A Lightweight Blockchain-Enabled Trust Management Model for Secure Vehicular Communication

Muhammad Rizwan Rashid Rana[1], Touqeer Ahmad[2], Muhammad Hasaan Mujtaba[1], Muhammad Tariq[3]

[1]Department of Robotics and Artificial Intelligence, Shaheed Zulfikar Ali Bhutto Institute of Science and Technology, Islamabad, Pakistan

[2]University Institute of Information Technology, Pir Mehr Ali Shah Arid Agriculture University, Rawalpindi, Pakistan

[3]School of Computer Science and Technology, Taiyuan University of Science and Technology, Taiyuan, Shanxi, China

*__Correspondence__: Touqeer Ahmad and tauqeer.ahmed443@gmail.com

Citation | Rana. M. R. R, Ahmad. T, Mujtaba. M. H, Tariq. M, "A Lightweight Blockchain-Enabled Trust Management Model for Secure Vehicular Communication", IJIST, Vol. 07, Issue. 03 pp 1597-1611, July 2025

Received | June 10, 2025 **Revised |** July 25, 2025 **Accepted |** July 26, 2025 **Published |** July 27, 2025.

Vehicular Ad Hoc Networks (VANETs) are emerging as a pivotal component in intelligent transportation systems, offering safety-critical and comfort-related information to drivers and passengers. The effectiveness of VANETs relies on the timely exchange of messages between vehicles and roadside units (RSUs), where the trustworthiness of shared data is paramount. Traditional centralized trust models, though efficient in information validation, suffer from single points of failure, limited scalability, and vulnerability to insider threats. This has driven a paradigm shift toward decentralized architectures, with blockchain technology standing out due to its immutable, transparent, and distributed nature. This study presents a comprehensive review of existing centralized and decentralized trust management models in VANETs, analyzing their methodologies, strengths, and limitations. By examining trust metrics, validation schemes, and message verification strategies across the literature, it identifies critical gaps in scalability, response time, and resistance to malicious behavior. Addressing these limitations, we propose a novel blockchain-based trust model named CB-RTM (Consortium Blockchain for RSU-Assisted Trust Management), an intelligent framework designed to ensure secure, verifiable, and real-time dissemination of safety messages in VANETs. The CB-RTM model integrates consortium blockchain with RSU-based validation and a Proof-of-Authority (PoA) consensus mechanism to filter and authenticate event messages using location certificates and trust scores. Unlike existing approaches, the model localizes trust updates and block propagation to geographically bounded regions, enhancing scalability and latency performance. Experimental evaluation demonstrates that the proposed CB-RTM outperforms state-of-the-art models across key metrics. The model achieves a trust accuracy of 96.2%, a latency of 0.42 seconds, and a throughput of 245 messages per second, while maintaining a manageable communication overhead of 11.2%. These results confirm that CB-RTM is a robust, scalable, and efficient solution for trust management in real-time VANET environments

Keywords: Trust Management, Blockchain, Consortium Network, Proof-of-Authority

Introduction:

Intelligent Transportation Systems (ITSs) have gained substantial traction in both industry and academia due to their potential to enhance road safety, traffic efficiency, and driving comfort [1]. Among the core components of ITSs, Vehicular Ad Hoc Networks (VANETs) have emerged as a critical research area, facilitating real-time communication among vehicles (V2V) and between vehicles and infrastructure (V2I) [2]. These communications support a wide range of applications such as accident warnings, congestion alerts, lane-change assistance, and emergency services. In VANETs, vehicles continuously disseminate safety-critical and status messages, such as sudden braking, lane change intentions, or traffic congestion alerts, that neighboring nodes must evaluate in real time to make informed driving decisions [3]. However, the open, decentralized, and highly mobile nature of VANET environments introduces considerable complexity in verifying the authenticity and trustworthiness of such messages. The dynamic topology, absence of permanent infrastructure, and anonymity of participating nodes make the network highly vulnerable to a broad spectrum of security threats.

These include false data injection, where malicious vehicles intentionally broadcast deceptive event information; Sybil attacks, in which a single attacker generates multiple fake identities to manipulate network behavior; identity spoofing, used to impersonate legitimate vehicles; and denial-of-service (DoS) attacks that overwhelm communication channels to disrupt message dissemination. As such, trust management has become an indispensable component in VANET security architectures, offering a systematic approach to classify vehicles based on behavioral evidence and limit the influence of untrustworthy entities [4]. Over the past decade, numerous trust models have been proposed to tackle the problem of message verification and node reliability in VANETs [5]. Centralized trust mechanisms, typically managed by a central authority or trust server, offer high-level monitoring and global policy enforcement. While effective in smaller deployments, these models suffer from scalability bottlenecks, single points of failure, and latency issues, making them unsuitable for real-time, large-scale VANET environments.

On the other hand, decentralized and distributed reputation-based models rely on peer-to-peer observation and collective consensus to evaluate trust levels. These methods enhance resilience and availability but often face challenges in ensuring trust consistency, attack resistance, and traceability. Moreover, many existing solutions depend on auxiliary hardware components such as tamper-proof devices or specialized sensors, limiting their deploy ability in heterogeneous vehicle ecosystems [6]. Furthermore, delayed trust convergence and the propagation of unverifiable messages in high-density traffic conditions further deteriorate the performance and reliability of these systems. Therefore, a scalable, efficient, and verifiable trust management framework is urgently required to support secure and real-time communication in VANETs [7][8].

Objectives:

The primary objectives of this study are as follows:

- To develop a novel RSU-assisted trust management framework using permissioned blockchain with Proof-of-Authority consensus, enabling secure and verifiable event message dissemination without external reputation servers or additional hardware.
- To design a localized trust evaluation mechanism that validates event messages based on spatial relevance (PoL), timestamp, event ID, and historical trust scores stored on the blockchain.
- To implement and evaluate the CB-RTM model in a simulated VANET environment, assessing its performance in terms of trust accuracy, message latency, throughput, and communication overhead.

