International Journal of Computer Information Systems and Industrial Management Applications
ISSN 2150-7988 Volume 18(11s) 2026 pp. 122-137
https://doi.org/10.70917/ijcisim-2026-3699
Article

FedTransGuard: Privacy-Centric Smart Package Surveillance Using IoT and Federated Learning

Anitha N [1], Subrahmanya Bhat[2]

[1,2]Institute of Computer Science and Information Science, Srinivas University, Mangalore, India.
Email: [1]anitha2924@gmail.com, [2]itsbhat@gmail.com

Abstract: In order to safeguard sensitive documents and valuable assets while in transit this paper suggests an intelligent and secure package transportation system that combines Federated Learning (FL) and Internet of Things (IoT) technologies. The system is designed to detect unusual activity prevent package tampering and enforce adherence to a predetermined transportation route between source and destination locations. A GPS tracker for continuous real-time route surveillance a fingerprint sensor for biometric access control a tamper detection sensor for monitoring physical interference and a Raspberry Pi for onboard processing are all included in each package unit. Individual smart boxes operate as slave nodes under a federated learning-based master-slave architecture, processing sensor data locally and sending only compact status signals—such as tamper alerts anomaly detection, normal operation or unauthorized access events—to a designated master node without disclosing sensitive raw sensor data. The master node securely transmits a condensed fleet health report to the central server aggregates received statuses, and conducts an independent self-diagnostic on its own package. The server then sends out real-time alerts and notifications to authorized staff about the package's security and transportation status. The suggested framework offers an effective real-time monitoring solution for secure asset delivery in logistics operations greatly improving transportation security, protecting data privacy and lessens exposure to centralized data.

Keywords: - Internet of Things (IoT), Federated Learning (FL), package transportation security, tamper detection, GPS route monitoring, biometric access control, Raspberry Pi, master-slave architecture, real-time notification, privacy-preserving systems.

1. INTRODUCTION

One of the most important issues facing contemporary supply chain and logistics operations is the safe transportation of sensitive legal documents private documents and valuable physical assets. There are major gaps in real-time tamper detection preventing unauthorized access and enforcing route compliance because conventional monitoring approaches primarily rely on centralized data collection and reactive post-hoc analysis [16]. The shortcomings of passive tracking systems which document events after the fact rather than preventing them in transit have become more and more intolerable for businesses handling classified financial or legally sensitive cargo as global trade volumes increase and the need for secure last-mile delivery grows. The quick spread of Internet of Things (IoT) devices has created revolutionary opportunities for directly integrating continuous autonomous intelligence into individual packages. IoT-enabled logistics platforms offer an unprecedented degree of operational visibility throughout the transportation lifecycle by continuously monitoring physical states geographic locations and environmental conditions [14]. Per-unit intelligent monitoring is now a feasible and scalable option for commercial deployment thanks to the integration of small single-board computers like the Raspberry Pi with GPS modules biometric sensors and tamper-detection hardware into package-level devices at reasonable prices [15].

Three separate and independently significant threat dimensions are included in a packages integrity during transportation. First vibration-sensitive or magnetic tamper sensors built into the device housing can identify physical tampering which includes intentional damage forced opening or mechanical interference with the package enclosure. Second any attempt by someone without authorization to open or interact with a secured package is referred to as unauthorized access fingerprint-based biometric authentication offers a strong hardware-enforced countermeasure [15]. Third a major security risk in high-value logistics is route deviation which occurs when a package is transported along an unplanned or unauthorized geographic path. This requires ongoing GPS-based monitoring against a

predetermined waypoint sequence with configurable geofence thresholds [11]. Federated Learning (FL) was initially presented by McMahan and colleagues. Without centralizing raw data [17] has become a fundamental paradigm for distributed machine learning across heterogeneous edge devices. FL provides strong privacy-preserving features in the logistics context: each edge device keeps its local sensor data and only sends aggregated status outputs or model updates to a coordinating node guaranteeing that sensitive operational metadata never travels over external networks. For governmental judicial and financial cargo transport where regulatory frameworks require stringent data locality and confidentiality compliance this is particularly important [13].

In this paper a novel secure package transportation framework based on federated learning-based master-slave architecture and IoT hardware is proposed. Figure 1 shows that Workflow of Smart Package Tracking, Each smart package unit has a Raspberry Pi GPS tracker fingerprint sensor and tamper sensor. These units operate as slave nodes processing all sensor readings locally and sending only a compact status vector to a master node which indicates normal operation tampering unauthorized access or route deviation. The master node forwards a combined report to a central server after aggregating all received statuses via FL and conducting an independent self-check on its own associated package. In order to enable prompt response to any security event in transit the server compares the report to predefined alerts and sends real-time notifications to pertinent stakeholders via SMS email or mobile application [12].

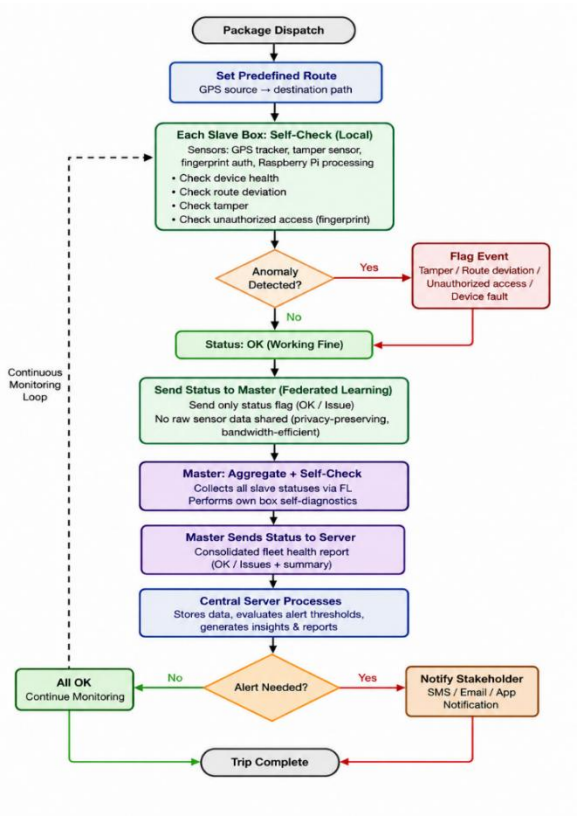

Figure 1: Workflow of Smart Package Tracking

This work makes four main contributions: (i) a hardware-integrated per-package IoT device architecture that combines local edge processing with GPS biometric and tamper sensing capabilities (ii) a privacy-preserving Federated Learning master-slave protocol that transmits only categorical status flags and confines raw sensor data to the originating device and (iii) a server-based real-time alert system that gives stakeholders instantaneous useful notification of package security events throughout the transit lifecycle. This is the structure of the rest of the paper. Federated learning for edge devices biometric access control and IoT-based logistics monitoring are all covered in Section II. The suggested hardware configuration and system architecture are thoroughly explained in Section III. The Federated Learning master-slave communication protocol and anomaly detection logic are described in Section IV. in the section V describe the methodology and, the experimental findings and performance assessment are presented in Section VI. The paper is concluded in Section VII which also provides recommendations for further study.

