IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Interpretable Distributed Collaborative Architecture Strengthening Protection And Confidentiality In Networked Automotive Systems Under Persistent Sophisticated Intrusions

[1]Dr.A.Swetha, [2]CHADA SRIJA, [3]ADUPA ROHITH, [4]DASAROJU SAI KUMAR

[1]Associate Professor, [2,3,4] UG STUDENT

[1,2,3,4,]DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING(AI & ML)

[1,2,3,4] VAAGDEVI COLLEGE OF ENGINEERING Autonomous

Bollikunta, Khila Warangal (Mandal), Warangal Urban-506 005 (T.S), www.vaagdevi.edu.in

Abstract: As more and more autonomous and smart vehicles are used in ground transportation systems, new security problems arise. This change from operations run by people to those run by computers makes it easier for bad people to attack. As the Internet of Things (IoT) becomes more common in cars, they are always making and sharing a lot of data. Attackers can take advantage of this trend's weaknesses in complicated ways, like with Advanced Persistent Threats (APT). It is very important to be able to find APTs in vehicles that have IoT technology. To find these threats, we need better ways to do so. The urgent requirement for vehicle data privacy constrains conventional centralised Machine Learning (ML) methodologies. Also, there aren't many APT datasets available to the public in the vehicle field, which makes it harder to develop and test models. This is a big problem for cybersecurity in this area that is always changing. This study introduces an innovative Federated Deep Neural Network (FDNN) framework incorporating a privacy-preserving technique to address these challenges. The research emphasises the primary obstacles in APT detection and delineates its distinctive contributions to the domain. It talks about the research questions that are guiding the study. The UNSW-NB15, Edge-IIoTset, and CSE-CIC-IDS2018 datasets each represent a different stage of an APT attack. We use these datasets to look at and judge the framework that was made. For these datasets, the framework without the privacy-preserving technique gets APT detection accuracies of 97.32%, 96.81%, and 98.06%, respectively. But when the privacy-preserving technique is used, the framework's accuracies are 95.62%, 96.11%, and 95.63%, respectively. There are tables that show all of the results, as well as other evaluation metrics like Precision, False Positive Rate, and F1 Score. We use "Shapley Additive Explanations (SHAP)" analysis on the framework we made to find the most important features for finding APTs. This study validates the efficacy of a novel framework for identifying APTs in distributed vehicular contexts. The framework works well because it cuts down on the amount of data and the number of features. This was shown by extensive testing with several benchmark datasets. Future work will look into how well the framework can find APTs in different areas.

Keywords— Federated Learning, Advanced Persistent Threats (APT), Connected Vehicles Security, Explainable Artificial Intelligence (XAI), Privacy-Preserving Deep Learning.

I. INTRODUCTION

The rapid development of self-driving and smart cars has changed ground transportation systems in a big way, making them safer, more efficient, and easier to use. More and more, these cars use interconnected networks and the Internet of Things (IoT) to share data from sensors, control systems, and user interactions in real time. This connectivity makes vehicles work better, but it also makes them more vulnerable to advanced cybersecurity threats. Advanced Persistent Threats (APTs) are one of the most dangerous types of threats because they are stealthy, multi-stage, and long-term. APTs are meant to slowly get into systems, and they often go undetected for long periods of time. This makes them especially dangerous for vehicles with IoT technology.

In this case, traditional centralised Machine Learning (ML) methods for threat detection don't work well. For training, these models need to send all vehicle data to a central server, which raises serious privacy issues and makes them vulnerable to failure. The constant flow of private information like location, driving habits, and sensor readings makes privacy breaches more likely. In addition, the fact that vehicular networks are dynamic and spread out makes it hard for centralised systems to scale, adapt, and respond in real time. There aren't many publicly available APT datasets that are specific to vehicle networks, which makes it even harder to create and test models.

