

Joint Minimax Optimization of Privacy-Preserving Authentication and Communication Overhead in Secure Vehicle-to-Edge Networks

Rekha M R¹, Dr Neelambike S²

¹Research Scholar, Department of Computer Science and Engineering, GM University, Davangere, Karnataka, India. rekhasadashiv_12@rediffmail.com

²Associate professor and head, Department of information science and engineering, GM University, Davanagere, India

Abstract

Internet of Vehicles (IoV) for provisioning Intelligent Transportation Systems (ITS) in Vehicular Ad Hoc Networks (VANETs) emphasized secure communication ensuring privacy-constraint of vehicle users among vehicles name as Vehicle-to-Vehicle (V2V) and among the infrastructure name as Vehicle-to-Infrastructure (V2I) communication. However, with the increase of vehicle density, congested urban roads, high-speed highway and open wireless nature, it is vulnerable to a wider range of network attacks. Existing security mechanisms in providing lightweight security mechanisms employed trust based authentication. However, these methods induce high network overhead and high latency for trust validation. This work addresses the research limitations by presenting a privacy preserving-aware authentication (PPA) algorithm with novel trust metrics, which guarantees lower latency and overhead, thus ensuring better security and improving the overall network performance requirement of ITS. The experiment is performed in complicated propagation environments, showing that PPA outperforms the baselines in terms of network performance satisfying the requirement of ITS.

Keywords: VANET, IoV, Intelligent Transportation Systems, Trust Management, Secure Authentication, V2I Communication

1. Introduction

With the rapid development of connected vehicles, autonomous driving technologies, and smart mobility services, Intelligent Intelligent Transportation Systems (ITS) have become an important research field [1]. In such an environment, Vehicular Ad Hoc Networks (VANETs) and Internet of Vehicles (IoV) enable the constant exchange of information among vehicles, roadside infrastructure, edge nodes and cloud platforms through Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) communication [2]. These communication mechanisms have important roles in various critical functions in ITS such as traffic optimization, accident prevention, emergency response, route planning, and real-time transportation monitoring [3]. However, although vehicular communication has some benefits, it is exposed to risks because of the open and dynamic nature of the wireless environment through which vehicles operate. Vehicles regularly exchange safety messages when working in a highly mobile environment and traffic with varying densities. In the process, there is risk of security threats like replay attacks, Sybil attacks, impersonation, packet manipulation, packet dropping, and false message spreading. Such challenges make it important for vehicular communication to be authentic and have trust adaptability [3], [4].

Current authentication methods depend mostly on centralized architecture-based systems, PKI-based systems [5], [6], certificateless cryptography systems [7], [8], and static trust management [9], [10]. Although such methods help enhance security in communication, they often result in issues like authentication delay, communication overhead, scalability problems, and reliance on centralized systems [11]. Other solutions that have been suggested lately include block chain-based authentication and trust evaluation, machine learning based trust management, lightweight cryptography models, and adaptive security mechanisms. However, the existing methods are faced with various issues like dynamic trust adaptability, malice behavior prediction, and communication consistency [12].

To tackle these challenges, this work presents a Privacy-Preserving Authentication (PPA), a dynamic trust-aware authentication framework for secure V2V and V2I communication. The proposed approach combines adaptive trust learning, reputation validation, communication consistency analysis, historical trust assessment, future trust prediction, and malicious vehicle isolation to enhance authentication reliability. PPA can detect malicious vehicles rapidly and the quality of communication is stable at the same time. The trust value is

updated continuously according to the communication behavior and packet forwarding performance. The main contributions are adaptive reputation management, integrated direct and indirect trust evaluation, communication reliability assessment, malicious behavior detection and secure authentication validation. The experimental evaluation on the CICIoV2024 dataset shows better throughput, higher packet success rate, lower packet failure and better attack detection capability in different vehicle densities and communication scenarios. The remainder of this manuscript is organized as follows. Section 2 describes architecture of PPA and working of PPA. Section 3 discusses the experimental setup, dataset description, and performance evaluation. Finally, Section 4 concludes the work and outlines future research directions.