Novelty Statement:

This study introduces a novel Consortium Blockchain-based RSU-Assisted Trust Management (CB-RTM) framework designed specifically for Vehicular Ad-hoc Networks (VANETs). Unlike existing trust management systems that rely on centralized reputation servers or require additional onboard hardware, the proposed CB-RTM framework utilizes a permissioned blockchain with Proof-of-Authority (POA) consensus, ensuring decentralized, secure, and verifiable event message dissemination. The incorporation of localized consensus zones and RSU-assisted validation significantly reduces communication overhead, enhances scalability, and improves real-time applicability. Furthermore, the localized trust evaluation mechanism, based on the sender's historical behavior, event ID, timestamp, and spatial relevance, sets this framework apart by enabling rapid detection and prevention of malicious or irrelevant data propagation within VANETs.

Literature Review:

Vehicular Ad Hoc Networks (VANETs) are critical enablers of intelligent transportation systems, supporting real-time communication between vehicles and infrastructure to improve road safety and traffic management. However, due to the dynamic topology, open environment, and lack of centralized control, VANETs are vulnerable to security threats such as false message dissemination and Sybil attacks. As a result, trust management has emerged as a key research focus. This section reviews existing trust management mechanisms in VANETs by organizing them into major thematic categories, highlighting their methodologies, strengths, and limitations.

Blockchain-Based Trust Models:

Blockchain has emerged as a promising solution in VANETs due to its decentralized, tamper-proof, and transparent nature. Author in [9] proposed a decentralized storage process in which blockchain is used to reduce malicious behavior in vehicular networks. The authors stored critical file metadata, file summaries, and file integrity tokens (the file itself was stored off-chip) on the blockchain, allowing secure and reliable file access. The authors in [10] also proposed a blockchain-based distributed storage and keyword search system where they stored the public keys of honest nodes and achieved authenticated (as in, consensus from the blockchain) open-access storage to increase trust through decentralization and immutability. In another study author[11] built on the CLAS scheme by implementing a dual-signature scheme with both the aggregator and the aggregate signature, allowing them to verify simultaneously. This dual signature allowed substantial reductions in computational overhead and communication latency and significantly reduced rogue key attacks.

Reputation and Probabilistic Trust Systems:

Reputation-based systems often rely on historical behavior to evaluate trustworthiness in VANETs. Authors in [12] developed a trust model based on Markov chains to encapsulate the variability of trust metrics as a function of vehicle behavior. Their model can characterize trust variations and account for monitoring constraints, and analyze performance under malicious and selfish node scenarios. In a study [13], author presented a hybrid trust management scheme to effectively discover and dissociate malicious vehicles to ensure that malicious vehicles do not configure trust-related distrust roles, such as cluster heads, to ensure more reliable communication and network security.

Clustering and Federated Learning-Based Models:

Clustering strategies are commonly utilized to provide scalability and efficiency in large-scale VANETs. A recent paper [14] contributed a clustering metric that has relative speed and parameter similarity aspects to facilitate solutions in handling data heterogeneity and mobility in non-IID environments. The authors demonstrated smooth transitions of leadership by transferring updated model parameters of Federated Learning (FL) models to the new cluster heads, providing trust and consistency in rapidly changing environments.

Credential and Authentication Frameworks:

Authentication is essential to maintaining integrity and preventing identity-based attacks in VANETs. In this respect, a decentralized threshold-based credential management system was proposed in [15], which provides fine-grained authentication without a single-point failure. The architecture contains multiple credential authorities comprising multiple credential managers that collectively issue credentials using the threshold approach. This improves fault tolerance and enables secure vehicle authentication in decentralized environments.

Despite significant advances in trust management for VANETs, current models still experience limitations that inhibit their performance in real-world deployment. Centralized approaches usually suffer from latency, low scalability, and single points of failure that are not suitable for time-sensitive vehicular communication. Alternatively, many decentralized models rely on imperfect, incomplete local observations, which can lead to biased trust assessments and trust convergence delays. Some of the existing solutions require additional hardware or rely on complex Cryptographic implementations, which lead to increased system overhead and lower real-world feasibility. Additionally, current models rarely include a secure, verifiable timeline of event messages, with sufficient tamper-resistance as well. These issues show the need for a better solution. The proposed CB-RTM model addresses these deficiencies through a decentralized, transparent, and efficient trust management system using blockchain, which will increase event verification accuracy, reduce computational cost, remove central dependency, and enable trustful interaction in high-mobility VANET applications.

Material and Methods:

This section presents a novel trust management framework for Vehicular Ad Hoc Networks (VANETs) that leverages a consortium blockchain architecture, integrated with Road-Side Units (RSUs) as the primary trust evaluators and validators. Traditional blockchain-based solutions, particularly those relying on Proof-of-Work (PoW), face significant challenges in VANET environments due to their high computational demands, latency, and scalability limitations. To overcome these barriers, the proposed model adopts a Proof-of-Authority consensus mechanism within a permissioned blockchain operated by a consortium of trusted entities such as RSUs, transportation authorities, and insurance stakeholders. This design ensures that event messages, such as traffic hazards or accident alerts, are validated, recorded, and propagated in a secure, efficient, and tamper-proof manner. By combining RSU-assisted verification, localized message dissemination, and dynamic trust score updates, the model ensures real-time reliability of safety messages while maintaining a decentralized yet controlled environment for trust propagation. The overall goal is to provide a lightweight, scalable, and trustworthy message verification infrastructure suitable for high-mobility vehicular environments. The complete architecture is shown in Figure 1.

Architecture:

The proposed Consortium Blockchain with RSU-Assisted Trust Management (CB-RTM) is architected to provide a decentralized, efficient, and secure framework for real-time vehicular trust evaluation and message verification in VANETs. The system is composed of three core components: vehicles, roadside units (RSUs), and a permissioned consortium blockchain. The interactions among these components are supported through secure communication interfaces, enabling distributed data validation and consensus. Figure 2 illustrates the complete message lifecycle within the CB-RTM model.

Vehicles:

Each vehicle v_i · In the VANET functions as a dynamic mobile node responsible for detecting traffic-related events and broadcasting event messages M_i. These messages encapsulate important metadata such as a pseudo-identity $PIDi$, event type ETi, event ID EID_i, timestamp t_i, location coordinates $Li = (lati, loni)$, speed si, direction θ, a Proof-

of-Location (PoL) certificate PoLi, and a temporary trust score $T_{L_i}^{Temp}$. The general structure of a vehicular event message can be represented as:

$$Mi = \{PIDiEIDiETi, ti, Li, si, \theta i, PoLi, TLi^{temp}\} \quad (1)$$

To ensure privacy, vehicles regularly update their pseudo-IDs and rely on RSU-issued certificates to validate their geographic position and communication legitimacy.

