IJEMD-CSAI, Special Issue (2026) https://doi.org/10.54938/ijemdcsai.2026.04.2.658

IJEMD

International Journal of Emerging Multidisciplinaries: Computer Science and Artificial Intelligence

Research Paper

Journal Homepage: www.ojs.ijemd.com
ISSN (print): 2791-0164 ISSN (online): 2957-5036

Privacy-Preserving Intrusion Detection in Smart Traffic Networks

Woh Xiang Huai [1], Lin Peng [1], Sarah Diong Yu Jie [1], Zhang Liangyu [1], Su Boyu [1], Zainab Hana [1], Tan Min Hong [1],

1. School of Computer Science, Taylor's University, Subang Jaya, 47500, Selangor Malaysia

1.0 Abstract

Smart transportation and associated systems are becoming more susceptible as they also apply to cyber threats such as Distributed Denial-of-Service (DDoS), model poisoning, node impersonation, and ransomware lateral movement using more interconnected IoT products (traffic controllers, sensors, cameras, etc.). The current centralized Intrusion Detection Systems (IDS) have structural disadvantages, namely, high latency, bandwidth overhead, privacy exposure, and single-point collision, which limit their applicability in real and safety-critical urban settings. In order to handle these gaps, this research will suggest a Federated Learning Multi-layer Intrusion Detection System (FL-IDS) that is specifically crafted to intelligent traffic infrastructures. The architecture incorporates edge-based anomaly detection, federated collaborative learning, secure aggregation, differential privacy, encrypted communication (TLS 1.3, MQTT-S, SNMPv3), and devices-integrity (Secure Boot and firmware signing). Every intersection does its local detection and transmits the encrypted model updates, which allows them to learn globally and capture the local traffic features. Detection performance, latency, and bandwidth consumption coupled with resistance to poisoning attacks were tested within a conceptual experimental framework comprising of the CICIoT2023 dataset and trafficking simulated variations in the real world. Findings indicate that FL-IDS is better at performance compared to Cloud-IDS and traditional ML-IDS, with a high detection rate of 95% and a false-positive rate of 1.8 percent along with a detection latency of 80 ms and bandwidth consumption of 2.3 MB. With the conditions of model-poisoning, the reduction in accuracy is only as high as 8 percent, proving to be highly resilient with secure aggregation and differential privacy.

Email Addresses : 0375150@sd.taylors.edu.my, 0370812@sd.taylors.edu.my, 0367917@sd.taylors.edu.my, 0378417@sd.taylors.edu.my, 0370332@sd.taylors.edu.my, 0378587@sd.taylors.edu.my, 0374100@sd.taylors.edu.my

Keywords: Federated Learning, Smart Traffic Security, Intrusion Detection System (IDS), IoT Cybersecurity, Distributed DDoS Défense

2.0 Introduction & Problem Identification

2.1 Smart City Adoption with IoT Technologies: An Introduction

Not only have cities become more intelligent, but improvements have also been made to the efficiency and the quality of the city's public services through IoT (Internet of Things) technologies due to the increase in the population of urban areas (Sunday et al., 2024; Keon et al., 2025). The infrastructure components are connected intelligent transportation, energy networks, environmental surveillance, waste management, and public health systems. A city's smartness mainly relies on its utilization of IoT systems with real-time monitoring and automation of indispensable public services being carried out. The amalgamation of sensors, communication networks, and data analytics with technologies consists of resource saving, reduction of operational costs, and citizen services (Toh, 2020; Kiyani et al., 2024).

Nonetheless, the emergence of IoT technologies on a large scale introduces complex security issues. Smart cities are the number one cybersecurity target due to a plethora of interconnected devices, which are considerably increasing the attack space (Sunday et al., 2024; Krishnan et al., 2021). Traditional IT systems differ from many IoT devices as they are resource-constrained systems having less power and requiring traditional security mechanisms to be applied, which might be ineffective (Riyaz, 2024). Smart city infrastructure consists of fundamental services, and insecurities can put all mission-critical operations at risk, infringe upon privacy, and endanger the public safety; therefore, the creation of a framework for the security of such cities has ranked as the highest priority (Yaacoub et al., 2023).

2.2 The Smart City Ecosystem's Security Threats

In smart cities, security is a multilayered issue with vulnerabilities at hardware, network, and application levels. For the case of embedded software, the security risks are based on poor coding, inadequate authentication. Such lapses enable the attackers to gain entrance quite easily (Chatterjee et al., 2022; Linqiang et al., 2024). The network layer gets a fair share of attackers that are called man-in-the-middle, distributed denial-or-service (DDoS), and eavesdropping, which, in turn, are capable of disrupting the public services (Neto et al., 2023; Sanjaya et al., 2025). On the application layer, there are threats like data breaches from APIs (Application Programming Interface) and poor encryption (Al-Garadi, 2020; Sindiramutty et al., 2024a).

One issue that technology experts have in mind is DDoS (Distributed Denial-of-Service) and ransomware attacks on smart transportation systems. Ransomware has an extreme impact by locking out digital assets for ransom, paralyzing traffic signal controller systems, and complicating emergency vehicle routes, even endangering lives. For example, the hackers were successful in seizing Dallas's traffic light locations in 2023, where they alternatively changed the signals, creating traffic that was not solved by authorities for

several days (Anthikempath, 2023). Likewise, in Baltimore in the year of 2019, ransomware paralyzed the city government, a part of which includes crippling the email system and payment portal of the city, showing the seized control of critical infrastructures (News, 2019) Through these cyber attacks, it became clear that the design of current security measures is not robust enough to detect or combat newly appeared threats such as DDoS attacks or polymorphic ransomware, which are frequently updated signature detection or cloud architecture (Wang et al., 2024; Sindiramutty et al., 2024b).

Security tactics being followed currently also have certain weaknesses. Unlike traditional signature-based detection systems that can create signatures of new attacks, artificial intelligence-based systems cannot create anti-viruses for new or modified threats. Latency is a very critical issue for cloud-based models for a real-time application such as traffic management. Moreover, such machine learning-based protecting models usually need central data processing and transfer, which can be inefficient and even have privacy issues (Truex et al., 2021). Another basis for security strategies lacking by AI is insufficient way of explaining how they make decisions; hence, trust and acceptance of thinkers concerned are reduced (Vilone, 2021) Creating a thin, explainable, and adaptable security framework becomes a necessity to secure smart city infrastructure from high-level threats like DDoS attacks and ransomware.

To prevent the smart traffic management system compromised from cyber-attack using its vulnerabilities causing road hazard. We proposed an advanced novel, secured system. This system particularly designed to mitigate threat of DDoS and ransomware attack which can cause major disruption on traffic signal daily operation, compromise emergency vehicle routes, and cause widespread traffic chaos. By implementing latest security protocol related to robust encryption, real-time threat monitoring and anomaly detection mechanism, our proposed system solution. Our system aimed to enhance and mitigate the modern cyber threat which were DDoS and ransomware to ensure the safety and efficiency of transportation networks in smart cities.

3.0 Literature Review & Gap Analysis

3.1 Literature review

3.1.1 Privacy and Federated Learning

Federated Learning (FL) is a machine learning technique where a node trains a model using its own local data, preserving privacy and reducing data transfers (Yaacoub, 2023). These types of systems work best in urban areas where the systems are spread out, in areas such as clinics, public transportation systems, or power services. FL isn't devoid of risks; it could be subjected to sabotage attempts, data leaks from models, or irregular syncing between devices. Without the right safeguards, if the machine learning model is attacked, the accuracy can drop by more than 25% (Yaacoub, 2023). Although it is currently being reached, it is still in the early stages; it lacks robustness against real-life attacks, like poisoning, model inversion, or unreliable devices. There is no unified or widely accepted framework for FL against IoT deployments. Only a few studies equip FL with sanity-checking rules or XAI tools.

3.1.2 IoT-based DDoS attacks detection mechanisms overview

Machine learning (ML) and deep learning (DL) functions as the central research field which studies these techniques to detect DDoS attacks through analysis of IoT network data. (Shukla, 2024) demonstrate that DL-based methods including CNNs, LSTMs, and autoencoders outperform traditional rule-based systems and signature-based systems when detecting abnormal traffic through their evaluation of contemporary IoT datasets. The current research identifies four main problems which stem from the lack of diverse real-world datasets and the difficulty to detect low-rate stealthy attacks and the security gaps in resource-limited IoT devices and the need for models to adapt to concept drift in changing network environments. The Mirai botnet demonstrates attackers achieve their goals through inadequate security protection of IoT devices. The situation demands immediate improvements in authentication methods together with hardware that provides built-in security and advanced detection capabilities in network edge systems.

The research demonstrates that ML and DL technologies show promise for IoT systems, yet these systems face major challenges with interoperability and scalability and continuous updates which attackers exploit. The upcoming research direction will focus on three main areas which include federated learning for private detection systems and lightweight models for edge computing devices and defense systems that combine anomaly detection with system resilience.

3.1.3 Federated Learning for IoT (Security-Focused)

This research (Nguyen, 2021) is about how Federated Learning (FL) has gained significant attention as a privacy-preserving solution for securing Internet of Things (IoT) environments because it enables model training directly on devices without sharing raw data. This research shows that FL improves data confidentiality and supports large-scale, distributed IoT applications such as smart healthcare, smart cities, transportation systems, and industrial automation. Studies show multiple security threats continue to affect FL systems even though they offer various advantages through model-poisoning and backdoor attacks and Byzantine client behaviour and gradient-based privacy leakage. This research investigates different solutions which include differential privacy and secure aggregation and homomorphic encryption and anomaly detection and blockchain-assisted federated architectures to solve these problems. Research studies show that these defence methods encounter three main barriers which stem from their excessive computational requirements and their negative effect on model performance and their inability to handle non-IID data and limited IoT device resources which proves that secure FL for IoT devices require additional research.

