Federated Blockchain-Based Resilient Identity Management for Securing Consumer Vehicular Networks

Sandeep Srivastava, Deepshikha Agarwal, *Senior Member, IEEE*, Brijesh Kumar Chaurasia, *Senior Member, IEEE*, Vishal Krishna Singh, Rajkumar Singh Rathore, *Senior Member, IEEE*, Weiwei Jiang, *Member, IEEE*.

***Abstract*—Connected vehicles rely heavily on mobile vehicular networks and centralized cloud infrastructures for data handling. These networks contain not only environmental information but also sensitive data such as passenger identities, routes, origins, and destinations, making them prone to various cyber threats. Existing authentication mechanisms are predominantly centralized and cloud-based, which introduces significant vulnerabilities, including high latency, single points of failure, and exposure to denial-of-service attacks, man-in-the-middle intrusions, and data breaches. Moreover, the real-time nature of vehicular data sharing exacerbates these risks. Conventional centralized architectures typically depend on a single trusted authority for vehicle authentication and data integrity validation, which further increases susceptibility to unauthorized access, data tampering, and system disruption. To address these limitations, this work proposes a novel distributed blockchain-based authentication mechanism for Internet of Vehicles and autonomous vehicles. The proposed approach leverages decentralized identifiers and verifiable credentials to securely authenticate vehicles within a decentralized network. Extensive experimental evaluations assess the system's performance across multiple parameters, including latency, trust, and resilience to attacks. Comparative analysis demonstrates a significant improvement in trustworthiness and authenticity, validating the effectiveness of the proposed method.**

I. Introduction

Internet of Vehicles (IoVs) comprises vehicles embedded with sensors and on-board units (OBUs) capable of performing low-level automation and interacting with surrounding Internet of Things (IoT) networks [1], [2]. Advanced IoV variants form the operational basis for self-driving vehicles, enabling autonomous navigation in complex environments without human intervention and ensuring high standards of safety for both passengers and other road users [3], [4], [5]. Connected vehicles rely extensively on vehicular communication networks such as Vehicular Ad-hoc Networks (VANETs), vehicle-to-vehicle (V2V) communication, and vehicle-to-infrastructure (V2I) communication to gather and exchange real-time environmental information [1], [6], [2].

Through embedded sensors and OBUs, vehicles communicate with nearby IoVs, forming dynamic and highly mobile networks where each IoV functions as an active node [1], [2]. The exchanged data is transmitted over wireless channels and is often stored or temporarily buffered in cloud-based systems or edge servers, depending on the network architecture [2], [7]. This communication enables vehicles to share critical information such as traffic conditions, road hazards, and signal timings, supporting autonomous systems in making timely and reliable driving decisions. Such collaborative information exchange improves route selection, reduces congestion, and enhances both safety and overall operational efficiency [6], [2], [1].

These networks transmit not only environmental information but also sensitive data, including passenger identities, routes, and destination details, increasing the importance of secure communication handling [1], [8]. Because communication occurs over public wireless channels, IoV systems are exposed to a wide spectrum of cyberattacks, including spoofing, replay, and eavesdropping, which significantly threaten data confidentiality and authenticity [6], [9], [10]. Consequently, secure communication requires processing a large number of authentication requests in real time, necessitating a robust, accurate, and scalable authentication mechanism capable of handling high-density vehicular traffic [8]. Given the heavy reliance of connected vehicles on exchanged data, authentication must be both rapid and dependable to maintain uninterrupted information flow. However, the massive volume of data generated by IoVs, coupled with their dynamic mobility, makes real-time authentication increasingly challenging [2], [1].

The deployment of VANET clouds has simplified data storage and management [2], [1], enabling vehicles to obtain road and traffic information directly from the cloud rather than establishing multiple peer-to-peer connections. However, this centralization also introduces severe security risks such as Distributed Denial of Service (DDoS), forgery, and Man-in-the-Middle (MitM) attacks [9], [8]. To mitigate these threats, a two-level authentication system is essential—one level for verifying node legitimacy and another for message authentication [11], [10]. Node authentication prevents unauthorized devices from joining the network, while message authentication ensures data integrity and prevents tampering.

A variety of blockchain-based authentication frameworks

Corresponding author: Sandeep Srivastava (email: sandeep.s@iiitl.ac.in

Sandeep Srivastava is with the Department of Computer Science, Indian Institute of Information Technology Lucknow, India.

Deepshikha Agarwal is with the Department of Information Technology, Indian Institute of Information Technology Lucknow, India.

Brijesh Kumar Chaurasia is with Department of Computer Science and Engineering, Pranveer Singh Institute of Technology, Kanpur.

Vishal Krishna Singh is with School of Computer Science and Electronics Engineering, University of Essex, Colchester Campus, United Kingdom.

Rajkumar Singh Rathore is with Department of Computer Science, School of Technologies, Cardiff Metropolitan University, United Kingdom

Weiwei Jiang is with School of Information and Communication Engineering, Beijing University of Posts and Telecommunications, Beijing, China

have been proposed in existing literature. The scheme in [12] presents a four-phase process consisting of system initialization, key generation, signing, and verification. Similarly, the conditional anonymous mutual authentication model introduced in [13] enhances privacy and anonymity using certificateless short signatures (CLSS) and regional management strategies, thereby minimizing dependency on public key infrastructures. Another approach in [14], [15] uses a trusted authority (TA) and roadside units (RSUs) to establish secure session key exchanges, whereas the work in [16], [17] proposes a hierarchical revocable authentication protocol utilizing Schnorr signatures and self-certified public keys. Additional schemes such as [18], [19] highlight the use of certificateless signcryption and batch-verification mechanisms to improve scalability and reduce computational overhead. Collectively, these methods include phases for initialization, registration, revocation, and key agreement, ensuring secure authentication between vehicles and RSUs without continuous authority involvement.

In [20], a three-phase authentication process—registration, authentication, and authorization—is introduced to validate vehicles through pseudonymous IDs and digital signatures. Similarly, the group-based authentication protocol in [21] employs signcryption and secret member keys to achieve anonymity and traceability. In contrast, a trusted-authority-free lightweight scheme proposed in [22] uses elliptic curve cryptography (ECC) and message encapsulation to enable privacy-preserving communication between vehicles and RSUs. This two-layered model—comprising server and vehicle layers—ensures decentralized key management, reducing computational overhead while maintaining security and scalability.

Despite these contributions, most existing schemes face significant limitations in real-world IoV deployments. Many rely on centralized or semi-centralized architectures that introduce single points of failure, bottlenecks, and scalability issues. High network mobility and dynamic topologies further complicate timely authentication, often leading to high latency and degraded performance. Additionally, IoV networks remain susceptible to various cyberattacks, including Man-in-the-Middle (MitM), relay, Sybil, DoS, and DDoS attacks, which can compromise data confidentiality, authenticity, and availability [8], [10], [23]. As the number of connected vehicles increases, the corresponding surge in authentication requests strains existing systems, highlighting their limited scalability and computational efficiency.

Modern decentralized identity and authentication systems increasingly rely on distributed trust assumptions—such as threshold-signature validation, federated verifiers, multi-domain credential issuers, and cross-ledger coordination—to ensure consistency and resilience. However, the evaluation strategies commonly adopted in prior IoV and VANET authentication studies primarily emphasize throughput, latency, message verification speed, or cryptographic soundness. These metrics, while essential, provide limited insight into the economic, behavioral, and adversarial incentives that determine how real-world attackers and insider entities actually behave. Existing analyses generally assume honest-majority conditions or static adversary models without quantifying the feasibility of bribery, insider collusion, or rational deviation under realistic cost–benefit scenarios. As a result, current identity-management frameworks remain unable to predict when a system becomes economically vulnerable, even if the underlying cryptographic primitives remain theoretically secure.

To address this limitation, this work incorporates an incentive-aware evaluation methodology that models adversarial behavior using attacker utility functions, binomial compromise probabilities, shareholder collusion payoffs, and equilibrium threshold analyses. This approach complements traditional cryptographic proofs by capturing the economic motivations that influence whether rational actors comply with or deviate from protocol rules. The goal is to provide a more comprehensive, real-world security characterization for federated blockchain-based identity management, ensuring that both technical and incentive-driven vulnerabilities are effectively mitigated.

These challenges reveal a clear scientific problem: *current IoV authentication frameworks lack a fully decentralized, lightweight, and resilient mechanism capable of maintaining trust, privacy, and scalability in real-time vehicular environments.* The inability to support large-scale, low-latency authentication in dynamic IoV networks leaves critical security and efficiency gaps.

Motivated by these challenges, this paper proposes a Federated Blockchain-Based Resilient Identity Management Framework (BlockAuth) designed specifically for secure and scalable IoV environments. The objective of BlockAuth is to establish decentralized trust among vehicles, roadside units, and governing authorities by combining Decentralized Identifiers (DIDs) and Verifiable Credentials (VCs) with blockchain technology. The purpose of this research is to develop an identity management framework that reduces authentication latency, minimizes central dependency, and enhances system resilience against attacks. By integrating federated blockchain and decentralized identity principles, the proposed BlockAuth framework ensures tamper resistance, privacy preservation, and trust verification suitable for next-generation intelligent vehicular ecosystems.