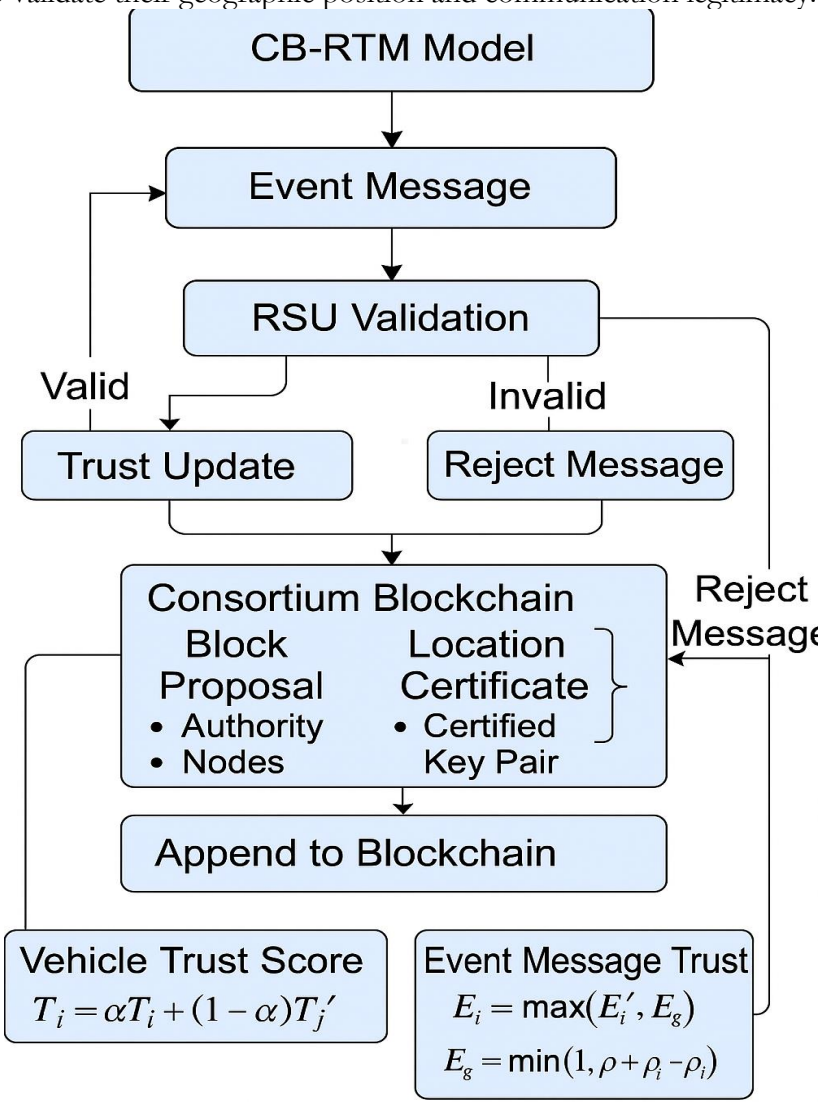

Figure 1. The Proposed CB-RTM Architecture

Road-Side Units (RSUs):

Road-Side Units Rj are fixed-position infrastructure nodes that perform two essential roles: trust evaluation and blockchain validation. Upon receiving an event message, Mi, an RSU executes multiple verification steps:

Digital Signature Verification:

$$Verify(M_i, Sig_i) = True \quad (2)$$

Proof-of-Location Validation:

$$Validate(P_0L_i) = R_j\big(Sign_{RSU}(Li, ti)\big) \quad (3)$$

Timestamp and Spatial Consistency Checks:

$$|t_i - t_{RSU}| \le \delta_t \|L_i - L_{RSU}\| \le \delta_l \quad (4)$$

If all verifications pass, the RSU proceeds to compute an updated Trust Score TLi for the vehicle. The score is based on three factors: historical validity ratio Vr, current consistency score Ci, and recent behavior Ri.

The combined trust score is calculated using a weighted sum:

$$TL_i = \alpha . V_r + \beta \cdot C_i + \gamma \cdot R_i \quad (5)$$

$$\alpha + \beta + \gamma = 1 \quad (6)$$

Where:

$v_r = \frac{h_i}{h_i + f_i}$, with hi as the count of verified (honest) messages and fi as false or discarded messages.

$Ci \in [0,1]$ quantifies the agreement of Mi with nearby vehicle reports or environmental context.

$Ri \in [0,1] R\_i \backslash in [0,1] Ri \in [0,1]$ represents the trust consistency over the most recent k interactions.

Consortium Blockchain:

The system employs a permissioned blockchain maintained by a consortium of pre-authorized validators, including RSUs and government or third-party entities (e.g., transport departments, insurance firms) [16]. Each verified message and updated trust score are immutably logged in a block.

A block Bk is structured as follows:

$$B_k = \left\{ H(B_{k-1}) t_k RSU_j, \{M_{i1}, M_{i2} + M_{in}\} \{\overline{TL}_{Li1, TLi2....}\} \right\} \quad (7)$$

Here, $H(B_{k-1})$ denotes the hash of the previous block, ensuring the immutability and integrity of the blockchain. The term t represents the timestamp of the current block's creation, indicating when the data was recorded. RSU_J Identifies the RSU responsible for proposing the current block. The set $\{M_{i1,} M_{i2,.....,M_{in,}}\}$ includes the verified trust messages collected during the epoch, while TLi_1, TLi_2, TLi_3 ... comprises the aggregated trust levels computed for the involved vehicles or entities. The hash of a new block B_k Is computed as:

$$H(B_k) = H\left(H\left(B_{k_{-1}}\right) \| H(M_i) \quad |t_i \| RRSU_j\right) \quad (8)$$

The blockchain consensus is achieved through Proof-of-Authority (PoA) [17]. Each authorized RSU in the consortium votes on block proposals. A block is accepted if it receives approval from at least a supermajority of validators:

$$\sum_{j=1}^{n} I_{aapprove}\left(R_j, B_k\right) \geq \left[\frac{2m}{3}\right] \quad (9)$$

This consensus mechanism ensures efficient and secure agreement while significantly reducing latency and computational overhead compared to traditional Proof-of-Work (PoW) systems. Moreover, it enhances resilience against Sybil attacks and fraudulent data injections.

