scientific reports

OPEN

A secure and efficient blockchain enabled federated Q-learning model for vehicular Ad-hoc networks

Huda A. Ahmed[1], Hend Muslim Jasim[2], Ali Noori Gatea[3], Ali Amjed Ali Al-Asadi[4] & Hamid Ali Abed Al-Asadi[2]✉

Vehicular Ad-hoc Networks (VANETs) are growing into more desirable targets for malicious individuals due to the quick rise in the number of automated vehicles around the roadside. Secure data transfer is necessary for VANETs to preserve the integrity of the entire network. Federated learning (FL) is often suggested as a safe technique for exchanging data among VANETs, however, its capacity to protect private information is constrained. This research proposes an extra level of security to Federated Q-learning by merging Blockchain technology with VANETs. Initially, traffic data is encrypted utilizing the Extended Elliptic Curve Cryptography (EX-ECC) technique to enhance the security of data. Then, the Federated Q-learning model trains the data and ensures higher privacy protection. Moreover, interplanetary file system (IPFS) technology allows Blockchain storage to improve the security of VANETs information. Additionally, the validation process of the proposed Blockchain framework is performed by utilizing a Delegated Practical Byzantine Fault Tolerance (DPBFT) based consensus algorithm. The proposed approach to federated Q-learning offered by Blockchain technology has the potential to develop VANET safety and performance. Comprehensive simulation tests are performed with several assessment criteria considered for number of vehicles 100, Throughput (102465.8 KB/s), Communication overhead (360.57 Mb), Average Latency (864.425 ms), Communication Time (19.51 s), Encryption time (0.98 ms), Decryption time (1.97 ms), Consensus delay (50 ms) and Validation delay (1.68 ms), respectively. As a result, the proposed approach performs significantly better than the existing approaches.

Keywords Vehicular Ad-hoc networks (VANETs), Blockchain system, Federated Q-learning, Extended elliptic curve cryptography (EX-ECC), Interplanetary file system (IPFS), Delegated practical byzantine fault tolerance (DPBFT).

Vehicle ad hoc networks (VANETs) are a kind of mobile ad hoc network that facilitates communication between automobiles and roadside equipment[1]. Drivers can benefit from the speed and safety that VANETs offer through their convenience and security applications[2]. An ambulance, for instance, may use communication with all other vehicles in the immediate area to establish the fastest path during an emergency, which would speed up the arrival time[3]. Additionally, in a weather-related situation, automobiles might provide real-time information regarding road conditions, assisting drivers in making decisions and possibly lowering the chance of collisions[4]. Applications involving collision avoidance, vehicle-to-vehicle communication, and traffic data in real-time are examples of such applications[5]. Big Data advancements have made it possible for VANETs to collect enormous volumes of unique traffic data, process it with Machine learning (ML)/Deep Learning techniques (DL), and deliver precise, low-latency operations[6]. However, VANETs require improved network safety and increased communication effectiveness[7].

A massive system consisting of many nodes associated with a network including smart vehicles either driven by individuals or their own, infrastructure that has been integrated with V2X communication, mobile computing, and cloud-based computing systems. In an attempt to deliver complex intelligent usage, it depends

[1]College of Computer Science and Information Technology, University of Basrah, Basrah, Iraq. [2]Department of Computer Science, College of Education for Pure Sciences, University of Basrah, Basrah, Iraq. [3]Advanced Electronics and Communication Technology, Istanbul Okan Üniversitesi, Istanbul, Türkiye. [4]Computer Science Department, American University of Science and Technology, Beirut, Lebanon. ✉email: hamid.abed@uobasrah.edu.iq

on a variety of fields including networking, communication, and cyber security. A vehicular system is essentially a flexible portable communication system that allows all required devices to communicate and share data by connecting vehicles and linked gadgets using vehicle-to-everything (V2X) transmission. The communication between a vehicle-to-vehicle (V2V), vehicle-to-pedestrian (V2P), vehicle-to-road (V2R), vehicle-to-cloud, and vehicle-to-infrastructure (V2I) is scenario shown in Fig. 1.

Data processing and secure communication of VANETs are the topic of many recent research efforts on privacy, integrity of data, node verification, and anti-reply assaults[8]. The majority of research has focused on centralized systems where hackers may easily carry out several types of network assaults like identity theft, manipulation of data, or network incapacity[9]. Federated Learning (FL) is vulnerable to inference of membership and network injection assaults, despite having been used to address some of these problems by sequential data storage[10]. Additionally, a number of ML/DL approaches have been applied to data analysis in order to extract significant data from extensive VANET systems[11]. However, many approaches were depend on a centralized server are not scalable, which causes latency and processing overhead to rise as the system expands[12].

The aim is to propose a broader solution, as these shortcomings highlight the necessity for Blockchain is regarded as one of the well-known methods for ensuring security in decentralized systems like VANETs[13]. Specifically, Blockchain-based VANET systems offer enhanced sequential network safety, high data accessibility, high trustworthiness, enhanced traceability, and permanence[14]. Conversely, FL has focused attention on addressing the limitations of data centralization in vital networks like VANETs. In FL, every user trains the local algorithm independently from local information after a centralized server sends an initialized global system to the end individuals[15]. In order to supply the local information the users send their learned model locally to the centralized server[16]. Until the training phase of model efficiency meets the needs of the cloud server, these three phases are repeated numerous times[17]. A deep neural network is utilized in the reinforcement learning technique termed Deep Q-learning to estimate the ideal action value ratio[18]. Federated deep Q-Learning to train an advanced Q-network cooperatively across several devices while protecting data privacy[19]. Hence, Blockchain and FL are two technologies that can assist VANETs in different ways, enhancement in safety, flexibility, and efficiency can be achieved by VANETs through the integration of both systems[20].

Motivation

VANETs offer enormous potential for improving traffic flow, roadway security, and comfort for passengers in the context of future autonomous vehicles. In traffic data, federated learning techniques often rely on a centralized server to spread and collect model variables throughout the training phase. A significant danger arises from the centralized strategy's vulnerability to a single point of entry for assaults. Furthermore, if standard federated learning approaches are unable to sufficiently secure data, then there exists a problem with privacy and data integrity. Blockchain and federated learning strategy integration provide an effective solution to these constraints by enabling total separation and highlighting security, transparency, and confidentiality in information exchange across multiple sets of data. Hence, by combining the components of federated learning with the use of Blockchain,

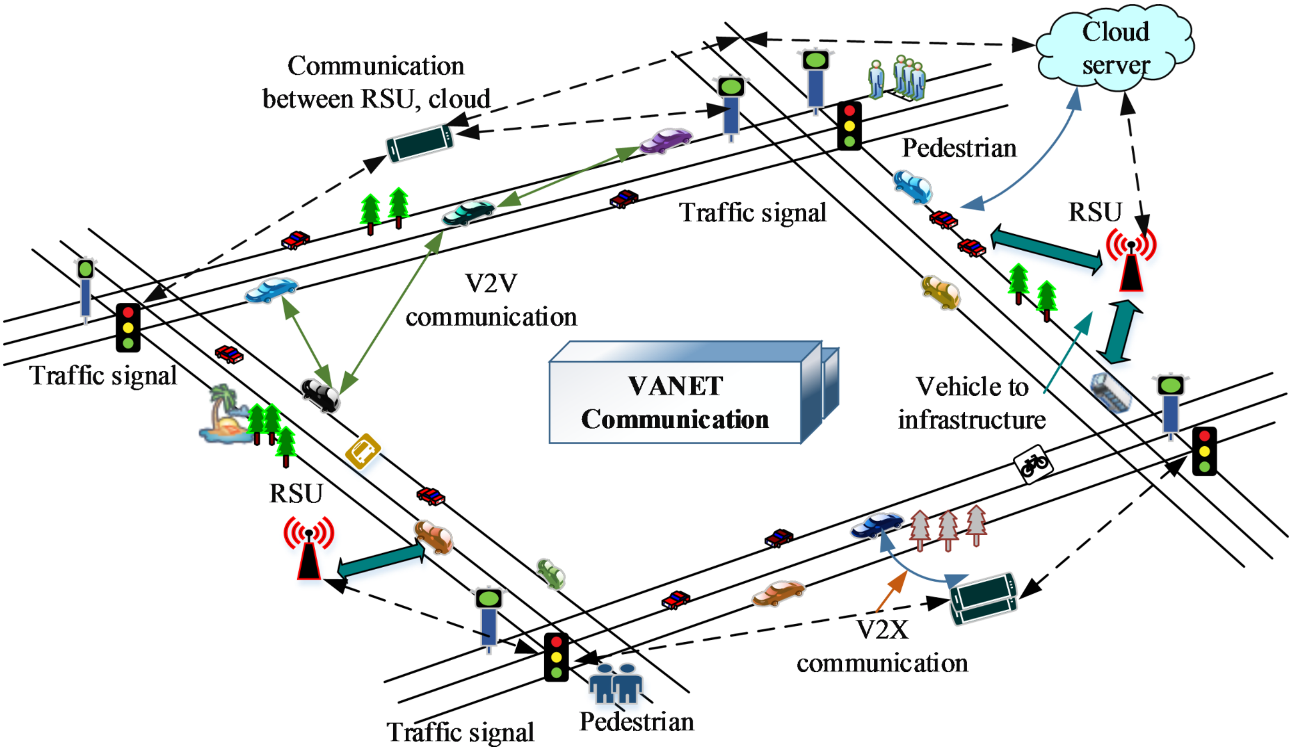


Fig. 1. VANET communication.

the proposed approach aims to provide a more efficient and secure system. By employing efficient consensus systems and extended encryption techniques, which provide data confidentiality, system security, and stability are significantly increased. Therefore, the proposed study enables the creation of a federated Q-Learning model for the VANET system utilizing Blockchain technology. The following is a summary of the major contributions produced by the suggested method:

- To present a Federated Q-learning with secured Blockchain-aided Elliptic Cryptography to prevent assaults in traffic data.
- To propose Extended Elliptic Curve Cryptography (Ex-ECC), an efficient encryption method for increased input data security.
- To develop Federated Q-learning is a novel learning model that is designed to analyze assaults and effective privacy protection.
- To evaluate higher storage and safety is attained by utilizing a Blockchain system, which is verified by a strong consensus algorithm.
- To provide an effective Delegated Practical Byzantine Fault Tolerance (DPBFT) consensus method for Blockchain technology validation.
- To validate the performance of the proposed study by evaluating varied metrics and comparing the results with other existing methods.

The remainder of this study is arranged as follows: Section "Related work" offers a comprehensive literature review, highlighting their limitations and performance metrics. Section "Proposed methodology" considers the proposed methodology discussion with a secure and efficient Blockchain-assisted Federated Q-learning approach. In Section "Result and discussion", the simulation results and brief discussion are presented. Conclusion and future work are described in Section "Conclusion and future work".

Related work

VANETs are a new class of wireless networks that make a world of security and comfort applications for vehicles. It uses Intrusion detection system (TDS) components at several layers to guarantee dependable and secure node-to-node communication. Nevertheless, IDS needs a large volume of information to process in order to detect intrusive network security. Consequently, there was an increase in the amount of traffic, which led to network difficulty. Additionally, Kumar et al.[21] suggested to unique IDS design that combines a random forest (RF) classifier with a local erroneous factor to reduce IDS-generated network activity. The suggested study produced high false negative and positive rates with a low degree of precision.

Vehicular Edge Computing (VEC) was a viable model for placing computing power closer to vehicles, hence enabling low-latency vehicle-to-everything (V2X) applications. Nevertheless, creating the best possible strategy for providing V2X services while guaranteeing security and prompt service delivery was extremely difficult due to the highly dynamic situation of vehicle networks. Fardad et al.[22] introduced to Blockchain-enabled vehicular Edge computing (BEVEC) system to address these issues. BEVEC utilizes a Blockchain with permissions to fuel a dual-layer verification mechanism that guarantees information security and correctness. The effectiveness of BEVEC was measured through a revolutionary system utility function that forms the framework of Blockchain's role within the consensus process. A deep reinforcement Learning (DRL) approach was suggested to maximize utility and allow efficient execution of services in BEVEC. The limits of this study have increased energy use and high delay.

The edge of the automotive network poses significant concerns about service consistency, handling of resources, and adaptability across dynamic vehicular settings. Gharehchopogh et al.[23] presented double Deep Q-networks (DDQN) as a multiple-goals technique. By combining the best features of DL and Deep neural networks (DNNs), this technique allows for dynamic managerial decisions that are adaptive to changing circumstances. The DDQN algorithm's ability to consider numerous objectives enables a comprehensive trade-off analysis, effectively balancing the various objectives to maximize system efficiency. The concept enhances data integrity by utilizing Blockchain technology, which was recognized for safe, decentralized design. This research has a time-consuming and computational cost.

In addition to accurately predicting congestion VANET reliability and quality of service (QoS), Shukla et al.[24] introduced the reliable, enduring, and blockchain congestion reduction system utilizing a variety of deep neural network (DNN), Q-learning and software Define network (SDN) algorithms to produce a precise outcome, fixed infrastructure. In order to create smart cities and connected vehicles, research was mostly focused on global SDN and blockchain technologies. This research has an expensive blockchain system with significant latency.

Multi-Objectives Reinforcement Federated Learning Blockchain (MORFLB) for transport networks was presented by Mohammed et al.[25]. MORFLB detects known and unexpected assaults on data from remote sensing in-vehicle systems with the goal of transmission delays and minimizing processes while optimizing the long-term benefits. MORFLB combines distributed deep neural system formation, proof-of-work mining, and multi-agent protocols. It consists of code nodes, distributed fog, and automotive devices built on lock chain reinforcement federated learning that simplifies benefits through experimentation. For automotive, the research establishes sequential issues that optimize and minimize a variety of parameters.

