Dr.Ritu Agarwal, 2026, 14:3
ISSN (Online): 2348-4098
ISSN (Print): 2395-4752

International Journal of Science, Engineering and Technology
An Open Access Journal

A Trust-Aware Blockchain and AI-Driven Secure Communication Framework for Internet of Vehicles Using Hybrid SDN and Modified PBFT

Dr.Ritu Agarwal[1], Aryan Sharma[2], Abhinav Singh[3]
[1]Assoc Professor Department of Information Technology
[2,3]Department of Applied Mathematics Delhi Technological University
Delhi, India

Abstract- The Internet of Vehicles (IoV) is playing a critical role in modern transportation systems, as vehicles interact with each other and roadside infrastructures in real-time. Although this technology can increase road safety and traffic efficiency, it creates various security challenges for IoV. For instance, Sybil, replay, and impersonation attacks can be launched on IoV networks, thereby making them susceptible to attacks. In this paper, we propose a hybrid model that utilizes blockchain tech-nology, SDN, and artificial intelligence-based anomaly detection mechanisms. Specifically, we use random forest to detect abnor-mal behavior of malicious vehicles based on their interactions. Moreover, a modified PBFT (mPBFT) algorithm is employed to improve consensus efficiency by selecting reliable nodes. The proposed model is tested under a simulated IoV envi-ronment and obtains approximately 92detection. In addition, it significantly decreases consensus delay as compared to the conventional PBFT algorithm. Overall, this model has shown good efficiency, scalability, and security in IoV systems.

Keywords: Internet of Vehicles (IoV), Blockchain, SDN, Artificial Intelligence, Security, mPBFT.

I. INTRODUCTION

The Internet of Vehicles (IoV) is emerging as a critical component of contemporary transport networks. It enables the exchange of data between vehicles and roadside infrastructure in real-time, facilitating better safety and traffic control.

For instance, when a vehicle senses an accident or braking incident, it could instantly transmit a notification message to neighboring vehicles, allowing the latter to react promptly and prevent any possible collision.

Nevertheless, such an environment poses a significant se-curity threat since vehicles frequently connect and disconnect from the network, making it hard to authenticate that a certain message comes from a credible source. Thus, the architecture is prone to various forms of attacks.

Some popular attacks in IoV include Sybil attacks, replay attacks, and impersonation attacks. In a Sybil attack, a solitary vehicle generates several aliases to manipulate the network's behavior. In a replay attack, a message already sent over the network is again broadcasted by the malicious party. Meanwhile, an impersonation attack involves an adversary who tries to pretend as a trustworthy vehicle to disseminate misinformation.

Suppose there is a vehicle that can produce false alerts about traffic based on different identities that would compel other cars to make route changes. The situation could cause traffic chaos and possibly dangerous incidents.

The traditional approach to central security will be inef-fective in the IoV environment. It has scalability problems and a single point of failure that would affect all users. Trust management in large vehicular networks would be difficult.

Blockchains offer decentralization in recording transactions that make the process of tampering with the stored data more complicated. However, the consensus algorithms like Proof-of-Work are slow since they involve solving mathematical problems.

To solve these challenges, this paper proposes a novel framework using blockchain, SDN, and AI anomaly detection techniques. mPBFT protocol will lower the delay in consensus by involving only trustworthy nodes in the process. The solu-tion involves using SDN controllers to manage the network, AI algorithm to detect anomalies, and blockchains for securely storing data.

The key contribution of this research is to leverage the combination of trust-based consensus along with AI-based detection in an SDN-controlled IoV scenario.

A. Problem Statement

Despite the considerable progress achieved in vehicular communications, the issue of secure and reliable vehicular message exchange in IoV networks remains very challeng-ing. State-of-the-art approaches can either rely on centralized control planes vulnerable to failure, or employ blockchain so-lutions imposing excessively high latencies and computational overheads.

In addition, most available schemes do not provide mecha-nisms for detecting malicious behavior at runtime along with managing reputation scores of the participating cars. As a result, there is a need for a robust and intelligent mechanism providing:

- Authentication and secure dissemination of the vehicular messages;
- Detection of vehicles with adversarial behavior patterns;
- Adequate latency required to fulfill real-time require-ments imposed by IoV;
- Robust trust management in highly dynamic environ-ments.

