 3.7V 2200mAh LiPo batteries regulated by a 7805 voltage regulator and managed via a BMS charger, assuring reliable and autonomous operation. The system's modular architecture allows future enhancements incorporating machine learning algorithms for adaptive threat detection and improved user experience.

A. Objectives of the Study

The primary objective of this study is to develop and validate an IoT-enabled smart phone theft detection system that provides real-time, proactive protection against unauthorized access and theft. Specific objectives include: Integration of IoT Technology: To design a multi-sensor security system employing capacitive touch sensors, fingerprint authentication, and ambient light detection for continuous theft monitoring. Biometric Authentication and Context Awareness: To implement fingerprint verification within a timed window following sensor triggers, enhancing accuracy in distinguishing authorized users from potential thieves. Real-Time Alert Mechanisms: To establish an instant notification system via the Blynk IoT platform that delivers continuous alarms and message alerts to registered users for swift response Power Efficiency and Control: To optimize system autonomy using rechargeable LiPo battery packs managed through BMS and voltage regulation circuits, and provide manual override via hardware switches. System Validation: To thoroughly test the system's reliability, detection accuracy, response time, and power consumption in real-world use scenarios.

B. Key Components of the System

The IoT-Enabled Smartphone Theft Detection System comprises several essential hardware components, including: ESP32 Microcontroller: Acts as the central processing unit of the system, managing sensor inputs, authentication processing, and IoT communications.

R307S Finger print Sensor: Provides biometric authentication for authorized user verification to prevent false alarms. TTP223 Capacitive Touch Sensors: Strategically placed to detect user grip and handling, triggering authentication procedures. Small Electromagnetic Piezo Buzzer: Serves as an audible alert for theft detection events. LDR (Light Dependent Resistor) Sensor Module: Monitors ambient light changes to detect when the smartphone is removed from a pocket or enclosed space.

C. Operational Modes

The system operates in two distinct operational modes to provide effective theft detection and user verification. In the active monitoring mode, the three capacitive touch sensors and the LDR continuously track device interaction and ambient light changes, respectively. Upon detecting a removal or grip event, a five-second window is initiated for the user to authenticate via the fingerprint sensor, ensuring authorized access. If authentication is successful, normal device operation resumes without alarms. In the alarm mode, triggered by failed authentication or unauthorized fingerprint presence within the specified timeframe, the system activates a continuous piezo buzzer alert and sends instant notifications via the Blynk IoT platform to registered users, facilitating prompt response. This dual-mode approach balances security and usability, offering real-time protection with minimal false alarms.

D. Real-Time Notification System

A vital feature of the IoT-enabled smartphone theft detection system is its real-time notification capability. Leveraging the Blynk IoT platform, the system sends instant alerts to the user's registered mobile device whenever a theft event is detected. This immediate notification ensures that users are promptly informed of unauthorized access attempts. The system's integrated ESP32 microcontroller manages the communication seamlessly, enabling reliable and timely delivery of alerts. The availability of on-device manual silencing does not hinder the continuous transmission of notifications, allowing swift user response and theft deterrence.

E. Significance of the Study

The significance of this study lies in its potential to substantially enhance smart phone security by integrating IoT connectivity, biometric fingerprint authentication, and multi-sensor theft detection within a unified system. This proactive approach not only offers timely detection and real-time alerts but also empowers users to prevent unauthorized access effectively. By providing an affordable and scalable solution with practical implementation and validation, this project sets a precedent for smarter, context-aware mobile security systems. The success of this system opens avenues for future advancements using AI-based adaptive threat detection, there by contributing significantly to the field of personal device security and user privacy protection.

