Discover Engineering
An International Journal

OPEN ACCESS

ISSN 3117-566X
Review Article

Check for updates

Federated Learning and IoT-Based Secure Package Transportation System Using TLS and AES Encryption

Anitha N., and **Subrahmanya Bhat***

Institute of Computer Science and Information Science, Srinivas University, Mangalore, India

Corresponding author: **Subrahmanya Bhat** | E-mail: **itsbhat@gmail.com**

Citation: Anitha N., and Subrahmanya Bhat (2026). Federated Learning and IoT-Based Secure Package Transportation System Using TLS and AES Encryption. *Discover Engineering: An International Journal.* **DOI: https://doi.org/10.51470/DE.2026.7.1.08**

Received 11 January 2026 | Revised 07 February 2026 | Accepted 13 March 2026 | Available Online 03 April 2026

Abstract

The private packages are protected from unauthorized access and data leaks during their transportation, and tamper detection is necessary with the use of continuous monitoring. In this paper, we propose an intelligent system for package transportation and ensures the packages can be delivered confidentially and securely with three individual elements: Federated Learning (FL), Internet of Things (IOT) and the Transport Layer Security (TLS) protocol. Each package contains a raspberry pi, GPS tracker, fingerprint sensor and tamper detection Sensor to track where it is located, identify whether an authorized user has signed for a delivery and detect any fast location compromise. In Smart package units are able to locally process sensor data and send only status updates to master such as at tamper alerts, anomaly detection outcomes, normal operations and unauthorized access events-optimised to never reveal raw sensor data. To protect the communication between central server and master node the TLC protocol uses symmetric encryption (AES). To maintain the privacy, enable safe data exchange and protection against the cyber-attacks, the master node encrypts the output of an aggregated report on fleet health (normal and critical state) before sending it out. The server decrypts the data after verifying its integrity and authenticity. Whenever there are any anomalies or signs of a security breach, the central server notifies designated staff with real time alerts while keeping a record about the live status of transport. This proposed system strengthens transportation security, maintenance data privacy, alertness the communication overhead involved in traditional system, and provides the physical access control mechanism when protecting sensitive packages during the transiting by integrating federated learning with TLS-enabled AES secured communication.

Keywords: *Federated Learning, Internet of Things, Transport Layer Security, AES, Package Tracking, Tamper Detection, Secure Communication, Edge Computing.*

1. INTRODUCTION

The secured transportation of private packages, including exam papers, legal documents, financial records, medical reports and other sensitive materials, has been become increasingly important in modern logistic and intelligence transportation systems.

While in transit, these packages are susceptible to numerous security threats, such as a theft, route deviation, physical manipulation, unauthorized access and cyberattacks. Traditional parcel transportation system rarely heavily on GPS tracking, centralized monitoring and manual supervision. Such technique is unable to monitor breaches in a real-time and offer a minimal protection against the types of trained threats. In addition, centralized system needs the continuous transfer of a raw sensor data which introduces not only a more communications overhead and network congestion but also a greater chance for sensitive information to be compromised or intercepted.

At this point, IoT has emerged out to be a dominant technology for real-time traffic monitoring because it provides a mechanism to collect data through communication and sensor device embedded in different constructs. In addition, an IoT-based package tracking system can also monitor environmental conditions during the transportation, track location in a continuous manner and determine physical tampering. These sensors provide helpful information about the movement and security conditions such as a GPS model, fingerprint authentication module and tamper detection sensors. There are also the real risks of privacy and bandwidth losses, not to mention security attacks from the direct porting or sensor data into a central server.

Federated Learning is a distributed machine learning framework with high privacy and intelligence decision-making capabilities without the need of providing raw data for training, which has recently received widespread attention.

The recent trend is to process a data locally on the devices own sensors measurements and so forth, with transmission of only summarized or compressed model updates, as opposed to raw data from the sensor back coordinating server. In this approach, you can communicate relatively very less while keeping the data private. Federated learning empowers smart package units with the ability to locally detect anomalies that could be something like route deviation or unauthorized access and tampering without outpacing sharing sensitive sensor data outside network.

