Journal of Autonomous Intelligence (2023) Volume 6 Issue 2
doi: 10.32629/jai.v6i2.828

ORIGINAL RESEARCH ARTICLE

Novel machine learning based authentication technique in VANET system for secure data transmission

Anand N. Patil[1,*], Sujata V. Mallapur[2]

[1] *Department of Computer Science & Engineering, Sharnbasva University Kalaburagi, Kalaburagi 585103, India*
[2] *Department of Artificial Intelligence & Machine Learning, Sharnbasva University Kalaburagi, Kalaburagi 585103, India*

*** Corresponding author:** Anand N. Patil, patilanand1990@gmail.com

ABSTRACT

Adaptive transport technologies based on vehicular ad hoc networks (VANET) has proven considerable potential in light of the developing expansion of driver assistance and automobile telecommunication systems. However, confidentiality and safety are the vital challenges in vehicular ad hoc networks which could be seriously impaired by malicious attackers. While protecting vehicle privacy from threats, it is imperative to stop internal vehicles from putting out bogus messages. Considering these issues, a novel machine learning based message authentication combined with blockchain and inter planetary file system (IPFS) is proposed to achieve message dissemination in a secured way. Blockchain is the emerging technology which attempts to solve these problems by producing tamper proof events of records in a distributed environment and inter planetary file system used in the framework is a protocol designed to store the event with content addressability. Along with this combined technology, the source metadata information collected from the inter planetary file system is stored via a smart contract and uploaded to the distributed ledger technology (DLT). For performing event authentication, K-means clustering and support vector machine (SVM) classifier is employed in this framework. K-means clustering performs clustering of vehicles and it is marked malicious or not malicious. After clustering, support vector machine classifier detects the malicious event messages. By this way, the malicious messages are identified and it is dropped. Only the secure messages are forwarded in the network. Finally, our approach is capable of creating a safe and decentralized vehicular ad hoc network architecture with accountability and confidentiality through theoretical study and simulations.

Keywords: VANET; IPFS; SVM; K-means clustering and blockchain

ARTICLE INFO

Received: 29 June 2023
Accepted: 19 July 2023
Available online: 8 August 2023

1. Introduction

India is growing through a period of drastic change in the transportation area due to rapid growth of economy, rising vehicle ownership levels, insufficient and inadequate public transportation system which all these problems are sort out by the intelligent transportation system[1]. It plays a prominent role and provides intelligent guidance for relieving traffic congestion by advanced communication approaches. In recent days, vehicular ad hoc networks are gaining high attention as it has an ad hoc nature and self-organized networks of vehicles. For vehicles beyond the scope, multi-hop routing is feasible. An internal vehicle component known as “on board unit” analyses information gathered from several sensors. Communication with outside networks, for instance other cars and frameworks, is carried out by the sensor that is fitted with the vehicle’s conditions. Transfer of data between vehicles and between vehicles and

infrastructure is made easier via VANET and it acts as a strong catalyst to improve traffic efficiency. The VANET communication model is represented in **Figure 1**.

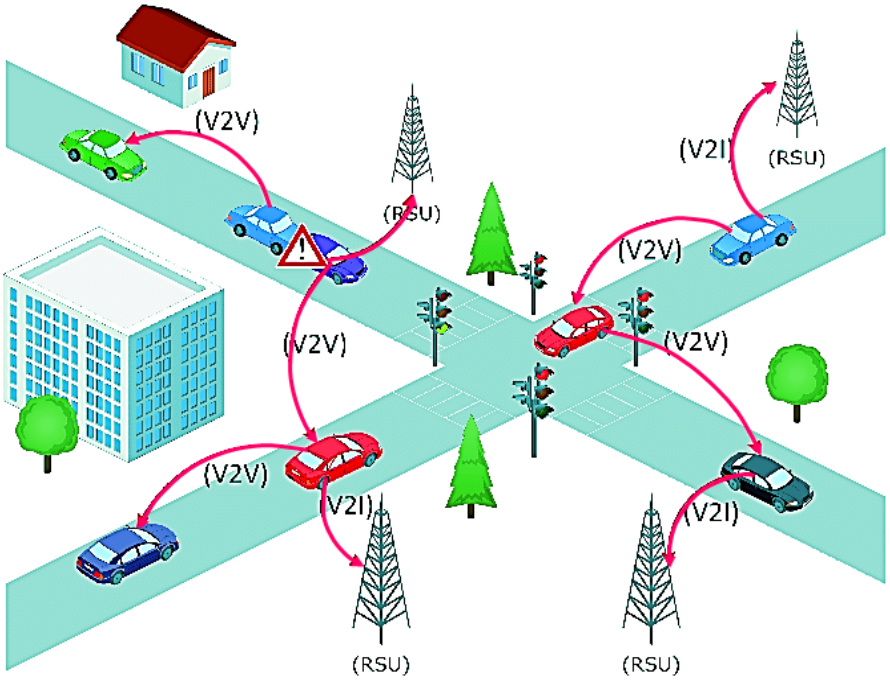

Figure 1. ANET communication model.

Vehicles in VANET can produce their own driving state information and collect information such as traffic congestion and slippery road[2–4]. The gathered data helps the vehicles in VANET to enhance driving comfort and safety. The VANET has characteristics of high mobility of nodes, the communication link is maintained for a limited period of range and no problem with power.

As the information exchange between inter-vehicle as well as an automobile to road side unit (RSU) within a VANET take place on the open wireless channel[5]. It paved the way for the attacker to carry out the evil ambitions, such as traffic surveillance. Moreover, inside attackers injects the fake message to report bogus events. Although increased connectedness and the abundance of communication channels, ccess points resulted in many advancements, they also raise several issues that must be taken into account when creating vehicular solutions[6–8], the most important of which are data eliability and onfidentiality. As a result, the central concerns are the confidentiality of the vehicles and the protection of communication exchanges, which must be achieved by verifying authenticity, validity and security of event messages. Various centralized solutions have been used in existing studies which incorporates cloud computing to address these problems[9,10]. However, in vehicular settings, it improves computing efficiency and resource usage. Due to its latency sensitivity needs and vehicle mobility, it is not suited for VANET applications. As vehicle networks are prone to several form of threats, various cryptographic techniques were implemented in the past approaches[11–13]. Some generally employed conventional security methods like password guarding, biometric security with key-based authentication are the methods employed for authentication. However, it fails to scrutinize if the transmitted information is genuine or not. For detection of events before hoarding to blockchain, in the existing approach, techniques such as edge service provider, multimedia data sharing technique is used but it consumes more time to perform authentication[14–16]. The problems in the existing approaches are addressed by the proposed technique.

Blockchain is a decentralized network which has a collection of blocks that involves different data and information and it act as an open ledger to all network entities. The data in the blockchain is extremely hard to

change hence it is used in our proposed work as a part due to its immutability, consensus and tamper-proof informational storage. In the existing work, various blockchain based solutions have been discussed in the study[17–19] addressing problems such as revoking access privileges for malicious vehicles, failing to verify the validity of an event before storing it on a blockchain, and a lack of attribute-based access control upon events premised on user characteristics. For solving aforementioned issues, we propose a novel machine learning based message authentication combined with blockchain and IPFS. The machine learning modules are put into effect with blockchain by collecting vehicular sensor data for making decision and perception which enhance the on-road driving safety in an intelligent manner[20–21]. The events collected at RSU are first stored in IPFS and smart contract is executed to learn the machine learning event authentication model to classify event to malicious or not malicious. The events collected at RSU are first clustered using K-means clustering algorithm to two clusters. RSU extract the vehicle's true identity and verify the legitimacy according to the database which mitigates the vehicle's computing burden. By using domain expert, it predicts the data. Vehicle executes a smart contract to fetch most updated decision rules from inter planetary file system (IPFS) and use it for validating the event. When event is decided as malicious by the decision rules, the message is dropped by the vehicle. By this way only valid messages are forwarded in the network. Vehicle frequency takes the decision rules via execution of smart contract and uses it to validate the messages before forwarding to next hop.

The following are the aspects of the work,

1) Integration of blockchain and IPFS with machine learning based message authentication.
2) To ensure reliability of data before sharing it by using a coactive event confidence model.
3) Access control using machine learning for reliable data transmission using IPFS.

