

AUTHENTICATION-BASED SECURE DATA DISSEMINATION IN 5G-ENABLED VANETS

Anupama Verma, Gulista Khan*

Faculty of Engineering, Teerthanker Mahaveer University
India

* Corresponding Author, e-mail: anupamaverma0907@gmail.com

Abstract: With the extensive usage of Vehicular Ad Hoc Networks (VANETs) in intelligent transportation, issues such as securing and lowering the latency period become increasingly important, particularly related to potential malicious nodes. This research proposes a secure data dissemination approach for VANETs. In the suggested model, Elliptic Curve Cryptography (ECC) is used for lightweight message signing, AES is used for encryption purposes, and the VeChainThor blockchain technology is used for trustless and decentralized management of public keys. A rule-based intrusion detection system is incorporated into the edge nodes to detect any suspicious behaviour that might threaten the safety of information. The proposed approach is evaluated through simulations involving 5000 data packets, achieving an average throughput of 8.94 Mbps and a low latency of 0.021 seconds, with authentication delays.

Keywords: 5G, VANETs, authentication, blockchain, trust management, intrusion detection system.

1. INTRODUCTION

VANETs provide wireless communication between Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I). The networks enable a set of applications that include traffic congestion updates, lane-changing warnings, real-time directions, and crash warnings, and are therefore a critical part of Intelligent Transportation Systems (ITS) [1]. A typical VANET architecture involves On-Board Units (OBUs) that are mounted in vehicles, Roadside Units (RSUs) mounted on roadsides, and a Trusted Authority (TA) that manages identity and keying operations. Communication is usually done with standards like Dedicated Short-Range Communication (DSRC) or Cellular-Vehicle-To-Everything (V2X) [2].

Despite their promising potential, VANETs are extremely susceptible to security attacks because of their dynamic and exposed nature. Vehicles within a VANET are constantly entering and leaving the network, and this creates highly dynamic, highly mobile topologies, which make consistent and reliable connectivity a problematic issue [3]. Among the various security measures, the fundamental need for secure communication in VANETs [4] is authentication. Traditional security measures like symmetric key algorithms or centralized authentication methods cannot meet the

VANETs' demands because of their low-latency and scalable requirements. Modern cryptographic algorithms, on the other hand, can provide higher security [5]. Approaches such as Public Key Infrastructure (PKI), identity-based cryptography, group signatures, and batch authentication enable vehicles to securely sign and validate messages, preserving message integrity and facilitating conditional privacy [6].

The proposed work offers an innovative, integrated solution that incorporates ECC-based authentication, blockchain-enabled identity management, trust assessment, rule-based IDS, and trust AODV routing, particularly for secure data dispatching within the 5G VANET environment. Most existing works develop models dealing with these components in isolation. The proposed solution develops a comprehensive and integrated lightweight security model.

The objective of this paper is to present a solution to authenticate the dissemination process in 5G-based VANETs. This paper makes the following contributions:

- Created a comprehensive security framework utilizing ECC-based authentication, VeChainThor blockchain-based identity management, dynamic trust evaluation, rule-driven intrusion detection, and trust-aware AODV routing for secure data dissemination in 5G-enabled VANETs.
- Employed a practical rule-based IDS to identify and prevent common VANET-specific attacks such as message forgery, replay, and flooding, ensuring real-time security with minimal computational overhead.
- Introduced a trust-aware message filtering mechanism that dynamically evaluates the credibility of each participating vehicle based on behavioural analysis, enabling the selective dissemination of only reliable data across the VANET.

The remaining paper is organized as follows: Section 2 presents a relevant review of existing studies by various authors. Section 3 outlines the proposed methodology. Section 4 discusses the results and analysis, and Section 5 concludes the paper with key findings and highlights future scope.

2. LITERATURE REVIEW

Over the past several years, the development of VANETs and 5G networks has fuelled the growth of efficient and secure VANET communication. In order to overcome issues of authentication, in [7] is presented an elliptic curve signature-based mutual authentication protocol based on edge computing that achieved a communication cost of 772 bytes and was resistant to replay and man-in-the-middle attacks. Expanding upon this, in [8] is presented an Efficient and Anonymous Identity Authentication (EAIA) protocol suitable for scenarios where there are no RSUs. The study attained a computation cost equal to 2.354 ms, providing lightweight and distributed security.