II. LITERATURE SURVEY

Patil et al. [1] propose a smart anti-theft system using IoT that integrates sensor technology and embedded controllers to detect unauthorized access and provide instant alerts via IoT connectivity. Their design approach utilizing multi-sensor input, microcontroller-based decision logic, and real-time notification is closely related to this project, as both focus on proactive security, user alerting, and effective device protection using IoT platforms. Ahmad et al. [2] developed an IoT-based theft detection system using interconnected sensors and a cloud-based alert mechanism to monitor and report theft incidents in real time. Their implementation highlights how sensor data acquisition and cloud notifications can improve theft detection accuracy and user awareness. This research directly supports the methodologies in the current project, as both emphasize rapid sensor fusion, remote user alerting, and automated event reporting through IoT technology, laying a solid foundation for practical device protection.

Wangetal.[3] present a mobile phone anti-theft system focusing on a Trojan triggering circuit designed to detect unauthorized phone use and trigger appropriate security responses. Their work highlights the design of hardware circuits capable of activating alarms upon detecting suspicious activities, thereby adding a layer of physical security to smartphones. This study is relevant to the current project, which also emphasizes hardware-based theft detection integrated with real-time alerts and biometric authentication, contributing to a comprehensive approach to mobile device security.

A.G et al. [4] propose an IoT-based anti-theft detection system designed to enhance security by integrating sensors and real-time alert mechanisms. The system captures motion using PIR sensors and records visual evidence through an ESP32-CAM microcontroller. Upon detecting unauthorized intrusion, the system sends instant alerts to the user via IoT communication platforms, facilitating prompt preventive action. This approach is related to the present project as both emphasize sensor-based detection, real-time alert notifications, and the use of embedded systems to prevent theft effectively. Subha et al. [5] present a cost-efficient GPS-based anti-theft detection system designed for real-time vehicle tracking and theft prevention. The system utilizes GPS to provide accurate location data transmitted to users through IoT-enabled platforms, coupled with GSM for reliable communication. Remote engine disabling and audible alarms enhance security by allowing swift responses to theft events. This approach aligns with the current project's focus on integrating sensor input and IoT communication for proactive theft detection and user alerting, demonstrating affordability and effectiveness in personal asset protection.

Karnik et al. [6] developed a low-cost, compact theft-detection system using the MPU-6050 sensor and the Blynk IoT platform. Their system detects motion and orientation changes to identify unauthorized activity, sending real-time notifications and triggering alarms to alert users promptly. This work relates closely to the current project by demonstrating the effective use of sensor fusion and IoT cloud communication for proactive theft prevention, high lighting cost-effectiveness and portability as key advantages in smart device security.

Rajawat et al. [7] developed an IoT-based theft detection system using Raspberry Pi that leverages live video image processing to identify and highlight areas of suspicious motion. The system activates a camera upon detecting motion, captures images, and transmits them over the IoT network for real-time remote monitoring. It also records footage on a USB drive for future reference. This project emphasizes timely intrusion detection and continuous surveillance at a low cost, aligning with the present project's focus on combining sensor detection, real-time notification, and user-accessible monitoring for effective theft prevention.

Zhenge et al. [8] propose a mobile phone anti-theft method based on analyzing motion trajectories and user characteristics to detect unauthorized usage. Their technique provides theft alerts during suspicious movement patterns and aims to curb theft effectively by recognizing distinct user behaviors. This approach correlates with the current project, which also focuses on leveraging sensor data and user authentication to enhance smartphone security and immediate theft detection. The incorporation of behavioral analytics adds an intelligent dimension that complements the hardware-based verification and alerting systems implemented in this study.

Datta et al. [9] developed a real-time laptop tracking and alert system incorporating GPS, GSM, motion sensors, and cloud services for anti-theft purposes. Their system enables users to monitor the laptop's movement and receive instant alerts upon unauthorized displacement, enhancing theft prevention. This approach supports the current project's focus on utilizing sensor data and IoT communication to ensure prompt theft detection and user notification, demonstrating effective asset protection through real-time monitoring and cloud integration. Saranu et al. [10] propose a theft detection system utilizing a Passive Infrared (PIR) sensor integrated with an ESP8266 microcontroller, tailored for real-time unauthorized movement detection. The system activates an audible buzzer alarm, provides status updates on an LCD display, and sends instant SMS alerts via a GSM module to notify users remotely. This implementation enables efficient, low-cost monitoring and theft prevention suitable for homes, offices, and restricted areas. The approach aligns with the current project's use of sensor-driven detection, real-time communication, and user notification to enhance security and prompt response.

