Enhancing Security in Automobile Edge Computing through Federated Learning and Blockchain

Dr. Sandosh S,
Faculty for Computer Science with specialization in Artificial Intelligence and Machine Learning
Vellore Institute of Technology, Chennai,India
sandosh.s@vit.ac.in

Sujay Doshi,
Computer Science with specialization in Artificial Intelligence and Machine Learning
Vellore Institute of Technology, Chennai,India
sujay.doshi2020@vitstudent.ac.in

Atharva Joshi
Computer Science with specialization in Artificial Intelligence and Machine Learning
Vellore Institute of Technology, Chennai,India
atharva.joshi2020@vitstudent.ac.in

***Abstract*— Vehicular networks that consist of interlinked automobiles and transportation network are prone to cyber-attacks due to the increased use of software and the presence of wireless interfaces. To counter these threats, intrusion detection systems can be tailored efficiently. In recent years, there has been significant development in detection of malicious attack traffic through the use of machine learning. However, traditional systems require powerful computing devices to continuously train and update complex network models, which can reduce the efficiency and effectiveness of the system due to resource constraints, untimely updates and dealing with large volumes of data. To address this issue, a cooperative intrusion detection mechanism which had been proposed has been improved with a classification based novel approach, that eases the burden by distributing the training model to distributed edge devices such as connected vehicles and roadside units. The previous approach has a slow response time to the increasing network issues. The proposed work offers a new approach through federated learning with the Extra Trees Classification algorithm. The Extra Trees Classifier performs better than other machine learning models in all aspects. The proposed approach provides a faster response to security threats in automobile edge computing. The use of a distributed federated approach reduces the load on the server while maintaining confidentiality by aggregating models using a blockchain.**

Keywords—intrusion detection system, federated learning, blockchain, decentralized.

I. Introduction

In the advent of artificial intelligence, computer vision, other key technologies & their development, it has been noted that the development of autonomous vehicles has become a major topic of interest in the field of transportation (Zhang et al., 2020)[1]. As computer vision and other key technologies continue to advance, the transportation sector has seen significant growth in recent years. Yang et al. (2021)[2] pointed out that "autonomous vehicles can now navigate through complex and unpredictable environments with increased efficiency and accuracy." However, the increased use of autonomous vehicles and smart road infrastructure has raised concerns about the potential for data security breaches and vulnerabilities. According to Li et al. (2021)[1], "the rise of autonomous vehicles and their corresponding infrastructure has made cybersecurity a crucial issue for ensuring the safety and reliability of these systems." Consequently, it is essential to address the potential security risks associated with autonomous vehicles and smart road infrastructure to ensure their effective and safe implementation.

More and more data is being generated by each of these vehicles, where in there is greater risk of sensitive information being intercepted by people with malicious intent when vehicle is transferring data to other entities in the infrastructure, like Road Side Units (RSU’s), other Automobiles, etc.

The utilization of deep learning techniques has been explored as a means to improve attack detection. According to Yue et al. (2020)[3], "Deep learning-based anomaly-detection IDSs can improve the accuracy of attack detection." Deep neural networks have gained significant popularity in this field, however they rely on powerful computing capacities and a centralized cloud training server, which can create vulnerabilities for data privacy and leakage. Cheng et al. (2021)[4] have noted that "these methods require powerful computing capacities and a centralized cloud training server." In light of these concerns, alternative solutions for training deep learning-based IDSs are necessary to address these security risks and improve the effectiveness of these systems.

Machine learning algorithms require data in order to produce accurate results. However, the centralization of model training and the potential for data leaks are significant challenges that must be addressed. Ensuring the privacy of the training data while completing the model training process is a crucial issue that must be resolved. With the rise of edge computing, strong foundation for collaborative systems has been laid out, and could be considered as a promising solution.

Federated Learning is an effective solution for collaborative machine learning (Chen et al., 2021)[1]. This method enables the training of machine learning models using data from multiple decentralized sources, thereby preserving data privacy and security. According to Yang et al. (2020)[3], Federated Learning allows organizations to build machine learning models without centralizing data, thereby avoiding the risks associated with data breaches. In Federated Learning, multiple participants collaborate to train the model while keeping their individual data on their devices or servers. As a result, Federated Learning has been proposed as a solution to the problem of centralized data and its associated security risks. Leveraging machine learning techniques with the advantages of Federated Learning ensures that organizations can maintain data security and privacy.

