Journal of Neonatal Surgery
ISSN(Online): 2226-0439
Vol. 14, Issue 32s (2025)
https://www.jneonatalsurg.com

OPEN ACCESS

Deep Reinforcement Learning Routing Engine and Threat Detection in Vehicular Networks through Federated Intelligence and Blockchain-Based Trust Ledger

Parveen Akhther. A[1*], A. Maryposonia[2], Prasanth. V. S[3]

[1]Ph.D Scholar, Assistant Professor, Department of CSE,
Sathyabama Institute of Science & Technology, Chennai - 600 119
[2]Professor & Head, Department of CSE,
Sathyabama Institute of Science & Technology, Chennai - 600 119
[3]Ph.D Scholar, Department of ECE,
Sathyabama Institute of Science & Technology, Chennai - 600 119.
[3]Assistant Professor, Department of ECE, Madanapalle Institute of Technology & Science, Andhra Pradesh - 517 325
[*]**Corresponding author:**
Parveen Akhther. A
Email ID: parveena77@gmail.com

Cite this paper as: Parveen Akhther. A, A. Maryposonia, Prasanth. V. S, (2025) Deep Reinforcement Learning Routing Engine and Threat Detection in Vehicular Networks through Federated Intelligence and Blockchain-Based Trust Ledger. *Journal of Neonatal Surgery*, 14 (32s), 1632-1645.

ABSTRACT
Vehicular Ad Hoc Networks (VANETs) defines a self-organizing network formed between vehicles in roadside infrastructure for facilitating real time decision making on road. However in real time trusted updates it can introduce a latency in high vehicular traffic conditions. To address these constrains, developed a blockchain based federated system with intrusion detection to secure the data flow of vehicular environment. Initially, Road Side Unit (RSU) and vehicle contains a Federated Learning Node (FLN), Edge Key Management Unit (EKMU), and access to the Blockchain-Backed Trust Ledger (BBTL). FLN gathers data, trains a local machine learning model and transfers encrypted data to an aggregator. The EKMU creates a lightweight cryptographic key pair and sets attaches a pseudonymized identity and a trust score on the blockchain. Truncated Polynomial Ring Unit (NTPRU) used in EKMU generates a lightweight cryptographic key pair. At the same time, the federated intrusion detection system uses the lightweight XGBoost which continuously monitors traffic patterns and the data points of behaviors while looking for abnormalities (anomalies), such as spoofing, replay attacks, or false-data injections. If found a threat, Federated Intrusion Detection System (FIDS) produces alerts and reports to BBTL. Finally, trust scores are constantly classified using DNN-19 and updated in BBTL. Then the Deep Reinforcement Learning Routing Engine (DRL-RE) can use these updated trust-based metrics to construct secure and adaptive routing decisions. The proposed strategy achieved recall of 97.91%, NPV of 97.62%, error of 2.240% and accuracy of 97.5% respectively. The proposed approach accomplishes secure Vehicular communication for employing a decentralized learning-based approach for enables a real-time threat detection for more resource resilience in intelligent transportation systems.

Keywords: *EKMU; BBTL; DNN; DRL-RE; VANET; Lightweight XGBoost; dynamic vehicular communication.*

1. INTRODUCTION

Vehicular Ad-hoc Networks (VANETs) are a new technology with a lot of potential for advancement [1]. VANETs aim is to develop services that are specifically pertinent to a vehicular context by connecting equipment within automobiles. They try to accomplish this without depending on infrastructure tools to help with network topology management [2]. In order for a vehicle to function, it needs an On Board Unit (OBU) and an application that will allow it to communicate [3]. Additionally, the RSUs that make up the infrastructure components are frequently linked to the internet. Roadside information stations, devices/sensors including GPS-enabled gadgets, vehicles, and a traffic management center (TMC) are the four main parts of a VANET [4]. Wireless communication standards and protocols, which govern the several facets of communication including data transmission range, latency, and security, are used by all of these components to communicate.

In VANET, the process of choosing routes for data transfer from source to destination vehicles is known as routing [5]. In this routing protocol contains several techniques such as Dynamic Source Routing (DSR), Mobile Infrastructure Based VANET Routing Protocol (MIBR) and Geographical Source Routing (GSR) [6]. These techniques all have some more drawbacks which includes in the presence of VANETs' great mobility, the conventional node-centric perspective of the routes results in many broken routes [7]. While, Routing becomes even more difficult when vehicles disconnect for extended periods of time because to obstructions or signal interference and finds it difficult to manage the special features of VANETs, such as their low-latency communication requirements, sporadic connection, and restricted capacity [8].

Researchers may develop a several cryptography techniques to protect data transmission between vehicles and roadside devices while guaranteeing secrecy, integrity, and authenticity based on trust score evaluation [9]. The techniques such Advanced Encryption Standard (AES), Elliptic Curve Cryptography (ECC) and Data Encryption Standard (DES) which may have few limitations they are, strong cryptographic solutions sometimes demand a large amount of memory storage for keys and other cryptographic data, which may be problematic for devices with limited resources and communication delays resulting from encryption time may affect VANETs' ability to provide safety-critical information on time [10]. It may be susceptible to side-channel attacks, in which a hacker takes use of data that has been exposed via the physical implementation. To overcome these several issues proposed an N-th degree Truncated Polynomial Ring Unit (NTPRU) technique for secure data transmission using trust score evaluation and intrusion detection. Major contribution of a work is given below.

- Vehicular communication is secured through federated learning, blockchain, trust management, and deep reinforcement learning.
- Federated Learning Node collects the data and N-th degree Truncated Polynomial Ring Unit (NTPRU) generates a lightweight cryptographic key pair to encrypt the data.
- Federated Intrusion Detection System (FIDS) based on LWXGB is employed to detect the anomaly behavior.
- DNN-19 is utilized to classify the trust score from the Federated Learning Node and update it to Blockchain-Based Trust Ledger.
- Deep Reinforcement Learning Routing Engine (DRL-RE) route the path for vehicle communication based on the trust score.

The remaining sections of the paper are organized in this order: Section 2 reviews the latest research in deep learning, machine learning, and network security-based intrusion detection methods and routing algorithm in VANET. Section 3 provides a detailed explanation of the design of the suggested model. An analysis of the system's evaluation study and results is given in Section 4. The conclusion of the entire study is described in section 5. Limitations and recommendations for further study are provided in Section 6.

2. LITERATURE REVIEW

Numerous techniques based on Routing, intrusion detection and Cryptography in VANET for secure data transmission. Several existing models are reviewed and analysed below,

Kandali et al. [11] have developed the Efficient Clustering Routing approach using a clustering algorithm based on Density Peaks Clustering and Particle Swarm Optimization (ECRDP) model for VANET using Intelligent Machine Learning. The cluster heads are first identified using the PSO method, or the DPC algorithm was used to create a new fitness function for identifying the best solutions. Based on the dependability of the connection parameter between vehicles, clustering was then carried out. After that, a maintenance phase was developed in order to relocate the vehicles inside the clusters and update the cluster heads. Overall stability was demonstrated by a 74% decrease in change rate, performance was improved by a 34% rise in intra-cluster throughput and a 47% increase in inter-cluster throughput, and average latency was reduced by 16% respectively.

