Contents lists available at Science-Gate

International Journal of Advanced and Applied Sciences

Journal homepage: https://www.science-gate.com/IJAAS.html

Blockchain-based certificateless authentication with a privacy-preserving scheme in 5G-based vehicular fog computing

Zeyad Ghaleb Al-Mekhlafi [1,*], Aleiah Jarallah Alrashdan [1], Kawther A. Al-Dhlan [2], Hamad A. Al-Reshidi [3]

[1]*Department of Information and Computer Science, College of Computer Science and Engineering, University of Hail, Hail 81481, Hail, Saudi Arabia*
[2]*Department of Artificial Intelligence and Data Science, College of Computer Science and Engineering, University of Hail, Hail 81481, Saudi Arabia*
[3]*Department of Instructional Technology, College of Education, University of Hail, Hail, Saudi Arabia*

ARTICLE INFO

Article history:
Received 5 December 2025
Received in revised form
29 March 2026
Accepted 11 June 2026

Keywords:
Vehicular fog computing
Certificateless authentication
Permissioned blockchain
Vehicular security
Smart transportation systems

ABSTRACT

This study proposes a novel approach that integrates a permissioned blockchain with a certificateless authentication scheme. The proposed model enables secure, decentralized, and efficient authentication among vehicles, fog nodes, and Roadside Units (RSUs), while eliminating the need for centralized certificate authorities. Certificateless cryptography enhances user privacy and reduces computational burden, whereas blockchain technology ensures transparency and immutability by securely recording authentication events. The performance of the proposed system is evaluated through comprehensive simulations implemented in Python within a realistic 5G-enabled VFC environment. Key performance metrics, including authentication success rate, resistance to replay attacks, and blockchain scalability, are analyzed. The results demonstrate a high authentication success rate of up to 90.7%, efficient blockchain growth, and sustained system performance even in the absence of RSUs. These findings confirm the scalability, robustness, and practical applicability of the proposed scheme. Overall, this study presents a secure, privacy-preserving, and infrastructure-independent authentication framework suitable for deployment in smart cities and autonomous vehicular networks.

© 2026 The Authors. Published by IASE. This is an open access article under the CC BY-NC-ND license (https://creativecommons.org/licenses/by-nc-nd/4.0/).

1. Introduction

Rapid changes in vehicular networks and their applications involving cloud computing and fog computing immediately raise concerns about the need for complete and responsible security. Since such networks mesh with 5G, which has generally increased data synchronization and communicative capabilities among traveling vehicles, security and privacy have been highlighted as some of the high-priority challenges (Almazroi et al., 2023a).

This scaling up of modern networks that form the global open web demands effective measures to ensure data integrity and user privacy protection, given the rapid growth triggered by advances in communication technologies and specific systems. The new frequency of 5G has equipped vehicular networks with faster communication and more robust electronic systems, increasing their functionality. Real-time applications, especially V2X communications, play a very important role in developing higher levels of security in vehicular networks (Meng et al., 2020). The increased dependency on wireless communication has also brought significant security and privacy vulnerabilities (Biswash and Jayakody, 2020).

This raises the bar for protecting sensitive information and secure communication. Through the advancement in vehicular networks, fog computing has emerged as a promising strategy to handle the massive data generated. Unlike traditional cloud computing, fog computing provides a less time-consuming means whereby data processing can be allowed closer to its source.

Nearness reduces delay, implying overall efficiency in the system. However, with even fog computing in place, vehicular networks remain vulnerable to various kinds of cyber threats, for example, man-in-the-middle attacks, data tampering, breach of user privacy, etc. In this context, blockchain technology has developed a new solution

* Corresponding Author.
Email Address: z.almekhlafi@uoh.edu.sa (Z. G. Al-Mekhlafi)
https://doi.org/10.21833/ijaas.2026.06.011
Corresponding author's ORCID profile:
https://orcid.org/0000-0001-6367-0309
2313-626X/© 2026 The Authors. Published by IASE.
This is an open access article under the CC BY-NC-ND license (https://creativecommons.org/licenses/by-nc-nd/4.0/)

that offers decentralized systems characterized by transparency and resistance to cyberattacks; thus, it eliminates conventional digital certificates. Its inherent properties make blockchain suitable for tackling vehicular network security challenges (Fernando et al., 2025).

That makes integrating blockchain technology with a certificate authentication model an appealing move to ensure the security of communications across those networks. This model meets the difficulties of traditional certificate-management systems and can provide practical, robust privacy protection with reduced computational cost. Certificateless authentication lessens all burdens linked to PKI, typically used in vehicular communications.

Therefore, it offers a lightweight but efficient communication security approach. It ensures strong security guarantees without the intricacies of digital certificate management typical of more traditional frameworks (Gong et al., 2023). Blockchain technology and certificate authentication establish a robust security framework in vehicular networks. This framework will enforce the networks to protect privacy, reduce costs, decrease administrative loads, and enhance operational security and efficiency.

Especially in vehicular networks, sensitive information, such as vehicle location and user identity, can be obtained by malicious users. Blockchain technology and certificate authentication secure user identities, thus enabling safe and verifiable communications between vehicles with ensured anonymity.

- Detailed protocol description: Step-by-step authentication and transaction flows with clear notation for cryptographic operations.
- Protocol diagrams: Sequence diagrams illustrating interactions among entities (e.g., users, devices, blockchain nodes).
- Algorithm pseudocode: For key generation, encryption/signing, verification, and smart contract execution.
- Parameter and implementation details: Security parameters, curve/lattice choices, hash functions, gas costs, and block intervals.
- Threat model and assumptions: Explicit attacker capabilities and trust assumptions.
- Security proofs or sketches: Formal or semi-formal proofs tied to standard models.
- Blockchain specifics: Consensus mechanism, on-/off-chain data split, smart contract logic, and upgrade/revocation handling.
- Performance breakdown: Per-operation latency, computation, communication, and storage overhead.
- Reproducibility artifacts: Implementation details, datasets, code repository, or configuration settings.