Moving to attack detection, in [9] is discussed a combination of an Adaptive Neuro-Fuzzy Inference System (ANFIS) with Particle Swarm Optimization (PSO) in the study. They detected black hole attacks with 95.62% packet delivery, 99.55% accuracy, and a detection time of 6.76 ms, reflecting excellent detection sensitivity. Building upon this line of work, in [10] is developed a two-layer Machine learning (ML)-based IDS

implemented between on-vehicle modules and Mobile Edge Computing (MEC) servers that offered a maximum network latency and energy consumption reduction of 80%.

In response to the quantum attacks, discussion in [11] created a lattice-based group signature with Bonsai-tree architecture with 3.99 ms signing and 1.12 ms verification, quantum attack-resistant under Learning with Errors (LWE) and Short Integer Solution (SIS) assumptions. In the meantime, paper [12] minimized latency in VANETs with a priority-based fog computing mechanism with 5G MEC, a 20% reduction in latency, and a 35% reduction in delay. Likewise, in [13] is presented a 5G data-sharing scheme without RSUs with a 66.67% reduction in signing cost and 13.89% communication overhead. Expanding the context to IoV, Ahash-based authentication scheme within a five-layer IoV framework called Authentication-based Medium Access Control (A-MAC) is proposed in [11], which attained a low storage cost of 158 bytes and robust security performance. Moving ahead with network-based approaches for security, In addition, in [15] is introduced an ensemble technique that could help detect jamming attacks in VANETs. The voting-based classification technique provided better results than any other model, detecting jamming attacks with an accuracy of 99.8125%.

Some main research gaps are presented below.

- Lack of an integrated lightweight authentication model incorporating ECC and Blockchain technologies for real-time VANET communication [7, 13].
- Absence of lightweight IDS solutions suitable for the fast-changing and resource-limited environment of VANETs [10].
- Limited integration of behavior-based trust evaluation in message dissemination frameworks [8, 14].
- Despite advances in secure data transmission, existing methods rarely integrate proven routing protocols with 5G to meet real-time responsiveness for safety-critical alerts [12].

Table 1 consolidates the main shortcomings identified in the literature and shows the specific design contributions of the proposed framework that address each of the outlined gaps.

Table 1: Gap–Contribution Mapping

Existing Studies Gaps	Proposed Contribution
Lack of an integrated VANET security framework	Unified ECC–Blockchain–Trust–IDS–AODV architecture
Limited trust evaluation	Dynamic trust-score mechanism
High IDS complexity	Lightweight rule-based IDS
Security-routing separation	Trust-aware AODV routing
Centralized key management	Blockchain-based identity management

Overall, the proposed framework effectively addresses the major limitations of existing VANET security solutions through a comprehensive and integrated security architecture.

As illustrated in Table 2, previous studies mostly examine separate elements like authentication, intrusion detection, or communication efficiency. However, none of the studies have collectively incorporated ECC-based authentication, blockchain-based decentralized identity management, and combined with dynamic trust evaluation, lightweight intrusion detection systems, and trust-based AODV routing in a single

framework for 5G-enabled VANET systems. This creates the primary originality of the work proposed.

Table 2: Feature Comparison with Existing Studies

Study	Authentication Type	Trust Model	IDS Approach	Routing Protocol	Blockchain Support	Simulation Scale
Abbood et al. (2025) [7]	ECC-based Mutual Authentication	Not Considered	Not Included	Not Specified	Not Included	Not Reported
Du et al. (2024) [8]	Anonymous Identity Authentication	Not Addressed	Not Addressed	Not Addressed	Not Addressed	Not Reported
Mirzaee et al. (2021) [10]	Authentication Framework	Absent	ML-based IDS	Absent	Absent	Vehicle-Edge Scenario
Farooqi et al. (2022) [12]	Secure Communication	Not Considered	Not Considered	Fog-Based Communication	Not Considered	Large VANET Scenario
Al-Shareeda et al. (2022) [13]	5G Authentication Scheme	Not Addressed	Not Addressed	Not Addressed	Not Addressed	Not Reported
Gupta et al. (2020) [14]	Authentication-Based Dissemination	Limited Support	Absent	Absent	Absent	IoV Framework
Proposed Work	ECC + Blockchain Authentication	Dynamic Trust Scoring	Rule-Based IDS	Trust-Aware AODV	VeChainThor Blockchain	50 Vehicles, 5000 Packets

3. METHODOLOGY

This section outlines the proposed secure communication framework for 5G-enabled VANETs, as shown in Figure 1. It details the architecture, authentication mechanism, intrusion detection, trust evaluation, and routing strategy. The framework leverages ECC, lightweight Blockchain, and Ad hoc On-demand Distance Vector (AODV) integrated with 5G Ultra-Reliable Low-Latency Communication (URLLC) to ensure efficient and secure data dissemination among vehicular nodes.