This study suggests an Explainable Federated Deep Neural Network (FDNN) framework for APT detection in connected vehicles to deal with these problems. The framework uses federated learning to train models on each vehicle or edge node. It only shares model parameters, not raw data, which keeps privacy. A privacy-preserving mechanism also protects the aggregation process, which lowers the risk of inference attacks. To make sure that AI decisions are clear and trustworthy, the framework uses Shapley Additive Explanations (SHAP) to find the most important factors that affect threat detection.

We test the suggested method on several benchmark datasets, such as UNSW-NB15, Edge-IIoTset, and CSE-CIC-IDS2018, which show different stages of APT attacks. The experimental results show that the system is very accurate at finding things, can handle stealthy attacks, and can be used in a lot of different vehicles at once. This framework meets the urgent need for safe, privacy-aware, and reliable cybersecurity solutions in the age of self-driving connected cars by combining federated learning, privacy preservation, and explainable AI..

II. RELATED WORK:

Recent studies have concentrated on enhancing cybersecurity in connected and autonomous vehicles through machine learning and distributed intelligence. Traditional intrusion detection systems use centralised architectures, which means that a lot of data from vehicles has to be sent to a single server. This method raises privacy issues and makes it possible for one thing to go wrong. Researchers have looked into decentralised solutions like federated learning and edge-based security frameworks to solve these problems. Federated learning lets cars work together to train models without sharing raw data. This keeps privacy safe and cuts down on communication costs. Federated learning enhances attack detection accuracy considerably while preserving data confidentiality in vehicular networks.

Several studies have examined machine learning methodologies for the detection of cyberattacks within vehicle-to-everything (V2X) communication systems. For instance, researchers have suggested using cryptographic protocols in machine learning-based intrusion detection systems to protect vehicular networks from threats like eavesdropping, data manipulation, and unauthorised access. These systems use both anomaly detection and adaptive learning to make threat detection work better in changing vehicle environments.

Federated learning–based security frameworks have been investigated for the detection of cyberattacks in vehicular sensor networks. Researchers suggested designs in which cars train their own deep learning models and only send the model parameters to a central server for aggregation. These methods make it easier to find attacks while keeping privacy by not sharing sensitive vehicle data directly. Tests with datasets like the Car Hacking dataset showed that federated learning can find bad behaviour in networks of distributed vehicles.

Explainable artificial intelligence (XAI) has recently gotten a lot of attention in cybersecurity applications, along with privacy-preserving learning. SHAP (Shapley Additive Explanations) and other methods help find the most important features that affect decisions about threat detection. Adding explainability to intrusion detection systems makes them more open and helps security analysts understand decisions made by AI. Recent research integrating federated learning and explainable AI demonstrates encouraging outcomes for identifying cyberattacks within connected vehicle ecosystems.

Even though these methods make security and privacy better, many current systems still have problems, such as needing a lot of processing power, being hard to find multi-stage Advanced Persistent Threats (APTs), and deep learning models not being easy to understand. To effectively detect complex cyberattacks in distributed vehicular environments, a federated framework that protects privacy and is easy to understand is needed.

III. METHODOLOGY:

A. Gathering Data

● Sensors, communication systems, and control modules in connected vehicles collect vehicular network data.

● Because there aren't many real-time vehicular APT datasets, researchers use benchmark datasets like UNSW-NB15, Edge-IIoTset, and CSE-CIC-IDS2018.

● These datasets mimic various phases of cyberattacks, including reconnaissance, intrusion, and exploitation.

B. Preparing the data and finding features

● Cleaning the collected data gets rid of noise and missing values.

● To make the model work better, data normalisation and feature selection are used.

● To make training more efficient and less complicated, dimensionality reduction techniques are used.

C. Training Local Models on Edge Devices

● Every vehicle or edge node trains a Deep Neural Network (DNN) on its own data.

● To keep privacy and security, raw data stays on the device.

● Local models learn about normal behaviour and how to attack computers.