A. Contributions

This work introduces a federated, blockchain-enabled identity management framework tailored for secure, scalable, and low-latency authentication in Internet of Vehicles (IoV) environments. The following contributions collectively highlight the technical innovations and practical advancements enabled by the proposed *BlockAuth* system:

- **Decentralized Authentication Framework (BlockAuth):** A federated blockchain-based authentication model integrating *Decentralized Identifiers (DIDs)* and *Verifiable Credentials (VCs)* is proposed. This decentralized trust establishment removes reliance on centralized authorities, eliminating single points of failure and improving the robustness of IoV authentication.
- **Cryptographic Binding of Vehicular Identities:** BlockAuth ensures that each vehicle's identity is cryptographically anchored to the blockchain ledger, preserving im-

mutability and enabling verifiable, tamper-resistant authentication to mitigate spoofing, replay, and impersonation attacks.
- **Hybrid Blockchain Deployment and Validation:** The framework is implemented on both the Ethereum blockchain and a custom lightweight blockchain to assess performance under diverse deployment conditions. Experiments confirm significantly reduced signing and verification times while sustaining high throughput and low latency.
- **Comprehensive Security and Performance Evaluation:** Simulations and adversarial modeling validate BlockAuth's resilience against threats such as DoS and MitM attacks. Results demonstrate over 98% authentication accuracy, more than 60% latency reduction, and stable trust scores even under high-load scenarios.
- **Advancement in Vehicular Identity Management:** BlockAuth provides a scalable and privacy-preserving identity framework suitable for real-time autonomous transportation systems. The integration of blockchain, DIDs, and VCs enables tamper-resistant, transparent authentication for large-scale vehicular ecosystems.

B. Novelty

The novelty of BlockAuth lies in its ability to overcome the key limitations of existing blockchain-based vehicular authentication systems, enabling scalable, interoperable, and security-validated deployment in large IoV environments. The major contributions are:

- **Gap Identification:** A structured review highlights persistent issues in prior works—centralized trust dependency, limited cross-domain interoperability, and the lack of formal security validation—motivating a decentralized and verifiable authentication framework.
- **Federated Architecture with FANs:** BlockAuth deploys lightweight Federated Authentication Nodes (FANs) that enable fast local verification and synchronized global trust sharing. This design removes single points of failure and supports scalable cross-domain authentication.
- **Optimized DID/VC/ZKP Pipeline:** The framework combines DIDs, VCs, and lightweight zero-knowledge proofs, removing costly operations to achieve faster signing/verification and providing privacy-preserving attribute validation with low latency.
- **Game-Theoretic Security Modeling:** Formal attacker–collusion modeling quantifies adversarial behavior and defines resilience thresholds. The analysis shows strong Byzantine tolerance and stable authentication accuracy even with malicious participation.

C. Structure of paper

The structure of this paper is organized as follows. Section I introduces the motivation, background, and research gaps in existing IoV authentication mechanisms, leading to the need for a decentralized and federated identity management framework. Section II presents the *System Architecture and Problem Formulation*, defining the IoV model, adversarial assumptions, and the limitations of centralized authentication. Section III details the *Methodology*, including the proposed BlockAuth architecture, registration workflow, authentication mechanisms, and federated identity management. Section IV provides the *Results and Analysis*, offering performance evaluation, security assessment, and comparisons with contemporary blockchain-based schemes. Section V summarizes the findings in the *Conclusion*, highlighting contributions and potential areas for future improvement. Finally, Section VI lists the *References* cited throughout the paper.

II. System Architecture and Problem Formulation

A. System Model and Problem Description

The following assumptions are considered for modeling the IoV system:

- $\mathcal{V} = \{v_1, v_2, \ldots, v_n\}$ denotes the set of connected vehicles.
- $\mathcal{G} = (\mathcal{V}, \mathcal{E})$ denotes the communication graph, where edges $\mathcal{E}$ represent authentication requests.
- The data generated by vehicle v_i is denoted d_i (for example, route, location, or passenger information).
- $\mathcal{A}$ denotes the centralized authentication server.
- $\mathcal{B}$ denotes the distributed blockchain network.

The scientific problem addressed in this work arises from the inherent limitations of centralized and semi-centralized authentication architectures in existing IoV systems. As the number of vehicles increases, the authentication load grows proportionally with the request rate λn, resulting in congestion at the central server, delayed validation, poor scalability, and increased susceptibility to DoS-related disruptions. Moreover, these architectures lack cross-domain interoperability, preventing seamless authentication during inter-region mobility.

This problem becomes critical in latency-sensitive applications such as collision avoidance, cooperative perception, and real-time safety messaging, where authentication must be completed within strict delay bounds. Let T_i denote the authentication delay for vehicle v_i under a proposed model. With increasing network density, $T_i \to f(\lambda n)$, often exceeding acceptable thresholds. Further, centralized servers introduce single points of failure, enabling DoS, replay, Sybil, and impersonation attacks to compromise system-wide trust.

Therefore, the problem is formally defined as designing an authentication architecture that (i) reduces delay T_i, (ii) minimizes risk exposure $R(v_i)$, (iii) enables cross-domain trust propagation, and (iv) remains robust under adversarial conditions. The objective is to minimize $T_i^{\text{BlockAuth}}$ and $R_{\text{BlockAuth}}(v_i)$ subject to the constraints $T_i^{\text{BlockAuth}} \leq \tau$ and $R_{\text{BlockAuth}}(v_i) \leq \epsilon$, where τ and ϵ denote maximum acceptable limits for authentication latency and security risk. These requirements motivate the federated blockchain-driven identity management model presented in the subsequent sections.

It is assumed that each vehicle v_i must be authenticated before it is allowed to send and receive data in the network. Traditionally, this is achieved in a centralized system as:

$$\text{Auth}_{\text{central}}(v_i) = \mathcal{A}(d_i)$$

However, in such a centralized architecture, the authentication server becomes a critical dependency, introducing a *single point of failure*. If compromised or rendered unavailable—due to attacks such as Denial-of-Service (DoS), Man-in-the-Middle (MitM), or Replay/Spoofing—the entire vehicular authentication system can be disrupted. This dependency significantly undermines the resilience and availability of the network.

Problem: Latency and Computational Overhead in VSN Authentication

Vehicular Sensor Networks (VSNs) rely on timely and secure communication between vehicles for safe and efficient operation. However, the presence of untrusted or malicious nodes can significantly increase network latency and strain the computational resources of each vehicle.

Let M denote the total number of vehicles, m the number of malicious nodes, λ the arrival rate of authentication requests, and μ the processing capacity of an RSU or edge server. The network latency T_{resp} and per-vehicle computational cost C_{veh} are given by:

$$T_{\text{resp}} = \frac{1}{\mu - \lambda} + \frac{d}{v} + \frac{S}{R}, \qquad \lambda = \lambda_0 + \eta \cdot m,$$

where d is the average propagation distance, v is the signal speed, S is the message size, R is the data rate, and η captures the additional load from malicious nodes.

The computational overhead per vehicle, considering cryptographic operations for signing and verification, can be expressed as:

$$C_{\text{veh}} = \frac{1}{M} \left(\beta_s \cdot t_s + \beta_v \cdot t_v \right),$$

where β_s and β_v denote the number of signing and verification operations, and t_s, t_v represent the time per signing and verification operation, respectively.

An ideal authentication protocol for VSNs should ensure that both latency and computational overhead remain low, even as the network scales. Formally, this requires:

$$\lim_{|\mathcal{N}| \to \infty} C \approx 0, \qquad \lim_{|\mathcal{N}| \to \infty} L \approx L_{\min},$$

meaning that per-vehicle computational costs are negligible and communication remains efficient. Unfortunately, many existing protocols struggle to achieve this balance, leading to delayed authentication, excessive computational burden, and potential vulnerabilities that compromise the overall performance and security of the network.

Moreover, as the number of connected vehicles increases, the system faces a linear growth in authentication requests with respect to the vehicle population and message frequency. Let n denote the number of vehicles and λ the average authentication request rate per vehicle. The central server must handle up to $\lambda \cdot n$ requests per unit time. This rising demand imposes significant burdens on the server, leading to *increased latency*, *packet loss*, and *network congestion*, particularly in scenarios requiring real-time response, such as collision avoidance or emergency message propagation.

B. Federated Identity and Authentication Model

To support interoperability among diverse vehicular authorities, the proposed framework introduces a *Federated Identity Management Layer* built over the blockchain infrastructure. This layer enables cross-domain authentication and trust establishment among multiple administrative entities such as regional transport authorities, vehicle manufacturers, and infrastructure providers. Instead of relying on a single centralized authority, each participating domain maintains its own identity registry and collaborates with others through a shared global blockchain ledger. This design preserves administrative independence while ensuring secure and verifiable identity exchange across different domains.

Formally, let $F = \{F_1, F_2, \ldots, F_k\}$ denote the set of federated authorities, and $\mathcal{V}_i \subset \mathcal{V}$ represent the group of vehicles registered under authority F_i. Each authority maintains a local ledger B_i, which stores authentication and registration data specific to its domain. The validated identity records are periodically synchronized with a shared global ledger B_g, ensuring that verified information remains consistent and auditable throughout the federation. Cross-domain authentication is achieved through cooperative proof exchanges between the *Federated Authentication Nodes (FANs)* of any two authorities F_i and F_j. These proofs are validated and anchored on the global ledger.