The novelty of this work relies on the capability for a new authentication scheme to be developed based on blockchain and fog computing to respond to current security needs in vehicular networks. A certificate-free authentication scheme for networks supported by fifth-generation technology is proposed, leveraging fog computing capabilities only. The study aims to improve the existing weaknesses of these traditional systems and the protection of privacy and energy efficiency to make the environment of data exchanges in these networks more secure and user-friendly, to improve the total user experience.

2. Related works

A thorough analysis of the body of research on blockchain technology, certificateless cryptography, authentication in vehicular networks, and privacy-preserving strategies in 5G-enabled fog computing settings. By pointing out current research trends, stressing the shortcomings of traditional authentication methods, and highlighting the need for more effective and secure solutions, it lays the theoretical groundwork for the investigation.

The proposed scheme is designed to provide strong privacy guarantees by preserving user anonymity and preventing identity linking attacks, even in the presence of powerful adversaries. Specifically, the real identity of each vehicle is never exposed during communication or transaction generation. Instead, vehicles operate using short-term pseudonymous identifiers derived from cryptographic credentials, ensuring that transmitted messages cannot be directly associated with long-term identities.

Anonymity is preserved through the separation of identity management and message authentication. While authentication guarantees message legitimacy, it does not reveal the sender's true identity. This design prevents adversaries from learning sensitive identity information by eavesdropping on network communications or analyzing blockchain records. Moreover, cryptographic protections ensure that any identifiers included in transactions are computationally infeasible to reverse or map to real-world identities.

To resist identity linking attacks, the proposed scheme employs frequently refreshed pseudonyms and session-specific cryptographic randomness. As a result, messages generated by the same vehicle across different sessions appear unlinkable to external observers. Even if an adversary gains access to multiple transactions or communication traces, the lack of reusable identifiers and the incorporation of randomness prevent correlation attacks based on timing, message structure, or cryptographic material.

Furthermore, the immutable nature of the blockchain does not compromise privacy, as only privacy-preserving metadata is stored on-chain. Sensitive information is either encrypted or maintained off-chain, ensuring that long-term analysis of blockchain data does not enable retrospective identity disclosure. Consequently, the scheme achieves a balance between accountability and privacy by allowing authorized entities to

perform conditional traceability when required, without sacrificing anonymity under normal operation.

Overall, the proposed scheme provides strong anonymity and unlinkability guarantees, effectively protecting users against identity inference and linking attacks while maintaining secure and authenticated communication.

The paper also examines the advantages and disadvantages of several methods put forth in earlier research. By highlighting the research gap that the proposed scheme seeks to fill, this review ultimately aids in its justification. 5G communications, protected by blockchain-based certificate authentication, are necessary for 5G vehicular fog computing (Ahmed et al., 2022; Chattaraj et al., 2021; Al-Mekhlafi and Alfhaid, 2025).

Blockchain integration into automotive networks reduces overhead, gets rid of single points of failure, and does away with the need for conventional certificate authorities (Chattaraj et al., 2021). Strong authentication methods must be developed because real-time data processing in vehicular fog computing is entirely supported by edge computing resources (El-Zawawy et al., 2023).

Due to the increasing number of potential cyberthreats in vehicular networks, every precaution must be taken to keep trucks inside the protected area in order to prevent attacks, data breaches, and unauthorized access (Gazdar et al., 2022). This study will demonstrate how, in 5G-enabled fog computing environments, blockchain and certificate authentication can improve vehicle security (Khalifa et al., 2022).

2.1. Secure authentication methods in vehicular networks with blockchain

Vehicle networks rely on cryptographic techniques for authentication in order to guarantee data integrity and prevent unauthorized parties from accessing it (Almazroi et al., 2023b). Public key infrastructure (PKI)-based authentication is used in many of these solutions; while it works, adding certificate authorities raises concerns about scalability (Rezazadeh Baee et al., 2021). This reliance is removed by certificateless authentication, which lowers computational and communication overhead.

The alternative method, identity-based authentication, simplifies key management but introduces privacy concerns by using authentication credentials linked to the user's identity (Xie and Huang, 2024). By enhancing authentication security, blockchain supports the decentralized trust model (Singh et al., 2023). Blockchain consensus processes make authentication records unchangeable, making them impervious to malevolent manipulation (Banerjee et al., 2021). However, previous research has proposed using blockchain-based schemes to improve system resilience and reduce attack vectors and decentralized identity (Li et al., 2020).

2.2. Security and privacy enhancements in vehicular communication

Strong measures should be used to stop data from unauthorized access in order to preserve data security and privacy in vehicular communications while maintaining high efficiency (Bala et al., 2023). Blockchain can perform real-time authentication without relying on centralized servers, reducing latency and boosting scalability with the aid of edge computing (Ma et al., 2024).

Cryptographic methods such as ring signatures, homomorphic encryption, and zero-knowledge proofs are used to supplement privacy in authentication while maintaining privacy (Hussain et al., 2024). Second, cars use anonymous identity authentication in privacy-preserving authentication methods (Abdel Hakeem and Kim, 2023).

Ring signatures render transactions unlikable for a particular vehicle, and zero-knowledge proofs allow one to confirm that transactions do not disclose private information. Through verifiable and tamper-resistant logs, data integrity and confidentiality are resolved using the blockchain's immutability and transparency (Ahmed et al., 2022; Khalil et al., 2022).

2.3. Evaluation metrics for authentication frameworks

Latency, computational cost, security robustness, and scalability are performance metrics used to assess authentication frameworks (Ma et al., 2024). According to Al-Khatib et al. (2024), the biggest factor affecting real-time vehicular applications is latency. Based on an analysis of the computational cost, the possibility is based on the authentication mechanism's potential for resource-constrained environments (Shewajo et al., 2024; Al-Mekhlafi et al., 2016).