B. Contributions

The primary contributions of this research paper are listed below:

- The design of a security system for IoV integrating Blockchain, SDN, and AI-based anomaly detection.
- A trust-conditioned mPBFT consensus algorithm that reduces signaling overhead and achieves around 40% less consensus delay compared to normal PBFT.
- A Random Forest model for detecting malicious nodes based on their communication behavior, with an average accuracy of approximately 92%.
- An always-on trust management module that con-tinuously evaluates the behavior of vehicles and prevents low-reputation nodes from accessing the network.
- A multi-layer defense mechanism that incorpo-rates cryptographic techniques, AI detection, and blockchain technology to counteract Sybil attacks, replay attacks, impersonation attacks, and DoS at-tacks.

II. RELATED WORK

The current research trend involves enhancing the security of IoV systems by employing various technologies including blockchain technology, artificial intelligence, and Software Defined Networking (SDN).

In [1], Zhang et al. developed a vehicular communica-tion system supported by a blockchain and PBFT consensus protocol to ensure the safety of data exchange. The method enhances data integrity, although it causes excessive commu-nication overhead.

In Liu et al.'s work [2], the authors considered using deep learning technologies in order to detect malicious activities in vehicular networks. Although their approach works well in terms of malicious detection, no distributed solution for trust information storage was provided, making it unreliable.

Sharma et al. [3] offered a vehicular network architecture based on SDN technology that uses centralized controllers to handle communications and traffic control operations. Such architecture allows increasing the effectiveness of vehicular networks; however, the lack of a trusted data storage method poses some problems in terms of security.
While addressing certain issues, all those techniques dis-cussed above solve only one part of the problem, with some focusing on blockchain, others – on artificial intelligence, or SDN, etc.

In our approach, we combine blockchain, artificial intelli-gence and vehicular networks to build a novel framework that will improve scalability and reduce latency of communications in the network while increasing the effectiveness of malicious activities detection.

III. SYSTEM ARCHITECTURE

The suggested framework for IoV security incorporates a hybrid approach consisting of blockchain, SDN, and AI for enabling protected, scalable, and intelligent vehicle to infrastructure communications. The system architecture com-prises four main components; these include Vehicles, Road Side Units (RSUs), SDN Controller Cluster, and Permissioned Blockchain Network (shown in Fig. 1).

A. Vehicles

Vehicles can be considered as nodes responsible for gen-erating and communicating safety information like conges-tion alerts, collision warnings, and hazard warnings to other entities in the network. The responsibility of performing all cryptographically-based operations lies on the On-Board Unit (OBU) present within each vehicle.

Prior to the transmission of any information by the vehicle, it first creates an ECC key pair and applies digital signatures with the help of its private key in order to associate a vehicle's identity with the message and prevent any alteration to the message. In practical scenarios, when a vehicle detects a road obstruc-tion, it creates and signs a safety message prior to broadcasting it for the benefit of receiving nodes.

B. Road Side Units (RSUs)

RSUs act as intermediary stations through which messages from mobile vehicles are routed back to the wider infrastruc-ture network.

Furthermore, RSUs undertake initial message validation processes such as eliminating duplicate messages and verify-ing the timestamps of messages to eliminate false messaging to the controller nodes.

For instance, in the event that multiple vehicles report an identical road hazard at the same time, the RSU integrates all of these notifications and sends out one unified message to the SDN layer.

C. SDN Controller Node Cluster

The SDN controller node cluster is the backbone of the entire system architecture. It facilitates centralized manage-ment and analyzes the data collected from vehicles using sophisticated analytics. The inclusion of SDN technology ensures precise traffic management and control within the vehicular environment [3].

Tasks delegated to the controller cluster involve:

- Verification of digital signatures to verify message origin
- Extraction of behaviour attributes associated with vehi-cles
- Application of artificial intelligence-based anomaly de-tection algorithms
- Recalculation of trust values of particular vehicles
- Routing of verified transactions to blockchain infrastruc-ture level

Using the AI component, malicious intention will be re-vealed through various behavioural traits such as rate of transmission, geographical consistency, and timing.

For instance, where there is rapid transmission of contra-dicting position updates by a particular vehicle, the AI unit will detect the Sybil behaviour and update the trust score of the said vehicle accordingly.

D. Blockchain Infrastructure

At this network infrastructure layer, decentralised and tamper-proof data storage is implemented via a permissioned blockchain model, thus limiting involvement to authorised parties such as SDN controllers to avoid Sybil attacks at the consensus layer.

Validation of transactions involves the use of mPBFT (modified PBFT) algorithm which maintains balance

between Byzantine resilience and processing time delay.