The remaining sections are arranged as follows. A short introduction about proposed work and its related existing techniques were analyzed in section II and section III describes the proposed approach for event authorization, verification, and secure event exchange. Section IV discusses the findings of the proposed work and finally concluded in section V.

2. Related works

Kim et al.[22] presented the blockchain system impacts in VANET due to mobility. It is analyzed using three measures, (1) the contingency of an effective block addition, (2) the reliability of a rendezvous as well as the volume of blocks traded during the rendezvous. These two metrics gets achieved by attaining stability through this proposed system but it failed to achieve efficiency and scalability when the network nodes are mobile and moving.

Zhang et al.[23] presented the secure information sharing between vehicles based on attribute based cryptographic technique. Static and dynamic attributes are used based upon the characteristics. A new group signature CP-ABE is used on the cipher text to attain verifiability and integrity and also it involves pairing operation. The drawback involved in this technique is, an attacker easily detects the attribute values by using attribute value guessing attack.

Horng et al.[24] presented a data access control technique to transfer data among several cloud storage systems and application service providers for automobiles in a VANET which maintains privacy and security against various malicious attacks and it achieves scalability and efficiency but it is takes more time for verification.

Zhong et al.[25] proposed an identity-based broadcast encryption technology. Through this technique, redundancies are reduced as well as improve the work efficiency of trusted authority and the comparative analysis is made between the sender's cipher-text overhead and the encrypted text's length.

Alharthi et al.[26] suggested a biometric blockchain infrastructure that safeguards the data between the transmissions of vehicles. It preserves obscurity while protecting the approved user's identity. To ensure dependable data delivery, biometric is integrated with the blockchain technology and also it is assessed using the packet's delivery rate and loss rate, and computational expense but when fusion of multiple biometric attributes occur, the problem arises.

Lin et al.[27] suggested BCPPA scheme for encrypted transmission. Blockchain and key derivation algorithm is integrated in this framework. In addition to this, to improve the performance PKI based signature is used with batch verification but PKI requires backup in case of data loss.

Aghabagherloo et al.[28] presented the privacy-preserving authentication schemes for VANETs to enhance the security and effectiveness of the current roadside side unit and tamper resistant device-aided CPPA. The security is proved by using random oracle model. The security requirements are provided by identifying and expelling individuals who violate the rules, spotting impersonated communications, and protecting the identities of othervehicle unlinkability and untraceability but its disadvantage is that it causes a large delay while travelling near an RSU.

Javed et al.[29] analyzed how safety awareness, quality of service, and security interrelate in a cooperative intelligent transportation system. To ensure that the critical neighbours were included for calculating awareness, they employed a vehicle heading-based filtration method. Additionally, weighted position error and the weighted average of the position flaws are used by vehicles to calculate awareness. This approach improves safety measures however safety awareness may be diminished if there is a history of driving violations causing neighbouring drivers to be more cautious.

Ahmad et al.[30] presented man at the centre attack a resilient trust in connected vehicles. With the help of this technique, the vehicles are able to swiftly detect malicious vehicles and their misbehaving drivers. These vehicles are subsequently removed from the list of trustworthy vehicles. It works in two stages: early identification of fraudulent nodes is the first stage, and many plausibility checks are introduced into the network to undertake entity-centric trust evaluations. Node is labelled malicious. If it doesn't meet all assessment criterion. Once a genuine node is identified then the next stage is the data-centric credibility analysis, which assesses the data reliability. The extra overhead created by using numerous sources to give the reputation of the sender is this trust model's flaw.

Guo et al.[31] proposed chameleon hashing for secure data communication in vehicles. The proposed protocol is extremely suited in a realistic vehicular environment because with substantially less computing effort, it accomplishes authentication process for both vehicle-to-vehicle and vehicle-to-roadside traffics. But the drawback in using chameleon hashing technique is key exposure problem that is the non-transferability attribute necessitates the recipient's consent to ultimately reveal a secret key which reduces the accuracy rate in performing detection.

Ghaleb et al.[32] proposed to detect sophisticated attacks using hybrid and multifaceted stastistical classifier. The suggested model is context aware and uses a context reference in place of static security criteria. The geographical and temporal correlation of the mobility data from the communication vehicles is used to generate and update the context reference using Kalman and Hampel filters. The hybrid context aware model (HCA-MDS) and non-hybrid context aware model (DCA-MDS) have low accuracy in identifying misbehaving and benign vehicles, respectively.

Haddadpajouh et al.[33] presented a multi-view fuzzy consensus clustering approach for identifying malware threat attribution. In this approach, five advanced persistent threat families along with 12 different extracted views for attribution are applied. Fuzzy criteria is also used in distinguish between existing overlaps between different sorts of malicious state which assist to solve the threat attribution problem effectively but it takes more time and the accuracy achieved through this approach is 95%.

3. Proposed system

In modern era, vehicular ad hoc network is highly proliferating in the area of intelligent transportation system, as it has a feature to sense the physical world with wireless sensor capable to sense, process and perform communication. While communicating, the data exchange between vehicles and road side units over non-secure channels makes the network vulnerable to several attacks and security flaws. So, to provide secure and reliable data sharing, this proposed mechanism implements the novel machine learning based authentication technique combined with blockchain and IPFS. The mechanism of this approach is performed as follows, the events which was retrieved by RSU is stored initially in IPFS and then smart contract is carried out to determine whether the event is malicious or non-malicious which was classified by the machine learning event authentication model. In this proposed system, initially each vehicle is assigned to cluster using K-means clustering approach. By using this approach, the vehicles are grouped together and the node with the highest performing capability is chosen as the cluster head. Cluster head plays a vital role and it keeps an eye on the neighbourhood vehicle to monitor it's behaviour. To categorize the vehicles into normal, abnormal and malicious vehicles, each vehicle is provided with a distrust value of 1.0 when the vehicle enters into the network. If the distrust value exceeds the threshold value, the vehicle is put into the category of blacklist and vehicles under the blacklist is taken as malicious vehicles. Based upon the distrust value, the vehicle is classified as malicious and non-malicious. After the categorization, a support vector machine classifier is used and it is provided with a set of training samples which detects the malicious event messages and after it is converted to decision rules. After each updating of decision rules, it is stored in IPFS which was later retrieved to validate the event. If the event is found to be malicious by decision rules, it is instantly dropped by the vehicle. In such manner, only valid messages are forwarded to the network. The functional diagram of the suggested system is depicted in **Figure 2**.

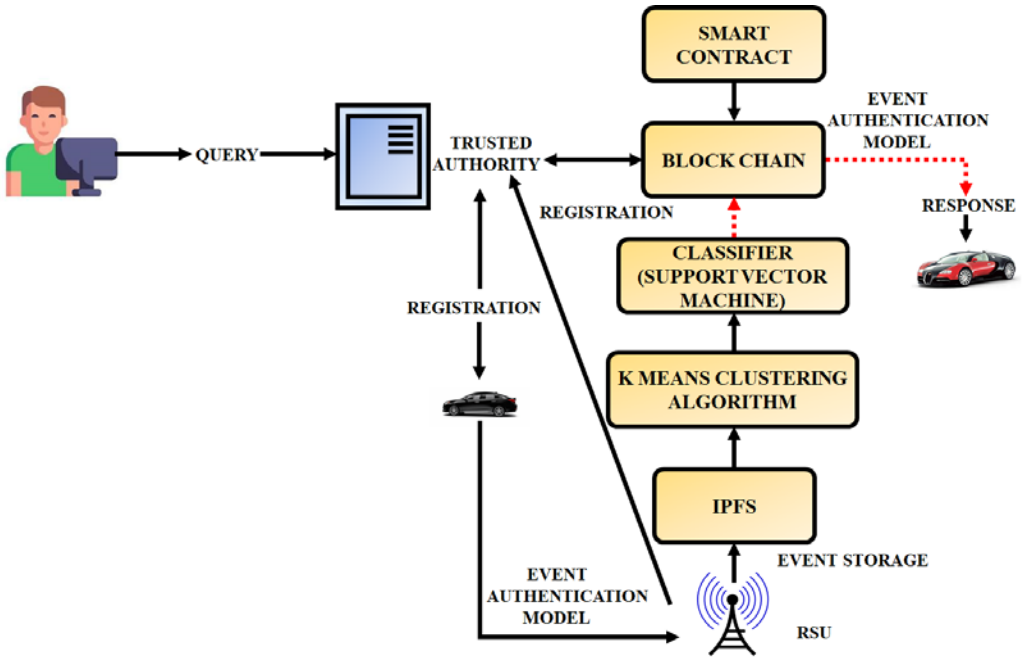

Figure 2. Proposed functional diagram.

