Secure and Reliable Vehicular Information Sharing via Edge Aware Trust and DAG Based Blockchain

IEEE Publication Technology, *Staff, IEEE,*

***Abstract*—Edge Aware Trust (Bayesian), Secure (Block Chain), Reliability (?), DPoS and DBFT, IoV, RSU,**

***Index Terms*—Block Chain, Internet of Vehicles, DAG, Bayesian Optimization.**

I. Introduction

The rapid advancement of computing power, storage capacity, battery technology, heterogeneous wireless access networks, and the Internet of Things (IoT) has significantly driven the evolution of the Internet of Vehicles (IoV) [1]. IoV represents a new paradigm that integrates intelligence into vehicles to overcome the inherent limitations of traditional Vehicular Ad hoc Networks (VANETs) [2]. Conventional VANETs were primarily designed to improve traffic efficiency and road safety through real time communication among vehicles using existing wireless technologies with or without the support of roadside units (RSUs) [3]. However with the increasing complexity of modern transportation systems and the rising number of traffic accidents worldwide, traditional VANETs face challenges in supporting large scale, intelligent, and safety critical vehicular applications. In this context, IoV provides a promising framework to enable smarter, safer, and more efficient vehicular communication and transportation services.

The IoV architecture supports diverse communication modes including Vehicle to Infrastructure (V2I), Vehicle to Sensor (V2S), Vehicle to Roadside Unit (V2RSU), Vehicle to Personal Device (V2P), and Vehicle to Vehicle (V2V). Among these the V2V communication plays a critical role by enabling the fastest and shortest information exchange between vehicles on the road. Through V2V communication, vehicles can share real time data such as speed, location, traffic congestion, and accident information which significantly improves driving safety, traffic efficiency, and overall traffic management. At the same time the V2RSU communication allows vehicles to upload sensed data to RSUs that serve as gateways to backend infrastructure and cloud platforms. Using onboard sensors such as cameras, LiDAR, and radar, vehicles continuously generate large volumes of data that are transmitted through V2V and V2RSU links to support intelligent transportation services.

Despite these benefits, V2V and V2RSU communications in IoV face serious security, privacy, and trust challenges. Malicious vehicles or compromised RSUs may inject false or forged information that does not reflect actual traffic conditions which can degrade traffic efficiency and, in extreme cases it lead to severe accidents that threaten human lives. Moreover, as the number of connected vehicles continues to grow, the IoV ecosystem becomes increasingly vulnerable to hacking, data manipulation, unauthorized access, and privacy leakage. Traditional V2V systems also struggle with scalability when supporting large scale IoV networks, while vehicles may hesitate to share data due to concerns about privacy and security. As a result the reliable trust evaluation and secure data sharing have become fundamental requirements for the practical deployment of IoV.

Existing trust management systems are typically classified into centralized and distributed approaches. Centralized trust management relies on a single authority to evaluate and store trust values which leads to excessive administrative overhead and creates a single point of failure by making it unsuitable for large scale vehicular networks. Distributed trust management systems store trust information across multiple RSUs, but RSU failures, intrusions, and frequent vehicle mobility across regions make it difficult to maintain synchronized and reliable trust values. These limitations highlight the need for a decentralized, tamper proof, and consistent trust management mechanism that can operate efficiently in dynamic IoV environments.

Blockchain technology provides a natural solution to these challenges due to its decentralized, transparent, tamper-resistant, and auditable data structure. In a blockchain-enabled IoV system, all vehicle messages and behaviors are recorded in an immutable distributed ledger that can be verified by all participating nodes, eliminating the need for a trusted central authority and preventing single-point failures. However, traditional public blockchains suffer from high latency, limited storage capacity, and heavy resource consumption, making them unsuitable for real-time and resource-constrained vehicular environments. Consequently, consortium blockchains, in which only pre-selected RSUs and authorities participate in consensus, are more suitable for IoV applications. Nevertheless, the efficiency and security of consortium blockchains strongly depend on the underlying consensus mechanism. Although PBFT provides strong Byzantine fault tolerance and its high communication overhead limits scalability, and although DPoS improves efficiency by selecting a small group of validators, it does not explicitly account for trustworthiness.