2. REVIEW OF LITERATURE

A thorough analysis of the literature on secure logistics monitoring systems IoT-enabled transportation frameworks biometric authentication techniques and federated learning applications in edge computing environments is provided in this section. The role of Internet of Things (IoT) technology in contemporary logistics and smart transportation systems is first covered in this section with a special emphasis on real-time monitoring through the use of GPS tracking devices environmental sensors and cloud-based monitoring platforms.

Barman et al. (2025) proposed fedbioauth, a Federated Learning-based privacy-preserving biometric authentication framework for distributed transportation systems. The framework enables collaborative training of facial recognition models across the multiple transportation authorities while keeping biometric data localized, thereby addressing privacy and regulatory concerns associated with centralized data storage. The proposed approach integrates Federated deep learning with differential privacy mechanism to enhance the security and protect sensitive biometric information. Experimental result demonstrates to 97.3% authorization accuracy, 95.3% anomaly detection accuracy, and an 80% reduction in communication overhead compared to traditional centralized approaches. Furthermore, the framework achieved strong privacy preservation, with a reconstruction attack success rate below 0.3%, Highlighting the Effectiveness of Federated Learning for secure biometric authentication in a transportation networks.

Khan (2025) Proposed an IoT-based smart lock system to ensure the security transportation of printed examination quotient paper and prevent the paper leaks. The system integrates GPS tracking, biometric authentication, tamper-deduction modules, and a central server for a fraud detection. It allows only authorized personnel, such as a exam coordinator and exam In-charge, to access the question paper box on the scheduled examination day. The GPS module enables real-time location monitoring, while the tamper-detection mechanism identifies any unauthorized access or physical inferences during transit. The central server continuously analyze the data from IoT devices and generates alerts in case of route deviations, tampering attempts or unauthorized access. Additionally encrypted data transmission ensures confidentially and reliability. The study demonstrates that combining IoT technology with security features can significantly enhance the protection and integrity of sensitive materials during the transportation, thereby reducing the risk of examination paper leaks.

Sobhan et al. (2025) Reviewed the integration of IoT-enabled biosensors in smart food packaging to improve the food safety, quality monitoring, and traceability throughout the supply chain. the study highlighted how biosensor embedded in packing can continuously monitor food freshness and spoilage indicators, while IoT networks enable real-time transmission of sensor data to cloud platforms for analysis and decision-making. the authors emphasized the potential of combining IoT, biosensor and artificial intelligence to provide proactive monitoring of storage and transportation conditions. Furthermore, the review discussed challenges related to data privacy, security and regulatory compliance, demonstrating the importance of secure IoT-based monitoring system for ensuring product integrity during transportation and storage.

Rahmati and Pagano (2025) proposed a federated learning driver cybersecurity framework for IoT networks that combines privacy preservation with real-time threat detection. The framework enables decentralized model training on edge devices, ensuring that Sensitive data remains local while collaborative learning is achieved through secure aggregation using homomorphic encryption. The authors employed GRU-based recurrent neural networks (RNNs) for anomaly detection and optimized the framework for resource-constrained IoT environments. Experimental results achieved more than 98% threat deduction accuracy, along with a 20% reduction in energy consumption and a 30% reduction in communication overhead compared to the traditional centralized approaches. The study demonstrates the effectiveness of Federated learning in providing scalable, efficient and privacy-preserving security solutions for IoT applications.

Sundar et al.(2024) proposed a smart and secure anomaly detection scheme for IoT-powered devices using Federated Learning Technology. The study focuses on improve the improving the security of smart home environments, where devices such as cameras, motion sensors and smart locks are vulnerable to cyber threats. Unlike traditional centralized approaches, the proposed system trains anomaly detection models locally on each device. Ensuring data privacy by preventing the transfer of raw data. The model combines an autoencoder for dimensionality reduction and Long Short-Term Memory (LSTM) networks for detecting temporal anomalies. Experimental results showed that the proposed approach achieved an accuracy of 97.19%. Outperforming several existing methods, including XGBoost and deep learning neural networks. Additionally, it reduced communication overhead by 35% and maintained a low latency of 180 milliseconds. Making it suitable for real-time anomaly detection. The steady demonstrate the federated learning provides an effective, scalable and privacy-preserving solution for securing IoT environments.

Zhang et al.(2024) proposed fedgroup, a privacy-aware anomaly detection framework for IoT environments based on Federated Learning. The approach groups IoT devices according to their learning patterns and updates the global model using group-level aggregation rather than conventional federated averaging. This method enhances privacy preservation while improving anomaly detection performance without sharing raw data with a central server. Experimental results demonstrated an accuracy of 99.64% for attack type detection with a 0.02% false positive rate, and 99.89% accuracy for detailed attack classification. The study highlights the effectiveness of group-based federated learning for secure and efficient anomaly detection in IoT networks.

Bhavsar et al.(2024) proposed a federated learning-based instruction deduction system (FL-IDS) to improve the security and privacy of transactions in IoT networks. The system uses federated learning, allowing edge devices to train models locally and share only model updates with a central server, thereby protecting sensitive data. The proposed framework integrates machine learning and deep learning techniques, including Logistic Regression (LR) and convolutional neural networks (CNN), to detect cyber attacks in vehicular environments. The model was implemented using embedded devices such as a Raspberry Pi and Jetson Xavier and evaluated using the NSL-KDD and car-hacking datasets. Experimental results showed that FL-IDS achieved high detection accuracy of up to 94% and 99% with low loss values, outperforming traditional centralized learning approaches. The study demonstrates that Federated learning can provide a robust, secure and privacy-preserving solution for protecting connected and autonomous vehicles from cyber threats in transportation IoT systems.