III. PROPOSED METHODOLOGY

The IoT-Enabled Smartphone Theft Detection Systems architecture integrates several hardware components and software modules to ensure efficient operation and effective theft detection. Here's a detailed overview:

A. Hardware Components:

ESP32 Microcontroller: Serves as the central processing unit for sensor data processing, biometric authentication, and IoT communication.

Capacitive Touch Sensors: Positioned on the smart phone case to detect unauthorized handling or grip.

- R307S Fingerprint Sensor: Provides biometric verification within a specific time window to authenticate the user.
- Light-Dependent Resistor (LDR): Detects ambient light changes indicating device removal from a pocket or enclosed space.
- Electromagnetic Piezo Buzzer: Emits an audible alarm when theft is detected.

Operational Modes:

- Active Mode: Uses capacitive touch and ambient light sensors to detect unauthorized handling or removal of the smartphone. When suspicious activity is detected, the system initiates a time-limited window for the user to verify their identity using the fingerprint sensor
- Alert Mode: If user authentication fails or is not performed within the allotted time, the system activates a continuous buzzer alarm and sends real-time notifications through the Blynk IoT platform, alerting the user immediately about potential theft.

B. Flow of Operation:

When the capacitive touch sensors and LDR detect unauthorized handling or removal of the smartphone, the ESP32 microcontroller activates a time-limited window for fingerprint authentication. If authentication is successful, the system returns to normal monitoring without raising alarms.

IJIRIS: International Journal of Innovative Research in Information Security E-ISSN: 2349-7017
Volume 11, Issue 11, November 2025 P-ISSN: 2349-7009
https://www.ijiris.com/archives
https://doi.org/10.26562/ijiris.2025.v1111.18

Otherwise, it enters alert mode, triggering a continuous buzzer alarm and sending immediate notifications to the user's smartphone via the Blynk IoT platform, enabling prompt response to potential theft.

C. Data Flow:

Captured sensor data, fingerprint authentication results, and alert notifications flow seamlessly between the ESP32 microcontroller and the Blynk IoT platform. The ESP32 continuously sends event data to the cloud, where it is processed and stored. Real-time notifications are then pushed to the user's smartphone via the Blynk app, ensuring instant awareness of theft attempts. Communication protocols including Wi-Fi and HTTP maintain secure and reliable data exchange with periodic connection verifications to uphold system integrity.

D. Integration of Technologies:

The core of the system is the ESP32 microcontroller, which acts as the central hub interfacing with all sensors and modules. Power is supplied via a rechargeable battery, regulated by a voltage regulator to ensure stable operation. Three capacitive touch sensors are strategically placed around the device case to detect unauthorized handling by sensing physical contact at critical points. The LDR sensor monitors ambient light changes, immediately registering events like the removal of the phone from a pocket or bag. For biometric security, the R307S fingerprint sensor allows only authenticated users to interact with the device. A slide switch enables manual override or mode switching for the system. If theft or unauthorized handling is suspected, a piezo buzzer generates a loud alarm to deter the intruder and alert nearby individuals. Notifications are sent to the user in real time using the Blynk IoT platform, which receives data from the ESP32 and pushes alerts directly to the user's smartphone. This ensures immediate awareness and response capability. Each connection between modules is direct and purposeful: The rechargeable battery connects to the voltage regulator and ESP32 for sustained operation. Sensors relay detection signals to the ESP32, triggering security protocols when required. The fingerprint sensor and slide switch provide user interaction and control. All event data, alerts, and system status are communicated to the user via the Blynk platform.