3.1.4 Ransomware-based Cyber Attacks: A Comprehensive Survey

This research discusses about ransomware threat towards Internet of Thing (IoT). Ransomware refers to malicious software trying to obtain the computer system without their permission. They break the system and ask for payment as “ransom” from legitimate and authorized user by destructing either important data or posting user’s data to public if ransom are refused to be paid. (Park, 2023; Pal et al., 2023)

The system becomes permanently unusable because of three main ransomware types, which include crypto-ransomware, locker ransomware, and Master Boot Record (MBR) attacks. The detection and prevention of ransomware attacks in IoT networks can become possible through the implementation of Artificial Intelligence (AI), Blockchain technology, and Software-Defined Networks (SDN). AI helps automate detection through machine learning and deep learning models, and Blockchain provides decentralized storage which enhances the security and integrity of IoT data.

3.1.5 Real-World Security and Policies

Most IDS research studies up to the technical model and does not consider how decision reports turn into real-world actions, like rerouting traffic, using fail-safe modes, or coordinating with first-responders across the city. Industry reports and operational case studies provide reports that more than 33% of IoT gadgets are getting exploited, hijacked, or have bad setups. When privacy or safety falls apart, cities sometimes hit pause or redo entire rollouts, as such cases in Singapore and Dubai (Sunday, 2024; Ponnusamy et al., 2021). A working detection setup needs to hook into real policies: how updates roll out, who's in charge, and what happens during an incident. Miss those links, and no tech stands a chance of growing or being believed (Toh, 2020). Governance rules, updating procedures, and accountability structures are often overlooked in technical research.

3.1.6 How IT Governance Can Assist IoT Project Implementation

The integration of Internet of Things (IoT) technology into organizational frameworks poses unique challenges, especially in the areas of governance. For organizations intent to achieve their goal through implementation of IoT project, IT governance (ITG) stands as critical component. (Henriques, 2021) The growing data output from IoT devices require organizations prioritizing data privacy along with data protection when designing IT governance frameworks like COBIT.

The research identifies three essential IT governance elements for IoT projects, which consist of strong data management systems, complete security measures, and standardized interoperability protocols. These elements could greatly enhance credibility for IoT system while they are enabling organizations to work together and protect against modern threat that may appear in complex IoT networks setup.

3.1.7 Smart traffic Management system for metropolitan cities of kingdom using cutting edge technologies

The research (Humayun, 2022; Sindiramutty, Tan, & Wei, 2024) paper presents a smart traffic management system for urban areas which combines IoT technology with cloud computing and 5G networks and big data analytics to improve traffic flow and decrease congestion levels. The system operates through three distinct layers which start with the physical layer that includes IoT sensors for vehicle detection and then move to the network layer which uses 5G for data transmission and ends with the application layer that delivers real-time information to dashboards and Google Maps. The system demonstrated its effectiveness through the Riyadh case study which showed early traffic jam detection and exact vehicle monitoring and immediate system updates that decreased both time and fuel usage. The system operates with low expenses and can handle growing numbers of users but continues to face

operational difficulties when operating in adverse weather conditions and scaling up. The research should continue by integrating AI technology to make the system operational in expanded metropolitan areas.

3.1.8 Blockchain-Technology-Based Solutions for IOT Security

The research (Al-Barazanchi, 2022; Weiqi et al., 2024) paper examines blockchain technology to find solutions which would secure Internet of Things (IoT) systems. It begins with an overview of blockchain's decentralized, immutable, and cryptographic features, contrasting public, consortium, and private types, and highlights its applications in finance, IoT, public services, reputation systems, and security, while noting vulnerabilities like 51% attacks. It also introduced IoT component such as sensor, data processing, connectivity etc, and its risk such as data privacy breach, high network traffic etc. Decentralized systems play a vital role in protecting data privacy and integrity and maintaining transparency when large amounts of sensitive information move through connected devices in networked environments. The paper describes how blockchain technology operates within IoT systems to secure smart homes and supply chains and smart appliances while protecting privacy and enabling secure transactions.

3.1.9 An Integrated Federated Machine Learning and Blockchain Framework with Optimal Miner Selection for Reliable DDOS Attack Detection

The research paper (Saveetha, 2024; Ying et al., 2024) presents a combined system which integrates Federated Machine Learning (FL) with blockchain technology to create a dependable DDoS attack detection solution for blockchain networks. The paper demonstrates how DDoS attacks create major obstacles for decentralized networks because machine learning-based anomaly detection systems need to gather worldwide attack information. The proposed system operates through FL to perform distributed learning at local nodes (miners) while blockchain immutability and miner reputation selection protect against harmful model updates. The method protects model integrity which yields exact detection results. The FL model receives protection against tampering because of blockchain integration, and the reputation system allows only miners with proven trustworthiness to participate in model training. The framework evaluation showed 99.1% detection accuracy for DDoS attacks through Random Forest and Multilayer Perceptron and Logistic Regression algorithms which exceeded the results of conventional detection approaches.

3.2 Gap Analysis

3.2.1 Weak Device Security & Easy Compromise (Fundamental Gap)

Fundamentally, the weak security posture of most devices presents a major security gap in IoT ecosystems. Most IoT devices, particularly that large-scale deployment in smart-city environments, are manufactured with low-cost hardware and computationally limited capacity. Consequently, manufacturers often ship devices with weak or default passwords, outdated firmware, insecure communication protocols, and, in many instances, no encryption of any kind. Such limitations make devices an easy target for attackers, who can easily compromise them with minimum effort and then recruit them into large-scale botnets like

Mirai Without secure-by-design principles, vulnerabilities remain unremedied throughout the device lifecycle, leaving critical smart-city infrastructures exposed to continuous exploitation.

3.2.2 Lack of Robust Authentication & Access Control

Lack of robust authentication and access control is another system vulnerability issue among IoT systems. Most IoT implementations lack fundamental components including robust authentication of devices, checking identity and ensuring safe authorization systems (Doshi, 2022). This opens the system to numerous attacks such as the hijacking of devices, identity spoofing (e.g. Sybil attacks), privilege escalation, and unauthorized access to sensitive networks. The basic problem is that there is no single, standardized method of authentication of heterogeneous IoT environments when IoT devices of different vendors are provided based on competing protocols, with multiple security layers and collective components (Sicari, 2023). Even in the absence of powerful and persistent access control, IoT networks are still susceptible to unauthorized intrusion and manipulations.

3.2.3 Privacy and Federated Learning

Federated Learning has become more popular in IoT environments because it lets devices learn from their own data without sending sensitive information to a central location. The introduction of FL technology creates various security vulnerabilities which lead to major protection weaknesses. The privacy benefits of FL do not protect it from multiple security threats which include data poisoning and model inversion and gradient leakage and adversarial manipulation during model updates (Bonawitz, 2020; R et al., 2021). The system contains multiple security weaknesses which jeopardize both the protection of user privacy and the integrity of the model. The synchronization between devices and model accuracy becomes unreliable because FL operates in smart-city environments which deal with unpredictable device availability and devices that have different hardware specifications and update schedules that do not match each other. The current FL implementation in IoT systems requires immediate research to develop secure aggregation protocols and anomaly checking mechanisms and adversarial-resistant optimization strategies because no established protection systems exist for these environments.

3.2.4 Real-World Security and Policies

The field of IoT intrusion detection has made great progress through technical research but smart-city environments fail to implement these systems effectively in their actual operations (Hussein, 2021). Most studies ignore essential inquiries about how to handle governance and policy integration and emergency response coordination during crisis events. The current system lacks an established protocol for automated systems to handle detected intrusions in traffic-light systems because it remains unclear how these systems should respond through traffic rerouting or emergency alerts or fail-safe operations or human operator intervention (Hussein, 2021; Ren et al., 2018). The current system lacks established protocols for automated systems to handle detected intrusions in traffic-light systems because it remains unclear how these systems should respond through traffic rerouting or emergency alerts or fail-safe operations or human operator intervention. The current system lacks established protocols for automated systems to handle detected intrusions in traffic-light systems because it remains unclear how these systems should

respond through traffic rerouting or emergency alerts or fail-safe operations or human operator intervention (Hussein, 2021; Saeed et al., 2022). The current system lacks established protocols for automated systems to handle detected intrusions in traffic-light systems because it remains unclear how these systems should respond through traffic rerouting or emergency alerts or fail-safe operations or human operator intervention. The gap that exists between detection and action shows the absence of functional governance systems and established decision-making protocols (Hussein, 2021).

3.2.5 Data Integrity and tampering

Recent work in FL and secure aggregation enhances privacy protection, but several gaps remain regarding data integrity and tamper protection. The secure aggregation method hides only the model update information from users but the research shows this approach fails to verify the authenticity of model updates during transmission. The global model faces destruction through malicious clients who introduce harmful or altered gradients which pass unchallenged through normal aggregation systems. The main objective of secure aggregation is to maintain privacy but contemporary systems fail to provide sufficient methods to detect any changes that occur during data transmission and storage. The system faces security risks because it lacks adequate provenance tracking methods which include immutable logging and verifiable model lineage and cryptographic consistency checks. The system enables attackers to perform undetected manipulation of outdated updates through replay attacks. The current state-of-the-art FL frameworks do not include protection mechanisms against model-version tampering and silent parameter corruption and unauthorized model replacement. The main difference between these systems is that FL-based distributed systems protect confidentiality but they do not properly protect data integrity or defend against tampering attacks.

4.0 System Overview

To overcome these downsides, we proposed a Federated, Multi-Layer Intrusion Detection System (IDS) for smart traffic management systems. The traffic intersection performs local training of lightweight anomaly-detection models by using own traffic data pattern instead of sending raw data to a central data processing location. Within intrusion detection systems (IDS) aimed at identifying zero-day attacks, effective data preprocessing and feature selection are crucial for maintaining both model accuracy and computational efficiency. (Alansary, 2025) Only encrypted model update, not sensor data are sent to central aggregator. Using Federated Learning (FL) ensure privacy, reduces bandwidth usage and defence against both DDoS and ransomware attacks.

Each traffic intersection operates as a local IDS node. The traffic light controller together with its sensor and communication module runs on a lightweight anomaly-detection model. The system tracks network traffic patterns through request rate and packet burst, as well as device actions including abnormal CPU activity and configuration changes to detect DDoS attack and ransomware installations at their initial stages.