After all validations are carried out successfully and trust score is achieved, the transaction will be recorded immutably on the blockchain as a ground truth record.

E. End-to-End Process of Message Transfer

The process is as follows:

1. Message composition and signing are done by the vehi-cle using its ECC private key.
2. Signed message is transferred to the nearest RSU.
3. RSU transfers the message further to the SDN controller cluster.
4. Message authentication and its analysis using AI algo-rithms.
5. Validated messages are sent to the blockchain network.
6. Transactions are validated and added to blockchain using mPBFT.

With such architecture, it is possible to ensure secure and effective communication in IoV, eliminating different types of attacks.

IV. METHODOLOGY OF PROPOSED SYSTEM

The method involves the use of blockchain technology, SDN, AI-powered anomaly detection, and trust management to provide reliable vehicular communications. Four major subsystems are presented within the architecture: Vehicles, RSUs, SDN Controller Cluster, and Permissioned Blockchain Network.

Main aspects include the protection of message origination, message validation, misbehaviour recognition, and decentral-ized storing of transactions. Optimised Consensus Process: To improve throughput efficiency, the framework employs trust-based admission control; hence, nodes with a high rep-utation are allowed to participate in consensus, thus reducing the cost of communication. The SDN controllers also allow parallel transactions to be verified to increase efficiency.

A. Creation of Vehicle Messages

The OBU of each vehicle is tasked with creating and dis-seminating traffic-related messages. As the message is about to be sent by the OBU, it is first digitally signed using a public key cryptosystem based on the ECC algorithm.

In a practical sense, upon detection of an emergency situa-tion such as a sudden brake or accident on the road, the vehicle creates a warning message, digitally signs it, and transmits it to the nearest RSU.

B.,Forwarding Messages through RSUs

RSUs serve as intermediaries that transfer messages from the vehicle layer to the network control plane layer. They accept messages from vehicles and relay them to the SDN controller layer.

To prevent duplication of messages and congestion, RSUs carry out preliminary checks regarding timestamps and dupli-cates.
In case of multiple reports by vehicles about the same congestion, RSU combines the signals and sends a notification to the controller, thereby lessening the amount of data sent up.

C. Message Validation and AI-based Anomaly Detection

1) Model Architecture: The anomaly detection model is based on a Random Forest model, trained on a set of data containing labeled messages from the vehicle's communication system. It utilizes a set of features that consist of communica-tion message rate, speed variability, location consistency, and timing of packets.

The reason for choosing the Random Forest algorithm is its effectiveness on structured data, with low complexity and requires minimal hyperparameter tuning when it comes to variations of the communication pattern.

Data Preparation and Model Training

The anomaly detection model was trained on synthetic IoV dataset created according to VeReMi design guidelines. VeReMi benchmark is a tool used for testing various types of attacks performed against vehicular communication systems, which

include attacks on legitimate driving trace, propagation of congestion, and coordinated Sybil and replay attacks.

The following are the feature vectors from the vehicle communication for each label:

- Message transmission rate
- Speed variance
- Location consistency
- Inter-packet transmission variance

An 80:20 ratio of training versus test data will be used in data segmentation. For the Random Forest, there are 100 individual tree learners; the Gini Index is utilised for the splitting criterion.

Classifier evaluation metrics include precision, recall, and accuracy. The machine learning framework employed during the classifier's training is the Python programming language.

Once messages have been received by the SDN controller from the RSUs, the following steps will take place in the processing pipeline:

- Validation of the message through digital signatures to authenticate its credibility
- Identification of the message's feature vector representing its behaviour
- AI-driven identification of any potential anomalies in the message
- updating each vehicle's trust score depending on the results

The AI system analyses parameters such as message rates location consistency, and any other abnormal transmissions. For instance, if a vehicle sending messages in an impossi- ble geographical area over very little time becomes a Sybil candidate based on the above analysis.

Trust Management Mechanism

Each vehicle possesses a dynamically generated trust score that changes based on how it behaves over time. Legitimate vehicles will have high scores, while suspicious or malicious vehicles will have deductions made from their scores.

Vehicles with low scores are marked for attention, where their messages can be either filtered out or examined more carefully.

Repeatedly generating false alarms makes a vehicle lose trust until it is not allowed to communicate in the network anymore.

F. Transaction Storage Using Blockchain Technology

After a message is verified, the message will become part of a transaction which will be broadcast to the blockchain network. Only authorized SDN controllers will be able to access the blockchain ledger and make modifications to it.