In this paper, the proposed schematic integrates decentralization and federated learning through multiple edge vehicles and novel architecture for better implementation of Data updating in the edge vehicles with the usage of machine learning techniques and string matching algorithms.

The remainder of the paper is organized in the following Sections. Section II describes the existing architecture followed by Section III which describes the infrastructure. Section IV contains information about blockchain followed by Section V which tells us more about Federated Learning. Section VI describes the proposed architecture followed by the concluding remarks of the study and the future works in Sections VII and VIII.

II. Abbreviations and acronyms

1. RSU's – Road Side Units
2. DOS – Denial of Service Attacks
3. DDoS – Distributed Denial of Service Attacks
4. VANET - Vehicular Ad Hoc Network
5. BMEC-FV - Blockchain-based Mobile Edge Computing Framework
6. MEC – Mobile Edge Computing
7. FL – Federated Learning
8. ML – Machine Learning
9. CL – Centralized Learning
10. FED – IDS - Federated Intrusion Detection System
11. IDS – Intrusion Detection System
12. VFC – Vehicular Fog Computing
13. VEC – Vehicular Edge Computing
14. KNN – K Nearest Neighbors

III. Existing Architecture

A. *Related Works*

Dajung Zhan et. al.[5] proposed a new framework for blockchain-based, hierarchical multi-access edge computing in VANETs, dubbed BMEC-FV. The framework uses MEC, a low-latency, high-speed technology, to enhance the network services for VANETs. To maintain the security of communication lines between cars, a trust model is put forth, with blockchain and compute offloading in charge of the architecture. In order to solve the joint optimization problem, a novel deep compressed neural network architecture is used. The provided framework protects system integrity while enhancing security, service quality, and throughput. However, the trust model may not be sufficient for complex security threats, and the optimization problem may be problematic for large-scale VANETs. Moreover, the proposed neural network approach might need a lot of computational power, which would limit its applicability.

Elbir et. al.[6] in their paper, emphasized on the use of federated learning (FL) for machine learning (ML) applications in vehicular networks, such as autonomous driving, traffic safety prediction, and object identification, is discussed in this article. Due to the enormous cost that the current industry standard of centralized learning (CL) entails, FL is a desirable alternative that preserves privacy. The applicability of FL for ML-based vehicle applications is explored while identifying learning and communication challenges, and recommending future research areas. The suggested FL-based system has benefits such as increased network privacy, improved resource efficiency, and decentralized model training. Challenges such data labelling, model training, data rate, dependability, transmission overhead, privacy, and resource management must be addressed in order to put the concept into practice. Moreover, the system might need a lot of processing power, which would restrict its usefulness.

Moustafa et. al.[7] described in their study, FED-IDS, which is a federated platform for intrusion detection based on deep learning that can identify cyberattacks on the traffic patterns of moving vehicles in smart transportation systems. Using a context-aware transformer network to learn spatial-temporal representations of vehicular traffic flows, the FED-IDS system enables networked vehicular edge nodes to deliver safe, distributed, and reliable training. FED-IDS outperformed cutting-edge techniques in testing using the public Car-Hacking and TON IoT datasets. FED-IDS has a number of advantages, such as improved attack detection performance, performance that is on par with central training environments, and blockchain-secured training and coordination. However, there are several disadvantages that must be considered, such as the requirement for a sizable amount of labelled heterogeneous vehicular data and the effects of a sizable imbalance in training data, and the difficulties that current blockchain systems and their consensus mechanisms must overcome

Zhang Ran[8] present a collaborative intrusion detection model presented in this research uses numerous agents grouped in a hierarchical structure and is flexible enough to respond to threats and changing environments. To make collaborative detection management simpler, the coordination domain concept is presented. The suggested model offers a number of benefits, including the capacity to pick up on suspicious behaviors that conventional systems would miss, adaptability to changing environments, and a theoretical foundation for the creation of flexible intrusion detection systems. The paradigm does, however, have several drawbacks, such as the production of enormous volumes of data, the need for powerful processing, and high-bandwidth communication between agents. The caliber of the tasks and the precision of the analysis of suspicious behaviour determine how well the model performs.