Mengistua and Yihunieb [12] have introduced the geo-graphical multicast routing algorithm (GMRA) for performance analysis regarding path selection. This research, evaluated various attack types and offers potential remedies, ensures the security of sensitive data sent between end users and vehicles in UVANETs. Additionally, several newly developed open issues, security concerns, and each node's power was recognized, monitored, and controlled. Compared to GPSR and AODV routing protocols, GMRA has a 10% and 7% higher packet loss, respectively.

Tangade [13] have developed a Trust Management scheme based on Hybrid Cryptography (TMHC) for secure communications in VANET. Shrikant Tangade have developed a Trust Management scheme based on Hybrid Cryptography (TMHC) for secure communications in VANET. Asymmetric identity-based (ID-based) digital signatures and symmetric hash message authentication codes (HMACs) are two components of hybrid cryptography. While the agent trusted authority (ATA) calculates the vehicle's trust-value based on its reward points, the trusted road-side unit (RSU) assesses trust-value. The findings demonstrate that the suggested plan works well and satisfies security criteria. This strategy improved the end-to-end latency by 4% to 15.85%, the compute overhead by 9% to 23%, the communication overhead by 6% to 15%, and the

storage overhead by 7% to 19% respectively.

Nazat et al. [14] have created An Explainable Artificial Intelligence Framework (XAI) for Enhancing Anomaly Detection in Autonomous Driving Systems. This model test the approach on two datasets from real-world autonomous driving. The system uses two XAI techniques to provide both local and global explanations for the black-box AI models. Additionally, providing a two new feature selection methods based on the accuracy of six distinct black-box AI models and the well-liked SHAP XAI approach to determine the salient characteristics that contribute to anomaly identification. It shows that the recommended feature selection methods outperform six cutting-edge feature selection methods on a number of assessment measures. The AI models of Random Forest and AdaBoost which contains the accuracy value of 80% and precision values of 83% and 84%.

Vijayalakshmi et al. [15] have illustrated the Long Short-Term Memory (LSTM) model for intelligent intrusion detection system in VANET enabled car parking system. The research was to prevent Distributed Denial-of-Service (DDoS) assaults, which happen when several users attempt to use the same resources at once, causing collisions and interfering with parking processes. An IDS powered by machine learning (ML) was suggested as a solution to this problem in order to detect DDoS attacks in the smart parking system. With this strategy, the educational institution's parking infrastructure was guaranteed to be organized and methodical. A variety of performance measures were used to simulate and assess the suggested IDS. The Long Short-Term Memory (LSTM) model detected DDoS attacks with 97% accuracy, according to the results.

2.1 Research Gap

According to the evaluations, a number of current approaches which may have some drawbacks including it struggle with high dimensional search space and its convergence rate was slow [11]. Packet transmission delay due to network disconnection [12], computational complexity in the model lead to network instability [13], failing to fully analyze the essential characteristics that show abnormalities and missing to provide adequate explainability for decisions [14], introduce latency and lack of transparency in decision making process leads to inaccurate prediction and struggle to overfitting due to large number of parameters and time consuming [15]. VANETs are susceptible to a number of security attacks from malicious entities. To overcome such drawbacks, the proposed model developed a secure routing model based on federated learning and intrusion detection algorithm using deep learning algorithm.

3. PROPOSED METHODOLOGY

The proposed methodology offers a solid architecture for secure communication in VANETs, which incorporates federated learning, blockchain, trust management, and deep reinforcement learning. The model is comprised of five main entities/units: Federated Learning Nodes, Edge Key Management Unit, Blockchain-Backed Trust Ledger, Deep Reinforcement Learning-Enabled Routing Engine, and Federated Intrusion Detection System (FIDS). The above entities/units must collectively allow for privacy preserving learning, dynamic trust evaluation, and data routing over a mobile and dynamic vehicular communication and learning environment. The detailed process is described as follows

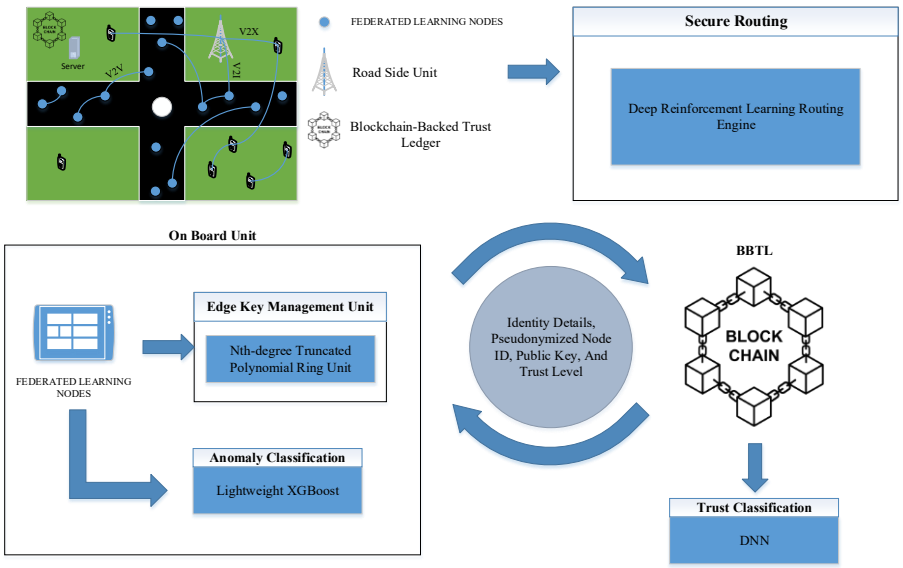

Figure 1. Workflow of the proposed secure routing approach in VANET.

The figure 1 shows the work flow of the proposed approach. The flow of the proposed architecture for secure VANET communication incorporates federated learning, blockchain, and deep learning for dynamic trust management and secure

routing. All vehicle and RSU has Federated Learning Node (FLN), Enhanced Key Management Unit (EKMU) and access to the Blockchain-Based Trust Ledger (BBTL). FLN on each vehicle collects the local data such as driving behavior, sensor readings, and network metrics. Every FLN trains a local machine learning model and transmits encrypted model updates to an aggregator or peers. Upon initialization, the EKMU generates a lightweight cryptographic key pair (Nth-degree Truncated Polynomial Ring Unit) and assigns an initial trust score based on predefined behavioral heuristics. A lightweight Federated Intrusion Detection System (FIDS) based on LWXGB operates in parallel with the FLN to detect cyber threats. FIDS monitors communication and behavior patterns to identify anomalies like false data injection, replay attacks, or routing manipulation. Upon detecting suspicious activity, FIDS triggers a local alert and updates the BBTL with the corresponding incident report. These reports are shared across the network, enabling collaborative and distributed threat awareness. Based on FIDS feedback and observed behavior, the EKMU reevaluates the trust score of each node. DNN-19 are employed to analyze patterns over time, enhancing the accuracy of trust classification. Nodes exhibiting malicious or abnormal behavior are assigned lower trust scores. These updates are committed to the BBTL, allowing other vehicles to make informed decisions based on real-time trust metrics. The Deep Reinforcement Learning Routing Engine (DRL-RE) leverages the latest trust scores, network performance indicators (e.g., latency, packet delivery rate), and routing history to make secure and quality-of-service (QoS) optimized routing decisions. The DRL agent is trained to select communication paths that avoid low-trust or congested nodes while maintaining low latency and high reliability. The blockchain enabled audit trail ensures that all events will be logged and uses for continued learning and auditing for secure, transactional vehicular communication.