2. Methodology

This section proposes a new security model called privacy-preserving-aware authentication (PPA) scheme, which is illustrated in Figure 1. The PPA scheme uses different trust factors to provide security in provisioning ITS in the IoV network. The full operation of the PPA scheme is explained step by step in Algorithm 1. The main objective of the PPA algorithm is to provide secured V2V/V2I communication as the vehicle/RSU and edge server constantly receives vital safety data from highly mobile vehicles. As such, any communication requests pass through various trust checks before authentication can be performed.

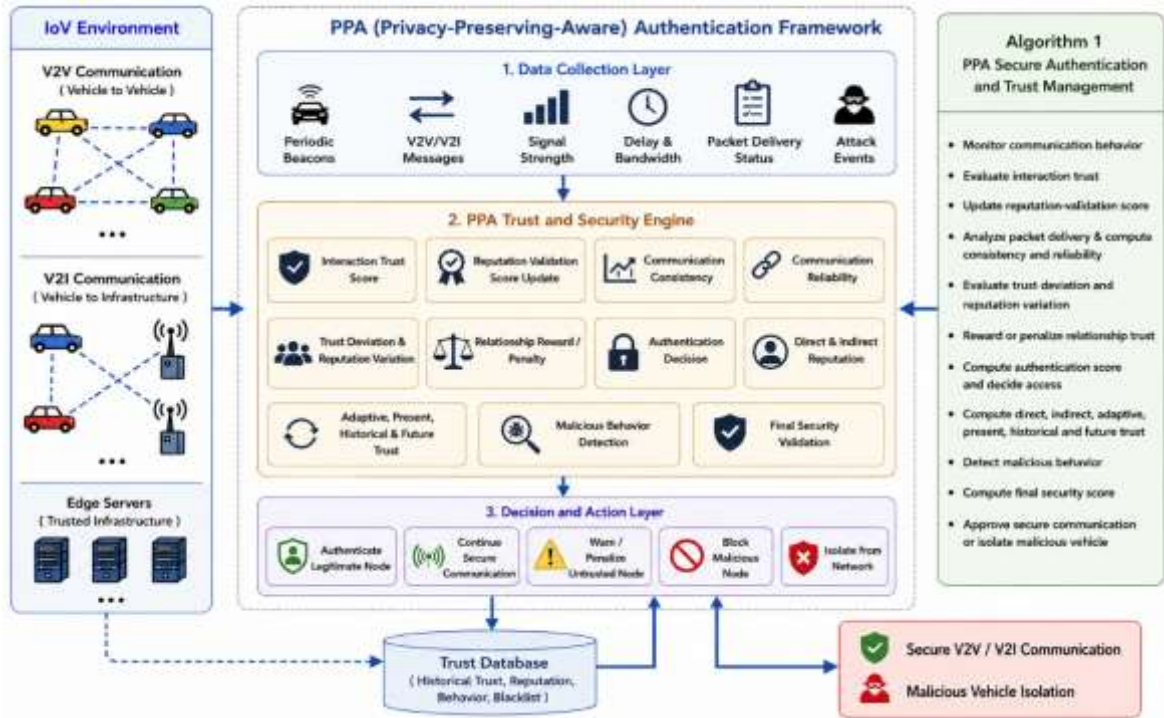


Figure 1. Overall Architecture of privacy preserving-aware authentication model.

Algorithm 1. PPA secure authentication and trust management	
Input	Vehicle node x , vehicle node/RSU y , neighbor vehicle set $\mathcal{H}(x, y)$, communication interval u , interaction duration o
Output	Secure authentication decision, trust score update, malicious detection
Step 1	Start
Step 2	Initialize x , y and trust database. Set interaction duration o and communication interval u
Step 3	Load previous trust values
Step 4	Initialize packet counters, i.e., $P_s(x, y) = 0$ and total packets $P_t(x, y) = 0$
Step 5	Monitor communication behavior between x and y
Step 6	Evaluate interaction trust score using $\text{Sec}_{\text{rec}} = \begin{cases} 0, & \text{if connection is completely untrustable} \\ 1, & \text{if connection is completely trustable} \\ \in (0,1), & \text{otherwise} \end{cases}$
Step 7	Compute updated reputation-validation score using $\text{Sec}_o^u(x, y) = \gamma * \text{Sec}_{\text{rec}}(x, y) + (1 - \gamma) * \text{Sec}_{o-1}^u(x, y)$