To address these limitations, this work introduces a Bayesian-optimized trust-driven consensus framework over a DAG-enabled consortium blockchain. First, each vehicle's trust value is calculated using Bayesian optimization based on its historical behavior, accuracy of data and consistency of interaction, allowing reliable and adaptive estimation of node credibility in dynamic IoV environments. Vehicles and RSUs with higher posterior trust values are selected as trusted

This paper was produced by the IEEE Publication Technology Group. They are in Piscataway, NJ.

Manuscript received April 19, 2021; revised August 16, 2021.

candidates. These candidates then participate in a DPoS-based election process, where voting power is determined by both stake and trust, ensuring that only highly reliable nodes can become delegates. The elected delegates execute a Delegated Byzantine Fault Tolerance (DBFT) protocol to achieve fast, secure, and Byzantine-resilient block confirmation. Furthermore, all validated transactions are stored on a Directed Acyclic Graph (DAG)-based blockchain, which enables parallel processing of transactions and significantly improves throughput and latency. Through the integration of Bayesian trust evaluation, hybrid consensus DPoS-DBFT, and DAG-based ledger architecture, the proposed framework provides a secure, scalable, and real-time solution for trusted V2V and V2RSU data sharing in IoV systems.

The major contributions of this work are summarized as follows:

- We propose a **Bayesian and graph-based trust evaluation framework** for the Internet of Vehicles (IoV), where the credibility of each vehicle is computed using BayesTrust from vehicular message correctness and refined through a VehicleRank mechanism over an implicit web of trust, enabling robust and uncertainty-aware identification of reliable vehicles.
- We develop a **Trust-DBFT consensus protocol** that integrates global Bayesian trust into a delegated Byzantine Fault Tolerant (DBFT) architecture, in which only the most trustworthy vehicles are selected as committee members and leaders, and consensus decisions are made through trust-weighted voting to suppress malicious and low-credibility nodes.
- We design a **hierarchical and trust-protected IoV blockchain architecture** in which geographically distributed clusters perform local Trust-DBFT consensus and exchange validated blocks through a global sharing layer secured by cluster-level trust, ensuring scalability, low latency, and strong Byzantine resilience for real-time vehicular information sharing.

The remainder of this paper is organized as follows. Section II surveys existing related work to highlight the research gap and motivate our proposed approach. Section III describes the proposed model in detail, including its system architecture, mathematical formulation, and design principles. Section V presents the implementation setup along with performance evaluation, analysis, and discussion of the results obtained for the proposed model. Finally, Section VI concludes the paper and discusses possible directions for future work.

II. Literature Review

Du et al. [4] combines Bayesian inference based trust management with an EPoW consensus algorithm to facilitate high-throughput information sharing and sub-second block generation while introducing centralized CA dependencies and potential centralization risks during miner set optimization.

Tong et al. [5] propose TI-BIoV, a three-chain blockchain architecture that integrates a nonsubjective trust mechanism based on traffic-information offset and a trust-based consensus protocol to resist bad-mouthing and collusion attacks, while a Q-learning-driven incentive strategy optimizes rewards under partially unknown parameters to promote accurate data sharing and sustain long-term system operation—though this introduces additional modeling and design complexity.

Jiang et al. [6] propose a distributed IoV data-privacy scheme that integrates Schnorr-based zero-knowledge authentication, IPFS edge storage, and consortium blockchain indexing to enhance privacy, scalability, and authentication efficiency, while proxy re-encryption strengthens key control — though this added security lowers data-sharing efficiency and increases system complexity.

Fan et al. [7] propose COBATS, a consortium-blockchain trust and data sharing framework that combines malicious filter trust evaluation with a hybrid PoS–PBFT consensus to improve security, data quality and detection of malicious vehicles, while still facing open challenges such as offline data sharing and cold-start trust initialization.