Compared to conventional approaches, the proposed system enhances its efficiency by less time consumption to perform vehicle and event authentication and the communication cost gets dropped. The SVM classifier in this proposed system not only enhances the attack detection rate but also it improves its efficacy in utilizing minimum time to perform detection. The proposed approach outperforms other conventional techniques in detecting the malicious events with high efficiency and accuracy. The proposed system work

involves entities such as trusted authority, RSU, IPFS, smart contract and blockchain. The workflow of this system is described as follows.

3.1. Registration and validation

Recently, the modern technologies have achieved tremendous growth which is adopted across all aspect of life that is interconnected to the internet, with intelligent vehicle (IV) being one of those. These IVs gets integrated with RSUs and interact among each other, generating a virtual network. If an IV needs to accompany with the network, it forwards a request message to trusted authority. In this proposed work, trusted authority act as a registrar and it gathers all the information which is related to IV and it issues a public key. The issued key comprises of a distinct ID, the pseudonym ID and the public and private key. By the issuance of this certificate, vehicles get interacted with each other. Trusted authority is also used in case of data authentication that keeps the data's integrity intact. To handle the data in a more secure way, registration as a means of data authentication is employed in the proposed system. This kind of operation enables users to access the system based on the reliability of their credentials, that improves the network's functionality as well as efficiency.

Analysis of algorithm

In this system work, initially registration is to be done if the vehicle needs to join the network. For performing registration, it has to upload its information to the trusted authority to retrieve a registration certificate. The issued certificate is digital secure based certificate which is cryptographically linked. Vehicle conducts with trusted authority and acquires the pseudonym ID during the event which happens once. The MAC address and actual ID are taken as an input for registration which assists to consume less computational time and power. The certification procedure is a secure technique, and throughout the network, vehicles interact for the first time employing the supplied pseudonym ID, and novel IVs are validated. The IVs which are registered are stored in the IPFS that uses minimal processing capability to store data.

Algorithm IV 1 Registration and validation

1: Initialization
2: **Inputs:** MAC address, No. of vehicles.
3: **Outputs:** IV registration, MAC address validation, stores in IPFS.
4: **While** IV is in connection with network do
5: Registration
6: Check $IV_{owner}, Real_{ID}, MAC_{address}$
7: Return registered IV
8: " validation of ID"
9: if $hash_1 = hash_2$ then
10: " Requested IV is authentic"
11: Else
12: " Requested IV is inauthentic "
13: end if
14: " MAC validation"
15: MAC_1= Address on IV
16: MAC_2= Address on IPFS
17: if $MAC_1 = MAC_2$ then
18: " MAC is valid. IV successfully registered on the network"
19: Else
20: " MAC is invalid. IV failed to register on the network"
21: end if
22: "Stored on IPFS"
23: "forward data to IPFS"
24: IPFS response
25: "return hash of data"
26: end while
27: END

3.2. Road side unit (RSU)

RSU is used in routing the packets between the distant locations. Roadside units, a specialized wireless device positioned on the side of the road, are used by V2I and V2V and it is a fixed infrastructure that sends data to other RSUs and roaming vehicles is coupled with an internet facility. In order to process and communicate information and to coordinate activities, it offers distributed and cooperative applications in which other RSUs and vehicles collaborate. In this topology, the events collected by road side units are stored in IPFS and then the execution is made by smart contract which uses the decision rules to validate the messages.

3.3. Inter planetary file system

Efficient storage management is a significant part in this proposed system which is carried out by inter planetary file system. It's a decentralized system that is used in both data gathering and exchange. It saves the data as hashes, which are mapped using a distributed hash table and posted on the blockchain. As soon as the data stored in this file system, they are broken up into little parts, each of which is 256 kbs. Each fragment's hash value is computed as well as uploaded into the distributed hash table which is then stored in the blockchain. To maintain the system in an efficient way. It offers hash storage that is independent and distributed. In addition to this, it computes the reputation values of the vehicle. It takes the stored data from IPFS and perform authentication by clustering into malicious and non-malicious. After performing K-means clustering, SVM is trained to determine the malicious messages which are then converted to decision rules. It decides whether to accept or reject before forwarding.

3.4. Cluster formation using K-means clustering

In K-means clustering approach, each vehicle is assigned to a cluster which considers the connection reliability model as an objective function. It is computed using numerous parameters such as traffic density, relative speed, and node distance. In clustering, the vehicles are grouped together and the node with the highest capacity is chosen to serve as the cluster head to perform efficient communication between the vehicles.

To perform grouping of vehicles, the K-means approach uses the connection reliability model. By using traffic density λ and relative speed ΔV, the connection reliability model is computed as,

$$P_t(t) = \frac{4.D_r}{\sigma\Delta v\sqrt{2\pi}} \times \frac{1}{t^2} \times e^{-\frac{\left(\frac{2Dr}{t}-\mu\Delta v\right)^2)}{2\sigma\Delta v^2}} \tag{1}$$

where $D_r[m]$ represents the vehicle transmission area and Δv denotes the relative speed. The relative speed [km/h] depicts the mobility of two vehicles. While traffic density [vehicle/km] represents the number of vehicles on a stretch of road.

Consider V_j be a vehicle; $1 < j < N$, with velocity V_j and position (x_j, y_j). C_i is taken as the centroid $1 < i < k$, with velocity v_i and position (x_i, y_i). By taking into account, the connection reliability model is computed in Equation (2) as,

$$p_{ij}(T_{ij}, \lambda) = \begin{cases} \frac{\delta.\lambda}{\lambda_c}\int_{t_o}^{t_o+T_{ij}} T_{ij}p(t)dt, & if\ \delta, \lambda < \lambda_c \\ \int_{t_o}^{t_o+T_{ij}} T_{ij}p(t)dt & otherwise \end{cases} \tag{2}$$

where T_{ij} in the equation represents the probability that the link between the vehicle and the centroid c_i remains available and it is computed using,

$$T_{ij} = \frac{L_{ij}}{\Delta v_{ij}} = \frac{(y_i-y_j)^2+(x_i-x_j)^2}{\overrightarrow{v_i-v_j}} \tag{3}$$

Based upon the value of the connection reliability model and the associated cluster head, each vehicle is assigned to a cluster. By accounting for acceleration and position changes, this value provides an

approximation of the maximum amount of time that this vehicle can stay in the cluster. So, using this strategy, the likelihood that a vehicle would join a cluster depends not only on the distance between it and the cluster head, but also on the speed and traffic density differences. As a result, the objective function *F* of the K-means algorithm is therefore based on network dependability and it is expressed as,

$$F = avgmax_c \sum_{i=1}^{k} \sum_{x_j \epsilon C_i} p_{ij}(T_{ij}, \lambda) \tag{4}$$

The cluster members are indicated by a red color and the cluster head is represented in yellow color which is shown in **Figure 3**.

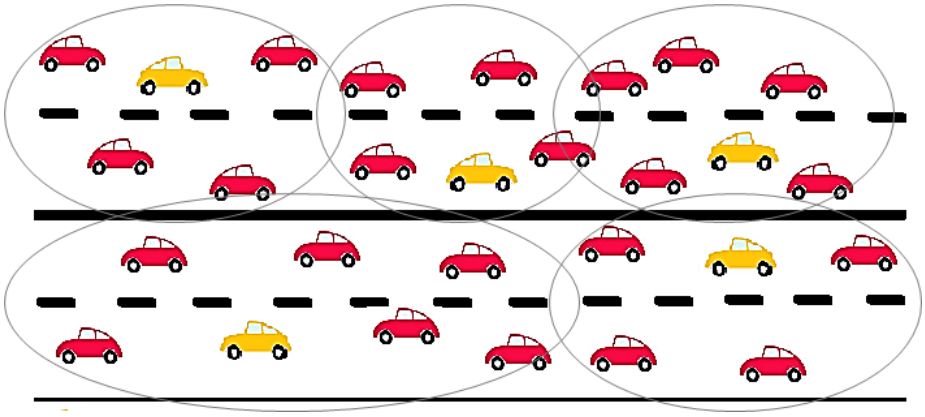

Figure 3. Clustering of vehicles.

