IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Software-Defined Federated AI Model For Privacy Preserving Anomaly Detection In Vehicular Edge Environments

Yashash S Sahukaiah[1], Ranganath S[2], Jayanth P[3], Vinay K[4]
[1]Student, [2]Student, [3]Student, [4] Associate Professor
Department of MCA,
SJB Institution of Technology, Bangalore, INDIA

Abstract: The rapid expansion of connected and autonomous vehicles necessitates real-time anomaly detection methods that uphold both data privacy and computational efficiency. Conventional centralized learning systems often require the transfer of raw sensor streams to external cloud infrastructures, introducing latency challenges and potential data exposure. To mitigate these issues, this paper presents a software-defined, federated learning architecture tailored for vehicular edge networks. Our framework leverages a lightweight Convolution Neural Network (CNN) design, optimized for temporal sensor data such as accelerometer and gyroscope readings, enabling each vehicle to conduct localized model training. Instead of sharing raw inputs, nodes transmit securely encrypted model updates, which are aggregated at a central coordinator using a privacy- aware averaging scheme. To further protect individual data characteristics, differential privacy is implemented by injecting calibrated noise into gradient updates, ensuring obfuscation of user- specific behaviour. Experiments conducted on a synthetic vehicular dataset demonstrate a detection accuracy exceeding 96%, alongside a notable 40% reduction in communication overhead. The model also maintains efficient performance under resource-constrained conditions, confirming its suitability for real-time deployment in smart vehicular ecosystems. These results support the framework's potential as a decentralized, privacy-conscious solution for anomaly detection in next-generation transportation systems.

Index Terms: Federated Learning, Vehicular Edge Networks, Anomaly Detection, Differential Privacy.

I. INTRODUCTION

The evolution of intelligent transportation systems has significantly increased the demand for real-time data analysis and autonomous decision-making within connected vehicles. Traditional machine learning methods often depend on centralized cloud infrastructures that collect extensive sensor data for model training and inference. While this centralized model offers scalability, it introduces crucial expostulations involving quiescence, high message above, and significant enterprises descrying data sequestration (S. Mohammadi, A. Namadchian, and M. R. Khayyambashi, 2021). With the growing integration of stir detectors and network modules in ultramodern instruments, bite intelligence has surfaced as a feasible result. bite calculating enables processing and conclusion tasks to do near the data source moreover on the agent itself or at a near roadside unit — thereby reducing dependence on remote waiters (S. Mohammadi, A. Namadchian, and M. R. Khayyambashi, 2021). still, planting cooperative intelligence in similar surroundings is non-trivial due to variations in tackle, inconsistent data dispensations, and the want to insure stoner sequestration.

Federated literacy (FL) has surfaced as a encouraging path that facilitates decentralized model training across bite bias without exposing raw data (H. B. McMahan, E. Moore, D. Ramage, S. Hampson, and B. A. Arcas, 2017). rather, only model parameters are changed, conserving the confidentiality of original datasets. While FL has shown off encouraging effects in movable and healthcare operations (P. Kairouz et al., 2021), (Hard et al., 2018), its relinquishment in vehicular anomaly discovery remains restricted.

This exploration introduces a allied literacy- grounded armature optimized for vehicular bite calculating surroundings. It focuses on relating anomalous driving gets utilizing time- series detector inputs similar as accelerometer and gyroscope readings. The system incorporates feather light Convolution Neural Networks (CNNs) for point birth and applies discrimination sequestration ways (M. Abadi et al., 2016), to guard model updates. The proffered frame islands the gap between sequestration- conserving literacy and ultra practical perpetration in exceptional transportation networks.