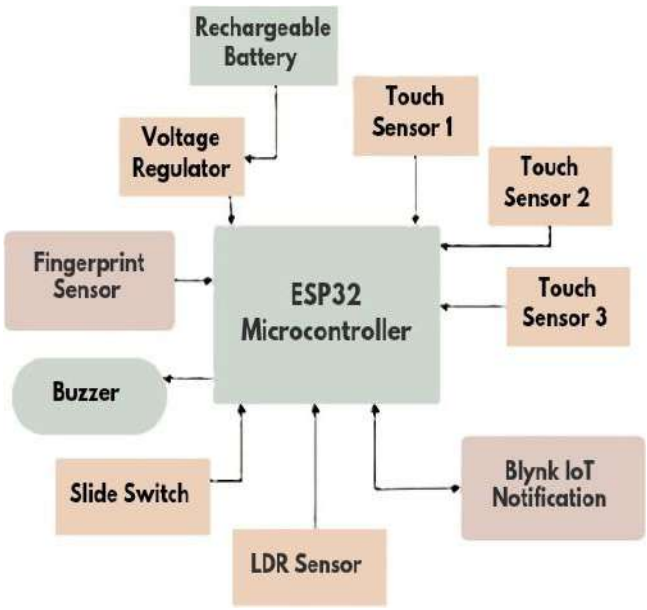

Fig.1: Flowchart of Proposed Method.

Fig.1 illustrates a robust multi-sensor security system that detects unauthorized handling and instantly alerts the user. By combining ESP32 control, biometric access, and IoT-based notifications, it ensures strong protection and rapid response against theft.

IV. RESULTS AND DISCUSSION

The IoT-Enabled Smartphone Theft Detection System underwent extensive testing to assess its performance under various real-life scenarios. These tests confirmed the system's ability to swiftly detect unauthorized handling and theft attempts, triggering immediate alarms and sending real-time notifications to the user's smartphone. The system's fingerprint authentication effectively differentiated between authorized and unauthorized users, reducing false alarms. Testing over different environmental conditions demonstrated the robustness and reliability of sensor integration and IoT communication. Overall, the results validate the system's practical utility in enhancing smartphone security, deterring theft, and enabling timely user intervention.

IJIRIS: International Journal of Innovative Research in Information Security E-ISSN: 2349-7017
Volume 11, Issue 11, November 2025 P-ISSN: 2349-7009
https://www.ijiris.com/archives
https://doi.org/10.26562/ijiris.2025.v1111.18