After performing clustering, the cluster head is given a distrust value. Each cluster head has provided with a cluster key as CA. The CA is in charge of maintaining the cluster keys. When one of the cluster nodes remains cluster head for an extended period of time, its CA can renew it. When a vehicle enters the VANET, it is assigned a distrust value of 1.0. The vehicle then transmits its initial distrust value to the nearby vehicle, which acknowledges and locates itself in the white list. When the distrust value exceeds the threshold value, the vehicle is added to the black list. To estimate the threshold value, the average number of vehicles within the range of communication is to be computed. The threshold value is computed by,

$$N_v = \frac{N\ avg}{R\ avg} \tag{5}$$

where *N avg* represents the average number of vehicles and *R avg* indicates the vehicles within the communication range.

The vehicle which act as the cluster head is the most reliable vehicle in the network. Monitoring is the process of keeping track of data on a vehicle's behaviour. The vehicle that keeps an eye on the other vehicle in the neighbourhood is said to be verifier. The distrust value of the verifier is on par with or lower than that of the other vehicle. Based upon the distrust value, verifier catergorizes the vehicles into malicious normal and abnormal vehicles. This categorization helps the SVM classifier to detect the malicious event messages easily. Rather checking all the vehicles inside the network, it takes only the malicious vehicles and identify the event messages which is not authentic and it is immediately dropped.

3.5. SVM classifier

SVM classifier is used to protect each vehicle against a fake data injection attack by performing authentication. It determines whether the message is authentic or not. After determining, it is transformed to decision rules. Each decision rules identified by this process is stored in IPFS with timestamp till final updation. Smart contract is carried out to obtain the most updated decision rules from IPFS and it is checked for validation. The smart contract is run over a blockchain network using if/then logic to analyse the harmful event

categorised by the machine learning event authentication model. If the decision rule is found to be malicious then it is instantly dropped by the vehicle. By this way, the authentic message is forwarded in the network.

A support vector machine classifier is figured out to validate the event in this work. Given a set of training samples.

The intension of this classifier will determine a division hyperplane from the sample space based upon the training sample *D*. The hyperplane can be modeled us shown in Equation (7).

$$D = \{(X_1, Y_1), (X_2, Y_2), \dots (X_n, Y_n)\} and\ Y_i \in (-1, +1) \quad (6)$$

$$W^T x + b = 0 \quad (7)$$

where, $W = w_1, w_2, \dots, w_d$. It represents the hyper plane's direction-determining normal vector, and *b* stands for the hyper plane's distance from the coordinate source. In sample space, the distance of point *X* is expressed as,

$$r = \frac{|w^T x + b|}{||w||} \quad (8)$$

Based upon the following constraints, the plane classifies the training sample.

$$w^T x_i + b \geq +1, y_i = +1 \quad (9)$$

$$w^T x_i + b \leq +1, y_i = -1 \quad (10)$$

For (x_i, y_i) in the training sample *D*.

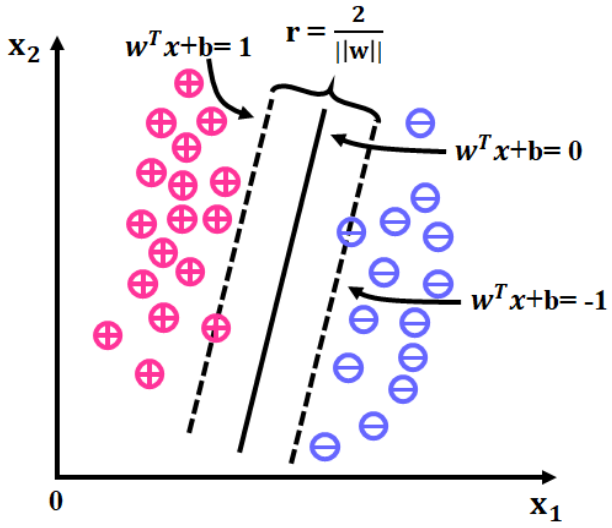

Figure 4. Training sample.

In **Figure 4**, the point in the training sample which is very near to the hyperplane is known as support vectors. The following equation is used to compute the total distance to the hyperplane from two different types of heterogeneous support vectors,

$$r = \frac{2}{||w||} \quad (11)$$

From the training sample D, the support vector machine gets constructed and it categorize the energy vectors retrieved from the first and second wavelet coefficients of current signal to valid or not valid. Though SVM act as a state of art models in data mining, it is incomprehensible black box model regarding non-linearity. Rules retrieved from SVM model provide comprehensibility and convenience to carry out the rules for classification without any requirement to maintain the bulk storage. After the determination of malicious event, the conversion to decision rules is done and it is shown in **Figure 5**.

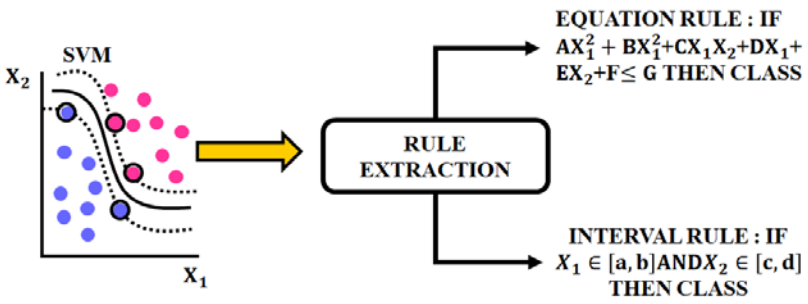

Figure 5. SVM to decision rule conversion.

In IPFS, the event gets uploaded by RSU. These stored events processed by smart contract and constructs the decision rules and update it in IPFS. Vehicle frequency pulls up the decision rules via execution smart contract and uses the decision rules to validate the messages before forwarding to next hop.

3.6. Smart contract

Smart contract is executed through a blockchain network by if/then logic and it carried out to assess the malicious event which is classified by the machine learning event authentication model. Furthermore, smart contracts do not require a middleman to execute since the code of a smart contract is checked by all blockchain network members. The elimination of the intermediary from the contract significantly reduces the expenses in addition to this it offers reliability, security, accuracy and sustainability.

3.7. Blockchain

The blockchain is downloaded and updated by all connected automobiles. Blockchain is a distributed ledger that records event reports and the whole record of the vehicle's trustworthiness. The workflow of blockchain is shown in **Figure 6.**

In the blockchain network, the vehicle that experiences an event, for instance a collision, will broadcast the event messages with various parameters to other vehicles. The vehicles consider the event message and determine whether it is local to the area. Next, the nearby vehicles examine the event message's other parameters. Before spreading an event message farther, each vehicle individually verifies it to stop spamming, DOS attacks, and other obtrusive system attacks. Prior to verifying the event message, the vehicles receiving the event message first examine the blockchain's reliability for the sender vehicle.

If the message is deemed reliable, it is stored in the local memory pool. The mining vehicles acquire various event messages from an unverified event message pool and check that the received messages' parameters are accurate. According to the verification policy, if the received event notification is legitimate and reliable, its trust level will be updated. Depending on whether messages are genuine or misleading, the trust level changes over time. The more true messages a vehicle has, the more trustworthy it becomes. Once a fresh block is introduced to the local chain, the mining vehicles will update the sender vehicle's trust level and send it to the blockchain. In order to stop malevolent vehicles from corrupting the database, the PoW consensus process is implemented which determines how long the new block should be kept in the network.

Blockchain is used to address the key problems with message distribution. The suggested solution uses blockchain to store the integrity of nodes and messages in a distributed public ledger that is suitable for reliable message dissemination. Through this blockchain, vehicle can access the required information.