Single control of access, simple tampering, and simplicity of disclosure are issues with information kept on the Internet of Vehicles (IoV). Li et al.[26] suggested the Blockchain Trust and Weighted Attribute-based Access Control Strategy (BTWACS), a security strategy for the IoV that leverages trust values, blockchain technology, and weighting attribute-related security to address this issue. Firstly, the use of both global and local blockchains to cooperatively manage the formation, verification, and storage of blocks, in order to attain distributed storage of data and guarantee that data can't be tampered with randomly. Second, to create Blockchain-based Trust

Evaluation (BBTE), a Blockchain-related system for evaluating trust. This suggested approach can satisfy the access needs of different groups and functions within the IoV while also significantly lowering the computation and transmission expenses of automobiles.

VANET was attacked through the self-centered On-Board-Unit (OBU) utilizing a variety of approaches in order to make revenue. However, a lot of current techniques rely on the concept of direct cooperation, resulting in simple for massive networks to collapse in the event of an assault. Zhang et al.[27] suggested an indirect reciprocate incentives system based on character to inspire OBUs within the VANET to assist each other, hence reducing the total amount of assaults. In order to guard against information manipulation attempts, which also use Blockchain-based technology to record OBU's actions. Every OBU in VANET has an indirect exchange mechanism that can be thought of as a Markov Decision procedure (MDP). An approach based on Deep reinforcement learning (DRL) was presented to block assault energy to enable OBU training in an evolving environment to produce intelligent choices and communicate properly without recognizing the assault system.

In order to mitigate the privacy preservation problems while analyzing false data injection attack (FDIA) in smart grids, Li et al.[28] have designed a secured federated deep learning is presented. This existing study integrates transformer, federated learning and pailleir cryptosystem for detecting the attacks in secured manner. In this, the transformer is placed in edge nodes which are connected among electrical quantities through multi-head self-attention mechanism. With the aid of federated learning, this study used the data from each node for collaboratively train the deep learning model while securing the data by maintaining it locally. Further, for enhancing the security of federated learning, a novel federated learning scheme is developing by integrating federated learning concept. The simulation results prove the efficacy of utilized federated learning in several scenarios.

Li et al.[29] have presented a novel federated deep reinforcement learning model for forecasting wind power with increased data privacy. This existing study integrates federated learning concept with deep reinforcement learning for maintaining the data privacy and openness while forecasting ultra-short term wind power. Initially, this study introduces deep deterministic policy gradient (DDPG) for enhancing the detection accuracy. After, the DDPG algorithm is integrated with the federated learning framework for attaining precise detection process in decentralized manner by distributing model parameters rather than the private data. The experimental results show that the developed mechanism outperforms other conventional prediction approaches. Comparisons of existing approaches are shown in Table 1.

Many methods are currently been developed to address the security issues with VANET systems. They were unable to provide better outcomes because of their limitations. While many encryption techniques have been employed in several studies to protect data privacy security remained the primary concern. The issues that occur within the area in avoiding harmful attacks and ensuring safety are the main focus of this research. A feasible approach of this study introduces a Blockchain innovation with federated deep Q-learning, which increases the security and effectiveness of the VANET network. Furthermore, research has been done on the efficient technique to prevent assaults, maintain consensus, and prevent specific areas of weakness. Hence, the proposed approach has provided the potential benefits and implementing Blockchain-based federated deep Q-learning in the VANET system. The ultimate goal of enhancing the VANET system's privacy and data security.

Proposed methodology

The transport system, which aims to increase road safety, traffic efficiency, and passenger comfort will mostly be built around VANET Networks. Because, vehicular systems are decentralized, highly mobility, significant security, operates in a hostile environment and communication problems arise for VANET applications.

Authors	Techniques used	Performance metrics	Limitations
Kumar et al.[21]	RF	Accuracy Detection time	High false negative and positive rates with low degree of precision
Fardad et al.[22]	BEVEC	Latency Energy consumption	Increased energy use and high delay
Gharehchopogh et al.[23]	DDQN	Latency Energy consumption Computational cost	Time-consuming and computational cost
Shukla et al.[24]	DNN	Throughput Energy consumption	Expensive blockchain system with significant latency
Mohammed et al.[25]	MORFLB	Delay	Less privacy system.
Li et al.[26]	BTWACS	Accuracy Encryption time	High computational cost and less security system.
Zhang et al.[27]	DRL	Latency Accuracy Energy consumption	Enhanced network congestion
Li et al.[28]	Transformer based FDIA	Accuracy Precision Recall F1-score	Failed to handle DoS attacks and replay attacks
Li et al.[29]	DDPG with federated learning	NMAE NRMSE	Failed to consider the effects of communication delay and packet loss

Table 1. Comparison of existing approaches.

Blockchain has recently been proposed as a solution to a number of VANET problems such as the distribution of reliable, potentially fatal information. Nevertheless, current safety message transmission strategies are ineffective, susceptible to illegal nodes, and predicated on the vast majority of accurate premises. Attackers can join together in the VANET environment to share misleading information that poses a major risk to public safety. This study proposes combining *Blockchain with a Federated Q-Learning (FdQLChain)* to provide an additional layer of security for VANETs. Specifically, to suggest an effective and secure Blockchain-based FL method to guarantee data privacy while ensuring efficient communications in VANETs. Using the FL model for VANETs has effectively reduced the congestion delay and communication overhead. A dependable and secure data communication method between automobiles, roadside equipment, and a cloud server is created viable by combining Blockchain with the FL framework. The block diagram of the proposed methodology is given in Fig. 2.

Initially, generated traffic data is encrypted using the *Extended Elliptic Curve Cryptography (EX-ECC) technique* to efficiently maintain the integrity and security of vehicles. By utilizing the sequential FL model, the proposed model minimizes the long delay and protects from possible threats and attacks that could use EX-ECC. Here, the *Federated Q-learning model* trains the inputs and evaluates the attacks to provide greater privacy preservation. After, the data is securely stored in Blockchain technology. Finally, Blockchain storage is enabled to enhance the security of VANET information through *Interplanetary File System (IPFS) technology*. A consensus technique based on *Delegated Practical Byzantine Fault Tolerance (DPBFT)* is used to validate the suggested Blockchain system. The proposed Blockchain-enabled security mechanism protects the data privacy of users.

Extended elliptic curve cryptography (EX-ECC)

The proposed extended ECC encryption method is utilized to encrypt the data. The ECC method is also more complex and difficult to implement, which raises the possibility of execution errors and lowers the security of the system[30]. This, enhanced ECC is suggested in order to improve security. Normal ECC only generates two types of keys: private and public. Extended ECC generates a secret key in addition to the public and private keys employed in the encryption algorithm and deducted from the decryption ratio. This increases the complexity of the two stages. It becomes extremely difficult to identify the original data if the encryption and decryption complexity is increased. It immediately raises the data's level of security. The extended ECC is represented mathematically by Eqs. (1)–(7),

$$x^2 == y^3 + ay + b \tag{1}$$

Hence, $a\ and\ b$denotes integers. The technique utilized to generate keys in a cryptographic operation determines secure encryption appears.

In the proposed method, three different kinds of keys must be generated. For data encryption, the public key is first generated. A private key is then created in order to decrypt the data. Ultimately, the secret key is constructed using the data points within the elliptic curve, private and public keys. Assume that the point B_s represents the curve baseline. Create a private key Pr_k by selecting a random number from 0 and n-1. Equations (2)–(3) demonstrate the public key was generated.

$$Pu_k = \Pr_k * B_s \tag{2}$$

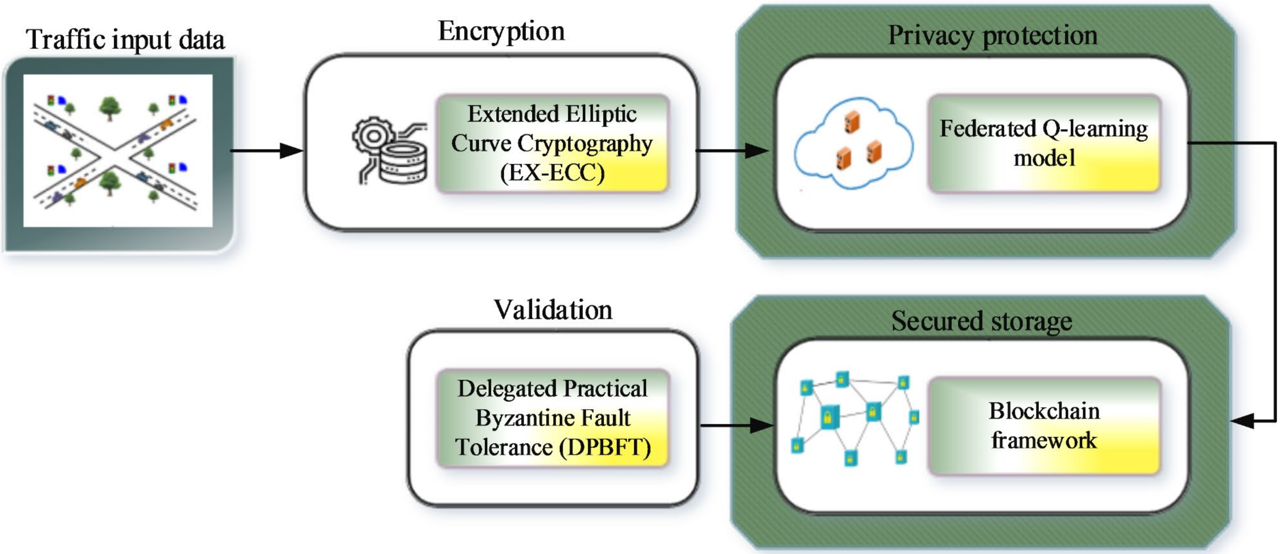

Traffic input data
Encryption
Extended Elliptic Curve Cryptography (EX-ECC)
Privacy protection
Federated Q-learning model
Validation
Delegated Practical Byzantine Fault Tolerance (DPBFT)
Secured storage
Blockchain framework

Fig. 2. Block diagram of the proposed method.

$$Pu_k = \prod (\Pr_k, B_s) \tag{3}$$

Where pu_krepresents a public key, $\Pr_k$indicates a private key, and $B_s$denotes an elliptic curve point. Then,pu_k, $\Pr_k$and B_s are combined to create the secret key, which is expressed as Eqs. (4),

$$S_k = \sum (pu_k, \Pr_k, B_s) \tag{4}$$

Thus, $S_k$represents a secret key. The data points generated from traffic data are encrypted following key generation. Equations (5)–(6) denotes the two cipher texts that are included in the encrypted data.

$$C_1 = (S_1 * B_s) + S_k \tag{5}$$

$$C_2 = M + (S_1 * Pu_k) + S_k \tag{6}$$

Through the decryption process, the original data can be stored. Since decryption was the opposite of encryption as Eq. (7) illustrates the secret key created during the decryption stage is eliminated from the standard equation for decryption.

$$M = ((C_2 - \Pr_k) * C_1) - S_k \tag{7}$$

Where, M denotes original message, S_1denotes random number in the range from 1 and n-1, $C_1\,and\,C_2$ represents cipher text 1 and 2.

Federated Q-learning model

In the proposed VANET systems, where traffic data privacy is particularly essential, identifying and reducing threats through the use of new technologies[31]. Its include Blockchain and federated learning has emerged as a possible method. In the beginning, sensitive data is encrypted to guarantee privacy. The most recent Blockchain-assisted federated learning framework, which integrates the performance of Blockchain with the interactive and secure privacy features of federated learning, receives the encrypted information as input within the proposed approach. The model continuously improves the ability of common data patterns and may identify deviations that can indicate potential attacks by utilizing reinforcement learning methods such as Q-learning.

The adaptability of the system to dynamically alter detection capabilities via adaptive learning strengthens the ability to evolve threats in the traffic sector. Moreover, the Blockchain component is necessary to maintain the federated learning technique's integrity and accessibility. Blockchain technology increases the entire transparency and dependability of the system by maintaining a distributed tamper-proof ledger of system modifications and learning data inputs from multiple users. As a result, federated learning with Blockchain technology facilitates enhanced privacy protection and effectively detects and reduces assaults within the field.

(a) *Reinforcement learning (RL).*

Reinforcement learning is defined as a type of data mining that enhances benefits for environmental vehicle activities by integrating user communication. The Markov Decision Process (MDP) in machine learning uses dynamic computing approaches to determine the most effective plan of action for maximizing rewards with time. RL's key actions are as follows: In order to perform activities and collect data, an individual essentially acts in direct interactions with environments for each of the stages. Second, the surroundings interact with the activity by providing either beneficial or harmful benefits. Third, by detecting alterations in the immediate surroundings, the system maximizes the benefits that are presently acquired. Fourth, in order to raise the probable reward quantity, the RL technique has been applied, beginning with current conditions. With the aid of RL, the researchers created an adaptive neural system for assault detection that is capable of independently identifying new threats.

(b) *Q-learning (QL).*

QL is a reinforcement learning technique in which the system estimates the value performed and updates each of the locations and behaviors for each iteration in order to decide which action *N* delivers the highest reward *R*. The approach is non-adaptive and doesn't depend on models to handle stochastic rewards. The simplest type of system state *S*, operates an action *N*, data reward *R*, and the subsequent state$\hat{S}$, and uses Eq. (8) to estimate the Q value.

$$Q(N_i, S_i) \leftarrow (1-\beta)\, Q(N_i, S_i) + \beta\,(R_i + \gamma \mathrm{max} Q(N_i S_i)) \tag{8}$$

Here, R_i , $S_i and\, N_i$ denotes reward, state, and action at a time *i*, $0 < \gamma < 1$indicates the relative range for rewards, and $0 < \beta < 1$represents learning rate, respectively. Furthermore, a non-adaptive method of stochastic incentives can be taken with Q-learning. Additionally, Q-learning can currently learn by constantly following the rules. The future reward is $K^{\lambda}(S)$ determined as Eqs. (9),

$$K^{\lambda}\left(S\right)=\sum_{N}\lambda\left(N,S\right)\sum_{S+}B_{SS+}\left(N\right)R\left(S,S^{+},N\right)+wK^{\lambda}\left(S^{+}\right) \tag{9}$$

Where $R\left(S,S^{+},N\right)$ represents reward evaluated as state transition, $B_{SS}\left(N\right)$ indicates the possibility of state transition, *w* denotes weight reduction for present and future rewards. Equation (10), $K_{j}^{\lambda}\left(S^{+}\right)$ represents the estimated value $R\,at\,S^{+}$ within the original iteration *j*.

$$K_{j+1}^{\lambda}\left(S\right)=\max_{N}\sum_{S+}B_{SS+}\left(N\right)R\left(S,S^{+},N\right)+wK^{\lambda}\left(S^{+}\right) \tag{10}$$

Hence $K_{j+1}^{\lambda}\left(S^{+}\right)$ represents the computed value of R the modified iteration$j+1$. Also, each iteration can be finished and the number of iterations in reinforcement learning may increase effectively.

