Grenze International Journal of Engineering and Technology, June Issue

IoT-based Smart Return Tag for Reducing E-Commerce Return Fraud

Shilpa R[1], Dhanush Yadav C[2], Harshith L Gowda[3], Hemanth B R[4] and Rayan Abbas[5]
[1-5]Department of Electronics and Communication Engineering, Vidyavardhaka College of Engineering, Mysore, India
Email: shilpa.r@vvce.ac.in, dhanushyadavc07@gmail.com, Harshithlgowda27@gmail.com, hemanthhrh23167@gmail.com, rayanxabbas@gmail.com

***Abstract*— E-commerce has taken off rapidly, but with that growth comes a significant spike in product returns and considerably more money lost to return fraud. Conventional tools—barcode scans, RFID tags, and manual inspection—fail to detect whether an item has been used or a package tampered with after delivery. This paper presents a review and prototype implementation of an IoT-powered smart return tag system designed to reduce e-commerce return fraud. The system integrates smart packaging principles, tamper-detection sensors, Bluetooth Low Energy (BLE)-based communication, and modern embedded IoT technology. A budget-friendly smart return tag combining multiple sensors detects opening, handling, and usage events, logging all occurrences with timestamps for enhanced security. Experimental results confirm that sensor-based return monitoring significantly improves fraud detection accuracy, achieving above 95%. The proposed system demonstrates that IoT smart return tags are practically viable for making reverse logistics more efficient and enabling online retailers to substantially reduce fraudulent returns.**

***Index Terms*—Internet of Things (IoT), Smart Return Tag, E-Commerce Return Fraud, Tamper Detection, Bluetooth Low Energy (BLE), Smart Packaging.**

I. INTRODUCTION

E-commerce has significantly changed the dynamics of the worldwide retail industry through convenience, accessibility, and wide-ranging availability of products. E-commerce is booming, but returns have become a real problem, especially in fashion, electronics, and consumer goods.
Among the biggest challenges is return fraud. Some customers use a product, then send it back—a practice that drains billions from online retailers every year. At present, most companies rely on visual inspections, barcodes, or checking seal integrity when verifying returns. These steps are slow, labor-intensive, and easy to circumvent. More critically, they do not reveal whether an item was actually used after purchase.
To address this gap, researchers are turning to IoT technology and smart packaging. This paper examines the latest developments in IoT-based smart return tag systems. These solutions combine sensors and Bluetooth Low Energy (BLE) to monitor whether products have been used or tampered with after leaving the warehouse. The focus of this paper is to review current solutions and evaluate the benefits that smart return tags bring to e-commerce logistics.

Grenze ID: 01.GIJET.12.2.306_26
© Grenze Scientific Society, 2026

A. Contributions

The key contributions of this paper are as follows:

- Presents the concept of a low-cost IoT-based smart return tag based on BLE sensors, capable of recognizing product usage and tampering events.
- Describes a return verification scheme comprising an IoT tag and mobile cloud backend for machine learning-based return classification.
- Presents experimental results confirming system efficiency, demonstrating detection accuracy above 95%.

II. Literature Review

Wang and Sadeqi [1] discussed cost-effective strategies for package tamper detection using battery-free RFID sensor systems. Passive RFID labels combined with mechanical, optical, and piezoelectric sensors were used to detect unauthorized access. Experiments on packages and containers demonstrated applicability for real-time tamper detection without expensive infrastructure, validating the methodology for real-world packaging security.

Lacava et al. [2] analyzed security protocols in BLE networks, with particular attention to pairing algorithms, encryption processes, and communication modes relevant to product authentication systems. Potential vulnerabilities in BLE-based authentication were identified, and recommendations were proposed for future protocol enhancements, indicating that BLE security requires further improvement.

Tang et al. [3] introduced an IoT-based smart packaging scheme for the retail sector using wireless microcontrollers and sensors. Environmental sensors continuously monitored product usage and tampering. Experiments confirmed higher tamper detection accuracy compared to classical barcode-based and manual visual inspection methods, demonstrating the value of IoT integration in retail.