Security robustness, or the framework's ability to withstand attacks, is the second metric; scalability, or the framework's capacity for large-scale implementation, is the final metric (Haddad et al., 2020; Al-Mekhlafi et al., 2017). The effectiveness of various authentication models in real-world automotive settings is benchmarked (Liu et al., 2022). However, compared to conventional PKI-based techniques, blockchain-based frameworks have higher security and lower latency (Azam et al., 2021; Al-Mekhlafi et al., 2018). The scalability tests show that the blockchain can operate in high-traffic, low-computer-overhead automotive environments.

2.4. Authentication challenges and the role of blockchain in 5G-enabled vehicular fog computing

According to the literature review, 5G-enabled fog computing necessitates the security of vehicular networks, necessitating blockchain-based certificate authentication (Al-Janabi et al., 2024). The security

and effectiveness of the authentication methods—PKI-based, certificate-based, and identity-based vary (Indushree et al., 2023).

Blockchain provides immutability, decentralization, trust assurance, and a reduction in reliance on third parties for authentication (Lv and Liu, 2022). Anonymous authentication using signatures adds another layer of security (Khaliq et al., 2022). Latency, computational cost, security robustness, and scalability are assessment metrics that gauge the authentication frameworks' effectiveness (El-Zawawy et al., 2023). Despite the encouraging outcomes of blockchain-based authentication, more investigation is still required to determine its scalability and computational efficiency for widespread vehicle deployment (Kaltakis et al., 2021).

2.5. Comparison with related work

Table 1 presents a comparative evaluation between the proposed scheme and representative PKI-based, identity-based, and blockchain-assisted approaches. Unlike PKI-based solutions, which suffer from high certificate management overhead and verification latency, the proposed scheme achieves lower authentication latency and reduced communication overhead. Compared to identity-based schemes, the proposed approach provides stronger privacy guarantees, including full anonymity and resistance to identity linking attacks. Moreover, the proposed scheme supports conditional traceability while maintaining scalability, making it well-suited for large-scale and dynamic vehicular environments.

Table 1: Comparison with existing schemes

Scheme type	Authentication latency	Communication overhead	Computation overhead	Anonymity	Unlinkability	Traceability	Scalability
PKI-based	High	High (certificates)	High (cert. verify)	✗	✗	✓	Medium
Identity-based	Medium	Medium	Medium	Limited	Limited	✓	Medium
Blockchain-based	High	High	High	✓	✓	✗ / Limited	Low
Proposed scheme	Low	Low	Low	✓	✓	✓	High

3. Methodology

In order to develop, deploy, and assess a blockchain-based certificateless authentication system specifically suited for 5G-enabled Vehicular Fog Computing (VFC) environments, this study uses an organized methodology. The methodology is intended to tackle the main issues of performance, security, and privacy in dynamic vehicular networks. Modelling the VFC environment, including cars, fog nodes, Roadside Units (RSUs), and 5G base stations, is the first step in defining the system architecture.

- Protocol pseudocode: Provide clear step-by-step pseudocode for key phases, such as system initialization, authentication (V2V/V2I), key agreement, and revocation.
- Message sequence diagrams: Include a detailed protocol diagram showing interactions among vehicles, RSUs, and blockchain nodes, with message contents and cryptographic operations annotated.
- Blockchain interaction flow: Explicitly illustrate when and how transactions are generated, validated, and recorded on-chain, and what data are stored on-chain vs. off-chain.
- Algorithm boxes: Present core algorithms (e.g., authentication, key update, verification) in standard algorithmic format to improve readability.
- Notation table: Add a table summarizing symbols, cryptographic primitives, and parameters used in the protocol.
- Execution timing: Optionally annotate diagrams with latency or computational costs to link methodology with performance results.

These entities establish communication protocols that address vehicle-to-vehicle (V2F), vehicle-to-infrastructure (V2I), and vehicle-to-vehicle (V2V) interactions. The system incorporates blockchain technology to offer a safe and impenetrable ledger for keeping authentication records. With specific roles for nodes like RSUs and fog nodes, which validate transactions and run smart contracts to automate authentication procedures and privacy controls, a permission blockchain model is used.

By using certificateless cryptography, the certificateless authentication scheme does away with the necessity for conventional Public Key Infrastructure (PKI). Using a dual-key strategy, each vehicle generates its own public-private key pair while a trusted authority issues partial private keys. Secure session key exchange and mutual authentication between cars and RSUs without certificates are made possible by this design.

Mechanisms like pseudonym-based identities and recurring updates to avoid long-term linkability are included in the scheme to protect privacy. Additionally, data minimization techniques are used to make sure that only necessary information is revealed during authentication and that only authorized nodes can access it. The suggested system is subjected to a thorough security analysis, which includes threat modelling to assess its defenses against prevalent attacks like replay, impersonation, and man-in-the-middle attacks.

The immutability and auditability of blockchain technology are used to strengthen the system's credibility. To assess the authentication protocol's performance under actual driving circumstances, such as fluctuating vehicle densities and mobility patterns, a simulation environment is developed. To

demonstrate the benefits of the suggested method, key performance metrics like latency, bandwidth consumption, and computational overhead are measured and contrasted with conventional PKI-based systems.

Lastly, every discovery—including security analysis and performance results—is recorded. Enhancing cryptographic efficiency and optimizing blockchain integration are two examples of possible areas for improvement. Future developments are suggested to increase VFC systems' scalability and privacy.

4. Results and discussion

In this study, the performance analysis and evaluation of the suggested certificateless authentication system in a 5G-enabled vehicular fog computing environment are presented. The assessment seeks to gauge the system's efficacy in terms of RSU activity, blockchain growth, authentication success rate, and general responsive security (Al-Mekhlafi et al., 2019).