Step 1: Node initialization and trust setup

Every vehicle and roadside unit (RSU) provides a Fog Layer Node (FLN), an Enhanced Key Management Unit (EKMU), and a Blockchain-Based Trust Ledger (BBTL) to achieve secure decentralized identity and trust management. In the initialization phase, each EKMU creates a lightweight cryptographic key pair using the Nth-degree Truncated Polynomial Ring Unit, which is suited for efficient cryptographic purposes in resource-constrained vehicular environments. This approach produces secure key generation and encryption in an efficient manner based on its low computational costs. After key generation, the key management unit assigns an initial trust score to each RSU or vehicle based on pre-established behavioral heuristics, including previous communication reliability and default behavior. This initial trust score is normal usable levels of trustworthiness, while providing an initial level of trustworthiness about whether to engage the RSU or vehicle with any sensitive communication. All identity and trust based information provided to each RSU or vehicle node is stored on a tamper-proof BBTL and is accessed in real-time.

- ***Nth-degree Truncated Polynomial Ring Unit:***

The Nth-degree Truncated Polynomial Ring Unit within the Edge Key Management Unit (EKMU) is a lightweight cryptographic engine is designed specifically for secure key generation and management in vehicular networking contexts. The Nth-degree truncated polynomial ring key management unit is a lightweight cryptographic engine based on polynomial rings, whereas polynomials can be truncated to a fixed degree. As a result, it can perform polynomial calculations with minimal computations via modular arithmetic via a polynomial ring. Furthermore, as keys can be truncated polynomial rings, it helps maintain the size of growing keys that would be better suited for on-board vehicular units, which are highly resource-constrained. The polynomial ring functions includes, simple multiplication, addition, as well as polynomials with modulo operations needed for many important cryptographic primitives (e.g., key exchange, digital signatures).

Truncated polynomial rings prevent the unauthorized growing of keys, all while preserving the properties of randomness and uniqueness of the keys, resisting brute-force and algebraic attacks against the polynomials to the point where they are not identifiable. This also includes a way to generate a unique pseudonym where polynomial coefficients combined with identity information. This pseudonym removes the identity of the node while authenticating for the existing vehicle unit. Ultimately, the truncated unit represents an improvement in the efficiency of cryptography, while maintaining the desired security goals and constraints unique to the dynamic context of vehicular networking.

The NTRU public key cryptosystem is one of the fastest known public key cryptosystems. Simultaneously, as a promising candidate for the future post-quantum cryptography standard, lattice-based cryptography enjoys the advantages of strong security guarantees and high efficiency, which makes it extremely suitable for the applications [16]. Due to the constrained resource the lightweight NTRU is used for data encryption in system.

The identity information, including the pseudonymized node ID, public key and trust level, is securely captured on the Blockchain-Backed Trust Ledger (BBTL). Using blockchain technology makes sure that identity management is structured on a decentralized, tamper-proof basis. This avoids unintended changes, maintains integrity, and supports verification, when needed. Trust data is shared across the distributed BBTL network and does not need a central authority to assess the accuracy of an interaction. Decentralization improves the security, reliability and scalability of trust-based interactions in vehicular communication applications.

Step 2: Federated learning and local model training

Federated Learning Node (FLN) is an intelligent decentralized module inside each vehicle that allows on-device learning of

driving behavior, sensor streaming, and network interaction. Instead of sending sensitive raw data (like relaying all vehicle data to the central server), FLNs train machine learning models locally and send model updates only in encrypted form, preserving user privacy. Thus, this reduces communication overhead, and the user maintains data sovereignty. Once local training has completed, model updates will be sent to a central aggregator, or updates may be sent to neighbor FLNs. These encrypted updates will be aggregated to collaboratively update a global model, where the vehicular network benefits from a diverse set of learning experiences while protecting each individual's data with varying degrees of training. This mechanism supports adaptive learning, in real-time environments, that improves the generalization of the machine learning model to a range of traffic scenarios and thereby increases connectedness and intelligence of the autonomous system. Ultimately, FLNs provide the capability for scalable, privacy-preserving, and adaptive learning in vehicular networks.

To improve learning across the system while preserving the privacy of the users. Decentralized training also avoids having to have user data stored in a central repository which can reduce liability with the data breach and increase secure responsive time for updates to the models. The FLN provides on-device learning which keeps the data on-board, making them particularly useful in deployment situations that are critical for privacy such as self-driving vehicle anomaly detection and dynamic traffic prediction systems in smart cities. The local learning processes permit change fast and in real-time in response to local traffic behaviors, road conditions, and user behaviors without challenging data ownership rights. And, as there are continual shared updates from multiple FLNs, a better and stronger global model can be developed. By permitting vehicle-to-vehicle, or vehicle-to-infrastructure collaboration happening from distributed vehicular nodes empowers a better, safer, and more efficient intelligent transportation ecosystem.

Step 3: Intrusion Detection through FIDS

A lightweight, real-time Federated Intrusion Detection System (FIDS) that operates using lightweight XGBoost, runs in tandem with the Federated Learning Node (FLN) to provide robust cyber threat detection in real-time. FIDS uses the lightweight XGBoost is a machine learning algorithm to constantly monitor the behavior of vehicles and cyber threats in terms of patterns of communication, data shared and behavioral flags to search for patterns of cyber threats in terms of false data injection, replay attacks, routing attacks. FIDS will issue local alerts as well as log the incident into the Blockchain-Backed Trust Ledger (BBTL) for incident accounting. Incident data on the car being compromised will be federated out to connected nodes to maintain a distributed collaborative defense and threat intelligence in order to defend the total vehicular network.

- ***Lightweight XGBoost***

XGBoost ('extreme gradient boosting') is a strong type of machine-learning algorithm predicated on gradient boosting decision trees that is efficient, scalable, and flexible. In the context of trust evaluation, XGBoost utilizes behavioral features such as message frequency, anomaly reports, and lag time, to jointly analyze the behavior over time to detect the most significant deviations which displayed an abnormal and malicious pattern over time. As an added benefit, XGBoost is lightweight and produces fast results, which is ideal for deployment in edge environments, like EKMU, allowing for rapid, responsive actions to changes in trust decisions. XGBoost also gives importance scores to features for trust evaluation, allowing users to discriminate feature importance to improve the interpretation of trust decisions. Regularization integrates to avoid overfitting and keeps processing of missing values optimally. The model can also adaptively produce trust scores while continually receiving behavioral data, which is then securely stored on the blockchain for visibility and distributed access and enables adaptive real-time trust evolution, designed to maintain the integrity and security of vehicular networks. The lightweight XGBoost operates at the Edge to detect anomalies, such as false data injection and replay attacks, by monitoring traffic flow and message integrity.