4.0.1 Federated learning (FL)

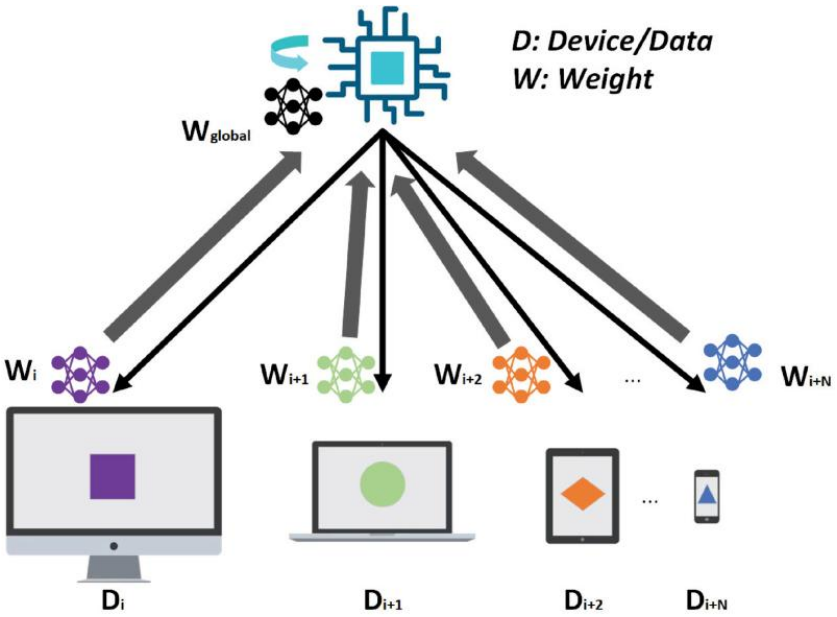

Figure 1 Federated Learning Overview (Siniosoglou, 2023)

We have deployed Federated learning (FL) inside the local IDS node to strengthen the system's ability to detect and stop DDoS and ransomware attacks. Federated Learning (FL) is well-suited to privacy-preserving decentralized approaches, where data remains local and models are trained without transfer. (Alharthi, 2024) The local IDS nodes operate independently to develop their models by using their specific raw traffic data and device behaviour which enables them to identify DDoS traffic irregularities and ransomware activities without sharing sensitive information with a centralized server for processing. The system reduces attack surface exposure which leads to improved privacy protection for each device and preserves network functionality when individual nodes face security breaches.

The system allows each local node to send encrypted model updates to the central aggregator (security operation centre) at specified time intervals for aggregated data processing. After the SOC have review and validate the latest global model is suitable to upgrade, it distributed back to all intersection, allowing each node to learn from each other nodes data under different location and condition. The system achieves ongoing detection enhancement by merging various traffic patterns with environmental conditions and threat detection data which boosts the smart traffic management network's security performance and operational accuracy.

4.0.2 Blockchain Integration for Enhanced Security

To further enhance our security of the system, we integrate blockchain technology enabling data are more secured and provide an immutable auditing log. Blockchain technology offers significant improvements for managing document versions and facilitating secure sharing. (Hammad, 2023) Blockchain technology enables a future where contracts are digital code held in secure, shared databases. This setup ensures they are permanently protected against any unauthorized changes, deletion, or manipulation. (Iansiti, 2017)

Because federated learning relies on sensitive user data, locally trained models are vulnerable to machine learning attacks. (Ferrag, 2021) Federated training managed through blockchain allows numerous edge nodes to collaborate securely and reliably without relying on a central authority. (Abdel-Basset, 2021) A permissioned blockchain which are blockchains that are closed (i.e., not publicly accessible) or have an access control layer is used to handle identify verification and transaction provenance and integrity while keeping sensitive information hidden from view. The system design requires each traffic intersection to run its own local IDS node which stores unprocessed traffic data and performs model training at the intersection site. The completed FL training round requires the node to send its encrypted model update to off-chain storage while storing only the update hash along with timestamp and digital signature and basic metadata on the blockchain.

To further enhance our security of the system, we integrate blockchain technology enabling data are more secured and provide an immutable auditing log. Blockchain technology offers significant improvements for managing document versions and facilitating secure sharing. (Hammad, 2023) Blockchain technology enables a future where **contracts are digital code** held in secure, shared databases. This setup ensures they are **permanently protected** against any unauthorized changes, deletion, or manipulation. (Iansiti, 2017) Because federated learning relies on sensitive user data, locally trained models are vulnerable to machine learning attacks. (Ferrag, 2021) Federated training managed through blockchain allows numerous edge nodes to collaborate securely and reliably without relying on a central authority. (Abdel-Basset, 2021) A permissioned blockchain which are blockchains that are closed (i.e., not publicly accessible) or have an access control layer is used to handle identify verification and transaction provenance and integrity while keeping sensitive information hidden from view. The system design requires each traffic intersection to run its own local IDS node which stores unprocessed traffic data and performs model training at the intersection site. The completed FL training round requires the node to send its encrypted model update to off-chain storage while storing only the update hash along with timestamp and digital signature and basic metadata on the blockchain.

Smart contracts perform security functions which include node registration and update verification and model version control and global model aggregation approval before distribution. The Security Operation Centre (SOC) functions as the primary validator which uses off-chain validation to identify poisoned or unusual model updates before it approves transactions for blockchain recording. The SOC posts the global model hash on the blockchain after verification to enable local nodes to verify the correct model version through off-chain storage retrieval.

4.0.3 Federated + Blockchain technology

The system achieves traceability and tamper-evidence and fast compromised node revocation through its implementation of blockchain with Federated Learning. The blockchain ledger protects against unauthorized updates because it requires validators to reach consensus before accepting any suspicious or unauthorized changes. The architecture design allows smart traffic management systems to operate with higher robustness and accountability and resilience while maintaining both low latency operation and data privacy protection.

4.1 Algorithm

4.1.1 Anomaly Detection Algorithms (Local IDS Node)

- Autoencoder (AE): Detects deviations in traffic patterns, lightweight for edge devices.
- Isolation Forest: Identifies outliers with low overhead (e.g., DDoS bursts).
- One-Class SVM: Flags deviations based on normal traffic; ideal for small datasets.
- LSTM: Detects traffic bursts and ransomware (requires tuning).
- Statistical Methods: Simple and fast for traffic anomalies.

Tip: Use Isolation Forest or Autoencoder for lightweight nodes.

4.1.2 Federated Learning Algorithm

- FedAvg: Standard FL algorithm, nodes train locally and send updates for averaging.
- FedProx: Handles heterogeneous data across nodes.
- Secure Aggregation: Encrypts model updates to ensure privacy.

Tip: Start with FedAvg + Secure Aggregation; use FedProx for varied traffic.

4.1.3 Blockchain Integration

- Consensus Algorithm: PBFT (low-latency) or Raft/Tendermint (lightweight).
- Smart Contracts: For node registration, update verification, and version control.
- Hashing & Digital Signature: SHA-256 for integrity, ECDSA/RSA for signing.

Tip: Use a fast, lightweight consensus algorithm for tamper-proof tracking.

4.2 Protocol

4.2.1 Communication Security Protocols

- TLS 1.3 — Secure communication, model update encryption, node authentication
- MQTTS (MQTT over TLS 1.3) — IoT messaging for status, alerts, FL triggers
- SSH v2 — Secure administrator access and firmware management

4.2.2 Federated Learning & Model Security Protocols

- Secure Aggregation Protocol — Protects individual model updates
- Differential Privacy (DP) — Prevents gradient leakage and model inversion

4.2.3 Blockchain Security Protocols

- PKI-Based Identity & Certificate Validation — Node authentication

- Smart Contract Verification — Validates update transactions and global model approval
- On-Chain Hash Integrity Protocol — Stores update hashes (CID) for tamper-proof provenance

4.2.4 Network Monitoring & IDS Protocols

- NetFlow / IPFIX — Traffic flow monitoring and DDoS detection
- SNMPv3 — Secure device health and network management

4.2.5 Device Integrity & Firmware Security

- Secure Boot — Ensures trusted firmware at startup
- Firmware Signing Protocol (PKI) — Authenticated firmware updates
- Code Signing (OTA Updates) — Verified IDS and controller software updates

4.2.6 Time Synchronization Protocol

- Secure NTP / NTP-Autokey — Accurate, authenticated time synchronization

4.2.7 Current System vs Proposed System

Feature	Traditional Systems	Our System (FL + Blockchain + Local IDS)	Benefit / Result
Single Point of Failure	Centralized server dependency.	Decentralized detection with blockchain-backed integrity.	**No Single Point of Failure:** Continual detection even if SOC is compromised.
DDoS Detection	Detection after data reaches the central server.	Local IDS detects anomalies in real time using FL-enhanced models.	**Earlier & Accurate Detection:** Faster response and reduced bandwidth usage.
Ransomware Detection	No behavior analysis or firmware integrity checks.	Local behavior analysis, file integrity, and automatic rollback.	**Early Prevention:** Detects ransomware before it locks systems or modifies configurations.
Network Resilience	Central server failure affects the entire system.	Local IDS continues, with blockchain ensuring integrity even during SOC downtime.	**High Resilience:** Traffic lights remain secure during attacks or outages.

Feature	Traditional Systems	Our System (FL + Blockchain + Local IDS)	Benefit / Result
Bandwidth Usage	High data transmission to central server.	Local processing with encrypted model updates sent via blockchain.	**Lower Bandwidth:** Reduced load and smoother performance.