Communication Interfaces:

The architecture supports three forms of communication to maintain real-time data flow and consensus synchronization:

Vehicle-to-Vehicle (V2V) communication is used for immediate local alerting. Each vehicle Vi shares Mi with nearby vehicles Vj∈Rv, where Rv is the transmission range.

Vehicle-to-Infrastructure (V2I) communication allows vehicles to send event messages to nearby RSUs for validation and trust updates. The total time for V2I communication is approximated by:

$$T_{v2i} = T_{comm} + T\,verify \quad (10)$$

Where Tcomm is transmission latency and Tverify is RSU-side processing time.

RSU-to-RSU / RSU-to-Consortium communication ensures ledger synchronization and distributed consensus across the blockchain. RSUs exchange trust updates and block data, and synchronization is confirmed when:

$$\Delta TL_i^R \vec{a}^R = TL_i^{(a)} - TL_i^{(b)} \rightarrow 0 \quad (11)$$

Message Flow and Trust Evaluation:

The message flow in the proposed CB-RTM framework follows a multi-phase pipeline, beginning with message generation at the vehicle level and ending with trust evaluation and ledger update by the RSUs through consortium blockchain consensus. The goal is to ensure that each safety event message is verified for authenticity, reliability, and geographic relevance before being accepted into the blockchain. Simultaneously, the sender vehicle's trust level is recalculated to reflect its behavioral history.

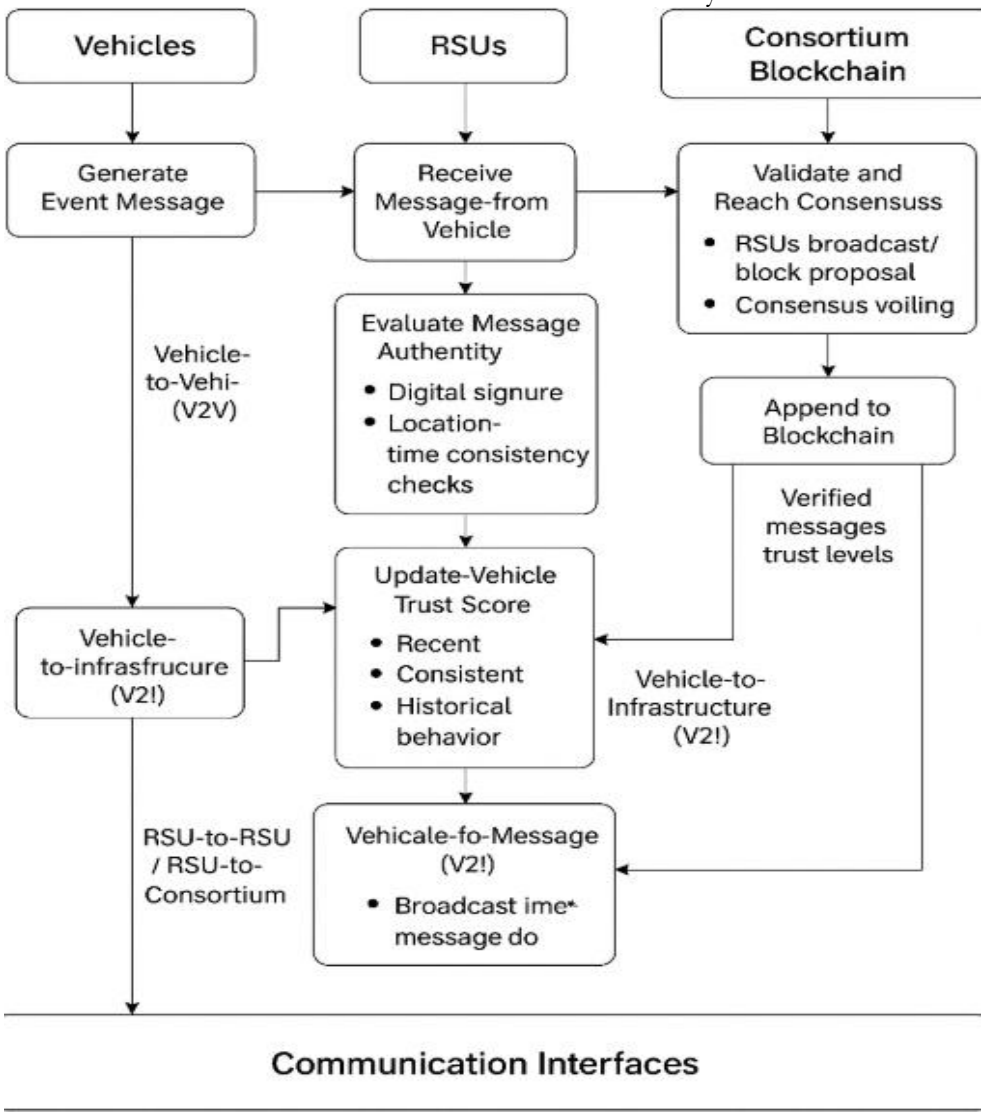

Figure 2. End-to-End Message Flow and Trust Evaluation Process in the Proposed CB-RTM Framework

Event Message Generation and Broadcast:

Each vehicle V_i monitors its environment using onboard sensors (e.g., cameras, LIDAR, GPS) and generates an event message M_i When it detects an incident such as an accident, obstacle, or traffic congestion. The message includes:

$$M_i = \{\mathrm{PID}_i, \mathrm{EID}_i, \mathrm{ET}_i, t_i, L_i, s_i, \Theta_i, \mathrm{PoL}_i, TL_l^{temp}, \mathrm{Sig}_i\} \quad (12)$$

The message is digitally signed with the sender's private key and broadcast to both nearby vehicles (V2V) and the nearest RSU (V21).

Message Validation at RSU:

Upon receiving the message, the RSU R_g Begins a multi-stage verification process to evaluate the trustworthiness of both the message and its sender. This involves:

Signature Validation:

$$\text{Verify } (M_i \text{ , Si}g_i \text{ }) = \text{True} \quad (13)$$

Location and Time Authenticity (via PoL):

$$\text{Validate } (\text{PO}L_i) = R_g \ (Sign_{RSU} \ (L_i \ , T_i \ )) \text{ and } |t_i - t_{RSU} \ | \quad (14)$$

Message Relevance:

The RSU checks if the event M_i Lies within its service region:

$$||L_i - L_{RSU} \ || \leq \delta_l \quad (15)$$

Duplication or Replay Detection:

The RSU maintains a local hash index H_{cache} Of recent messages and verifies that:

$$\text{H } (M_i) \notin \text{H}_{cache} \quad (16)$$

Only if all checks are passed does the RSU mark the message as valid and push it into the local event pool? P_{valid} For block inclusion.