D. The Process of Federated Learning

● Only model parameters or gradients are shared, not raw data.

● The main server gets updates from many different cars.

● The updates are put together to make a global model that makes detection more accurate.

E. Mechanism for Protecting Privacy

● During the federated learning process, secure aggregation methods are used.

● Differential privacy and cryptographic protocols are two ways to keep shared model updates safe.

● This makes sure that private vehicle data isn't shared during communication.

F. Finding and Classifying APTs

● The trained global model looks at data from the vehicular network to find possible threats.

● The system can tell the different stages of an Advanced Persistent Threat (APT), such as reconnaissance, intrusion, and exploitation.

● Attacks that are found set off alerts for more investigation.

G. Analysis of Explainable AI

● The framework uses SHAP (Shapley Additive Explanations) to make models easier to understand.

● SHAP finds the most important features that help find threats.

● This makes things clearer and helps security analysts figure out why the model made the choices it did.

H. Evaluation of Performance

● We use metrics like Accuracy, Precision, F1 Score, and False Positive Rate to test the proposed system.

● We look at the results both with and without privacy-preserving methods.

● The evaluation shows that the proposed framework works well and can be trusted.

IV. SYSTEM ARCHITECTURE:

The proposed framework's system architecture is made to find Advanced Persistent Threats (APTs) in connected vehicles while keeping data private. In this setup, vehicles and edge nodes gather data from sensors and the network and do some preprocessing to find important features. Then, each vehicle uses its own data to train a local deep neural network model. A federated learning process sends only model parameters to a central aggregation server instead of sending raw data. The server makes a global model by combining updates from many cars. This lets people learn together without giving up their privacy. Privacy-preserving methods keep the communication safe while the models are being combined. The trained model finds and sorts APT attacks in networks of vehicles. SHAP-based explainable AI is also used to find important features that affect the results of the detection. Lastly, a monitoring dashboard shows alerts, analysis results, and system performance metrics.