3.1. System Architecture Design

The architecture includes five fundamental components, each with a distinct role to play in the reliable communication network. Vehicles are mounted with OBUs [16], which are the fundamental nodes upon which real-time events on the road are sensed. RSUs are intermediate verifiers and forwarders within the network [17]. 5G Base Stations supply the network backbone of the system that is responsible for ultra-reliable and ultra-low latency data exchange between vehicles. Edge Servers are placed nearer to vehicles and RSUs such that the requirement to directly interact with distant cloud servers or with the entire blockchain network is eliminated.

3.2. Identity & Key Management using VeChainThor

Instead of relying on traditional PKI-based certificate authorities, the system employs a lightweight blockchain model using VeChainThor [18], which provides decentralized, tamper-proof identity validation, public key distribution, and revocation handling through smart contracts.

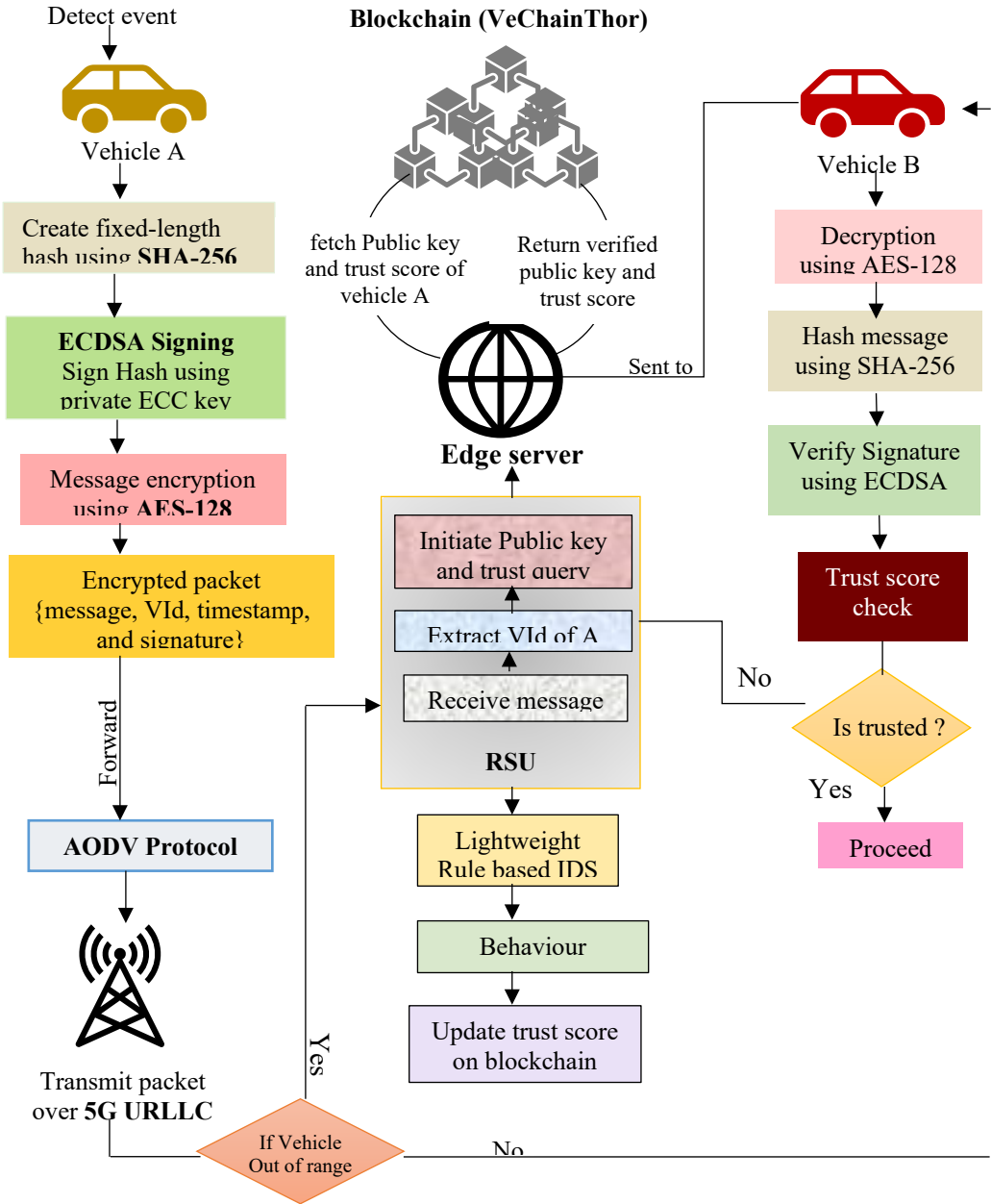


Figure 1. Proposed architecture

Vehicle Registration and Key Assignment. Every vehicle V_i gets a pseudonymous identity called (VID_i) and an ECC key pair, where the public key is (K_i^{pub}) and the private key is (K_i^{priv}) . This key pair gets generated once in a secure registration process