(c) *Federated learning.*

The proposed federated learning provides a method for machine learning that permits cooperative approach training by numerous vehicles without requiring users to share their raw data[32]. Rather, clients use their own data to train local methods, only sending upgrades to a central server. These changes are combined through the server to produce a global method, which is subsequently sent back to clients. Figure 3 depicts the procedure of federated learning.

The proposed FL framework assumes that a cloud server *Y*, Road side unit (RSU) (R), a collection of vehicles $V=\{1,2,3,4,?N\}$, trusted regulating authority, and license authority are connected. For taking part in the FL training, every vehicle participating *V* uses local data for size *s*. A set of vectors containing features from a sample of data comprises the input and output pair which forms the training data and every input matrix identified is the output. With each participant vehicle *V*, *Y* the server distributed a global method ωt using *R* communication rounds. The *V* use distributed stochastic gradient descent (DSGD) to train local methods. Following local training, an autonomous communication approach is used to upload and create a local method ω_{t}^{k} to the server *Y*. Where the cloud server creates an entirely new global method ω_{t+1} for further communication round. The required level of convergence is reached then the process is repeated. VANETs' federated Q-learning approach uses node-specific learning updates and adaptive synchronization to adjust to evolving topologies. To minimize disruption to the global model, the model utilizes incremental learning to preserve local updates when nodes join or leave the network. Vehicles can upload their changes after being reconnected due to buffered data storage, which handles temporary disconnections. By applying consensus techniques like DPBFT, which approve transactions even when node involvement varies, the Blockchain ledger maintains the consistency and integrity of the decentralized network while ensuring continuity.

Blockchain-based storage using interplanetary file system (IPFS)

The proposed Blockchain is utilized to facilitate federated learning, ensuring the authenticity of the gathered local data and learned models[33]. The proposed IPFS communication with Blockchain is required to solve the problem of storing huge amounts of VANET information. A distributed, peer-to-peer network for data storage is made possible by a novel protocol known as IPFS. Furthermore, IPFS offers the ability to store large files in a dependable and allocated manner. Figure 4 shows how IPFS allows many peers to share files.

Figure 4a shows the content identifier (CID), also known as the file hyperlink or address, which is an encrypted hashing technique and value for every file uploaded to the IPFS network. Additionally, as shown in Fig. 4b, the file may be accessed and received by other CID persons. In IPFS, each peer serves as a file server, facilitating the quick sharing and storing of enormous volumes of files. A peer may be able to get a record from many data sources, as shown in Fig. 4c.

Because of the distributed strategy, the principal operator cannot alter data. Because the contents of the file have been altered in Fig. 4d, the CID further provides proof for the file's validity. Because of its enormous capability for dealing with the problem of redundant, large data storage in Blockchain, IPFS is regarded as a responsive Blockchain component. Peers have the option to add CIDs to Blockchain activities and save layout files and records into IPFS for the purpose of protecting authenticity and dependability.

Validation using delegated practical byzantine fault tolerance (DPBFT)

The proposed model is validated utilizing the DPBFT consensus procedure. The option of a consensus method for a Blockchain system is critical since it immediately affects features like safety, capacity, centralization, and energy consumption. Due to a number of reasons, the DPBFT consensus method is distinct from other consensus processes including Proof of Work (PoW), Proof of Stake (PoS), and Delegated Proof of Stake (DPoS). Initially, PoW, PoS, and DPoS offer a more scalable, which requires a large amount of processing power. The proposed DPBFT uses a small number of selected delegates to reach consensus, greatly reducing the amount of energy needed and the computational load.

The proposed DPBFT technique is a distributed consensus algorithm defined by phase machine replication[34]. Nodes cannot change messages transmitted by other nodes, and all conversations must be signed by all nodes. Once a client request is issued, it won't be executed again until the previous request has been completed through

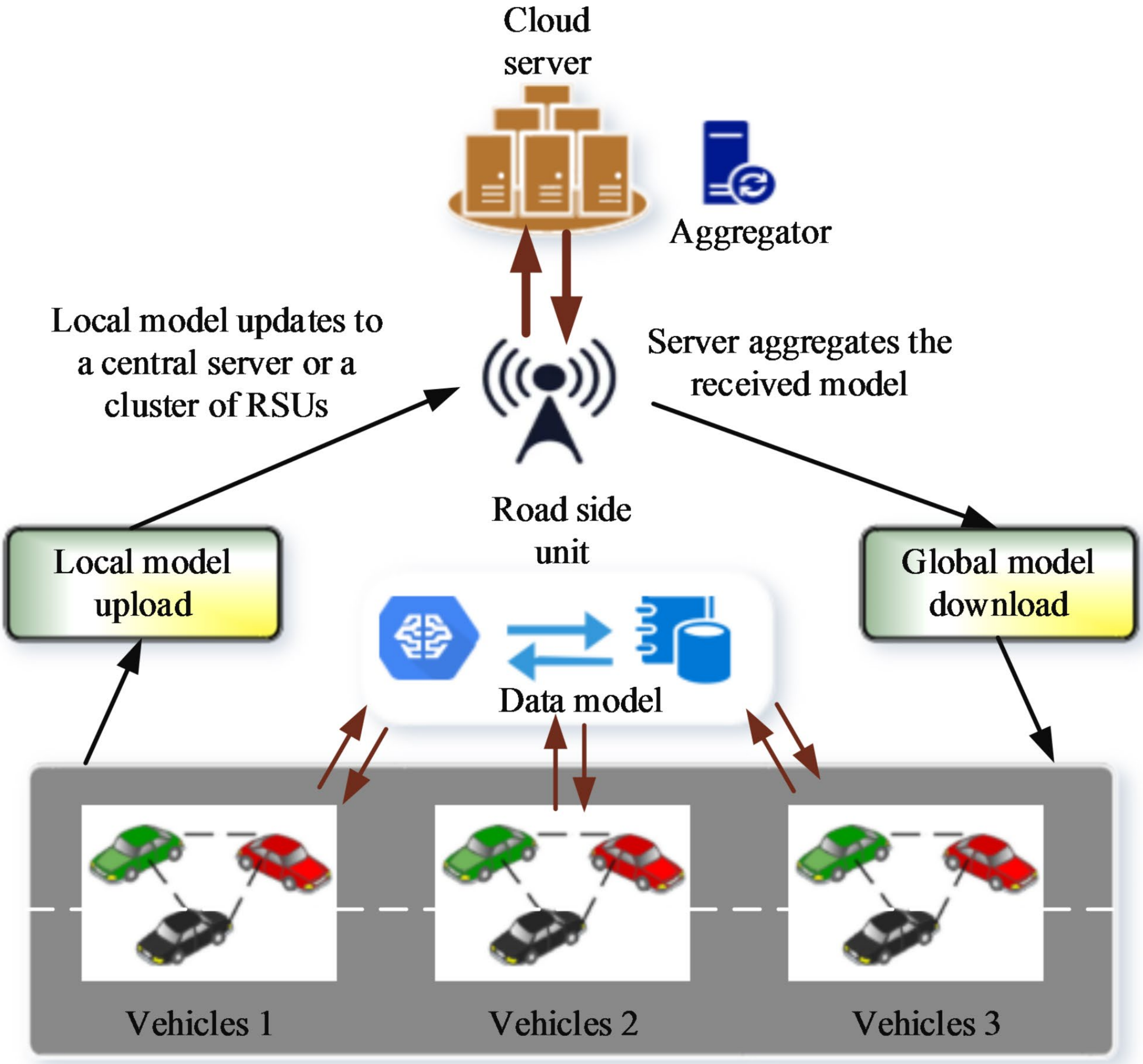


Fig. 3. Process of federated learning.

a network-wide connection. In the DPBFT method, every node operates identically, consisting of a single main node and replica nodes for every other node. The master node is in charge of handling client requests and sending data to the replica nodes in the proper sequence as shown in Fig. 5.

The DPBFT algorithm consists of three basic stages: prepare, commit, and pre-prepare. First, a client sends a request to the main node. The primary NO will then send a Pre-prepare communication to the other nodes after transmitting the client request. After receiving the Pre-prepare data, other nodes initiate the fundamental tri-phase consensus process. The details are as follows:

- *Pre-prepare stage*: The Pre-Prepare signal is sent to the node, which then determines whether to accept the request according to the message items or the number of the request order.
- *Prepare phase*: The node notifies other nodes to get ready after accepting the request. The Prepare stage is finished if, within a predetermined time frame, more than 2f represents the maximum amount of fault-tolerant malicious nodes distinct nodes obtain a train message.
- *Commit phase*: Broadcast commit information to different nodes. The majority of nodes are entering the Commit stage and consensus is established when a 2f + 1 commit message is received. At this point, the node performs the request and transfers the data. The node notifies the client, once the operation has been completed.

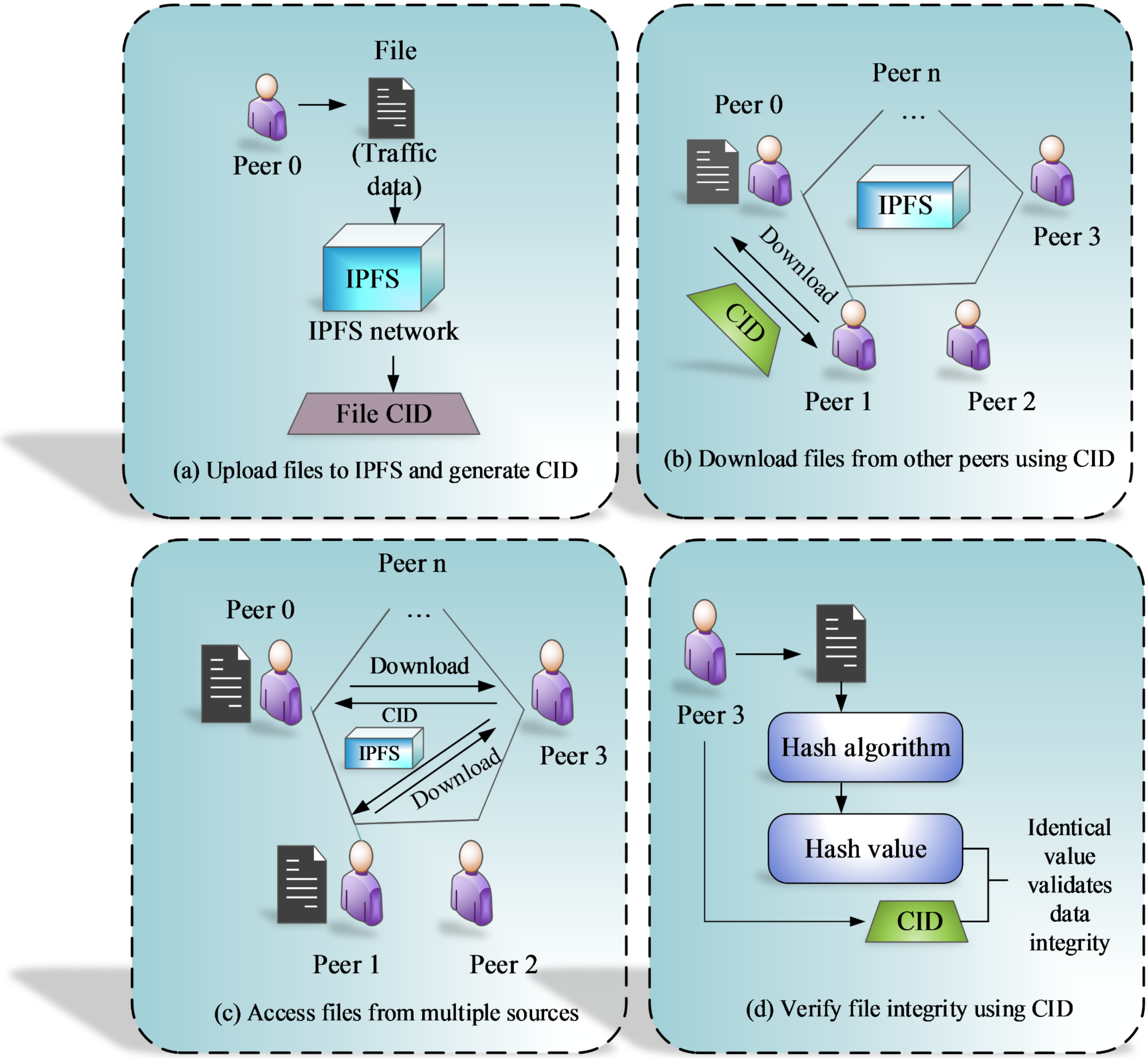

File
Peer 0
(Traffic data)
IPFS
IPFS network
File CID
(a) Upload files to IPFS and generate CID
Peer n
Peer 0
IPFS
Peer 3
Download
CID
Peer 1
Peer 2
(b) Download files from other peers using CID
Peer n
Peer 0
Download
CID
IPFS
Download
Peer 3
Peer 1
Peer 2
(c) Access files from multiple sources
Peer 3
Hash algorithm
Hash value
CID
Identical value validates data integrity
(d) Verify file integrity using CID

Fig. 4. IPFS system: (**a**) Uploading files to IPFS and generate the Content identifier, (**b**) Downloading the files from other peers using Content identifier (CID), (**c**) Accessing files from multiple sources, and (d) Verifying file integrity using CID.