Lee et. al.[9] investigate system architectures for addressing the computing requirements of contemporary intelligent transportation systems, such as vehicle platooning and autonomous driving. While vehicular edge computing (VEC) and vehicular fog computing (VFC) have been proposed to decrease latency in vehicle communications, mobile edge computing (MEC) and mobile cloud computing both have drawbacks. With the expectation that next-generation communication technologies would increase their effectiveness, research is currently being done to improve the vehicular work offloading settings in VEC and VFC designs. The lack of load balancing in VEC architecture, the lack of a clear framework for compatibility in VFC architecture, and the high cost and maintenance of numerous edge nodes and communication facilities are some of the disadvantages of VEC and VFC.

Selamnia et. al.[10] Using the federated learning (FL) technique, which enables distributed machine learning model construction without centralised data storage, the study suggests a new intrusion detection system (IDS) for cellular vehicle-to-everything (C-V2X) networks. The recommended method makes use of edge computing to accomplish low latency intrusion detection while conserving network resources. The suggested system has the ability to recognise numerous threats, such as D.O.S, DDoS, and botnets, while also accounting for reaction time and protecting data privacy. Although employing fewer network resources, the system detects assaults more precisely than previous systems. The recommended FL-based IDS for C-V2X networks has some shortcomings, although these limitations are not fully covered in the research. This will be addressed in further work, which will increase the ML model's precision and incorporate an unsupervised learning model to detect zero-day assaults, and use transfer learning to cover more attacks.

Brik et. al.[11] propose a clustering ensemble-based unsupervised anomaly detection system for intrusion detection is the suggested system. To precisely cluster data and find abnormalities, it employs iterative K-means runs and a hierarchical clustering tree with a single link. The system's benefits include a high detection rate with fewer false positives and the capacity to recognize clusters with anomalistic structures. Further work is suggested to enhance its capacity to detect novel sorts of assaults utilizing applicable domain information, rule extraction, and a more precise threshold calculation. Nevertheless, its limitations or downsides are not highlighted in the research.

Mohan Krishna et. al. [12] address the crucial problems of privacy and trust in automation systems, notably in transportation systems, the essay suggests using blockchain technology. The suggested remedy, referred to as "P-Chain employing Blockchain Technology," offers improved security and data privacy, a decentralized system for data storage and management, and is affordable, scalable, and effective. In order to ensure the ethical and secure application of Blockchain Technology in transportation systems, the article emphasize the need for additional research to address scalability and compatibility issues, the development of efficient governance models, and the creation of regulatory frameworks.

B. *The Existing System*

The existing architecture includes multiple modalities to solve the identified challenge of security concern for edge computing in vehicular networks. Multiple solutions focus on using custom developed frameworks to introduce decentralization by the means of using blockchain technology, for eg, Zhang et. al. in their paper proposes a solution called BMEC-FV. Other current methods involve collaborative approaches to resolve the presented issue uses collaborative methods like Federated Learning as a means of effective approach. However, information for efficacious application of Federated Learning in the problem along with the issue of addition of new threat into the existing directory has not been addressed.

IV. INFRASTRUCTURE

Infrastructure pertains to the foundational structure or system of physical or digital assets that provides support for a specific activity, procedure, or service. It is composed of various interrelated and mutually dependent components that collaborate to facilitate the operation of a more extensive system or network.

1) *Vehicular Network*

The proposed model is based on a progressive dual-layer architecture, of which the major constituents are the vehicular network's devices and the usage of blockchain technology for the inclusion and maintenance of the highest degree of security through encryption and transparency. In the first layer, vehicles that approach an Road Side Unit area within a specific time frame can obtain a pre-existing intrusion detection network model that has been trained beforehand by the Road Side Unit. The vehicle on receiving model, uses its own data collected data to test & retrain the model on the new found data. Proceeding to the next and the final layer, the Road Side Units receive the retrained model from every vehicle crossing it. It then aggregates the models for acquiring the master model. The blockchain, which stores the master model is jointly maintained by all the Road Side Units contributing to the blockchain. This method ensures timely renewal and verification of integrity.

1.1) Road Side Units

Road Side Units or RSU’s are the constituents of the block chain network that are processors for the edge machine learning models. RSU’s in the infrastructure act as consensus nodes. Multiple road side units collectively maintain a blockchain based intrusion detection model. Collection of the edge machine learning models to train a new aggregation model also happens on the RSU’s where in several RSUs engage in a competition to validate the transactions and aggregates the models to form the master model. The road side unit which wins writes the master model into the network for the next update on the vehicles.