Step 8	Store updated reputation score
Step 9	While communication-active == True do For each packet transmission do Increment total transmitted packet counter as $P_t(x, y) = P_t(x, y) + 1$ If packet successfully received Increment successful packet counter as $P_s(x, y) = P_s(x, y) + 1$ Else Mark packet transmission failure End If End For Compute communication consistency score using $\psi_o^u(x, y) = \frac{P_s(x, y)}{P_t(x, y)}$ Measure communication bandwidth $B(x, y)$ Measure transmission delay $D(x, y)$ Compute communication reliability using $\Omega_o^u(x, y) = \frac{\psi_o^u(x, y) \times B(x, y)}{D(x, y)}$ For each neighboring vehicle p do Compute trust deviation $(\text{Sec}_o^u(x, p) - \text{Sec}_o^u(u, p))^2$ Store deviation values End for Compute reputation variation score using $V_o^u(x, y) = \sqrt{\frac{\sum_{p \in \mathcal{H}} (\text{Sec}_o^u(x, p) - \text{Sec}_o^u(y, p))^2}{ \mathcal{H}(x, y) }}$ If $V_o^u(x, y) < \mathcal{H}$ then Reward relationship trust using $\mathbb{R}_o^u(x, y) = \begin{cases} \mathbb{R}_{o-1}^u(x, y) + \frac{1 - \mathbb{R}_{o-1}^u(x, y)}{x}, & \text{if } V_o^u(x, y) < \mathcal{H} \\ \mathbb{R}_{o-1}^u(x, y) - \frac{1 - \mathbb{R}_{o-1}^u(x, y)}{y}, & \text{otherwise} \end{cases}$ Else Penalize relationship trust using $\mathbb{R}_o^u(x, y) = \begin{cases} \mathbb{R}_{o-1}^u(x, y) + \frac{1 - \mathbb{R}_{o-1}^u(x, y)}{x}, & \text{if } V_o^u(x, y) < \mathcal{H} \\ \mathbb{R}_{o-1}^u(x, y) - \frac{1 - \mathbb{R}_{o-1}^u(x, y)}{y}, & \text{otherwise} \end{cases}$ End if If $V_o^u(x, y) > \theta$ then Compute authentication score using $\mathbb{F}_o^u(x, y) = \begin{cases} 1 - \frac{\log(\text{Sec}_o^u(x, y))}{\log \theta}, & \text{if } \mathbb{R}_o^u(x, y) > \theta \\ 0, & \text{else} \end{cases}$ Authenticate vehicle Else Reject communication request End If Compute direct reputation using $\mathbb{L}_o^u(x, y) = \text{Sec}_o^u(x, y)$ If $Z - \{x\} > 0$ then Compute indirect reputation using $\mathbb{G}_o^u(x, y) = \begin{cases} \frac{\sum_{p \in Z - \{x\}} \mathbb{F}_o^u(x, p) * \mathbb{L}_o^u(x, y)}{\sum_{p \in Z - \{x\}} \mathbb{F}_o^u(x, p)}, & \text{if } Z - \{x\} > 0 \\ 0, & \text{if } Z - \{x\} = 0 \end{cases}$ Else Set indirect reputation End If Compute adaptive reputation using $\delta = \frac{T^u(x, y)}{T^u(x, y) + \bar{T}^u(x, y)}$ Compute neighboring interaction average using $\bar{T}^u(x, y) = \frac{\sum_{p \in Z - \{x\}} \mathbb{F}_o^u(x, p) * T^u(p, y)}{ Z - \{x\} }$ Compute present reputation using $\mathbb{C}_o^u(x, y) = \delta * \mathbb{L}_o^u(x, y) + (1 - \delta) * \mathbb{G}_o^u(x, y)$ Compute historical reputation using $\mathbb{H}_o^u(x, y) = \frac{\varphi * \mathbb{H}_{o-1}^u(x, y) + \mathbb{C}_{o-1}^u(x, y)}{2}$ Compute future trust prediction using $\mathbb{F}_o^u(x, y) = \begin{cases} 0, & \text{if neither } \mathbb{L} \text{ or } \mathbb{C} \text{ is available} \\ \alpha \mathbb{C}_o^u(x, y) + (1 - \alpha) \mathbb{L}_o^u(x, y), & \text{if either } \mathbb{L} \text{ or } \mathbb{C} \text{ is available} \end{cases}$