DPBFT is a strong option for systems that need efficiency and security, such as intelligent VANET systems, because it ensures byzantine fault tolerance while maintaining effective transaction authority and block processing.

Result and discussion

In this section, the performance estimation and result analysis of the proposed model are explained. The Intel(R) Core (TM) i7-3770 CPU @ 3.40 GHz with 16 GB of installed memory and a 64-bit operating system is implemented utilizing the MATLAB platform, and no pen or touch input is required. Metrics including communication time, communication rounds, average latency, communication overhead, average accuracy, computational cost, Execution time, consensus delay, Encryption time, decryption time, and throughput are used to assess performance. Additionally, the proposed study was compared to the most recent baseline methodologies.

Performance metrics evaluation

The following computations are performed for the assessment parameters in order to assess the effectiveness of the proposed schemes. To improve transportation systems, increase road safety, and comprehend traffic patterns, transport vehicle details are essential. Initially, traffic vehicle data are created at random and transmitted to

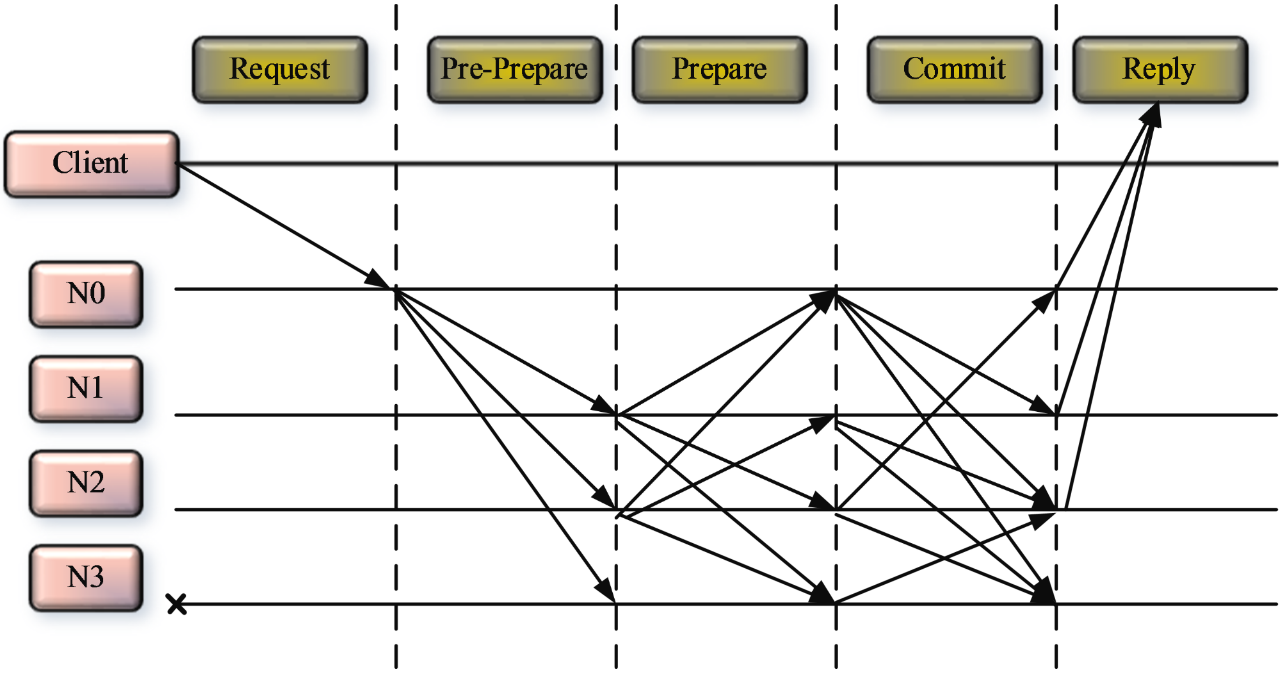


Fig. 5. Structure of DPBFT algorithm.

Parameters	Measurement
Simulation time	1000 s
Network dimensions	3000 m × 3000 m
Number of vehicles	100
Speed of vehicle	60 km/h
Vehicle length	5 m
Vehicle width	3.5 m
RSUs	10
Range of vehicle-to-vehicle transmission	0–350 m
Maximum network bandwidth	3 MB/s

Table 2. Simulation parameters and values.

various locations. These programs gather information regarding network dimensions, number of vehicles, speed of vehicle, etc. Efficient and secure transportation systems can be constructed through efficient data collection, processing, and analysis of traffic vehicle information. Table 2 shows the simulation parameters and values.

The evaluation matrix can be used to establish the performance of the suggested strategy in the following ways:

- *Communication overhead (MB)*: The extra information needed for a process of communication in addition to the actual data transmitted is referred to as communication overhead. It includes a range of elements that lower communication effectiveness.

$$Communication\ overhead = \frac{(Total\ data\ transfered -\ Actual\ data)}{100\%} \tag{11}$$

- *Throughput (KB/s)*: The quantity of data units a device can handle in a specific length of time is known as throughput. It is widely used in a wide range of components, from associations and networks to different parts of gadgets. It can be stated as follows:

$$Throughput = \frac{Total\ packet\ received}{Time} \tag{12}$$

- *Average Latency (ms)*: The average amount of time that a data packet takes for it to move between sources to destination is called average latency.

$$Average\ latency = \frac{Sum\, of\ \ all\, latency\ measurements}{Total\ measurements\ time} \tag{13}$$

- *Encryption time (ms)*: The term encryption time refers to the amount of time it takes a suggested vehicle sector to protect an area of data using a certain encryption process.

$$Encryption\ \ time = \sum (T_{ei})/N_p \tag{14}$$

- *Decryption time (ms)*: The duration required by data to convert an acquired Cipher text data back into plaintext is termed as the decryption time.

$$Decryption\ \ time = N_p/\sum (T_{di}) \tag{15}$$

Where T_{ei} denotes the duration of data encryption, N_p indicates the total amount of data, and T_{di} represents the time required for each data to be decrypted.

Performance evaluation of various methods

This section provides the result analysis and comparison of the proposed model with existing methods in terms of advanced encryption system (AES)[35], Elliptic Curve Cryptography (ECC), Data encryption system (DES), Rivest cipher4 (RC4), and blowfish[36].

In Fig. 6a, the encryption time of proposed EX-ECC is compared with other encryption methods for proving the ability of proposed work. The analysis shows that the proposed method has attained lower encryption time than other existing methods. The proposed method attains 0.98 ms for encryption time. The existing ECC consumes the encryption time of 2.34 ms and the existing blowfish has a higher encryption time than RC4, AES, and DES. The AES approach achieves a value of 4.47 ms, it has taken less encryption time. The DES, RC4, and Blowfish attain values of 8.48, 12.87, and 14.1 ms. Hence, the existing encryption approaches are computationally intensive and impacting performance. So, the proposed encryption offers a secure link for information exchange between vehicle systems. In Fig. 6b, the proposed approach obtains a value of 1.97ms and the existing ECC consumes 2.45 ms for decrypting the data. However, the other existing approaches like AES, DES, RC4 and Blowfish obtains increased decryption time as 3.25, 7.76, 10.56, and 12.78 ms respectively. Existing approaches utilizes more energy that reduces the lifespan of batteries in vehicles. Effective group handling of key methods has the potential to decrease the overhead associated with sharing keys and updates within VANETs, hence improving encryption/decryption times effectively. Also, as compared with conventional ECC, the proposed EX-ECC has attained better outcomes in terms of encryption time and decryption time. The ability of EX-ECC is enhanced by creating additional secret key. This secret key helps to maintain the data integrity and mitigates the complexity problem. Also, the efficiency in EX-ECC speed ups the operation with reduced computational resources than conventional ECC which is proved in Table 3. Table 3 depicts the values of the encryption and decryption algorithm.

A number of assessment criteria highlight the effectiveness of the proposed approach such as FedAvg, Fair, and privacy-preserving deep learning (FPPDL)[37], and Distributed resource allocation method based on Blockchain federated learning approach[38].

The communication time of proposed and existing approaches for varying the number of vehicles are shown in Fig. 7. A total amount of 100 vehicles are considered for the proposed approach. For vehicle data 10, the proposed approach attains a value of 6.32 s, whereas existing approaches are DRAM-BFL, FPPDL, and FedAvg achieving values of 5.53, 4.21, and 2.29 s. For vehicle data 40, the proposed approach attains a value of 10.85 s, the existing approaches are 8.10, 6.78, and 4.66 s. For vehicle data 80, the proposed approach attains a value of 17.62 s, the existing approaches are 11.69, 11.78, and 8.20 s. For vehicle data 100, the proposed approach attains

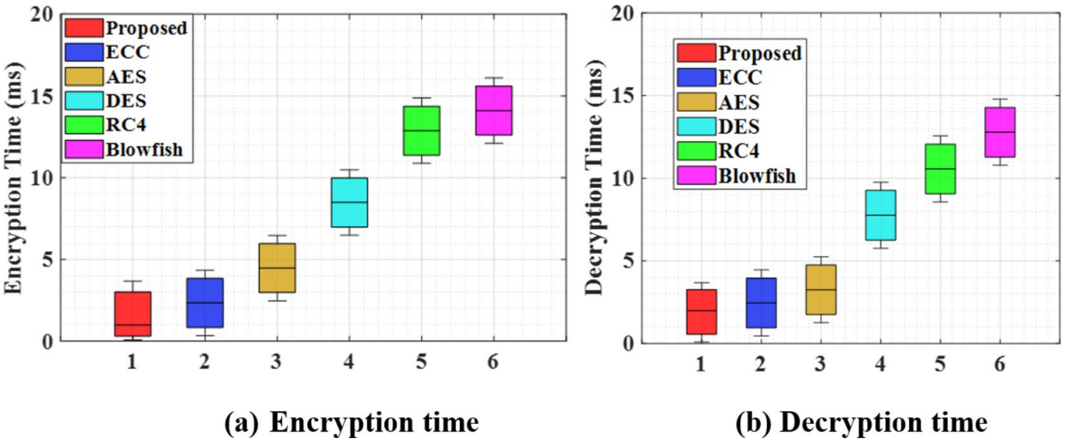


Fig. 6. **a**, **b** Comparison of encryption and decryption time for the proposed model.

Encryption time (ms)					
Proposed	*AES*	*DES*	*ECC*	*RC4*	*Blowfish*
0.98	4.47	8.48	2.34	12.87	14.1
Decryption time (ms)					
Proposed	*AES*	*DES*	*ECC*	*RC4*	*Blowfish*
1.97	3.25	7.76	2.45	10.56	12.78

Table 3. Encryption and decryption algorithm.

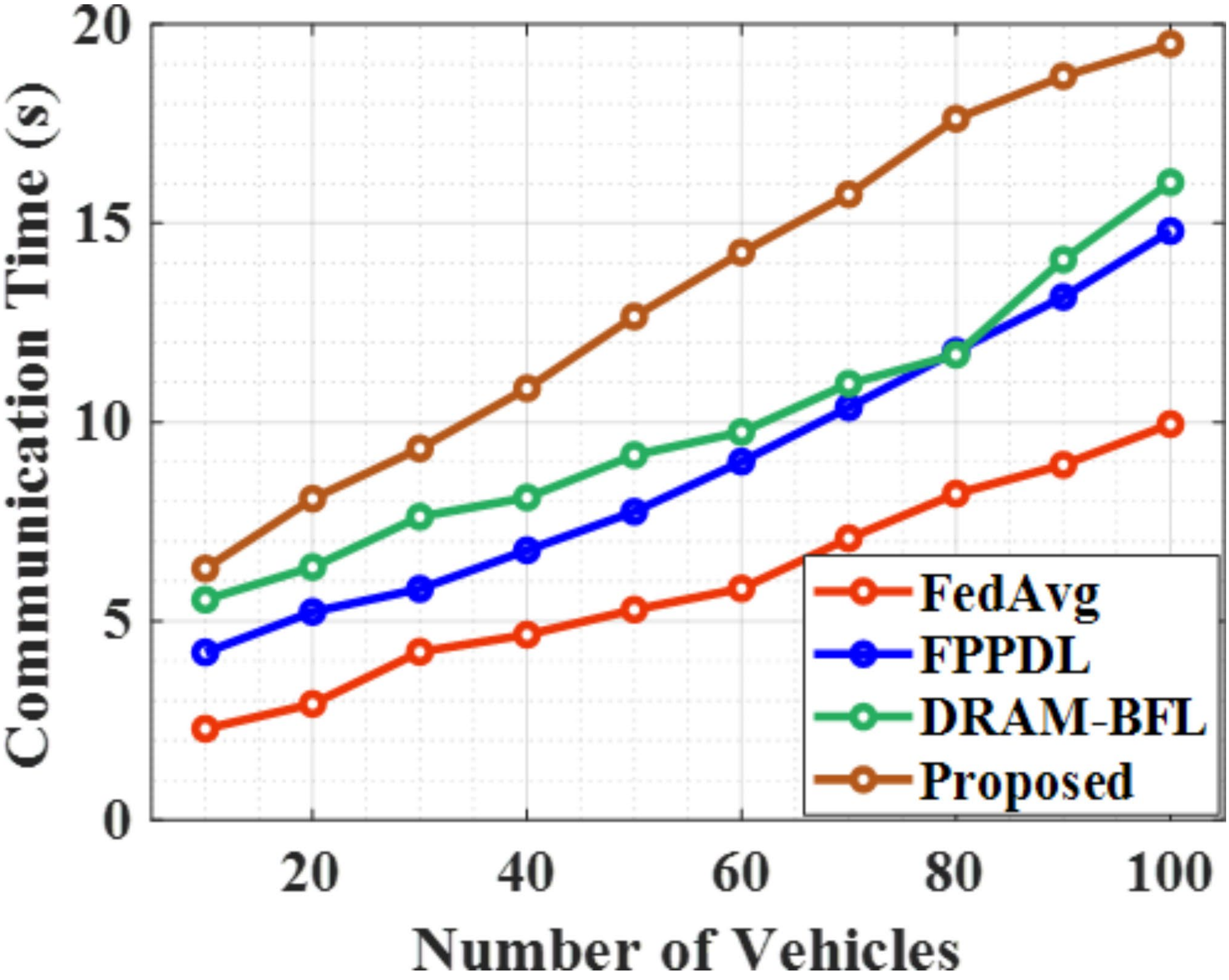


Fig. 7. Analysis of communication time.

a value of 19.51 s, the existing approaches are 9.95, 14.80, and 16.03 s. So, the existing approaches are privacy concerns arise when comprehensive communication data is gathered, particularly in critical settings. Thus, the proposed approach has a faster communication time than compared to existing approaches are mentioned value in Table 4.