The proposed system offers a novel and secure package delivery framework by combining IoT devices with Federated Learning, TLS and AES. Each package continues a Raspberry Pi, GPS tracker, fingerprint sensor and tamper detection sensor are to monitor the progress along the transit. Federated Learning based master slave architecture uses individual smart packages as a slave node in the sandbox. Each slave node has a status report of the compact that shows, a normal function, route deviation, unauthorized access or tampering, anomaly detection. To protect privacy and reduces cost of communication, only these condensed status message are what being sent to the master node instead of original sensor data. Beside self-monitoring, master-node creates fleet health report by aggregating the status data it received from each slave node. The aggregated data is encrypted with AES by the master node, which then establishes a secure TLS communication channel and send this report to the central server.

For real-time transport monitoring, the data is verified and decrypt in server and for a validation transferred, in a case of any suspicious activity or a delicate cross, unauthorized personal receives an immediate alert and notice to the intervene at the earliest thereby avoiding a potential security breaches. Unlike traditional support monitoring systems, the Federated learning integrated with TLC-security AES communication has some advantages. the proposed framework ensures secure communication in presence of cyberattacks, lowers the network bandwidth by performing a local processing, protects data privacy as there is no transmission of raw sensor data and allows efficient real time anomaly detection. in addition, since AES has a low computational demands, the system can run on embedded Internet of Things (IoT) platform which reasonable processing latency.

The proposed model integrate about technique and tools to provide solution for securing packages in transportation the framework offers a reliable way of ensuring that the sensitive package transported or well protected using current Smart Logistic system. In addition, this model enhanced the safety of the packages, minimizes the amount of communication required, and ensures data privacy integrity.

2. LITERATURE REVIEW

Federated learning SL as an alternative to traditional centralized anomaly detection and lightweight authentication as well as TLS based transport security for constrained devices have been widely explored as methods of securing IoT based monitoring systems while retaining privacy of information. In this section, some exemplary research in each direction is discussed and the proposed solution is compared to them

Several architectures involve Federated deep learning have been proposed in various studies in which IoT devices perform local training and exchange only model parameters with the center node. One of them uses Federated deep neural network, in which each IoT device performs local training on its data and sends the way upgrade to a central server performing global model aggregation using mini batch averaging.

Prior to local prediction, mutual-information techniques are used to select features [5]. In order to overcome the scalability and privacy constraints of conventional centralized intrusion detection systems, a related fog-federated design specifically addresses smart-home intrusion detection by using a decentralized architecture that allows devices to cooperatively train a detection model while maintaining the privacy of local data [1].

Group-aware aggregation has also been studied. Instead of treating every client equally, FedGroup modifies the standard FedAvg update rule by aggregating contributions according to IoT device categories. The authors show that this enhances anomaly detection across heterogeneous smart-home devices in terms of both accuracy and fairness [3]. The tamper-detection part of the suggested system is most similar to the study on privacy-preserving detection of tampered radio-frequency transmissions in LoRa-based IoT networks, which compared various FL-enabled one-class anomaly detectors (convolutional autoencoder, isolation forest, one-class SVM, local outlier factor, and k-means variants) trained without centralizing raw RF data [4]. With an accuracy of more than 97%, the convolutional-autoencoder variant beat centralized machine-learning baselines. This demonstrates that FL-based one-class detectors can reliably identify tampering-type events at the edge without revealing sensitive raw signal data, supporting the design choice of local anomaly scoring at each smart-package slave node.

Because embedded package units have limited compute and power budgets, several works have benchmarked lightweight authenticated-encryption (AE) schemes amenable to constrained hardware. In particular, one study implemented secure end-to-end encryption for MQTT using AES-128-GCM in conjunction with NIST lightweight-cryptography finalists (GIFT-COFB, Romulus-N, Tiny JAMBU) in ESP8266 and STM32L4 microcontrollers, measuring encryption/decryption latencies directly on the target hardware and concluding that these algorithms could provide confidentiality and authenticity of data with acceptable overheads for MQTT messaging on resource-constrained microcontrollers [7]. Meanwhile, a systematic review of 77 manuscripts on lightweight cryptography for IoT found several mentions of AE being central to the confidentiality/integrity-security goals for real-time IoT communication, with AES-GCM being frequently used in conjunction with lightweight message authentication codes (MACs) or digital signatures to

provide the necessary tamper-proofing of data [2].