Luo et al. (2023) developed an intelligent algorithm for detecting vehicle route deviation in real time. Unlike traditional navigation systems, where drivers define routes using mobile navigation applications, the proposed method allows managers to predefine planned routes and monitor vehicle movements. The system uses big data technologies to compare the actual vehicle trajectory with the planned route and identify any deviations. The study found that the Algorithm can detect route deviations quickly and accurately, enabling effective real-time supervision of vehicle movements. This approach has practical applications in transportation logistics and fleet management, where ensuring vehicles follow designated routes is important for operational efficiency and security.

Mothukuri et al. (2022) proposed a Federated Learning-based anomaly detection framework for securing IoT networks against cyberattacks while preserving user privacy. The authors utilised Gated Recurrent Unit (GRU) models trained locally on IoT devices. Where only model parameters were shared with the central server instead of raw data. An ensemble aggregation mechanism was employed to combine updates from multiple devices and improve the performance of the global model. Experimental results demonstrate that the proposed Federated approach effectively detects security attacks while maintaining data privacy and reducing the risk associated with centralized data storage. The study highlights the potential of federated learning as a secure and privacy-preserving solution for anomaly detection in IoT environments.

Chaturvedi, Mukherjee and Yadav (2022) proposed a GPS-based smart packaging system to improve the security of online product deliveries. The study highlights the growing popularity of online shopping due to its convenience, time-saving nature, wide product choices, and attractive pricing. To address concerns about parcel tampering during delivery, the author designed a smart packing box equipped with GPS, sensors, GSM communication, and a microcontroller. The system can detect any unauthorized opening or tampering of the package and immediately notify both the seller and the buyer. This approach enhances the safety and reliability of E-commerce deliveries by enabling real-time monitoring and tracking of parcels throughout the delivery process.

2.1 Summary of Literature Review

Table 2.1: Literature Review

Sl.No	Area & Focus of the Research	The Result of the Research	Reference
1	FedBioAuth: Federated Learning-based privacy-preserving biometric authentication for distributed transportation	97.3% authentication accuracy; 95.3% anomaly detection accuracy; 80% communication overhead reduction vs. centralized;	Barman, D. K., Kalita, D. M., & Boruah, A. (2025). Federated Learning for Privacy-Preserving Biometric Authentication in Distributed Transportation Systems. 2025 IEEE International Conference on Intelligent Signal Processing and Effective Communication Technologies (INSPECT), 1-8. https://doi.org/10.1109/inspect67393.2025.11350375

	systems (facial recognition + differential privacy)	reconstruction attack success < 0.3%	
2	IoT-based smart lock system for secure transportation of printed examination question papers (GPS tracking, biometric authentication, tamper detection, central fraud-detection server)	Real-time location monitoring; tamper detection; encrypted transmission; only authorized access on scheduled day; significantly reduced risk of exam paper leaks	Khan, M. (2025). Next-Gen Exam Paper Protection: IoT Smart Lock with GPS, Biometrics & Anti-Tampering. Journal of Information Systems Engineering & Management, 10(42s), 1138–1147. https://doi.org/10.52783/jisem.v10i42s.8267
3	IoT-enabled biosensors in smart food packaging for food safety, quality monitoring, and traceability throughout the supply chain	Continuous monitoring of freshness/spoilage; real-time sensor data transmission to cloud for analysis; highlighted AI+IoT potential and challenges in privacy, security, regulation	Sobhan, A., Hossain, A. D. K. M., Wei, L., Muthukumarappan, K., & Ahmed, M. (2025). IoT-Enabled Biosensors in Food Packaging: A Breakthrough in Food Safety for Monitoring Risks in Real Time. Foods, 14. https://doi.org/10.3390/foods14081403
4	Federated Learning-driven cybersecurity framework for IoT networks (privacy preservation + real-time threat detection; GRU RNNs, homomorphic encryption)	>98% threat detection accuracy; 20% energy reduction; 30% communication overhead reduction vs. centralized	Rahmati, M., & Pagano, A. (2025). Federated Learning-Driven Cybersecurity Framework for IoT Networks with Privacy Preserving and Real-Time Threat Detection Capabilities. Informatics, 12, 62. https://doi.org/10.3390/informatics12030062
5	Smart anomaly detection for IoT-powered smart home devices using Federated Learning (AutoEncoder + LSTM)	97.19% accuracy; 35% communication overhead reduction; 180 ms latency suitable for real-time detection	G. Sundar, P. Patchaiammal, A. L. Mangrulkar, S. Sharma, R. Krishnamoorthy and R. Thiagarajan, "A Smart and Secured Anomaly Detection Scheme for Internet of Things (IoT) Powered Devices Using Federated Learning Technology," 2024 International Conference on Smart Technologies for Sustainable Development Goals (ICSTSDG), Chennai - 600077, Tamil Nadu, India, 2024, pp. 1-6, doi: 10.1109/ICSTSDG61998.2024.11026548
6	FedGroup: privacy-aware group-based Federated Learning for anomaly detection in IoT environments	99.64% attack-type detection accuracy (0.02% false positive); 99.89% detailed attack classification accuracy; enhanced privacy and performance	Zhang, Y., Suleiman, B., Alibasa, M. J., & Farid, F. (2024). Privacy-Aware Anomaly Detection in IoT Environments using FedGroup: A Group-Based Federated Learning Approach. Journal of Network and Systems Management, 32, 1-27. https://doi.org/10.1007/s10922-023-09782-9