Wang et al. [8] propose TEBChain, a blockchain-based trusted data-sharing scheme for UAV-assisted IoV disaster rescue that combines a lightweight framework, a BLS threshold-based key update mechanism and the consensus LS-PBFT to ensure data authenticity, reduce communication overhead and improve rescue efficiency, while introducing additional cryptographic complexity and reliance on committee coordination.

Wang et al. [9] propose a hybrid PoS-based blockchain framework for IoV, where block producers are selected by stake and mutually supervising trusted managers periodically update head blocks, enabling secure distributed data sharing with low computation cost while increasing system coordination requirements and design complexity.

Han et al. [10] propose an IoV Data Management System (IDMS) that integrates blockchain, DAO incentives, and parallel intelligence to overcome data silos, privacy risks, poor data quality, and weak collaboration in IoV networks, enhancing security, trust, and efficiency in vehicular data sharing while introducing additional coordination and system-design complexity through decentralized governance and parallel management mechanisms.

Zhou et al. [11] propose a blockchain-based conditional privacy-preserving authentication scheme that employs hierarchical key generation and a hierarchical–zonal blockchain to support efficient cross-domain IoV data sharing and traceability, enhancing privacy, security, and communication efficiency while introducing added coordination requirements across domains and management nodes.

Zhang et al. [12] introduce a dynamic vehicle reputation consensus algorithm (DVRC) that evaluates vehicle behavior and consensus contributions to improve V2X security and communication efficiency, utilizing high-reputation vehicles as communication relays in infrastructure-less scenarios while requiring complex multimodal coordination and dynamic threshold management.

Chen et al. [13] integrate a CNN-based pre-reward-penalty mechanism with a trust-based consensus protocol to enhance message authenticity prediction and system robustness in IoV while increasing computational overhead for real-time neural network inference and system complexity.

Surapaneni et al. [14] proposes a blockchain-based vehicle authentication framework for IoV that leverages a Proof-of-Trust (PoT) consensus mechanism to eliminate redundant re-authentication during RSU handovers, thereby reducing computation and communication overhead while improving scalability and latency. The scheme decentralizes trust and vehicle revocation among RSUs without relying on a central authority, demonstrates resilience against identity theft, replay, and Sybil attacks through formal security analysis, and achieves efficient, low-latency authentication in dynamic vehicular scenarios, albeit with potential blockchain scalability and storage challenges as network size grows.

Chunduri et al. [15] proposes a blockchain-based trust management framework for vehicular cyber-physical systems to ensure reliable message exchange and trustworthy vehicle behavior. It introduces trust evaluation, vehicle trust updating, and a PoI-GSPBFT consensus mechanism to improve scalability, robustness, and resistance to malicious nodes. Simulation results demonstrate enhanced scalability, resilience, and efficiency compared to existing trust management approaches.

Chen et al. [16] propose a role-adaptive trust model integrated with a GenAI-enhanced PBFT consensus to improve reliability and efficiency in blockchain-based vehicle platooning, while introducing algorithmic complexity through trust computation, diffusion-driven DRL optimization, and modified consensus coordination.

Wang et al. [17] propose LT-DBFT, a hierarchical blockchain consensus mechanism that clusters geographically distributed IoT nodes and selects committee members using trust values to reduce latency and communication overhead, outperforming traditional PBFT and GeoBFT in throughput and efficiency — while still relying on centralized identity management and lacking richer node-selection metrics, which introduces security and deployment limitations.

Yadav et. al [18] presents a trust-enabled DPoS consortium blockchain for IoV, where miners are selected based on trust scores derived from entropy- and binomial-based transaction analysis to improve security, latency, and malicious vehicle detection, while still being limited by one-hop trust evaluation and opportunities to further enhance consensus precision and network efficiency.