Figure 8 depicts the comparison of proposed and existing approaches by varying communication rounds. For 100 rounds, the proposed approach attains a value of 926.35 s, than existing Fedavg, FPPDL, and DRAM-BFL approaches are 1620.86, 1255.22, and 1046.66 s. For 200 rounds, the proposed approach attains a value of 2009.53 s, and the existing approaches are 2699.25, 2365.88, and 2189 s. For 300 rounds, the proposed approach attains a value of 3009.43 s, the existing approaches are 3710.11, 3569.84, and 3278.32 s. For 400 rounds, the proposed approach attains a value of 4001.98 s, the existing approaches are 4702.25, 4540.67, and 4173.87 s. For 500 rounds, the proposed approach attains a value of 5019.13 s, the existing approaches are 5493.43, 5525.76, and 5123.13 s. Thus, the existing approaches are communication time can be impacted by variations in the quantity of data delivered every round. The proposed approach has communication efficiency and enhances model performance.

Communication time (s)				
Number of vehicles	FedAvg	FPPDL	DRAM-BFL	Proposed
10	2.296	4.215	5.538	6.323
20	2.919	5.233	6.36	8.077
30	4.23	5.81	7.625	9.342
40	4.661	6.782	8.107	10.85
50	5.29	7.75	9.174	12.656
60	5.82	9.01	9.754	14.266
70	7.083	10.373	10.968	15.726
80	8.203	11.784	11.695	17.627
90	8.93	13.146	14.085	18.696
100	9.951	14.804	16.03	19.51

Table 4. Values for proposed and existing communication time.

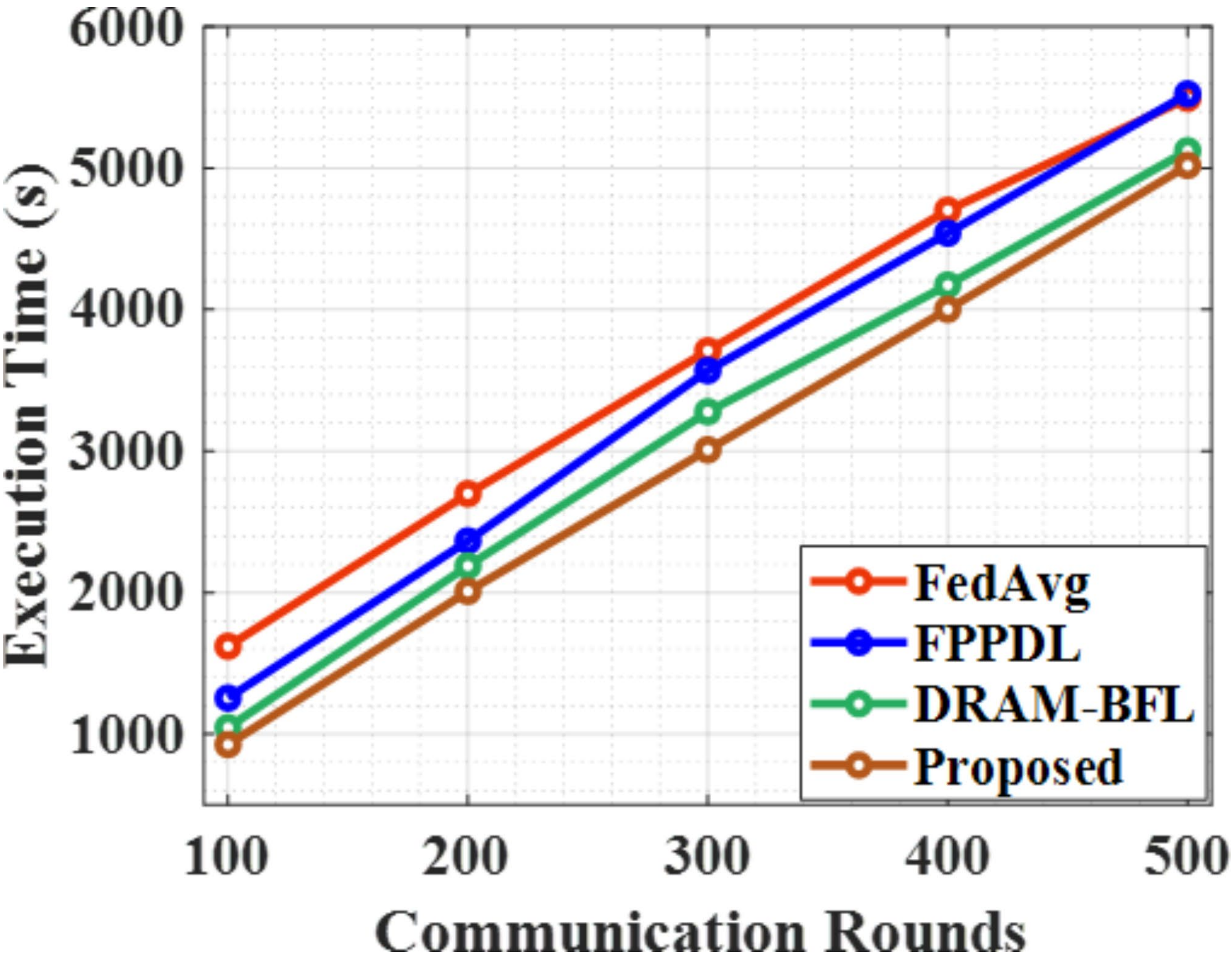


Fig. 8. Analysis of execution time by varying communication rounds.

A comparison of the average latency of proposed and existing approaches is illustrated in Fig. 9. The proposed approach has lower latency than existing approaches. For vehicle data 10, the proposed approach attains a value of 79.95ms, whereas existing approaches are FedAvg, FPPDL, and DRAM-BFL achieve values of 406.80, 261.54, and 145.32ms. For vehicle data 30, the proposed approach attains a value of 177.59ms, the existing approaches are 911.21, 584.37, and 308.31ms. For vehicle data 60, the proposed approach attains a value of 371.27, the existing approaches are 1765.98, 1402.74, and 676.40ms. For vehicle data 80, the proposed approach attains a value of 628.769ms, the existing approaches are 2328.56, 2030.69, and 1073.42 s. For vehicle data 100, the proposed approach attains a value of 864.42ms, the existing approaches are 2920.02, 2426.15, and 1213.04ms.

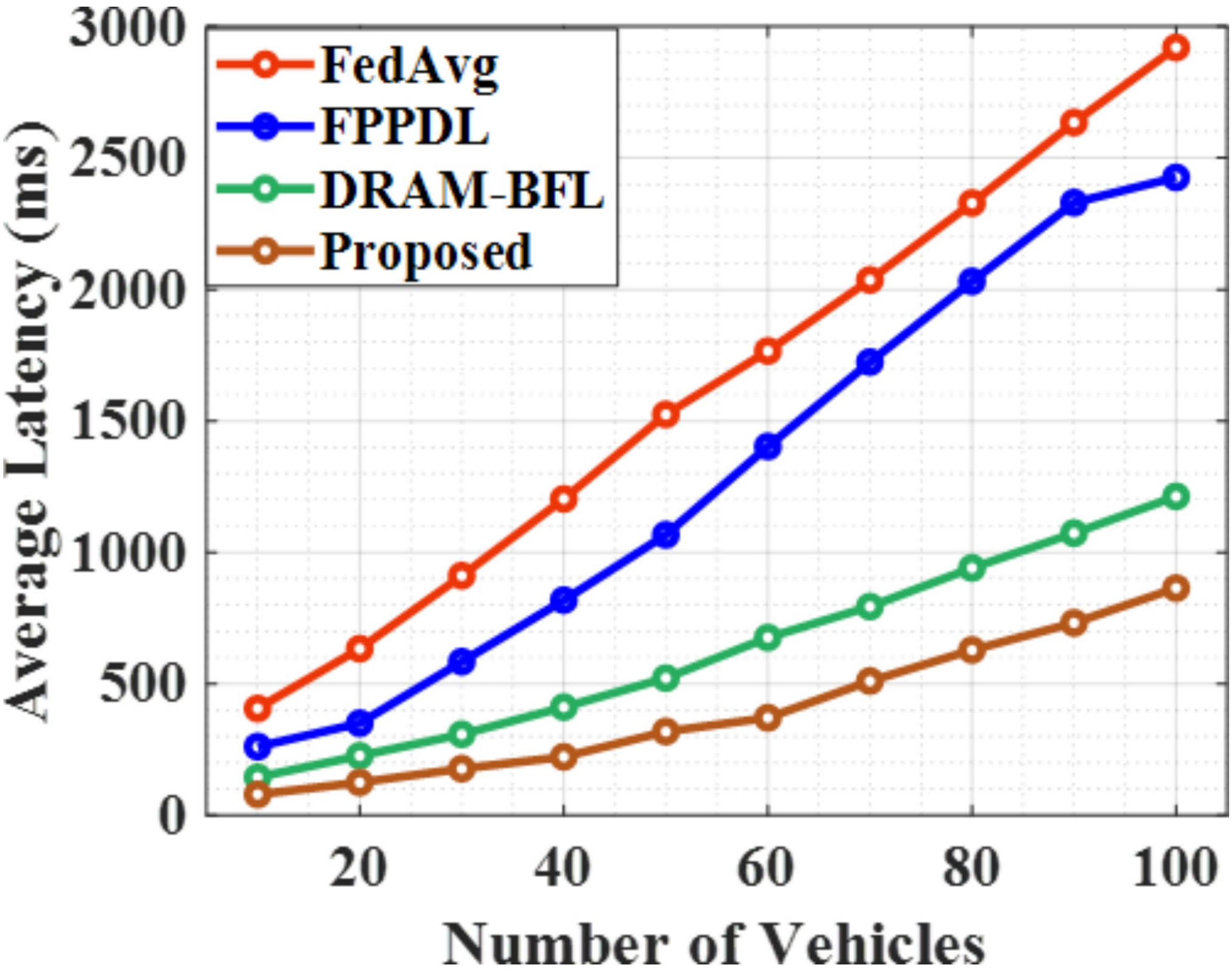


Fig. 9. Analysis of average latency.

Hence, the existing approaches have low responses and increased latency, than proposed method has less latency and an effective model. Table 5 illustrates the value of average latency.

Figure 10 shows the communication overhead of proposed and existing approaches by varying numbers of vehicles. The communication overhead of existing approaches is higher than the proposed approach. For vehicle data 10, the proposed approach attains a value of 100.962 Mb, than existing approaches are FedAvg, FPPDL, and DRAM-BFL achieve values of 1024.03, 519.23, and 230.76 Mb. For vehicle data 30, the proposed approach attains a value of 201.923 Mb than existing approaches are 1658.65, 706.73, and 346.15 Mb. For vehicle data 60, the proposed approach attains a value of 331.73 Mb, than existing approaches are 2682.69, 1182.69, and 764.42 Mb. For vehicle data 80, the proposed approach attains a value of 375 Mb, than existing approaches are 3302.88, 1788.46, and 1009.61 Mb. For vehicle data 100, the proposed approach attains a value of 360.57 Mb, than existing approaches are 41.25, 2639.42, and 1557.69 Mb. Therefore, the existing approaches have higher communication overhead and large amounts of data. So, the proposed approach minimizes overhead and improves performance. Table 6 depicts the proposed and existing communication overhead values.

Figure 11 depicts the comparison of average accuracy with proposed and existing approaches by varying communication rounds. The model attains a greater training accuracy rating concerning communication rounds. The proposed model includes the use of encryption techniques, which raises the training model's security and helps resist processing efforts. So, the existing models have inaccurate outcomes and fewer privacy concerns. For proposed approach has efficient data training and transmission on the VANETs system.

The performance analysis of proposed and existing approaches for throughput by varying data size is shown in Fig. 12. For data size 20, the proposed approach attains a value of 20,547 KB/s whereas existing FedAvg, FPPDL, and DRAM-BFL approaches obtain values of 16,712, 17,808, and 19,726 KB/s. For data size 40, the proposed approach achieves a value of 41095KB/s than the existing approaches are 35,890, 2904, and 38,356 KB/s. For data size 60, the proposed approach attains a value of 60,273 KB/s than existing approaches are 50,684, 41,917, and 57,260 KB/s. For data size 100, the proposed approach has 102,465 than existing approaches are 79,178, 66,027, and 93,972 KB/s. So, the existing methods throughput measures can be impacted by mistakes,

Average latency (ms)				
Number of vehicles	FedAvg	FPPDL	DRAM-BFL	Proposed
10	406.801	261.549	145.327	79.953
20	633.662	350.346	226.836	125.117
30	911.219	584.371	308.319	177.595
40	1203.38	818.42	411.669	222.758
50	1524.671	1066.997	522.258	318.82
60	1765.984	1402.741	676.405	371.272
70	2036.303	1723.982	794.207	510.867
80	2328.563	2030.695	941.141	628.769
90	2635.176	2330.094	1073.421	732.019
100	2920.022	2426.155	1213.04	864.425

Table 5. Comparison values for average latency.