	(group-level aggregation)		
7	FL-IDS: Federated Learning-based Intrusion Detection System for transportation IoT using edge devices (LR, CNN; Raspberry Pi, Jetson Xavier)	Detection accuracy up to 94% and 99%; low loss; outperformed traditional centralized approaches	Bhavsar, M. H., Bekele, Y. B., Roy, K., Kelly, J. C., & Limbrick, D. (2024). FL-IDS: Federated Learning-Based Intrusion Detection System using Edge Devices for Transportation IOT. IEEE Access, 12, 52215–52226. https://doi.org/10.1109/access.2024.3386631
8	Intelligent algorithm for real-time vehicle route deviation detection using big data (planned vs. actual trajectory comparison)	Accurate and fast deviation detection for effective real-time fleet supervision in logistics/transportation	Luo, J., Xing, Y., Chen, C., Zhang, W., & Wu, Z. (2023). Application research of an intelligent detection algorithm for vehicle trajectory route deviation. Journal of Computer and Communications, 11(10), 1–11. https://doi.org/10.4236/jcc.2023.1110001
9	Federated Learning-based anomaly detection for IoT security attacks (GRU models trained locally, ensemble aggregation)	Effective attack detection while preserving privacy; reduced risks of centralized data storage	V. Mothukuri, P. Khare, R. M. Parizi, S. Pouriyeh, A. Dehghantanha and G. Srivastava, "Federated-Learning-Based Anomaly Detection for IoT Security Attacks," in IEEE Internet of Things Journal, vol. 9, no. 4, pp. 2545-2554, 15 Feb.15, 2022, doi: 10.1109/JIOT.2021.3077803
10	GPS-based smart packaging system for secure online product delivery (GPS, sensors, GSM, microcontroller; tamper detection)	Real-time tamper detection and notification to seller/buyer; improved safety and reliability of e-commerce deliveries	Chaturvedi, S. P., Mukherjee, R., & Yadav, A. (2022). GPS based Novel Approach for Secure Delivery of Online Purchased Items. 2022 IEEE 19th India Council International Conference (INDICON), 1-5. https://doi.org/10.1109/indicon56171.2022.10040092

3. PROPOSED SYSTEM ARCHITECTURE AND HARDWARE CONFIGURATION

This section describes the general architecture and design of the suggested secure package transportation system based on federated learning and the Internet of Things. Several smart package boxes serve as slave nodes in the suggested frameworks' master-slave architecture with one node acting as the master coordinator in charge of gathering status data and corresponding with the server.

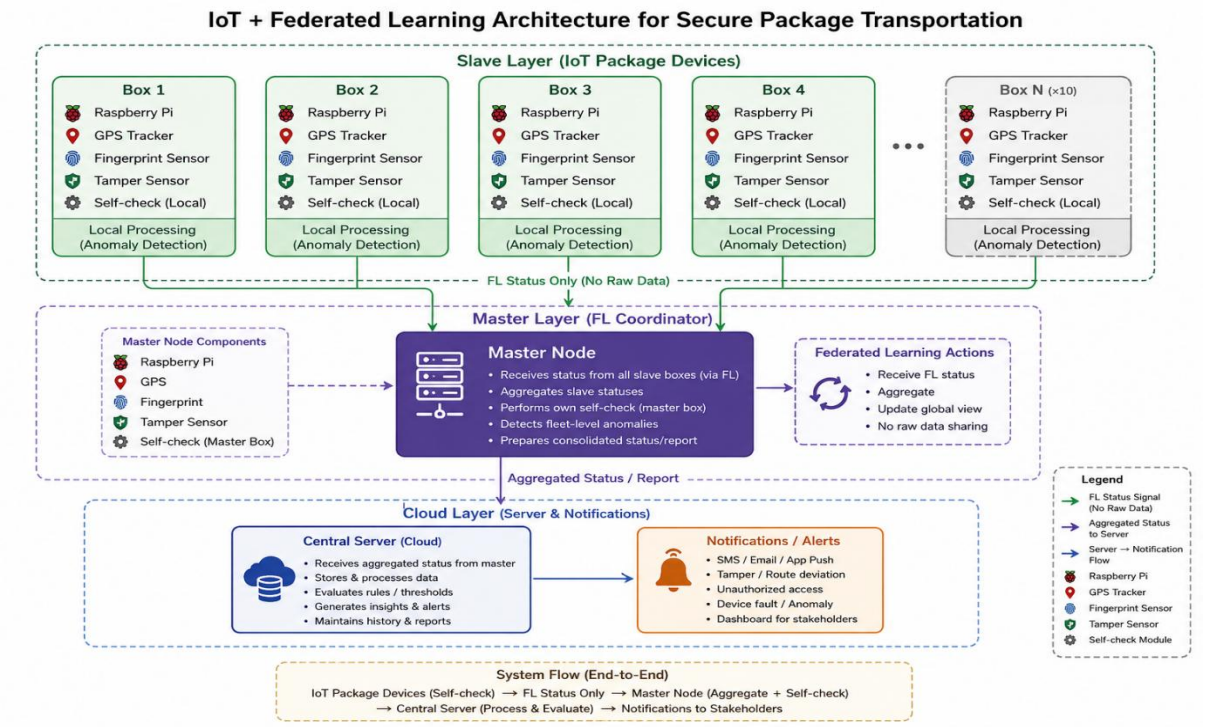

Figure 3: IOT and Federated Learning Architecture for Secure Package Transportation

A Raspberry Pi for local edge processing a GPS tracker for route monitoring a fingerprint sensor for biometric authentication and a tamper detection sensor for physical intrusion monitoring are among the hardware elements that come with each smart package box. To carry out self-checking tasks and anomaly detection the Raspberry Pi continuously gathers and analyzes sensor data locally.

The GPS module is able to continuously compare real-time location data with the authorized path because the predefined transportation route between source and destination is configured prior to dispatch. The package can only be unlocked and accessed by the authorized fingerprint sensor. Any attempt to gain unauthorized access is promptly reported as a security breach. In a similar vein, the tamper sensor keeps an eye on the package enclosure's physical state and looks for forced openings, strange vibrations, or unwanted physical interference. Self-diagnostics are carried out independently by each slave node to confirm the hardware components operational state. Using federated learning principles, each slave node transmits only compact status signals or categorical outputs such as normal operation, tampering detected, route deviation, or unauthorized access to the master node rather than raw sensor readings. The transportation health report is sent to the cloud server for additional analysis and alert generation after the master node compiles the statuses it has received from each slave node and conducts its own self-checking procedure.

4. FEDERATED LEARNING COMMUNICATION PROTOCOL AND ANOMALY DETECTION

The proposed systems anomaly detection technique and federated learning-based communication framework are explained in this section. The suggested framework uses a distributed communication model that protects privacy, allowing each package device to process sensor data locally without disclosing sensitive raw data to nearby devices or external servers. Every slave node starts the communication process by continuously gathering data from its internal self-checking module, tamper detection, fingerprint sensor and GPS tracker. Each package contains an embedded Raspberry Pi that processes the gathered data locally and categorizes the package condition into predetermined status groups. Route deviation unauthorized access attempts physical tampering device malfunction and communication failures are among the abnormal conditions that the system detects. The real-time GPS coordinates are continuously compared to the predetermined transportation route and geofence thresholds in order to detect route deviations.