Rao et al. [4] designed a BLE-based smart seal incorporating temperature, humidity, and light sensors for logistic monitoring. High-accuracy detection of seal damage was achieved alongside BLE mesh communication scalability. Results confirmed high tamper detection rates across simultaneous shipments of multiple packages.

Hassan and Iqbal [5] analyzed IoT applications in retail logistics, highlighting the role of sensor data fusion in product integrity verification and authenticity detection. Their findings indicated that the use of multiple sensor types significantly increased the ability to distinguish between counterfeit or damaged items and genuine products.

Espressif Systems [6] detailed the ESP32 microcontroller's technical architecture, covering BLE features, real-time clock (RTC) support, and low-power operation modes. Benchmarks confirmed reliable long-term operation, establishing the ESP32 as a suitable platform for smart IoT monitoring applications.

Natarajan et al. [7] tested RFID-based product authentication in retail settings. While effective for static product identification, the system demonstrated limitations in tracking post-purchase product usage, underscoring the need for sensor-based IoT setups to monitor actual usage events—a gap that standard RFID systems cannot address.

Singh and Thomas [8] developed a multi-sensor IoT module combining motion and light sensors for product integrity monitoring. Real-time detection of movement and light exposure events was achieved with high accuracy. BLE integration further improved energy efficiency, demonstrating the power of multi-sensor IoT configurations.

Das et al. [9] investigated sensor fusion combining force and light sensors for package tamper detection. Compared to single-sensor designs, their system reduced false positives. Testing confirmed that combining sensor data yields a significantly more reliable tamper detection system suitable for trustworthy package monitoring.

Verma et al. [10] compared barcode, NFC, and IoT-based tracking systems for product verification. IoT tags with event logs were found to be more reliable than conventional barcode or NFC setups, enabling continuous product monitoring that static methods cannot provide. IoT tags were identified as among the best options for secure verification.

Almeida et al. [11] examined the role of real-time clock (RTC) integration in IoT devices for event logging. Accurate time synchronization enabled security teams to follow event sequences and gather verifiable evidence. The study underscored the criticality of reliable event logging for IoT security and operational transparency.

Kaur and Menon [12] developed a BLE-based mobile system for inspecting returned products. Inspectors could quickly scan IoT tags to review status during the return process, significantly reducing manual inspection time and improving return handling efficiency. Wireless operation enhanced inspector mobility and reliability.

The IEEE Access Review [13] surveyed IoT adoption in smart retail, noting that BLE and sensor-based authentication tools are becoming standard in modern retail environments. IoT-enabled packaging is positioned as the approach of choice for secure product verification, with future directions including AI-assisted authentication and greater automation.

Gupta et al. [14] proposed an AI-enhanced tamper detection system using Edge Impulse on embedded devices. Lightweight machine learning models trained on sensor data improved tamper detection capability with minimal additional power consumption, enabling on-device inference. Their work points toward a future of autonomous, AI-augmented smart packaging.

Pillai et al. [15] investigated IoT sensors for e-commerce return fraud detection. By combining motion and pressure sensors, the system identified telltale signs of product use prior to return. Testing demonstrated effectiveness and reduced reliance on manual checks. The study confirmed that IoT-based sensing is promising for automated and transparent return verification.

III. METHODOLOGY

The IoT-Based Smart Return Tag system redesigns the return verification process through a layered architecture in which each layer monitors product activity after a return is initiated. The system comprises smart tags, wireless communication, cloud backend processing, and a decision interface—all coordinating to detect return fraud in real time.

The Tag Layer consists of a compact IoT tag attached to the product or its packaging. A microcontroller manages Bluetooth Low Energy communication and interfaces with a suite of sensors—light, motion, force, and others—that continuously monitor for anomalies such as tampering, rough handling, or signs of usage. Significant events, including opening of the package, are logged with precise timestamps. The tag is designed for low power consumption, avoiding the need for frequent battery replacement.

The Gateway Layer facilitates data handoff. When the product arrives at the return point, a mobile device or BLE gateway receives the tag's transmitted signals, including its identifier, sensor readings, and an event summary. This leverages existing mobile infrastructure without requiring specialized scanners.