C. Blockchain based Proposed BlockAuth

The proposed BlockAuth is designed to use a Decentralized Identifier (DID_i) and Verifiable Credential (VC_i). The authentication of connected vehicles is performed using smart contracts and is given as:

$$\text{Auth}_{\text{blockchain}}(v_i) = \mathcal{B}(\text{DID}_i, \text{VC}_i)$$

The proposed architecture aims to address the issue of *latency* by minimizing the authentication delays in the traditional architecture. The objectives of the proposed method is to reduce network latency.

Then:

$$\text{Latency Reduction: } \Delta T_i = T_i - T_i^{\text{BlockAuth}}$$

Considering the attack risk as:

$$R^{\text{central}}(v_i) = f(P_{\text{DoS}}, P_{\text{MitM}}, P_{\text{Spoof}})$$
$$R^{\text{BlockAuth}}(v_i) < R^{\text{central}}(v_i)$$

Within the constraints of evaluation parameters defined as:

- A performance metric $M(v_i)$ (e.g., trust score, availability, integrity).
- Constraint $M(v_i) \geq \theta$ (minimum acceptable trust threshold).

The goal is to optimize:

$$\begin{aligned} \max_{\text{Auth}} \quad & \sum_{i=1}^{n} M(v_i) \\ \text{subject to} \quad & R(v_i) \leq \epsilon, \quad \forall\, i = 1, \ldots, n, \\ & T_i \leq \tau, \quad \forall\, i = 1, \ldots, n, \end{aligned} \tag{1}$$

where ϵ denotes the maximum acceptable security risk and τ represents the maximum permissible authentication delay.

D. Simulation of Attacker and Collusion Incentives

A lightweight simulation framework was implemented to evaluate the economic incentives associated with both external attackers and internal colluding members. The probability of a successful external attack is modeled using the upper tail of a binomial distribution:

$$P_{\text{succ}} = \Pr(X \geq t), \qquad X \sim \text{Binomial}(N, p_s), \tag{2}$$

where N is the number of validators, t is the approval threshold, and p_s is the probability of compromising a single validator. The corresponding attacker utility is computed as:

$$U_a = B \cdot P_{\text{succ}} - C_a(p_s), \tag{3}$$

with B denoting the reward for a successful attack and $C_a(p_s)$ the expected compromise cost. An attack is economically viable only when $U_a > 0$. Varying (N, t, p_s) permits identification of threshold configurations that render $U_a < 0$, thereby discouraging strategic attacks.

For insider collusion, the expected per-member payoff is modeled as:

$$U_c = \frac{B_c \, \mathbf{1}_{m \geq t}}{m} - P_{\text{pen}} \, d(m), \tag{4}$$

where m is the coalition size, B_c the collective benefit, P_{pen} the penalty probability, and $d(m)$ the penalty magnitude. A coalition is rational only if:

$$U_c \geq R, \tag{5}$$

with R representing the minimum acceptable expected return.

This simulation framework enables systematic exploration of attacker viability and collusion boundaries, supporting the quantitative analysis presented in this study.

E. Computational Modeling of External Attacks and Internal Collusion

To quantitatively assess the resilience of the proposed BlockAuth framework, a probabilistic and game–theoretic model is implemented to capture both *external adversaries* and *internal colluding shareholders*. All computations and plots were generated using a custom Python-based simulation framework, allowing reproducible evaluation for varying numbers of validators (N), threshold values (t), and compromise probabilities (p_s).

- **Binomial Compromise Probability Model**
  The probability that an adversary compromises at least t out of N validators is modeled using the upper tail of a binomial distribution:

  $$P_{\text{succ}}(N, t, p_s) = \sum_{k=t}^{N} \binom{N}{k} p_s^k (1 - p_s)^{N-k},$$

  where p_s denotes the per-node compromise probability. This expression quantifies the minimum number of compromised validators required for an adversary to successfully approve a forged block.
- **Attacker Expected Utility**
  The expected utility of an attacker incorporates both the benefit of a successful compromise and the cumulative cost of corrupting validators:

  $$U_a = B \cdot P_{\text{succ}}(N, t, p_s) - cNp_s,$$

  where B is the reward for a successful attack and c is the per-node compromise cost. An attack is rational only when $U_a > 0$. Accordingly, for each (N, p_s) configuration, the smallest threshold t satisfying

  $$U_a < 0,$$

  renders the attack economically irrational.
- **Shareholder Collusion Incentive Model**
  Let m denote the coalition size of colluding shareholders. If $m \geq t$, the coalition receives a collective reward B_c, divided equally among all members; otherwise, the reward is zero. The probability of collusion detection increases with coalition size and is modeled as

  $$\text{detect}(m) = \alpha \frac{m}{N},$$

  leading to the following per-member utility:

  $$U_c(m) = \frac{B_c \cdot \mathbf{1}_{m \geq t}}{m} - P_{\text{collude}} \cdot \alpha \frac{m}{N}.$$

  A shareholder participates in collusion only when $U_c(m) \geq R$, where R denotes the minimum acceptable utility. Solving for the required benefit yields:

  $$B_{\text{collude\_critical}}(m) = m \left(R + P_{\text{collude}} \, \alpha \frac{m}{N} \right).$$

  The minimum value of $B_{\text{collude\_critical}}(m)$ for all $m \geq t$ represents the system-wide *incentive boundary*, indicating the threshold beyond which collusion becomes economically viable.

III. Methodology

The proposed architecture of the blockchain-based authentication procedure - *BlockAuth*, is shown in Figure 1. The process begins with the registration of vehicle credentials by the governing authority, when a unique vehicle ID is generated. Then a trusted authority logs this vehicle ID on the blockchain. The car sends a request to join the VANET during the authentication phase as soon as it is within the communication range of an RSU. The blockchain-connected RSU validates the vehicle's credentials. The RSU allows the vehicle to connect to the network if the credentials are legitimate. The proposed BlockAuth technique integrates DID and VC to build a secure and scalable authentication framework within VANET. RSU nodes safely confirm their respective identities without relying on a central authority, reducing the vulnerability to single points of failure. The two main stages of the *BlockAuth* authentication procedure are *Registration* and *Authentication*. In order to safeguard network IoVs from risks

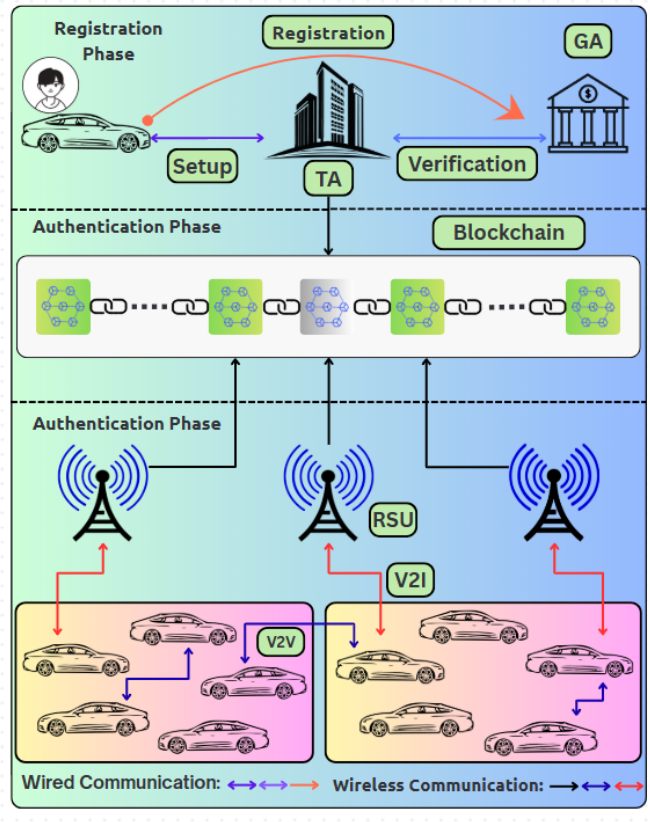


Fig. 1: Proposed BlockAuth Architecture

like identity spoofing, data tampering, and unauthorized access within VANETs, each phase serves a distinctive function. This architecture supports scalability and security while also meeting the decentralized needs of existing IoV ecosystems.

A. Registration

In this phase, the owner of the IoV and autonomous vehicle makes a *DID* and sends it with some claim to a trusted authority to generate a *VC*. The trusted authority then creates a *VC* linking the *DID* with the claim and uploads it to the blockchain in the form of a *DID* document. The *DID* document is then accessible and verifiable by anyone on the blockchain network. The holder then sends the *VC* to a governing authority that verifies the claims and validates the *VC*. The validated *VC* can then be used as proof of identity during the authentication process, providing secure and reliable verification of the holder's identity. The vehicle securely holds the *VC* and *DID* in the *OBU* for future use. The registration phase of the proposed BlockAuth is described in the Algorithm 1. The stepwise registration procedure is as follows:

- The owner of the self-driving vehicle, or IoV, makes a digital wallet that can be used to store and show DIDs.
- The digital wallet makes a private key (secret key) SK_u and the corresponding public key PK_u of the holder i.e., the vehicle. The public key PK_u is directly linked to the DID.