4.3 System Architecture Overview

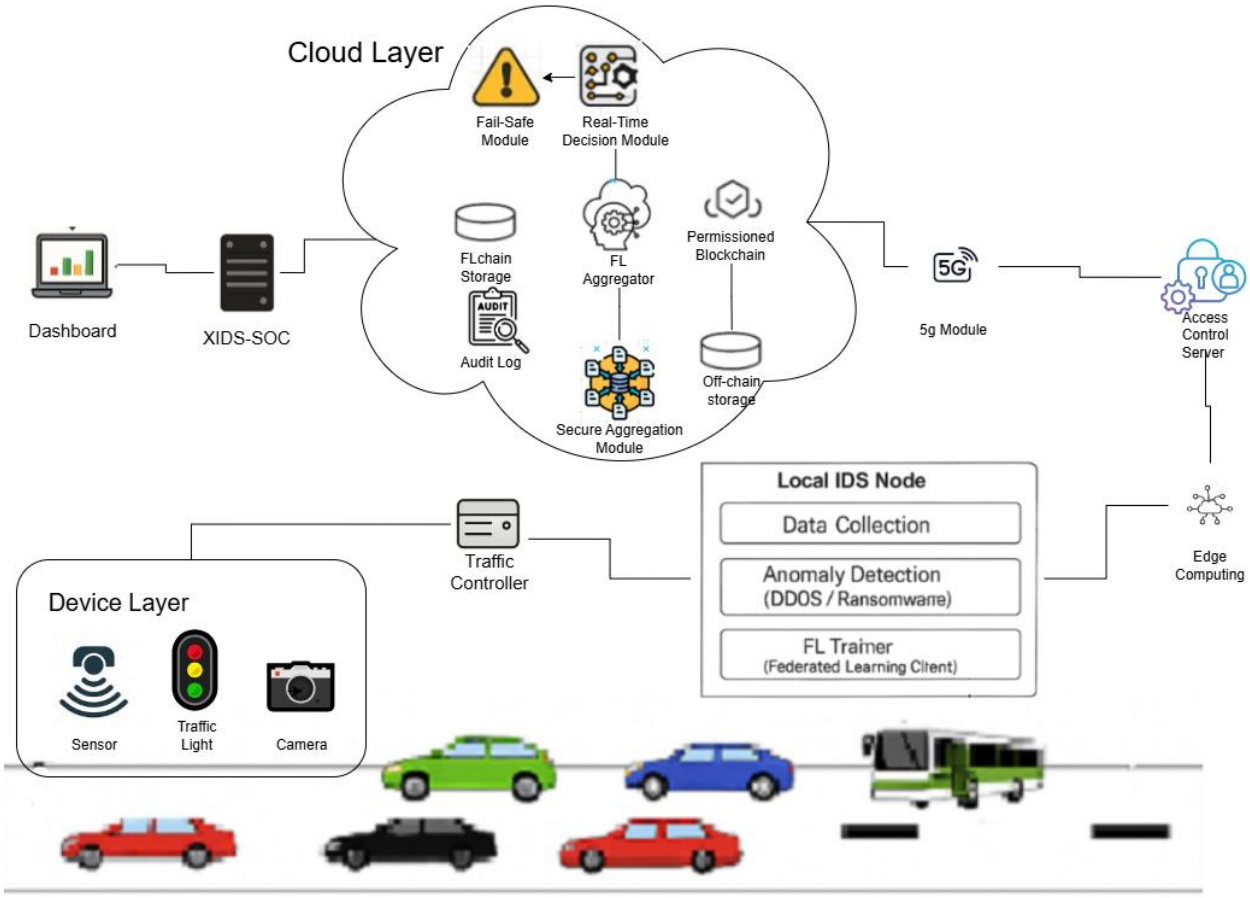

Figure 2 2 Proposed Federated Learning–Enhanced Smart Traffic Security Architecture

4.3.1 Device Layer

This layer contains all field IoT components that sense traffic conditions and generate raw operational data.

Key components:

Sensors: operate to detect vehicle numbers, speeds, and to measure road occupancy and environmental conditions.
Traffic Lights: Execute timing plans and switch to fail-safe modes during anomalies.
Cameras: record visual traffic information. This helps detect incidents and verify unusual occurrences.
Main role:
The system delivers immediate ground-level data for both traffic management and security breach detection.

4.3.2 Network Layer

This layer connects field devices to edge processing and the cloud while enforcing secure and reliable communication.
Key components:
Traffic Controller: Aggregates sensor/camera inputs and manages signal phases. (Rachmadi, 2011)
Local IDS (Edge IDS): Performs lightweight anomaly detection (e.g., DDoS, spoofing).
Edge computing systems: perform real-time inference operations to generate immediate results at the location where the data exists. (Boush, 2023)
5G Module: Ensures high-speed, low-latency data transfer. (Singh, 2024)
Access Control Server (IAS): Authenticates devices and prevents unauthorized access. (Reis, 2025)

Main role:
The system provides fast, secure communication for detecting and solving edge-level problems.

4.3.3 Cloud Layer

The system allows multiple intersections to train intrusion detection models together while keeping their original data private.
Key components:
FL Aggregator: The FL Aggregator system collects encrypted model updates from various intersections to build a single global model which improves anomaly detection capabilities in different traffic settings (Khan L. K., 2021).
Secure Aggregation Module: The Secure Aggregation Module protects model updates from exposure and safeguards them against poisoning attacks and gradient-inference threats through cryptographic multi-party masking and aggregation methods which it utilizes (Zhang, 2022).
Audit Log: Records all FL events for transparency and forensic tracking. (Mugunthan, 2020)
Real-Time Decision Module: Evaluates and deploys updated models. (Uddin, 2025)
Fail-Safe Module: Which blocks dangerous changes while switching to backup models. (Venčkauskas, 2025)
Permissioned Blockchain: Permissioned Blockchain systems achieve tamper-evident verification through their restricted write access which permits only authorized consortium members to add model-update hashes on the ledger (Chen X. L., 2020).

Off-chain Storage: Off-chain Storage keeps all encrypted model parameters in outside storage systems while storing only their hashes on the blockchain which reduces ledger load and maintains verifiable provenance (Salah, 2021).

Main role:

The main function of this position requires organizations to provide adaptable, privacy-maintaining model updates while keeping their machine learning systems operational and protected from failures.

4.3.4 Application Layer

The smart traffic system operates through its centralized intelligence and monitoring layer, which functions as its control centre.

Key components:

Dashboard: Visualizes system status, device health, traffic flow, and security alerts.

XIDS-SOC: The XIDS-SOC functions as the main security centre. It links threat data to enforce rules while managing security incident responses. (Bennouri, 2023)

Main role:

The system provides complete network visibility through centralized security management and advanced traffic monitoring capabilities.

4.4 Flow Diagram

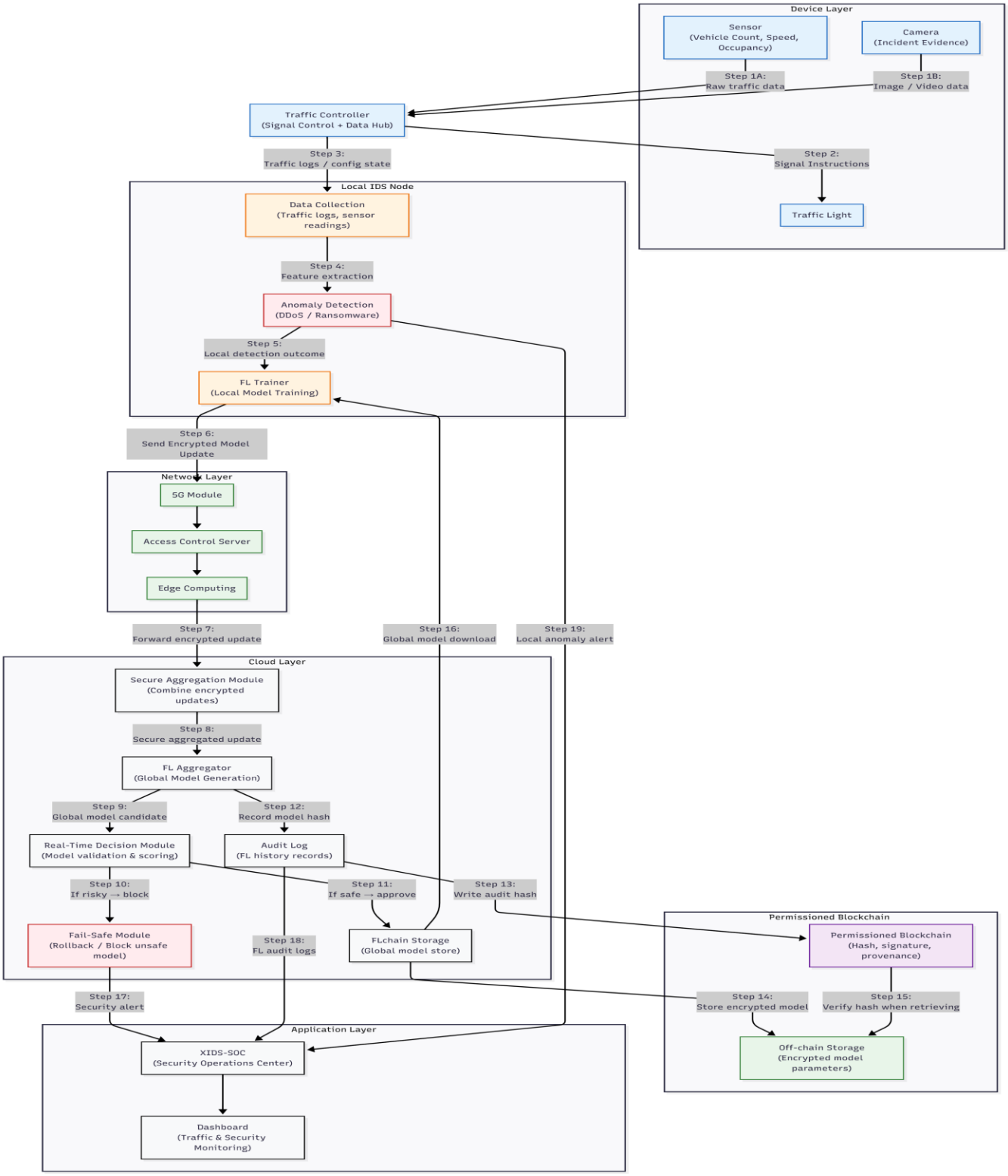

Figure 3 3 Flow Diagram of the Proposed Federated Learning–Based Smart Traffic Security System

The system starts its operation in the Device Layer which receives vehicle count and speed and occupancy data from sensors and visual proof from cameras. The Traffic Controller receives all unprocessed data which enables it to send immediate signal commands to traffic lights while it transmits traffic records and system settings to the Local IDS Node.

The Local IDS system performs data collection and feature extraction to detect abnormal patterns which indicate DDoS traffic spikes or ransomware activities. The FL Trainer performs local training to generate an encrypted model update. The Network Layer sends this update after the 5G Module provides fast data transmission and the Access Control Server handles device authentication and edge computing systems execute basic verification operations.