1.2) Automobile

The automobiles within the network serve as edge devices. Each automobiles is a dynamic and mobile edge computing device with unique intrusion detection requirements. Equipped with sensors the vehicle generates intrusion detection data that is specific to its movement. When a vehicle enters the range under an RSU area, it asks a pre-trained intrusion detection model from a neighbouring RSU. The vehicle can then use its data to train and update the model and upload the updated model to the RSU. The integrity of the data collected by vehicles is maintained with the usage of Federated Learning as the entire data is not transferred and only the parameters like weights, biases and gradients are transferred.

V. BLOCK CHAIN

Decentralization involves distributing power, control, or authority away from a central entity to a larger group or network of individuals or entities. Decision-making and control are distributed across multiple nodes in a decentralized system, leading to increased transparency, security, resilience, participation, and ownership by the involved parties. Blockchain, a digital, decentralized, distributed ledger, records transactions in a secure and transparent way. Each block contains several transactions and a unique cryptographic code, known as a hash, linking it to the previous block in the chain. Once added to the chain, a block cannot be altered or deleted, making blockchain tamper-evident and resistant to manipulation. This technology is used in various applications, such as cryptocurrency transactions, supply chain management, and voting systems. In the proposed approach for intrusion detection in vehicular networks, roadside units act as mining nodes to collectively maintain a blockchain based intrusion detection model. Vehicles request intrusion detection models from nearby RSUs and use their own collected data for the purpose of training and updating the models, which are then uploaded to the RSUs for aggregation into a new intrusion detection model. The system utilizes a distributed consensus mechanism for transaction verification and security.

VI. Federated Learning

a) Edge Computation Model

Edge computing is a computing infrastructure that is located at the edge of the network, as defined by Shi et al. (2016)[13] in their research. In vehicular networks, edge computing can be used to support various applications and services, including safety-critical applications, intelligent transportation systems, and infotainment services. The most significant advantage of utilizing edge computing in this context is the ability to perform real-time analysis and processing of sensor and camera data from vehicles. This facilitates the development of predictive and collaborative safety applications, which can enhance the efficiency and safety of vehicular networks.

b) Federated Learning

The usage of federated learning is proposed as a decentralized machine learning approach that trains models on local data sources without transferring data to a central server. This technique helps to address privacy and security concerns while enabling scalable machine learning. It has been applied in various domains, including healthcare, finance, and IoT applications.

In vehicular networks, federated learning and edge computing can be used hand in hand to effectively address data privacy and security issues. By leveraging local data processing and collaborative learning, edge devices such as vehicles can train machine learning models without compromising the privacy of the data generated by the vehicles. Edge computing can support federated learning by providing local data processing and reducing the need for data transfer to a centralized server. This can improve the efficiency of the training process and reduce the latency associated with data transfer.

VII. Proposed Architecture

A. Dataset

UNSW NB15 dataset is a network-based dataset is chosen for this study, which for many is a standard benchmark dataset for evaluating intrusion detection system performance.[14] Containing approximately 2.5 million network-based attacks, the dataset was created at the University of New South Wales in 2015. It includes a range of attack scenarios such as DoS, Probing, R2L, and U2R, and is a representative sample of a real-world network environment generated in a controlled lab environment using a virtualized network topology. The dataset is categorized into two subsets: a training set with around 1.8 million records and a testing set with around 700,000 records.

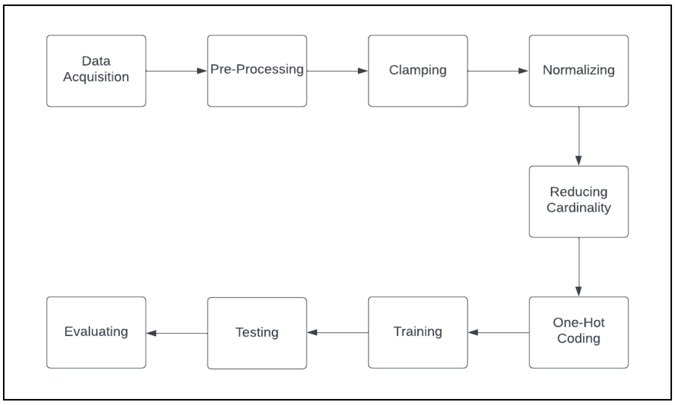

Figure 1
Process Flow Diagram

B. Methodology

The concept though being viable, the mentioned infrastructure isn’t feasible as it has not been developed yet and can be implemented in a smart city only. In the proposed methodology the vehicular models are trained on a static dataset (as mentioned in Section III B. b.) and can be implemented on real-time dataset once the infrastructure is developed.