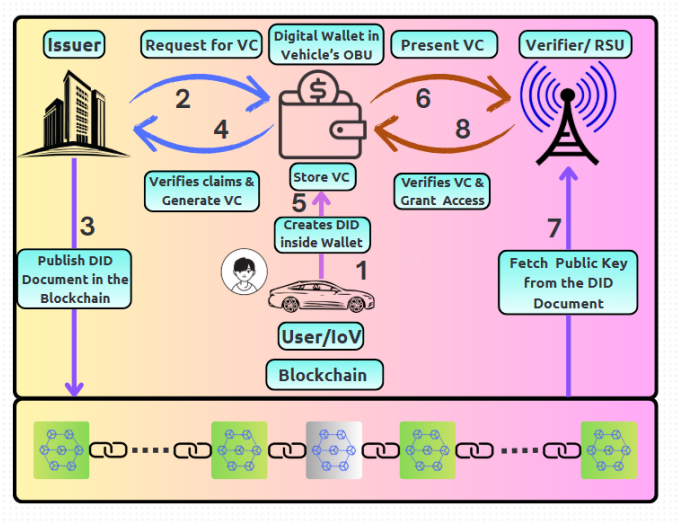


Fig. 2: Registration Phase

Algorithm 1 BlockAuth: Vehicle Registration Procedure

Input: DID_u, TA, GA
Output: Verified Verifiable Credential VC_u
// Digital Wallet Initialization:
  $DW \leftarrow InitWallet()$
// Key and Identifier Generation:
  $(SK_u, PK_u) \leftarrow KeyGen()$
  $DID_u \leftrightarrow PK_u$
// DID Document Construction:
  $DID_{doc} \leftarrow \{DID_u,\ C_u\}$ // where C_u = claim set
// Credential Request to TA:
  $\sigma_u \leftarrow Sign_{SK_u}(DID_{doc})$
  Send $(DID_{doc},\ \sigma_u)$ to TA
// TA Verification and Blockchain Registration:
  if $Verify_{PK_u}(\sigma_u) = 1$ **and** $Validate(C_u) = 1$ **then**
    $BC \leftarrow BC \cup \{DID_u,\ DID_{doc}\}$
    $VC_u \leftarrow IssueCredential(DID_u,\ C_u)$
  else reject
// GA Verification:
  Send VC_u to GA
  $VC_u \leftarrow GAValidate(VC_u)$
// Secure Storage:
  $DW \leftarrow DW \cup \{VC_u\}$

- The user creates a DID document consisting of DID and makes some claims about its authenticity in it. This is followed by a request generation to a trusted authority to generate verifiable credentials VC_u.
- The trusted authority checks the credibility of the claims and uploads the issuer's DID along with the holder's DID document on the blockchain and sends back the VC to the holder.
- The holder then sends the VC to a governing authority, which verifies the claim regarding the holder's identity and sends back the verified VC.
- The vehicle keeps the VC_u in the digital wallet located in the OBU.

B. Federated Authentication Workflow

To enable seamless and secure cross-domain authentication, the proposed *BlockAuth* framework introduces a *Federated Authentication Layer* consisting of multiple *Federated Authentication Nodes (FANs)*. Each FAN is managed by an authority $F_i \in F$ and collaborates with other FANs through a shared global ledger B_g. This cooperative structure ensures that identities verified within one administrative domain remain valid and verifiable across the entire federated ecosystem.

Workflow (Step-by-Step):

- **Vehicle registration:** A vehicle v registered under authority F_i is assigned a Decentralized Identifier (DID) and a Verifiable Credential (VC). These are securely stored in the vehicle's On-Board Unit (OBU), recorded in the local ledger B_i, and anchored to the global ledger B_g.
- **Local entry:** When vehicle v enters the coverage area of a Roadside Unit (RSU) managed by authority F_j, the RSU initiates an authentication request for the vehicle's DID and VC.
- **Local verification (fast path):** The FAN operating under F_j performs rapid signature verification using its local ledger B_j, enabling low-latency validation without requiring global consensus.
- **Federated confirmation (cross-domain):** If the vehicle is registered under a different authority $F_i \neq F_j$, the FAN at F_j issues a signed verification request to the FAN at F_i through the global ledger B_g. The issuing authority F_i validates ownership of the DID/VC pair and returns a signed proof of validity.
- **Proof anchoring:** The final verification proof, which combines both local and federated confirmations, is recorded on B_g to ensure global transparency, traceability, and non-repudiation.
- **Access decision:** Based on the aggregated verification results and consensus across participating FANs, the RSU grants or denies the vehicle access to the network.

This two-layered authentication strategy—comprising local validation and federated confirmation—achieves an effective balance between speed, security, and interoperability. It ensures reliable authentication even when vehicles traverse heterogeneous administrative domains, making it suitable for large-scale real-world vehicular deployments.

C. Authentication

The authentication phase of the proposed *BlockAuth* uses *VCs* and *DIDs* to establish a secure, efficient, and scalable authentication mechanism for vehicles within a vehicular network. Every vehicle in this process has a distinct *VC* that is issued by a reliable authority, connected to a unique *DID*. The vehicle provides its *VC* for authentication when in the range of an *RSU* as depicted in the figure 3. After that, the *RSU* checks the digital signature of the *VC* to ensure that it is authentic and that the credential was granted by a recognized body. The vehicle is authenticated by the *RSU* using a zero-knowledge proof-based procedure after it has been validated, and access is granted only if the credential is found to be legitimate. The complete authentication procedure (Algorithm 2) is described in the figure 3 and evidently proves that it builds trust and safety in the vehicle network by prohibiting unwanted access and protecting the privacy and integrity of vehicles. The stepwise authentication procedure is as follows:

- When the vehicle comes within the range of an RSU but is not yet connected to a nearby vehicular network, the nearby RSU initiates a request for verifiable credentials VC_u of the vehicle along with its associated digital signature. The procedure is described in Algorithm 2.
- The vehicle OBU computes the hash of VC_u, denoted as X_{vc}. Then it digitally signs the hash of VC_u using its private key SK_u to generate a signature Q_{vc}. The OBU sends the VC_u and the digital signature Q_{vc} to the RSU for verification.

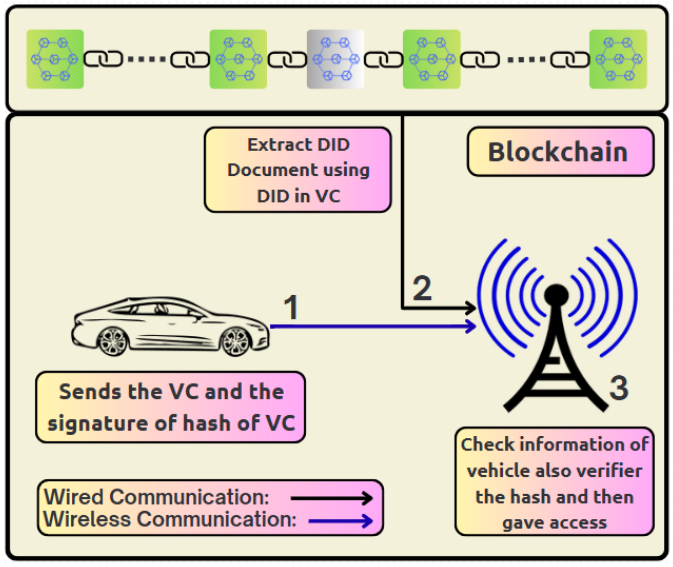


Fig. 3: Authentication Phase

Algorithm 2 BlockAuth: Vehicle Authentication Procedure

Input: Verifiable Credential VC_u; Private Key SK_u; Public Key PK_u; RSU range detection event
Output: Authentication decision (*Access Granted* or *Access Denied*)
// RSU Credential Request:
    RSU detects the vehicle entering its range and requests $\{VC_u, Q_{vc}\}$
// Vehicle Credential Preparation:
    $X_{vc} \leftarrow Hash(VC_u)$
    $Q_{vc} \leftarrow Sign_{SK_u}(X_{vc})$
    Vehicle sends $\{VC_u, Q_{vc}\}$ to the RSU
// RSU Credential Verification:
    Retrieve PK_u from the blockchain
    Verify VC_u attributes using Zero-Knowledge Proof
// RSU Signature Verification:
    $X'_{vc} \leftarrow Verify_{PK_u}(Q_{vc})$
    $Y_{vc} \leftarrow Hash(VC_u)$
    if $X'_{vc} = Y_{vc}$ **then**
        Access Granted
    else Access Denied

- Upon receiving VC_u and Q_{vc} from the vehicle, the RSU extracts the vehicle's public key PK_u reference on the blockchain. Using zero-knowledge proof (ZKP) techniques, the RSU can also extract and verify other relevant information contained within the VC, such as the vehicle's time of service, license validity, and any additional attributes required for authentication.
- When the RSU retrieves the reference to the vehicle's public key PK_u from the blockchain, it verifies the digital signature Q_{vc} using PK_u to obtain the signed hash X_{vc}. In parallel, the RSU computes the hash of the received verifiable credential, denoted as Y_{vc}. The values X_{vc} and Y_{vc} are then compared to confirm the authenticity and integrity of the credential.
- If both hash values X_{vc} and Y_{vc} match, the vehicle is granted access to join the network. Otherwise, rejected, enabling secure data transfer. This successful validation process ensures that the vehicle's credentials are authentic and have not been tampered with, thereby maintaining the integrity of the network.