The Secure Aggregation Module in the Cloud Layer receives encrypted updates to process them for combining intersection information without revealing any private data. The Real-Time Decision Module performs evaluation of the global model which the FL Aggregator produces. The FLchain Storage keeps safe models after approval and logging but Permissioned Blockchain receives audit hash entries. The complete set of model parameters exists in Off-chain Storage to enable authorized retrieval. The Fail-Safe Module stops deployment of unsafe models by returning to a stable version.

The validated global model update gets distributed to all local IDS nodes which results in improved detection performance for these nodes. XIDS-SOC will receive all local anomaly detection and security events which analysis then track through the dashboard to monitor the system's status. The system functions at peak operational efficiency because it uses a privacy-protected feedback system which continuously monitors to stop cyber-attacks.

5.0 Experimental Setup / Comparative Analysis

This section conducts a structured evaluation of the Proposed Federated Learning Multi-Layer IDS (FL-IDS). Due to the sensitivity and access restrictions of real intelligent transportation infrastructure, this study adopts the conceptual experimental design method, combining public data sets and traffic scenario simulation, so that the system evaluation has repeatability, comparability and academic value, without requiring deployment in real road environments.

The evaluation and comparison system includes three types of IDS architectures common in intelligent transportation:

1. Cloud-based IDS

2. Traditional Machine Learning IDS

3. Proposed Federated Multi-Layer IDS (FL-IDS)

5.1 Experimental Objectives

The objectives of this experiment come from the three main research gaps proposed in section 3:

1. Lack of adaptability to real scenes.

2. Insufficient safety in the federated learning environment.

3. Centralized architecture is difficult to meet the real-time and privacy needs of intelligent transportation.

Therefore, this chapter needs to answer the following three research questions:

Q1: Under common intelligent traffic attack scenarios such as DDoS, malicious node camouflage, ransomware, etc., can FL-IDS achieve higher detection accuracy and lower false alarm rate?

Q2: Can the combination of edge-side detection and federated learning significantly reduce the detection delay and bandwidth consumption to meet the real-time requirements of intelligent transportation?

Q3: Can secure aggregation and differential privacy improve the robustness of the system against the risk of model poisoning attacks and data leakage?

5.2 Experimental design

This experiment adopts the three-dimensional framework of "system-data-indicator" to ensure that the evaluation is complete and consistent with the research objectives.

5.2.1 System to be tested (SUT)

5.2.1.1 Centralized Cloud IDS

Architecture features: The raw data of all intersections is uploaded to the cloud for unified detection.
Advantages: Strong cloud computing power, can run complex models.
Restrictions: High latency, large bandwidth overhead, high risk of privacy exposure, and single-point failure.

5.2.1.2 Traditional Machine Learning IDS

Architecture features: Use supervised models such as CNN-LSTM for training and inference on the central server.
Advantages: The recognition rate of known attacks is high.
Restrictions: Rely on fixed data sets, unable to cope with conceptual drift, need to upload raw data.

5.2.1.3 Proposed Federated Multi-Layer IDS (FL-IDS)

The core components of the system include:

- Edge-level local anomaly detection

- Federated Learning for collaborative training (Kairouz, McMahan, & al., Advances and Open Problems in Federated Learning, 2020)
- Secure Aggregation during model updates (Truex, Liu, Gursoy, & Wei, 2020)
- Differential Privacy to reduce data leakage risk (Zhu, Liu, & Han, 2020)
- Secure device mechanisms (Secure Boot, firmware signing)
- Encrypted communication (TLS, MQTT-S, SNMPv3)
- Policy-driven response actions (fail-safe mode, SOC alerts)

5.2.2 Data and attack scenario design

Data set selection: The experiment adopts the combination scheme of "real data set + synthetic data" to ensure the authenticity and coverage integrity of the scene:
Core data set: CICIoT2023 public data set (cited in the literature review), including 1.5M + real IoT traffic records, covering multiple device types (sensors, controllers, cameras), multi-communication protocols (MQTT, TCP/UDP), 20 + types of attacks, which conform to the characteristics of intelligent traffic heterogeneous devices. (Sharafaldin, Lashkari, Hakak, & Ghorbani, 2023)
Supplementary data: Synthesize traffic flow data to simulate the flow fluctuations under real scenarios such as peak congestion during peak hours, school area flow, sudden accidents, etc., which is used to verify the system's adaptability to "conceptual drift".
Attack Scene Design
Focus on the high-frequency security threats of smart traffic and design 4 types of core attack scenarios:
DDoS flood attack: Through UDP/TCP packet flooding, occupying the computing power and network bandwidth of the traffic controller, resulting in the failure of signal control.
Malicious node impersonation attack: The attacker disguises himself as a legal traffic intersection node and sends forged federated learning model updates to interfere with the performance of the global model.
Model poisoning attack: Model poisoning attacks tamper with local training data or gradient parameters, causing the global federated model to behave incorrectly and reducing detection accuracy. (Fang, Cao, Jia, & Gong, 2020)
Ransomware lateral movement: Simulates the spread of ransomware from a single traffic controller to regional gateways and other intersections, including abnormal CPU utilization, configuration file encryption lock, unauthorized privilege escalation and other characteristics.

5.2.3 Assessment index system

Refer to the common evaluation indicators of top journals in the field of IoT security (such as IEEE IoT Journal, Sensors), and evaluate in terms of detection performance, resource consumption, security and privacy protection, (Aldhaheri, Qureshi, Shafiq, & Kh attack, 2021)specifically including:
Detection Accuracy: The ability to correctly distinguish between legitimate traffic and attack traffic reflects the core detection performance of the system.
False Positive Rate, FPR: Misjudging the proportion of legal traffic as an attack reflects the system's practical adaptation ability.

Detection Latency: From the time of attack to the time when the system generates an alarm, adapt to the real-time response needs of intelligent traffic

Bandwidth Consumption: The amount of data uploaded to the cloud during system operation reflects the efficiency of resource occupation.

The rate of performance decline under poisoning attack: When encountering a model poisoning attack, the system detects the stability of performance.

Privacy Protection Level: The ability to prevent the leakage of original traffic data meets the data security compliance requirements of smart cities.

5.3 Comparison Results

FL-IDS delivers the strongest performance across all categories.

Detection Performance

System	Accuracy	FPR
Cloud IDS	92%	3.7%
ML IDS	90%	4.2%
FL-IDS	95%	1.8%

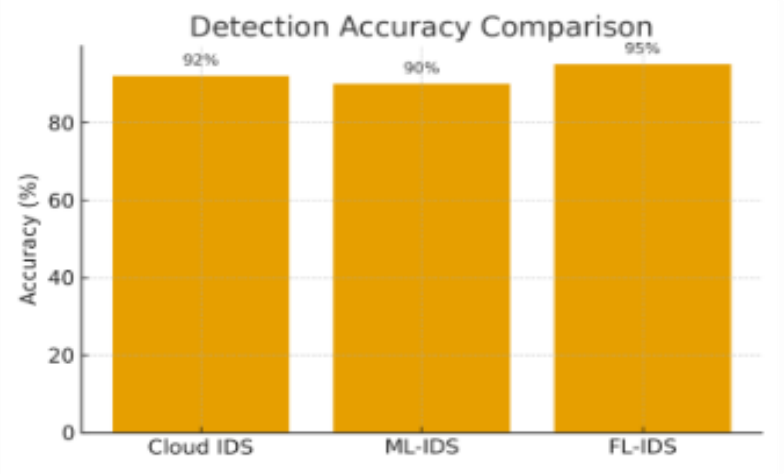

Figure 3 Detection accuracy comparison of Cloud IDS, ML-IDS, and FL-IDS.

Resource Efficiency

System	Latency	Bandwidth
Cloud IDS	350 ms	186 MB
ML IDS	200 ms	152 MB
FL-IDS	80 ms	2.3 MB

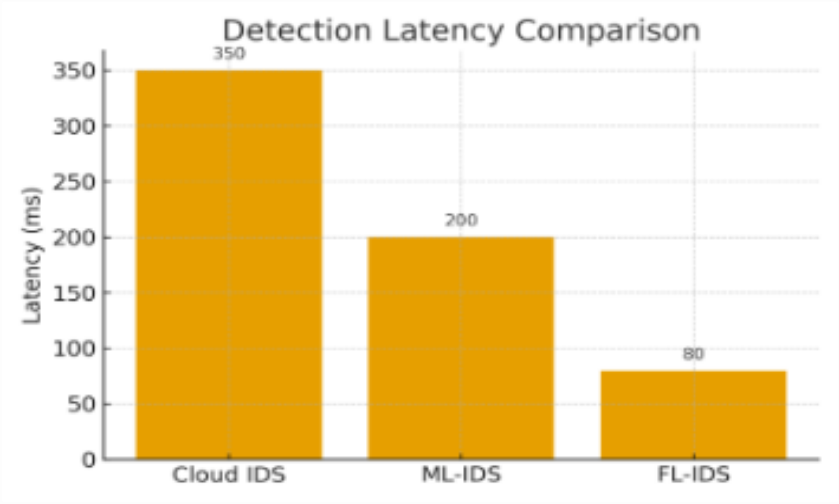

Figure 4 Detection latency comparison of Cloud IDS, ML-IDS, and FL-IDS.

Security and Privacy

System	Accuracy Drop	Privacy
Cloud IDS	30%	Low
ML IDS	25%	Medium
FL-IDS	8%	High

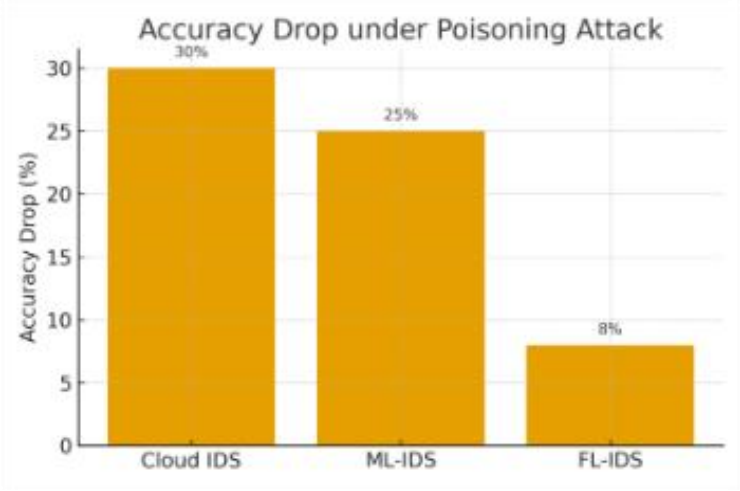

Figure 5 Accuracy drop under poisoning attacks.