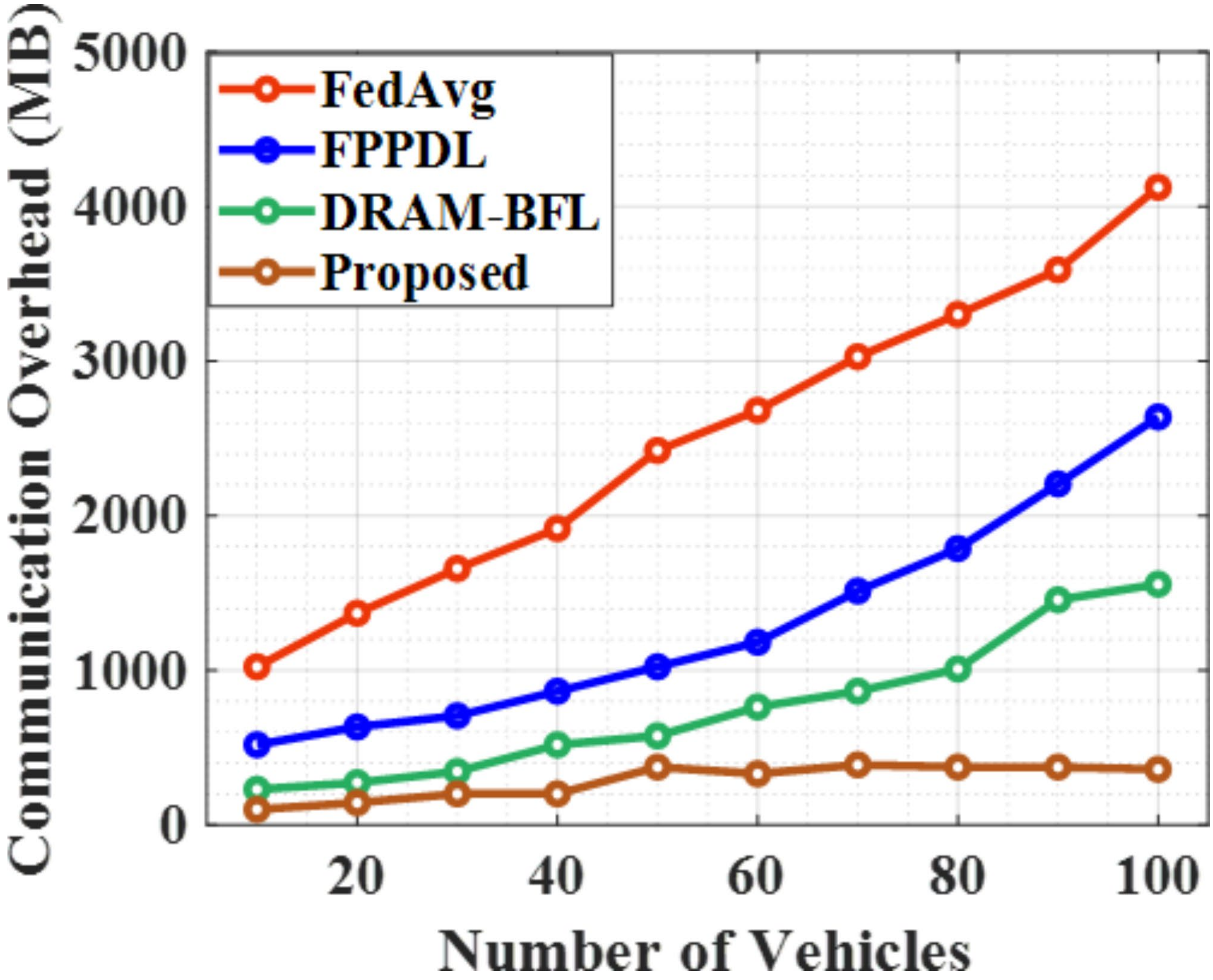


Fig. 10. Analysis of communication overhead.

discrepancies, or missing data. Thus, the proposed approach has evaluated various data sizes and analyzed the efficiency of the proposed model. Throughput by varying data size values is mentioned in Table 7.

Blockchain protocols and new consensus algorithms can be developed by contrasting verification and consensus delay. To maximize privacy and performance, it is essential to recognize the fine distinctions between consensus latency and verification. Selecting the most effective consensus method for a particular use case can be determined by comparing the proposed and several existing algorithms. In order to evaluate the efficacy of

Communication overhead (MB)				
Number of vehicles	FedAvg	FPPDL	DRAM-BFL	Proposed
10	1024.038	519.231	230.769	100.962
20	1370.192	634.615	274.038	144.231
30	1658.654	706.731	346.154	201.923
40	1918.269	865.385	519.231	201.923
50	2423.077	1024.038	576.923	375
60	2682.692	1182.692	764.423	331.731
70	3028.846	1514.423	865.385	389.423
80	3302.885	1788.462	1009.615	375
90	3591.346	2206.731	1456.731	375
100	4125	2639.423	1557.692	360.577

Table 6. Values for communication overhead.

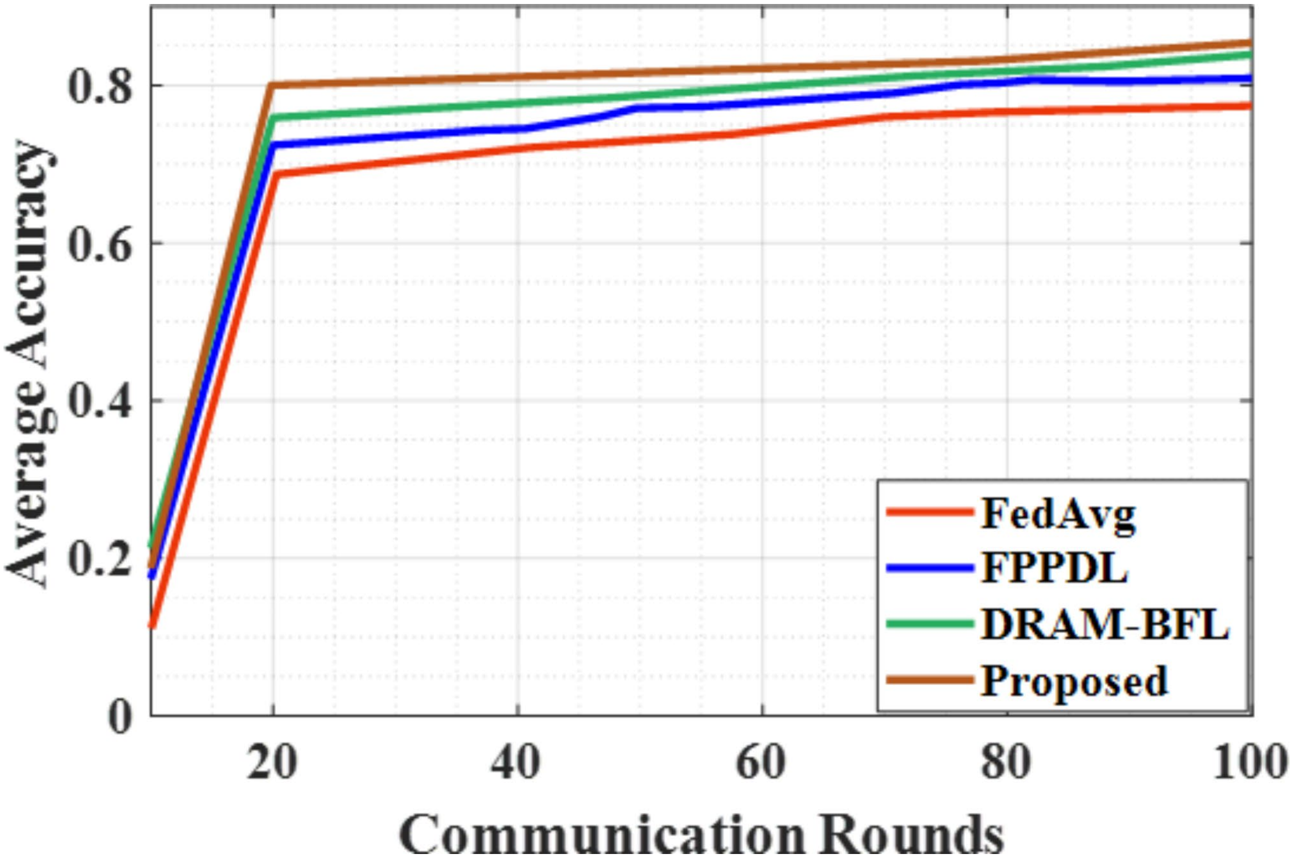


Fig. 11. Analysis of average accuracy by varying communication rounds.

proposed DPBFT, consensus and validation delay is calculated and compared with other the existing consensus algorithm like proof of trustworthiness (PoT), Proof of stack (PoS), Proof of elapsed time (PoET), and Proof of quality factor (PoQF)[39].

Figure 13 illustrates the consensus delay and validation delay comparison of proposed and existing methods. Through this comparison, the trade-offs between network latency and scalability is revealed because of varying the input traffics and calculating the latency achieved. In Fig. 13a, the time required for confirming that the event message is accurate has been included within the consensus delay. The proposed approach has decreased consensus delay, it has attained a value of 50ms. But, the existing approaches have attained higher consensus delay as PoT (80 ms), PoS (120 ms), PoET (180 ms), and PoQF (230 ms). In Fig. 13b, the validation delay of existing approaches is higher delay than existing approaches. The PoQF has a higher delay than the PoT and PoS methods. In comparison to existing approaches are attained PoT (3.47 ms), PoS (6.48 ms), PoET (10.87 ms) and PoQF (14.8 ms). The consensus and validation delay has a direct impact on the average latency. In the meantime, the proposed approach achieves a validation delay of 1.68 ms, respectively. The graphical representation of Fig. 13

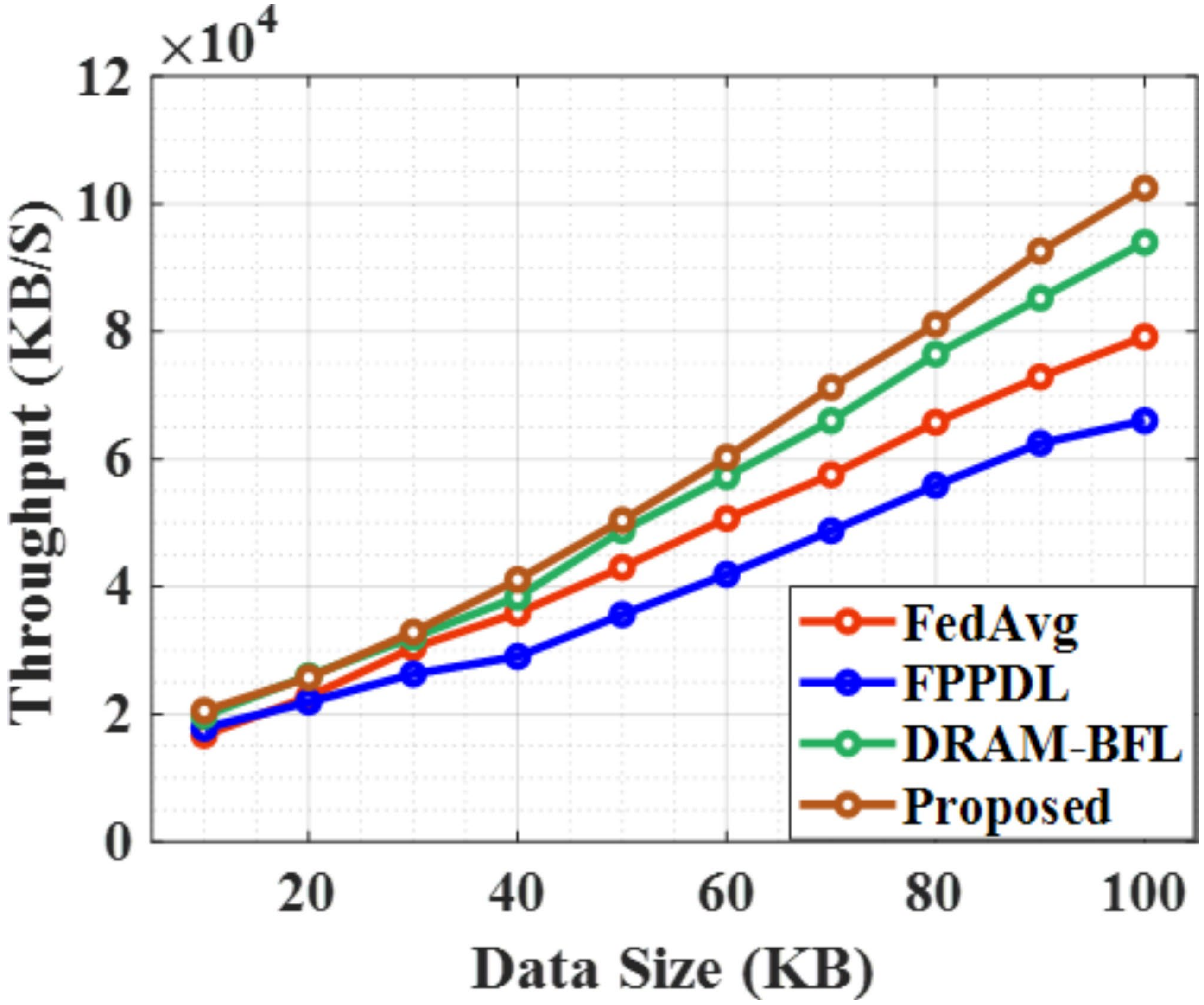


Fig. 12. Analysis of throughput by varying data size.