involving the Blockchain. The (VID_i) and (K_i^{pub}) get stored on the VeChainThor Blockchain for transparent verification:

$$B \leftarrow B \cup \{(VID_i, K_i^{pub})\} \quad (1)$$

In the above expression, B refers to the blockchain ledger and $\cup$ stands for the immutable appending of the tuple to the Blockchain. The proposed framework employs a 256-bit ECC key pair for vehicle authentication and digital signature generation.

Public Key Retrieval for Authentication. When any vehicle or RSU gets a message signed using the pseudonym ID, it queries the VeChainThor blockchain through the Edge Server to obtain the public key for signature verification:

$$K_i^{pub} = \text{QueryBlockchain}(VID_i) \quad (2)$$

Immutable Logging of Communication Events. Every important message exchanged within the network (such as alerts, trust modifications) undergoes hashing and recording on the Blockchain for future auditing purposes. The event log E for a message M is:

$$E = H(M) \text{ where } H: \text{SHA} - 256 \quad (3)$$

Hash (E) is stored on the VeChainThor network through the smart contract, which comprises Sender VID, Timestamp, Message type, and Trust update (if applicable).

Revocation via Smart Contracts. As opposed to traditional Certificate Revocation Lists (CRLs), the blockchain system uses smart contracts to label vehicles with any malicious activity. In case a vehicle V_X is found to be misbehaving:

- A smart contract gets invoked to flag the vehicle:

$$B[VID_X].\text{revoked} \leftarrow \text{True} \quad (4)$$

- Any subsequent searches for VID_X would show it as revoked status, and its messages would be disregarded in the VANET.

3.3. Mutual Authentication Protocol using ECC + Blockchain

The suggested approach makes use of the Elliptic Curve Digital Signature Algorithm (ECDSA) [19] for lightweight and secure digital signature generation. The four essential parts of each message sent are as follows: Time Stamp to guarantee message freshness, Sender Pseudonym (VID) to keep identity confidential, Digital Signature for message authentication, and Message Hashed Payload.

3.4. Message Integrity & Confidentiality

Message integrity guarantees that the message data has not been altered during transmission, whereas the confidentiality aspect guarantees that only authorized individuals gain access to the message content. In order to accomplish this goal, SHA-256 [20] is utilized for hashing of the message to confirm its integrity. The AES-128 [21] was selected because it provides a strong balance between security and computational efficiency, while maintaining low latency suitable for real-time 5G-enabled VANET communications.

3.5. Blockchain-Based Trust Management System

A dynamic trust score is given to each vehicle and is adjusted according to its performance. The RSU and edge server keep track of the message consistency,

Timestamp accuracy, and Global Positioning System (GPS)- reported position compared to its actual position.

3.6. Rule-Based IDS

Since computationally costly ML-based intrusion detection systems might not be suitable for VANETs that require real-time performance, a lightweight IDS based on rule-based systems is used in RSUs and Edge Servers [22]. It uses predefined heuristics to detect suspicious activities.

3.7. Trust-Filtered AODV Routing Protocol

The Ad hoc On-demand Distance Vector (AODV) routing protocol creates paths only if required and selects the best path depending on hop count and availability.

$$\text{Trusted Neighbour Set: } R = \{i \in \text{neighbors} \mid \tau_i \geq \tau_{\text{thresh}}\} \quad (5)$$

$$\text{Next Hop Selection: } \text{NextHop} = \arg \min_{i \in R} d(i, D) \quad (6)$$

where $d(i, D)$ represents the distance between node i and the destination node D .