In order to make sure that the dataset is consistent, accurate, and representative of real-world network traffic, various data pre-processing techniques are used in the first step of training a machine learning model on a dataset. The techniques used in the study include removing of null values and dropping unnecessary or excessive features.

The data is then standardised and extreme values are removed in the subsequent stage of clamping to guarantee that the models operate as effectively as possible. The next step involves the usage of log function to normalise the numbers such that the value fall inside the desired range of the distribution.

Furthermore, it is critical to lower the cardinality of categorical features since high cardinality features might lead to the "curse of dimensionality," which makes it difficult for machine learning models to function properly. It helps solve this problem and also reduces issues that arise in one hot encoding with many values.

The fifth stage involves converting categorical features to numerical values since many machine learning models need numerical data as input. Machine learning models can function more effectively with categorical data when it is represented as a set of binary values using one hot encoding.

Modelling is the sixth phase, where models like logistic regression, KNN, decision trees, Extra trees, and Random-Forest are chosen because they have been shown to work effectively in various machine learning applications especially on intrusion detection tasks.

Evaluation is the final phase of the implementation, where in the models are assessed and trained based on high accuracy, high recall, quick training, and quick prediction. To guarantee that the model accurately predicts both positive and negative situations, accuracy and recall are crucial. Short training and prediction durations are also required since the model has to be able to anticipate events effectively and the deploy time needs to be minimal.

VIII. CONCLUSION & INFERENCES

In conclusion, the study finds that among the five ML models evaluated, the Extra Trees Classifier is the best performing model. This model can be effectively deployed on vehicles as part of a federated learning scenario, with the leader model running on RSUs that act as nodes in a blockchain network. The deployment of ML models on vehicles can provide valuable insights into the transportation system's behavior and enable improvements in safety, congestion reduction, and resource optimization.