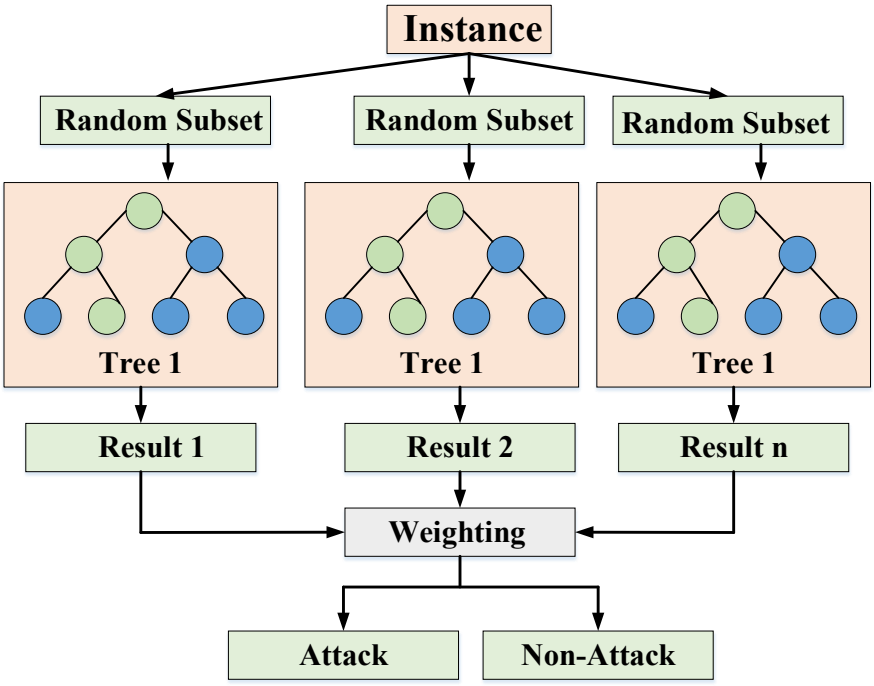

Figure 2. Architecture of Lightweight XGBoost for anomaly detection.

Architecture of Lightweight XGBoost for anomaly detection is depicted in figure 2. XGBoost is a potent toolkit for problems including regression, classification, and ranking [17]. It uses decision trees and ensemble learning to predict labels based on features. For feature selection, XGBoost helps identify important features by regularizing the model to avoid overfitting, improving prediction accuracy and model efficiency as shown below in eqn (1)

$$Obj = \sum_{i=1}^{n} L(y_i, \hat{y}_i^{(t-1)} + f_i\,(x_i)) + \Omega(f_k) \qquad (1)$$

Where, $L(y_i, \hat{y}_i^{(t-1)}$ denotes the loss function by measuring the error, $f_i(x_i)$ represents the model's prediction of the output, $\sum_{k=1}^{t} L$ is the regularization penalty applied to the model parameters, (f_i) denotes the regularization function, Ω represents the constant.

Step 4: Trust score evaluation and update

EKMU adjusts the trust score of each node dynamically, based on FIDS input and observed behavior. It leverages the predictive capabilities of DNN-19, a Deep Learning algorithm which examines behavioral data over a period of time, and provides an improved interpretation from a trust perspective. As a node's malicious or suspicious behavior increases, the trust score assigned to that node decreases. All current trust scores will be safely stored in the Blockchain-Backed Trust Ledger (BBTL), and vehicles will be able to access trust scores accurately and securely in real-time. This trust management mechanism will contribute to managing trust, within the vehicular communication environment, by ensuring compromised or untrusted nodes are not capable of partaking in important communication events with other nodes in the network, thus increasing the resilience and security within the vehicular communication environment.

- ***Deep Neural Network 19***

The Federated Intrusion Detection System (FIDS) designed with DNN19 is a lightweight deep neural network architecture for identifying trust scores in vehicular networks is illustrated in figure 3. It includes a total of 19 layers, which include input layer, hidden layer and output layer, and optimized to recognize patterns concerning communication and behavioral data. The DNN19 operates at the Edge to detect anomalies, such as false data injection and replay attacks, by monitoring traffic flow and message integrity. The federated structure allows for human-in-the-loop collaborative learning without having to share raw data, while preserving the right to privacy and also improving accuracy across all distributed nodes.

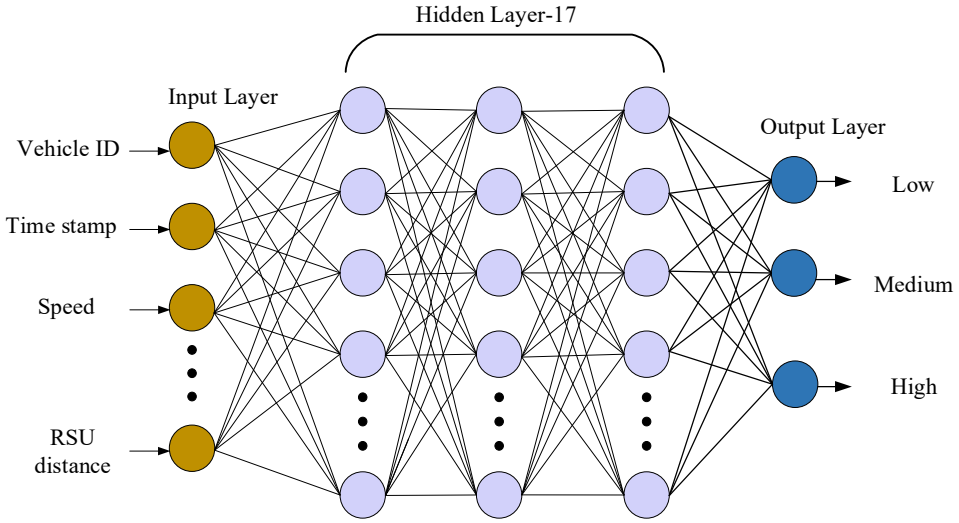

Figure 3. DNN-19 architecture for trust score classification.

DNN model networks with several hidden layers and nodes to automatically extract pertinent characteristics or patterns from data that has been collected. One or more linked artificial neurons make up each network layer [18]. Consequently, the vector provides the input layer I's expression $X = [x_1, x_2, \ldots, x_n]$ as shown below in eqn (2) as seen below

$$h_j = \sum_{i=0}^{n} x_i \times w_{ij} b_j \qquad (2)$$

Where, h_j represents the concealed layer, x_i symbolizes the input layer, w_{ij} is the kernel, b_j represents the bias coefficient.

Step 5: Secure Routing with DRL-RE

Deep reinforcement learning Routing Engine (DRL-RE) uses updated trust scores, real-time indicators of network performance such as latency and packet delivery rate, as well as historical routing data to make informed, secure, and QoS-optimized routing decisions. A DRL agent will continuously learn from the rapidly changing vehicular environment, to select the most optimal communication path to avoid using nodes with low trust scores, unreliable functions, or congested nodes. This enables minimal communication delay and packet loss, while maximizing network reliability. To facilitate routing in situations where sustained performance is critical with respect to both safety and secure operations, like emergency services to promptly get information such as the route to the action discussed earlier, could mean the difference between life and death. The DRL-RE is also pertinent to seamless autonomous vehicular platooning, which depends on the seamless communication between vehicles (V2V) and vehicles conflicting with infrastructure (V2I). There will also be applications of DRL-RE to support the content of the RSU's operations in optimizing V2X exchanges and support smarter and safer coordination along roads or at intersections. The DRL-RE greatly contributes to the resiliency and efficiency of Intelligent Transportation Systems (ITS).

- **Deep Reinforcement Learning Routing Engine**

DRL-RE is a key component for enabling intelligent and secure routing within dynamic vehicular ad hoc networks (VANETs). The concepts of deep reinforcement learning have been integrated into the routing engine allowing the engine to match, or "action," routing strategies that are optimal based on multiple, real-time aspects including trust scores, latency controls, packet delivery stats, availability of nodes, and historical routing performance [19]. DRL-RE does not utilize any fixed or predefined routing strategies, but rather learns through ongoing, micro-level experiences within the network as the environment continues to change. The DRL-RE implements an agent that interacts with a vehicular network environment and receives rewards and penalties based on its routing decisions. The agent is trained to achieve rewards and maximize cumulative rewards based upon the driver environment. The agent learns and improves routing, accuracy, reliability, and security over time. Low trust or compromised nodes are determined from the FIDS (Federated Intrusion Detection System) and trust measurement and are disqualified from routing decisions, thereby preventing adversaries from affecting critical communication flows.