4. RESULTS AND DISCUSSION

In this section, a complete analysis of results related to the suggested algorithm is provided, which would be based on the following measures.

$$\text{Throughput} = \frac{\text{Total Simulation}}{\text{TimeTotal Data Delivered}} \quad (7)$$

$$\text{Latency} = \frac{1}{N} \sum_{i=1}^N (t_i^{\text{recv}} - t_i^{\text{send}}) \quad (8)$$

where t_i^{recv} denotes the received time, and t_i^{send} represents the send time of the message.

$$\text{Packet Delivery Ration} = \frac{\text{Packets Received}}{\text{Packets Sent}} \times 100\% \quad (9)$$

$$D_{\text{auth}} = t_{\text{verify}} + t_{\text{blockchain_lookup}} \quad (10)$$

$$\text{ADR} = \frac{\text{Detected Attacks}}{\text{Total Actual Attacks}} \times 100\% \quad (11)$$

Figure 1 shows how the first 50 vehicles were deployed in a 1000 m x 1000 m simulation area. The random waypoint mobility model was used to simulate the vehicles with mobility speeds of 20 to 80 km/h. The vehicles moved incessantly for a period of 300 seconds in the simulation. The continuous motion was intended to model the shifting connection topology in a real-world vehicular network. This feature assesses the applicability of the proposed authentication system, trust management, intrusion detection, and routing in a scenario of changing network connectivity.

Table 3 outlines the simulation parameters used in the performance evaluation of the proposed framework. This includes the B-based implementation, network design, mobility model, vehicle density, packet load, and the length of the simulation.

The experiment was carried out using a model VANET comprising five vehicles, which were represented by IDs from VID_A to VID_E. The simulated entries in the Blockchain are listed in Table 4, whereby each unique VID is assigned a unique ECC public key.

The vehicle creates an alert message that carries appropriate metadata whenever it senses something noteworthy, like a crash or an obstacle on the road. As indicated in Table 5, the generated secure message would consist of the VID, signature, payload, and

time stamp. This packet can now be sent directly to adjacent vehicles or an RSU in the vicinity through the 5G communication system.

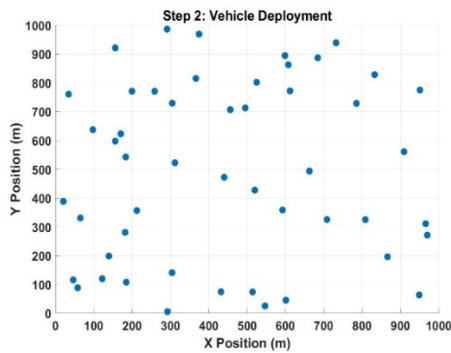


Figure 2: Vehicle Deployment

Table 3: Simulation environment

Parameter	Value
Simulation Tool	MATLAB R2024a Custom Script
Network Type	5G-enabled VANET
Mobility Model	Random Waypoint Mobility Model
Simulation Area	1000 m × 1000 m
Vehicles	50
Packets	5000
Speed Range	20–80 km/h
Simulation Time	300 s

Table 4. Simulated Blockchain Ledger

VID	PubKey_X
VID_7430_ELZH	8D54749AB0EA4467C73DDDCBB34FC6F03E84C231CF6F5DD5AE50BC5715127EA30
VID_3976_UZIS	99FFE4F4DC34911B1E9B80A0F914A38F9E1055B72902BAA843C5D7FD4DE51D4
VID_4598_CORT	E4BC9FBCCE7E4ADDF071068DC3BDC91C0AAF4D2D8E860B6579C0861C5024
VID_6760_DMMU	25FDB6B5051BD04385C380E0BA23ED912A51FB7850DEF2A5123C0646F9D0907
VID_6752_OWEZ	DBF1349C5FF65311FACD7DE3C2A46F22D5500165D832C5D1EA705E783B1AF09

Table 5. Generated Packets

Field	Value
VID_A	VID_7430_ELZH
Signature	4b2ae2345869c421d8e17e75ea7c9e8804c855cdacc4f620f36228413becb04a
EncryptedMsg	04ab9452af72bbe2da8935cd45edca992118699f83eb0e246ac7ba8cfc0664ed52f1fb0aca0043d1c472f3d35c2c89be2d65da5f4
Timestamp	2025-07-16 17:43:54

When the destination node receives a packet, the first thing that happens is that it looks up the Sender's VID to get the corresponding public key from the Blockchain, as seen in Table 6 below. Messages from vehicles that have a low trust score are discarded despite having proper signatures. However, trusted cars such as VID_6752_OWEZ are allowed without any issues.

Table 6. Signature Verification and Trust Check

S. No	Vehicle ID	Signature Validity	Trust Score	Action Taken
1	VID_7430_ELZH	Valid	4	Message Ignored
2	VID_3976_UZIS	Valid	8	Message Accepted
3	VID_4598_CORT	Invalid	-	Message Rejected
4	VID_6760_DMMU	Valid	3	Message Ignored
5	VID_6752_OWEZ	Valid	9	Message Accepted

Table 7 demonstrates trust scores that are updated in real time to show the punishment on the score for exhibiting any suspicious or malevolent behaviour. This system is both dynamic and transparent, so a trust score can be restored by engaging in legitimate activities rather than punitive behaviour.