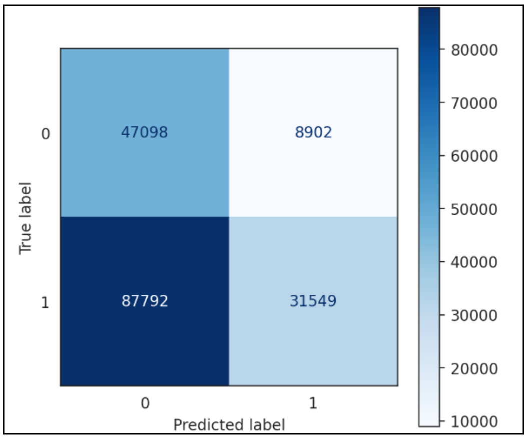

Figure 2
Logistic Regression Confusion Matrix

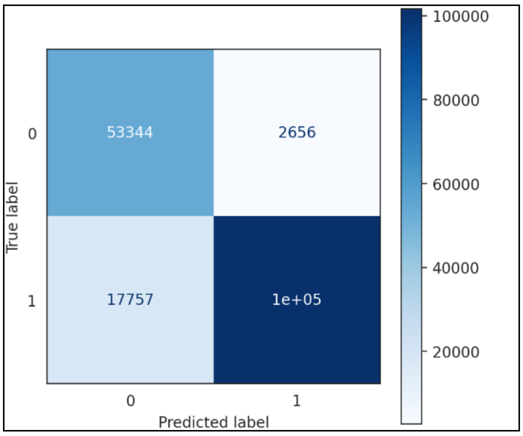

Figure 3
KNN Confusion Matrix

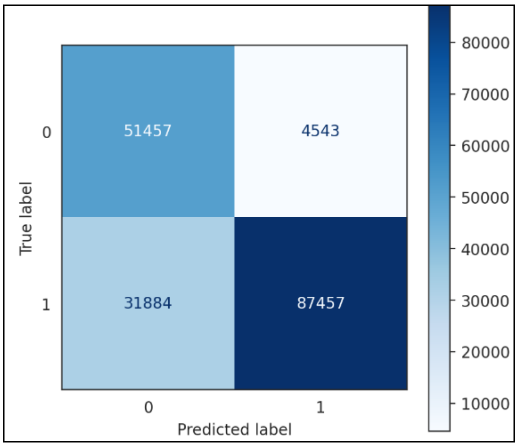

Figure 4
Decision Tree Confusion Matrix

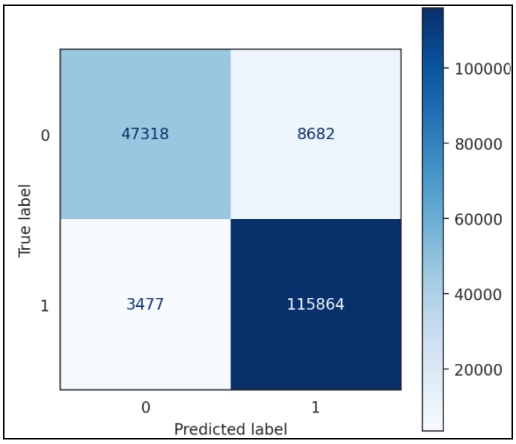

Figure 5
Extra Trees Confusion Matrix

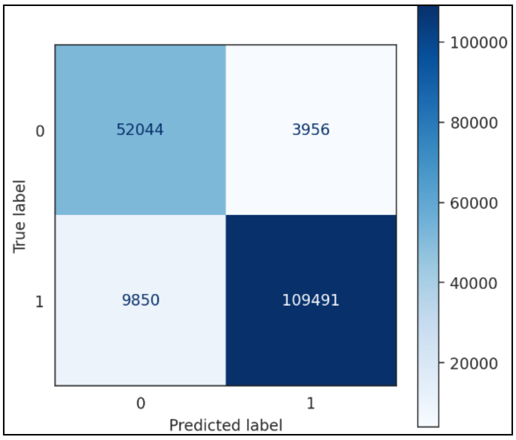

Figure 6
Random Forest Confusion Matrix

Table 1 - Comparison Report of all Chosen Models

Model	Accuracy	Recall	Precision	F1-Score	Time to train	Time to predict	Total time
Logistic	44.85%	26.44%	77.99%	39.49%	0.92	0.01	0.93
KNN	88.36%	85.12%	97.45%	90.87%	0.01	220.09	220.10
Decision Tree	79.23%	73.28%	95.06%	82.76%	1.39	0.02	1.41
Extra Trees	93.07%	97.09%	93.03%	95.01%	2.76	0.42	3.17
Random Forest	92.13%	91.75%	96.51%	94.07%	4.46	0.52	4.98
MLP (Keras)	90.27%	90.27%	90.27%	90.27%	29.66	7.41	37.07
GRU (Keras)	86.29%	86.29%	86.29%	86.29%	76.84	21.16	98.01

The performance metrics of various machine learning models used on the dataset are compared in the table. Accuracy, recall, precision, F1-score, time to train, time to forecast, and overall time are some of these metrics. It was observed that the Extra Trees Classifier had the best accuracy—93.07%—which is significant for this particular experiment. It is also important to note that the KNN model outperformed the Extra Trees Classifier in terms of precision score. However, it is important to understand that for an IDS system which has low accuracy, it may not detect all attacks, leaving the system vulnerable. In contrast, if an IDS system has high precision but low accuracy, it may generate false alarms which can be expensive.

Therefore, for an IDS system accuracy is of paramount importance and thus, Extra Trees Classifier becomes the most ideal model to be deployed on this architecture.

IX. FUTURE WORKS

Based on the conclusions of our study, there are several areas where in future research could improve the proposed schema. In particular, three such areas are observed:

- The development of the infrastructure mentioned for smart road and transportation.
- Block Chain sustainability - development and deployment of blockchain technology in a way that minimizes its environmental impact.
- The Block chain is vulnerable to the 51% attack and development should take place to prevent this for compromising the entire RSU Network.
- On development of mentioned infrastructure, more refined work using Py-Syft can be implemented for worker-leader configurations.

X. ACKNOWLEDGEMENT

We extend our sincere appreciation to our project mentor and professor, Dr. Sandosh S., Assistant Professor at the School of Computer Science Engineering at the Vellore Institute of Technology in Chennai. We are deeply grateful for his unwavering support and insightful guidance during the course of our project.

We would also like to express our gratitude to the Head of Department, the Dean of Academics, and the University Dean for their encouragement and imparting their wisdom to us. We are thankful for the opportunity to take this course and work on this project.