III. PROPOSED MODEL DESCRIPTION, FORMULATION AND DESIGN

A. Trust Computation for Each Vehicle in Trust-DBFT

In the proposed Trust-DBFT blockchain for the Internet of Vehicles (IoV), the trust of each vehicle is computed through a two-layer probabilistic and graph-based framework that directly drives committee selection and Byzantine fault tolerant consensus. First, a Local Trust Value (LTV) is computed using Bayesian inference (BayesTrust), where each vehicle evaluates its neighbors based on historical message exchanges and behavioral correctness. Second, all local trust values are aggregated into a directed weighted trust graph, and a VehicleRank mechanism is applied to compute the Global Trust Value (GTV) of each vehicle. Unlike conventional reputation systems that rely only on consensus behavior, this approach captures

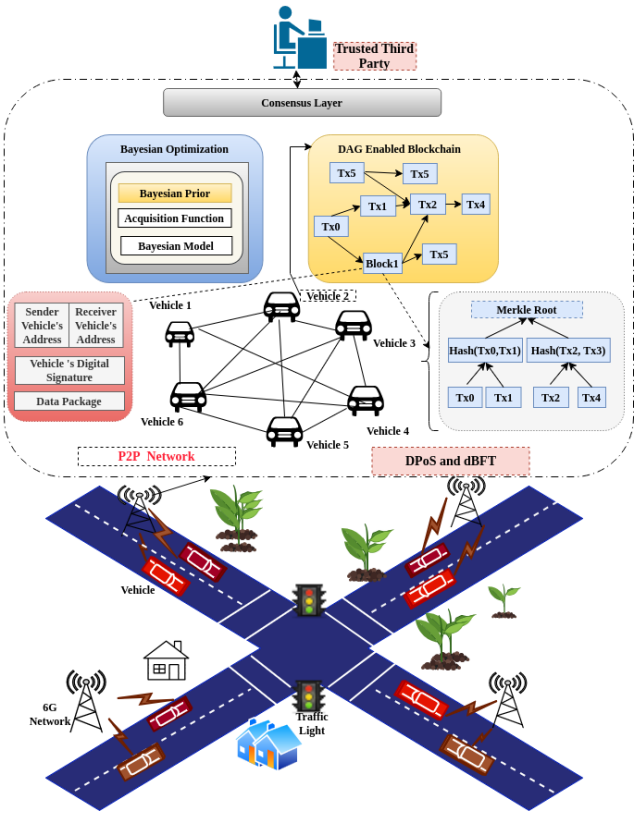

Fig. 1. Proposed architecture for information sharing

both physical-world driving behavior and network-wide trust propagation. The resulting global trust values are then used to determine committee membership, leader selection, and voting weight in the Trust-DBFT consensus protocol.

1) Local Trust Computation Using BayesTrust: For every pair of vehicles v_i and v_j, vehicle v_i evaluates the behavior of v_j during message exchanges. Let n_{ij} denote the total number of interactions between v_i and v_j, and let y_{ij} be the number of correct messages received from v_j. The trust of v_j as perceived by v_i is modeled as a random variable $\pi_{ij} \in [0, 1]$, representing the probability that v_j behaves honestly. A Beta distribution is adopted as the prior, $\pi_{ij} \sim \text{Beta}(a, b)$, where $a = b = 1$ represents an uninformed prior. Assuming a binomial observation model, the likelihood of observing y_{ij} correct messages out of n_{ij} interactions is given by

$$f(y_{ij} \mid \pi_{ij}) = \binom{n_{ij}}{y_{ij}} \pi_{ij}^{y_{ij}} (1 - \pi_{ij})^{n_{ij} - y_{ij}}. \tag{1}$$

Applying Bayes' theorem, the posterior distribution of π_{ij} becomes

$$g(\pi_{ij} \mid y_{ij}) = \text{Beta}(y_{ij} + a,\ n_{ij} - y_{ij} + b). \tag{2}$$