DRL-RE enhances the functionality of Road Side Units (RSUs) by efficiently managing Vehicle-to-Everything (V2X) communications. It optimizes data exchange between vehicles and infrastructure, especially at critical points like intersections and highways. By learning from environmental feedback, DRL-RE ensures adaptive, context-aware routing decisions that contribute to minimal delays and improved traffic coordination. This intelligent routing approach bolsters the resilience, safety, and responsiveness of Intelligent Transportation Systems (ITS), even under high traffic density or dynamic

conditions. Overall, DRL-RE ensures reliable and secure vehicular communication essential for real-time transportation operations.

Step 6: Continuous Learning and Blockchain Logging

All routing decisions, trust updates, and intrusion alerts generated by various components in the vehicular network are always logged in the Blockchain-Based Trust Ledger (BBTL). BBTL provides continuous logging to ensure all security and communication events across the network are auditable in their entirety. The BBTL logs every action for each node and creates a verifiable and immutable record, enabling downstream nodes with a decentralized backbone for trust evaluation, conflict detection, and inconsistency resolution. The record of activity is also meant to highlight or provide a history of repeated malicious action, lend to long-term behavioral analysis, or simply provide a historical view to contextualize the adjustment of short-term or dynamic trust scores. The BBTL leverages the immutable nature of blockchain technology because recorded information once on the ledger cannot be modified or deleted, but provides assurance that critical records will remain trustworthy. Moreover, the ability for authorized nodes to reference that record provides a real-time understanding of information needed for decision-making. Vehicles and infrastructure units can independently assess the trustworthiness of peer nodes before engaging in any sensitive communications. Nothing speaks to security better than guaranteeing that the most trusted nodes are involved in the decision-making process of network.

- ***Blockchain-Based Trust Ledger***

The BBTL is essential in enabling continuous learning and secure logging in the vehicular network. It is a decentralized and tamper-proof record of occurrences of significance, including relevant routing decisions, trust score updates, and reports from intrusion detection systems, for every node in the network. This means that an immutable historical record is readily available, should it be required for auditing, conflict resolution, and behavioral assessment. In continuous learning, the BBTL is a repository for a wealth of useful labeled data that includes previous trust determinations, attack reports and routing results and these can be input into federated learning and machine learning to continue to retrain, improve and update. The system will use historical data from the BBTL to update trust classification procedures, improve threat detection capabilities and adjust routing strategies. The BBTL can be interrogated and used by all authorized nodes, which encourages transparency and real-time node behaviour validation, allowing past issues not be ignored if a node's behaviour becomes malicious or faulty, these behaviours are kept accountable for the long-term. The decentralized nature of the BBTL means that there are no single points of collapse, opening the door for resilient communication between nodes, which is developed through trust before reliability can be assured by sharing data.

4. RESULT AND DISCUSSION

This paper presented a secure routing using Deep reinforcement learning and threat detection in automotive networks using lightweight XGBoost and DNN-19. Lightweight XGBoost is used to detect the anomaly and DNN-19 utilized to trust classification while Deep Reinforcement Learning Routing Engine route the path for data communication. With an Intel Core i5 CPU, 16GB of RAM, and Nvidia GeForce GTX 1650 graphics, the proposed setup is built using Python 3.8.

4.1 Dataset Description

The dataset includes 10,000 data for vehicle communication events, capturing key mobility, communication, and environmental parameters. Key Features of Vehicle Data like Position, speed, acceleration, direction, lane [20]. Then for Communication Data: Signal strength, packet loss rate, latency. Environmental Context: Traffic density, weather, road type.

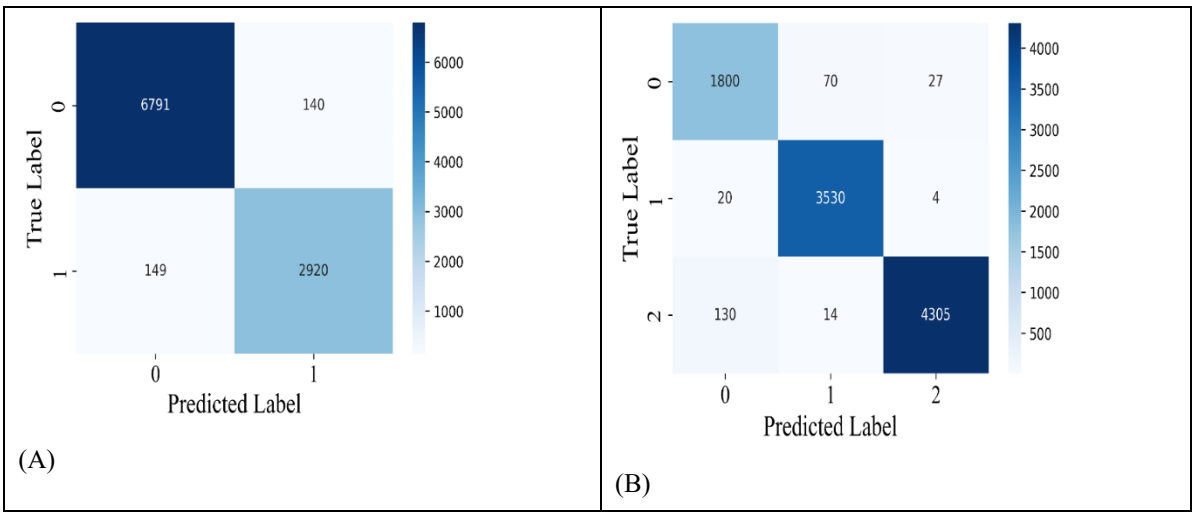

Figure 4. Confusion matrix for the proposed approach (A) Anomaly Classification (B) Trusted Classification.

To assess the accuracy of the classification method, the confusion matrix for two dataset namely Anomaly Classification and Trusted Classification is shown in Figure 4. The effectiveness of the procedure is assessed by the analysis of two distinct classes generated from VANET dataset. For Anomaly Classification, the output classified as Class 0 (attack) received 6791, and Class 1 (non-attack) scored 2920. In Trusted Classification, low Class 0 obtained an outcome of 1800 while medium Class 1 achieved a score of 3530 and high class 2 received as 4305.

4.2 Comparison Analysis for Intrusion Detection and Trusted Classification

The comparison analysis for the Intrusion Detection proposed Lightweight XGBoost (LWXGB) model is compared to a number of current algorithms, such as Deep Neural Network (DNN), Long Short Term Memory (LSTM), Deep Convolutional Neural Network (DCNN) and Robust Support Vector Machine (RSVM) in order to evaluate its effectiveness. Additionally, trust classification is compared with proposed DNN model and existing algorithm such as Bidirectional Long Short-Term Memory (Bi-LSTM), Recurrent Neural Network (RNN) and Artificial Neural Network (ANN). Accuracy, Precision, Recall and Negative Positive Value (NPV) are some of the performance measures used in this comparison. A graph of these factors may be shown below.