A more in-depth analysis of the hardware costs of authenticated-encryption modes revealed Galois/Counter Mode to be particularly attractive, as it only requires a minor additional gate overhead (about 30K gates) compared to the AES in plain counter mode; thus, being among the most resource-light AE designs for constrained IoT platforms [6]. Therefore, AES was deemed a reasonable choice in terms of balancing cryptographic security and computational overhead for the sporadic small-size transmissions of the proposed system's fleet status messages.

Meanwhile, a design closely following the use case of the transport monitoring scenario was described, where a fleet monitoring system was constructed, securing MQTT traffic over Transport Layer Security (TLS). In this design, the choice between different GPS modules (SIM800, ESP32, and SIM7000G) was made based on the precision of coordinate extraction during TLS encryption overhead. Ultimately, the SIM7000G module was selected for its balance between the precision of coordinate extraction and battery consumption capabilities, as well as the storage requirements for storing TLS cryptographic keys [10].

An IoT-based security solution for smart transportation was proposed by Zhang et al. (2021). The solution was based on geo-spatial modeling to secure intelligent transportation systems. The proposed architecture was designed to monitor transportation infrastructures and improve security by utilizing IoT devices in combination with cyber-physical security mechanisms. The solution was experimentally evaluated and showed improvements in monitoring and detection capabilities for transportation-related security threats. However, the research did not address the aspect of authenticated encryption for the secure transmission of data between edge computing devices and the monitoring server.

[8] Restuccia et al. experimentally evaluated the performance of TLS 1.3 and DTLS 1.3 security protocols in terms of memory, energy consumption, and communication overhead on low-power IoT devices. The results showed that TLS provides higher security with only a marginal increase in resource utilization. The study did not address the aspect of secure transmission of sensitive transportation data using authenticated encryption. [9]

3. Proposed System Architecture

The mentioned methodology aims to provide secure communication between the monitoring system and the central server by implementing Transport Layer Security (TLS) protocol using AES authenticated encryption. In this case, transportation status information will be transmitted through the channel established on the TLS layer, which will provide encryption to guarantee confidentiality and data integrity.

First, the package monitoring system needs to form a transportation status message, which may contain the specific location of the delivery, tampering evidence, authentication status, and detected anomalies.

To initiate a secure connection with the central server, the master node should execute a TLS handshake procedure, during which two sides of communication will verify each other and agree on particular algorithms which will define the TLS session and secure data transmission.

3.1 TLS Secure Transmission

The Transport Layer Security (TLS) protocol is used for secure communication between the master node and central server during package transportation Since the fleet has report consists of sensitive information like the location of the package, whether any tamper evident feels were broken results from authentication tests and analysis regarding it is important to ensure that strong encryption techniques are employed to avoid interception and tampering by unintended parties. TLS enables secure communication by authenticating your master mode and central server, meanwhile encrypting all data transported between them protecting against some of the more common cyber security threats such as interception and message modification.

In addition the proposed solution also use of TLS that generates an encrypted session key and allow the data to be encrypted by using AES encryption algorithm over this secure channel while transmitting. In view of the entire detail it can be said that TLS protocol is an integral part of the package transportation system where confidentiality integrity and authenticity guarantees communication between the central server and master node (significant real time information exchange) while building up reliability in the system first is the master node set as a TLS (Transport layer Security) connection with server then gradually finds and send the fleet health report from its case it has received in the handshake the server certificate is validated and a session key is created then the document is encrypted by AES (Advanced Encryption Standard). First the Master node generates a unique initialization vector for each message. Subsequently, a session key is employed to encrypt the report. To avoid reply attacks is calculated on an encrypted message some other data (a timestamp and a sequence number for example). From that point onwards the server receives a tag, ciphertext and. Now the server calicates the tag again to check if they are equal to the one sent with the message. If the tags do not match the package is simply discarded and logged and messages that have been replayed are tampered which are never processed. Since the AES encryption algorithm used for this architecture protect both confidentiality and integrity, authentication the design omits a message authentication code (MAC) to conserve limited bandwidth from brief but repeated messages master node encryption and central server decryption and authenticating algorithm to an algorithm 3.2.1and 3.2.2 and respectively. flow chart.

3.2 AES Encryption

The Prospect system is developed to securely transmit the transportation status information using AES (Advanced Encryption Standards) to send transportation status information to the central server.