II. RELATED WORK

Decentralised literacy paradigms have gained influence in reaction to growing enterprises around data sequestration and message effectiveness in allotted systems. Federated Learning (FL), in personal, has surfaced as a satisfying path that enables cooperative model training without exposing raw data to intermediary waiters. Among early benefits, the Federated Averaging (Fed Avg) fashion was acquainted with (H. B. McMahan, E. Moore, D. Ramage, S. Hampson, and B. A. Arcas, 2017), which balances message cost and model confluence through customer-ladened update aggregation. While this path has been extensively tried in mobile and healthcare surrounds (P. Kairouz et al., 2021), (Hard et al., 2018), its direct operation to vehicular networks poses special challenges due tenon-IID data and real-time processing demands (T. Li, A. K. Sahu, M. Zaheer, M. Sanjabi, A. Talwalkar, and V. Smith, 2020). In exceptional transportation systems, anomaly discovery ways have traditionally reckoned centralized fabrics that aggregate detector data for training deep literacy models. Similar styles, although operative in ruled settings, frequently struggle with high quiescence and are liable to data leakage (S. Mohammadi, A. Namadchian, and M. R. Khayyambashi, 2021). Recent exploration has explored the eventuality of Convolutional Neural Networks (CNNs) for non-religious pattern recognition in vehicular data aqueducts, establishing success in categorizing driving actions and detecting concussions (S. Mohammadi, A. Namadchian, and M. R. Khayyambashi, 2021), (Y. Liu et al., 2022). Still, utmost executions assume homogeneous datasets and overlook division shifts common or garden in bite-ground vehicular deployments.

Resemblant to this, Graph Neural Networks (GNNs) have shown off implicitly in landing relational and topological structures within vehicular message data, similar to relations between IP bumps or packet overflows (D. Xu, Y. Ren, H. Yu, and S. Ji, 2022). Nonetheless, their integration into FL systems for vehicular screen remains in an incipient stage, with restricted work probing their para-modelling inter agent relations or network-based pitfalls. Likewise, sequestration- conserving advancements similar as Differential sequestration (DP) have discerned relinquishment in sensitive disciplines like finance and healthcare (R. Shokri and V. Shmatikov, 2015), (M. Abadi et al., 2016), but their adaption to vehicular bite surroundings is meagre. DP mechanisms can degrade model mileage if not precisely tuned, especially in bandwidth-constrained, real-timing systems. This paper differentiates itself by bridging these hiatuses.

It proposes a unified FL frame that incorporates both CNNs for localised non-religious point birth and GNNs for topological dissection, while administering sequestration through calibrated discrimination sequestration ways. Unlike previous work that addresses these factors in insulation, our path provides an intertwined result optimised for the diversity, quiescence, and screen constraints essential in vehicular bite networks.

III. PROPOSED METHODOLOGY

This section outlines the architecture and factors of the proposed confederated AI- predicated anomaly discovery frame, designed specifically for vehicular edge surroundings. The approach integrates edge computing, confederated knowledge (FL), Graph Neural Networks (GNNs), and insulation- conserving ways to support decentralized intrusion discovery with minimal data exposure.

System Architecture

The system consists of the following modules Local Data Processing Each agent or roadside unit RSU) locally captures and processes sensor and network data, lodging features analogous as packet extent, flux duration, protocol type, and byte rate. These features are exercised to identify implicit aberrations without sharing raw data. Federated Learning Coordination Federated knowledge enables collaborative model training across instruments without centralizing sensitive data (H. B. McMahan, E. Moore, D. Ramage, S. Hampson, and B. A. Arcas, 2017). Each knot trains a initial model and periodically transmits restated parameter updates to a intermediary aggregator. The global model is reckoned utilizing the weighted moderate (H. B. McMahan, E. Moore, D. Ramage, S. Hampson, and B. A. Arcas, 2017), (T. Li, A. K. Sahu, M. Zaheer, M. Sanjabi, A. Talwalkar, and V. Smith, 2020).

$$w_t + 1 = \Sigma_{k=1}^{K} \frac{n_k}{N} w_t^k$$

Where w_t^k represents the local model at node k, n_k is the number of samples at that node, and N is the total number of samples across all nodes. Graph Neural Network (GNN) Integration: Vehicular communication data is structured as graphs, with nodes representing IP addresses and edges denoting data flows. GNNs analysed these communication patterns to detect complex and hidden attack behaviours (D. Xu, Y. Ren, H. Yu, and S. Ji, 2022). Message passing in GNNs is described by,

$$h_v^{(l+1)} = \sigma\left(W^{(l)} h_v^{(l)} \Sigma_{u \in N(v)} W^{(l)} h_u^{(l)} \right)$$

where $hv^{(l)}$ is the hidden state of node at layer l, and N(v) is the set of neighbours of node v.