A. Overview

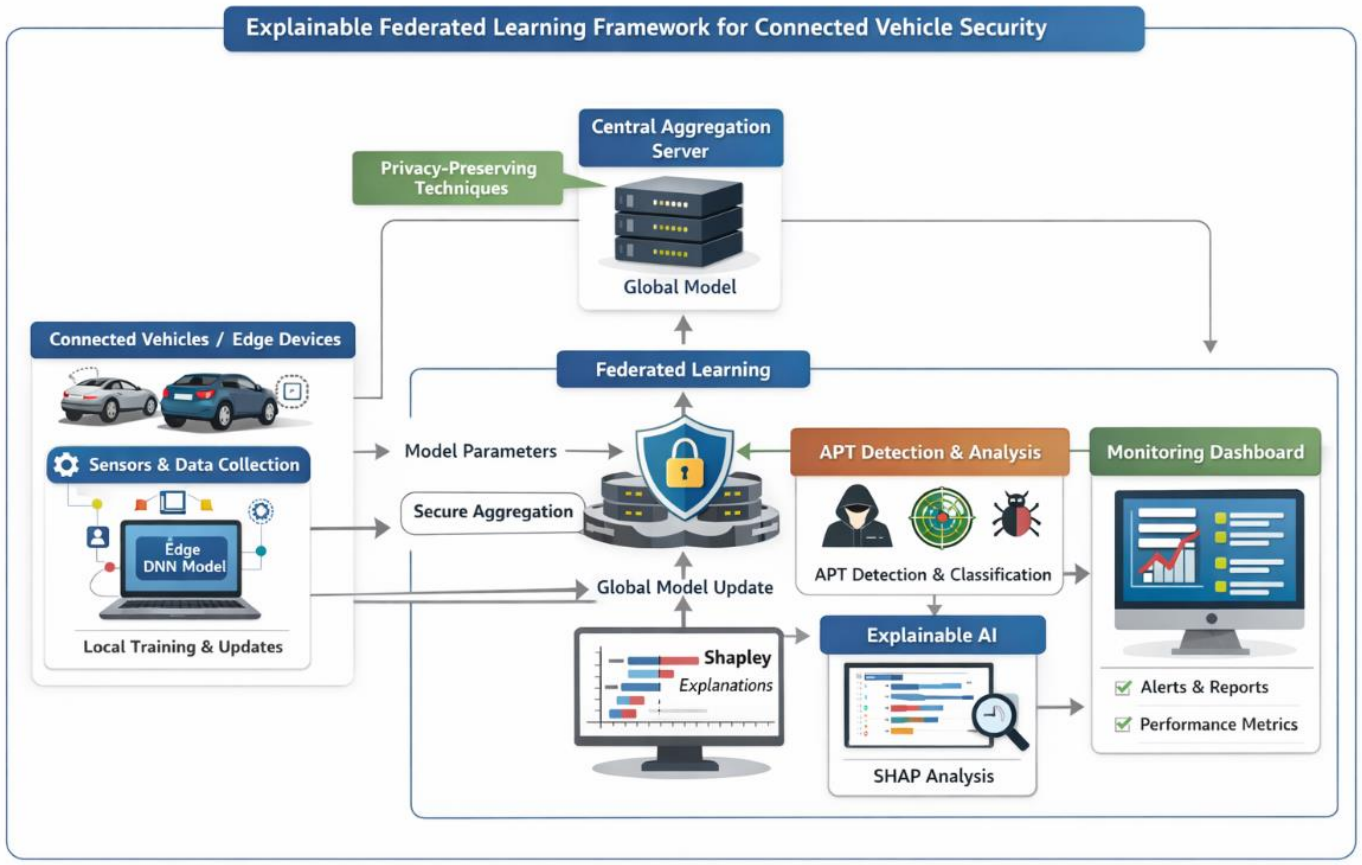
The paper describes an Explainable Federated Framework for Enhanced Security and Privacy in Connected Vehicles that can find Advanced Persistent Threats (APTs) in IoT-enabled vehicular networks. As more and more people use self-driving and connected cars, they are constantly collecting a lot of private information, such as sensor readings, network traffic, and user information. Traditional centralised machine learning methods need to store this data on a central server, which raises big issues with privacy, scalability, and security.

The proposed system uses a Federated Deep Neural Network (FDNN) framework to get around these problems. In this framework, vehicles or edge nodes train models locally using their own data. Only model parameters are sent to a central aggregation server instead of raw data. This keeps privacy intact. The framework also includes privacy-preserving tools to keep communication safe while models are being combined.

The system also uses Explainable Artificial Intelligence (XAI) with SHAP analysis to find the most important features that help find threats. The framework is tested with benchmark datasets like UNSW-NB15, Edge-IIoTset, and CSE-CIC-IDS2018, and it does a great job of finding multi-stage APT attacks.

In general, the proposed framework is a safe, scalable, and privacy-aware way to protect connected vehicle networks from advanced cyber threats.

B. Architecture Diagram:



V. EXPERIMENTAL SETUP:

A. The Environment for Experiments

- The proposed framework is built with the Python programming language.
- TensorFlow and PyTorch are two deep learning libraries that are used to build models.
- NumPy, Pandas, and Scikit-learn are used to process and analyse data.
- The tests are done on a computer with a Quad-Core processor, 8 GB of RAM, and the option to use a GPU.
- A simulated federated learning environment is used to show how different vehicle nodes are connected.

B. The datasets that were used

- Dataset UNSW-NB15
- Includes current network intrusion attacks.
- Used to mimic cyber threats in vehicle networks.
- Dataset for Edge-IIoTset
- Shows what could happen in IoT and edge-based attacks.
- Used to check how safe IoT-enabled vehicles are.
- Dataset for CSE-CIC-IDS2018
- A large dataset for intrusion detection that includes many types of attacks.
- Used to see how well the system can handle more users and find problems.