The transactions are validated using the mPBFT consensus algorithm, and stored in the immutable ledger. Since the transactions are chosen by reputable nodes according to the trust management scheme, less node-to-node communication is required.

A verified accident alert message will be stored in the ledger and becomes immutable, and hence cannot be changed.

G. Workflow Process

The end-to-end workflow process of the proposed architec-ture can be described as follows:

1. The vehicle creates a message and signs the message with ECC.
2. The signed message is then sent to the closest RSU.
3. The RSU sends the message to the SDN controller.
4. The controller checks the signature and runs anomaly detection with AI.
5. The vehicle trust score is updated dynamically depend-ing on the result.
6. Only the message that comes from trusted vehicles will proceed for more processes.

Fig. 1. Proposed IoV Blockchain Security Architecture

Algorithm 1 Secure IoV Communication based on Trust, Blockchain and AI Techniques
Require: M , V ID, Ti
Ensure: Message is saved in blockchain
1: Generate ECC keys: (PK, SK)
2: Sign message M using SK
3: Broadcast ⟨V ID, M, Signature⟩ to RSU
4: Relay message to SDN controller
5: if signature is invalid then
6: Mark vehicle as malicious
7: Decrease trust score Ti
8: Reject message
9: else
10: Extract message features
11: Perform AI anomaly detection
12: if malicious activity detected then
13: Decrease trust score Ti
14: Add malicious activity in blockchain
15: else
16: Update trust score Ti
17: Add message into pool of transactions
18: end if
19: end if
20: Select trusted nodes Neff = {i | Ti > Tthreshold}
21: Select Leader Leader = r mod |Neff |
22: Perform parallel verification
23: if number of verifications |Nverified| ≥ 2 |Neff | then
24: Run consensus protocol
25: Add block to blockchain
26: end if
27: Prune malicious nodes

- The qualified message will be forwarded to theblockchain system.
- Finally, the blockchain verifies and records the transac-tion using the optimized mPBFT with the trust condition.

This layered structure provides efficient, safe, and intelligent IoV communications while eliminating potential Sybil, replay, and impersonation attacks. The filtering technique based on dynamic trust scores and the enhanced consensus algorithm reduce signaling costs.

V. ALGORITHM FOR SECURE IOV COMMUNICATION CONSENSUS MECHANISM

In the presented system architecture, an efficient, safe, and low latency transaction verification is accomplished by using a trust-based version of the Practical Byzantine Fault Tolerance algorithm (mPBFT). The main reason behind the popularity of PBFT among permissioned blockchains is its high fault tolerance and low latency [6].

While the classic version of PBFT allows all nodes to participate in any consensus round, the proposed framework limits participation only to the trusted nodes having live scores above a certain level.
The eligible node set for admission is defined as:

$$N_{eff} = \{i \mid T_i > T_{threshold}\} \quad (1)$$

The use of selective admission results in a reduction of communication costs and increased scalability. Besides, SDN controllers allow for concurrent transaction validation, and consensus is reached once two-thirds of trusted nodes agree on a transaction.

A. Leader Selection Mechanism

The consensus coordinator is chosen dynamically each round via:
Leader = r mod |Neff | (2) where r represents the present round number and |Neff | is the size of the trusted node set.

The round-robin approach to task distribution ensures that no particular node faces an excessive workload and that attacks on the coordinator cannot be easily focused.

By way of illustration, with four SDN controllers (N = 4):

- Round 1 → Leader = 1 mod 4 = 1
- Round 2 → Leader = 2 mod 4 = 2
- Round 3 → Leader = 3 mod 4 = 3
- Round 4 → Leader = 4 mod 4 = 0

Each controller therefore receives an equitable share of lead-ership responsibility.

B. Consensus Phases

The mPBFT protocol unfolds across three sequential phases:

- **Pre-prepare Phase:** The elected leader gathers the ver-ified transactions that were sent by the SDN controllers and makes up a candidate block.
- Once the incoming messages from vehicles are validated, the leader then makes a block proposal out of the validated transactions, and sends it to other peer controllers.
- **Prepare Phase**: Independent audits for reception con-trollers are performed on the candidate block, ensuring that the transactions are genuine and the messages are authentic. Controllers that validate the message send out a prepare signal to the other reception controllers.

The validation process involves checking whether the mes-sages enclosed within the vehicle are tagged as hostile by the AI system and whether their digital signature is valid.