For the sake of argument, it is noted that using an algorithm clearly shows confidentiality, integrity and authentication of the data within a specific encryption method it used to provide secrecy while the authentication tag guarantees data integrity. Simultaneously, due to AES high speed processing and low overhead, it is benefiting for the real time IoT based secure package transportation system.

Once the TLS session is established, Fleet Health reports get encrypted using AES authenticated encryption algorithm. Here, a randomly generated 96 bits force is required to be used for the encryption process. It is then sent using the shared session key to encrypt this report.

3.2.1 Algorithm: AES Encryption Process (Master Node)

Initialization Vector (IV), Secret Key (K), and Fleet Health Report (R) are the inputs. Ciphertext (C) and Authentication Tag (Tag) are the output. Commence.

1: Create the Fleet Health Report (R) using the Master Node.
2: Create an initial vector (IV) from scratch.
3. Enter the secret key (K).
4: To obtain the ciphertext (C), encrypt the Fleet Health Report using AES and K and IV.
5. Create the Authentication tag (Tag).
6: Add the authentication tag and the initialization vector to the final ciphertext.
7: Use the secure TLS channel to transmit an encrypted message (C, IV, Tag) to the Central Server. Give up.

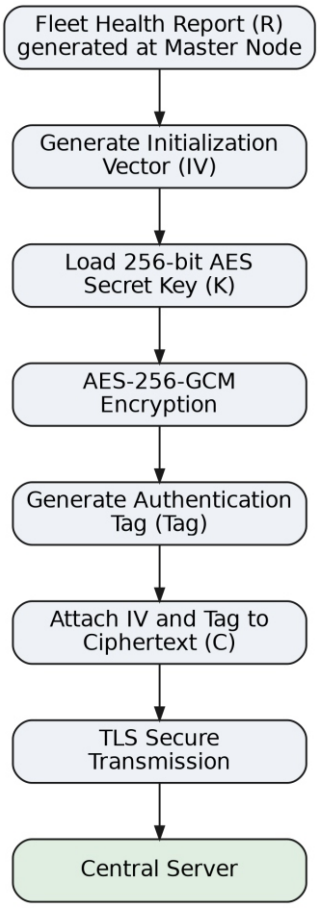

Fig 3.2.1 Encryption workflow executed at the Master Node

3.2.2 Algorithm: AES Decryption Process (Central Server)

After obtaining the ciphertext, the main server checks the Authentication Tag and tries to decrypt the message. Decryption will be successful only if the message was not tampered with during transmission. In turn, the server decrypts the ciphertext using the session key to obtain the original Fleet Health Report. On the other hand, if the Authentication Tag fails the check, the message should be discarded, and the incident needs to be reported. A proposed cryptographic algorithm for secure transmission of data packets.

Ciphertext(C), Secret key (K), Initialization vector(IV), Authentication tag(Tag)
Output: Original Fleet Health Report(R)
1: Start
2: Accept encrypted message (block of Ciphertext (C), IV, Tag) from master node
3: Load secret key from the system K
4: Verify the authenticity of the given message
5: If valid then perform AES Decryption to get the Original Fleet Health report R
6: Update the monitoring system and send notification
7: Else raise a security concern (log as failed transmission)
8: Stop

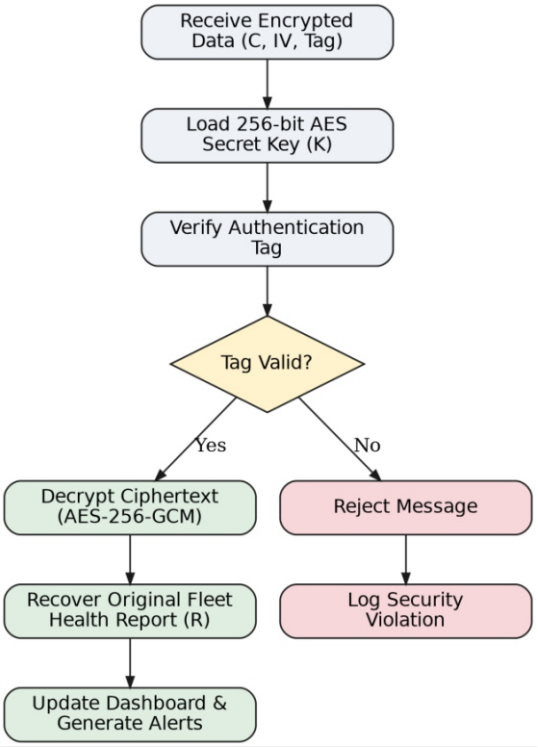

Fig 3.2.2. Decryption and verification workflow executed at the Central Server

4. RESULTS

The proposed secure communication framework was experimentally evaluated to verify the performance of the TLS protocol with AES in terms of encryption/decryption latency, communication overhead, and the data security level.