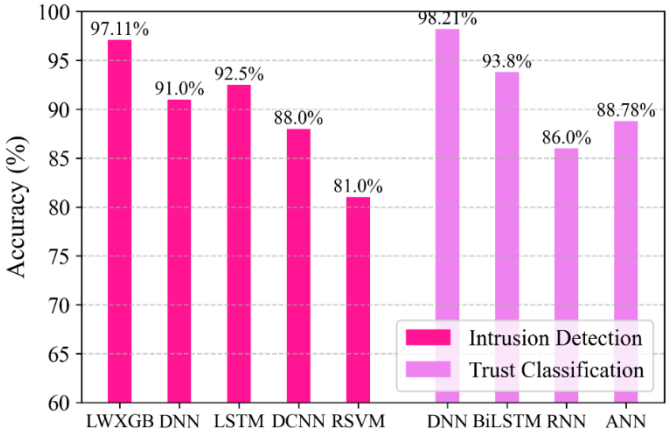

Figure 5. Comparison of LWXGB and DNN Accuracy among different Algorithms.

Figure 5 illustrates the comparative analysis of accuracy using different methods, through the “Intrusion Detection," and "Trust Classification." For Intrusion Detection, the proposed LWXGB method shows the highest accuracy (97.11%), and is still larger than the other methods, which are LSTM (92.5%), DNN (91.0%), DCNN (88.0%), and RSVM (81.0%). Additionally, for Trust Classification, the proposed DNN method shows better performance with an accuracy of 98.21%, compared to otherwise applicable methods like BiLSTM (93.8%), ANN (88.78%), and RNN (86.0%). The proposed methods are primarily concerned with their greater accuracy values, in both titles, and mean it as supporting evidence for their improved means of detecting intrusions and classifying trust levels than conventional ones.

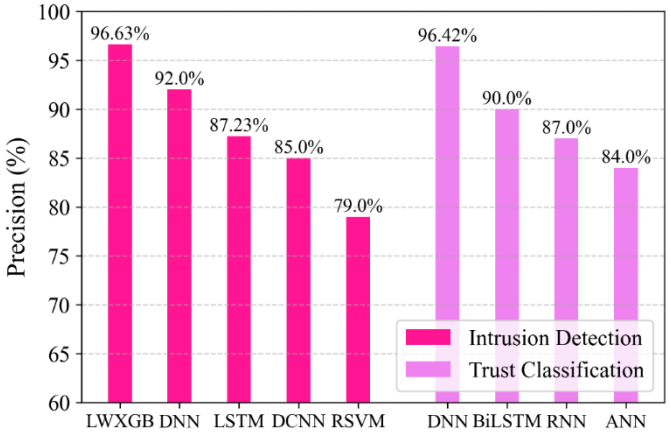

Figure 6. LWXGB and DNN’s precision value in comparison to other algorithms.

Figure 6 depicts the performance of the various algorithms for "Intrusion Detection" and "Trust Classification" regarding the

Precision metrics, as proposed the LWXGB method attains highest precision for Intrusion Detection with 96.63%, compared to DNN (92.0%), LSTM (87.23%), DCNN (85.0%) and RSVM (79.0%). In Trust Classification, the proposed DNN method has the highest precision, achieving 96.42% compared to BiLSTM (90.0%), RNN (87.0%) and ANN (84.0%). This confirms the higher detection precision of proposed methods for detecting threats and assessing trust. The increase in precision guarantees a lowered level of false positives, which establishes more reliability for real time secure vehicular communication.

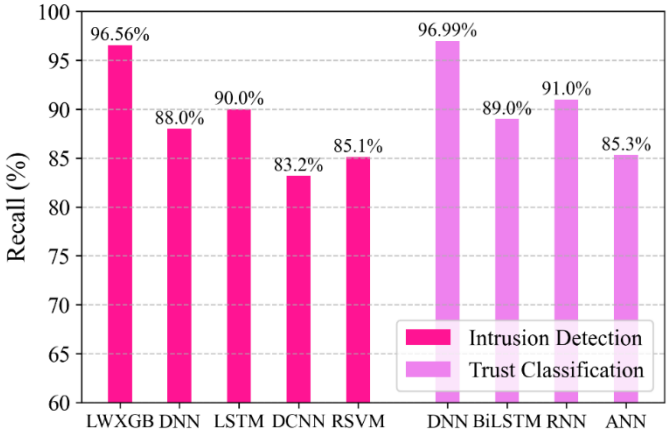

Figure 7. Recall of LWXGB and DNN in comparison to other existing algorithms.

Figure 7 illustrates the Recall values from Intrusion Detection and Trust Classification. The proposed LWXGB for Intrusion Detection had a recall of 96.56% and was significant better than other techniques like DNN (88.0%), LSTM (90.0%), DCNN (83.2%), and RSVM (85.1%). The proposed DNN method for Trust Classification also led with a recall of 96.99%, which was better than BiLSTM (89.0%), RNN (91.0%), and ANN (85.3%). It is quite simply that the proposed LWXGB and DNN models were able to better identify instances in both domains. Both methods had less false negatives which overall assisted them in better image classification and detection tasks.

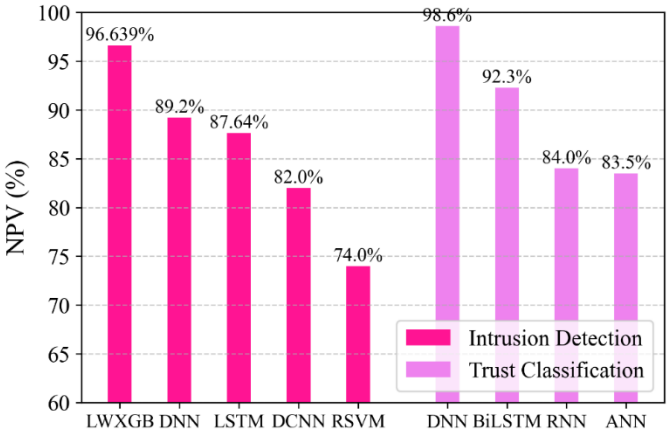

Figure 8. Comparing the NPV value of LWXGB and DNN with various existing methods.

Figure 8 shows the NPV values of the proposed methods for both "Intrusion Detection" and "Trust Classification" that the methods have performed better than other existing methods. The proposed method of LWXGB for Intrusion Detection produced an NPV of 96.639%, which is on the higher end of the existing methods; DNN had an NPV of 89.2%, LSTM had an NPV of 87.64%, DCNN had an NPV of 82.0%, and RSVM had an NPV of 74.0%. Similarly, the proposed method of DNN for Trust Classification had an NPV of 98.6%, while the other methods; BiLSTM had an NPV of 92.3%, RNN had an NPV of 84.0%, ANN had an NPV 83.5%. Since the proposed LWXGB and DNN models produced high NPV values in their respective domains, we can conclude they are effective at accurately classifying true negatives and minimizing false positives to increase reliability in the classification systems.

4.3 Performance Evaluation of Cryptography Approaches

Various cryptography approaches, focusing on security enhancement based on homomorphic cryptography. Other

contemporary algorithms like Modified Optimal Advanced Encryption Standard (MOAES), Multiple Layers of Robust Encryption Algorithms of Lemperl Ziv Markow Algorithm (LZMA), Hybrid Elliptic Curve Cryptography (HECC) and Optimum Oblique Cryptography Algorithm (OOCC) are contrasted with Nth-degree Truncated Polynomial Ring Unit (NTPRU). The effectiveness of the proposed approaches is assessed using a variety of metrics, including decryption, and encryption times.