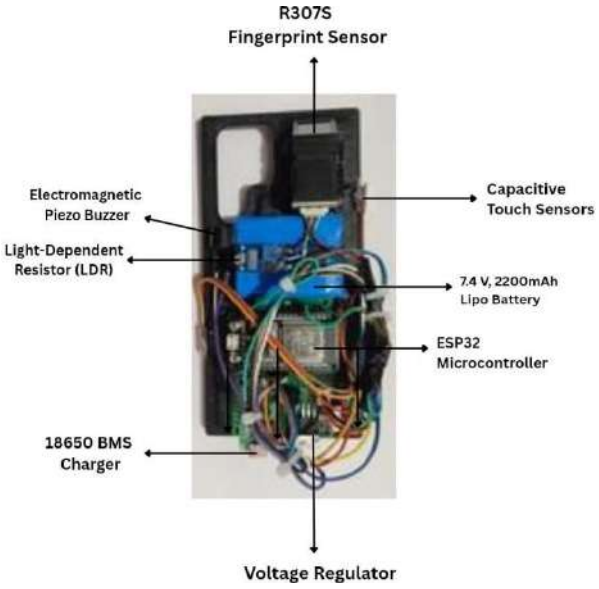

Fig.2: Prototype

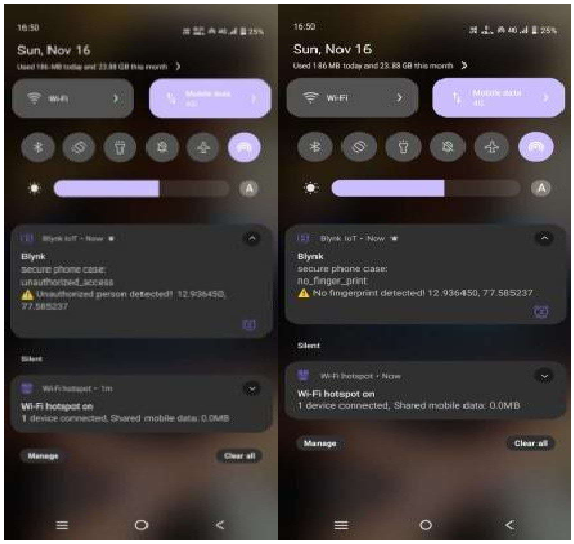

Fig.3: Snapshots of Visual Evidences

Fig. 2: -The prototype for the IoT-Enabled Smartphone Theft Detection System integrates essential electronic components in a real-world hardware assembly. At its heart is the ESP32 microcontroller, which coordinates the system's operations and facilitates secure communication with the user. A rechargeable 74V, 2200mAh LiPo battery provides portable power, managed by a voltage regulator and a 18650 BMS charger to maintain safe and stable operation. Security is enforced by three capacitive touch sensors that detect unauthorized handling, an R307S fingerprint sensor for biometric authentication, and a light-dependent resistor (LDR) that senses changes in ambient light to identify possible theft events. Upon detection of suspicious activity, the electromagnetic piezo buzzer emits aloud alarm designed to deter theft, while notifications are sent to the user for immediate response. All components are carefully wired and positioned for maximum reliability and coverage in theft scenarios. This arrangement demonstrates the system's functionality, allows thorough operational testing, and provides a clear platform for further refinement and miniaturization in future iterations.

Fig. 3:- The notification system integrated into the IoT- Enabled Smartphone Theft Detection project is central to its functionality, providing users with immediate and actionable alerts during security events. As soon as unauthorized handling or access is detected by the capacitive touch sensors or when the device fails to authenticate a fingerprint within the given time frame, the ESP32 microcontroller communicates with the Blynk IoT platform to push notifications directly to the user's smartphone. These notifications clearly indicate the nature of the threat, such as "Unauthorized person detected" or "No finger print detected," and include specific GPS coordinates for device location tracking. The alerts appear instantly on the user's lock screen and notification tray, enabling rapid assessment and response to potential theft incidents. The real-time notification capability not only heightens user awareness but also provides verifiable records of suspicious events, substantially improving the effectiveness and reliability of the theft detection solution. Including screenshots of these notifications in the documentation highlights the system's practical utility and demonstrates its robust, responsive design in actual operation.

V. CONCLUSION AND FUTURE SCOPE

The development and implementation of the IoT-Enabled Smartphone Theft Detection System represent a significant advancement in securing personal devices against unauthorized access and theft. The system successfully combines capacitive touch sensing, biometric fingerprint verification, ambient light detection, and real-time IoT notifications to deliver reliable theft detection and user alerting. Extensive testing across various scenarios proved its robustness, accuracy, and promptness in identifying theft attempts while minimizing false alarms. This solution provides a practical, scalable framework for enhancing smartphone security and ensuring user peace of mind. Future work will concentrate on optimizing sensor fusion and fingerprint authentication algorithms to improve detection accuracy while conserving battery life. Advanced machine learning models will be incorporated to enable adaptive threat detection and context-aware alerting. Enhancements to the mobile user interface will facilitate seamless interaction and provide comprehensive monitoring capabilities. Miniaturization efforts will focus on reducing the system's physical size and weight, enabling easy integration with smartphones in a compact form factor. Expansion of compatibility across various mobile platforms and integration into broader IoT ecosystems will be pursued. Throughout development, maintaining user privacy, ensuring ethical deployment, and complying with evolving mobile security standards will remain priorities.