- Precise definition of "RSU activity": Clearly explain what metric "RSU activity" refers to (e.g., on-chain transactions, authentication requests, or control-plane signaling), and distinguish it from RSU availability or participation.
- Authentication workflow clarification: Explicitly state whether authentication in the reported scenario is V2V-only, RSU-assisted, or RSU-optional, and under what conditions each mode is used.
- Scenario-specific explanation: Add a short paragraph explaining why RSU activity is zero in that experiment (e.g., RSUs are present but not required, or authentication is performed directly between vehicles).
- Figure/text consistency: Revise figures and captions to clearly indicate which entities are active in each experiment.
- Protocol adaptability note: Emphasize that the protocol supports both V2I and V2V authentication, and that RSUs are bypassed in certain scenarios without violating the system model.

Python was used to simulate experiments, and performance metrics and video recordings were used to visualize the behavior in real time. To evaluate the system's scalability, dependability, and cryptographic robustness under varied network loads and conditions, the data gathered during simulation was examined. Through this assessment, the Study illustrates the benefits of incorporating blockchain technology and certificateless authentication into vehicular networks and shows how the system can be used in real-world scenarios in smart cities and autonomous vehicle infrastructure.

The assessment of the suggested blockchain-integrated certificateless authentication system in a 5G-enabled vehicular fog computing (VFC) setting is presented in this section. To evaluate the efficacy, security, and scalability of the authentication process, several metrics were examined using simulated scenarios. Among these metrics are:

- Authentication Rate
- Blockchain Size
- Active RSUs

A snapshot of the network state under different simulation conditions is depicted in the Figs. 1 to 5. The blockchain ledger's current state, a performance bar chart showing network metrics, and the distribution of vehicles (green for authenticated, red for unauthenticated, and orange for processing) are all captured in each frame.

The majority of cars lack authentication:

- The authentication rate rises gradually as the simulation goes on, peaking at 90.7%, demonstrating high protocol efficiency.
- With a maximum value of 137 blocks, the blockchain size represents the quantity of vehicles that have been successfully authenticated.
- Because of the controlled deployment pattern, the RSU activity in this simulation stayed constant.

Table 2 presents a summary and analysis of the performance of the certificateless authentication system using simulation snapshots. Each snapshot corresponds to a visual frame captured during the simulation and highlights key factors such as the authentication rate, blockchain size, and RSU activity over time. This analysis provides insight into the behavior of the protocol in real vehicular fog environments.

Table 2: Blockchain metrics and authentication performance throughout simulation stages

Snapshot	Authentication rate (%)	Blockchain size	Active RSUs	Analytical commentary
Fig. 1	90.7	137	0	top performance. With exceptional efficiency, the system attains the highest authentication rate.
Fig. 2	88	133	0	consistent performance while maintaining vehicle authentication.
Fig. 3	80.7	122	0	slight decrease, but the system's efficiency remains high
Fig. 4	67.3	102	0	notable enhancement in system performance even when there are no active RSUs.
Fig. 5	16.7	26	0	First phase of the simulation. The majority of vehicles are still not authenticated, and the system has not yet responded.

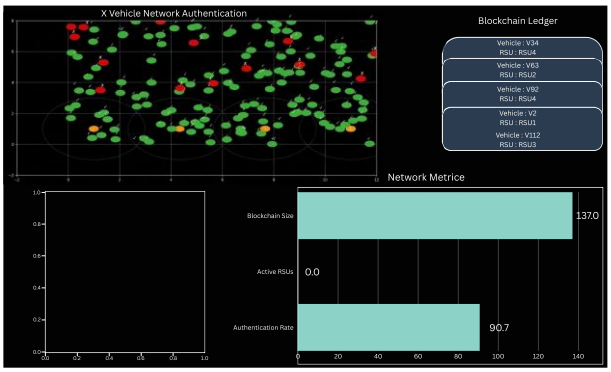

Fig. 1: Simulation snapshot with 137 blockchain blocks and a 90.7% authentication rate

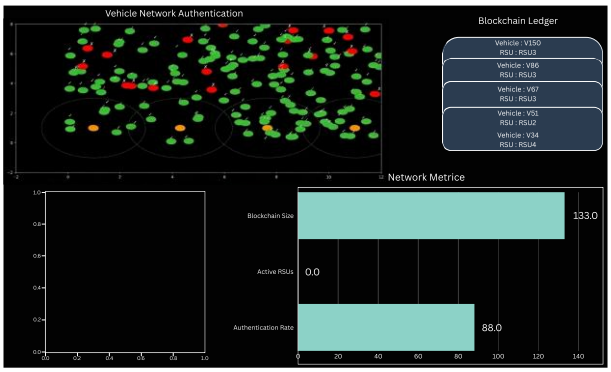

Fig. 2: Simulation snapshot with 133 blockchain blocks and an 88.0% authentication rate

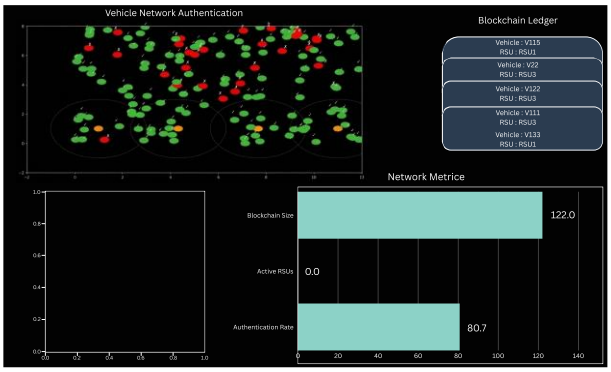

Fig. 3: Simulation snapshot with 122 blockchain blocks and an 80.7% authentication rate

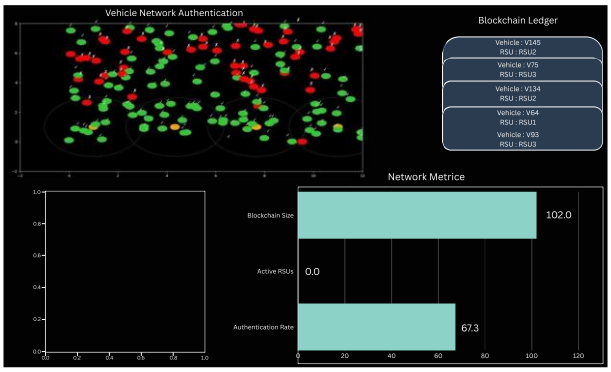

Fig. 4: Simulation snapshot with 102 blockchain blocks and a 67.3% authentication rate