Dynamic Trust Score Update:

The trust level of a vehicle is continuously updated based on its messaging behavior. Let h denote the count of valid messages and f denote false or misleading messages. Then the Trust Level is defined as:

$$TL_i = \frac{h_i}{h_i + f_i} \qquad \text{where TL } [0,1] \quad (17)$$

Each time a new event message is verified, the RSU updates hi or fi using:

If M_i Is valid: H_i (H_i + 1); Else: $f_i = f_i$+1

And recalculates the new trust score:

$$TL_i^{new} = \frac{h_i}{h_i + f_i} \quad (18)$$

To integrate recent behavior more sensitively, a weighted moving average can be applied:

$$TL_i^{updated} = \lambda TL_i^{prev} + (1 - \lambda).TL_i^{new} with \ \lambda \ E|0,1| \quad (19)$$

This allows the system to prioritize recent performance without ignoring historical behavior.

Block Creation and Consensus:

Once the RSU has accumulated a set of verified messages $\{M_i\} \in P_{valid}$ It initiates the creation of a new block B containing:

Previous block hash H (B_{k-1})

Current timestamp T_k

Set of validated messages $\{M_i1, M_i2 \ldots M_i\text{n}\}$

Updated trust scores $\{\text{T}L_{i1}, \text{T}L_{i2} \}$

The block hash is generated using:

$$\text{H } (B_k) = \text{H (H } (B_{k-1})) \ || \ \text{H } (M_i) \ || \ T_k \ || \ R_j \quad (20)$$

The block is then broadcast to other consortium RSUs for Proof-of-Authority (POA) consensus. The block is added to the ledger if approved by more than two-thirds of the authorized validators:

$$\sum_{j=1}^{m} I_{approve}(R_j, B_k) \geq \left[\frac{2m}{3}\right] \quad (21)$$

Public Verification and Distribution:

Once a block is finalized and committed, it is distributed across the network. All vehicles can access the chain to verify:

The authenticity of event messages in their vicinity

The trust level of sender vehicles, TL

Historical events relevant to traffic, insurance, or law enforcement

This public verifiability ensures that the blockchain acts as a tamper-proof trust anchor across the VANET ecosystem.

Blockchain Implementation for Secure Message Dissemination:

To ensure trust, immutability, and traceability of vehicular event messages in real time, the proposed CB-RTM framework integrates a permissioned blockchain designed specifically for the VANET environment. This blockchain is governed by a consortium of RSUs and trusted entities, and it employs a Proof-of-Authority (PoA) consensus mechanism for efficient and low-latency block validation. The blockchain not only stores verified event messages but also dynamically updates the trust scores of vehicles, allowing for transparent and decentralized trust management.

Block Structure and Hash Chaining:

Each block B_k In the blockchain, records are verified messages along with their associated trust evaluations and are cryptographically linked to their predecessors to maintain data integrity. A block consists of the following fields:

$$B_k = \{\text{Block ID}, T_k, \text{H}(B_{k-1}), H_{MR}, \{M_i\}, \{TL_i\}, RSU_j, N_k\} \quad (22)$$

Where:

T_k is the current timestamp,

H (B_{k-1}) is the hash of the previous block,

$\{M_i\}$ are the validated event messages,

$\{TL_i\}$ are the updated trust levels of the sender vehicles,

RSU_j Is the identity of the RSU that mined the block?

N_k is a nonce used in difficulty calculation (if required),

H_{MR} Is the Merkle root of message hashes, computed as:

$$H_{MR} = \text{MerkleRoot}(\text{H}(M_1), \text{H}(M_2), \ldots, \text{H}(M_n \quad (23)$$

The final block hash is calculated as:

$$\text{H}(B_k) = \text{H}(\text{H}(B_{k-1}) \,||\, H_{MR} \,||\, t_k \,||\, RSU_j \,||\, N_k \quad (24)$$

This ensures immutability of the chain; any tampering with message data would alter the hash and break the chain's continuity.

Consensus Mechanism: Proof of Authority (POA):

To ensure low computational overhead and fast block generation, the system adopts Proof-of-Authority. In POA, a fixed set of authorized RSUs participates in block validation. A block is accepted into the chain only if approved by a supermajority of RSUs:

$$\sum_{j=1}^{n} I_{approve}(R_j, B_k) \geq \left\lceil \frac{2m}{3} \right\rceil \quad (25)$$

Where approve is an indicator function returning 1 if RSU R; validates B, and m is the total number of validators. PoA minimizes delay, making it suitable for real-time VANET operations, while also protecting against Sybil and DoS attacks by limiting participation to verified RSUs.

Trust Score Integration and Update:

Each event message M carries a temporary trust score Temp, which is either accepted or recalculated based on RSU-side validation. If the message is confirmed to be true, the vehicle's trust history is updated as:

$$TL_i = \frac{p_i}{p_i + q_i} \quad (26)$$

Where:

P is the count of verified (true) messages from vehicle Vi,

Q is the count of false or rejected messages from Vi.

If the new message is:

True: Pi← Pi + 1

False: qi + 1

To smooth trust fluctuations, a weighted trust update is performed:

$$TL_i^{new} = \lambda . TL_i^{prev} + (1 - \lambda) . \frac{p_i}{p_i + q_i} \quad (27)$$

Where E [0, 1] is the trust decay factor. The list of parameters used in this research, along with their descriptions, is given in Table 1.

Block Creation and Broadcast:

After accumulating a sufficient number of verified event messages in the local message pool P_{valid}The Roadside Unit (RSU) initiates the process of generating a new block for the blockchain. First, the RSU constructs a proposed blockByBy, which encapsulates the validated message set $\{M\}$ along with their associated trust levels (TL scores). Once the content of the block is finalized, the RSU computes the cryptographic hash of the block $H(B)$ to ensure the integrity and immutability of its contents. Following this, the RSU digitally signs the block using its private key, thereby guaranteeing its authenticity and preventing unauthorized modifications. The signed block is then broadcast to other RSUs in the consortium blockchain network, where a consensus voting mechanism, based on Proof-of-Authority (PoA), is used to validate the proposed block. Only after a quorum of trusted RSUs reaches agreement, the block is considered valid, appended to the distributed ledger, and synchronized across all participating consortium nodes, thus ensuring consistency, trust transparency, and secure event recordkeeping throughout the VANET environment.