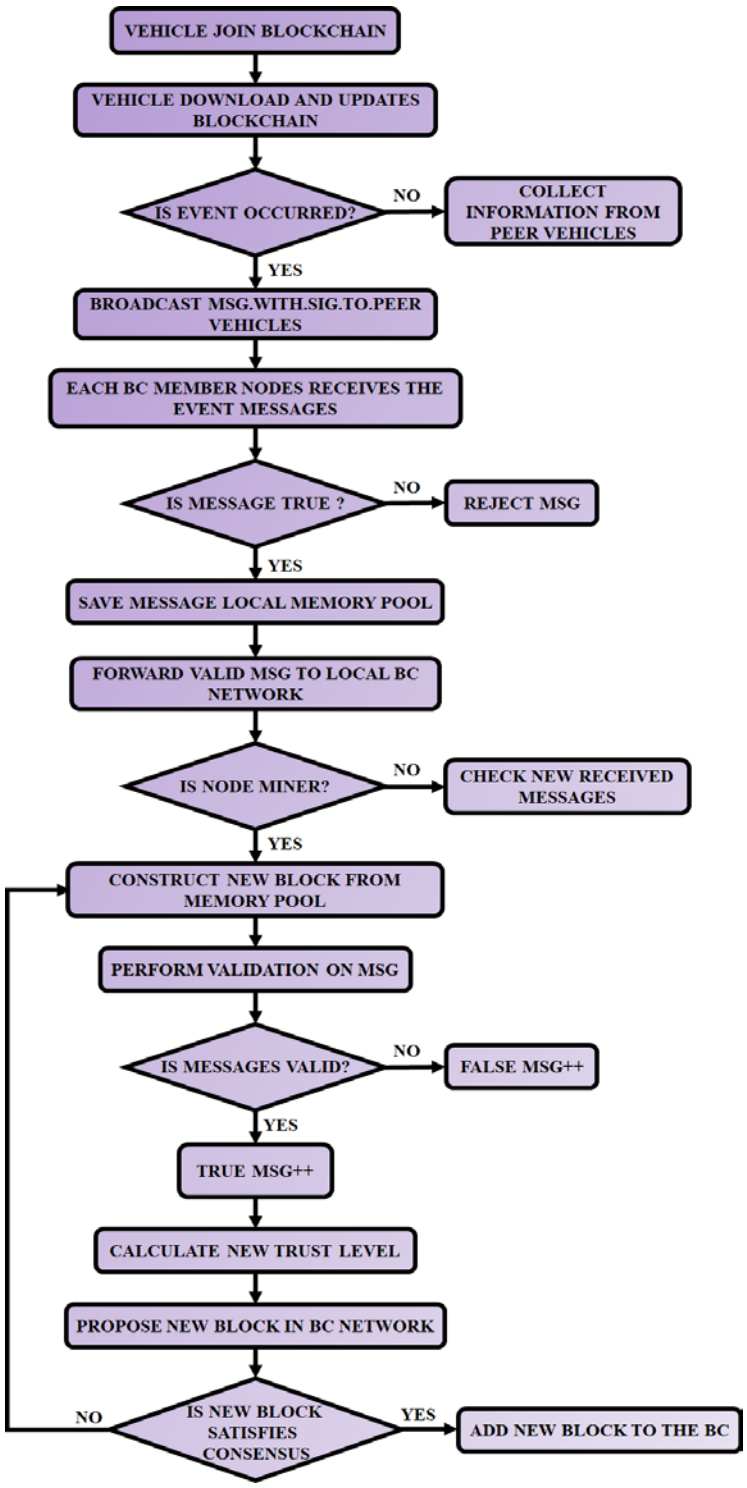

Figure 6. Workflow of blockchain.

4. Results and discussion

Recently, intelligent vehicle plays a vital role in transportation sector as it has many advantageous features. But privacy and security problem arises when sharing of events between the vehicles takes place. So, to get rid of this problem, in this proposed framework, SVM with the assistance of K-means clustering technique is employed to detect the malicious events which assist to share the events in a secure way and it is implemented with distributed blockchain technique for secure message dissemination. The performance analysis is carried out in NS2 simulator and is validated with other existing approaches to scrutinize its efficiencies. **Table 1** lists the parameter specifications of the proposed work.

Table 1. Parameter specifications.

Parameters	Values
Total vehicles	200–500
Transportation model	Krauss
Transmission range	300 m
Simulation area	3000 m × 3000 m
Speed of vehicle	20 to 90 Kmph

Performance metrics: regarding event validation time, vehicle verification time, and communication expense, the suggested system's effectiveness was assessed and is compared with the existing technique such as IBFS with EES technique, multimedia data sharing scheme, blockchain IBFS framework and edge service provider technique.

Vehicle authentication time is carried out by computing the vehicles per unit of time for authentication. In **Table 2**, the measured average vehicle authentication time by altering the vehicle count is represented.

Table 2. Vehicle verification time.

Vehicle count	Suggested system (SVM)	Blockchain IBFS framework	IBFS with EES technique	Edge service provider technique	Multimedia data sharing scheme
100	1.72	2.3	2.5	2.9	2.8
200	1.75	2.5	2.4	2.8	3.0
300	1.80	2.4	2.6	3.1	3.2
400	1.85	2.6	2.2	3.0	3.4
500	1.88	2.1	2.7	3.2	3.3
600	1.89	2.7	2.9	3.3	3.6
700	1.97	2.8	3.2	3.2	3.5
Average	1.83	2.48	2.64	3.07	3.25

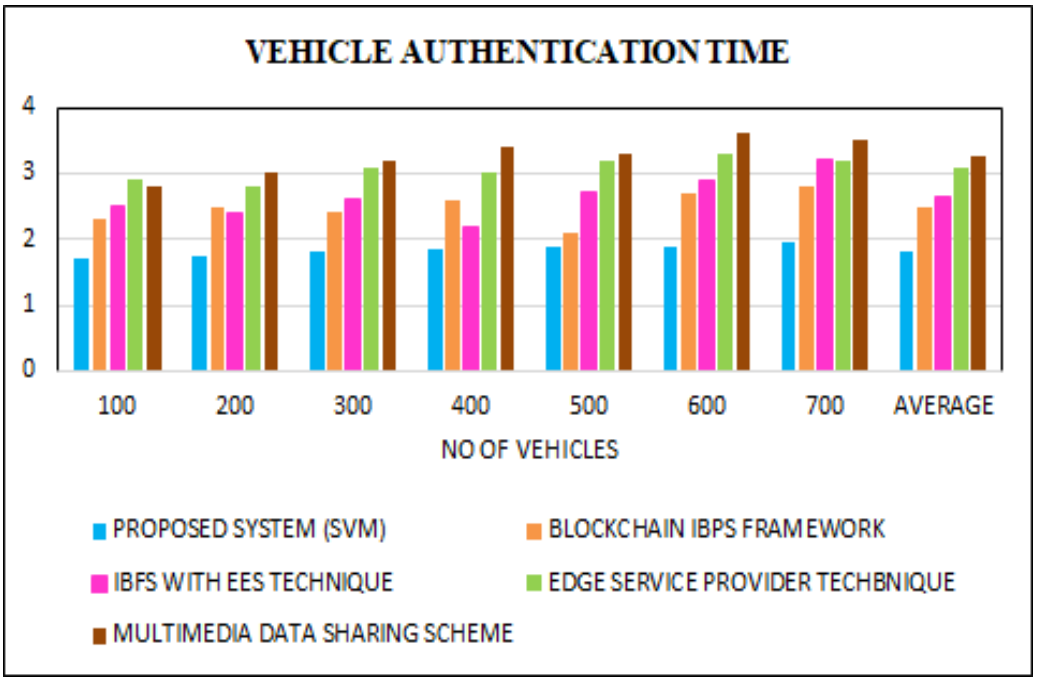

Figure 7. Vehicle authentication time analysis.

In this proposed system, vehicle authentication time is compared with other approaches by changing the vehicle's count. From the comprehensive outcome which was shown in **Figure 7**, the proposed average vehicle authentication consumes less time compared to existing techniques. SVM classifier not only performs detection in an efficient way but also it achieves less time consumption. **Table 3** shows the results of altering the number of vehicles used to measure the average event validation time.