The Local Trust Value (LTV) of v_j as evaluated by v_i is defined as the posterior mean

$$m_{ij} = \frac{y_{ij} + a}{n_{ij} + a + b}, \tag{3}$$

and the associated uncertainty is

$$\text{Var}_{ij} = \frac{(y_{ij} + a)(n_{ij} - y_{ij} + b)}{(n_{ij} + a + b)^2 (n_{ij} + a + b + 1)}. \tag{4}$$

TABLE I
COMPARATIVE ANALYSIS OF BLOCKCHAIN-BASED IOV TRUST MANAGEMENT WORKS

Year	Key Advantage(s)	Technique(s) Used)	Limitation(s)
2023	Efficient trust-based information sharing with reduced consensus overhead	Consortium Blockchain, Bayesian Inference, EPoW, 5G NR-V2X	Semi-trusted RSUs vulnerable to compromise; public chains too slow, private chains too centralized
2023	Objective trust evaluation prevents bad-mouthing and improves incentive fairness	Three-chain architecture, Q-learning, Trust-based consensus	Increased transaction latency due to trust computation overhead
2023	Strong privacy-preserving authentication and secure data storage	Zero-Knowledge Proof (Schnorr), IPFS, Hyperledger Fabric, Proxy Re-Encryption	Reduced data-sharing efficiency; no adaptive security for low-sensitivity data
2024	Reliable data sharing in disaster scenarios with minimal infrastructure	Lightweight blockchain, BLS threshold signature, LS-PBFT, UAV-assisted IoV	Energy consumption and power constraints not considered
2024	Improved decentralization by allowing all nodes to participate in consensus	Hybrid PoS, PBFT, coordinate-based coin-tossing	High disk write consumption during consensus
2024	Eliminates data silos and enables decentralized collaboration	DAO, Parallel Intelligence, Smart Contracts, Blockchain	Privacy risks and limited accuracy in trust evaluation
2024	Conditional privacy with traceability and scalable cross-domain trust	Hierarchical/Zonal blockchain, HD wallets, cross-chain verification	Key derivation efficiency decreases with hierarchy depth
2024	Intelligent message reliability prediction with incentive-aware trust	CNN-based trust evaluation, Trust-based consensus, Reward–Penalty mechanism	Privacy leakage and potential bias in trust assessment
2024	Adaptive reputation improves communication reliability and coverage	DVRC algorithm, reputation-based consensus, V2V/V2I/V2N	Scalability and security issues in large heterogeneous networks
2025	Secure and fast RSU handover by avoiding redundant re-authentication	Proof of Trust (PoT), ECC, SUMO, Scyther	Blockchain size growth causes storage and synchronization issues
2025	Fast punishment discourages malicious behavior and reduces edge latency	Permissioned blockchain, AIMD trust model, Edge–Fog–Cloud architecture	Higher execution time with a small number of miners
2025	Improved scalability via regional trust evaluation and semi-distributed design	PoI-GSPBFT, Bayesian inference, semi-distributed architecture	Consensus latency and resource usage remain high
2025	Optimized platooning consensus using intelligent trust adaptation	DESAC (GenAI-DRL), role-adaptive trust model, modified PBFT	High computational complexity and long training time
2025	Reduced latency through location-aware hierarchical consensus	LT-DBFT, location-based clustering, trust-based committee selection	Dependence on centralized CA/MSP for identity authentication

This probabilistic formulation enables each vehicle to quantify both the expected trustworthiness and the uncertainty of its neighbors based on real vehicular interactions.

2) Global Trust Computation Using VehicleRank: After computing all LTVs, the vehicles form a directed weighted trust graph, where each vehicle is a node and each trust relationship is an edge. The normalized trust weight from vehicle v_i to vehicle v_j is defined as

$$w_{ij} = \frac{m_{ij}}{\sum_{k \in S_i} m_{ik}}, \tag{5}$$

where S_i denotes the set of vehicles evaluated by v_i. This normalization produces a stochastic trust transition matrix W that represents the implicit web of trust.