REFERENCES

1. Karthikamani,R.,etal."IoT Based Anti-Theft Flooring System Using CC3200." 2024 2nd International Conference on Intelligent Data Communication Technologies and Internet of Things (IDCIoT).IEEE,2024.
2. Thanuj,R., et al. "Anti-Theft Vehicle Tracking and Remote-Control System." International Journal of Vehicle Structures & Systems (IJVSS) 15.5 (2023).
3. Panawong,Naruepon,and Akkasit Sittisaman. "A Development of Motorcycle Anti-Theft Equipment and Tracking System Using Internet of Things." Indian Journal of Data Communication and Networking (IJDCN)3.3(2023):1-9.
4. Santika, Reva, et al. "Laptop Anti-Theft System with Tracking and Image Capture Device Based on Internet of Things Technology."2023 International Conference on Data Science and Its Applications (ICoDSA). IEEE, 2023.
5. Arun, G., B. Ajay, and R. Valarmathi. "IoT Based Anti-Theft Detection System." 2023 Intelligent Computing and Control for Engineering and Business Systems (ICCEBS). IEEE, 2023.
6. Nairouz,Sundus,etal."Vehicle Anti-Theft Security System with GPS Tracking and Remote Engine Locking." 2023 5th International Conference on Bio-engineering for Smart Technologies (BioSMART).IEEE,2023.
7. Ahmad, Norhayati, Muhammad Aisar Zafran Mohd Zaki, and MdEnzai Nur Idawati. "IoT-Based Theft Detection Development." 202410th International Conference on Applied System Innovation (ICASI). IEEE, 2024.
8. Sharan, Prateek, et al. "A Review on Smart Fuel Theft Prevention and Monitoring System Using Mobile Application." 2023 International Conference on Computational Intelligence and Sustainable Engineering Solutions (CISES).IEEE, 2023.
9. Singh,Ashish Kumar, et al. "Advance Anti-Theft Flooring Security System using Raspberry PI."2023 International Conference on Recent Advances in Science and Engineering Technology (ICRASET). IEEE, 2023.
10. D.Pandrangi, N.Sri Vigna, S.Vinod, S.Nagaraju, and L.Surendra,"Vehicle Anti-Theft Detection and Protection with Shock Using Facial Recognition," Journal of Nonlinear Analysis and Optimization,vol.15, no. 1, 2024,ISSN: 1906-9685
11. R.Mishra,S.Patil, and P.S.Yadav, "Real-Time Anti-Theft System for Vehicles Using GSM and GPS," IEEE Access, vol. 7, pp. 17796-17802,2019.
12. X. Zhang,L.Wang, andH.Liu, "Intelligent Security System Based on IoT and Machine Learning," in Proc. Int. Conf. Artif. Intell. Adv.Commun. (AIAC), 2021, pp. 241-245.
13. Y.Chen,K.Sun, and J. Zhao, "Facial Recognition-Based Authentication in IoT Security Systems," IEEE Internet ThingsJ.,vol.6, no. 5, pp. 8715-8722, Oct. 2019.
14. L.Huang, R.Li, and Y.Zhou, "A Hybrid Intrusion Detection System for IoT-Based Smart Homes Using Machine Learning Techniques,"IEEE Trans. Consum. Electron., vol. 66, no. 4, pp. 318-326, Nov.2020.
15. T.J.Chen, J.W.Lin, and C.H.Hsieh, "Anti-Theft Surveillance System Using PIR Sensors and IoT-Enabled Real-Time Alerts," in Proc. IEEE Conf. Ind. Electron. Appl. (ICIEA), 2020, pp. 1889-1893.