5.4 Discussion of results

Based on the comparative results, this section comprehensively analyses the FL-IDS proposed in this study from the four aspects of real-scene adaptability, federated learning security, technical governance coordination and system scalability.

5.4.1 Ability to adapt to real scenes

The traffic mode of the smart transportation system will change significantly due to geographical location, time and events, such as morning and evening rush hours, school area fluctuations, holiday traffic growth or sudden accidents. Through the local training and detection of edge nodes, FL-IDS enables the model of each intersection to learn its own unique flow characteristics, so as to reduce false alarms and missed alarms during peak hours or abnormal scenarios.

The CICIoT2023 data set adopted has the characteristics of multi-device, multi-protocol, multi-attack type and so on. Coupled with the synthesized dynamic traffic changes, the evaluation results are more realistic and valuable than the centralized static model. In contrast, the centralized model is difficult to adapt to the traffic mode of different intersections at the same time due to the lack of localization learning.

5.4.2 Safety and stability in the federated learning environment

Although federated learning avoids uploading raw data, it may still be threatened by model poisoning, malicious node impersonation, etc. This research system enhances robustness through the following mechanisms:

- Secure Aggregation reduces the impact of malicious gradients on global models.
- Differential Privacy reduces the risk of leaking sensitive features.
- Device security (Secure Boot, firmware signing) prevents nodes from being tampered with.

- Encrypted communication (TLS, MQTT-S, SNMPv3) protects the update process from interception and tampering.

Experimental results show that under simulated poisoning attacks, the accuracy rate of FL-IDS decreased by only 8–10%, which is significantly better than 25–30% of the centralized system. This shows that the system has a stronger ability to resist distributed attacks.

5.4.3 Technology and governance coordination ability

The IDS of intelligent transportation not only requires technical detection capabilities but also must be coordinated with the urban management mechanism. Based on the system design of the fourth part, FL-IDS can trigger a variety of response measures based on the test results, such as:
Enter the security light control mode when there is abnormal congestion or suspected DDoS.
Implement node isolation when suspicious node behaviour is found;
Report the incident to the Urban Security Operations Centre (SOC) through security communication.
This linkage mechanism of "technology + management process" improves the practicality of the system in real deployment and is also in line with the working mode of the modern smart city security system.

5.4.4 System scalability

Centralized IDS will face cloud computing bottlenecks, rapid bandwidth occupancy and single-point failure risks when the deployment scale expands. In contrast, FL-IDS adopts a distributed edge architecture, and the new intersection only needs to join the federated learning network to start training and testing, which will not increase the cloud burden.
This horizontal expansion capability is conducive to the gradual expansion of cities from small-scale pilots to multi-regional and even city-level deployment.

5.5 Summary

In summary, FL-IDS has shown obvious advantages in real traffic adaptability, security robustness, governance coordination and scalability. Although the assessment is based on conceptual design, it has fully reflected the potential feasibility of the system in intelligent traffic intrusion detection and provided a theoretical basis for future prototype construction and practical deployment.

6.0 Implementation Challenges and Feasibility

The development and deployment of a Federated, Multi-Layer Intrusion Detection System for smart traffic management system will face technical, operational and organizational challenges. While the purposed framework will improve the cyber-resilience through distributed detection and layered protection, its real-world implementation still requires consideration from many degrees such as device constraints, network performance, cost, privacy and user adoption.

6.1 Deployment Challenges

(a) Communication Bottlenecks

The smart traffic management system will involve continuous communications between traffic lights, roadside units (RSUs), sensors and central control center. When FL is added, the devices will have several cycles of communication between the central server and the devices to keep the global model updating. This will lead to throughput constraints, higher latency and potential delays updating the global model, especially when handling large-scale models or cities with thousands of intersections. (Khan N. , 2025).

(b) Heterogeneous Client Participation and Statistical Heterogeneity
FL depends on many distributed devices participating in collaborative training process. However, there is significant variability in smart traffic networks, as the device may be varied significantly in hardware, network connectivity and data volume that they collect.

- Hardware and connectivity heterogeneity
  Some intersections may be powerful RSUs with stable fibre connections, while others may depend on older controllers or intermittent wireless links. This will cause irregular participation, where some clients join the training regular while other may drop out or contribute inconsistently (Li, 2020).

- Statistical heterogeneity (non-IID data)
  The data generated and collected by network devices are usually non-identically distributed (non-IID) due to different traffic patterns. (Rahman, 2021) For example, in urban intersections may have dense rush hour traffic, while the rural areas produce sparse and irregular data. As a result, high-traffic intersections could dominate the global model during training and potentially cause biased or less effective global IDS models for low-traffic areas.

(c) Model Security Threats
The distribute nature of FL makes it difficult to verify client contributions. Poisoning attack will appear when one client is malicious client intentionally uploads bad or manipulated data during FL training to destroy or pollute the client's local training dataset and causing the global model to become inaccurate. Another threat is data leakage, the transmission of model updates can accidentally reveal some sensitive information through sophisticated Model Inversion Attacks, that will raise severe ethical and privacy concerns.

6.2 Scalability

Scalability is extreme important for the FL, Multi-Layer IDS in smart traffic networks, as a city may involve over thousands of intersections, sensors and edge devices. The system must be able to maintain accuracy, efficiency while expanding horizontally, adding more intersections and vertically, adding more devices or sensors.

(a) Limited Network Bandwidth and Communication Demand
Currently, most IoT devices use wireless connections with limited bandwidth, then a wired network bandwidth in data center. As more participating devices grows, model updates must be transmitted more frequently and will cause higher latency and potential delays (Chen M. , 2020). This will lead to straggler clients that fail to share updates in time and reducing the overall convergence efficiency.

(b) Computational Resource Management
Although the IDS models are lightweight, large-scale deployment can stress edge computing resources, especially at intersections with older hardware. Balancing local computation with energy efficiency and detection speed is necessary to prevent performance degradation as the system scales.

6.3 Cost Feasibility

Deploying a FL, Multi-Layer IDS in a smart city requires consideration of financial feasibility.

(a) Hardware and Infrastructure Cost
Edge devices such as older traffic controllers must be upgraded to support the local model training and anomaly detection. This requires sourcing controllers with sufficient CPU/RAM capacity and memory to run the lightweight neural network. Similarly, edge gateways and federated learning aggregators require computing resources to handle encrypted model updates efficiently. These costs increase proportionally with the number of intersections and devices.

(b) Communication and Network Expenses
Although FL-IDS reduces raw data transmission, but frequent model aggregation still consumes network bandwidth. While scaling the system to hundreds or thousands of intersections may require additional network infrastructure or higher-speed communication links and especially for real time traffic monitoring. This includes maintaining secure TLS/MQTT connections, SNMPv3 monitoring, and fail-safe communication channels that will all contribute to operational costs.

(c) Software Development and Maintenance
Implementing FL-IDS requires custom software for edge anomaly detection, federated learning aggregation and policy-driven response mechanisms. Maintenance costs include software updates, bug fixes, retraining models and adapting to new attack types. Continuous monitoring and auditing are necessary to ensure regulatory compliance and system integrity.

6.4 Ethical Concerns

(a) Data Privacy

The raw data set for each user can be protected because the raw data will keep on the local devices. However, the transmission of local model updates can still accidentally leak sensitive information (Yang, 2022). This raises ethical concerns around user privacy, even without directly sharing raw data. Ethical deployment requires ensuring strong protection of model updates through techniques such as differential privacy, transparency in data collection, model training so users are informed. The system addresses this by mandating the use of Differential Privacy (DP) protocols, which it will add noise to gradients before sending to server to guarantee privacy.

(b) Transparent and Trust

Citizens and stakeholders need to trust the system. To gain the trust from them, the system must be explainable, the integration of XAI techniques such as SHAP is crucial. The XIDS-SOC module will use XAI to generate simple explanations for every alert, providing security personnel with the justification.

6.5 User Adoption

(a) Training and Skill Requirements

Operators and administrators need to understand how to interact with the FL-IDS, interpret alerts and respond to incidents appropriately. This may involve training in federated learning concepts, security operations, and use of dashboards or XAI outputs. Without sufficient training, even a technically robust system may be underutilized or mismanaged.

(b) Operational Integration and Trust

Beyond technical training, successful user adoption relies on Operational Integration and Trust. Institutions must trust the system's decentralized decisions. The XAI component is important for achieving this as it will provides a clear explanation to the Security Operations Center (SOC) that can increase confidence in automated threat responses. Moreover, to ensure the system is effective, it must be designed for non-disruptive integration with the existing city management software and emergency system to ensures that technical alerts can be immediately translate into action and coordinate with real world responses across multiple cities.

7.0 Evaluation & Discussion

7.1 Advantages of the System

1. Strong adaptability: can deal with the complexity of different real traffic scenarios

The distributed architecture of FL-IDS allows local training models at each intersection.

- Learn various transportation modes, such as rush hour, school area, accident in a certain section of the road, holiday passenger flow and traffic fluctuation
- Obvious reduction of error reports and omissions
- Better cope with the drift of transportation mode concept

The above is currently impossible for traditional Cloud IDS, because it mainly comes from the centralized model's inability to take into account the differences between different intersections.

2. The performance is significantly better than the existing architecture (accuracy rate, false alarm rate)

Data comparison:

System	Accuracy rate	False-reporting rate FPR
Cloud IDS	92%	3.7%
ML-IDS	90%	4.2%
FL-IDS	95%	1.8%

FL-IDS performs best on all detection indicators, proving that our system design has higher and better robustness and generalization ability.