Table 7. Update of Trust Score and Anomaly Detection.

S. No	Vehicle ID	Trust Score		Actions
		Previous	Updated	
1	VID_7430_ELZH	5	3	Suspicious activity detected → Trust score penalized
2	VID_3976_UZIS	7	7	No anomaly detected → Trust maintained
3	VID_4598_CORT	6	4	Minor irregularity → Trust slightly reduced
4	VID_6760_DMMU	8	5	False message detected → Trust penalized
5	VID_6752_OWEZ	9	9	Clean behaviour → No change
6	VID_1234_XYZQ	4	2	Repeated suspicious packets → Severe penalty

Figure 2 shows that throughput initially increases, reaching a maximum of 9 Mbps when the number of packets is 4000. The improvement is due to more efficient processing of higher data amounts due to better cryptography and routing schemes.

As shown in Figure 3, there is a clear downward trend in latency as packet count increases. Between 500 and 3000 packets, the latency reduced from 0.028 seconds to 0.021 seconds. For 3000 to 5000 packets, latency remained constant at 0.021 seconds. From this, we can deduce that the framework handles rising communication demands with minimal transmission delays. Thus, the framework is tailored for 5G-based, real-time, VANET applications.

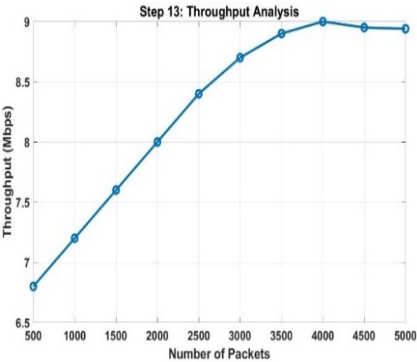


Figure 2. Throughput analysis

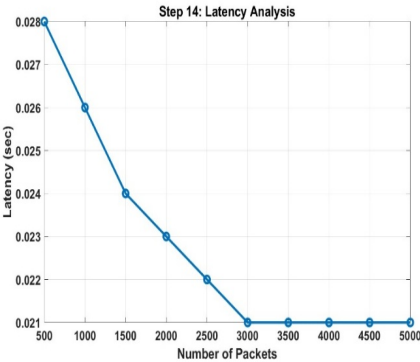


Figure 3. Latency analysis

After the 50 packets onwards, there would be an increase in latency, which then remained steady at 0.033 seconds. The cause of this small increase in latency is due to queuing delays and the increase in cryptographic workload, particularly when there are extensive signature verification processes and blockchain lookup operations going on.

The proposed framework demonstrates reliable communication performance and secure message dissemination in the evaluated 5G-enabled VANET scenario. As can be seen from Table 8, out of 5000 transmitted packets, 4725 were delivered successfully,

thus resulting in 94.5% of Packet Delivery Ratio (PDR), indicating successful delivery of the majority of transmitted packets. In addition, the system maintained an average throughput rate of 8.94 Mbps and had a very low latency of 0.021 seconds for data transfer. The authentication took merely 0.003 seconds on average.

Comparative analysis. Figure 4 compares the communication cost of the proposed framework and existing VANET authentication schemes by results in [7, 23-26]. The proposed framework communication cost was 96 bytes, which is better than the 124, 108, 237, 772, and 544-byte costs of the compared systems. The proposed framework has lower communication costs and provides ECC-based authentication, blockchain-based identity management, trust assessment, and intrusion detection services. The proposed framework achieves the right mix of security and communication cost and is therefore appropriate for 5G-enabled VANET systems that are real-time.

Table 8. Performance results of the suggested mechanism

Metrics	Value
Total Packets Simulated	5000
Successful Deliveries	4725
Average Throughput	8.94 Mbps
Average Latency	0.021 sec
Average Authentication Time	0.003 sec
Packet Delivery Ratio	94.5%
Attack Detection Rate	98.8%
Trust Accuracy (≥ 5 Score)	91.3%
Communication Cost	96 bytes