Let t_i denote the Global Trust Value (VehicleRank) of vehicle v_i. At iteration k, trust is propagated according to

$$c_{ij}^{(k)} = w_{ij} t_i^{(k)}, \tag{6}$$

and the global trust of v_j is updated as

$$t_j^{(k+1)} = \sum_{i \in P_j} c_{ij}^{(k)}, \tag{7}$$

where P_j denotes the set of predecessors of v_j. In matrix form,

$$t^{(k+1)T} = t^{(k)T} W. \tag{8}$$

To guarantee convergence and avoid rank sinks, a dangling-node correction and a welfare term are incorporated, producing the final transition matrix

$$T = \alpha S + (1 - \alpha) e \tilde{t}^T, \tag{9}$$

where S is the adjusted trust matrix, e is a vector of ones, $\tilde{t}$ is the previous trust vector, and $\alpha \in (0, 1)$ is a damping factor. The global trust vector is obtained by

$$t^{(k+1)T} = t^{(k)T} T, \tag{10}$$

which converges to $t = \lim_{k \to \infty} t^{(k)}$.

Algorithm 1 BayesTrust–VehicleRank Based Global Trust Computation

Require: Vehicle set $\mathcal{V} = \{v_1, v_2, \ldots, v_N\}$, interaction history $\{n_{ij}, y_{ij}\}$
Ensure: Global trust vector $t = \{t_1, t_2, \ldots, t_N\}$

Bayesian Local Trust
for each (v_i, v_j) **do**
  Compute m_{ij} using Eqs. (1)–(3)
end for
Trust Graph Construction
for each v_i **do**
  Compute w_{ij} using Eq. (5)
end for
Form trust matrix W
VehicleRank Update
Initialize $t^{(0)} = \frac{1}{N}$
repeat
  Update trust using Eqs. (6)–(10)
until convergence
return t

IV. T-DBFT Consensus Protocol for the IoV Information Sharing Scheme

A. Committee Selection in Trust-DBFT

In the Trust-DBFT consensus protocol, committee formation and leader selection are driven by the global Bayesian trust values obtained from the BayesTrust–VehicleRank framework. Let $t_i \in [0,1]$ denote the global trust of vehicle v_i. For a cluster $\mathcal{C} = \{v_1, v_2, \ldots, v_N\}$, vehicles are ranked according to their trust values, and only the top c vehicles are selected to form the consensus committee:

$$\mathcal{K} = \{v_i \mid t_i \text{ is among the top } c \text{ values}\}, \tag{11}$$

where $c = 3f + 1$ ensures Byzantine fault tolerance. This guarantees that at most f malicious vehicles can exist in the committee.

The primary (leader) node of the cluster is chosen as the most trusted vehicle within the committee,

$$p = \arg\max_{v_i \in \mathcal{K}} t_i. \tag{12}$$

Because the trust values t_i are derived from Bayesian inference on vehicular message correctness and refined through VehicleRank over the implicit web of trust, the committee and leader selection reflect the physical-world reliability and long-term behavior of vehicles rather than only their short-term voting behavior.

B. Trust-Weighted DBFT Voting

During the consensus process, committee nodes vote on proposed blocks. Let $s_i \in \{0,1\}$ denote the vote of committee node v_i. Instead of treating all votes equally, Trust-DBFT weights each vote by the global trust of the corresponding node. A block is accepted when the following trust-weighted voting condition is satisfied:

$$\sum_{v_i \in \mathcal{K}} t_i s_i \geq \frac{2}{3} \sum_{v_i \in \mathcal{K}} t_i. \tag{13}$$

This rule ensures that consensus is dominated by vehicles that collectively hold at least two-thirds of the total trust in the committee. As a result, even if several low-trust malicious vehicles collude, they cannot override the decision of a small number of highly trusted honest vehicles. Therefore, Byzantine influence is bounded by accumulated trust rather than node count, which significantly strengthens resilience against coordinated attacks in dynamic IoV environments.