	Update adaptive parameter α using $\alpha = \begin{cases} \alpha + 0.1, & \text{if } \mathbb{C}_0^u(x, y) - \mathbb{L}_0^u(x, y) > \omega \\ \alpha - 0.1, & \text{if } \mathbb{C}_0^u(x, y) - \mathbb{L}_0^u(x, y) < -\omega \\ \alpha, & \text{if } -\omega < \mathbb{C}_0^u(x, y) - \mathbb{L}_0^u(x, y) < \omega \end{cases}$
	If $\mathbb{C}_0^u(x, y) - \mathbb{L}_0^u(x, y) > \Omega$ then
	$\alpha = \alpha + 0.1$
	Else if $\mathbb{C}_0^u(x, y) - \mathbb{L}_0^u(x, y) < \Omega$ then
	$\alpha = \alpha - 0.1$
	Else
	$\alpha = \alpha$
	End If
	Compute malicious behavior score using $\mathbb{D}_0^u(x, y) = \begin{cases} \mathbb{D}_{0-1}^u(x, y) + \frac{\mathbb{C}_0^u(x, y) - \mathbb{L}_0^u(x, y)}{\rho}, & \text{if } \mathbb{C}_0^u(x, y) - \mathbb{L}_0^u(x, y) > \tau \\ \mathbb{D}_{0-1}^u(x, y) + \mathbb{L}_0^u(x, y) - \mathbb{C}_0^u(x, y), & \text{if } \mathbb{C}_0^u(x, y) - \mathbb{L}_0^u(x, y) > -\tau \\ \mathbb{D}_{0-1}^u(x, y), & \text{otherwise} \end{cases}$
	If $\mathbb{D}_0^u(x, y) > \text{malicious}_{\text{threshold}}$ then
	Mark vehicle as malicious
	Block communication access
	Else
	Continue secure communication
	End if
	Compute final security score using $\mathcal{F}_0^u(x, y) = \mathbb{F}_0^u(x, y) * \mathbb{D}_0^u(x, y)$
	If $\mathcal{F}_0^u(x, y) < \text{security}_{\text{threshold}}$ then
	Reject authentication request
	Isolate malicious vehicle
	Else
	Approve secure V2V/V2I communication
	End If
	End while
Step 10	End communication process

he proposed PPA secure authentication and trust management algorithm aims to provide adaptive and dependable security for V2V and V2I communication through continuous trust assessment and malicious vehicle identification. First, the vehicle node x , vehicle/RSU node y , communication intervals, trust records and packet monitoring variables are initialized to set up a secure communication environment. The algorithm continuously monitors the interaction behavior between communicating entities and computes trust values to keep updated reputation information once the communication is initiated. Packet transmission activities are then observed to determine communication consistency and reliability based on successful packet delivery, bandwidth conditions and transmission delay. This process ensures the stable communication performance and also helps to achieve the higher throughput and better packet delivery success. Moreover, the framework analyzes the trust deviation and reputation variation among neighboring vehicles to enhance authentication accuracy. The evaluations result in dynamic rewarding or punishing of trust relationships before authentication decisions are made. This mechanism also integrates direct interactions and indirect recommendations to produce adaptive, present, historical and predictive trust assessments. Finally, abnormal behavior patterns are analyzed for detection of malicious vehicles and decision of whether to continue or block communication. PPA proposes dynamic trust adaptation and security validation to realize scalable, secure, and reliable vehicular authentication, and improve communication reliability and attack resilience in intelligent transportation systems.