Throughput (KB/s)				
Data size	**FedAvg**	**FPPDL**	**DRAM-BFL**	**Proposed**
10	16712.33	17808.22	19726.03	20547.95
20	22739.73	21917.81	26027.4	25753.42
30	30410.96	26301.37	32054.79	32876.71
40	35890.41	29041.1	38356.16	41095.89
50	43013.7	35616.44	48767.12	50410.96
60	50684.93	41917.81	57260.27	60273.97
70	57534.25	48767.12	66027.4	71232.88
80	65753.42	55890.41	76438.36	81095.89
90	72876.71	62465.75	85205.48	92602.74
100	79178.08	66027.4	93972.6	102465.8

Table 7. Values for throughput by varying data size.

clearly shows that the proposed DPBFT have attained reduced consensus delay and validation delay as compared with other existing consensus algorithms. This is because, the utilized DPBFT can reduce the demand for energy intensive computations which leads to minimum power and computational resources. Also, by assuring the consensus, DPBFT can handle byzantine faults so that the reliability in dynamic VANET environment is getting

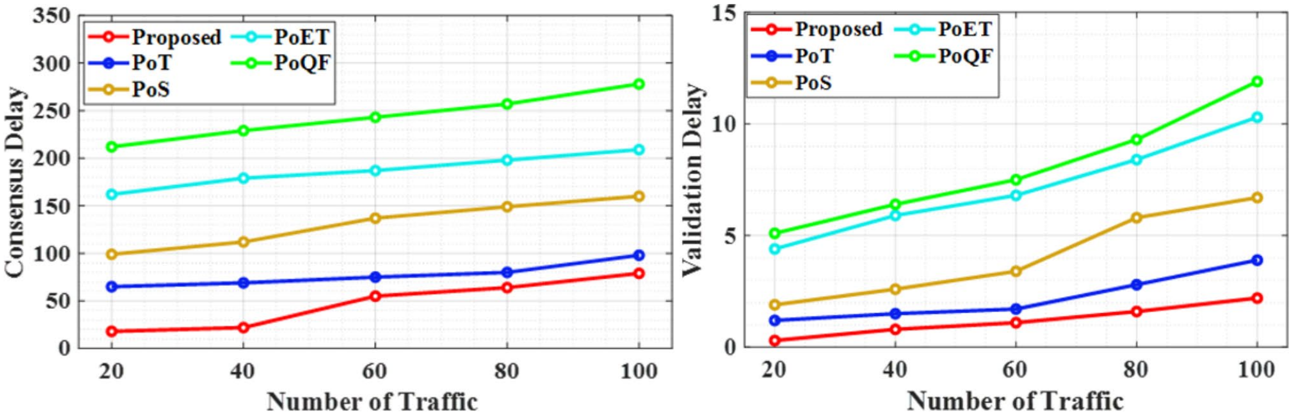
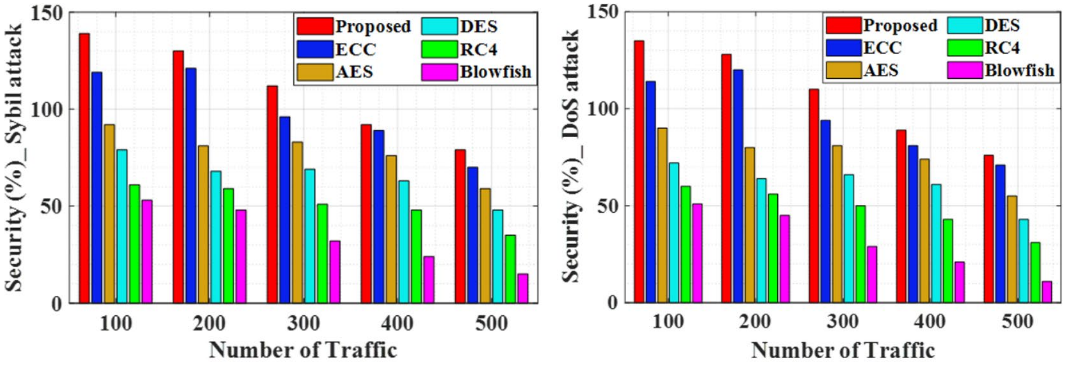


Fig. 13. Comparison of consensus delay and validation delay.



(a) Sybil attack

(b) DoS attack

Fig. 14. **a**, **b** Security percentage comparison of proposed and existing methods.

improved. Moreover, the small amount of trusted delegated nodes in DPBFT is elected by stakeholders. By processing with limited stakeholders, DPBFT provides a faster consensus process. This can helps to minimize the overall network latency computational overhead as compared with other consensus algorithms like PoT, PoS, PoET and PoQF. Figure 14 shows the security percentage comparison of proposed and existing methods.

The comparison analysis in Fig. 14 proves the ability of proposed EX-ECC approach. As compared with other encryption algorithms like ECC, AES, DES, RC4 and Blowfish, the security of input traffic information are enhanced in the proposed EX-ECC approach. Here, the security is analysed under dynamic network environments in which 500 vehicular nodes are considered by real-time. By varying the traffic rates from 100 to 500, the security is analysed against Sybil attacks and Denial of Service (DoS) attacks. The proposed study prevents Sybil attacks and DoS attacks because of the great efficiency of EX-ECC and blockchain framework. Through the specific cryptographic keys, each participating nodes are assigned and securely recorded on the decentralized ledger (blockchain). The utilized EX-ECC performs secure key exchange process which ensures only authenticated nodes. This can helps to prevent malicious Sybil and DoS attacks from generating various false identities to impact the learning process.

Analysis of proposed technique for real-time scenarios

The real-time data were considered to determine the scalability of proposed technique. This data was considered based on various parameters of vehicles and RSU which includes the number of vehicles as 1000, number of RSU, location of each vehicle data, signal strength, and so on. The ratio of training and testing is 80:20, and the size of training and testing data are 1056 and 264. Here, 80% of the data was utilized to train the model, and 20% of the data was used for testing. The proposed uses adaptive learning rates and weighted aggregation in the federated Q-learning framework to handle bias and data skew in VANETs. To ensure that nodes with bigger or more diversified datasets contribute adequately to the global model, a weight is applied to each vehicle's local model update based on the volume and quality of its data. Additionally, bias from prevalent data sources is reduced by methods like data regularization and normalization. The method ensures balanced learning, encourages equitable representation from a variety of vehicular data sources, and enhances overall model adaptability by routinely assessing model performance across various vehicle types (such as urban vs. highway). The convergence analysis is conducted for real-time data to determine the efficiency of federated learning techniques for varying numbers of vehicles which is represented in Fig. 15.

The proposed technique attained 55.4% accuracy for 100 vehicles by analysis of non-independent and identically distributed (IID) data. Similarly, the performance of the proposed technique was analyzed for varying numbers of vehicles to determine its convergence. The proposed technique attained 66.8% accuracy for 200 vehicles, 68.98% accuracy for 300 vehicles, 73.93% accuracy for 400 vehicles and 85.77% accuracy for 1000 vehicles. Several strategies are required to ensure convergence in federated learning among highly mobile and intermittently related vehicles in VANETs. To secure the data, adaptive synchronization systems allow vehicles to transmit non-IID data when it's reconnected. Weighted aggregation ensures that updates from various nodes are suitably balanced depending on data quality and relevance while handling non-IID data. Moreover, local models can improve on different data patterns while increasing to the global model due to strategies like personalized federated learning. These methods enable high convergence despite data mobility and heterogeneity when combined with dynamic model averaging and recurrent global validation. The comparison of latency for varying numbers of vehicles is represented in Fig. 16.

The latency of proposed technique for real-time data is analyzed for varying numbers of vehicles to determine its efficiency. The proposed technique attains 506.80 ms for 100 vehicles, 733.66 ms for 200 vehicles, 911.21 ms for 300 vehicles, 2203.380 ms for 400 vehicles, and 4920.02 ms for 1000 vehicles. The proposed method combines priority-based transaction processing and dynamic consensus adjustment to reduce the effect of Blockchain overhead on latency and real-time responsiveness in VANETs, especially during emergencies or periods of high traffic. To improve the validation, critical messages (such as emergency alerts) are given preference over less urgent transactions. By employing pre-selected nodes for rapid decision-making and minimizing the number of validation stages, the DPBFT consensus method is tuned for low latency. Finally, IPFS off-chain data storage reduces on-chain transaction burden by making sure that only necessary data is handled on the Blockchain, ensuring real-time performance even in situations with high traffic. The proposed Blockchain and federated learning method is utilized for handling thousands of vehicles highly scalable due to a few essential techniques. To reduce communication overhead and ensure effective model aggregation, hierarchical federated learning divides vehicles into clusters. By dividing the ledger into smaller, more manageable sections, sharding is used on the Blockchain side to improve throughput and allow transactions to be performed in parallel.

Discussions

The use of artificial intelligence in safety-sensitive scenarios such as self-driving vehicles, smart medical care IoT, etc. The existing methods have significant issues regarding the need for trustworthy artificial intelligence methods to ensure safety and privacy through logical reasoning. FL was considered a promising secure privacy system to train local and global model devices and a more reliable system.

Nevertheless, there are security issues with the FL framework such as hostile servers and system tampering assaults from malevolent devices. Which can reduce or completely eliminate the reliability of the trained model. Certain ECC patents may restrict application, which could impact installation expenses and adaptability.

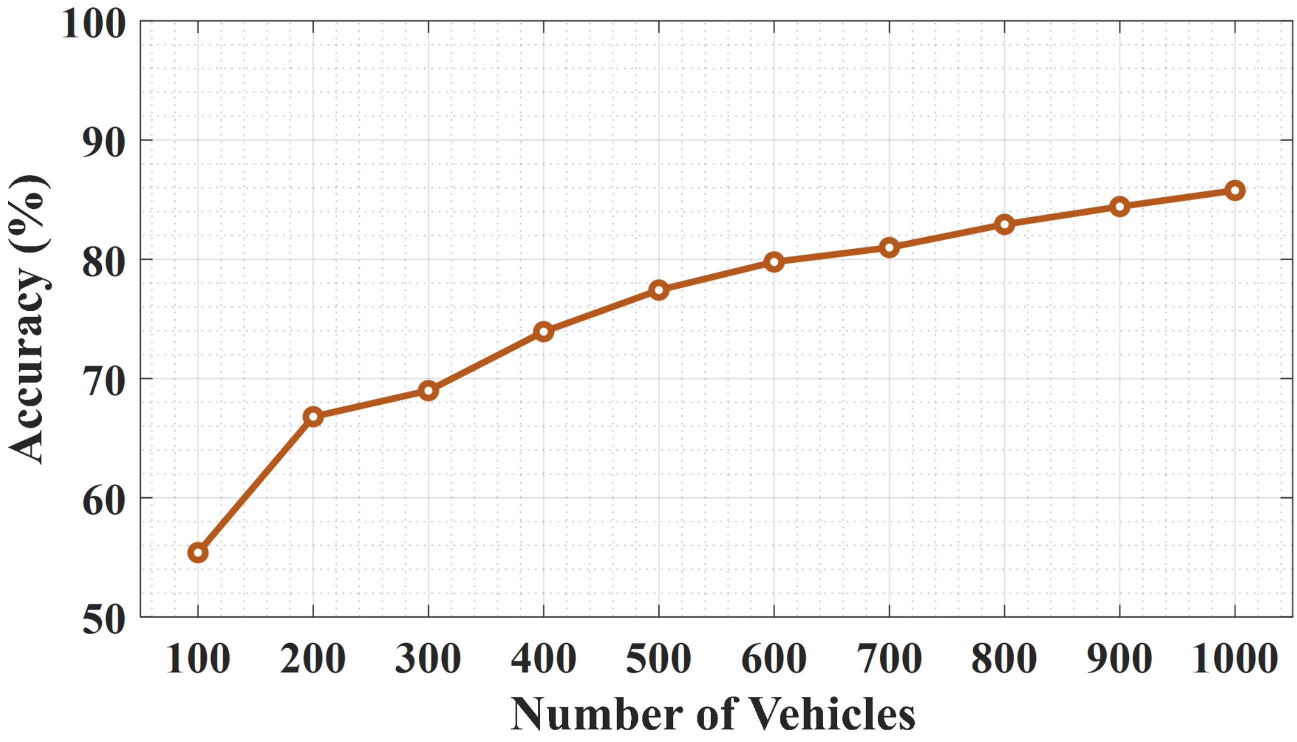


Fig. 15. Convergence analysis of proposed technique for varying number of vehicles.

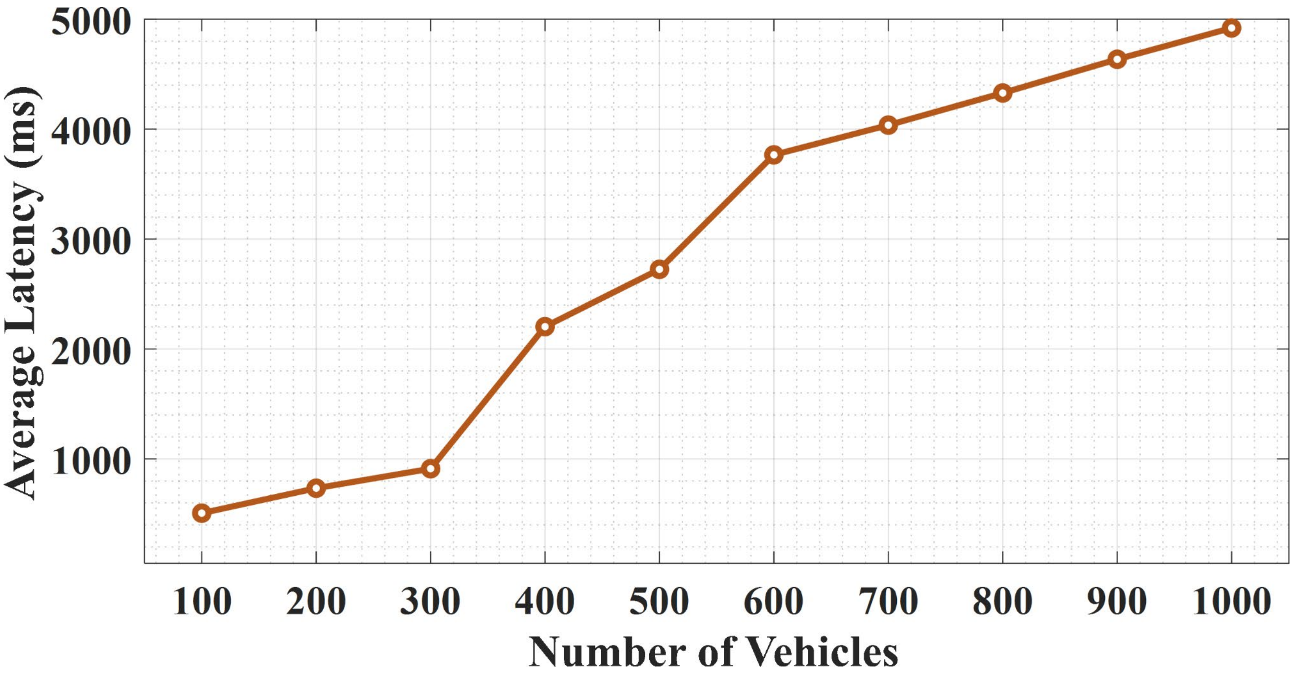


Fig. 16. Comparison of average latency of proposed technique for varying number of vehicles.