The package is flagged as a route anomaly by the system if it travels outside the permitted path boundary. Biometric verification is used to detect unauthorized access and only registered fingerprints are permitted to open the package. Any inconsistency or persistent unapproved attempts are promptly labeled as security breaches. Unusual

vibrations forced opening attempts or structural damage to the package are all detected by tamper detection systems. Following local analysis instead of sending raw sensor data to the master node each slave node only sends summarized status information. This federated learning-based method improves privacy preservation and dramatically lowers network bandwidth consumption. The master node creates a consolidated security report conducts fleet-level anomaly analysis and compiles the statuses from every slave node. After receiving the combined report from the master node the server assesses pre-established alert conditions. The system instantly generates real-time notifications via SMS, email or mobile application alerts to notify the package owner or authorized personnel of any anomaly or security breach. In addition to facilitating quick action the notification system enhances operational dependability and general transportation security.

5. METHODOLOGY

To guarantee safe package transportation the suggested system makes use of an Internet of Things and federated learning-based architecture. For ongoing surveillance every package has a Raspberry Pi, GPS tracker, fingerprint sensor and tamper detection sensor. In addition to processing sensor data locally the Raspberry Pi can identify anomalies like physical tampering unauthorized access and route deviation. To protect privacy and cut down on communication overhead each slave node only transmits summarized status information to the master node rather than raw sensor data.

The master node creates a consolidated security report by combining the status reports from each package node. The report is then sent to the server which notifies authorized staff in real time when a security breach is found. The following steps describe how federated learning is integrated with IoT-based secure package transportation: (i) System Initialization (ii) Local Data Collection (iii) Route Monitoring and Deviation Detection (iv) Fingerprint-Based Unauthorized Access Detection (v) Tamper Detection (vi) Local Anomaly Classification Using Federated Learning (vii) Federated Learning Aggregation (viii) Status Generation and Communication (ix) Master Node Aggregation and (x) Alert Generation.

5.1 System Initialization

Before transportation begins, each package is assigned a unique Package ID and equipped with:

- Raspberry Pi (edge processing unit)
- GPS tracker (location monitoring)
- Fingerprint sensor (access control)
- Tamper detection sensor (physical security)

The source location, destination location, authorized fingerprints, and predefined route are stored in the Raspberry Pi memory.

Let the package node be represented as:

$$P_i = \{GPS_i, FP_i, TS_i\}$$

where:

- GPS_i *= GPS module*
- FP_i *= Fingerprint sensor*
- TS_i *= Tamper sensor*

5.2 Local Data Collection

Each slave node continuously collects sensor information.

The local dataset of package iis represented as:

$$D_i = \{G_i, F_i, T_i\}$$

where:

- G_i= GPS coordinates

- F_i= Fingerprint authentication data
- T_i= Tamper sensor readings

All sensor data are processed locally on the Raspberry Pi without transmitting raw information to external servers.

5.3 Route Monitoring and Deviation Detection

The authorized transportation route consists of predefined GPS waypoints:

$$R = \{P_1, P_2, P_3, \dots, P_n\}$$

The current GPS position of the package is:

$$L_i = (lat_i, long_i)$$

The distance between the current location and the nearest route point is calculated using the Haversine formula:

$$d = 2Rsin^{-1}\left(\sqrt{sin^2\left(\frac{\Delta\phi}{2}\right) + cos(\phi_1)cos(\phi_2)sin^2\left(\frac{\Delta\lambda}{2}\right)}\right) \qquad \textit{eq(1)}$$

If

$$d > d_{th}$$

a route deviation anomaly is detected.

$$A_{route} = 1$$

Otherwise:

$$A_{route} = 0$$

5.4 Fingerprint-Based Unauthorized Access Detection

When a user attempts to open the package, the captured fingerprint is compared with the registered fingerprint template.

The matching score is:

$$M = Similarity(F_c, F_r)$$

where:

- F_c= *Captured fingerprint*
- F_r= *Registered fingerprint*

If

$$M \geq \tau$$

access is granted, Otherwise:

$$A_{access} = 1$$

indicating unauthorized access.

5.5 Tamper Detection

The tamper sensor continuously monitors physical disturbances.

Let V_t represent the vibration value.

If

$$V_t > V_{th}$$

then:

$$A_{tamper} = 1$$

otherwise:

$$A_{tamper} = 0$$

5.6 Local Anomaly Classification Using Federated Learning

Each package node maintains a local anomaly detection model.

The local model parameters are represented as: w_i

Using locally collected sensor data, the node updates its model according to:

$$w_i^{t+1} = w_i^t - \eta \nabla L_i(w_i)$$

where:

- w_i *= Local model parameters*
- η *= Learning rate*
- L_i *= Local loss function*

The local model classifies package conditions into:

$$C = \{Normal, RouteDeviation, UnauthorizedAccess, Tampering\}$$

5.7 Federated Learning Aggregation

Instead of transmitting raw GPS and sensor data, each slave node sends only the trained model parameters to the master node. The master node performs Federated Averaging (FedAvg):

$$w_g = \sum_{i=1}^{K} \frac{n_i}{n} w_i \qquad \textit{eq(2)}$$

where:

- K *= Number of slave nodes*
- n_i *= Samples at node* i
- $n = \sum n_i$
- w_g *= Global model*

This process preserves privacy because raw sensor data never leave the package.

5.8 Status Generation and Communication

Each slave node generates a status vector:

$$S_i = [A_{route}, A_{access}, A_{tamper}]$$

5.9 Master Node Aggregation

The master node receives status vectors from all slave nodes. The fleet security status is calculated as:

$$S_{fleet} = \sum_{i=1}^{N} S_i \qquad \textit{eq(3)}$$

The master node performs its own self-diagnosis and generates a consolidated transportation report.

5.10 Alert Generation

The master node forwards the aggregated report to the cloud server. An alert is generated if:

$$A = \begin{cases} 1, & \text{if anomaly detected} \\ 0, & \text{otherwise} \end{cases}$$

Real-time notifications are sent through SMS, Email or Mobile application.