TABLE I
COMPARISON OF PBFT AND PROPOSED MPBFT

Metric	PBFT	Proposed mPBFT
Consensus Delay	High	Low
Throughput	Moderate	High
Scalability	Limited	Improved
Communication Overhead	High	Reduced
Leader Selection	Static	Dynamic (Fair Rotation)
Fault Tolerance	Good	Enhanced
Node Participation	All Nodes	Trusted Nodes Only
Verification Mode	Sequential	Parallel
Trust Awareness	No	Full

3) Commit Phase: Controllers proceed to the commit stage once the quota of votes for preparation is gathered (usually a supermajority). The block is then finalized and added to the chain.
Once a certain percentage of the controllers validate the authenticity of the block, it becomes an immutable part of the blockchain.

C. Advantages of mPBFT in IoV

Adopting mPBFT within the proposed architecture confers multiple benefits:

- **Reduced Latency**: Faster round completion relative to computation-heavy Proof-of-Work mechanisms
- **Scalability:** Graceful performance in dense vehicular deployments
- **Fault Tolerance:** Continued operation despite the pres-ence of faulty or adversarial nodes
- **Decentralisation:** Equitable leader rotation guards against single-controller dominance

Under a high-traffic situation when numerous vehicles are simultaneously sending data, mPBFT can achieve transaction confirmation in an instant without overburdening any specific controller.
The entire consensus algorithm enhances the level of secu-rity, efficiency, and reliability of IoV network communication.

D. Complexity Analysis

Conventional PBFT has an O(n2) cost for the number of messages that must be sent between nodes because all nodes communicate with each other. However, in the mPBFT based on trust, the number of messages drops to O(k2), which is less than O(n2). This leads to better scalability and efficiency in large-scale applications in IoVs.

It is evident from Table I that the designed mPBFT sig-nificantly surpasses the standard version in terms of latency, scalability, and communication cost. With the load balancing technique in the leader rotation phase and efficient message exchange method, the solution is ideal for time-sensitive IoV applications.

VII. PERFORMANCE ANALYSIS

Simulation testing for the system performance evaluation will be performed using different traffic load scenarios and varying adversarial injection rates. The main categories of vehicle attacks include Sybil, replay, and impersonation

A. Simulation Setup

Evaluation uses an artificial IoV environment to model realistic vehicular communication scenarios including benign traffic and adversarial behavior. Normal driving, congestion spreading, and three types of attacks are modeled.

Messages from vehicles are modeled according to prede-fined behaviors for speed, consistency in location, and message sending frequency. Adversarial messages are introduced using Sybil, replay, and impersonation attacks.

This artificial environment provides an environment for analyzing performance in different scenarios and generates results that can be reproduced.

However, an artificial environment may not accurately model the irregularity of real-world IoVs, and further research will use real traces.

- Number of Vehicles: 100–1000
- Number of RSUs: 10
- Communication Protocol: IEEE 802.11p
- Blockchain Type: Permissioned blockchain
- Consensus Mechanism: Proposed mPBFT

B. Evaluation Metrics

The framework is characterised using standard classification and networking metrics that jointly capture detection quality and operational efficiency.

1) Precision: Precision captures the fraction of system-flagged vehicles that are genuinely adversarial, indicating low false-alarm propensity.

$$Precision = \frac{TP}{TP + FP} \quad (3)$$

where TP denotes true positives and FP denotes false positives. If, for example, 90 of 100 vehicles identified as malicious are confirmed as such, precision equals 0.9.

2) Recall: Recall quantifies the fraction of all genuinely malicious vehicles that the framework correctly flags, reflect-ing coverage completeness.
where FN represents false negatives.

$$Recall = \frac{TP}{TP + FN} \quad (4)$$

If 90 of 120 actual malicious vehicles are detected, recall is 0.75.

3) Detection Accuracy: Accuracy provides a holistic mea-sure of classification correctness, accounting for both legiti-mate and adversarial vehicle classifications.

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \quad (5)$$

where TN denotes true negatives.
Elevated accuracy reflects broad competence in distinguish-ing legitimate from adversarial behaviour.

4) Consensus Delay: Consensus delay records the elapsed time from transaction submission to block commitment on the ledger.
Minimising consensus delay is critical for sustaining the responsiveness demanded by real-time IoV safety applications.

5) Network Throughput: Throughput counts the number of successfully committed transactions per unit time.
High throughput reflects the approach's capacity to handle peak loads without degradation, a prerequisite for dense ve-hicular deployments.