3. Results And Discussion

Evaluation of the PPA (Privacy Preserving Authentication) scheme was conducted under realistic vehicular communication scenarios in order to analyze its capacity for providing secure and reliable authentication services between both V2V and V2I communications. In order to provide an impartial comparison of both schemes, simulation parameters were set in a similar manner to that of the LDSAV [8] study, and carried out using the SIMITS simulator which was designed in C# [13], [14]. The experiments utilized the CICIoV2024 dataset [15], [16] which comprises of legal vehicular interaction scenarios, malicious communication, different types of traffic, and various types of attacks. The throughput comparison between PPA and LDSAV in the complex environment under different densities of vehicles is depicted in Fig. 2. It can be seen from the figure that PPA always performs better than LDSAV under different situations. Though throughput decreases when

the number of vehicles increases due to the contention in communication and channel usage, PPA shows stability and efficient packet transmission.

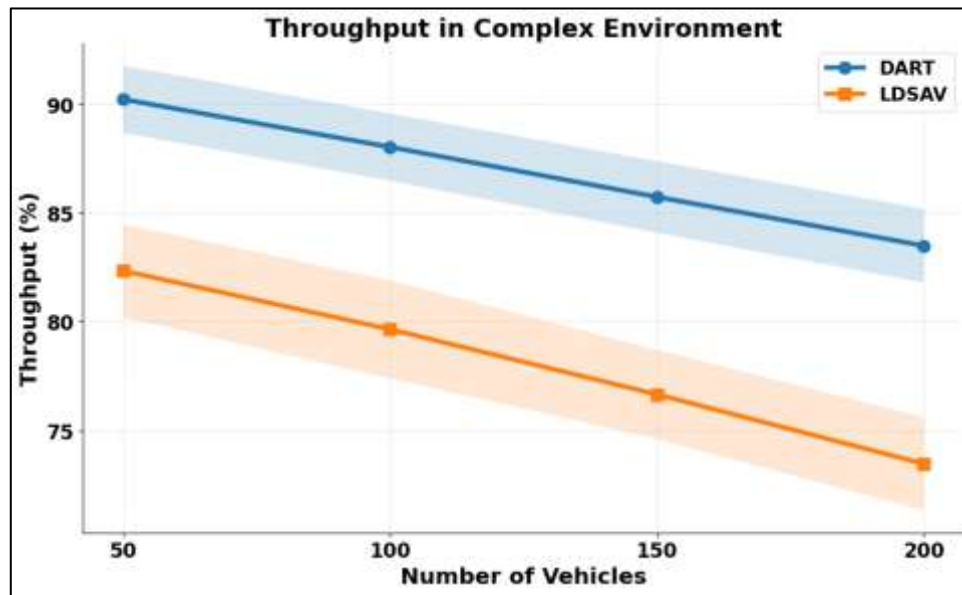


Figure 2. Throughput comparison of PPA and LDSAV in complex mobility and radio propagation environment.

The packet success rate of both algorithms in the complex environment is shown in Fig. 3. PPA shows better packet delivery rate compared to LDSAV. This implies that PPA shows high reliability of communication and supports efficient authentication [17], [18]. Packet failure rate is shown in Fig. 4. It can be seen from the figure that the failure rate of packets increases for both algorithms in the complex environment when the number of vehicles increases [19],[20], [21]. However, PPA shows considerably lower failure rates than LDSAV, which implies the robustness and efficiency of PPA.