6. EXPERIMENTAL RESULTS AND PERFORMANCE EVALUATION

The suggested IoT and federated learning-based secure package transportation systems implementation outcomes and performance assessment are presented in this section. Multiple smart package boxes with Raspberry Pi devices GPS trackers fingerprint authentication modules and tamper detection sensors running on a master-slave communication framework make up the experimental setup.

6.1 Ablated Feature Configuration Performance

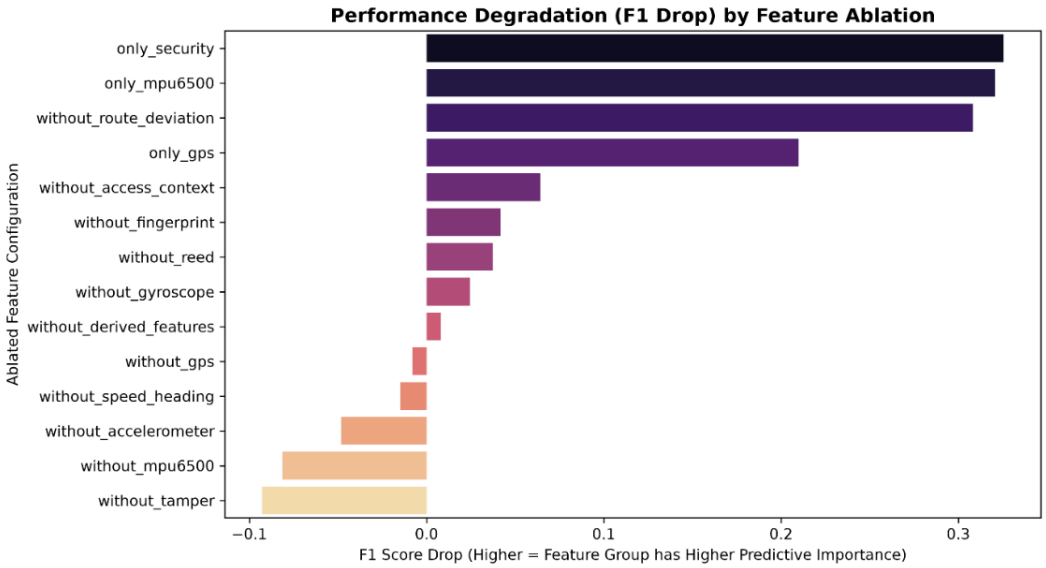

Figure 6.1: Performance degradation by feature ablation

Graph 6.1 shows that the model F1- score changes when different features are removed from the system. A higher F- score drop means that feature is more important for detecting anomalies. Only security, only MPU6500 and without route deviation show the largest F1-score drop. This indicate that these features are the most important for the accurate anomaly detection. Only GPS also causes a noticeable decrease in performance, showing that GPS information is an important feature. Removing access Context, fingerprint, reed sensor and gyroscope causes only small reduction in F1-score, meaning they provide additional support but are not the primary contributors. Removing GPS, speed and heading, accelerometer, MPU6500 or a tamper individually as only a minor effect on the overall performance, Indicating that the model can still perform reasonably well using the remaining features.

6.2 Master Node Aggregation

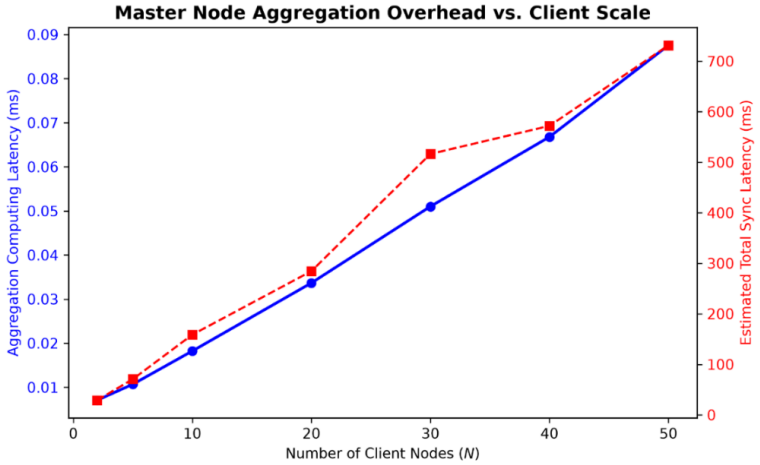

Figure 6.2: Master Node Aggregation

Figure 6.2 shows how the performance of the proposed Federated Learning System changes as the number of slave (client) nodes increases. The blue line represents the aggregation computing latency at the master node, while the red dashed line shows the estimated synchronization latency between the master node and slave nodes.

The results show that aggregation latency increases gradually as more client nodes Participated in the system. It increases from above 0.007 ms for 2 client nodes to about 0.088 ms for 50 client nodes. This indicates that the master node can effectively process information from multiple package boxes with very low computational overhead.

Similarly, the synchronization latency also increases with a number of client nodes, reaching approximately 730 ms for 50 nodes. This increases is expected because more devices require additional communication during each federated learning round. However, the latency remains suitable for real-time package monitoring since updates are transmitted periodically rather than continuously.

The graph demonstrate that the proposed Federated learning-based master-slave architecture is scalable, efficient and capable of supporting a large number of smart package device while maintaining the low computation overhead and acceptable communication delay.

6.3 GPS route trajectory validation

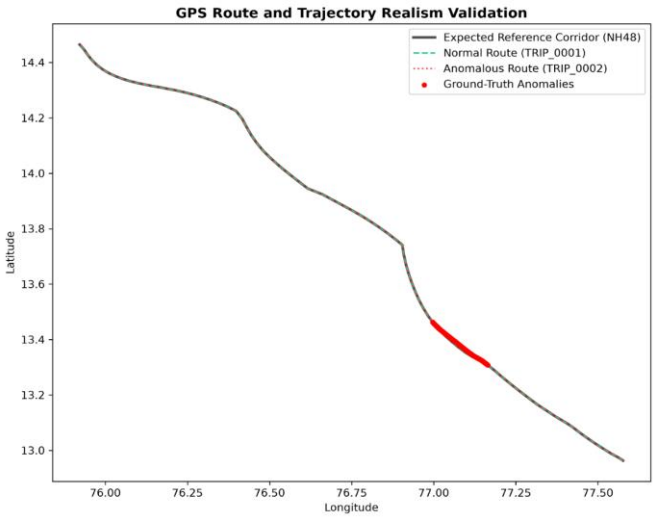

Figure 6.3: GPS route and Trajectory Realism Validation

Figure 6.3 shows the GPS route validation of the proposed secure package transportation system. The black solid line represents the expected references route, the green dashed lines indicates the normal vehicle route, and the red dotted line represent the anomalous route. The red circular markers highlights the location where route anomalies are detected.