C. Results and Analysis

The proposed solution has shown significant enhancements compared to existing PBFT-based frameworks concerning de-tection precision, latency, and scalability. The AI anomaly detector helps increase precision and recall, whereas trust-based mPBFT decreases the cost of consensus.
More specifically, the suggested algorithm reaches 92% detection precision with corresponding improvement in pre-cision and recall values. The consensus latency is decreased by approximately 40%, and the throughput becomes higher for different network scales.

Moreover, the comparison between the existing framework and the proposed algorithm confirms the validity of the de-sign. The trust-driven mPBFT decreases consensus latency by admitting only specific nodes and performing parallel verification, which means that the amount of communication required by the baseline PBFT decreases because all nodes are included.

Finally, AI-based anomaly detection provides additional
optimization of trust scores, thus decreasing the number of qualified consensus participants, which ultimately leads to bet-ter scalability and throughput even in heavily loaded networks, ensuring its suitability for real-time vehicular applications.

As depicted in Fig. 2, trust-based node filtering increases precision by eliminating false positives at an early stage of the pipeline. The recall rate is consistent irrespective of vehicle density, indicating

that adversarial attacks have been thoroughly mitigated. Consensus latency is considerably lower than the PBFT protocol, and the impact on throughput under heavy loads is minor.

The results demonstrate improved scalability along with lower consensus delay under varying traffic conditions.

D. Discussion

The experimental results confirm that the proposed approach outperforms traditional methods in terms of detection accuracy

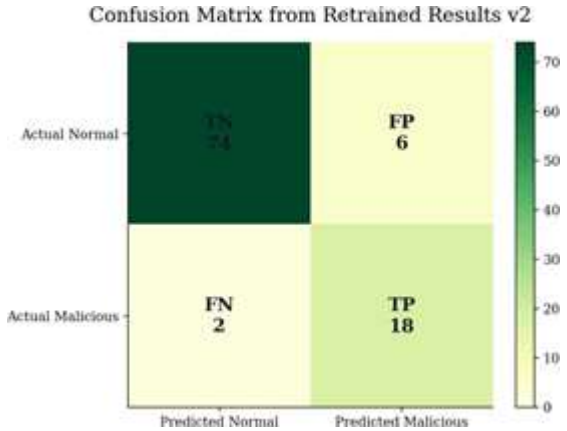

Fig. 2. Confusion matrix of the proposed Random Forest classifier.

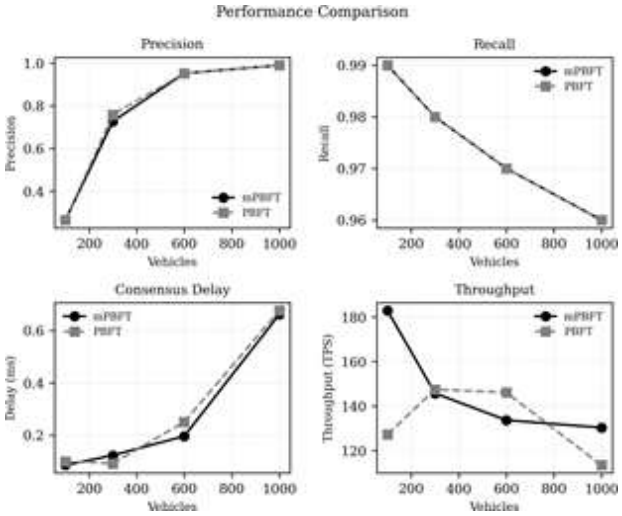

Fig. 3. Performance comparison between PBFT and the proposed trust-based mPBFT framework.

and communication delay. A combination of blockchain, AI, and SDN leads to an integrated vehicular communication platform.

It successfully combines strict security requirements with high efficiency, making its application feasible in real-world vehicular scenarios.

VIII. SECURITY ANALYSIS

The vehicular network introduces an extended attack vector due to its distributed structure and its intrinsic mobility and unpredictability [9].

The designed IoV architecture effectively defends itself from the most common attacks due to its multi-layer security based on blockchain guarantees, artificial intelligence behav-ioral monitoring, and cryptographic verification schemes.