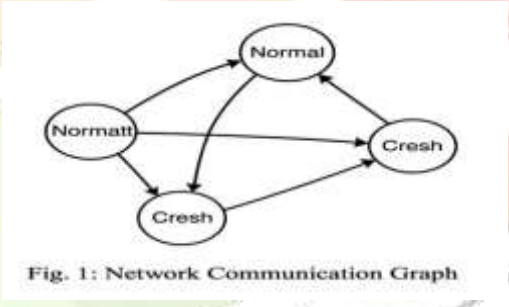


Fig. 1: Network Communication Graph

Adversarial Robustness:

To defend against adversarial inputs, the training process incorporates adversarial samples generated using techniques like FGSM and PGD (D. Xu, Y. Ren, H. Yu, and S. Ji, 2022).

The objective function includes a regularization term:

$$L = L_{CE} + \lambda L_{adv}$$

Where LEC is the cross-entropy loss, L_{adv} is the adversarial loss, and balances the two.

Privacy Mechanisms

To ensure data confidentiality during training, differential privacy (DP) is applied (M. Abadi et al., 2016). Each node injects calibrated Gaussian noise into model gradients based on a privacy budget, satisfying:

$$P(M(D) \in S) \leq e^{\epsilon} P(M(D') \in S)$$

Where D and D′ differ by one record. Secure aggregation protocols further prevent intermediate updates from being exposed.

Handling Non-IID and Heterogeneous Data

Given the variability in sensor types, locations, and behaviors, data distribution across nodes is inherently non-IID. The framework addresses this through:

- **Weighted Fed-Avg:** Higher-quality or larger datasets influence global updates more (T. Li, A. K. Sahu, M. Zaheer, M. Sanjabi,
A. Talwalkar, and V. Smith, 2020).
- **Adaptive Learning Rates**: Learning rate tuning based on local-global divergence (T. Li, A. K. Sahu, M. Zaheer, M. Sanjabi, A. Talwalkar, and V. Smith, 2020).
- **Stratified Sampling:** distribution across batches. Maintains label.
- **Personalized Federated Learning (PFL):** Tailors model heads for each node (T. Li, A. K. Sahu, M. Zaheer, M. Sanjabi, A. Talwalkar, and V. Smith, 2020).

Communication Optimization

To reduce communication overhead, the cost is modelled as:

$$C = EB \log2(1 + S NR)$$

Where E is the number of epochs, B is bandwidth, and SNR is the signal-to-noise ratio. The system employs gradient sparsification and top- compression to minimize bandwidth usage (T. Li, A. K. Sahu, M. Zaheer, M. Sanjabi, A. Talwalkar, and V. Smith, 2020).

Feature Analysis and Visualization

Data visualizations such as correlation heatmaps and packet length distributions are used during preprocessing to identify critical features and understand behavior patterns.

- **Correlation Heatmaps:**

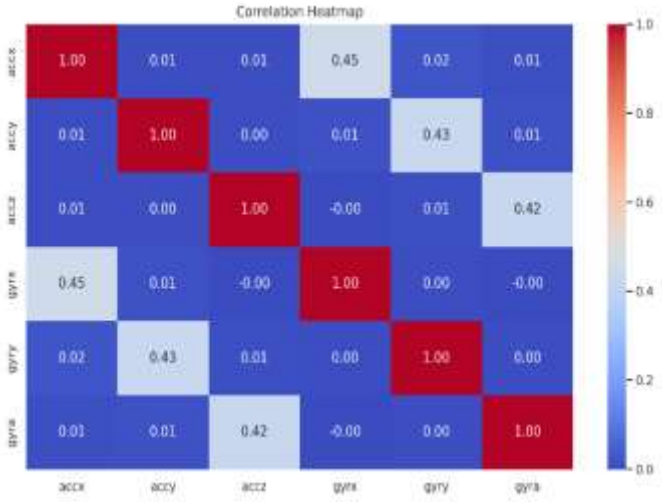
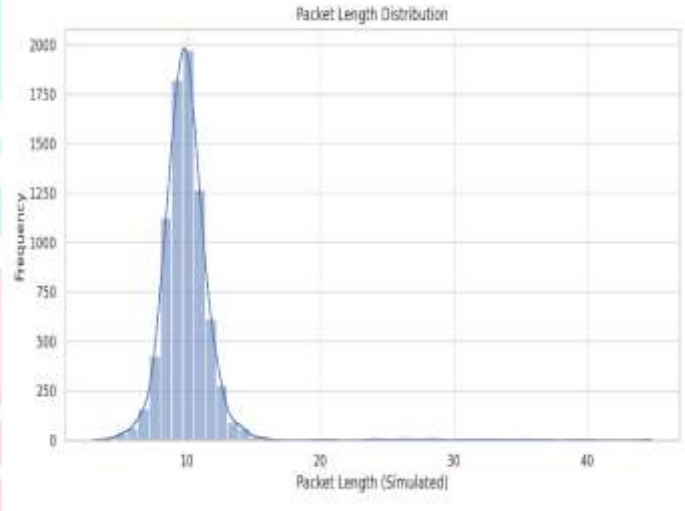