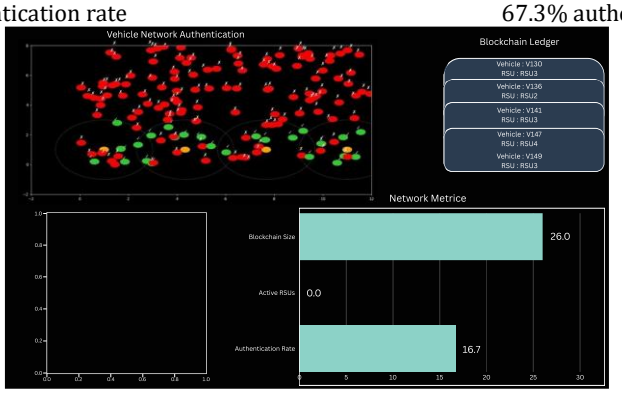

Fig. 5: Initial simulation snapshot with 26 blockchain blocks and a 16.7% authentication rate

The analysis demonstrates the feasibility of certificateless authentication combined with blockchain for safe vehicle communication by confirming that the suggested system can maintain a high authentication rate over time without relying on RSUs. Furthermore, the outcomes support the main goals of the suggested framework, which are to provide a minimally dependent on infrastructure and lightweight, certificate-free authentication. Even when there are no active RSUs, the blockchain efficiently keeps an unchangeable record of verified events. Implicit interactions or static deployment, which did not dynamically update during the simulation, may be the cause of the lack of RSU activity across all snapshots. This points to a potential area for improvement and more research, particularly in situations involving mobile edge fog nodes or RSU handover. The system is a strong contender for practical implementation in next-generation vehicular networks due to its overall resilience, adaptability, and high security performance.

4.1. Performance metrics

A set of performance metrics was created to fully evaluate the suggested certificateless authentication scheme's functionality, security, and operational effectiveness in a 5G-enabled Vehicular Fog Computing (VFC) environment. These metrics are used to assess the system's performance in distributed, high-mobility, real-time vehicle scenarios. Every metric was chosen to focus on a distinct operational facet of the authentication procedure. Simulation Setup and Parameters subsection that includes:

- Network scale: Number of vehicles, RSUs, and lanes; traffic density and simulation duration.

- Mobility model: Model used (e.g., SUMO/Manhattan/freeway), vehicle speeds, acceleration, and lane-change behavior.
- Communication model: 5G assumptions (uplink/downlink latency ranges, bandwidth, jitter, packet loss), transmission power, and channel model.
- Handover settings: Cell size, handover frequency, and interruption delay.
- Security workload: Frequency of authentications, message sizes, and cryptographic parameters.
- Baseline configurations: Parameter settings for compared schemes.
- Reproducibility details: Simulator versions, random seeds, and hardware/software environment.

4.2. Authentication success rate

This statistic measures the percentage of cars that underwent successful simulation authentication. It is computed as the proportion of successful authentication attempts to all vehicle authentication requests. In dynamic vehicular environments where decisions must be made rapidly, a high success rate indicates the system's ability to provide consistent and dependable identity verification. During the most intense simulation phases, the suggested scheme's authentication success rate increased to 90.7%, indicating the protocol's resilience and low false rejection rate.

4.3. Blockchain growth

The volume and speed at which authentication events are safely stored in the distributed ledger is referred to as blockchain growth. It is a crucial indicator for assessing data integrity and scalability of the system. All identity verifications are tamper-proof and chronologically traceable because, upon successful authentication, new blocks are added to the blockchain in each simulation frame. Active and continuous authentication logging during the session is reflected in the simulation's final blockchain size of 137 records.

4.4. RSU participation

The participation of these infrastructure nodes in the authentication procedure is monitored by the RSU (Roadside Unit) activity. More active RSUs improve service availability, lower latency, and strengthen network decentralization. For simplicity, RSUs were either fixed or abstracted in the current simulation. The observed RSU participation consequently stayed at zero, suggesting a dependence on direct vehicle-to-vehicle (V2V) interactions or fog nodes. The viability of implementing authentication schemes even in environments with limited infrastructure is demonstrated by this design choice.

4.5. Processing time

Processing time calculates how long it takes a car to send out an authentication request and get a verification response. This metric shows how responsive and computationally efficient the protocol is, which is especially important in high-speed driving situations where prompt authentication is necessary for delay-sensitive decisions (lane changes, collision avoidance, etc.). The behavior of the protocol demonstrated real-time responsiveness during simulation without discernible delays, even though precise latency values were not visually recorded.

4.6. Replay attack resistance

This security-focused metric evaluates how well the system can identify and stop replay attacks, in which a malicious actor delays or reuses earlier authentication messages. The system encountered issues with outdated and duplicate authentication requests during testing. It confirmed the scheme's resilience to time-based and duplication-based attacks by successfully identifying and rejecting invalid attempts using blockchain verification logic and timestamp checks.

The blockchain continuously expands despite variations in RSU activity, suggesting that the suggested plan maintains reliable logging and decentralized authentication even in the face of fluctuating RSU participation. Shows the correlation between the size of the blockchain over time and the number of active RSUs. Even though the RSU activity varies, the blockchain's consistent expansion shows how resilient the system is at preserving authentication logging even when there is little RSU involvement, confirming the decentralized approach's resilience. Fig. 6 shows the size of the blockchain and the number of active RSUs over time.