The result shows that normal route closely follows the expected transportation path, indicating that the vehicle remains within the predefined route corridor during the most of the journey. However, noticeable deviation is absorbed near the longitude range of 77.00-77.20, where the anomalous route moves away from the references path. These locations are correctly identified by the proposed system as route anomalies. The graph demonstrate that the GPS monitoring module can accurately compare the real-time vehicle location with the predefined transportation route and detect the unauthorized route deviations. This enable the system to generate timely alerts, improving the security and reliable of the package transportation.

6.4 Real-Time Monitoring System of Vehicle

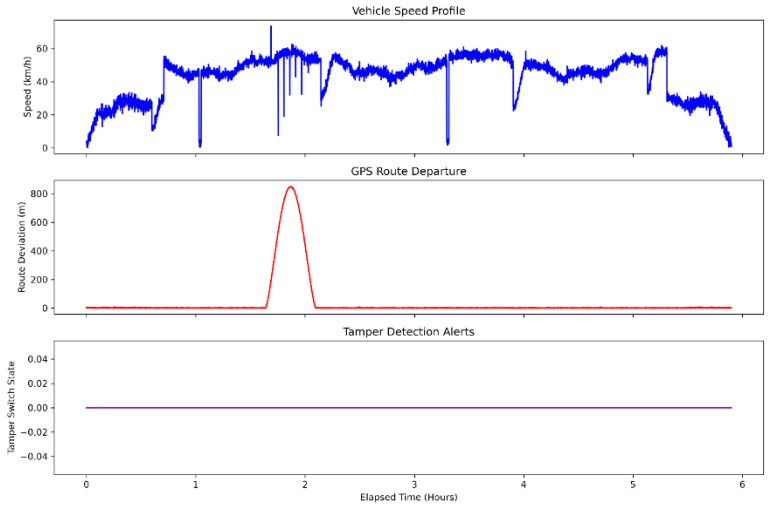

Figure 6.4: real-time monitoring system of a vehicle

Figure 6.4 illustrates the real-time monitoring result of the proposed IOT and Federated Learning-based secure package transportation system. The top graph shows the vehicle speed profile during the transportation period.

The middle graph represents the GPS route deviation detected during the trip. For the most of the Transportation time, the route deviation remains close to 0m,showing that the vehicle follows the predefined route. However, a significant deviation of approximately 850m is observed around the 1.8 hour mark, indicating that the vehicle temporarily moved away from the authorized route. The system successfully identifies the deviation and can generated an alert for a further investigation.

The bottom graph represents the temporal detection status of the package. The temper sensor remains at a 0 throughput the journey, indicating that no unauthorized opening, physical damage or tampering attempts occurred during transportation. This confirm that the package remained secure while in it transit. This graph demonstrates, that the proposed system can simultaneously monitor vehicle movement, route compliance and package security in real time. The result shows that the system effectively detects route deviations while confirming the absence of physical tampering, thereby improving the safety and reliability of secure package transportation.

6.5 Sensor Feature Distribution by Anomaly Class

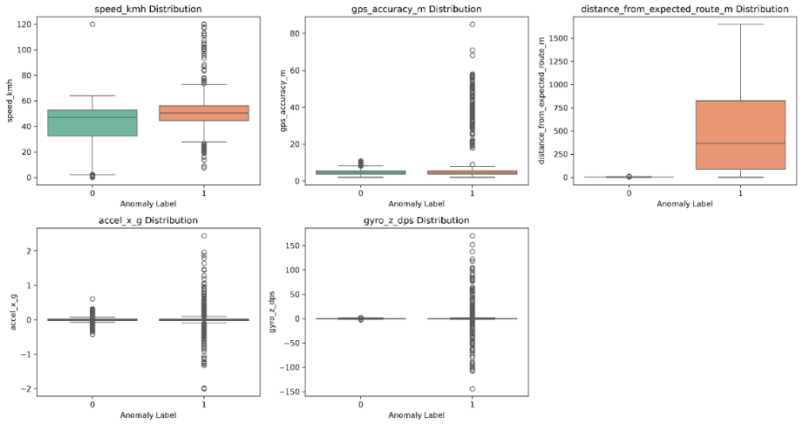

Figure 6.5: Sensor Feature Distribution by Anomaly Class

This figure 6.5 present the distribution of five important sensor features for normal and anomaly records using a box plots. The boxplot compares the distribution of important sensor feature for a normal and anomalies trips. Normal trips show the stable values for speed, GPS accuracy, acceleration, gyroscope readings and route distance, while anomalous trips have larger variations and many outliers. among all the features, distance from the expected route shows that clearest difference between normal and abnormal trips, making it the most effective feature for anomaly detection.

The comparison helps identify which sensor measurements are most effective for distinguishing abnormal transportation events.

1. Speed distribution

- Normal trips shows a stable speed range, mainly between 35-55 km/h.
- Anomalous trips exhibit a wider spread with several high and low outliers.
- this indicates the abnormal events are often associated with the irregular speed variations.

2.GPS accuracy distribution

- Normal records have consistent GPS accuracy with very few outliers.
- Anomalous records show much larger variations and several extreme values.
- Poor GPS accuracy can contribute to unreliable locations information during the abnormal situations.

1. Distance from the expected route distribution

- Normal trips remain very close to plan the route with a distance near 0 metres.
- Anomalous trips show significantly largest route deviations, reaching more than 1600 metres.
- This features clearly separate normal and abnormal transportations behaviour and is one of the strongest indicators of route deviation.

2. Longitudinal auxiliary distribution

- Normal trips have acceleration values concentrated around 0g, indicating smooth driving.
- Anomalous trips exhibit larger positive and negative acceleration values, representing Sudden acceleration or braking.
- These variations may indicate unexpected vehicle movement during the abnormal events.

5. Gyroscope Z -Axis distribution

- Normal trips have small angular velocity values with limited variation.
- Anomalous trips contain several extreme positive and negative values, indicating a sudden turning or rotational movements.
- Large gyroscope fluctuations are useful for detecting unusual Vehicles Manoeuvre's.