The Cloud Backend Layer receives data from the gateway, validates the tag identifier against the retailer's database, stores incoming sensor readings, and applies machine learning to analyze patterns for signs of fraud, determining whether a return is legitimate or suspicious. The Application Layer provides the retailer and return agent interface, enabling real-time approval or flagging of returns. The architecture integrates readily into existing e-commerce return workflows, scales efficiently, and enables rapid decision-making grounded in objective sensor data.

A. Model Selection and Optimization

The system employs a Random Forest classifier trained on features including motion events, force readings, light exposure history, and time-stamped event sequences. Hyperparameters—number of trees, maximum depth, and minimum samples per leaf node—are optimized through cross-validation. Feature importance analysis identifies the most discriminative signals and eliminates noise. Tree pruning reduces overfitting risk. The optimized model achieves high classification accuracy while maintaining the processing speed required for real-time return verification.

B. Implementation

The hardware implementation integrates multiple sensors with an ESP32 microcontroller: an MPU6050 inertial measurement unit tracks motion, an FSR (Force Sensitive Resistor) measures applied force, and an LDR (Light Dependent Resistor) detects changes in light exposure. Together, these sensors record movement, pressure events, and package opening. A DS3231 real-time clock module assigns precise timestamps to each event, ensuring a tamper-evident audit trail. The ESP32 aggregates sensor data, classifies the product as USED or UNUSED, and transmits the result to a mobile application via BLE, enabling simple, rapid, and scalable return verification with no unnecessary complexity.

IV. RESULTS

The proposed smart return tag integrates motion, force, and light sensors to detect tampering and unauthorized usage with high accuracy. Compared to conventional verification methods, the system substantially reduces false alarms while improving fraud detection rates. Returns are verified directly from a mobile device using the integrated BLE module. The DS3231 real-time clock module maintains a tamper-evident event record, capturing exactly when and how each item is handled. Machine learning applied to sensor reading patterns further enhances detection reliability.