Table 1. List of Symbols and Descriptions

Symbols	Descriptions
δ_t	Acceptable timestamp deviation
δ_l	Acceptable spatial deviation (distance threshold)
V_r	Historical validity ratio
C_i	Current consistency score
R_i	Recent behavior score
TL_i	Trust level/score of vehicles Vi
α, β, γ	Weight coefficients for computing trust score (sum to 1)
h_i	Number of verified (honest) messages by Vi
f_i	Number of false/discarded messages by V;
λ	Trust decay/weight factor for moving average
B_k	Block k in the blockchain
H_{bk-1}	Hash of the previous block
T_k	Timestamp of block B
H_{mi}	Hash of message M;
$H_{(MR)}$	Merkle root of all messages in the block
N_k	Nonce value used for block hashing (if needed)
$I_{Improve}(R_J, B_k)$	Indicator function returning 1 if RSU R approves block B
M	Total number of authorized validators (RSUs)
P_i	Number of true/verified messages from Vi
q_i	Number of false/rejected messages from Vi
T_{v2i}	Number of false/rejected messages from Vi
T_{comm}	Total time for vehicle-to-infrastructure communication, Transmission latency

Local Chain Update and Public Access:

All Roadside Units (RSUs) and authorized stakeholders, such as traffic management authorities and insurance companies, maintain a synchronized and tamper-resistant copy of the blockchain ledger. This distributed architecture ensures consistent access to validated information across the network. Vehicles can query their nearest RSU or local roadside cache

to retrieve essential data, including verified event messages within their geographic region, trust levels of message-sending vehicles, and historical records of traffic incidents and driving behaviors. Such access facilitates transparency and accountability, empowering entities to make informed decisions based on verifiable data. Moreover, the system supports privacy-preserving auditing, as each vehicle's trust reputation evolves based on its messaging behavior, yet remains decoupled from the driver's real identity. This ensures a balance between security, trust evaluation, and user privacy in dynamic vehicular networks.

Discussion:

This section presents the empirical evaluation of the proposed CB-RTM model for secure and trust-aware message dissemination in Vehicular Ad Hoc Networks (VANETs). The performance of the model is assessed through simulations conducted in a controlled vehicular environment that closely mimics real-world traffic dynamics. The key objectives of the evaluation are:

- To verify the accuracy of trust computation and its resilience against false event messages,
- To measure blockchain propagation latency and block confirmation time,
- To evaluate network throughput, communication overhead, and storage efficiency,
- And to compare the performance of CB-RTM with traditional blockchain-based and trustless VANET systems.

Experimental Setup:

The CB-RTM model is implemented using a custom simulation environment built over SUMO (Simulation of Urban Mobility) for vehicular mobility, OMNeT++ for network simulation, and a lightweight blockchain framework implemented in Python. The simulation scenario involves:

- Number of vehicles: 100 to 500 (scalable)
- Number of RSUs: 10 (acting as consortium validators)
- Blockchain block size: 1 MB
- Message rate: 1–5 messages per second per vehicle
- Consensus protocol: Proof-of-Authority (PoA)
- Simulation duration: 1000 seconds

Vehicles generate event messages (e.g., accident alerts, congestion, sudden stops), which are validated by RSUs before being added to the blockchain. A variety of message sources are simulated, including trustworthy, malicious, and random-noise emitters to test system robustness. The proposed framework utilizes the Elliptic Curve Digital Signature Algorithm (ECDSA) for digitally signing blocks, offering strong security with lower computational overhead, ideal for resource-limited RSUs in VANETs. For block integrity, the SHA-256 hash function is applied to generate cryptographic hashes, ensuring the immutability and tamper resistance of blockchain records. This combination of ECDSA and SHA-256 establishes a lightweight yet secure foundation for trust management and message verification within the consortium blockchain network.

Results:

To validate the performance and reliability of the proposed CB-RTM (Consortium Blockchain for RSU-Assisted Trust Management) framework in VANETs, a series of simulation-based experiments were conducted. The outcomes are analyzed across several critical dimensions, including trust accuracy, latency, throughput, communication overhead, and trust score stability over time. The model is compared against three baseline approaches: a trust-less VANET [18], a reputation-based trust model without blockchain [19], and a blockchain VANET using PoW consensus [20]. All tests were repeated across 10 independent

simulation runs to ensure statistical reliability. The results are reported as mean ± standard deviation (SD). Where applicable, 95% confidence intervals (CI) were also calculated.

Trust Accuracy Evaluation:

The primary metric in trust-based message dissemination systems is trust accuracy, the ability to correctly classify event messages as genuine or malicious based on the sender's behavioral history and location proofs.

The CB-RTM model achieved a trust accuracy of 96.2% ± 0.34, significantly outperforming baseline systems ($p < 0.01$). This is attributed to the combined effect of real-time RSU validation, PoL verification, and the immutable blockchain ledger. The results are shown in Table 2.

Table 2. Results: Trust Accuracy

Model	Trust Accuracy (%)
CB-RTM (Proposed)	96.2 ± 0.34
Trust-less VANET	64.8 ± 1.1
Reputation-Based Model	81.5 ± 0.8
VANET using PoW	95.45 ± 0.37

Block Confirmation Time:

Low latency in block confirmation is crucial for real-time vehicular communication. In the CB-RTM model, block confirmation time was measured from the moment an RSU generated a block proposal until it received enough votes (from >67% validators) to confirm the block. CB-RTM, leveraging PoA (Proof-of-Authority) consensus, demonstrated an average confirmation time of 0.42 ± 0.05 seconds, significantly faster than the PoW-based blockchain (8.5 ± 0.6 seconds). The improvement results from deterministic finality and reduced computation overhead. The results are shown in Table 3.

Table 3. Results: Block Confirmation Time

Model	Average Confirmation Time (sec)
CB-RTM (Proposed)	0.42 ± 0.05
Blockchain with PoW	8.5 ± 0.6
Reputation Model	3.4 ± 0.3
Trust-less VANET	4.8 ± 0.4

Network Throughput:

Network throughput indicates the system's ability to process messages under load. CB-RTM achieved a stable throughput of 245 ± 6.8 messages/sec, maintaining performance even as traffic density increased. In contrast, PoW-based systems experienced sharp declines due to mining delays. The results are shown in Table 4.