Authors	Techniques used	Performance metrics
Kumar et al.[21]	RF	Accuracy (1.16%), detection time (1.18 s)
Fardad et al.[22]	BEVEC	Latency (18%), energy consumption (65%)
Gharehchopogh et al.[23]	DDQN	Latency (6.87%) Energy consumption (26.4%) Computational cost (7.41%)
Shukla et al.[24]	DNN	Throughput (70%) Energy consumption (40.32%)
Mohammed et al.[25]	MORFLB	Delay (72%)
Li et al.[26]	BTWACS	Accuracy (80%), encryption time (78%)
Zhang et al.[27]	DRL	Latency (7.5%) Accuracy (73.2%) Energy consumption (42.51%)
Proposed	EX-ECC, federated Q-learning model, IPFS, DPBFT	The number of vehicles 100, throughput (102465.8 KB/s), communication overhead (360.57 Mb), average latency (864.425 ms), communication time (19.51 s), encryption time (0.98 ms), decryption time (1.97 ms), consensus delay (50 ms) and validation delay (1.68 ms)

Table 8. Detailed evaluation of existing and proposed approach.

This study presents a safe global aggregation-based Blockchain FL-Q learning framework. An approach that combines low computational complexity with higher system efficiency is based on deep reinforcement learning. The vehicle data can be securely protected with the help of the Ex-ECC algorithm. The validation of the low-power, highly effective function of the consensus algorithm is used. The suggested Blockchain enables security methods to safeguard user privacy concerning the data. In this study, the performance of the proposed method is evaluated and compared with existing models as demonstrated in Table 8. Based on the performance metrics values, the proposed model is compared with various metrics such as accuracy, detection time, Latency, Energy consumption, Computational cost, and throughput. Then, the existing RF achieved Accuracy (1.16%), because the model had high false negative and positive rates with a low degree of precision[21]. The performance of another existing model was BEVEC, this model has increased energy use and high delay[22].

The DDQN[23] model has a more time-consuming and computational cost. Then, DNN[24] and MORFLB[25] are Expensive blockchain systems with significant latency and fewer privacy systems. The performance of BTWACS[26] and DRL[27] models is High computational cost, less security system, and Enhanced network congestion. Compared to the other existing models, the proposed model attained a higher value and improved model performance. Hence, the proposed model is capable of efficiently managing an enormous quantity of data interactions and vehicles. Table 8 illustrates a detailed evaluation of the existing and proposed approaches.

Conclusion and future work

This paper aims to analyze a robust and secure Blockchain-based federated Q-learning system for VANETs. In order to protect the input traffic data, the extended elliptic curve cryptography (Ex-ECC) technique is used. This technique has stronger security and a faster decryption and encryption process. To guarantee improved privacy, the federated Q-learning network evaluated the data and examined the assaults. Utilize the FL framework of distributing VANETs, while computation work is transferred to specific vehicles that lower communication overhead and congestion delay. Then, the IPFS technology is used to improve the security and storage of the VANET system. IPFS can accelerate data access by distributing content. To preserve the privacy of all individuals, we have designed a safe communication approach among vehicle-to-vehicle and vehicle-to-RSU that utilizes Blockchain technology. The Delegated Practical Byzantine Fault Tolerance approach is employed to verify the proposed model. Hence, Blockchain technology allows for data flow between many platforms straightforward and secure. A Blockchain-based federated Q-learning has permitted a security measure system that can greatly improve user safety and data privacy in the VANETs network. The following outcomes are obtained by the proposed approach for a number of vehicles 100, throughput (102465.8 KB/s), communication overhead (360.57 Mb), Average Latency (864.425 ms), Communication Time (19.51 s), Encryption time (0.98 ms), Decryption time(1.97 ms), Consensus delay (50 ms) and Validation delay (1.68 ms), respectively. Future work will require extending potential effort to implement the suggested structure, which would involve interacting with device, user, and cloud layers. An instance of this interaction will be gathering data from wearable sensors and analyzing it in real time. To train the suggested algorithm, this research should add greater complexity and more relevant datasets in the future. Also, investigate more security improvements in addition to compressing computing capacity, enhancing scalability, and resolving model staleness. FL is utilized to produce autonomous driving systems that gather information from various vehicles in order to operate better. By combining data from cameras, sensors, and other sources autonomous vehicles to forecast traffic trends in real time.

Data availability

The datasets used and/or analyzed during the current study are available from the corresponding author upon reasonable request.

Received: 21 August 2024; Accepted: 6 December 2024
Published online: 28 December 2024

References

1. Mohammed, B. et al. Alayba. Service based VEINS framework for vehicular Ad-hoc network (VANET): a systematic review of state-of-the-art. *Peer-to-Peer Netw. Appl.* : 1–23. (2024).
2. Al-Ani, R., Baker, T. & Qi Shi. Privacy and safety improvement of VANET data via a safety-related privacy scheme. *Int. J. Inf. Secur.* **22**(4), 763–783 (2023).
3. Abbas, G., Ullah, S. & Waqas, M. Ziaul Haq Abbas, and Muhammad Bilal. A position-based reliable emergency message routing scheme for road safety in VANETs. *Comput. Netw.* **213**, 109097 (2022).
4. Wei, X. Enhancing road safety in internet of vehicles using deep learning approach for real-time accident prediction and prevention. *Int. J. Intell. Netw.* **5**, 212–223 (2024).
5. Dudhe, A. S., Salim, Y., Amdani & Suresh, S. Asole. Real time communication model for vehicular communication in VANET. *Int. J. Sci. Res. Comput. Sci. Eng. Inform. Technol.* **8**(2), 115–120 (2022).
6. Natarajan, R. et al. Optimizing radio access in 5G vehicle networks using novel machine learning-driven resource management. *Opt. Quant. Electron.* **55**(14), 1270 (2023).
7. Moridi, E. Increasing efficiency and reliability in multicasting geographical routing based on fuzzy logic in VANETs. *J. Soft Comput. Inform. Technol.* **12** (1), 11–19 (2023).
8. Sajini, S., Mary Anita, E. A. & Janet, J. Improved security of the data communication in VANET environment using ASCII-ECC algorithm. *Wirel. Pers. Commun.* **128**(2), 759–776 (2023).
9. Nova, Kannan, A. et al. Floyd–Warshalls algorithm and modified advanced encryption standard for secured communication in VANET. *Measurement: Sens.* **27**, 100796 (2023).
10. Tsetseruk, D. Federated learning for privacy-preserving autonomous vehicle data analysis. *J. Artif. Intell. Res. Appl.* **3**(2), 293–320 (2023).
11. Peixoto, M. L. M., Edson Mota, Adriano, H. O., Maia, W., Lobato, M. A. & Salahuddin Raouf Boutaba, and Leandro A. Villas. FogJam: a fog service for detecting traffic congestion in a continuous data stream VANET. *Ad Hoc Netw.* **140**, 103046 (2023).
12. Wei, Y. et al. The eternal tussle: exploring the role of centralization in {IPFS}. In 21st USENIX Symposium on Networked Systems Design and Implementation (NSDI 24), pp. 441–454. (2024).
13. Fernandes, C. et al. Wangham. A blockchain-based reputation system for trusted VANET nodes. *Ad Hoc Netw.* **140**, 103071 (2023).
14. Ma, Z. Secured scalable blockchain networks for trustworthy distributed deep learning in VANETs. PhD diss (Carleton University, 2023).
15. Dhasaratha, C. et al. Ahmed Ibrahim Alzahrani, Nasser Alalwan, Nguyen Vo, and Md Akhtaruzzaman. Data privacy model using blockchain reinforcement federated learning approach for scalable internet of medical things. *CAAI Trans. Intell. Technol.* (2024).
16. Nikolaidis, F., Symeonides, M. & Demetris Trihinas. Towards efficient resource allocation for federated learning in virtualized managed environments. *Future Internet.* **15**(8), 261 (2023).
17. Arya, M., Sastry, H., Dewangan, B. K., Rahmani, M. K. I. & Bhatia, S. Abdul Wahab Muzaffar, and Mariyam Aysha Bivi. Intruder detection in VANET data streams using federated learning for smart city environments. *Electronics* **12**(4), 894. (2023).
18. Haris, M., Shah, M. A. & Carsten Maple. Internet of intelligent vehicles (IoIV): an intelligent VANET based computing via predictive modeling. *IEEE Access.* **11**, 49665–49674 (2023).
19. Gholizadeh, N., Kazemi, N. & Musilek, P. A comparative study of reinforcement learning algorithms for distribution network reconfiguration with deep Q-learning-based action sampling. *IEEE Access.* **11**, 13714–13723 (2023).
20. Kim, M., Oh, I., Yim, K. & Sahlabadi, M. and Zarina Shukur. Security of 6G enabled vehicle-to-everything communication in emerging federated learning and blockchain technologies. *IEEE Access.* (2023).

21. Kumar, Y., Kumar, V. & Subba, B. Optimization techniques for IDS-Generated traffic congestion control in VANET. *Internet Technol. Lett.* : e518 .
22. Fardad, M., Muntean, G. M. & Tal, I. A blockchain-enabled vehicular edge computing framework for secure performance-oriented V2X service delivery. *IEEE Trans. Veh. Technol.* (2024).
23. Gharehchopogh, F. S. Multi-objective secure task offloading strategy for blockchain-enabled IoV-MEC systems: a double deep Q-network approach. (2024).
24. Shukla, P., Patel, R. & Varma, S. A novel of congestion control architecture using edge computing and trustworthy blockchain system. *J. Intell. Fuzzy Syst.* **44**(4), 6303–6326 (2023).
25. Mohammed, M., Abed, A., Lakhan, K. H. & Abdulkareem Mohd Khanapi Abd Ghani, Haydar Abdulameer Marhoon, Jan Nedoma, and Radek Martinek. Multi-objectives reinforcement federated learning blockchain enabled Internet of things and Fog-Cloud infrastructure for transport data. *Heliyon* **9**(11) (2023).
26. Li, L., Wan, J. & Liu, C. Access control strategy for the internet of vehicles based on blockchain and edge computing. *Electronics* **12**(19), 4057. (2023).
27. Zhang, B. et al. A reputation mechanism based deep reinforcement learning and blockchain to suppress selfish node attack motivation in Vehicular Ad-Hoc Network. *Future Generation Comput. Syst.* **139**, 17–28 (2023).
28. Li, Y., Wei, X., Li, Y., Dong, Z. & Mohammad Shahidehpour. Detection of false data injection attacks in smart grid: a secure federated deep learning approach. *IEEE Trans. Smart Grid*. **13**(6), 4862–4872 (2022).
29. Li, Y., Wang, R., Li, Y., Zhang, M. & Chao Long. Wind power forecasting considering data privacy protection: a federated deep reinforcement learning approach. *Appl. Energy*. **329**, 120291 (2023).
30. Lahraoui, Y., Lazaar, S., Amal, Y. & Abderrahmane Nitaj. and. Securing data exchange with elliptic curve cryptography: a novel hash-based method for message mapping and integrity assurance. *Cryptography* **8**(2), 23. (2024).
31. Zheng, Z., Zhang, H. & Xue, L. Federated Q-learning with reference-advantage decomposition: almost optimal regret and logarithmic communication cost. arXiv preprint arXiv:2405.18795 (2024).
32. Chen, X., Qiu, W., Chen, L., Ma, Y. & Ma, J. Fast and practical intrusion detection system based on federated learning for VANET. *Computers Secur.* **142**, 103881 (2024).
33. Saif, B., Muhammad, S., Migliorini & Spoto, F. Efficient and secure distributed data storage and retrieval using interplanetary file system and blockchain. *Future Internet*. **16**(3), 98 (2024).
34. Li, C., Qiu, W., Li, X., Liu, C. & Zheng, Z. A dynamic adaptive framework for practical byzantine fault tolerance consensus protocol in the internet of things. *IEEE Trans. Comput.* (2024).
35. Walle, Y. Hybrid RSA–AES-based software-defined network to improve the security of MANET. *Open. Inform. Sci.* **8**(1), 20240001 (2024).
36. Rathnayake, R. G. G. A. and D. V. D. S. Abeysinghe. A deep investigation to enhance secure communication of satellite images through encryption techniques.
37. Liu, J., Li, Y., Zhao, M., Liu, L. & Kumar, N. EPFFL: enhancing privacy and fairness in federated learning for distributed e-healthcare data sharing services. *IEEE Trans. Dependable Secur. Comput.* (2024).
38. Zhi, H. & Wang, Y. Network resource allocation method based on blockchain and federated learning in IoT. *J. Commun. Netw.* **26**(2), 225–238 (2024).
39. Ghaleb, F. A., Ali, W., Al-Rimy, B. A. S. & Sharaf, J. Malebary. Intelligent proof-of-trustworthiness-based secure safety message dissemination scheme for vehicular ad hoc networks using blockchain and deep learning techniques. *Mathematics* **11**(7), 1704. (2023).

Author contributions

All authors contributed to the study, conception, and design. all authors commented on the manuscript. All authors read and approved the final manuscript.

Funding

The authors did not receive support from any organization for the submitted work.

Declarations

Competing interests

The authors declare no competing interests.

Ethical approval

This paper does not contain any studies with human participants or animals performed by any of the authors.

Consent to participate

Not applicable.

Additional information

Correspondence and requests for materials should be addressed to H.A.A.A.-A.

Reprints and permissions information is available at www.nature.com/reprints.

Publisher's note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.