A. Sybil Attack

A Sybil attack occurs when a node uses multiple virtual identities in order to alter the decisions of the whole network

Fig. 4. Sybil Attack Detection using AI and Trust Management

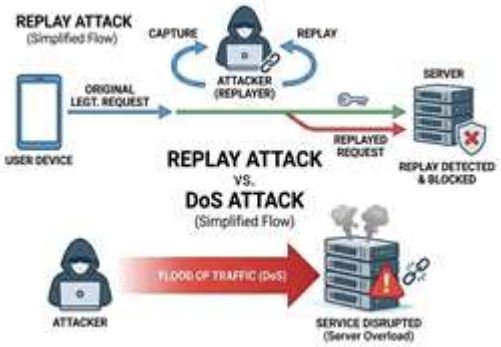

Fig. 5. Replay Attack Prevention using Timestamp and Nonce

and affect legitimate communications negatively.
The proposed approach combines AI-based behavioural analysis with dynamic trust management to identify suspicious vehicles. Abnormal communication patterns such as incon-sistent locations, excessive message transmission, or repeated identity changes reduce the trust score of the corresponding vehicle.

For instance, in case the same physical node creates several fake identities and produces conflicting traffic reports from different locations within a short period of time, the AI classifier notices it and flags the corresponding vehicle.

B. Replay Attack

A replay attack is one where an attacker captures and then resends a message from the past to create an illusion of either an event happening in the past or not occurring at all.

The system can withstand such attacks through checking the validity of message timestamps and the uniqueness of each message nonce. Any message sent using old timestamps or a repeated nonce is dropped.

C. Impersonation Attack

In an impersonation attack scenario, the attacker poses as a legitimate vehicle in order to introduce forged messages into the system through identity deception.

This can be countered using ECC-based digital signatures. In ECC-based digital signatures, the vehicles sign their mes-sages with their unique private keys which are validated by the SDN controller with the help of their respective registered public keys. Any message that cannot pass the validation process will not be accepted.

Thus, even if the attacker tries to send a message with the identity of a legitimate user vehicle, it will get detected at the verification stage.

D. Denial of Service (DoS) Attack

In a DoS attack, the network is crippled by sending too many messages to the network so that they become unman-ageable and normal communications cannot occur.

In response to this type of attack, the following two approaches can be used: The traffic analyzer that uses AI technology checks for anomalies and high message volumes which are likely signs of flooding, while the SDN controller ensures node-rate limits and quarantines the nodes involved.

If the vehicle sends too many messages over a short period compared to the expected number, it will be flagged as a flooding source, rate-throttled, and assigned a reduced trust score.

E. Summary

The multi-layered defensive posture of the proposed system—spanning cryptographic verification, AI-based be-havioural analysis, SDN-enforced traffic governance, and blockchain-enforced immutability—provides comprehensive resistance against the principal threat categories confronting IoV deployments.

F. Mathematical Security Model

The security properties of the framework are formalised through a probabilistic trust model that quantifies the like-lihood of a given vehicle being adversarial.

1) Trust Score Model: Each vehicle i is assigned a com-posite dynamic trust score Ti:

$$T_i = \alpha \cdot B_i + \beta \cdot H_i + \gamma \cdot A_i \qquad (6)$$

where:

- Bi = Behavioural consistency (message frequency, loca-tion stability)
- Hi = Historical trust score
- Ai = AI-based anomaly detection output
- α, β, γ are weighting factors such that α + β + γ = 1

Interpretation: A high Ti value corresponds to a reputable vehicle, whereas a low value signals adversarial or erratic conduct.

2) Attack Detection Probability: The probability of cor-rectly identifying a malicious vehicle is:
Pdetect = 1 − Pfalse (7) where Pfalse is the false-classification probability.

$$P_{detect} = 1 - P_{false} \quad (7)$$

With a false detection rate of 0.1, the detection probability evaluates to Pdetect = 0.9.

3) Replay Attack Prevention Model: Message validity with respect to replay prevention is expressed as:

$$Valid(M) = \begin{cases} 1, & \text{if } |t_{current} - t_{message}| < \Delta t \text{ and } n \notin N_{used} \\ 0, & \text{otherwise} \end{cases}$$

where Δt is the allowable time window.
Interpretation: Messages exceeding the temporal tolerance or bearing a recycled nonce are unconditionally rejected.

$$f < \frac{N}{3} \quad (9)$$

4) Consensus Security Model: The mPBFT protocol main-tains safety provided the fraction of Byzantine nodes satisfies:

where:

- f = number of malicious nodes
- N = total number of SDN controllers

Interpretation: This approach tolerates up to one-third of the controller population being adversarial without compro-mising the integrity of consensus outcomes.