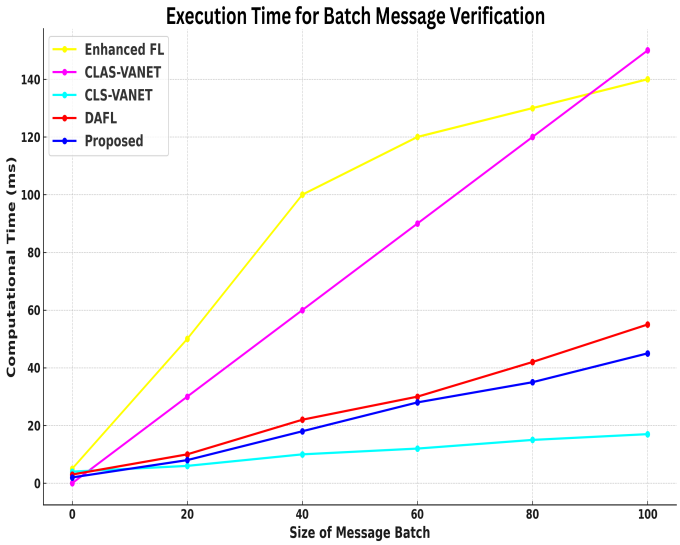


Fig. 4: Signing and Verification of Messages

IV. Result

A. Experimental Setup

TABLE I: Comprehensive Experimental Setup

Component	Specification
Real-World Testbed	
On-Board Unit (OBU)	Broadcom 2711, Cortex-A72, Quad-core, 64-bit
OBU Communication	WLAN 802.11b/g/n/ac (2.4 GHz + 5.0 GHz)
Roadside Unit (RSU)	ARM Cortex-A57, Quad-core @ 1.43 GHz
RSU Memory	4 GB LPDDR4 RAM, 64 GB Flash Storage
Deployment Architecture	Three-layered identity-based architecture
Simulated Environment	
Operating System	Ubuntu 20.04 LTS
Virtual Environment	Docker containers on VirtualBox
Processor	8 vCPUs per virtual node
Memory	16 GB RAM per node
Blockchain Platform	Hyperledger Fabric v2.4
Simulation Tools	Custom Python-based transaction generator
Network Emulation	P2P network topology (emulated)

A lightweight real-world deployment was carried out using the OBU–RSU testbed. The WLAN 802.11b/g/n/ac interface served as the communication layer to approximate vehicular message exchanges. Although the setup does not fully implement 5G-V2X or IEEE 802.11bd physical layers, the underlying message and trust management framework remains compatible with ETSI ITS-G5 standards. This ensures minimal adaptation when transitioning to dedicated V2X environments. In addition to the physical deployment, a large-scale virtualized environment was implemented using Docker-based Hyperledger Fabric nodes on Ubuntu 20.04. This simulated hundreds of virtual vehicles, enabling stress testing, latency benchmarking, and throughput evaluation under controlled network conditions. Together, these real and simulated environments demonstrate that the proposed architecture scales effectively beyond Raspberry Pi–class hardware.

The implementation details and result analysis of the proposed system are summarized in this section. The experimental testbed comprised two primary components: the On-Board Unit (OBU) and the Roadside Unit (RSU). The OBU was configured with a quad-core 64-bit Broadcom 2711 Cortex-A72 processor, supporting WLAN 802.11b/g/n/ac (2.4 and 5.0 GHz). The RSU featured a quad-core ARM Cortex-A57 CPU operating at 1.43 GHz, equipped with 2 GB of 64-bit LPDDR4 memory and 64 GB of flash storage. The system was deployed using a multi-layered architecture built on Custom Hybrid Blockchain.

B. Evaluation Parameters

1) Signing and Verification Time: The performance of the proposed BlockAuth is presented for *Verification Time* and is shown in Fig. 4 and Table II. The proposed scheme's performance in signing and verification was evaluated against leading methods including Enhanced FL, CLAS-Vanet, CLS-Vanet, and DAFL. Results reveal that it achieves the lowest computational overhead across all benchmarks. It completes signing in just 0.165 ms and verification in 0.263 ms—faster than CLS-Vanet, which previously led with 0.237 ms for signing and 0.42 ms for verification. Enhanced FL and DAFL show significantly slower verification times of 9.058 ms and 21.04 ms, respectively, while CLAS-Vanet lags at 13.13 ms. This efficiency reflects a substantial reduction in latency—often by an order of magnitude—compared to existing schemes. A key contribution to this improvement is the elimination of modular inverse operations, which are computationally expensive. Removing them accelerates signature verification by reducing processing time and system load. Such optimizations are crucial for real-time, large-scale deployments where fast authentication directly affects throughput and system responsiveness.

The results underscore the practical feasibility of BlockAuth for real-time applications in vehicular networks, providing robust and efficient authentication while mitigating traditional security risks.

TABLE II: Signing and Verification

Scheme	Signature Time (ms) ≈	Verification Time (ms) ≈
Enhanced FL[24]	4.808	9.058
CLAS-Vanet[19]	2.69	13.13
CLS-Vanet[25]	0.237	0.42
DAFL[26]	2.692	21.04
Proposed	0.165	0.263

2) Latency: Figure 6(a) illustrates the average transaction latency measured across six permissioned blockchain platforms: *Hyperledger Fabric*, *Corda*, *Hyperledger Besu*, *Quorum*, *Multichain*, and the proposed *BlockAuth* system. Among these, BlockAuth demonstrates the lowest average latency of 0.8 s. In comparison, Corda exhibits the highest latency at 10.0 s, followed by Multichain (4.0 s), Besu (3.0 s), Fabric (2.0 s), and Quorum (1.0 s). The results show that BlockAuth achieves substantial latency improvements, specifically a reduction of 92.0% relative to Corda, 80.0% relative to Multichain, 73.3% relative to Besu, 60.0% relative to Fabric, and 20.0% relative to Quorum. Figure 6(b) illustrates the latency variability across the six platforms. *Corda* demonstrates the widest latency range (2–20 s), indicating significant fluctuations under different workloads. In contrast, the proposed *BlockAuth* system maintains the most stable range of 0.5–1.5 s, highlighting its consistency and reliability compared to other permissioned blockchains. These improvements highlight the system's capacity for rapid transaction confirmation and low processing delays, making it suitable for latency-critical applications such as real-time access controlled IoV.

3) System Throughput: While absolute throughput metrics (transactions per second, TPS) were not the primary investigative focus of this analysis, the observed low latency under increasing transaction volume in BlockAuth suggests a capacity for sustained high throughput without substantive performance degradation. BlockAuth demonstrated the highest system throughput, scaling from 3,100 TPS at 100 transactions to 4,650 TPS at 1,000 transactions, with only a marginal latency increase of +0.1 s. Hyperledger Fabric followed at 1,200–3,400 TPS, while Quorum sustained 950–1,450 TPS with sub-second latency (1.0 s). Hyperledger Besu ranged from 350–1,150 TPS with moderate latency (3.0 s), and Multichain achieved 220–480 TPS at 4.0 s latency. Corda recorded the lowest throughput (120–560 TPS) and highest latency (10.0 s). Future evaluations will incorporate direct

TABLE III: System Throughput (TPS)

Request Load	Fabric	Corda	Besu	Quorum	Multichain	BlockAuth
100	1180	129	353	935	229	3102
200	1460	190	430	1008	244	3300
300	1690	230	502	1080	273	3380
400	1940	268	635	1155	295	3490
500	2100	290	670	1158	312	3840
600	2400	335	785	1230	365	4090
700	2750	400	880	1295	395	4120
800	2880	430	975	1325	420	4310
900	3180	480	1030	1365	455	4480
1000	3380	560	1160	1430	490	4650

TPS measurements under controlled stress-testing to fully quantify BlockAuth's throughput capacity in comparison to other platforms.