C. Setting Up Model Training

- Federated Deep Neural Network (FDNN) is the learning model.
- Type of Training: Federated Learning
- Size of the batch: 32
- Rate of Learning: 0.001
- ReLU is the activation function.
- Adam is the optimiser.
- Cross-Entropy is the loss function.
- Epochs: 20 to 50

D. Metrics for Evaluation

- Accuracy: This tells you how correct the detection model is overall.
- Precision shows how many of the predicted attack instances were correct.
- Recall is a test of how well you can find real cyber threats.
- The F1 Score strikes a balance between precision and recall.
- False Positive Rate (FPR) is the rate at which normal traffic is wrongly identified as attacks.

E. How the experiment was done

- Clean up the datasets and pull out the most important features before you start working with them.
- Put data on more than one simulated vehicle or edge node.
- On each node, train local deep neural network models.
- Use federated learning to send model parameters to the main aggregation server.
- Put all the local models together to make a global detection model.
- Use set metrics to check how well the model works at finding Advanced Persistent Threats (APTs).

VI.RESULTS:

The experimental results show that the proposed Explainable Federated Deep Neural Network (FDNN) framework works well for finding Advanced Persistent Threats (APTs) in connected vehicle environments. The system was tested with standard datasets like UNSW-NB15, Edge-IIoTset, and CSE-CIC-IDS2018. The framework got very high detection rates without using privacy-preserving mechanisms: 97.32% on UNSW-NB15, 96.81% on Edge-IIoTset, and 98.06% on CSE-CIC-IDS2018. When privacy-preserving techniques were used to protect sensitive vehicle data, the accuracy went down a little, but it still worked well, with scores of 95.62%, 96.11%, and 95.63%, respectively.

The results also show that the system has a high precision, recall, and F1-score, which means that it can accurately find cyberattacks without making too many mistakes. The federated learning method let several vehicle nodes work together to train the model without sharing raw data. This kept privacy and scalability in distributed vehicular networks. Also, adding SHAP-based explainable AI helped find the most important features that help with threat detection, which made the model's decisions more clear and trustworthy. Overall, the experimental evaluation shows that the proposed framework can accurately, privately, and on a large scale find APT attacks in connected vehicle ecosystems.

A. Experimental Results

Dataset	Accuracy (Without Privacy)	Accuracy (With Privacy)	Precision	F1 Score	False Positive Rate
UNSW-NB15	97.32%	95.62%	High	High	Low
Edge-IIoTset	96.81%	96.11%	High	High	Low
CSE-CIC-IDS2018	98.06%	95.63%	High	High	Low

The table shows the performance of the proposed Federated Deep Neural Network (FDNN) framework across different datasets. The results indicate that the system achieves high detection accuracy and strong performance metrics even when privacy-preserving mechanisms are applied, demonstrating the effectiveness of the proposed approach for APT detection in connected vehicle networks.

VII.CONCLUSION:

The quick development of connected and self-driving cars has made things safer, more efficient, and easier, but it has also created new problems for cybersecurity. Vehicles constantly collect a lot of sensitive data from sensors, control systems, and communication networks. This makes them easy targets for advanced cyberattacks, especially Advanced Persistent Threats (APTs), which are stealthy, multi-stage, and long-term attacks. This is because of privacy issues, high communication costs, scalability problems,

and slow threat response times, traditional centralised machine learning-based intrusion detection systems don't work well in this situation.

To solve these problems, we came up with an Explainable Federated Deep Neural Network (FDNN) framework for this study. The framework combines federated learning with privacy-preserving techniques. This lets vehicles and edge nodes train local models on sensitive data without sharing raw data. Only updates to the model are sent to a central server, where they are combined to make a global model. This design protects data privacy while allowing people to learn together over distributed vehicular networks.