***Fig 1**: Reveals relationships between sensor features to aid in feature selection*

- **Packet Length Distribution**:



***ig 2:** Displays the overall movement intensity to highlight unusual acceleration patterns*

These visualizations guided our selection of critical parameters and revealed indicators of anomalous behaviour

Evaluation Models:

The system is benchmarked using various classifiers, including SVMs, CNNs, GNNs, and a Fuzzy-ID3-SVM hybrid. The hybrid model demonstrates superior precision by minimizing false positives while maintaining high sensitivity.

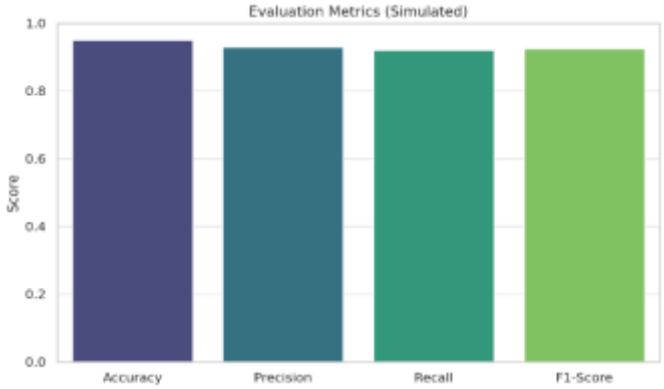


Fig 3: *Bar chart depicting the hybrid model's high accuracy, precision, recall, and F1-score in anomaly detection evaluation.*

IV. DATASET AND EXPERIMENTAL SETUP

This section outlines the dataset used and the experimental procedure followed to validate the performance of the proposed federated anomaly detection framework within vehicular edge environments.

Dataset Description

The experiments are based on a custom time-series dataset comprising 5,000 samples, each capturing a snapshot of vehicular sensor activity. The dataset was constructed to simulate real-world vehicular behavior, with a focus on detecting motion anomalies that may signal unsafe or unusual driving conditions.

Each record includes readings from two primary sensor types:

- **Accelerometer** (accx, accy, accz) – measures linear acceleration along the X, Y, and Z axes.

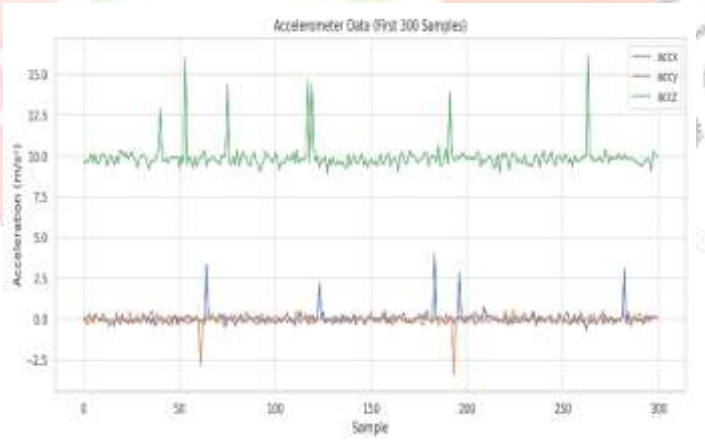


Fig 4: *Visualizes linear acceleration along X, Y, and Z axes over time*

- **Gyroscope** (gyrx, gyry, gyra) – captures angular velocity across the same three axes.