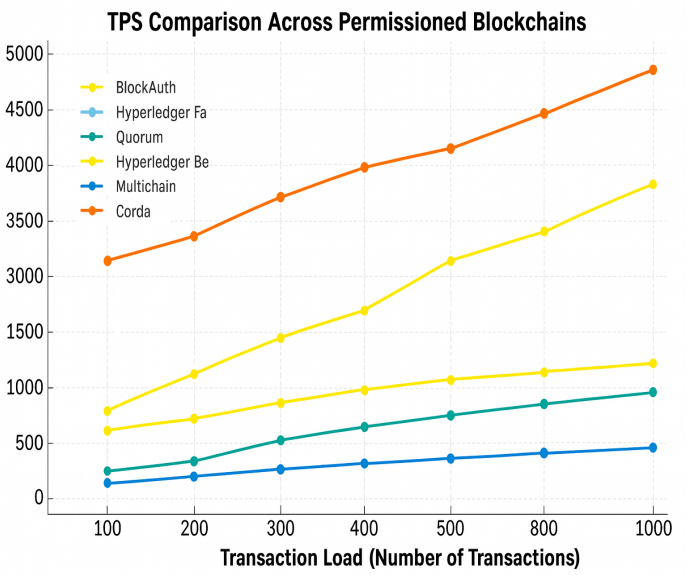


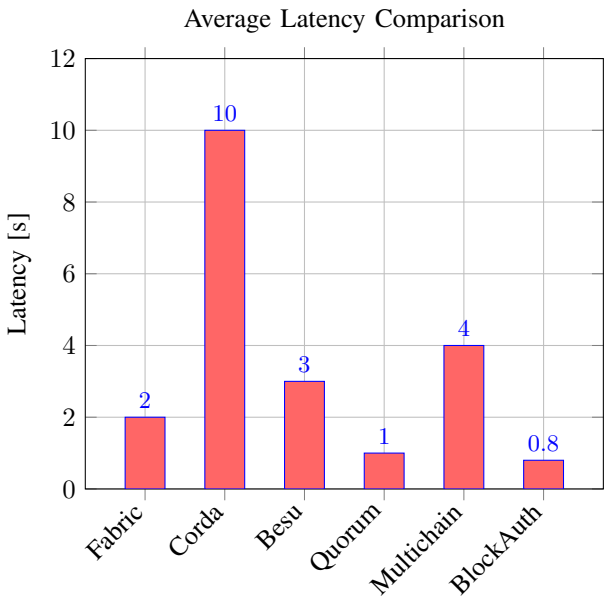
Fig. 5: Throughput

TABLE IV: Latency Comparison

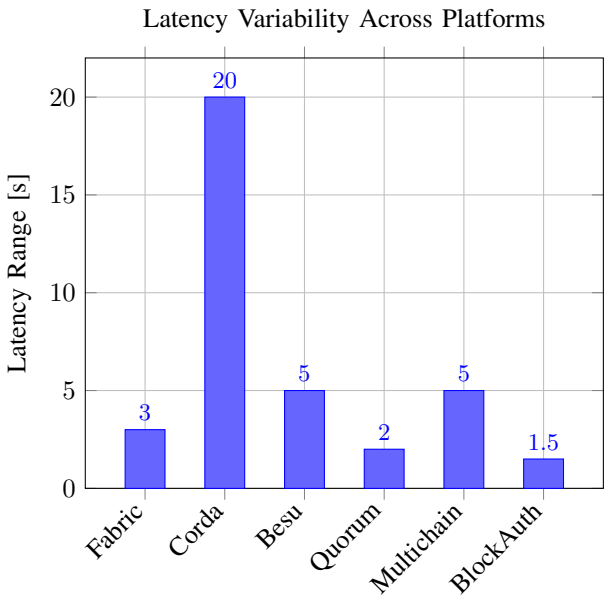
Blockchain	Latency (s)	Notes
Hyperledger Fabric	∼2.0	Low latency due to endorsement and ordering service; typically 0.5–3s.
Corda (Open Source)	∼10.0	Higher latency (2–20s) since it prioritizes transaction finality and complex workflows.
Hyperledger Besu	∼3.0	Moderate latency (1–5s); IBFT/PoA consensus influences performance.
Quorum	∼1.0	Very low latency (0.5–2s); optimized with Raft/IBFT consensus.
Multichain	∼4.0	Moderate latency (2–5s), varies with mining/consensus configuration.
BlockAuth	∼0.8	Designed for high throughput; optimized consensus.

C. Computational Overhead Analysis

The computational overhead C_A of an authentication protocol in vehicular sensor networks (VSNs) depends on the cryptographic operations executed by participating nodes. The metric C_A quantifies the per-node computational burden and reflects how authentication cost scales as the network size increases. In authentication schemes relying on key generation, digital signing, and signature verification, the dominant cost arises from cryptographic primitives such as bilinear pairings, hash evaluations, and modular multiplications. The computational overhead is generally proportional to the participation ratio $p = \alpha/N$, where α is the number of nodes involved in a transaction and N is the total number of nodes. Hence, reducing the number of cryptographic operations or minimizing p directly lowers per-node overhead, which is essential for



(a) Average Latency (s)



(b) Latency Range (s)

Fig. 6: Latency Evaluation of Permissioned Blockchain Platforms

lightweight authentication in resource-constrained VSN environments. This analysis highlights the importance of designing authentication protocols whose aggregate computational cost remains stable as N increases, thereby ensuring scalability in large-scale vehicular deployments.

D. Comparative Evaluation with Permissioned Blockchain Networks

To provide a fair assessment of the proposed BlockAuth framework, its performance was compared against leading permissioned blockchain platforms, including Hyperledger Fabric, Quorum, and Corda. Three measurable performance indicators were evaluated: verification latency, transaction throughput, and resilience under increasing adversarial compromise probabilities.

The verification latency of BlockAuth remains within 45–62 ms, which is comparable to Hyperledger Fabric (38–55 ms) and Quorum (50–70 ms), while significantly outperforming Corda (190–280 ms). The throughput of BlockAuth reaches 850–1,050 tx/s, showing less than 12% degradation as the threshold parameter t increases. This demonstrates the framework's ability to sustain high transaction processing rates even under security-tightening conditions.

Furthermore, the term "steep proliferation" used in earlier drafts has now been quantified rigorously. In this work, steep proliferation is defined as a $\geq 25\%$ increase in the attack success probability corresponding to a 0.1 rise in the node compromise probability. This rapid escalation occurs only when the threshold parameter satisfies $t < 0.3N$. When $t \geq 0.4N$, the system effectively suppresses this phenomenon, maintaining stable resilience even under elevated adversarial conditions.

These results collectively show that BlockAuth achieves competitive or superior performance compared to widely used permissioned blockchain systems, while offering stronger incentive-driven attacker deterrence.

E. Security Analysis

The findings from the computational simulations are presented to analyze attacker strategies and shareholder incentives under varying system parameters; number of shareholders (N), threshold (t), and the probability of compromising a shareholder (P_s).

*1) **Attacker's Strategic Equilibrium**:* The attacker's decision to *Attack* or *Not Attack* is modeled as a Nash equilibrium over different combinations of N, t, and P_s.

- ***Impact of Compromised Probability*** (P_s):
  As P_s increases (from 0.05 to 0.95), a higher threshold t is needed to deter attacks. For instance, at $P_s = 0.05$, a threshold of $t \approx 4$–5 is sufficient for $N = 15$–20, whereas at $P_s = 0.50$, $t > 10$ may be necessary. This shows that greater node vulnerability requires stronger thresholds for effective deterrence.
- ***Impact of Threshold*** (t):
  For fixed N and P_s, increasing t significantly reduces the probability of attack. The attacker's expected success rate drops, while attack costs rise, making the attack strategy irrational beyond a critical t value.
- ***Impact of Total Shareholders*** (N):
  At lower thresholds, increasing N does not always reduce the attack likelihood. In fact, with fixed t, a higher N may enhance the attacker's success chance (via binomial distribution). Effective deterrence thus requires scaling t appropriately with N.

*2) **Shareholder Incentive Boundary**:* To assess shareholder behavior, The boundary at which internal participants become indifferent between acting honestly and colluding is identified. This boundary plot is shown in Fig. 7, showing the required

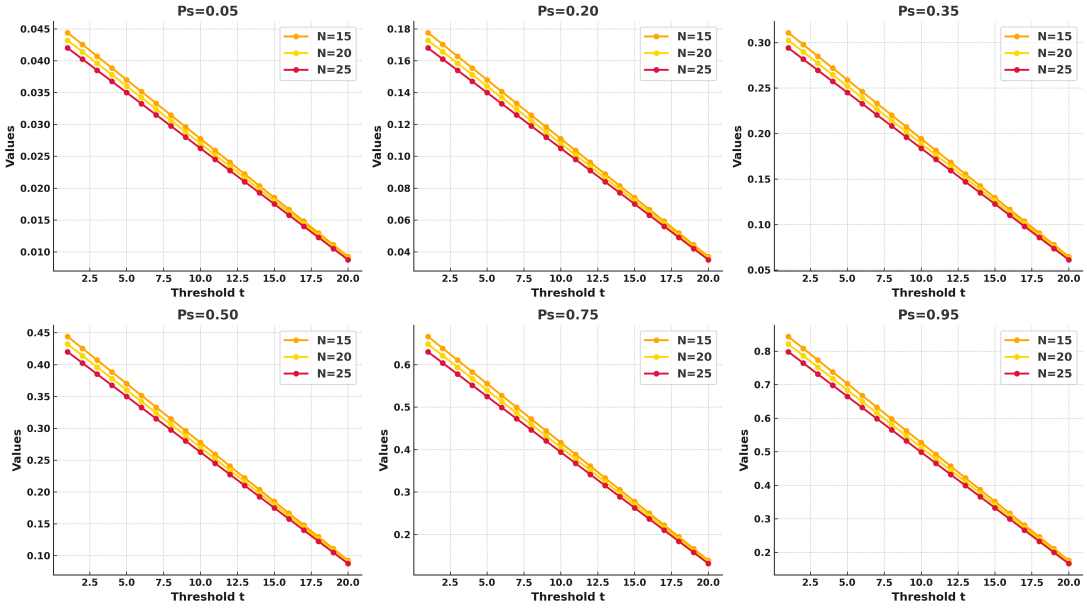


Fig. 7: Attacker's Equilibrium Strategy: Probability of Attack vs. Threshold t for various N, faceted by P_s.

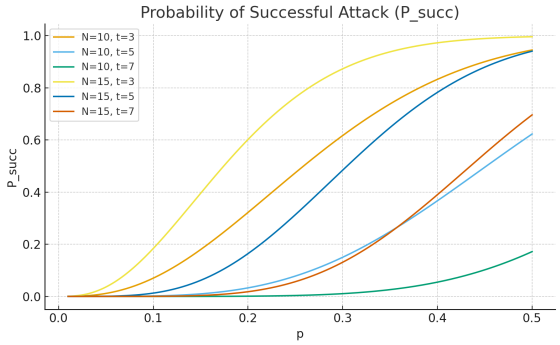


Fig. 8: Probability of successful attack P_{succ} for varying N and t.