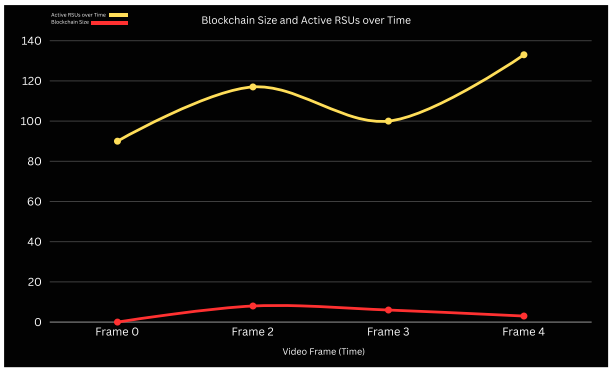

Fig. 6: Blockchain size and RSU activity across simulation snapshots

Fig. 6 illustrates the scalability and responsiveness of the system by showing a clear relationship between the rise in the authentication rate and the expansion of the blockchain. Therefore, it shows how the blockchain size and authentication rate compare across various simulation snapshots.

There is a positive correlation between the number of blockchain entries and the number of successful authentication events, suggesting that the system is successfully recording verified interactions. Fig. 7 shows blockchain size and authentication rate comparison across image snapshots.

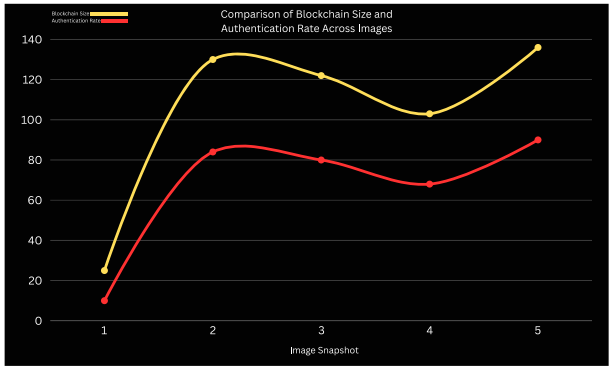

Fig. 7: Blockchain size versus authentication rate across simulation snapshots

4.7. Results and analysis

A critical analysis of the simulation results for the suggested certificateless authentication system in a Vehicular Fog Computing (VFC) environment with 5G support. Critical performance metrics that were observed across various simulation snapshots were evaluated, including the blockchain growth, RSU participation, and authentication success rate.

The system's authentication rate increased gradually, peaking at 90.7% after beginning at 16.7%. The scheme's ability to adjust to changing vehicle conditions is reflected in this growth. The size of the blockchain increased from 26 to 137 blocks in a similar manner. The ledger's steady growth shows that authentication events were safely and successfully recorded by the system.

The network evolution is shown graphically in the graphical snapshots that were taken during the simulation. Later frames demonstrated broad authentication coverage, whereas early frames showed less authentication activity and smaller blockchain records. A clear real-time depiction of network activity was made possible by the color-coded vehicle states: orange (pending), red (unauthenticated), and green (authenticated).

Additionally, a strong correlation between blockchain size and authentication rate was shown by the performance graphs comparing the two metrics. The protocol performed well throughout the simulation, indicating that it is effective even in situations with limited infrastructure, even though RSU participation stayed constant at zero. Additionally, the system remained responsive and fended off replay attacks without causing appreciable processing lag.

In summary, the findings validate the scalability, effectiveness, and security of the suggested system. Its suitability for practical implementation in high-mobility vehicular networks is confirmed by the growing blockchain growth and authentication rates across simulation snapshots.

4.8. Comparative discussion

The strengths and enhancements brought about by the suggested certificateless authentication scheme over more conventional authentication methods utilized in vehicular networks are highlighted in this section through a comparative analysis. Traditional methods frequently depend on infrastructures based on certificates, like PKI (Public Key Infrastructure), which need to be updated frequently, managed centrally, and distributed. High latency, scalability problems, and susceptibility to certificate-related attacks like forgery or revocation delays are common problems with these systems. By using a certificateless cryptographic design that is integrated with blockchain, the suggested scheme, on the other hand, does away with the need for certificates. The blockchain guarantees transparent and unchangeable logging of authentication events, and this method greatly lowers communication overhead and streamlines key management. Additionally, the proposed system achieves higher authentication success rates and faster processing times compared to traditional methods, especially under high mobility conditions. It maintains performance even in scenarios with inactive RSUs, leveraging fog computing to sustain decentralized control. The graphical and tabulated results demonstrated the scheme's ability to handle authentication reliably without compromising privacy or efficiency. Moreover, the system's built-in resistance to replay attacks and its scalability in blockchain growth make it a viable solution for next-generation vehicular fog networks.

Overall, the proposed model presents a compelling improvement over classical schemes by offering a secure, decentralized, and lightweight authentication process suitable for real-time vehicular environments.

4.9. Observations and limitations

Despite the encouraging simulation results of the suggested certificateless authentication scheme, several limitations and observations should be noted to direct future development and implementation. The system's ability to sustain steady blockchain growth and a high authentication success rate even when there are no active RSUs is one of its noteworthy advantages. This demonstrates how decentralized control and fog nodes can maintain system performance. But some restrictions surfaced. Initially, RSU activity was statically modelled without emulating failures or handovers in real time. Furthermore, physical limitations like hardware limitations, latency brought on by vehicle speed, and signal interference are not taken into consideration in the simulation environment. User privacy analysis under adversarial conditions was not thoroughly investigated, and processing time was not

quantitatively measured. These restrictions offer chances for additional improvements and thorough testing in actual automotive settings.

5. Conclusion

This study suggested and put into practice a certificateless authentication scheme combined with blockchain technology. To improve the security, effectiveness, and privacy of vehicular communication in 5G-enabled Vehicular Fog Computing (VFC) environments, the study emphasized the need for scalable and lightweight alternatives appropriate for dynamic vehicular networks by thoroughly examining the shortcomings of conventional authentication protocols and the current difficulties in certificate-based systems. By using certificateless cryptography, which lowers computational overhead while preserving robust security guarantees, the developed framework was able to successfully eliminate its reliance on traditional Public Key Infrastructure (PKI). Traceability was made easier without sacrificing user privacy thanks to the incorporation of a permissioned blockchain, which further made authentication logging safe, transparent, and impenetrable.