The experiments were conducted by transmitting the Fleet Health Reports with different sizes from the master node to the central server through the secure TLS channel.

This result specifies that AES adds only a small processing overhead to the encryption and decryption process. With the increases in larger data sets, the processing time was affected due to higher complexity nature of the algorithm. The overhead, however, was small enough that the encrypted message never had to wait in line in processing inside of the IOT environment. The data confidentiality and integrity of the proposed framework was also Proven secure, as these properties are ensured by the security model for a authenticated encryption schema over transmitted data.

This was provided by implementing a communication channel establishment using TLS protocol among the IoT nodes in a secure manner. Specifically, the test run successfully established a shared session key and mutual certificate authentication. as such, any reaction without permission from the data transmission phase could not be performed due to the fact that the communication channel was encrypted with TLS. Such eavesdropping failed since the message were encrypted with changing session key, which updates on-the-fly.

In addition, on the security side, any attempt for data corrupt during the transmission can be detected by the tag verification on receiver side. These result from the performance analysis shows that with embedded TLS and a lifespan of time, our proposed secure communication architecture will be able to provide security and reliable communication for IoT based package transportation system. The framework offered encryption and decryption for data in near real time while operating over efficiency.

5. CONCLUSION

To provide enough assurance of security this study present a secure communications framework for intelligence transport of a package employing AES authenticated encryption and TLS transport layer security. it is our scope hence to identify the encryption and authentication algorithms that can fight against these identified threads in the system with a low computational overhead, so first, we focused on transferring a fleet health report over security TLS channel between central server and the master note to avoid unauthorized disclosure, modification, reply and eavesdropping since it was found that (AES) authenticated encryption standard works both as encryption function and authentication function almost at a lower cost. Results of the experiment also indicated that both encryption and decryption processes had low latency which made it suitable for real time applicability in Internet of Things based intelligent transportation systems.

References

1. Anomaly Detection in IoT Networks Using Federated Machine Learning Approaches (2FIDS, smart-home fog-federated IDS), *ResearchGate*, 2025.
2. A Systematic Review of Light-Weight Cryptographic Schemes for Security and Privacy in IoT, *Discover Computing*, Springer, 2025.
3. Privacy-Aware Anomaly Detection in IoT Environments using FedGroup: A group-based federated learning approach, *Journal of Network and Systems Management*, Springer, 2024.
4. Senol, N.S.; Baza, M.; Rasheed, A.; Alsabaan, M. Privacy-Preserving Detection of Tampered Radio-Frequency Transmissions Utilizing Federated Learning in LoRa Networks. *Sensors* 2024, 24, 7336. https://doi.org/10.3390/s24227336
5. Federated Deep Learning for Anomaly Detection in the Internet of Things, *Computer Communications*, ScienceDirect, 2023.
6. A Comprehensive Review of Lightweight Authenticated Encryption for IoT Devices, *Wireless Communications and Mobile Computing*, Wiley, 2023.
7. A Novel Secure End-to-End IoT Communication Scheme Using Lightweight Cryptography Based on Block Cipher, *Applied Sciences*, MDPI, 2022.
8. Zhang, J., Wang, Y, Li, S. et al. (1 more author) (2021) An architecture for IoT-enabled smart transportation security system: a geospatial approach. *IEEE Internet of Things Journal*, 8 (8). pp. 6205-6213. ISSN: 2327-4662
9. Restuccia, G., Tschofenig, H., & Baccelli, E. (2020). Low-Power IoT Communication Security: on the performance of DTLS and TLS 1.3. *arXiv* (Cornell University). https://doi.org/10.48550/arxiv.2011.12035.
10. LTE Based Vehicle Tracking and Anti-Theft System Using Raspberry Pi Microcontroller (TLS-secured MQTT fleet monitoring), *ResearchGate*, 2019.