The average event processing time is computed by

$$Average\ event\ processing\ time = \frac{time\ span\ for\ all\ events}{total\ number\ of\ events}$$

Table 3. Event validation time.

Vehicle count	Suggested system (SVM)	Blockchain IBFS framework	IBFS with EES technique	Edge service provider technique	Multimedia data sharing scheme
100	103	113	123	142	146
200	101	115	125	143	148
300	105	121	127	145	147
400	108	126	135	146	152
500	107	131	132	148	154
600	106	134	133	144	151
700	110	136	138	149	156
Average	105.7	125.1	130.4	145.2	150.5

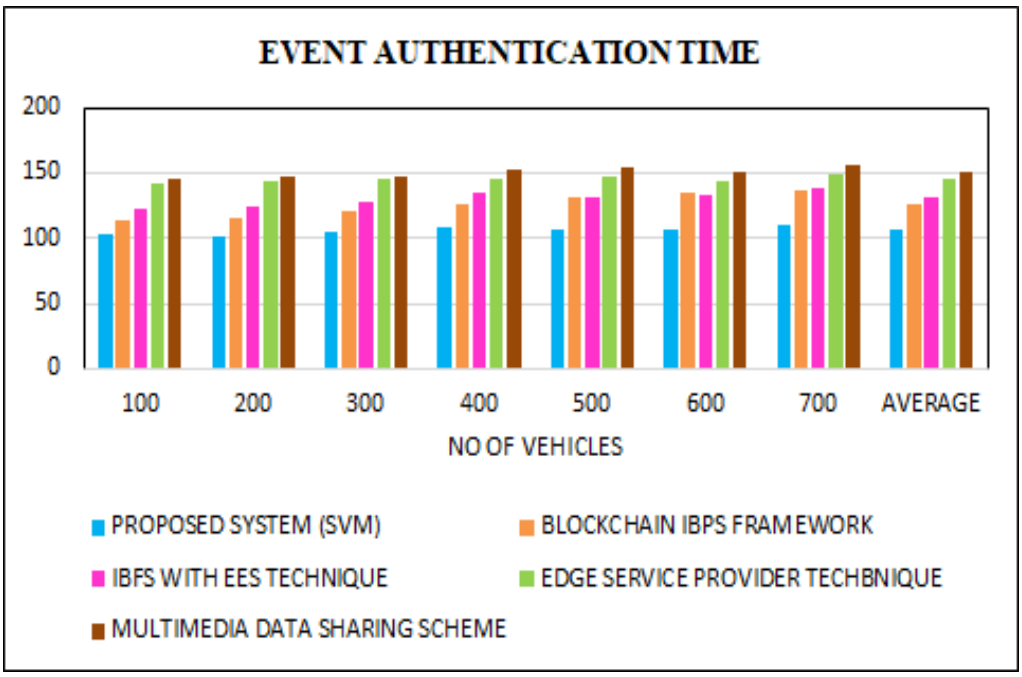

Figure 8. Event authentication time analyses.

Figure 8 clearly illustrates that as compared to other methods the suggested solution's average event validation time is minimal. The minimum time consumption is achieved because the information required for authentication is quickly updated and it is placed in blockchain with the fraction of time. **Table 4** illustrates how the number of vehicles affects the communication cost.

The average communication expense for the suggested work seems to be minimal which is represented in **Figure 9**. The reason for low time consumption in communication cost is, almost all the information required by vehicles is kept in inter-planetary file system. In order to reduce packet payloads, just the notice message is forwarded to VANET. Hence the communication cost is minimized.

Comparison of vehicle density between proposed system and blockchain IBFS framework is represented in **Table 5** and **Figure 10**.

Table 4. Communication expense.

Vehicle count	Suggested system (SVM)	Blockchain IBPS framework	IBFS with EES technique	Edge service provider technique	Multimedia data sharing scheme
100	14,342	17,231	22,354	28,695	29,787
200	20,124	32,342	36,553	35,654	38,965
300	25,987	42,563	47,635	49,845	48,698
400	28,934	45,767	50,564	45,468	56,789
500	31,392	46,223	51,673	50,123	51,232
600	32,542	47,212	52,356	54,652	53,698
700	33,045	49,834	54,765	53,214	54,652
Average	26,623	40,167	45,128	45,336	47,688

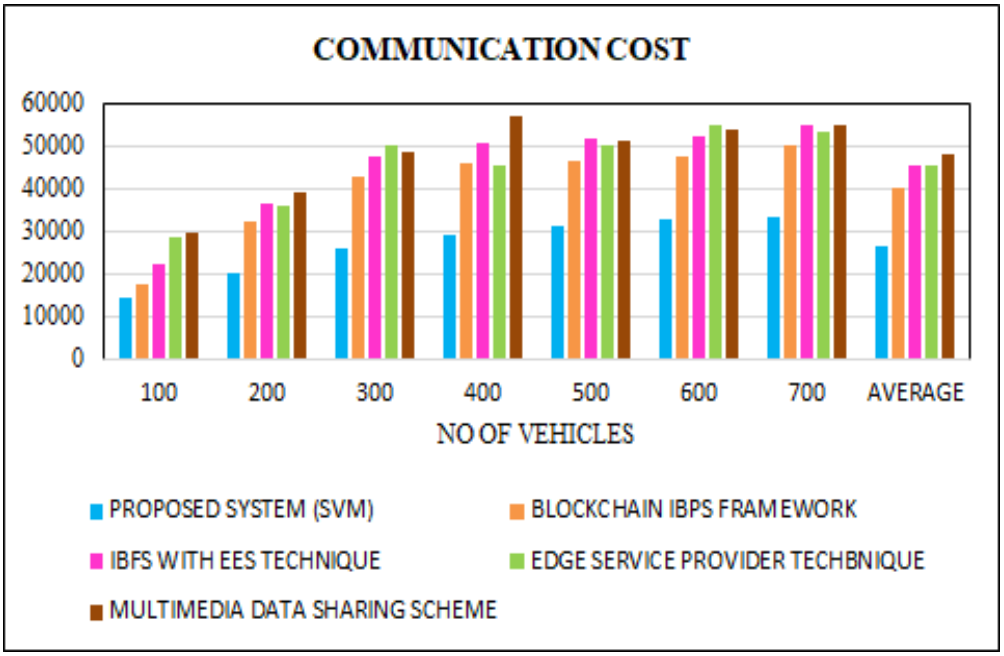

Figure 9. Communication expense analyses.

Table 5. Vehicle density comparison.

Vehicle density	Proposed system (SVM)	Blockchain IBFS framework
100	89	88
200	92	81
300	88	85
400	95	80
500	94	87
600	90	84
700	95	82

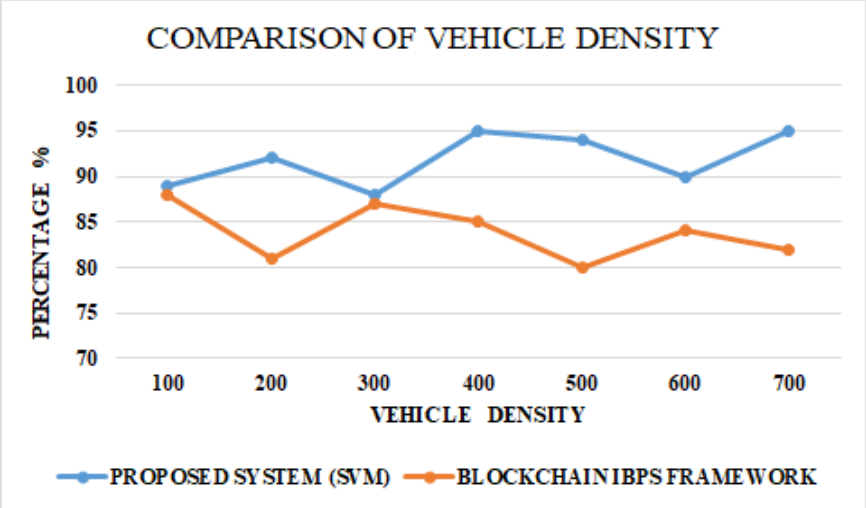

Figure 10. Comparison of vehicle density.