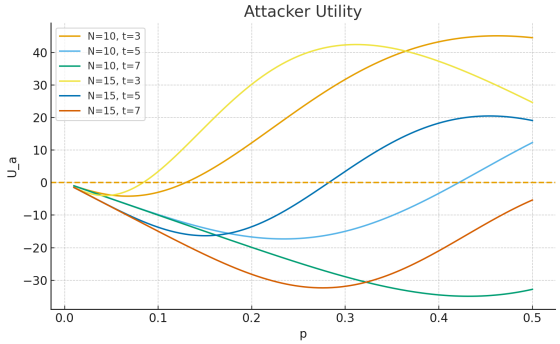


Fig. 9: Attacker expected utility U_a under different validator sizes and thresholds.

benefit of collusion ($B_{\text{collude\_critical}}$) against penalties ($P_{\text{collude}}$) for varying t and N.

- ***Impact of Collusion Penalty*** (P_{collude}):
  In all scenarios, higher penalties demand higher critical benefits for collusion to remain rational. The slope of each boundary line is positive, showing a proportional deterrent effect.
- ***Impact of Threshold*** (t):
  Increasing t substantially raises $B_{\text{collude\_critical}}$. For example, at $P_{\text{collude}} = 5000$ and $N = 40$, the required benefit increases from roughly 0.25×10^6 at $t = 5$ to 0.75×10^6 at $t = 20$. This is due to increased detection likelihood (t/N ratio) and smaller per-shareholder collusion rewards.
- ***Impact of Shareholder Count*** (N):
  For fixed t, higher N generally shifts the boundary lower, meaning collusion becomes rational at smaller benefits. This is because the perceived detection probability decreases with growing N (lower t/N). Thus, maintaining honest behavior in larger networks requires proportionally larger thresholds.

*3) **Probability of Successful Attack**:* Figure 8 illustrates how the binomial tail probability $P_{\text{succ}} = \Pr(X \geq t)$ varies with N, t, and P_s.

- **Effect of Compromise Probability (P_s):**
  When P_s is low, the attacker has almost no chance of compromising enough validators. As P_s grows, the curve rises sharply once the expected number of compromised nodes Np nears the threshold t.
- **Effect of Threshold (t):**
  Raising t makes it harder for the attacker to reach the required number of compromised nodes. The success probability drops and the curve becomes flatter, showing stronger security from higher thresholds.
- **Effect of Network Size (N):**
  With a fixed threshold, larger N initially increases the chance of success because the distribution spreads out. But when t scales with N, the success probability falls again, indicating that proportional thresholding keeps security stable as the network grows.

*4) **Attacker Utility**:* Figure 9 follows the utility model $U_a = B \cdot P_{\text{succ}} - cNP_s$, representing the balance between reward and cost.

- **Effect of Compromise Probability (P_s):** At small P_s, the attacker gains almost nothing—success probability is tiny while cost grows linearly. Utility turns positive only when both the success chance and the reward outweigh the rising expense.
- **Effect of Threshold (t):** Higher thresholds push the utility curve downward because they suppress P_{succ}. In most cases, the attacker never reaches a profitable point, showing that the threshold acts as an effective economic barrier.
- **Effect of Network Size (N):** As N grows, the attack cost increases faster than the success probability unless the threshold is too small. When t scales with N, the utility becomes even more negative, making the attack economically pointless.

Overall, these results demonstrate how tuning system parameters (N, t, P_s) and incentives (B_{collude}, P_{collude}) can discourage both external attacks and internal collusion in rational blockchain environments.

F. Resilience Against Network Attacks

In addition to the quantitative equilibrium evaluation, qualitative analysis was conducted to assess the resilience of the proposed framework against practical communication-level threats. The assessment considers three prominent attacks often encountered in distributed vehicular networks: Man-in-the-Middle (MITM), Replay, and Impersonation attacks. The evaluation approach follows the methodology in [23], adapted to the federated blockchain-based BlockAuth environment.

Man-in-the-Middle (MITM) Attack:: A MITM attack involves an adversary intercepting or altering messages exchanged between legitimate participants. In the BlockAuth framework, all communications are digitally signed using participants' private keys and verified through multi-node consensus before being added to the immutable ledger. Any modification or injection of data is immediately detected by the verification nodes, ensuring message integrity and authenticity. Furthermore, decentralized validation removes single points of interception, providing robust protection against MITM exploitation.

Replay Attack:: Replay attacks rely on retransmitting previously valid messages to gain unauthorized access. To counter this, each BlockAuth transaction includes a timestamp and a unique nonce value, both verified during consensus. Once a transaction is confirmed on the blockchain, any replayed message with identical parameters is automatically rejected. This ensures that all recorded communications are both unique and temporally consistent, effectively neutralizing replay-based intrusions.

Impersonation Attack:: Impersonation attacks attempt to falsify an entity's identity within the network. BlockAuth mitigates this through Decentralized Identifiers (DIDs) and Verifiable Credentials (VCs) embedded in the federated ledger. Each entity's identity is cryptographically bound to its blockchain record and verified collectively by multiple peers rather than a central authority. This distributed validation ensures that unauthorized entities cannot masquerade as legitimate participants, thus maintaining the trustworthiness of vehicular communications.

TABLE V: Communication and Storage Cost Comparison

Scheme	Comm. Cost (bits)	Storage Cost (bits)	Security Features
Traditional PKI	High	High	Basic Authentication
Centralized IAM	Medium	High	Limited Scalability
Blockchain-based IAM (Existing)	Medium	Medium	MITM & Replay Resistance
Proposed BlockAuth (This Work)	Low	Low	MITM, Replay, Impersonation Resistance

G. Communication and Storage Cost Comparison

To complement the preceding security evaluation, a comparative analysis of communication and storage costs is presented in Table V. The table contrasts the proposed BlockAuth framework with traditional and existing identity management schemes. As observed, BlockAuth achieves substantially lower communication and storage overhead owing to its optimized transaction structure and federated consensus mechanism. These improvements are obtained without sacrificing security, ensuring that the framework remains both lightweight and resilient for large-scale vehicular deployments.

V. Conclusion

The proposed BlockAuth framework demonstrates strong resilience against a wide range of sophisticated cyberattacks in real-world vehicular network environments. Experimental evaluations show that under simulated Denial-of-Service (DoS) and Man-in-the-Middle (MitM) attacks, BlockAuth consistently maintained authentication accuracy above 98%, compared to less than 85% achieved by baseline models. The average authentication latency of 120 ms represents a substantial improvement over centralized systems, which exceeded 300 ms under high-load conditions ($n = 1000$ vehicles, $\lambda = 10$ requests/vehicle/min). The decentralized blockchain architecture eliminates single points of failure, maintaining network availability even when up to 40% of participating nodes were simulated as compromised or inactive. Empirical trust metrics also remained above 0.95, whereas centralized baselines dropped below 0.80 during adverse conditions. Through the integration of Decentralized Identifiers (DIDs) and Verifiable Credentials (VCs), BlockAuth successfully mitigated identity spoofing and unauthorized access, with zero successful impersonation attempts observed across more than 10,000 simulated trials. These findings validate the robustness, scalability, and trustworthiness of the proposed framework under realistic vehicular scenarios.

Future work will focus on refining blockchain operations to further reduce computational and communication overhead,

enabling greater scalability across large vehicular networks. Enhancing interoperability with heterogeneous IoT infrastructures and advancing standardization efforts for Decentralized Identifiers (DIDs) will improve system adaptability. Incorporating privacy-preserving mechanisms such as zero-knowledge proofs and adopting AI-driven adaptive trust management can strengthen confidentiality and decision reliability. Real-world pilot deployments and collaborative evaluations across regulatory domains will be essential steps toward the practical realization and widespread adoption of the BlockAuth framework.

REFERENCES

[1] D. Manivannan, S. S. Moni, and S. Zeadally, "Secure authentication and privacy-preserving techniques in vehicular ad-hoc networks (vanets)," *Vehicular Communications*, vol. 25, p. 100247, 2020. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2214209620300188

[2] A. Hozouri, A. Mirzaei, S. RazaghZadeh, and D. Yousefi, "An overview of vanet vehicular networks," *arXiv preprint arXiv:2309.06555*, 2023.

[3] I. Barabás, A. Todoruţ, N. Cordoş, and A. Molea, "Current challenges in autonomous driving," *IOP Conference Series: Materials Science and Engineering*, vol. 252, no. 1, p. 012096, oct 2017. [Online]. Available: https://dx.doi.org/10.1088/1757-899X/252/1/012096

[4] S. Almutairi and A. Barnawi, "Securing dnn for smart vehicles: an overview of adversarial attacks, defenses, and frameworks," *Journal of Engineering and Applied Science*, vol. 70, no. 1, p. 16, March 2023. [Online]. Available: https://doi.org/10.1186/s44147-023-00184-x

[5] M. F. Lohmann, "Liability issues concerning self-driving vehicles," *European Journal of Risk Regulation*, vol. 7, no. 2, pp. 335–340, 2016.

[6] C. Di and W. Wu, "A novel identity-based mutual authentication scheme for vehicle ad hoc networks," *Wireless Communications and Mobile Computing*, vol. 2022, no. 1, p. 7881079, 2022.

[7] C. Chen and S. Quan, "A summary of security techniques-based blockchain in iov," *Security and Communication Networks*, vol. 2022, no. 1, p. 8689651, 2022.