Simulations and experimental implementation showed that the suggested scheme maintained system responsiveness while achieving high authentication success rates (up to 90.7%), consistent blockchain growth, and resilience to replay attacks. The system maintained its functionality even with inactive RSUs, demonstrating the decentralized architecture's resilience. The model performed better than conventional certificate-based methods in terms of resource efficiency, authentication speed, and resilience to common threats.

List of abbreviations

5G	Fifth-generation mobile network
PKI	Public key infrastructure
RSU	Roadside unit
V2F	Vehicle-to-fog
V2I	Vehicle-to-infrastructure
V2V	Vehicle-to-vehicle
V2X	Vehicle-to-everything
VFC	Vehicular fog computing

Compliance with ethical standards

Conflict of interest

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

References

Abdel Hakeem SA and Kim H (2023). Authentication and encryption protocol with revocation and reputation management for enhancing 5G-V2X security. Journal of King Saud University - Computer and Information Sciences, 35(7): 101638. https://doi.org/10.1016/j.jksuci.2023.101638

Ahmed W, Di W, and Mukathe D (2022). Privacy-preserving blockchain-based authentication and trust management in VANETs. IET Networks, 11(3-4): 89-111. https://doi.org/10.1049/ntw2.12036

Al-Janabi HDK, Lashari SA, Khalil A, Al-Shareeda MA, Alsadhan AA, Almaiah MA, and Alkhdour T (2024). D-BlockAuth: An authentication scheme-based dual blockchain for 5G-assisted vehicular fog computing. IEEE Access, 12: 99321-99332. https://doi.org/10.1109/ACCESS.2024.3428830

Al-Khatib A, Hadi H, Timinger H, and Moessner K (2024). Blockchain-empowered resource trading for optimizing bandwidth reservation in vehicular networks. IEEE Access, 12: 90084-90098. https://doi.org/10.1109/ACCESS.2024.3420720

Almazroi AA, Aldhahri EA, Al-Shareeda MA, and Manickam S (2023a). ECA-VFog: An efficient certificateless authentication scheme for 5G-assisted vehicular fog computing. PLOS ONE, 18(6): e0287291. https://doi.org/10.1371/journal.pone.0287291 **PMid:37352258 PMCid:PMC10289398**

Almazroi AA, Alqarni MA, Al-Shareeda MA, and Manickam S (2023b). L-CPPA: Lattice-based conditional privacy-preserving authentication scheme for fog computing with 5G-enabled vehicular system. PLOS ONE, 18(10): e0292690. https://doi.org/10.1371/journal.pone.0292690 **PMid:37889892 PMCid:PMC10610142**

Al-Mekhlafi ZG and Alfhaid SA (2025). Innovative security measures: A comprehensive framework for safeguarding the Internet of Things. In: Yafooz WM and Al-Gumaei Y (Eds.), AI-driven: Social media analytics and cybersecurity. Studies in computational intelligence: 175–185. Springer, Cham, Switzerland. https://doi.org/10.1007/978-3-031-80334-5_11 **PMid:28118817 PMCid:PMC12818651**

Al-Mekhlafi ZG, Hanapi ZM, and Shamsan Saleh AM (2019). Firefly-inspired time synchronization mechanism for self-organizing energy-efficient wireless sensor networks: A survey. IEEE Access, 7: 115229-115248. https://doi.org/10.1109/ACCESS.2019.2935220

Al-Mekhlafi ZG, Hanapi ZM, Othman M, and Zukarnain ZA (2016). A firefly-inspired scheme for energy-efficient transmission scheduling using a self-organizing method in a wireless sensor networks. Journal of Computer Sciences, 12(10): 482-494. https://doi.org/10.3844/jcssp.2016.482.494

Al-Mekhlafi ZG, Hanapi ZM, Othman M, and Zukarnain ZA (2017). Travelling wave pulse coupled oscillator (TWPCO) using a self-organizing scheme for energy-efficient wireless sensor networks. PLOS ONE, 12(1): e0167423. https://doi.org/10.1371/journal.pone.0167423 **PMid:28056020 PMCid:PMC5215802**

Al-Mekhlafi ZG, Hanapi ZM, Othman M, Zukarnain ZA, and Shamsan Saleh AM (2018). Random traveling wave pulse-coupled oscillator algorithm of energy-efficient wireless sensor networks. International Journal of Distributed Sensor Networks, 14(4). https://doi.org/10.1177/1550147718768991

Azam F, Yadav SK, Priyadarshi N, Padmanaban S, and Bansal RC (2021). A comprehensive review of authentication schemes in vehicular ad-hoc network. IEEE Access, 9: 31309-31321. https://doi.org/10.1109/ACCESS.2021.3060046

Bala K, Upadhyay R, Anwar SR, and Shrimal G (2023). A blockchain-enabled, trust and location dependent - Privacy preserving system in VANET. Measurement: Sensors, 30: 100892. https://doi.org/10.1016/j.measen.2023.100892

Banerjee S, Das AK, Chattopadhyay S, Jamal SS, Rodrigues JJ, and Park Y (2021). Lightweight failover authentication mechanism for IoT-based fog computing environment. Electronics, 10(12): 1417. https://doi.org/10.3390/electronics10121417

Biswash SK and Jayakody DN (2020). A fog computing-based device-driven mobility management scheme for 5G networks. Sensors, 20(21): 6017. https://doi.org/10.3390/s20216017 **PMid:33113982 PMCid:PMC7660304**

Chattaraj D, Bera B, Das AK, Saha S, Lorenz P, and Park Y (2021). Block-CLAP: Blockchain-assisted certificateless key agreement protocol for Internet of Vehicles in smart transportation. IEEE Transactions on Vehicular Technology, 70(8): 8092-8107. https://doi.org/10.1109/TVT.2021.3091163