Table 4. Results: Network Throughput

Model	Throughput (message/sec)
CB-RTM (Proposed)	245 ± 6.8
Blockchain with PoW	76 ± 5.1
Reputation Model	300 ± 10.2 (no filtering)
Trust-less VANET	112 ± 3.4

Communication Overhead:

CB-RTM introduces some communication overhead due to the inclusion of trust metadata (e.g., PoL, pseudo-IDs, signatures) and consensus messages among RSUs. However, this overhead is significantly lower than traditional blockchain systems. The proposed system maintained an average communication overhead of 11.2 ± 0.3%, as compared to 19.4 ± 0.5% in PoW-based blockchain and 9.8 ± 0.2% in basic reputation models. The results are shown in Table 5.

Table 5. Results of Communication Overhead

Model	Throughput (message/sec)
CB-RTM (Proposed)	11.2 ± 0.3
Blockchain with PoW	19.4 ± 0.5
Reputation Model	9.8 ± 0.2
Trust-less VANET	3.6 ± 0.1

Discussion:

The experimental evaluation of the proposed CB-RTM (Consortium Blockchain for RSU-Assisted Trust Management) framework demonstrates its strong performance in terms of trust accuracy, latency, throughput, communication overhead, and trust score stability. Compared to the three baseline approaches, trust-less VANET [18], a reputation-based trust model without blockchain [19], and a blockchain VANET using PoW consensus [20], CB-RTM consistently outperforms across all key metrics. This discussion interprets the empirical findings and positions CB-RTM within the context of related studies.

A significant highlight of the results is the high trust accuracy achieved by CB-RTM, measured at 96.2%, which is considerably higher than the trust-less VANET (64.8%) and the reputation-based model (81.5%). While the blockchain with PoW consensus showed comparable performance (95.45%), CB-RTM's tighter integration of Proof-of-Location (PoL), real-time RSU validation, and tamper-proof blockchain storage provides a more robust and context-aware trust mechanism. Unlike the reputation-based model, which primarily relies on behavioral history and can be susceptible to identity spoofing or collusion, CB-RTM leverages spatial-temporal evidence and authenticated identities, thereby increasing resistance against common VANET threats like message injection and Sybil attacks.

Another key strength of CB-RTM is its block confirmation latency, which was recorded at 0.42 seconds. This is a substantial improvement over the 8.5 seconds observed in the PoW-based blockchain VANET. The PoW model, while secure, introduces prohibitive delays due to its computational complexity, making it unsuitable for time-sensitive vehicular applications. In contrast, CB-RTM uses Proof-of-Authority (PoA) consensus, which enables rapid block validation with minimal overhead. Even when compared to the reputation-based model (3.4 seconds) and trust-less VANET (4.8 seconds), CB-RTM provides superior responsiveness, making it viable for real-time scenarios such as collision avoidance and emergency message dissemination. In terms of network throughput, CB-RTM maintains an average of 245 messages per second, outperforming both the PoW-based blockchain (76 messages/sec) and trustless VANET (112 messages/sec). Although the reputation-based model showed a higher raw throughput (300 messages/sec), it lacks the filtering and validation mechanisms integrated into CB-RTM, which raises concerns about the reliability of disseminated messages. CB-RTM strikes a balance between volume and integrity, ensuring that only verified and trusted messages propagate through the network.

CB-RTM's communication overhead was 11.2% which is higher than both the trust-less VANET overhead (3.6%) and the reputation-based model overhead (9.8%) but significantly lower than the PoW overhead of the blockchain approach (19.4%). Although CB-RTM incurs higher costs in communication overhead as a result of trust metadata (PoL certificates, digital signatures, and pseudo-identifiers), this overhead cost is widely justified in terms of message security, accountability, and relevance via RSU validation and geofencing for message propagation.

Beyond the quantitative results, CB-RTM offers architectural advantages that enhance scalability and modularity. RSUs serve as localized validators, enabling regional consensus and reducing the need for global synchronization. This geo-fenced consensus mechanism improves the system's ability to scale horizontally across larger urban areas without introducing bottlenecks. Furthermore, by embedding trust management directly into the

blockchain layer, rather than treating it as a loosely coupled or external module, CB-RTM ensures that all trust-related decisions are auditable, immutable, and verifiable.

In contrast with previous research, CB-RTM combines the strengths of both blockchain and trust systems without the weaknesses. First, CB-RTM provides the same high levels of accuracy as PoW-based blockchains, at the same time as providing low latency like centralized reputation systems and the scalability of modular RSU-based validation, all while avoiding the high overhead and centralization disadvantages exhibited in previous designs. Secondly, C B-RTM also offers third-party stakeholders such as law enforcement, traffic regulators, and insurance companies the transparency and audibility benefits of the framework so they can also leverage the trust records that are stored in the blockchain for their post-incident analysis or disputes.

Conclusion:

This paper presents CB-RTM, a blockchain-based decentralized trust management framework designed specifically for VANETs. After conducting a systematic literature review, the study identified critical limitations in existing centralized and decentralized trust models, including latency, reliance on single points of failure, limited verifiability, and high computational overhead. The proposed CB-RTM framework addresses these challenges by leveraging consortium blockchain technology to ensure transparent, tamper-resistant, and real-time verification of event messages. It effectively tracks the trustworthiness of vehicles based on historical behavior and enables consensus-based validation among RSUs. Extensive simulation and evaluation demonstrate that CB-RTM achieves improved trust accuracy, low validation latency, and efficient resource usage, without requiring additional hardware or centralized infrastructure. Its ability to record vehicle reputation and event reliability in an immutable ledger establishes a dependable ground truth for future vehicular interactions.

Future recommendations:

Future work will focus on enhancing the scalability of CB-RTM by integrating adaptive consensus mechanisms suitable for dense traffic environments. Additionally, real-world deployment scenarios will be explored to test performance under dynamic mobility patterns and diverse attack models. We also aim to integrate privacy-preserving identity mechanisms and explore the fusion of federated learning with trust scoring to further improve decision-making accuracy in highly mobile vehicular networks.