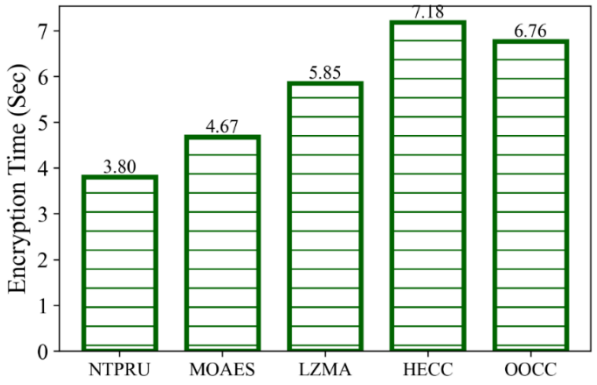

Figure 9. Comparison in Encryption time for other current algorithms.

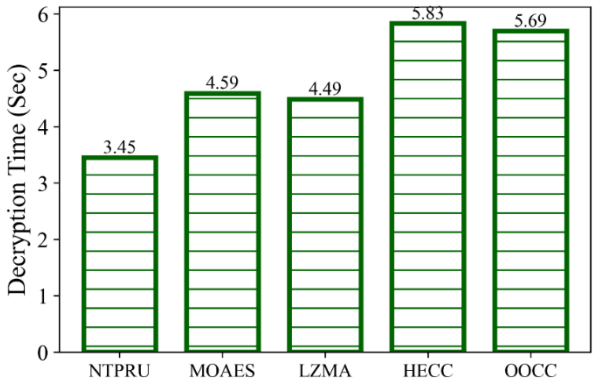

Figure 10. Comparison of Decryption time for proposed and other existing algorithms.

Figure 9 shows a comparison of encryption times. Encryption time approaches contains NTPRU of 3.80 sec, MOAES of 4.67 sec, LZMA of 5.85 sec, HECC of 7.18 sec and OOCC of 6.76 sec. Figure 10, displayed a Decryption time. Decryption time approaches contains NTPRU of 3.45 sec, MOAES of 4.59 sec, LZMA of 4.49 sec, HECC of 5.83 sec and OOCC of 5.69 sec. For both encryption and decryption, the NTPRU recorded the lowest time in every test. It has superior speed than other methods; therefore, the proposed method (NTPRU) is better with respect to processing time for encryption and decryption.

4.4 Comparison Analysis for Routing Algorithm

Performance metrics are used to assess the proposed Deep Reinforcement Learning Routing Engine (DRL-RE) approach and other models, such as Geographical Source Routing (GSR), UAV Assisted VANET Routing Protocol (UVAR), Optimized Link State Routing (OLSR) and Efficient Clustering Routing approach using a new clustering algorithm based on Density Peaks Clustering and Particle Swarm Optimization (ECRDP). The proposed method implementations are compared with the existing methods in order to assess the network performance metrics involving Latency, Jitter, Throughput and Trust score.

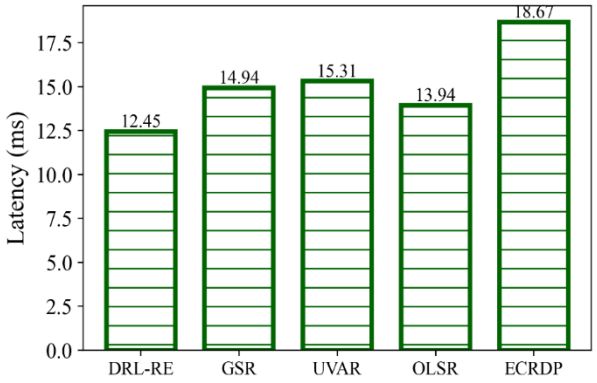

Figure 11. Comparison of the proposed DRL-RE Latency with existing approaches.

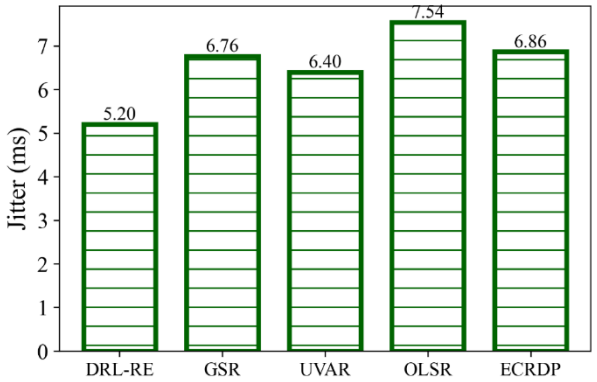

Figure 12. Analysis of the Jitter for the proposed DRL-RE and existing approaches.

Figure 12 exhibits the Latency determination of the proposed DRL-RE algorithm and the existing models, GSR, UVAR, OLSR and ECRDP. The value measured using the proposed DRL-RE approach is 12.45ms while the values produced by the existing methods include GSR, UVAR, OLSR and ECRDP are 14.94ms, 15.31ms, 13.94ms and 18.67ms. Consequently, compared to the other approaches, the DRL-RE value produced by the proposed approach is higher. In terms of data transmission efficiency, the proposed DRL-RE methodology performs better than current methods. Figure 10 shows an analysis of the Jitter for both the DRL-RE and the current model. The results for GSR, UVAR, OLSR and ECRDP techniques are 6.76 ms, 6.40 ms, 7.54 ms and 6.86 ms respectively, yet the proposed DRL-RE strategy yields a result of 5.20 ms. DRL-RE has a high Jitter than the other models.

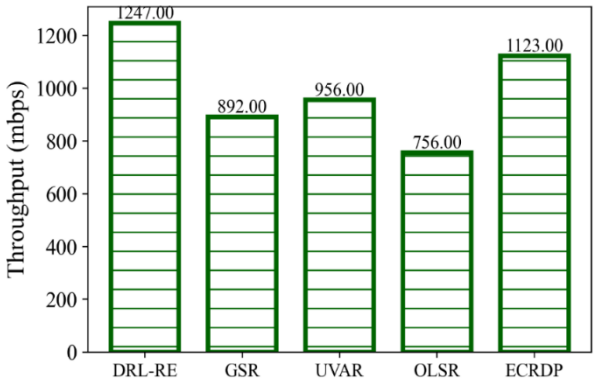

Figure 13. Throughput analysis for both proposed and existing model.

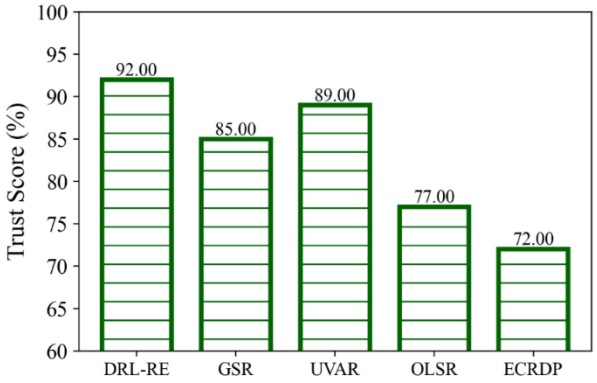

Figure 14. Comparison of the proposed DRL-RE's Trust Score with existing approaches.

Figure 13 shows an analysis of the Throughput for both the proposed DRL-RE and the current model. The results for GSR, UVAR, OLSR and ECRDP techniques are 892 mbps, 956 mbps, 756 mbps and 1123 mbps, respectively, yet the proposed DRL-RE strategy yields a result of 1247. DRL-RE has a high Throughput than the other models. Figure 14 exhibits the Trust Score determination of the proposed DRL-RE algorithm and the existing models, GSR, UVAR, OLSR and ECRDP. The value measured using the proposed DRL-RE approach is 92% while the values produced by the existing methods include GSR, UVAR, OLSR and ECRDP are 85%, 89%, 77% and 72%. Consequently, compared to the other approaches, the DRL-RE value produced by the proposed approach is higher.