5) Overall Security Condition: Global system security holds when:

where Tthreshold is the minimum admissible trust level.

$$T_i > T_{threshold} \quad \text{and} \quad P_{detect} \to 1 \quad (10)$$

Vehicles whose trust scores fall beneath this threshold are quarantined and excluded from the network, ensuring that only reputable nodes contribute to vehicular communication.

IX. LIMITATIONS

The proposed architecture was evaluated using simulated vehicular communication data, which may not completely represent real-world traffic conditions. In large-scale vehic-ular environments, the SDN controller layer may experience additional processing overhead during peak traffic conditions. Furthermore, the anomaly detection module currently relies on lightweight machine learning techniques prioritised for low latency, which may limit the detection of highly sophisticated attacks.

X. FUTURE WORK

Future work will focus on validating the framework using real vehicular datasets and large-scale smart transportation environments. More advanced deep learning approaches such as GNN and LSTM models may also be explored for im-proved behavioural analysis. In addition, adaptive consensus mechanisms and edge-assisted processing can be investigated to further reduce latency and improve scalability.

XI. CONCLUSION

This work has outlined a comprehensive security model for IoV through blockchain technology, SDN, AI-driven anomaly detection, and trust-dependent mPBFT. The entire model tack-les issues related to vehicular networking: message integrity, live trust management, and on-the-go threat mitigation.

The AI component detects malicious nodes by analyzing their behavior, the blockchain is used for storing secure transactions, SDN acts as a central point for efficient message handling, and mPBFT minimizes signaling requirements while being Byzantine fault tolerant.

In real-world applications, any abnormal activities such as fake congestion reports or replying safety messages are detected by the anomaly detector, which prompts timely adjustments in the trust ratings, thereby ensuring that any suspicious data does not enter the blockchain. It enhances the

credibility of information across the network and promotes safe driving conditions.

Experiments show that the developed model surpasses exist-ing PBFT-based systems in terms of detection accuracy, preci-sion and recall, lower consensus delay, and higher transaction rates.

mPBFT with trust condition benefits these improvements through the reduction of nodes, parallel verification, and lim-ited rounds of consensus, allowing low latency and necessary conditions for real-time applications.

Overall, the presented architecture provides a scalable and secure approach for intelligent vehicular communication in IoV environments and offers a practical direction for future IoV security research.

REFERENCES

1. Y. Zhang et al., "Blockchain based secure vehicular communication system," IEEE Transactions on Vehicular Technology, 2020.
2. X. Liu et al., "AI driven security framework for Internet of Vehicles," IEEE Access, 2021.
3. J. Kang et al., "Blockchain for secure and efficient data sharing in vehicular edge computing," IEEE Internet of Things Journal, 2019.
4. M. Dorri et al., "Blockchain in Internet of Things: Challenges and solutions," IEEE IoT Journal, 2019.
5. M. Conti et al., "A survey on security and privacy issues of blockchain technology," IEEE Communications Surveys & Tutorials, 2018.
6. M. Castro and B. Liskov, "Practical Byzantine Fault Tolerance," in Proc. OSDI, 1999.
7. S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008.
8. H. Hartenstein and K. Laberteaux, "A tutorial survey on vehicular ad hoc networks," IEEE Communications Magazine, 2008.
9. J. Petit and S. E. Shladover, "Potential cyberattacks on automated vehicles," IEEE Transactions on Intelligent Transportation Systems, 2015.
10. W. Viriyasitavat et al., "Blockchain-based business models for Internet of Vehicles," IEEE Communications Magazine, 2019.
11. X. Lin et al., "Security and privacy in vehicular networks: Challenges and opportunities," IEEE Wireless Communications, 2017.
12. K. Zhang et al., "Blockchain-based secure data sharing system for Internet of Vehicles," IEEE Access, 2018.
13. Q. Xia et al., "MeDShare: Trust-less medical data sharing among cloud service providers via blockchain," IEEE Access, 2017.
14. L. Zhou et al., "A secure and efficient data sharing scheme based on blockchain in vehicular networks," Future Generation Computer Systems, 2020.
15. Z. Lu et al., "Connected vehicles: Solutions and challenges," IEEE Internet of Things Journal, 2014.
16. A. Singh et al., "AI-enabled secure communication in IoV using blockchain," IEEE Access, 2023.
17. B. Kumar et al., "Trust-based vehicular communication using SDN and ML," IEEE Internet of Things Journal, 2022.