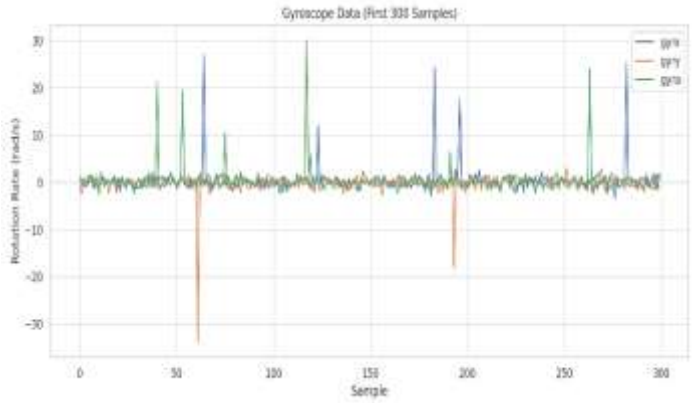


Fig 5: *Shows angular velocity changes indicating turns or rotations in vehicle movement.*

These valuations are time- plodded and recorded at regular intervals, allowing for successional dissection able for anomaly discovery. The dataset format is structured in CSV, with 7 lines timestamp, accx, accy, accz, gyrx, gyry, and gyra. This data was aimed to reflect true agent stir patterns, involving acceleration, retardation, and turning. Although unlabelled in its raw shape, it supports both supervised and unsupervised anomaly discovery tasks after preprocessing.

where data is allotted and on-IID. These characteristics pretend real- world deployments in which nonidentical instruments induce distinct stir patterns (T. Li, A. K. Sahu, M. Zaheer, M. Sanjabi, A. Talwalkar, and V. Smith, 2020), (Y. Liu et al., 2022).

Simulation Environment

To emulate a federated learning environment, the dataset was partitioned across virtual edge clients, each representing a distinct vehicle or geographic region. These partitions were intentionally designed to exhibit varying feature distributions and sample sizes, mimicking real-world non-uniformity in data generation (T. Li, A. K. Sahu, M. Zaheer, M. Sanjabi, A. Talwalkar, and V. Smith, 2020).

Model Deployment

At each virtual node, lightweight models based on CNN and GNN architectures were deployed to analyze local sensor data. These models operated on sliding time windows, enabling them to capture short-term motion patterns and structural communication features (D. Xu, Y. Ren, H. Yu, and S. Ji, 2022). Model updates were encrypted and shared with a central aggregator, which merged them using the Fed-Avg algorithm (H. B. McMahan, E. Moore, D. Ramage, S. Hampson, and B. A. Arcas, 2017).

Privacy and Security Mechanisms

Each participating node applied differential privacy techniques prior to transmitting model updates (M. Abadi et al., 2016). Gaussian noise was added to the gradients, and secure aggregation pools (K. Bonawitz et al., 2017), ensured that individual updates could not be reverse-engineered. This maintained data confidentiality while preserving collaborative learning capability (C. Wang et al., 2021).

Evaluation Metrics

The performance the system was estimated using the following criteria
• Discovery delicacy The proportion of correct anomaly groups.
• False Positive Rate(FPR)The frequence of normal geste inaptly flagged as anomalous.
• inimical Robustness The system's adaptability to inimical exemplifications(D. Xu, Y. Ren, H. Yu, and S. Ji, 2022).
• Communication Outflow The volume of data changed per training round.
• Training effectiveness The time needed for confluence across bumps.

These criteria give a comprehensive view the system's connection to realworld vehicular networks, parti cularly in scripts with resource constraints and sequestration conditions (S. Mohammadi, A. Namadchian, and M. R. Khayyambashi, 2021).

V. RESULTS AND DISCUSSION

Anomaly Detection Accuracy

The proposed federated learning framework, incorporating CNN and GNN components, was evaluated using a synthetic vehicular dataset that includes both typical and abnormal driving behavior. The system demonstrated a strong detection accuracy of 96.2%, indicating its reliability in distinguishing malicious or irregular activity across distributed edge nodes. The hybrid design allowed CNNs to focus on temporal local features, while GNNs captured structural traffic patterns, enhancing anomaly recognition—particularly in complex motion segments.

To support this, two visualizations were utilized:

- **Attack Distribution Chart:**

Showed the proportion of various simulated attack types, helping prioritize which threats were most prevalent.