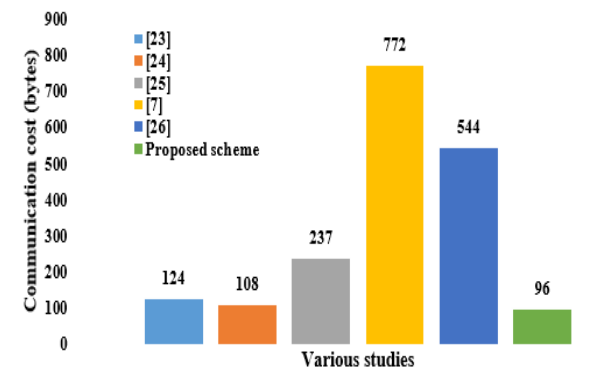


Figure 4. Comparison with existing approaches

5. CONCLUSION AND FUTURE SCOPE

The suggested scheme proves highly efficient in providing a possible remedy for the critical issues facing reliable and secure data dissemination in 5G-equipped VANET systems. This system integrated ECC-enabled authentication, AES encryption, blockchain-powered trust management, and the use of an intrusion detection system based on the network edge. The simulation results prove the efficiency of the suggested scheme, where the PDR is 94.5%, throughput averages 8.94 Mbps, and the latency time is 0.021 seconds. Even though the average communication overhead is 96 bytes per transaction, this approach proves far more effective and secure. The future research could focus on incorporating machine learning algorithms for trust models to improve dynamic threat detection and trust accuracy.

REFERENCES

[1] Petrov, T., Sevcik, L., Pocta, P., Dado, M. A performance benchmark for dedicated short-range communications and LTE-based cellular-V2X in the context of vehicle-to-infrastructure communication and urban scenarios. *Sensors*, vol.21, no.15, 2021, Article 5095.

[2] Mir, Z.H., Toutouh, J., Filali, F., Ko, Y.-B. Enabling DSRC and C-V2X integrated hybrid vehicular networks: Architecture and protocol. *IEEE Access*, vol.8, 2020, pp. 180909-180927.

- [3] Arif, M., Wang, G., Geman, O., Balas, V.E., et al. SDN-based VANETs, security attacks, applications, and challenges. *Applied Sciences*, vol.10, no.9, 2020, Article 3217.
- [4] Jiang, Y., Ge, S., Shen, X. AAAS: An anonymous authentication scheme based on group signature in VANETs. *IEEE Access*, vol. 8, 2020, pp. 98986-98998.
- [5] Verma, G.K., Chamola, V., Tiwari, et al. Escrow-free and efficient dynamic anonymous privacy-preserving batch verifiable authentication scheme for VANETs: *Ad Hoc Networks*, vol.166, 2025, Article 103670.
- [6] Sheik, A.T., Liu, J., Dianati, M., Maple, C. Comparative evaluation of pseudonym-based anonymisation techniques for connected autonomous vehicles (CAVs). *Frontiers in Future Transportation*, vol.6, 2025, Article 1519759.
- [7] Abbood, A.A., Al-Shammri, F.K., Alzamili, Z.M., et al. Secure and efficient mutual authentication protocol for VANETs using edge computing and signature-based cryptography. *Journal of Robotics and Control (JRC)*, vol.6, no.2, 2025, pp. 649-659.
- [8] Du, Q., Zhou, J., Ma, M. EAIA: An efficient and anonymous identity-authentication scheme in 5G-V2V. *Sensors*, vol.24, no.16, 2024, Article 5376.
- [9] Thiruppathy Kesavan, V., Murugavalli, S., Premkumar, M., Selvarajan, S. Adaptive neuro-fuzzy inference system and particle swarm optimization: A modern paradigm for securing VANETs. *IET Communications*, vol.17, no.19, 2023, pp. 2219-2236.
- [10] Mirzaee, P.H., Shojafar, M., Bagheri, H., Chan, T.H., Cruickshank, H., Tafazolli, R. A two-layer collaborative vehicle-edge intrusion detection system for vehicular communications. *2021 IEEE 94th Vehicular Technology Conference (VTC2021-Fall)*, 2021, pp. 1-6.
- [11] Cao, Y., Xu, S., Chen, X., He, Y., Jiang, S. A forward-secure and efficient authentication protocol through lattice-based group signature in VANETs scenarios. *Computer Networks*, vol.214, 2022, Article 109149.
- [12] Farooqi, A.M., Alam, M.A., Hassan, S.I., Idrees, S.M. A fog computing model for VANET to reduce latency and delay using 5G network in smart city transportation: *Applied Sciences*, vol.12, no.4, 2022, Article 2083.
- [13] Al-Shareeda, M.A., Manickam, S., Mohammed, B.A., Al-Mekhlafi, Z.G., Qtaish, A., Alzahrani, A.J., Alshammari, G., Sallam, A.A., Almekhlafi, K. Provably secure with efficient data sharing scheme for fifth-generation (5G)-enabled vehicular networks without roadside unit (RSU). *Sustainability*, vol.14, no.16, 2022, Article 9961.
- [14] Gupta, N., Manaswini, R., Saikrishna, B., Silva, F., Teles, A. Authentication-based secure data dissemination protocol and framework for 5G-enabled VANET. *Future Internet*, vol.12, no.4, 2020, Article 63.
- [15] El-Shafai, W., Azar, A.T., Ahmed, S., AI-driven ensemble classifier for jamming attack detection in VANETs to enhance security in smart cities. *IEEE Access*, 2025.
- [16] Ganeshkumar, N., Kumar, S. OBU (on-board unit) wireless devices in VANET(s) for effective communication – A review. *Computational Methods and Data Engineering: Proceedings of ICMDE 2020*, vol.2, 2020, pp. 191-202.
- [17] Kim, D., Velasco, Y., Wang, W., Uma, R.N., Hussain, R., Lee, S. A new comprehensive RSU installation strategy for cost-efficient VANET deployment. *IEEE Transactions on Vehicular Technology*, vol.66, no.5, 2016, pp. 4200-4211.
- [18] Izaguirre Diaz, I. Decentralized application (dApp) on the VeChainThor blockchain for business processes: *Master's Thesis*, University of South-Eastern Norway, 2024.