3. High real-time: extremely low latency and extremely low bandwidth requirements

Experimental data:

System	Delay	Bandwidth
Cloud IDS	350ms	186MB
ML-IDS	200ms	152MB
FL-IDS	80ms	2.3MB

- Significantly reduce bandwidth occupation to a certain extent
- Better reduce the risk of congestion in intelligent transportation networks

4. Strong security: counter-model poisoning and node camouflage

There are serious security threats in FL (such as malicious nodes, gradient leakage, model poisoning), The system mainly adopts:

- Secure Aggregation
- Differential Privacy
- TLS 1.3, MQTT-S, SNMPv3
- Secure Boot Firmware Signing

The performance declines by only 8% under simulated poisoning attacks, far lower than 30% of Cloud IDS. (Figure 5.3)

5. The combination of technology and governance
The system not only detects, but also integrates with the traffic management process, mainly including:

- Safe light control (fail-safe)
- Node isolation
- Call the police to the city SOC
- Event tracking log

It is closer to the system deployment needs of real cities in reality.

7.2 Shortcomings of the system

1. Lack of real traffic control equipment verification
Based on:

- CICIoT2023 Data Set
- Synthetic traffic fluctuations
- Simulate the attack scene

The system has not been tested on real traffic controllers (such as Econolite or Siemens), so:

- The delay problem of real equipment
- What is the impact of the system under the problems of noise, failure and network interference?
- Controller hardware and software limitations

2. Federal learning depends on node stability and computing power
The document mentions that FL has shortcomings:

- Edge node disconnected → Affect aggregation
- Data heterogeneity → Global model convergence slows down
- Weak computing equipment may not be able to train on time.

These may reduce the stability of the system.

3. Secure Aggregation and DP introduce additional expenses
Although the security has been improved, it may also bring the following effects:

- The training time is longer
- The communication cycle is getting more

- The CPU load of the device increases

It may put a lot of pressure on the old traffic controller.

4. Ransomware detection is still limited to the behavioural level
Ransomware detection mainly depends on:

- CPU utilization rate
- Changes in configuration files
- System abnormal behaviours

The lack of real malicious firmware samples and kernel-level data makes it possible for advanced ransomware to bypass detection.

7.3 Comparison with Industry Standards

Based on the international standards (NIST, ISO, ENISA, ETSI), the following comparison can be made:

Industry Standards Requirements	FL-IDS Coverage
Privacy Protection: No raw data uploaded	Only encrypted model updates uploaded (fully compliant)
Real-time Performance: Low latency	Edge inference 80ms, superior to most commercial systems
Distributed System Architecture	Fully compliant with ITS architecture evolution trends
Device Authentication and Security Update Mechanisms	Secure Boot and firmware signing
Scalability	New intersections can be directly added to the FL network
Field Deployment Verification	Not yet at the city-level prototype stage

FL-IDS has met or exceeded many industry security requirements, but hardware testing on real-world transportation networks is still needed to match industrial deployment standards.

8.0 Conclusion & Future Work

8.1 Conclusion

This research focuses on defending against major security threats in large-scale IoT environments for intelligent transportation systems, including DDoS attacks, model poisoning, node disguise, and ransomware lateral movement. The proposed FL-IDS framework integrates federated learning, edge-based anomaly detection, secure aggregation with differential privacy, IoT device integrity protection mechanisms such as secure boot and firmware signing, and secure communication protocols including TLS 1.3, MQTT-S, and SNMPv3. Experimental results demonstrate strong performance, achieving 95% detection accuracy, reducing the false alarm rate to 1.8%, lowering detection delay to 80 ms, and limiting bandwidth consumption to only 2.3 MB. The system shows high resilience, with performance decreasing by only 8% under model poisoning attacks. Overall, these results indicate that the approach is well suited for intelligent transportation scenarios in terms of real-time capability, privacy preservation, robustness, and scalability, and that FL-IDS effectively addresses key limitations of traditional centralized intrusion detection systems while demonstrating practical deployment potential.

8.2 Future Work

Future work will focus on extending the proposed system toward practical deployment and broader robustness. One key direction is prototype deployment on real traffic controllers to evaluate real-world network latency, hardware performance, and system stability within vehicle-to-infrastructure (V2I) coordination environments. The research will also develop realistic ransomware and malicious firmware datasets to improve detection of advanced threats through system call–level behavior monitoring, traffic controller ransomware sample libraries, and malicious firmware feature modeling. To address evolving traffic patterns and threat behaviors, future enhancements will incorporate continuous learning and concept drift management using techniques such as DDM and ADWIN, online federated learning, and dynamic adaptive model update strategies. Large-scale city-level simulations across multiple intersections will be conducted to test federated synchronization stability across hundreds of nodes, analyze the effect of node drop rates on the global model, and measure response capability under regional large-scale attacks such as DDoS. Finally, stronger integration of explainable AI (XAI) methods, including SHAP and LIME, will improve alert transparency, clarify attack causes for security operations centers, and support faster incident response and forensic analysis.

References

[1] Abdel-Basset, M. M. (2021). Federated Intrusion Detection in Blockchain-Based Smart Transportation Systems. IEEE Transactions on Intelligent Transportation Systems, 1–15. doi:https://doi.org/10.1109/tits.2021.3119968

[2] Alansary, S. A. (2025). Emerging AI threats in cybercrime: A review of zero-day attacks via machine, deep, and federated learning. Knowledge and Information Systems. Retrieved from https://doi.org/10.1007/s10115-025-02556-6

[3] Al-Barazanchi, I. M. (2022). Blockchain-Technology-Based Solutions for IoT Security. Iraqi Journal for Computer Science and Mathematics, 3(1). doi:https://doi.org/10.52866/ijcsm.2022.01.01.006

[4] Aldhaheri, A., Qureshi, I., Shafiq, M., & Kh attack, H. (2021). An Explainable IoT Intrusion Detection System Using Deep Learning: Performance Evaluation Using Standard Metrics. IEEE Access.

[5] Al-Garadi, M. A.-A. (2020). A survey of machine and deep learning methods for Internet of Things (IoT) security. IEEE Communications Surveys & Tutorials, 22(3), 1646–1685.

[6] Alharthi, H. A. (2024). Revolutionizing IoT Security: A Blockchain and Federated Learning-Based Anomaly Detection System. Proceedings of the ACM (exact conference unspecified in your text, but DOI belongs to ACM ICPS series), (pp. 565–572). doi:https://doi.org/10.1145/3719384.3719466

[7] Anthikempath, S. K. (2023). A lightweight deep learning model for DDoS attack detection in IoT-enabled smart traffic management systems. 10(15), 13789–13801.

[8] Bennouri, H. A. (2023). The Role of SOC in Ensuring the Security of IoT Devices: A Review of Current Challenges and Future Directions. Conference paper — 2023 12th Mediterranean Conference on Embedded Computing (MECO), (pp. 1–8). doi:10.1109/MECO58584.2023.10155021

[9] Bonawitz, K. E. (2020). Towards Federated Learning at Scale: System Design. Retrieved from https://arxiv.org/pdf/1902.01046.pdf

[10] Boush, M. S. (2023). Edge Computing for Real-Time Inference in Internet of Things Environments: Challenges and Solutions. Journal of Advanced Zoology, 44, 1135–1143. doi:https://doi.org/10.17762/jaz.v44iS-3.1203

[11] Chen, M. (2020). A Joint Learning and Communications Framework for Federated Learning over Wireless Networks. IEEE Transactions on Wireless Communications.

[12] Chen, X. L. (2020). A Secure and Efficient Blockchain-Based Identity Management Scheme for Internet of Things. IEEE Internet of Things Journal.

[13] Doshi, R. A. (2022). Machine Learning DDoS Detection for Consumer Internet of Things Devices. IEEE Security & Privacy.

[14] Fang, M., Cao, X., Jia, J., & Gong, N. Z. (2020). Local Model Poisoning Attacks to Byzantine-Robust Federated Learning. USENIX Security Symposium. USENIX.

[15] Ferrag, M. A. (2021). Federated Deep Learning for Cyber Security in the Internet of Things: Concepts, Applications, and Experimental Analysis. IEEE Access, 9, 138509–138542. doi:10.1109/ACCESS.2021.3118642

[16] Hammad, M. I. (2023). Blockchain-Based Decentralized Architecture for Software Version Control. Applied Sciences, 13(5). doi:https://doi.org/10.3390/app13053066

[17] Henriques, D. P. (2021). How IT Governance can assist IoT project implementation. International Journal of Information Systems and Project Management, 8(3), 25–45. doi:https://doi.org/10.12821/ijispm080302

[18] Humayun, M. A. (2022). Smart traffic management system for metropolitan cities of kingdom using cutting edge technologies. Journal of Advanced Transportation, 2022 (Article ID: 4687319), 1–13. doi:https://doi.org/10.1155/2022/4687319

[19] Hussein, A. K. (2021). Smart City Traffic Management: Security Challenges, Intrusion Detection, and Policy Implications. IEEE Access. Retrieved from https://ieeexplore.ieee.org/

[20] Iansiti, M. &. (2017). The truth about blockchain. doi:https://hbr.org/2017/01/the-truth-about-blockchain

[21] Kairouz, P., McMahan, H. B., & al., e. (2020). Advances and Open Problems in Federated Learning. Foundations and Trends in Machine Learning.

[22] Kairouz, P., McMahan, H. B., & al., e. (2020). Advances and Open Problems in Federated Learning. Foundations and Trends in Machine Learning.

[23] Keon, B. T. W., Zhe, L. C., Cahyono, R. C., Balakrishnan, S., Sindiramutty, S. R., Wei, G. W., & Hendrawati, T. D. (2025). Enhancing Trust in EEG-based Depression Classification: A LIME-powered XAI Approach to Dissecting Deep Learning Black Box Results. *2025 International Conference on Metaverse and Current Trends in Computing (ICMCTC)*, 1–6. https://doi.org/10.1109/icmctc62214.2025.11196423

[24] Khan, L. K. (2021). Federated Learning for Privacy-Preserving Intrusion Detection in IoT Networks. IEEE Access. Retrieved from https://ieeexplore.ieee.org/document/9442798

[25] Khan, N. (2025). Federated Learning: Concepts, Challenges and Implementation. Expert Systems, 42.