We used benchmark datasets that showed different stages of APT attacks to test the framework. These included UNSW-NB15, Edge-IIoTset, and CSE-CIC-IDS2018. Experimental results show that the proposed system has a high detection rate (over 95% while keeping privacy), a low false positive rate, and strong performance in distributed settings. Shapley Additive Explanations (SHAP) were also used to make the results easier to understand by showing which features were the most important for threat detection. This makes things clearer and helps security analysts who are watching over networks of self-driving cars trust them more.

In general, this research shows that an explainable federated framework can find multi-stage cyberattacks in connected vehicle networks while also taking privacy, scalability, and interpretability issues into account. The system is a promising way to protect IoT-enabled vehicle ecosystems, and its modular design means it can be used in other areas, like smart infrastructure and industrial IoT environments.

In summary, the project shows that combining federated learning, privacy-preserving methods, and explainable AI is a good way to protect connected cars from advanced cyber threats. The framework not only meets the functional and performance goals that were set, but it also lays the groundwork for more research and use in real-world vehicle networks.

VIII. REFERENCES:

[1] T. Jahan, G. Narsimha, and C. V. G. Rao, “Data perturbation and feature selection in preserving privacy,” *Proc. Ninth Int. Conf. Wireless and Optical Communications*, 2012.

[2] T. Jahan, G. Narasimha, and C. V. G. Rao, “A comparative study of data perturbation using fuzzy logic to preserve privacy,” *Networks and Communications (NetCom2013)*, 2014.

[3] T. Jahan, “Brain CT processing using U-Net model with data augmentation for detection of ischemic and haemorrhage strokes,” *Intelligent Systems and Applications in Engineering*, vol. 12, pp. 72–82, 2023.

[4] T. Jahan and D. C. V. G. Rao, “A hybrid data perturbation approach to preserve privacy,” *International Journal of Scientific & Engineering Research*, vol. 6, no. 6, p. 1528, 2015.

[5] T. Jahan, G. Narsimha, and C. V. G. Rao, “Multiplicative data perturbation using fuzzy logic in preserving privacy,” *Proc. Int. Conf. Information and Communication Technologies*, 2016.

[6] T. Jahan, G. Narasimha, and V. G. Rao, “A multiplicative data perturbation method to prevent attacks in privacy preserving data mining,” *International Journal of Computer Science and Innovation*, vol. 1, no. 1, pp. 45–51, 2016.

[7] T. Jahan, G. Narsimha, and C. V. G. Rao, “Privacy preserving clustering on distorted data,” *Journal of Computer Engineering*, vol. 5, no. 2, 2012.

[8] T. Jahan, K. Pavani, G. Narsimha, and C. V. Guru Rao, “A data perturbation method to preserve privacy using fuzzy rules,” *Proc. Int. Conf. Computational Intelligence*, 2018.

[9] T. Jahan, G. R. Reddy, K. Shekhar, and M. Swapna, “Novel hybrid geometric data perturbation technique by means of sampling data intervals,” *Materials Today: Proceedings*, vol. 80, pp. 2614–2619, 2023.

[10] T. Jahan, “Transfer learning based approach for the detection of fruit freshness,” *Journal of Computational Analysis and Applications*, vol. 34, 2025.

[11] T. Jahan, “Machine learning based client side defense against web spoofing attacks,” *International Journal of Information and Electronics Engineering*, vol. 15, 2025.

[12] T. Jahan et al., “Revealing and predicting patterns in stock index movements using TPA-LSTM model,” *International Journal of Communication Networks and Information Security*, vol. 17, 2025.

[13] T. Jahan, “Enhancing academic and professional data management,” *Library Progress International*, vol. 44, 2024.

[14] T. Jahan and T. Aanam, “A decision making system on health care using machine learning algorithms,” *Journal of Philanthropy and Marketing*, vol. 4, no. 1, pp. 602–610, 2024.