Lastly, we would like to thank our loved ones for their constant support and for being there for us during the project. Their unwavering encouragement and support meant a great deal to us.

REFERENCES

[1] Li, Z., Li, X., & Feng, H. (2021). Security risk analysis of autonomous vehicles and smart road infrastructure. Journal of Advanced Transportation, 2021, 1-11. Yang, Q., Chen, W., & Fang, Z. (2021).

[2] Zhang, L., Song, X., & Lin, H. “Autonomous vehicle navigation with improved accuracy and efficiency. Journal of Advanced Transportation”, 2021, 1-14. (2020).

[3] Zhang, J., Mao, S., Zhang, L., Li, J., Li, X., & Li, Y. (2020). Deep learning-based autonomous driving: A review. Proceedings of the IEEE, 108(10), 1782-1797.

[4] Yang, L., Wang, Z., Chen, Y., Chen, X., Zhang, Y., & Cui, X. (2021). Autonomous driving: Progress and challenges. IEEE Intelligent Systems, 36(3), 10-22.

[5] D. Zhang, F. R. Yu and R. Yang, "Blockchain-Based Multi-Access Edge Computing for Future Vehicular Networks: A Deep Compressed Neural Network Approach," in IEEE Transactions on Intelligent Transportation Systems, vol. 23, no. 8, pp. 12161-12175, Aug. 2022, doi: 10.1109/TITS.2021.3110591.

[6] Ahmet M. Elbir, Burak Soner, Sinem Coleri, Deniz Gunduz, Mehdi Bennis, “Federated Learning in Vehicular Networks”, doi = 10.48550/ARXIV.2006.01412.

[7] M. Abdel-Basset, N. Moustafa, H. Hawash, I. Razzak, K. M. Sallam and O. M. Elkomy, "Federated Intrusion Detection in Blockchain-Based Smart Transportation Systems," in IEEE Transactions on Intelligent Transportation Systems, vol. 23, no. 3, pp. 2523-2537, March 2022, doi: 10.1109/TITS.2021.3119968.

[8] Z. Ran, "A Model of Collaborative Intrusion Detection System Based on Multi-agents," 2012 International Conference on Computer Science and Service System, Nanjing, China, 2012, pp. 789-792, doi: 10.1109/CSSS.2012.202.

[9] J. Lee and W. Na, "A Survey on Vehicular Edge Computing Architectures," 2022 13th International Conference on Information and Communication Technology Convergence (ICTC), Jeju Island, Korea, Republic of, 2022, pp. 2198-2200, doi: 10.1109/ICTC55196.2022.9952556.

[10] A. Selamnia, B. Brik, S. M. Senouci, A. Boualouache and S. Hossain, "Edge Computing-enabled Intrusion Detection for C-V2X Networks using Federated Learning," GLOBECOM 2022 - 2022 IEEE Global Communications Conference, Rio de Janeiro, Brazil, 2022, pp. 2080-2085, doi: 10.1109/GLOBECOM48099.2022.10001675.

[11] A. M. Krishna and A. K. Tyagi, "Intrusion Detection in Intelligent Transportation System and its Applications using Blockchain Technology," 2020 International Conference on Emerging Trends in Information Technology and Engineering (ic-ETITE), Vellore, India, 2020, pp. 1-8, doi: 10.1109/ic-ETITE47903.2020.332.

[12] W. Shi, J. Cao, Q. Zhang, Y. Li and L. Xu, "Edge Computing: Vision and Challenges," in IEEE Internet of Things Journal, vol. 3, no. 5, pp. 637-646, Oct. 2016, doi: 10.1109/JIOT.2016.2579198.

[13] Nour Moustafa & Jill Slay (2016) The evaluation of Network Anomaly Detection Systems: Statistical analysis of the UNSW-NB15 data set and the comparison with the KDD99 data set, Information Security Journal: A Global Perspective, 25:1-3, 18-31, DOI: 10.1080/19393555.2015.1125974

[14] Majeed, I. A., “Comparative assessment of federated and centralized machine learning”, 2022. doi:10.48550/arXiv.2202.01529.

[15] V. Hassija, V. Chamola, V. Gupta and G. S. S. Chalapathi, "A Framework for Secure Vehicular Network using Advanced Blockchain," 2020 International Wireless Communications and Mobile Computing (IWCMC), Limassol, Cyprus, 2020, pp. 1260-1265, doi: 10.1109/IWCMC48107.2020.9148201.