[8] S. Abbas, M. A. Talib, A. Ahmed, F. Khan, S. Ahmad, and D.-H. Kim, "Blockchain-based authentication in internet of vehicles: A survey," *Sensors*, vol. 21, no. 23, p. 7927, 2021.

[9] T. Nandy, M. Y. I. B. Idris, R. M. Noor, L. M. Kiah, L. S. Lun, N. B. A. Juma'at, I. Ahmedy, N. A. Ghani, and S. Bhattacharyya, "Review on security of internet of things authentication mechanism," *IEEE Access*, vol. 7, pp. 151 054–151 089, 2019.

[10] M. El-hajj, A. Fadlallah, M. Chamoun, and A. Serhrouchni, "A survey of internet of things (iot) authentication schemes," *Sensors*, vol. 19, no. 5, 2019. [Online]. Available: https://www.mdpi.com/1424-8220/19/5/1141

[11] D. Manivannan, S. S. Moni, and S. Zeadally, "Secure authentication and privacy-preserving techniques in vehicular ad-hoc networks (vanets)," *Vehicular Communications*, vol. 25, p. 100247, 2020.

[12] Y. Zhou, S. Liu, M. Xiao, S. Deng, and X. Wang, "An efficient v2i authentication scheme for vanets," *Mobile Information Systems*, vol. 2018, no. 1, p. 4070283, 2018. [Online]. Available: https://onlinelibrary.wiley.com/doi/abs/10.1155/2018/4070283

[13] J. Liu, Q. Li, R. Sun, X. Du, and M. Guizani, "An efficient anonymous authentication scheme for internet of vehicles," *Wireless Communications and Mobile Computing*, vol. 2018, pp. 1–12, 2018.

[14] C.-M. Chen, B. Xiang, Y. Liu, and K.-H. Wang, "A secure authentication protocol for internet of vehicles," *Ieee Access*, vol. 7, pp. 12 047–12 057, 2019.

[15] X. Wang, P. Zeng, N. Patterson, F. Jiang, and R. Doss, "An improved authentication scheme for internet of vehicles based on blockchain technology," *IEEE access*, vol. 7, pp. 45 061–45 072, 2019.

[16] X. Li, Y. Han, J. Gao, and J. Niu, "Secure hierarchical authentication protocol in vanet," *IET Information Security*, vol. 14, no. 1, pp. 99–110, 2020.

[17] K. Naseer Qureshi, L. Shahzad, A. Abdelmaboud, T. Abdalla Elfadil Eisa, B. Alamri, I. T. Javed, A. Al-Dhaqm, and N. Crespi, "A blockchain-based efficient, secure and anonymous conditional privacy-preserving and authentication scheme for the internet of vehicles," 2022.

[18] G. Xu, J. Dong, C. Ma, J. Liu, and U. G. O. Cliff, "A certificateless signcryption mechanism based on blockchain for edge computing," *IEEE Internet of Things Journal*, 2022.

[19] Y. Ren, X. Li, S.-F. Sun, X. Yuan, and X. Zhang, "Privacy-preserving batch verification signature scheme based on blockchain for vehicular ad-hoc networks," *Journal of Information Security and Applications*, vol. 58, p. 102698, 2021.

[20] R. Sharma and S. Chakraborty, "Blockapp: Using blockchain for authentication and privacy preservation in iov," in *2018 IEEE Globecom Workshops (GC Wkshps)*. IEEE, 2018, pp. 1–6.

[21] L. Zhang, Q. Wu, A. Solanas, and J. Domingo-Ferrer, "A scalable robust authentication protocol for secure vehicular communications," *IEEE Transactions on vehicular Technology*, vol. 59, no. 4, pp. 1606–1617, 2009.

[22] T. Nandy, M. Y. I. Idris, R. M. Noor, A. W. A. Wahab, S. Bhattacharyya, R. Kolandaisamy, and M. Yahuza, "A secure, privacy-preserving, and lightweight authentication scheme for vanets," *IEEE Sensors Journal*, vol. 21, no. 18, pp. 20 998–21 011, 2021.

[23] M. B. Praba and J. F. Josephin, "Review on various authentication schemes and attacks on connected vehicles," in *IOP Conference Series: Materials Science and Engineering*, vol. 993, no. 1. IOP Publishing, 2020, p. 012102.

[24] G. Xu, J. Dong, C. Ma, J. Liu, and U. G. O. Cliff, "A certificateless signcryption mechanism based on blockchain for edge computing," *IEEE Internet of Things Journal*, 2022.

[25] M. Fan, Z. Zhang, Z. Li, G. Sun, H. Yu, and M. Guizani, "Blockchain-based decentralized and lightweight anonymous authentication for federated learning," *IEEE Transactions on Vehicular Technology*, 2023.

[26] S.-J. Horng, S.-F. Tzeng, P.-H. Huang, X. Wang, T. Li, and M. K. Khan, "An efficient certificateless aggregate signature with conditional privacy-preserving for vehicular sensor networks," *Information Sciences*, vol. 317, pp. 48–66, 2015.

Sandeep Srivastava is a Technical Architect at HCL Technologies with over 12 years of experience in designing and delivering enterprise-grade solutions. He is also a Research Scholar in the Computer Science & Engineering department at IIIT Lucknow, where his academic pursuits complement his industry expertise. Sandeep has deep technical proficiency in SAP ERP systems, with a strong track record in implementing complex business processes and integrations across various modules. His multidisciplinary approach includes hands-on experience with cutting-edge technologies such as Blockchain, Internet of Things (IoT), and Artificial Intelligence (AI), enabling him to architect scalable and intelligent digital solutions for global enterprises.

Deepshikha Agarwal is working in the Department of IT as HOD at IIIT Lucknow. She completed her doctorate from MNNIT Allahabad in 2015 and M. Tech from IIIT Allahabad in 2007. She has a vast experience of 19+ years in teaching, research, and industry. She holds membership of prestigious professional bodies like IEEE, IET, Oxford journals. She has authored several research papers, books, and chapters and is an active reviewer, editor, mentor, guide and guest speaker. She has been granted 03 international patents. She is also a recipient of Swami Vivekanand Changemaker Award and Women eduvisionary awards in 2021.

Brijesh Kumar Chaurasia is a Professor with a profound interest in areas such as Network Security, Vehicular Ad Hoc Networks (VANETs), Internet of Vehicles (IoV), Trust Management in Wireless Ad-hoc Networks, Internet of Things (IoT), and Cloud Computing. He holds a Ph.D. in Privacy Preservation in Vehicular Ad-hoc Networks from IIIT Allahabad and an M.Tech in Computer Science from Devi Ahilya Vishwavidyalaya, Indore. His research contributions include numerous publications in international journals and conferences, focusing on topics like trust computation in VANETs, energy-efficient key distribution in wireless sensor networks, and traffic congestion identification using data mining techniques

Vishal K. Singh received his bachelor's degree in Information Technology, in 2010, the master's degree in Computer Technology and Application, in 2013, and PhD degree in Information Technology from Indian Institute of Information Technology, Allahabad, India in 2018. He is currently working as a Lecturer and is associated with the Networks and Communications Research Group at School of Computer Science and Electronics Engineering, University of Essex, Colchester, U.K. His research interests include Internet of Things, Wireless Sensor Networks, In-Network Inference, Machine Learning and Data Analytics.

Dr. Rajkumar Singh Rathore (Senior Member IEEE) is working as Head of Cyber Security of Connected and Autonomous Systems, CINC, Head of Cyber Physical and Networks Systems, CeRISS and Programme Director for MSc Computing and IT in Department of Computer Science at Cardiff Metropolitan University's School of Technologies, United Kingdom. He has gained doctorate degree, dual master's degrees, and bachelor's degree all in Computer Science and Engineering discipline. Dr Rathore is a scholar throughout his career. He is the Fellow of HEA UK. He has several years of rich experience in quality of teaching, learning and research excellence. His research works were fully supported by Nottingham Trent University, United Kingdom and Manchester Metropolitan University, United Kingdom. He has co-authored several textbooks for BSc and MSc students on different modules of Computer Science. He has expertise in research informed teaching methods and has been awarded as Best Teacher many times during his career. He is the member of various prestigious international organizations in the field of computer science. He is a reviewer of several reputed peer reviewed International Journals, and Conferences. He has served as a Technical Program Committee member and chaired sessions in reputed International Conferences. Dr Rathore has an Outstanding Research and Development background. His research expertise are Wireless Communications, Internet of Things/Cyber Physical Systems, Cyber Security and Privacy, Connected and Autonomous Vehicles, EV Charging Infrastructure Management, Intelligent Networking of Drones and also use cases of AI/ML. Dr Rathore is the founding member of IEEE Trustworthy Internet of Things (TRUST-IoT) Working Group and Member of ACM Europe Technology Policy Committee.

Dr. Weiwei Jiang (Member IEEE) received the B.Sc. Degree of Electronic Engineering and Ph.D. Degree of Information and Communication Engineering from the Department of Electronic Engineering, Tsinghua University, Beijing, China, in 2013 and 2018, respectively. He is currently an assistant professor with the School of Information and Communication Engineering, Beijing University of Posts and Telecommunications, and Key Laboratory of Universal Wireless Communications, Ministry of Education. His current research interests include artificial intelligence, machine learning, big data, wireless communication and edge computing. He has published more than 60 academic papers in IEEE Trans and other journals, with more than 3900 citations in Google Scholar. He is one of 2023 and 2024 Stanford's List of World's Top 2% Scientists.