Attack detection rate

Attack detection rate vs network density is represented in **Figure 11**. In this figure, *x*-axis and *y*-axis is represented by network density and attack detection rate respectively. The figure clearly illustrates that compared to traditional approaches, the proposed system has improved its attack detection rate in a tremendous way.

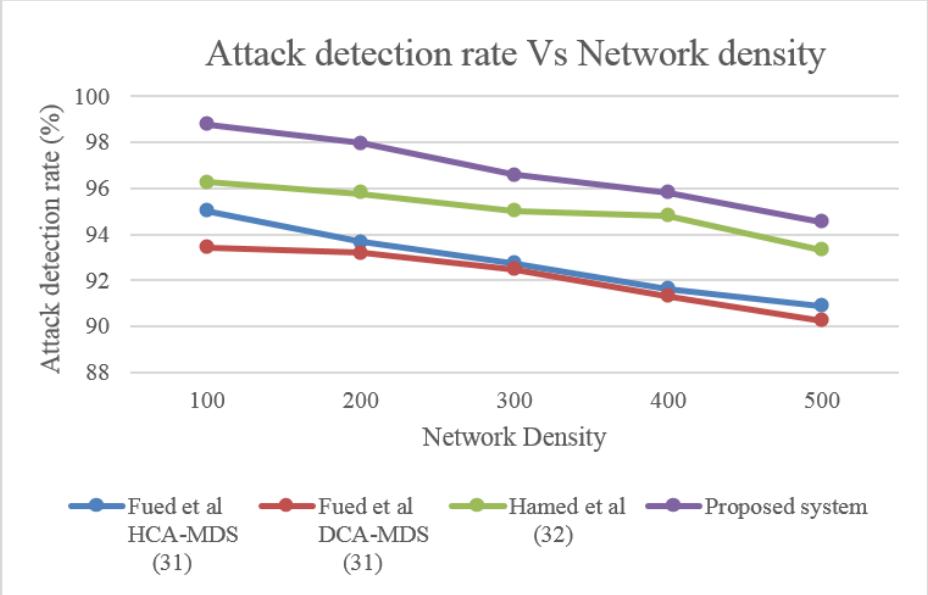

Figure 11. Attack detection rate vs network density.

Attack detection rate vs number of malicious vehicles is represented in **Figure 12**. In this figure, *x*-axis and *y*-axis is represented by number of malicious vehicles and attack detection rate respectively. **Figure 12** clearly indicates that the SVM classifier in this proposed system performs better in detecting the attack compared to traditional techniques concerning percentage of malicious vehicles.

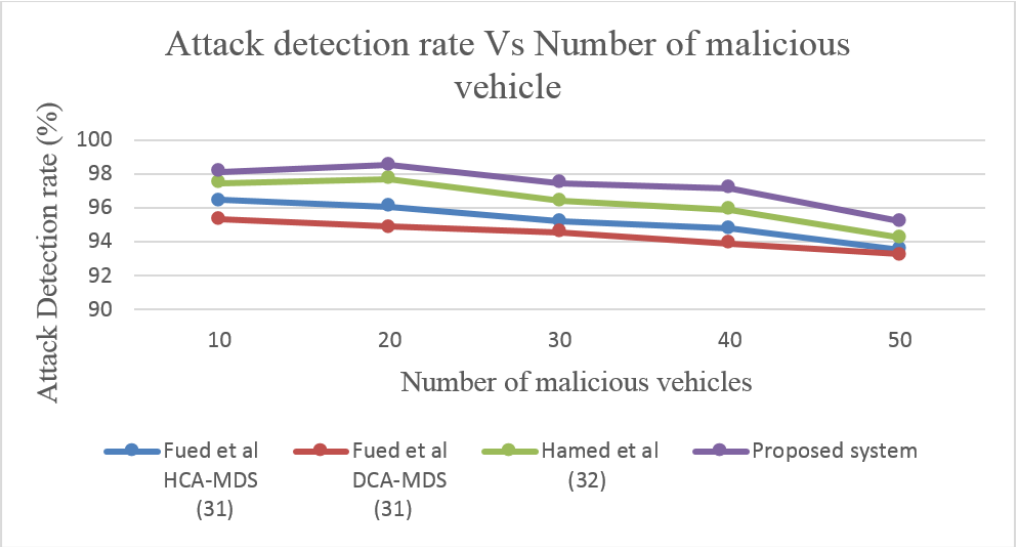

Figure 12. Attack detection rate vs number of malicious vehicles.

With regard to the two scenarios that were chosen, the detection capacity dropped as network density and the presence of malicious nodes increases.

The proposed work examines the accuracy of event spoofing detection against other approaches. The accuracy graph is shown in **Figure 13**. It clearly indicates that, the proposed approach improves event spoofing detection accuracy by 96%. The confidence model of the event utilized in this system proposal distinguishes genuine and false occurrences in an efficient way because of persistent monitoring as well as nodes scoring. Due to additional neighbours being taken into consideration for collaborative event validation in the proposed solution, event source behavior's time and duration component is more accurately portrayed.

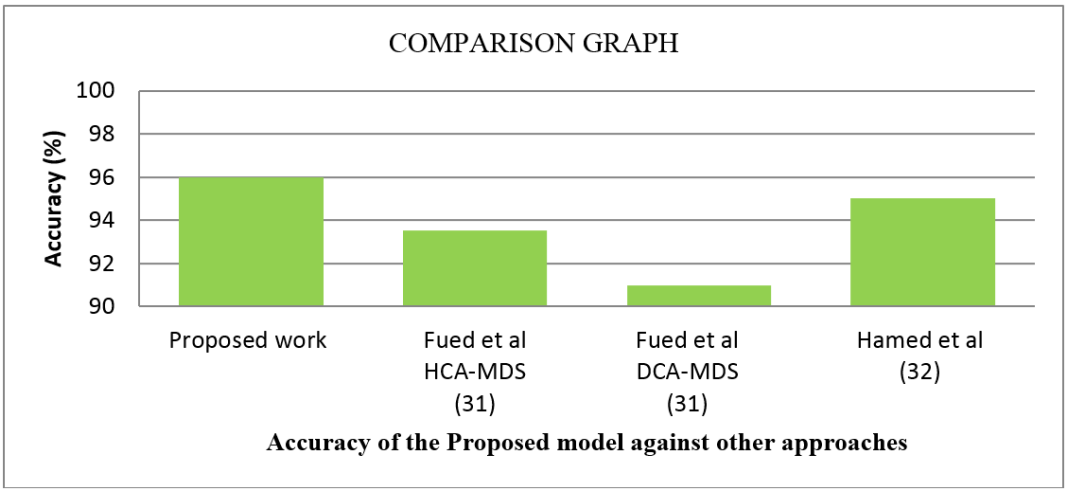

Figure 13. Accuracy of the proposed model against other approaches.

5. Conclusion

In attempt to prevent internal vehicles from broadcasting misinformation, this proposed work implements the novel machine learning based approach for message authentication by integration of blockchain with IPFS. This system works efficiently in executing protected event sharing, certification, and verification between IVs. The distributed blockchain based transaction storage model, which effectively defends against hostile assaults while identifying rogue vehicles. The efficacy of this access authentication system is then assessed after examining the safety and legitimacy of the suggested system. The proposed system is validated according to its vehicle verification time, event validation time and communication expense. Analogizing with other

existing work, it performs its process with minimum consumption time and the event confidence model in this presented system achieves higher in malicious event detection. It outperforms the existing approaches and it attains high security and protects the vehicle from malicious attackers. A potential future research focus on this field is proposing a unique, lightweight, and improved neural network-based message authentication system which will successfully detect network intruders.

Author contributions

Conceptualization, ANP and SVM; methodology, ANP and SVM; software, ANP and SVM; validation, ANP and SVM; formal analysis, ANP and SVM; investigation, ANP and SVM; resources, ANP and SVM; data curation, ANP and SVM; writing—original draft preparation, ANP and SVM; writing—review and editing, ANP and SVM; visualization, ANP and SVM; supervision, SVM; project administration, SVM.

Conflict of interest

The authors declare no conflict of interest.