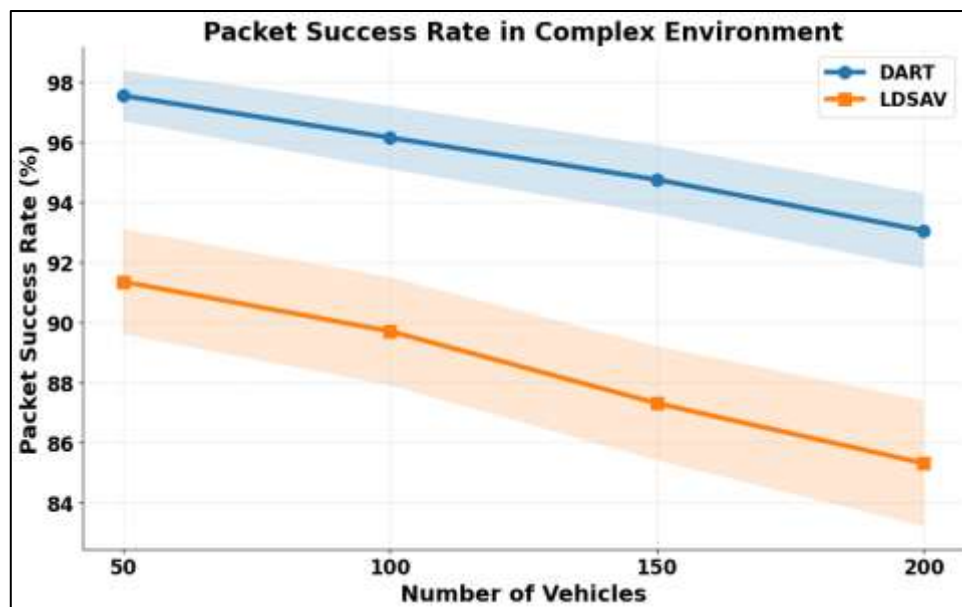


Figure 3. Packet success rate comparison of PPA and LDSAV in complex mobility and radio propagation environment.

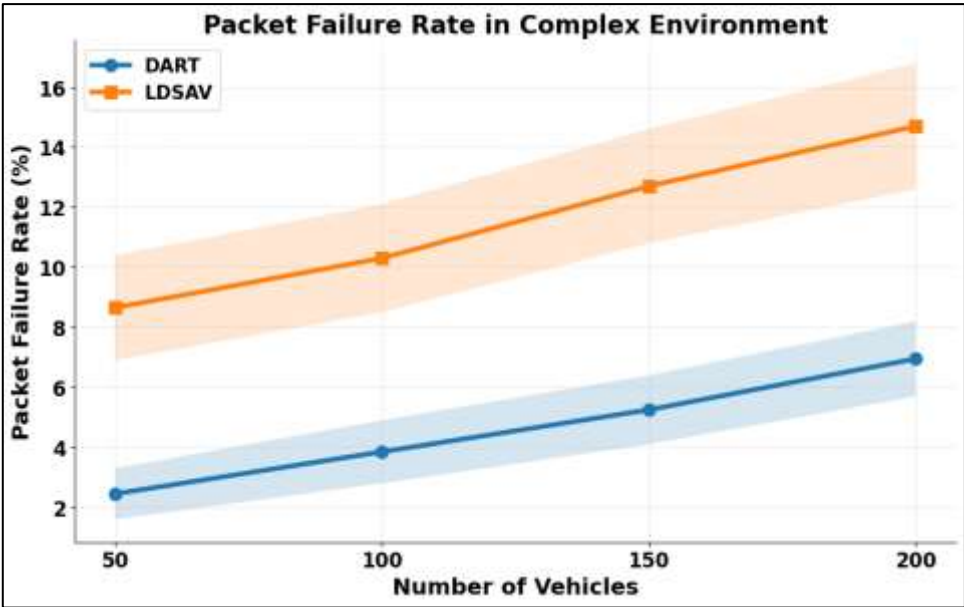


Figure 4. Packet failure rate comparison of PPA and LDSAV in complex mobility and radio propagation environment.

The experimental results reveal that PPA outperforms LDSAV in terms of communication reliability and authentication efficiency in the complex vehicular environment. Better scalability and stronger resilience of the communication are demonstrated by increased throughput and packet success rates and decreased packet failure rates [22],[23],[24]. The variation of the performance control with the increasing vehicle densities indicates that PPA is able to adapt to the dynamic network conditions while ensuring stable and secure vehicular communication [25], [26], [27].

4. Conclusion

The work introduced PPA, a privacy-preserving authentication and trust management framework, to improve the security and reliability of V2V and V2I communication in intelligent transportation systems. The proposed approach integrates continuous trust evaluation, communication reliability assessment, adaptive reputation modeling and malicious behavior detection to promote dynamic authentication decisions in highly mobile IoV environments. With this combination of direct interactions, historical trust information and predictive trust adaptation, PPA enhances the stability of communication and reduces the influence of malicious nodes. Experimental results demonstrated that the proposed framework outperforms the baseline approach in terms of higher throughput, higher packet delivery success, lower packet failure and attack resistance under different vehicle densities. Despite promising performance of the proposed framework, future work will focus on extending PPA for large-scale real-time vehicular deployments and heterogeneous network environments. Lightweight blockchain integration, federated learning based trust optimization, energy-aware authentication strategies, and validation under emerging 6G-enabled ITS scenarios are expected to improve scalability, privacy preservation and communication efficiency further.