5. CONCLUSION

Communication between trusted vehicles is necessary for vehicular ad hoc networks (VANETs). VANET is a multi-dimensional network where the vehicles are constantly moving around. Secure routing is required during the routing procedure to ensure mutual trust among these nodes. Other times, the malicious node broadcasts false information to other nodes. Building trust is difficult when one or more fraudulent nodes try to interfere with the network's ability to find routes or send data. To address these concerns, the proposed model developed a secure routing for data transmission in VANET using deep reinforcement learning route engine through Federated Intelligence and Blockchain-Based Trust Ledger. All vehicle and RSU has FLN, EKMU and access to the BBTL. FLN on each vehicle collects the local data such as sensor readings, driving behavior, and network metrics as well as trains a machine learning model, sharing encrypted updates for aggregation along with NTPRU creates a lightweight cryptographic key pair for encryption. In parallel, a lightweight FIDS using LWXGB for monitoring and detecting the threats such as replay attacks, data injection or routing manipulation. It triggering alerts and logging reports to BBTL. Node Trust scores are reevaluated by EKMU on the basis of FIDS feedback. DNN-19 classifies the trust score over time and malicious nodes receives trust score is updated in BBTL. The Deep Reinforcement Learning Routing Engine (DRL-RE) gets the updated trust metrics, routing history and network condition for making decision to secure and optimal routing for vehicle communication that avoids unreliable and congestion nodes while maintaining low latency and high reliability. The performance metrics for proposed model is compared with existing models and the obtained values for proposed model are accuracy of 97.11%, 98.21%; precision of 96.63%, 96.42% for anomaly and trust classification as well as latency time is 12.45ms, throughput is 1247mbps. Thus the proposed model performs better than other existing models.

5.1 Limitation and Future Scope

The adaptation of trust scores in highly volatile environments can lead to the dynamic trust score being sensitive to misclassifying trust decisions. In future, the architecture may enhance the design using Quantum Secure Communication protocols while introducing proposed task categories to resist attacks at quantum levels. Another option may utilize a hybrid approach using Blockchain-DAG (Directed Acyclic Graph) for enhanced throughput and scalability. Also, embracing Explainable AI, when designing a form of trust, could allow for closing the loop of greater transparency and enhance the organizations confidence in the decisions being made by the system. These continued enhancements could offer more extensive improvements for privacy, performance, and trustworthiness in VANET communications.

REFERENCES

[1] Alharthi, A., Ni, Q., & Jiang, R. (2021). A privacy-preservation framework based on biometrics blockchain (BBC) to prevent attacks in VANET. *Ieee Access*, *9*, 87299-87309.

[2] Bibi, A., Jabbar, S., Saeed, Y., Iqbal, M. M., Ahmad, A., Akbar, H., & Qureshi, I. (2024). TR-Block: a trustable content delivery approach in VANET through Blockchain. *IEEE Access*.

[3] Ali, A., Iqbal, M. M., Jabbar, S., Asghar, M. N., Raza, U., & Al-Turjman, F. (2022). VABLOCK: A blockchain-

based secure communication in V2V network using icn network support technology. *Microprocessors and Microsystems*, *93*, 104569.

[4] Gayathri, M., & Gomathy, C. (2022). AI-TASFIS: an approach to secure vehicle-to-vehicle communication. *Applied Artificial Intelligence*, *36*(1), 2145636.

[5] Chandramohan, K., Manikandan, A., Ramalingam, S., & Dhanapal, R. (2024). Performance evaluation of VANET using directional location aided routing (D-LAR) protocol with sleep scheduling algorithm. *Ain Shams Engineering Journal*, *15*(3), 102458.

[6] Abualola, H., Otrok, H., Mizouni, R., & Singh, S. (2022). A V2V charging allocation protocol for electric vehicles in VANET. *Vehicular Communications*, *33*, 100427.

[7] Ali, I., Chen, Y., Ullah, N., Kumar, R., & He, W. (2021). An efficient and provably secure ECC-based conditional privacy-preserving authentication for vehicle-to-vehicle communication in VANETs. *IEEE Transactions on Vehicular Technology*, *70*(2), 1278-1291.

[8] Sepasgozar, S. S., & Pierre, S. (2022). Network traffic prediction model considering road traffic parameters using artificial intelligence methods in VANET. *IEEE Access*, *10*, 8227-8242.

[9] Singh, G. D., Prateek, M., Kumar, S., Verma, M., Singh, D., & Lee, H. N. (2022). Hybrid genetic firefly algorithm-based routing protocol for VANETs. *IEEE Access*, *10*, 9142-9151.

[10] Sharma, M., Kumar, P., & Tomar, R. S. (2022). Weight-based clustering algorithm for military vehicles communication in VANET. *SAIEE Africa Research Journal*, *114*(1), 25-34.

[11] Kandali, K., Bennis, L., El Bannay, O., & Bennis, H. (2022). An intelligent machine learning based routing scheme for VANET. *IEEe Access*, *10*, 74318-74333.

[12] Mengistu, F. G., & Yihunie, H. D. (2024). Performance analysis of path selection routing protocol for UVANET based on geographical multicast routing algorithm. *Cogent Engineering*, *11*(1), 2311526.

[13] Tangade, S., Manvi, S. S., & Lorenz, P. (2020). Trust management scheme based on hybrid cryptography for secure communications in VANETs. *IEEE Transactions on Vehicular Technology*, *69*(5), 5232-5243.

[14] Nazat, S., Li, L., & Abdallah, M. (2024). XAI-ADS: An explainable artificial intelligence framework for enhancing anomaly detection in autonomous driving systems. *Ieee Access*.

[15] Vijayalakshmi, S., Bose, S., Logeswari, G., & Maheswaran, N. (2025). Smart parking: intelligent intrusion detection system in VANET enabled car parking system. *Automatika*, *66*(2), 281-299.

[16] Wang, W., Huang, H., Yin, Z., Gadekallu, T. R., Alazab, M., & Su, C. (2023). Smart contract token-based privacy-preserving access control system for industrial Internet of Things. *Digital Communications and Networks*, *9*(2), 337-346.

[17] Kazemi, M. M. K., Nabavi, Z., & Armaghani, D. J. (2024). A novel hybrid XGBoost methodology in predicting penetration rate of rotary based on rock-mass and material properties. *Arabian Journal for Science and Engineering*, *49*(4), 5225-5241.

[18] Keleko, A. T., Kamsu-Foguem, B., Ngouna, R. H., & Tongne, A. (2023). Health condition monitoring of a complex hydraulic system using Deep Neural Network and DeepSHAP explainable XAI. *Advances in Engineering Software*, *175*, 103339.

[19] Chen, Y. R., Rezapour, A., Tzeng, W. G., & Tsai, S. C. (2020). RL-routing: An SDN routing algorithm based on deep reinforcement learning. *IEEE Transactions on Network Science and Engineering*, *7*(4), 3185-3199.

[20] Dataset1:Python Developer [12-06-2025] (kaggle): [https://www.kaggle.com/datasets/programmer3/vanet-threat-dataset] Accessed on 12-06-2025