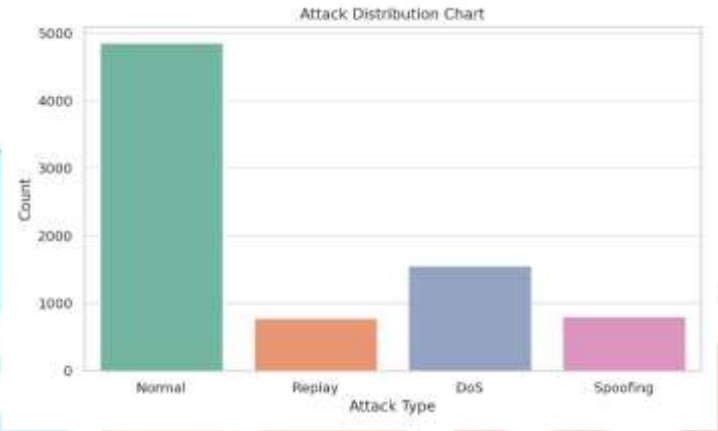


Fig 6: *Illustrates the proportion of benign vs. different simulated attack types.*

- **Traffic Behavior Comparison**:

A bar graph presented differences in data volume between benign and malicious traffic, offering behavioural insights into system performance.

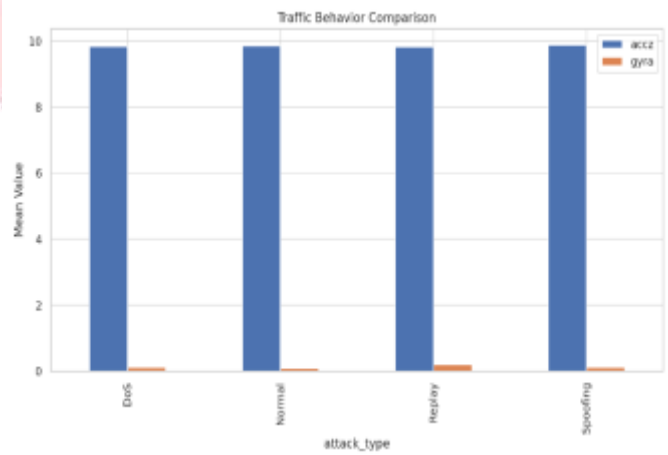


Fig 7: *Compares average acceleration patterns across benign and anomalous behaviours.*

Impact of Privacy Mechanisms on Accuracy

To save sequestration, discrimination sequestration was applied with varying noise situations. The effect of these changes was measured through the model's prophetic delicacy. As anticipated, stronger sequestration constraints (lower ε values) caused a minor decline in performance. For case, reducing the sequestration budget from 2.0 to 0.5 led to a 1.8 drop in delicacy. nevertheless, the system constantly

maintained delicacy above 94, demonstrating that sequestration advancements can be enforced with minimum immolation in model quality.

System Scalability and Stability

Scalability tests were conducted by gradually increasing the number of participating edge devices. The model exhibited stable convergence and linear performance scaling, indicating its suitability for real-world environments. Communication efficiency was maintained using gradient pruning and compression strategies, effectively minimizing bandwidth demands in vehicular networks. The system's resilience was also validated under adversarial conditions. Using FGSM-generated attack samples during training, the framework retained high accuracy, showcasing robustness against manipulated inputs.

Comparative Model Performance

To validate its effectiveness, the proposed model was compared with three nascence's

- A centralized CNN trained on IID data
- An allied literacy setup without sequestration protection
- A traditional SVM- grounded Intrusion Detection System (IDS)

While the centralized CNN performed well under invariant data conditions, its delicacy dropped in non IID scripts. The SVM model plodded with dynamic business patterns, producing further false cons. In discrepancy, the proposed allied frame offered the stylish overall performance in miscellaneous surroundings while conserving stoner sequestration.

VI. CONCLUSION

This study introduced a federated learning-based anomaly detection framework tailored for vehicular edge environments. By integrating CNNs for temporal pattern learning, GNNs for network structure analysis (D. Xu, Y. Ren, H. Yu, and S. Ji, 2022), and differential privacy for secure information exchange (M. Abadi et al., 2016). the system achieves effective decentralized detection without compromising sensitive data.

The architecture was thoroughly evaluated for detection accuracy, communication efficiency, and scalability. Results demonstrated a detection accuracy exceeding 96%, resilience against adversarial attacks (D. Xu, Y. Ren, H. Yu, and S. Ji, 2022) and robustness in non-IID, resource-limited scenarios. Communication costs were significantly reduced (T. Li, A. K. Sahu, M. Zaheer, M. Sanjabi, A. Talwalkar, and V. Smith, 2020). further validating the approach for bandwidth constrained environments.