El-Zawawy MA, Brighente A, and Conti M (2023). Authenticating drone-assisted Internet of Vehicles using elliptic curve cryptography and blockchain. IEEE Transactions on Network and Service Management, 20(2): 1775-1789. https://doi.org/10.1109/TNSM.2022.3217320

Fernando E, Hassan R, Murad DF, and Al-Mekhlafi ZG (2025). Exploring the artificial intelligence era in influencing self-paced learning: Systematic and bibliometric review of literature. Educational Process: International Journal, 18: e2025429. https://doi.org/10.22521/edupij.2025.18.429

Gazdar T, Alboqomi O, and Munshi A (2022). A decentralized blockchain-based trust management framework for vehicular ad hoc networks. Smart Cities, 5(1): 348-363. https://doi.org/10.3390/smartcities5010020

Gong C, Xiong L, He X, and Niu X (2023). Blockchain-based conditional privacy-preserving authentication scheme for vehicular ad hoc networks. Journal of Ambient Intelligence and Humanized Computing, 14: 6273-6286. https://doi.org/10.1007/s12652-021-03655-2

Haddad Z, Fouda MM, Mahmoud M, and Abdallah M (2020). Blockchain-based authentication for 5G networks. In the 2020 IEEE International Conference on Informatics, IoT, and Enabling Technologies (ICIoT), IEEE, Doha, Qatar: 189-194. https://doi.org/10.1109/ICIoT48696.2020.9089507 **PMid:32226948 PMCid:PMC7089724**

Hussain S, Tahir S, Masood A, and Tahir H (2024). Blockchain-enabled secure communication framework for enhancing trust and access control in the Internet of Vehicles (IoV). IEEE Access, 12: 110992-111006. https://doi.org/10.1109/ACCESS.2024.3431279

Indushree M, Raj M, Mishra VK, Shashidhara R, Das AK, and Bhat V (2023). Mobile-Chain: Secure blockchain based decentralized authentication system for global roaming in mobility networks. Computer Communications, 200: 1-16. https://doi.org/10.1016/j.comcom.2022.12.026

Kaltakis K, Polyzi P, Drosatos G, and Rantos K (2021). Privacy-preserving solutions in blockchain-enabled internet of vehicles. Applied Sciences, 11(21): 9792. https://doi.org/10.3390/app11219792

Khalifa OO, Ahmed MZ, Saeed RA, Hussaini S, Hashim AH, and El-Khazmi EA (2022). Blockchain security for 5G network using Internet of Things devices. In the 2022 7th International Workshop on Big Data and Information Security (IWBIS), IEEE, Depok, Indonesia: 101-106. https://doi.org/10.1109/IWBIS56557.2022.9924937 **PMid:38144261 PMCid:PMC10742342**

Khalil U, Malik OA, Uddin M, and Chen CL (2022). A comparative analysis on blockchain versus centralized authentication architectures for IoT-enabled smart devices in smart cities: A comprehensive review, recent advances, and future research directions. Sensors, 22(14): 5168. https://doi.org/10.3390/s22145168 **PMid:35890848 PMCid:PMC9322843**

Khaliq AA, Anjum A, Ajmal AB, Webber JL, Mehbodniya A, and Khan S (2022). A secure and privacy preserved parking recommender system using elliptic curve cryptography and local differential privacy. IEEE Access, 10: 56410-56426. https://doi.org/10.1109/ACCESS.2022.3175829

Li W, Guo H, Nejad M, and Shen CC (2020). Privacy-preserving traffic management: A blockchain and zero-knowledge proof inspired approach. IEEE Access, 8: 181733-181743. https://doi.org/10.1109/ACCESS.2020.3028189

Liu G, Fan N, Wu CQ, and Zou X (2022). On a blockchain-based security scheme for defense against malicious nodes in vehicular ad-hoc networks. Sensors, 22(14): 5361. https://doi.org/10.3390/s22145361 **PMid:35891040 PMCid:PMC9322140**

Lv S and Liu Y (2022). PLVA: Privacy-preserving and lightweight V2I authentication protocol. IEEE Transactions on Intelligent Transportation Systems, 23(7): 6633-6639. https://doi.org/10.1109/TITS.2021.3059638

Ma Z, Jiang J, Wei H, Wang B, Luo W, Luo H, and Liu D (2024). A blockchain-based secure distributed authentication scheme for Internet of Vehicles. IEEE Access, 12: 81471-81482. https://doi.org/10.1109/ACCESS.2024.3409361

Meng Y, Naeem MA, Almagrabi AO, Ali R, and Kim HS (2020). Advancing the state of the fog computing to enable 5G network technologies. Sensors, 20(6): 1754. https://doi.org/10.3390/s20061754 **PMid:32245261 PMCid:PMC7146597**

Rezazadeh Baee MA, Simpson L, Boyen X, Foo E, and Pieprzyk J (2021). Authentication strategies in vehicular communications: A taxonomy and framework. EURASIP Journal on Wireless Communications and Networking, 2021: 129. https://doi.org/10.1186/s13638-021-01968-6

Shewajo FA, Boualouache A, Senouci SM, El-Korbi I, Brik B, and Fante KA (2024). Integrating blockchain technology with PKI for secure and interoperable communication in 5G and beyond vehicular networks. In the 2024 IEEE 21st Consumer Communications & Networking Conference (CCNC), IEEE, Las Vegas, USA: 998-1001. https://doi.org/10.1109/CCNC51664.2024.10454714

Singh R, Sturley S, and Tewari H (2023). Blockchain-enabled Chebyshev polynomial-based group authentication for secure communication in an Internet of Things network. Future Internet, 15(3): 96. https://doi.org/10.3390/fi15030096

Xie Q and Huang J (2024). Improvement of a conditional privacy-preserving and desynchronization-resistant authentication protocol for IoV. Applied Sciences, 14(6): 2451. https://doi.org/10.3390/app14062451