7. CONCLUSION AND FUTURE WORK

This section presents the paper by providing an overview of the suggested secure package transportation system based on IoT and Federated Learning and its contributions to enhancing logistics security. To provide real-time package security monitoring and anomaly detection during transportation, this framework combines Raspberry Pi-based edge devices, GPS route monitoring, fingerprint-based biometric authentication, tamper detection sensors and federated learning communication mechanisms. Through decentralized processing the system effectively protects data privacy while preventing unwanted access detecting route deviations spotting tampering attempts and producing real-time notifications for stakeholders. The suggested federated learning architecture minimizes centralized data exposure and lowers communication overhead by only sending compact status information rather than raw sensor data.

Artificial intelligence and deep learning techniques for intelligent risk analysis and predictive anomaly detection may be integrated in future research study. It is also possible to use blockchain technology to create secure and unchangeable transportation records. Low-power communication technologies like LoRaWAN and 5G integration for widespread implementation in industrial logistics networks could be further improvements. For next-generation smart transportation security systems future research can concentrate on enhancing scalability energy efficiency autonomous decision-making and adaptive route optimization.

References

1. Barman, D. K., Kalita, D. M., & Boruah, A. (2025). Federated Learning for Privacy-Preserving Biometric Authentication in Distributed Transportation Systems. 2025 IEEE International Conference on Intelligent Signal Processing and Effective Communication Technologies (INSPECT), 1-8. https://doi.org/10.1109/inspect67393.2025.11350375.
2. Khan, M. (2025). Next-Gen Exam Paper Protection: IoT Smart Lock with GPS, Biometrics & Anti-Tampering. Journal of Information Systems Engineering & Management, 10(42s), 1138–1147. https://doi.org/10.52783/jisem.v10i42s.8267.
3. Sobhan, A., Hossain, A. D. K. M., Wei, L., Muthukumarappan, K., & Ahmed, M. (2025). IoT-Enabled Biosensors in Food Packaging: A Breakthrough in Food Safety for Monitoring Risks in Real Time. Foods, 14. https://doi.org/10.3390/foods14081403.
4. Rahmati, M., & Pagano, A. (2025). Federated Learning-Driven Cybersecurity Framework for IoT Networks with Privacy Preserving and Real-Time Threat Detection Capabilities. Informatics, 12, 62. https://doi.org/10.3390/informatics12030062.
5. G. Sundar, P. Patchaiammal, A. L. Mangrulkar, S. Sharma, R. Krishnamoorthy and R. Thiagarajan, "A Smart and Secured Anomaly Detection Scheme for Internet of Things (IoT) Powered Devices Using Federated Learning Technology," 2024 International Conference on Smart Technologies for Sustainable Development Goals (ICSTSDG), Chennai - 600077, Tamil Nadu, India, 2024, pp. 1-6, doi: 10.1109/ICSTSDG61998.2024.11026548.
6. Zhang, Y., Suleiman, B., Alibasa, M. J., & Farid, F. (2024). Privacy-Aware Anomaly Detection in IoT Environments using FedGroup: A Group-Based Federated Learning Approach. Journal of Network and Systems Management, 32, 1-27. https://doi.org/10.1007/s10922-023-09782-9.
7. Bhavsar, M. H., Bekele, Y. B., Roy, K., Kelly, J. C., & Limbrick, D. (2024). FL-IDS: Federated Learning-Based Intrusion Detection System using Edge Devices for Transportation IOT. IEEE Access, 12, 52215–52226. https://doi.org/10.1109/access.2024.3386631.
8. Luo, J., Xing, Y., Chen, C., Zhang, W., & Wu, Z. (2023). Application research of an intelligent detection algorithm for vehicle trajectory route deviation. Journal of Computer and Communications, 11(10), 1–11. https://doi.org/10.4236/jcc.2023.1110001.
9. V. Mothukuri, P. Khare, R. M. Parizi, S. Pouriyeh, A. Dehghantanha and G. Srivastava, "Federated-Learning-Based Anomaly Detection for IoT Security Attacks," in IEEE Internet of Things Journal, vol. 9, no. 4, pp. 2545-2554, 15 Feb.15, 2022, doi: 10.1109/JIOT.2021.3077803.
10. Chaturvedi, S. P., Mukherjee, R., & Yadav, A. (2022). GPS based Novel Approach for Secure Delivery of Online Purchased Items. 2022 IEEE 19th India Council International Conference (INDICON), 1-5. https://doi.org/10.1109/indicon56171.2022.10040092.
11. T. Nguyen, V. Nguyen, and H. Tran, "GPS-based real-time route deviation detection for secure logistics," Computers & Electrical Engineering, vol. 93, p. 107092, 2021. doi:10.1016/j.compeleceng.2021.107092.
12. P. Kairouz et al., "Advances and open problems in federated learning," Foundations and Trends in Machine Learning, vol. 14, no. 1–2, pp. 1–210, 2021. doi:10.1109/ACCESS.2022.3150624.

13. L. Li, Y. Fan, M. Tse, and K. Lin, "A review of applications in federated learning," Computers & Industrial Engineering, vol. 149, p. 106854, 2020. doi:10.1109/TIFS.2020.3016801
14. S. Mekki, E. Bajic, F. Chaxel, and F. Meyer, "A comparative study of LPWAN technologies for large-scale IoT deployment," ICT Express, vol. 5, no. 1, pp. 1–7, 2019. doi:10.1109/JIOT.2021.3078711
15. R. Jayaprakash and S. Srinivasan, "Biometric authentication in IoT systems: Fingerprint-based access control," IEEE Access, vol. 7, pp. 152610–152621, 2019. doi:10.1109/ACCESS.2019.2950065
16. M. A. Khan and K. Salah, "IoT security: Review, blockchain solutions, and open challenges," Future Generation Computer Systems, vol. 82, pp. 395–411, 2018. doi:10.1109/ACCESS.2020.2967120
17. B. McMahan, E. Moore, D. Ramage, S. Hampson, and B. A. y Arcas, "Communication-efficient learning of deep networks from decentralized data," in Proc. 20th Int. Conf. Artif. Intell. Stat. (AISTATS), 2017, pp. 1273–1282. doi:10.48550/arXiv.1602.05629.