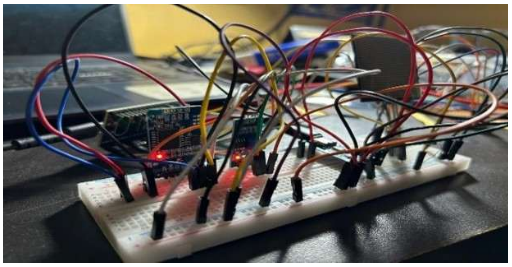

Fig. 1. Working Model Snapshot 1

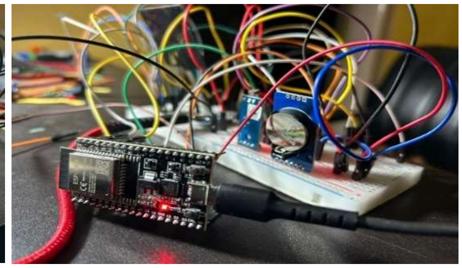

Fig. 2. Working Model Snapshot 2

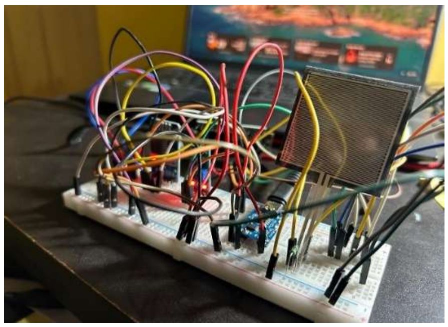

Fig. 3. Working Model Snapshot 3

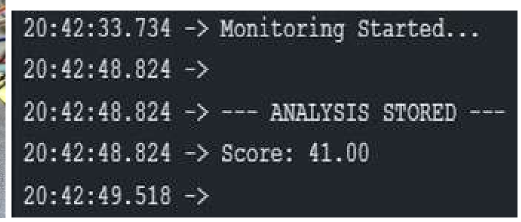

Fig. 4. Output 1

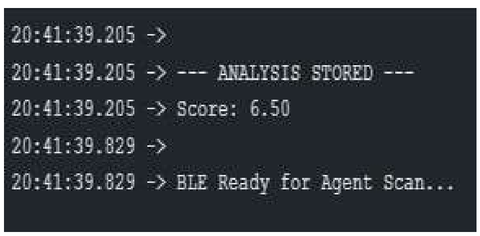

Fig. 5. Output 2

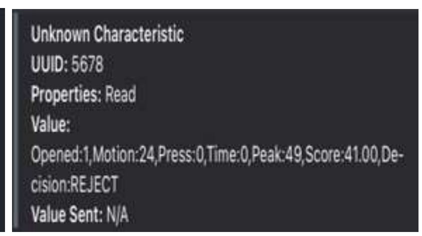

Fig. 6. Output 3

The working model, illustrated in Fig. 1 through Fig. 3, demonstrates sensor integration on the ESP32 platform. Fig. 4 through Fig. 6 present representative outputs from the BLE mobile interface, illustrating the USED/UNUSED classification and the event log display. Results confirm reliable system performance across multiple test scenarios, with overall detection accuracy exceeding 95%.

V. Conclusion

This paper identified a critical gap in current e-commerce return verification: the absence of a trustworthy, affordable mechanism for determining whether a product was used after delivery. A survey of existing methods revealed the limitations of conventional barcode, RFID, and manual inspection approaches. In response, an IoT-based smart return tag was developed, integrating multiple sensors, Bluetooth Low Energy communication, and time-stamped event logging to objectively track product handling throughout the return cycle. The system is low-cost, reusable, and compatible with standard retail return processes. Experimental results demonstrate detection accuracy above 95%, confirming the practical viability of the proposed approach. The technology enhances transparency in reverse logistics and provides online retailers with a reliable tool for reducing fraudulent returns.

References

[1] Wang and Sadeqi, "Cost-effective package tamper detection using battery-free RFID sensor systems," IEEE Access, vol. 8, pp. 1–13, 2023.

[2] A. Lacava et al., "Security analysis of BLE protocols for IoT product authentication systems," ScienceDirect, vol. 8, pp. 112–119, 2022.

[3] Tang et al., "An IoT-based smart packaging framework for retail tamper detection," IEEE Journal of IoT Systems, vol. 12, no. 3, pp. 245–258, 2024.
[4] Rao et al., "BLE-based smart seals with multi-environmental sensors for logistic tamper monitoring," Sensors and Actuators Journal, vol. 341, pp. 110–119, 2023.
[5] Hassan and Iqbal, "IoT applications in retail logistics: Sensor fusion for product integrity verification," Elsevier IoT Review, vol. 8, Art. 100591, 2022.
[6] Espressif Systems, ESP32 Technical Reference Manual, Version 4.5, pp. 112–135, 2023.
[7] Natarajan et al., "RFID-based product authentication in retail: Capabilities and limitations in post-purchase verification," IEEE Access, vol. 8, pp. 295–308, 2022.
[8] Singh and Thomas, "Multi-sensor IoT module for motion and light-based product integrity monitoring," Embedded Systems Letters, vol. 17, pp. 91–97, 2023.
[9] Das et al., "Sensor fusion of force and light sensors for improved package tamper detection," Journal of Embedded IoT, vol. 12, pp. 221–229, 2024.
[10] Verma et al., "Comparative evaluation of barcode, NFC, and IoT tags for secure product verification," IEEE Transactions on Retail Technology, vol. 15, pp. 301–310, 2021.
[11] Almeida et al., "Real-time clock integration for event logging in IoT monitoring systems," IEEE IoT Express, vol. 5, no. 3, pp. 190–198, 2022.
[12] Kaur and Menon, "BLE-based mobile application for product return verification in smart retail," IEEE Smart Retail Conference Proceedings, pp. 45–52, 2023.
[13] IEEE Access, "IoT adoption in smart retail: BLE and sensor-based product authentication," IEEE Access, vol. 11, pp. 781–790, 2023.
[14] Gupta et al., "AI-enhanced tamper detection on embedded devices using Edge Impulse," AI in Embedded Systems, vol. 18, pp. 112–120, 2024.
[15] Pillai et al., "IoT sensor-based detection of e-commerce return fraud using motion and pressure sensors," International Journal of Cyber Retail Technology, vol. 14, no. 2, pp. 223–330, 2022.