References

1. Zhu H, Yuen KV, Mihaylova L, et al. Overview of environment perception for intelligent vehicles. *IEEE Transactions on Intelligent Transportation Systems* 2017; 18(10): 2584–2601. doi: 10.1109/TITS.2017.2658662
2. Al-Shareeda MA, Anbar M, Hasbullah IH, et al. Survey of authentication and privacy schemes in vehicular ad hoc networks. *IEEE Sensors Journal* 2020; 21(2): 2422–2433. doi: 10.1109/JSEN.2020.3021731
3. Qu F, Wu Z, Wang FY, et al. A security and privacy review of VANETs. *IEEE Transactions on Intelligent Transportation Systems* 2015; 16(6): 2985–2996. doi: 10.1109/TITS.2015.2439292
4. Al-Heety OS, Zakaria Z, Ismail M, et al. A comprehensive survey: Benefits, services, recent works, challenges, security, and use cases for SDN-VANET. *IEEE Access* 2020; 8: 91028–91047. doi: 10.1109/ACCESS.2020.2992580
5. Verma S, Zeadally S, Kaur S, et al. Intelligent and secure clustering in Wireless Sensor Network (WSN)-based intelligent transportation systems. *IEEE Transactions on Intelligent Transportation Systems* 2021; 23(8): 13473–13481. doi: 10.1109/TITS.2021.3124730
6. Elkhail AA, Refat RUD, Habre R, et al. Vehicle security: A survey of security issues and vulnerabilities, malware attacks and defenses. *IEEE Access* 2021; 9: 162401–162437. doi: 10.1109/ACCESS.2021.3130495
7. Yang A, Weng J, Cheng N, et al. DeQoS attack: Degrading quality of service in VANETs and its mitigation. *IEEE Transactions on Vehicular Technology* 2019; 68(5): 4834–4845. doi: 10.1109/TVT.2019.2905522
8. Jan S A, Amin NU, Othman M, et al. A survey on privacy-preserving authentication schemes in VANETs: Attacks, challenges and open issues. *IEEE Access* 2021; 9: 153701–153726. doi: 10.1109/ACCESS.2021.3125521
9. Liu B, Jia D, Wang J, et al. Cloud-assisted safety message dissemination in VANET-cellular heterogeneous wireless network. *IEEE Systems Journal* 2015; 11(1): 128–139. doi: 10.1109/JSYST.2015.2451156
10. Alsayfi MS, Dahab MY, Eassa FE, et al. Securing real-time video surveillance data in vehicular cloud computing: A survey. *IEEE Access* 2022; 10: 51525–51547. doi: 10.1109/ACCESS.2022.3174554
11. Ribouh S, Phan K, Malawade AV, et al. Channel state information-based cryptographic key generation for intelligent transportation systems. *IEEE Transactions on Intelligent Transportation Systems* 2020; 22(12): 7496–7507. doi: 10.1109/TITS.2020.3003577
12. Thoms GRW, Muresan R, Al-Dweik A. Chaotic encryption algorithm with key controlled neural networks for intelligent transportation systems. *IEEE Access* 2019; 7: 158697–158709. doi: 10.1109/ACCESS.2019.2950007
13. Tan H, Choi D, Kim P, et al. Comments on “dual authentication and key management techniques for secure data transmission in vehicular ad hoc networks”. *IEEE Transactions on Intelligent Transportation Systems* 2017; 19(7): 2149–2151. doi: 10.1109/TITS.2017.2746880
14. Zhao Z, Guardalben L, Karimzadeh M, et al. Mobility prediction-assisted over-the-top edge prefetching for hierarchical VANETs. *IEEE Journal on Selected Areas in Communications* 2018; 36(8): 1786–1801. doi: 10.1109/JSAC.2018.2844681
15. Zhu C, Zhu X, Ren J, et al. Blockchain-enabled federated learning for UAV edge computing network: Issues and solutions. *IEEE Access* 2022; 10: 56591–56610. doi: 10.1109/ACCESS.2022.3174865
16. Li Q, Tian Y, Zhang Y, et al. Efficient privacy-preserving access control of mobile multimedia data in cloud computing. *IEEE Access* 2019; 7: 131534–131542. doi: 10.1109/ACCESS.2019.2939299
17. Li B, Liang R, Zhu D, et al. Blockchain-based trust management model for location privacy preserving in VANET. *IEEE Transactions on Intelligent Transportation Systems* 2020; 22(6): 3765–3775. doi: 10.1109/TITS.2020.3035869

18. Tan H, Chung I. Secure authentication and key management with blockchain in VANETs. *IEEE Access* 2019; 8: 2482–2498. doi: 10.1109/ACCESS.2019.2962387
19. Xu R, Li C, Joshi J. Blockchain-based transparency framework for privacy preserving third-party services. *IEEE Transactions on Dependable and Secure Computing* 2022. doi: 10.1109/TDSC.2022.3179698
20. Liu T, Yang Y, Huang GB, et al. Driver distraction detection using semi-supervised machine learning. *IEEE Transactions on Intelligent Transportation Systems* 2015; 17(4): 1108–1120. doi: 10.1109/TITS.2015.2496157
21. Virupakshappa MM. An efficient vehicle traffic maintenance using road side units in VANET. *Imperial Journal of Interdisciplinary Research* 2016; 3(2016): 783–784.
22. Kim S. Impacts of mobility on performance of blockchain in VANET. *IEEE Access* 2019; 7: 68646–68655. doi: 10.1109/ACCESS.2019.2918411
23. Zhang L, Wang J, Mu Y. Secure and privacy-preserving attribute-based sharing framework in vehicles ad hoc networks. *IEEE Access* 2020; 8: 116781–116795. doi: 10.1109/ACCESS.2020.3004247
24. Horng SJ, Lu CC, Zhou W. An identity-based and revocable data-sharing scheme in VANETs. *IEEE Transactions on Vehicular Technology* 2020; 69(12): 15933–15946. doi: 10.1109/TVT.2020.3037804
25. Zhong H, Zhang S, Cui J, et al. Broadcast encryption scheme for V2I communication in VANETs. *IEEE Transactions on Vehicular Technology* 2021; 71(3): 2749–2760. doi: 10.1109/TVT.2021.3113660
26. Alharthi A, Ni Q, Jiang R. A privacy-preservation framework based on biometrics blockchain (BBC) to prevent attacks in VANET. *IEEE Access* 2021; 9: 87299–87309. doi: 10.1109/ACCESS.2021.3086225
27. Lin C, He D, Huang X, et al. BCPPA: A blockchain-based conditional privacy-preserving authentication protocol for vehicular ad hoc networks. *IEEE Transactions on Intelligent Transportation Systems* 2020; 22(12): 7408–7420. doi: 10.1109/TITS.2020.3002096
28. Aghabagherloo A, Delavar M, Mohajeri J, et al. An efficient and physically secure privacy-preserving authentication scheme for vehicular ad hoc networks (VANETs). *IEEE Access* 2022; 10: 93831–93844. doi: 10.1109/ACCESS.2022.3203580
29. Javed MA, Hamida EB. On the interrelation of security, QoS, and safety in cooperative ITS. *IEEE Transactions on Intelligent Transportation Systems* 2016; 18(7): 1943–1957. doi: 10.1109/TITS.2016.2614580
30. Ahmad F, Kurugollu F, Adnane A, et al. MARINE: Man-in-the-middle attack resistant trust model in connected vehicles. *IEEE Internet of Things Journal* 2020; 7(4): 3310–3322. doi: 10.1109/JIOT.2020.2967568
31. Guo S, Zeng D, Xiang Y. Chameleon hashing for secure and privacy-preserving vehicular communications. *IEEE Transactions on Parallel and Distributed Systems* 2013; 25(11): 2794–2803. doi: 10.1109/TPDS.2013.277
32. Ghaleb FA, Maarof MA, Zainal A, et al. Hybrid and multifaceted context-aware misbehavior detection model for vehicular ad hoc network. *IEEE Access* 2019; 7: 159119–159140. doi: 10.1109/ACCESS.2019.2950805
33. Haddadpajouh H, Azmoodeh A, Dehghantanha A, et al. MVFCC: A multi-view fuzzy consensus clustering model for malware threat attribution. *IEEE Access* 2020; 8: 139188–139198. doi: 10.1109/ACCESS.2020.3012907