C. Global Sharing with Trust Protection

Following local Trust-DBFT consensus within each cluster, the primary nodes participate in the global sharing layer to exchange locally agreed blocks. Each cluster k is associated with a global trust value T_k, computed as the aggregate of VehicleRank values of its committee members. During global sharing, the probability that a malicious block is accepted across clusters is upper-bounded by the total trust held by malicious clusters:

$$P(\text{false block accepted}) \leq \sum_{k \in \mathcal{M}} T_k, \tag{1}$$

where $\mathcal{M}$ denotes the set of compromised clusters. Since trust is accumulated through long-term correct behavior and Bayesian verification of vehicular data, honest clusters naturally dominate the global trust distribution. Consequently, false or manipulated blocks cannot propagate unless attackers control a majority of system trust, making cross-cluster attacks statistically improbable.

D. Trust Update Loop

After each consensus round, the trust of each vehicle is updated by jointly considering its historical consensus behavior and its global Bayesian trust derived from vehicular interactions. The trust update rule is defined as

$$TS_i^{new} = \lambda TS_i^{old} + (1-\lambda) t_i, \tag{14}$$

where TS_i^{old} is the previous consensus-based trust score, t_i is the VehicleRank value of vehicle v_i, and $\lambda \in [0,1]$ controls the balance between historical behavior and newly observed physical-world reliability.

This fusion ensures that a vehicle must be honest both in IoV data generation and in blockchain consensus participation to maintain a high trust score. Vehicles that transmit false information or behave maliciously during consensus experience a rapid decay in their trust, leading to automatic exclusion from committee and leader roles. As a result, Trust-DBFT remains robust, adaptive, and secure in highly dynamic and adversarial IoV environments.

Algorithm 2 Trust-DBFT Consensus Protocol

Require: Cluster $\mathcal{C}$, global trust values $\{t_i\}$, trust scores $\{TS_i\}$
Ensure: Finalized block and updated trust scores
Step 1: Committee Selection
Select committee $\mathcal{K}$ using Eq. (11)
Select primary node p using Eq. (12)
Step 2: Proposal
Primary p proposes a candidate block to all $v_i \in \mathcal{K}$
Step 3: Trust-Weighted Voting
for each committee node $v_i \in \mathcal{K}$ **do**
  Verify proposal and cast vote $s_i \in \{0,1\}$
end for
if trust-weighted condition in Eq. (13) holds **then**
  Block is accepted locally
else
  Reject block and trigger leader or committee update
end if
Step 4: Global Sharing
Exchange locally accepted blocks among cluster primaries
Accept global block if trust condition in Eq. (13) holds across clusters
Step 5: Trust Update
for each vehicle v_i **do**
  Update trust score using Eq. (14)
end for
return Final block and updated trust scores

V. Assessment and Analysis of the Performance of Proposed Model

- Malicious Nodes - Trust

VI. Conclusion

References

[1] S. B. Hakim, M. Adil, A. Ali, A. Farouk, and H. H. Song, "Internet of vehicles security threats, countermeasures, open challenges with future research directions," *IEEE Internet of Things Journal*, 2025.

[2] G. Yan, K. Liu, C. Liu, and J. Zhang, "Edge intelligence for internet of vehicles: A survey," *IEEE Transactions on Consumer Electronics*, vol. 70, no. 2, pp. 4858–4877, 2024.

[3] B. Liang, F. Wang, and B. Ran, "Optimizing roadside unit deployment in vanets: A study on consideration of failure," *IEEE Transactions on Intelligent Transportation Systems*, vol. 25, no. 9, pp. 10 835–10 850, 2024.

[4] G. Du, Y. Cao, J. Li, Y. Zhuang, X. Chen, Y. Li, and J. Chen, "A blockchain-based trust-value management approach for secure information sharing in internet of vehicles," *IEEE Internet of Things Journal*, vol. 11, no. 1, pp. 333–344, 2023.