- [19] Genç, Y., Afacan, E. Design and implementation of an efficient elliptic curve digital signature algorithm (ECDSA). *2021 IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS)*, 2021, pp. 1-6.
- [20] Appel, A.W. Verification of a cryptographic primitive: SHA-256. *ACM Transactions on Programming Languages and Systems (TOPLAS)*, vol.37, no.2, 2015, pp. 1-31.
- [21] Farouk, F., Alkady, Y., Rizk, R. Efficient privacy-preserving scheme for location-based services in VANET system. *IEEE Access*, vol.8, 2020, pp. 60101-60116.
- [22] Tomandl, A., Fuchs, K.-P., Federrath, H. REST-Net: A dynamic rule-based IDS for VANETs. *7th IFIP Wireless and Mobile Networking Conference (WMNC)*, 2014, pp.1-8.
- [23] Ali, I., Lawrence, T., Li, F. An efficient identity-based signature scheme without bilinear pairing for vehicle-to-vehicle communication in VANETs—*Journal of Systems Architecture*, vol.103, 2020, Article 101692.
- [24] Alazzawi, M.A., Lu, H., Yassin, A.A., Chen, K. Efficient conditional anonymity with message integrity and authentication in a vehicular ad-hoc network. *IEEE Access*, vol.7, 2019, pp. 71424-71435.
- [25] Bayat, M., Barmshoory, M., Pournaghi, S.M., Rahimi, M., Farjami, Y., Aref, M.R. A new and efficient authentication scheme for vehicular ad hoc networks. *Journal of Intelligent Transportation Systems*, vol.24, no.2, 2020, pp. 171-183.
- [26] Alzaidi, Z.S., Yassin, A.A., Abduljabbar, Z.A., Nyangaresi, V.O. A fog computing and blockchain-based anonymous authentication scheme to enhance security in VANET environments. *Engineering, Technology & Applied Science Research*, vol.15, no.1, 2025, pp. 19143-19153.

Information about the authors:

Anupama Verma - Anupama Verma is a PhD research scholar in the Department of Computer Science and Engineering at Teerthanker Mahaveer University with over 5.5 years of academic and professional experience. Her research interests include Internet of Things (IoT) Security, Data Authenticity, Cryptographic Protocols, Secure Communication, and emerging trends in management studies. She possesses technical proficiency in Excel and SQL and has actively contributed to academic research and scholarly publications. Her current research focuses on analytical and management-based applications aimed at bridging the gap between theoretical concepts and practical implementation. Alongside research, she is passionate about teaching, academic development, and interdisciplinary learning.

Prof. (Dr.) Gulista Khan - Prof. (Dr.) Gulista Khan is a Professor in the Department of Computer Science & Engineering at Teerthanker Mahaveer University, with over 19 years of academic and industry experience. She holds a Ph.D. in Computer Science & Engineering and specialises in Security and Cryptography. Her research interests include Cyber Security, Cryptographic Protocols, Internet of Things (IoT) Security, Data Authenticity, Wireless Sensor Networks, and Secure Communication Frameworks. She has published several research papers in reputed national and international journals and conferences, contributing significantly to advancements in secure and intelligent computing systems.

Manuscript received on 15 May 2026