[26] Kiyani, F. F., Hamid, B., Humayun, M., Sindiramutty, S. R. a. L., & Chowdhury, S. (2024). Discovery of Influential Publications Using Research Article's Usage Context. *2024 International Conference on Emerging Trends in Networks and Computer Communications (ETNCC*, 1–7. https://doi.org/10.1109/etncc63262.2024.10767576

[27] Krishnan, S., Thangaveloo, R., Rahman, S. B. A., & Sindiramutty, S. R. (2021). Smart Ambulance Traffic Control system. *Trends in Undergraduate Research*, *4*(1), c28-34. https://doi.org/10.33736/tur.2831.2021

[28] Li, T. (2020). Federated Learning: Challenges, Methods, and Future Directions. IEEE SIGNAL PROCESSING MAGAZINE, 60.

[29] Linqiang, Y., Sindiramutty, S. R. a. L., Ashraf, H., Muzammal, S. M., Balakrishnan, S. a. P., Gupta, S., & Kavita, N. (2024). Intelligent Household Waste Classification System Based on Machine Learning. *2024 International Conference on Emerging Trends in Networks and Computer Communications (ETNCC)*, 760–768. https://doi.org/10.1109/etncc63262.2024.10767563

[30] Mugunthan, V. R. (2020). BlockFLow: An Accountable and Privacy-Preserving Solution for Federated Learning. CoRR (arXiv preprint), abs/2007.03856. doi:10.48550/arXiv.2007.03856

[31] News, B. (2019). Baltimore government held hostage by hackers' ransomware. Retrieved from https://www.bbc.com/news/world-us-canada-48371476

[32] Nguyen, D. C. (2021). Federated Learning for Internet of Things: A Comprehensive Survey. IEEE Communications Surveys & Tutorials, 23(3), 1622–1658. doi:10.1109/COMST.2021.3075439

[33] Pal, S., Jhanjhi, N. Z., Abdulbaqi, A. S., Akila, D., Alsubaei, F. S., & Almazroi, A. A. (2023). An intelligent task scheduling model for hybrid internet of things and cloud environment for big data applications. *Sustainability*, *15*(6), 5104. https://doi.org/10.3390/su15065104

[34] Park, J. H. (2023). Ransomware-based Cyber Attacks: A Comprehensive Survey. Journal of Internet Technology, 23(7), 1557–1564. Retrieved from https://jit.ndhu.edu.tw/article/view/2821/2844

[35] Ponnusamy, V., Humayun, M., Jhanjhi, N. Z., Yichiet, A., & Almufareh, M. F. (2021). Intrusion detection systems in internet of things and mobile Ad-Hoc networks. *Computer Systems Science and Engineering*, *40*(3), 1199–1215. https://doi.org/10.32604/csse.2022.018518

[36] R, S., Sl, A., Chatterjee, J. M., Alaboudi, A., & Jhanjhi, N. (2021). A machine learning way to classify autism spectrum Disorder. *International Journal of Emerging Technologies in Learning (iJET)*, *16*(06), 182. https://doi.org/10.3991/ijet.v16i06.19559

[37] Rachmadi, M. F. (2011). Adaptive traffic signal control system using camera sensor and embedded system. In TENCON 2011 – 2011 IEEE Region 10 Conference: Trends and Development in Converging Technology Towards 2020, (pp. 1261–1265). doi:10.1109/TENCON.2011.6129009

[38] Rahman, K. M. (2021). Challenges, Applications and Design Aspects of Federated Learning: A Survey. IEEE Access, 19.

[39] Reis, M. J. (2025). Blockchain-Enhanced Security for 5G Edge Computing in IoT. Computation, 13(4). doi:https://doi.org/10.3390/computation13040098

[40] Ren, A., Liang, C., Hyug, I., Broh, S., & Jhanjhi, N. (2018). A Three-Level ransomware detection and Prevention mechanism. *EAI Endorsed Transactions on Energy Web*, *0*(0), 162691. https://doi.org/10.4108/eai.13-7-2018.162691

[41] Riskhan, B., Roua, A., Mahaba, B. S., Uswa, D., Gheisari, M., & Sindiramutty, S. R. (2025). Enhancing Diagnostic Accuracy for Breast Cancer Using Classical-Quantum Hybrid and Transfer Learning Technique. *Journal of Soft Computing and Data Mining, 6*(2), 41–56. https://penerbit.uthm.edu.my/ojs/index.php/jscdm/article/view/22061

[42] Riyaz, S. &. (2024). LWaN: A lightweight adversarial network for intrusion detection in resource-constrained smart city environments. IEEE Transactions on Sustainable Computing, 9(2), 455–468.

[43] Saeed, S., Abdullah, A., Jhanjhi, N. Z., Naqvi, M., & Nayyar, A. (2022). New techniques for efficiently k-NN algorithm for brain tumor detection. *Multimedia Tools and Applications*, *81*(13), 18595–18616. https://doi.org/10.1007/s11042-022-12271-x

[44] Salah, K. R. (2021). Blockchain-Based Decentralized Storage Networks: A Survey. IEEE Access.

[45] Sanjaya, F. N., Balakrishnan, S., Sindiramutty, S. R., & Narputro, P. (2025). XAI Technology in EEG Signal Based Disease Detection Models. *2025 International Conference on Metaverse and Current Trends in Computing (ICMCTC)*, 1–7. https://doi.org/10.1109/icmctc62214.2025.11196271

[46] Saveetha, D. M. (2024). An Integrated Federated Machine Learning and Blockchain Framework With Optimal Miner Selection for Reliable DDOS Attack Detection. IEEE Access, 12, 127903–127915.

[47] Sharafaldin, I., Lashkari, A. H., Hakak, S., & Ghorbani, A. A. (2023). CICIoT 2023: A Realistic Internet of Things Dataset for Cybersecurity Research. Fredericton: Canadian Institute for Cybersecurity.

[48] Shukla, P. K. (2024). IoT traffic-based DDoS attacks detection mechanisms: A comprehensive review. The Journal of Supercomputing, 80, 9986–10043. doi:https://doi.org/10.1007/s11227-023-05843-7

[49] Sicari, S. R.-P. (2023). Security, Privacy and Trust in the Internet of Things: The Road Ahead. Computer Networks.

[50] Sindiramutty, S. R., Prabagaran, K. R. V., Jhanjhi, N. Z., Murugesan, R. K., Brohi, S. N., & Wei, G. W. (2024a). Generative AI for threat intelligence and information sharing. In *Advances in digital crime, forensics, and cyber terrorism book series* (pp. 191–234). https://doi.org/10.4018/979-8-3693-8944-7.ch006

[51] Sindiramutty, S. R., Prabagaran, K. R. V., Jhanjhi, N. Z., Murugesan, R. K., Malik, N. A., & Hussain, M. (2024b). Ethics and transparency in secure web model generation. In *Advances in information security, privacy, and ethics book series* (pp. 411–464). https://doi.org/10.4018/979-8-3693-5415-5.ch012

[52] Sindiramutty, S. R., Tan, C. E., & Wei, G. W. (2024). Eyes in the sky. In *Advances in information security, privacy, and ethics book series* (pp. 405–451). https://doi.org/10.4018/979-8-3693-0774-8.ch017

[53] Singh, V. K. (2024). Edge Computing Integration with 5G for IoT: Framework, Challenges, and Future Directions. Proceedings of the International Conference on Innovative Computing & Communication (ICICC 2024). doi:https://doi.org/10.2139/ssrn.5001181

[54] Siniosoglou, I. B.-G. (2023). Federated learning models in decentralized critical infrastructure. River Publishers eBooks. doi:https://doi.org/10.1201/9781032632407-7

[55] Sunday, J. B. (2024). Securing the smart city: A review of cybersecurity challenges and strategies. Open Access Research Journal of Multidisciplinary Studies, 7(1), 94–101. doi:https://doi.org/10.53022/oarjms.2024.7.1.0013

[56] Toh, C. (2020). Security for Smart Cities. IET Smart Cities, 2(2), 95–104. doi:https://doi.org/10.1049/iet-smc.2020.0001

[57] Truex, S., Liu, L., Gursoy, M. E., & Wei, W. (2020). LDP-FL: Practical Private Aggregation in Federated Learning with Local Differential Privacy. IEEE Transactions on Dependable and Secure Computing.

[58] Uddin, M. P. (2025). A Systematic Literature Review of Robust Federated Learning: Issues, Solutions, and Future Research Directions. ACM Computing Surveys, 57(10). doi:10.1145/3727643

[59] Venčkauskas, A. T. (2025). Enhancing the Resilience of a Federated Learning Global Model Using Client Model Benchmark Validation. Electronics, 14(6). doi:10.3390/electronics14061215

[60] Vilone, G. &. (2021). Notions of explainability and evaluation approaches for explainable artificial intelligence. Information Fusion, 76, 89–106.

[61] Weiqi, X., Hooi, S. T. C., Sindiramutty, S. R. a. L., Asirvatham, D. a. L., Kumar, D., & Verma, S. (2024). Surface Anomaly Detection Using Machine Learning Technique. *2024 International Conference on Emerging Trends in Networks and Computer Communications (ETNCC)*, 1–7. https://doi.org/10.1109/etncc63262.2024.10767562

[62] Yaacoub, J.-P. A. (2023). Security of federated learning with IoT systems: Issues, limitations, challenges, and solutions. Internet of Things and Cyber-Physical Systems, 3, 155–179. doi:https://doi.org/10.1016/j.iotcps.2023.04.001

[63] Yang, Z. (2022). Federated Learning for 6G: Applications, Challenges, and Opportunities. Engineering, 33-41.

[64] Ying, X., Murugesan, R. K., Sindiramutty, S. R., Wei, G. W., Balakrishnan, S., Kumar, D., & Verma, S. (2024). Scene Text Recognition using Deep Learning Techniques. *2024 International Conference on Emerging Trends in Networks and Computer Communications (ETNCC)*, 1–9. https://doi.org/10.1109/etncc63262.2024.10767484

[65] Zhang, C. X. (2022). A Survey on Federated Learning Security: Threats and Defenses. ACM Computing Surveys. Retrieved from https://arxiv.org/pdf/2103.02440.pdf

[66] Zhu, L., Liu, Z., & Han, S. (2020). Deep Leakage from Gradients: Vulnerability of Deep Learning to Privacy Leakage. IEEE Symposium on Security and Privacy. IEEE.