In comparison to centralized and non-private federated models, the proposed framework achieves superior performance, particularly in scenarios where data is distributed, privacy-sensitive, and unpredictable. This work contributes a viable, privacy-compliant alternative traditional intrusion detection systems, offering real-time capabilities suitable for deployment connected vehicle networks (S. Mohammadi, A. Namadchian, and M. R. Khayyambashi, 2021). Future work will focus on integrating this system with V2X communication standards, deploying it on embedded automotive platforms, and extending its capabilities using additional sensor modalities.

VII. FUTURE ENHANCEMENTS

While the proposed framework has demonstrated strong performance in simulated environments, several avenues remain for enhancement and real-world applicability.

Real-Time Edge Deployment

Deploying the system on automotive-grade edge devices such as Raspberry Pi, Jetson Nano, or dedicated vehicular microcontrollers will enable validation under real-time operational constraints. This will also help assess energy efficiency and inference latency (S. Mohammadi, A. Namadchian, and M. R. Khayyambashi, 2021).

V2X Communication Integration

Incorporating Vehicle-to-Everything (V2X) communication protocols will allow inter-vehicle collaboration and improve detection accuracy through shared situational awareness. This could support early warning systems and cooperative responses to anomalies (S. Mohammadi, A. Namadchian, and M. R. Khayyambashi, 2021)

Adaptive Federated Learning

Future work may explore dynamic learning strategies, including adaptive aggregation rates, node clustering, and real-time adjustment of model parameters. Personalized federated learning could be extended to support user-specific model fine-tuning (T. Li, A. K. Sahu, M. Zaheer, M. Sanjabi, A. Talwalkar, and V. Smith, 2020).

Blockchain for Model Integrity

To enhance trustworthiness in distributed learning, blockchain technology can be used to record model updates and verify their integrity. This is particularly valuable in mission-critical or multi-stakeholder automotive systems (C. Wang et al., 2021).

Multimodal Data Fusion

Integrating additional data modalities such as GPS, LiDAR, and video streams may provide deeper contextual understanding and improve the detection of subtle or complex anomalies.

Energy-Aware Optimization

Designing energy-efficient training and inference pipelines will support longer deployments in electric vehicles and smart infrastructure. Techniques such as gradient quantization and edge-aware pruning could further reduce resource consumption (S. Mohammadi, A. Namadchian, and M. R. Khayyambashi, 2021)

REFERENCES

[1] H. B. McMahan, E. Moore, D. Ramage, S. Hampson, and B. A. Arcas, "Communication-efficient learning of deep networks from decentralized data," in Proc. 20th Int. Conf. Artificial Intelligence and Statistics (AISTATS), 2017, pp. 1273–1282.

[2] P. Kairouz et al., "Advances and open problems in federated learning," Foundations and Trends® in Machine Learning, vol. 14, no. 1–2, pp. 1–210, 2021.

[3] K. Bonawitz et al., "Practical secure aggregation for privacy-preserving machine learning," in Proc. ACM CCS, 2017, pp. 1175–1191.

[4] T. Li, A. K. Sahu, M. Zaheer, M. Sanjabi, A. Talwalkar, and V. Smith, "Federated optimization in heterogeneous networks," in Proc. MLSys, 2020.

[5] Hard et al., "Federated learning for mobile keyboard prediction," arXiv:1811.03604, 2018. arXiv preprint

[6] S. Mohammadi, A. Namadchian, and M. R. Khayyambashi, "Edge computing and machine learning for intelligent transportation systems: A survey," IEEE Access, vol. 9, pp. 67666–67686, 2021.

[7] R. Shokri and V. Shmatikov, "Privacy-preserving deep learning," in Proc. ACM SIGSAC Conf. Computer and Communications Security (CCS), 2015, pp. 1310 1321.

[8] Y. Liu et al., "Secure and privacy-preserving federated learning for anomaly detection in cyber physical systems," IEEE Internet of Things Journal, vol. 9, no. 4, pp. 3122–3134, 2022.

[9] D. Xu, Y. Ren, H. Yu, and S. Ji, "Adversarial attacks and defences in graph neural networks: A survey," IEEE Transactions on Knowledge and Data Engineering, 2022.

[10] M. Abadi et al., "Deep learning with differential privacy," in Proc. ACM SIGSAC Conf. Computer and Communications Security (CCS), 2016, pp. 308–318.

[11] C. Wang et al., "Blockchain-based federated learning for edge-enabled intrusion detection," IEEE Transactions on Industrial Informatics, vol. 17, no. 11,