[5] W. Tong, X. Dong, Y. Zhang, Z. Zhang, L. Yang, W. Yang, and Y. Shen, "Ti-biov: Traffic information interaction for blockchain-based iov with trust and incentive," *IEEE Internet of Things Journal*, vol. 10, no. 24, pp. 21 528–21 543, 2023.

[6] W. Jiang and X. Lv, "A distributed internet of vehicles data privacy protection method based on zero-knowledge proof and blockchain," *IEEE Transactions on Vehicular Technology*, vol. 73, no. 5, pp. 6332–6345, 2023.

[7] Q. Fan, Y. Xin, B. Jia, Y. Zhang, and P. Wang, "Cobats: A novel consortium blockchain-based trust model for data sharing in vehicular networks," *IEEE Transactions on Intelligent Transportation Systems*, vol. 24, no. 11, pp. 12 255–12 271, 2023.

[8] H. Wang, C. Wang, K. Zhou, D. Liu, X. Zhang, and H. Cheng, "Tebchain: A trusted and efficient blockchain-based data sharing scheme in uav-assisted iov for disaster rescue," *IEEE Transactions on Network and Service Management*, vol. 21, no. 4, pp. 4119–4130, 2024.

[9] N. Wang, Z. Zhou, J. Liu, L. Deng, and J. Fu, "Secure and distributed iov data sharing scheme based on a hybrid pos blockchain protocol," *IEEE Transactions on Vehicular Technology*, vol. 73, no. 8, pp. 11 995–12 009, 2024.

[10] S. Han, Y. Bai, T. Zhang, Y. Chen, and C. Tellambura, "Parallel management of iov information enabled by blockchain and decentralized autonomous organizations," *IEEE Transactions on Intelligent Vehicles*, vol. 9, no. 4, pp. 4759–4768, 2024.

[11] Z. Zhou, N. Wang, J. Liu, W. Zhou, J. Fu, and L. Deng, "Conditional privacy-preserving and efficient distributed iov data sharing scheme based on a hierarchical and zonal blockchain," *Vehicular Communications*, vol. 49, p. 100832, 2024.

[12] L. Zhang, L. Hang, K. Zu, Y. Wang, and K. Yang, "Dynamic vehicle reputation consensus: Enhancing iov communication with a blockchain algorithm," *IEEE Transactions on Vehicular Technology*, vol. 74, no. 3, p. 4788, Mar. 2025.

[13] C. Chen, L. Wang, and Q. Shi, "Blockchain enabled trust management in internet of vehicles: A joint pre-reward-penalty and consensus approach," *IEEE Internet of Things Journal*, 2024.

[14] P. Surapaneni, S. Bojjagani, and M. K. Khan, "Dynamic-trust: Blockchain-enhanced trust for secure vehicle transitions in intelligent transport systems," *IEEE Transactions on Intelligent Transportation Systems*, 2025.

[15] V. Chunduri, M. Alsaadi, S. Gupta, T. A. Ahanger, A. Gopi, F. Y. Alghayadh, N. Shavkatov, and G. K. Mahato, "Blockchain-based secure trust management scheme for internet of vehicles over cyber-physical system," *IEEE Transactions on Intelligent Transportation Systems*, 2024.

[16] H. Chen, X. Fu, Q. Yuan, Z. Zhuang, J. Kang, Z. Liu, J. Wang, and D. Niyato, "Trust model-based consensus optimization for vehicle platooning networks: A novel deep reinforcement learning approach with genai," *IEEE Transactions on Intelligent Transportation Systems*, 2025.

[17] Y. Wang, X. Xing, P. Li, and G. Wang, "Lt-dbft: A hierarchical blockchain consensus using location and trust in iot," *IEEE Internet of Things Journal*, 2025.

[18] S. Yadav, K. Singh, A. K. Yadav, S. A. Chaudhry, A. K. Das, M. Shariq, and M. Manjul, "Efficient and reliable information sharing for internet of vehicles using trust and blockchain," *IEEE Transactions on Vehicular Technology*, vol. 74, no. 11, Nov. 2025.