References:

[1] L. M. Eslam Farsimadan, "A Review on Security Challenges in V2X Communications Technology for VANETs," *IEEE A*, 2025, [Online]. Available: https://ui.adsabs.harvard.edu/abs/2025IEEEA..1331069F/abstract

[2] K. R. Esti Rahmawati Agustina, "A Systematic Literature Review on Privacy Preservation in VANETs: Trends, Challenges, and Future Directions," *IEEE Access*, vol. 99, 2025, doi: 10.1109/ACCESS.2025.3570491.

[3] A. Heidari, M. A. J. Jamali, and N. J. Navimipour, "An Innovative Performance Assessment Method for Increasing the Efficiency of AODV Routing Protocol in VANETs Through Colored Timed Petri Nets," *Concurr. Comput. Pract. Exp.*, vol. 37, no. 3, p. e8349, Feb. 2025, doi: 10.1002/CPE.8349;REQUESTEDJOURNAL:JOURNAL:15320634;WGROUP:STRING:PUBLICATION.

[4] A. T. A. Walid El-Shafai, "AI-Driven Ensemble Classifier for Jamming Attack Detection in VANETs to Enhance Security in Smart Cities," *IEEE Access*, vol. 99, 2025, doi: 10.1109/ACCESS.2025.3552544.

[5] Q. Tao, X. Cui, H. Ding, Z. Shen, and Y. Li, "ELSP-MA: An Efficient Lightweight and Security-enhanced Privacy-preserving Message Authentication Scheme for VANETs," *IEEE Trans. Veh. Technol.*, 2025, doi: 10.1109/TVT.2025.3571380.

[6] F. P. Xiaoliang Wang, Peng Zeng, Guikai Liu, Kuan-Ching Li, Yuzhen Liu, Biao Hu, "A

privacy-preserving certificate-less aggregate signature scheme with detectable invalid signatures for VANETs," *J. Inf. Secur. Appl.*, vol. 89, p. 104001, 2025, doi: https://doi.org/10.1016/j.jisa.2025.104001.

[7] A. Z. J. Shahparian, S.H. Erfani, "A secure and efficient authentication and key agreement protocol in blockchain-enabled VANETs," *Comput. Electr. Eng.*, vol. 122, p. 109947, 2025, doi: https://doi.org/10.1016/j.compeleceng.2024.109947.

[8] C. S. Huimin Li, "A certificateless aggregate signature scheme for VANETs with privacy protection properties," *PLoS One*, vol. 20, no. 2, p. 2, 2025, doi: 10.1371/journal.pone.0317047.

[9] C. Cai, X. Yuan, and C. Wang, "Towards trustworthy and private keyword search in encrypted decentralized storage," *IEEE Int. Conf. Commun.*, vol. 0, Jul. 2017, doi: 10.1109/ICC.2017.7996810.

[10] A. Kosba, A. Miller, E. Shi, Z. Wen, and C. Papamanthou, "Hawk: The Blockchain Model of Cryptography and Privacy-Preserving Smart Contracts," *Proc. - 2016 IEEE Symp. Secur. Privacy, SP 2016*, pp. 839–858, Aug. 2016, doi: 10.1109/SP.2016.55.

[11] W. J. & H. L. Qiuling Yue, "A lightweight certificateless aggregate signature scheme without pairing for VANETs," *Sci. Rep.*, vol. 15, no. 23663, 2025, doi: https://doi.org/10.1038/s41598-025-08656-1.

[12] H. Hasrouny, A. Samhat, C. Bassil, and A. Laouiti, "Trust model for group leader selection in VANET," *Int. J. Digit. Inf. Wirel. Commun.*, vol. 8, no. 2, pp. 139–143, 2018, doi: 10.17781/P002421.

[13] U. Javaid, M. N. Aman, and B. Sikdar, "DrivMan: Driving trust management and data sharing in VANETs with blockchain and smart contracts," *IEEE Veh. Technol. Conf.*, vol. 2019-April, Apr. 2019, doi: 10.1109/VTCSPRING.2019.8746499.

[14] S. C. M. Saeid HaghighiFard, "Hierarchical Federated Learning in Multi-hop Cluster-Based VANETs," *arXiv:2401.10361*, 2024, doi: https://doi.org/10.48550/arXiv.2401.10361.

[15] H. Zhang, Jing and Wang, Xin and Cui, Jie and Li, Ru and Zhong, "A Decentralized Threshold Credential Management With Fine-Grained Authentication for VANETs," *IEEE Trans. Inf. Forensics Secur.*, 2025, [Online]. Available: https://ieeexplore.ieee.org/document/11027789

[16] P. Vinayasree and A. M. Reddy, "A Reliable and Secure Permissioned Blockchain-Assisted Data Transfer Mechanism in Healthcare-Based Cyber-Physical Systems," *Concurr. Comput. Pract. Exp.*, vol. 37, no. 3, p. e8378, Feb. 2025, doi: 10.1002/CPE.8378.

[17] A. Deng, Q. Ren, Y. Wu, H. Lei, and B. Chen, "Proof of Finalization: A Self-Fulfilling Function of Blockchain.," *IEEE Trans. Inf. Forensics Secur.*, vol. 19, pp. 8052–8065, 2024, doi: 10.1109/TIFS.2024.3451355.

[18] C. Chukwuocha, P. Thulasiraman, and R. K. Thulasiram, "Trust and scalable blockchain-based message exchanging scheme on VANET," *Peer-to-Peer Netw. Appl.*, vol. 14, no. 5, pp. 3092–3109, Sep. 2021, doi: 10.1007/S12083-021-01164-9/METRICS.

[19] G. Q. Yingqing Wang, Yanhua Liang, Yue Huang, "VECLLF: A vehicle-edge collaborative lifelong learning framework for anomaly detection in VANETs," *Comput. Networks*, vol. 265, p. 111328, 2025, doi: https://doi.org/10.1016/j.comnet.2025.111328.

[20] K. R. Dhawale, P. Dubey, A. R. P. Bhagat, K. R. Dhawale, P. Dubey, and A. R. P. Bhagat, "Blockchain Enhanced VANETs for Secure, Resilient, and Efficient Urban Mobility," *https://services.igi-global.com/resolvedoi/resolve.aspx?doi=10.4018/979-8-3373-0265-2.ch013*, pp. 247–270, Jan. 1AD, doi: 10.4018/979-8-3373-0265-2.CH013.