ACKNOWLEDGEMENT

I would like to express our sincere gratitude to all those who have supported and contributed to this research project. Primarily, I extend our heartfelt thanks to our guide for his unwavering guidance, invaluable insights, and encouragement throughout the research process. No funding is raised for this research.

FUNDING INFORMATION

No funding is raised for this research.

AUTHOR CONTRIBUTIONS STATEMENT

Name of Author	C	M	So	Va	Fo	I	R	D	O	E	Vi	Su	P	Fu
Rekha M R	✓	✓	✓	✓	✓	✓		✓	✓	✓			✓	
Dr Neelambike S	✓	✓	✓	✓	✓	✓	✓		✓	✓	✓		✓	✓

C: Conceptualization	I : Investigation	Vi : Visualization
M : Methodology	R: Resources	Su : Supervision
So : Software	D : Data Curation	P : Project administration
Va : Validation	O : Writing - Original Draft	Fu : Funding acquisition
Fo : Formal analysis	E: Writing - Review & Editing	

CONFLICT OF INTEREST

The Author declares no conflict of interest.

DATA AVAILABILITY

The dataset is utilised in this research, reference [15].

REFERENCES

- [1] Y. Li, Y. Xie, Q. Liu and J. Li, "DMTAS-VB: Dynamic Model Update-Based Trust Assessment Strategy for VANETs Considering Blockchain," in *IEEE Internet of Things Journal*, vol. 12, no. 10, pp. 14691-14708, 15 May15, 2025, doi: 10.1109/JIOT.2025.3527119.
- [2] A. Gupta and A. K. Sagar, "An Extensive Study on the State-of-the-Art Literature to Identify Major Approaches and Trust Issues of Trust-based Models in VANETs," in *Journal of Mobile Multimedia*, vol. 21, no. 3-4, pp. 429-446, July 2025, doi: 10.13052/jmm1550-4646.21345.
- [3] P. Surapaneni, S. Bojjagani and M. Khurram Khan, "DYNAMIC-TRUST: Blockchain-Enhanced Trust for Secure Vehicle Transitions in Intelligent Transport Systems," in *IEEE Transactions on Intelligent Transportation Systems*, vol. 26, no. 7, pp. 10918-10932, July 2025, doi: 10.1109/TITS.2025.3545755.
- [4] P. Das et al., "Mutual Authentication and Trust Establishment (MATE) Protocol in VANET Using Puncturable Pseudorandom Function (PPRF): MATE-PPRF," in *IEEE Transactions on Intelligent Transportation Systems*, vol. 26, no. 9, pp. 13293-13305, Sept. 2025, doi: 10.1109/TITS.2025.3589123.
- [5] C. Liu, H. Wei, Z. Xue, J. Kang, X. Xu and G. Han, "Cybertwin-Enhanced Distributed Authentication with Lightweight Cryptography for Secure Internet of Vehicles," in *IEEE Transactions on Vehicular Technology*, Jan. 2026, doi: 10.1109/TVT.2026.3654936.
- [6] A. Kumar, M. Malhotra, A. Anjali and A. S. Yadav, "A Low-Latency Post-Quantum Group Authentication Framework for VANETs," in *IEEE Networking Letters*, vol. 8, pp. 125-129, Feb. 2026, doi: 10.1109/LNET.2026.3666683.
- [7] S. S. Voon et al., "Trust management in the internet of vehicles: a survey of learning-based mechanisms," *Journal of King Saud University - Computer and Information Sciences*, vol. 38, no. 4, Feb. 2026, doi: 10.1007/s44443-026-00554-4.
- [8] Y. Zhao et al., "LDSAV: Lightweight and Dynamically Scalable Authentication Key Agreement for Vehicle-Cloud Collaboration," in *IEEE Transactions on Vehicular Technology*, Mar. 2026, doi: 10.1109/TVT.2026.3669949.
- [9] S. Srivastava, D. Agarwal and B. K. Chaurasia, "Secure Communication using Blockchain in Vehicular Sensor Network," in *IEEE Sensors Journal*, Apr. 2026, doi: 10.1109/JSEN.2026.3678320.
- [10] S. Guo, D. Huang, C. Ki Ahn, Y. Zhou and J. Song, "Monitoring Intelligent Connected Vehicles: Embedding Trust Levels in Status Within Zero-Trust Network Architecture," in *IEEE Transactions on Intelligent Transportation Systems*, vol. 27, no. 5, pp. 5250-5262, May 2026, doi: 10.1109/TITS.2026.3651533.
- [11] S. Ahmed, N. Tariq, F. A. Khan and S. H. Chauhdary, "Post-Quantum DAG-based Blockchain for Securing Vehicular Sensor Networks," in *IEEE Transactions on Consumer Electronics*, doi: 10.1109/TCE.2026.3688933.
- [12] S. Srivastava, D. Agarwal and B. K. Chaurasia, "Secure Communication Using Blockchain in Vehicular Sensor Network," in *IEEE Sensors Journal*, vol. 26, no. 10, pp. 16322-16334, 15 May15, 2026, doi:

10.1109/JSEN.2026.3678320.

[13] N. Ababneh and J. N. Al-Karaki, "On the Lifetime Analytics of IoT Networks," 2020 International Conference on Communication and Signal Processing (ICCSP), Chennai, India, 2020, pp. 1086-1090, doi: 10.1109/ICCSP48568.2020.9182272. 1.

[14] N. Gadde, B. Jakkali, R. B. HalasinanagenahalliSiddamallaih, and G. Gowrishankar, "Quality of experience aware network selection model for service provisioning in heterogeneous network," International Journal of Electrical and Computer Engineering (IJECE), vol. 12, no. 2, p. 1839, Apr. 2022, doi: 10.11591/ijece.v12i2.pp1839-1848.

[15] CICIoV2024 "IoV Dataset 2024 | Datasets | Research | Canadian Institute for Cybersecurity | UNB," www.unb.ca. <https://www.unb.ca/cic/datasets/iov-dataset-2024.html> (Accessed May. 11, 2026).

[16] L. Singh, S. J. Nanda and R. P. Yadav, "A Simplified Constraint Heuristic Optimization Algorithm for Energy Efficient Edge Server Placement in 5G Network," 2025 International Conference on Microwave, Optical, and Communication Engineering (ICMOCE), Bhubaneswar, India, 2025, pp. 1-5, doi: 10.1109/ICMOCE64100.2025.11076853.

[17] H. Liu, S. Wang, H. Huang and Q. Ye, "On the Placement of Edge Servers in Mobile Edge Computing," 2023 International Conference on Computing, Networking and Communications (ICNC), Honolulu, HI, USA, 2023, pp. 496-500, doi: 10.1109/ICNC57223.2023.10074304.

[18] P. Bhuvaneswari, D. Neelamegam and S. Satish, "Improving Decentralized Connectivity in 6G Communication using Blockchain Technology," 2025 6th International Conference on Electronics and Sustainable Communication Systems (ICESC), Coimbatore, India, 2025, pp. 545-549, doi: 10.1109/ICESC65114.2025.11212421.

[19] X. Ma, X. Jia, Y. Li and K. Xue, "Minimizing Age of Information in wireless powered communication network based on short packet communication," 2024 IEEE 100th Vehicular Technology Conference (VTC2024-Fall), Washington, DC, USA, 2024, pp. 1-5, doi: 10.1109/VTC2024-Fall63153.2024.10757648.

[20] Z. Lang, J. Shi, Q. Zhang, Z. Guan, L. Xu and Z. Qin, "A Resource-Aware Lightweight Semantic Communication System in Heterogeneous Edge-End Networks," in IEEE Wireless Communications Letters, vol. 15, pp. 2844-2848, 2026, doi: 10.1109/LWC.2026.3683871.

[21] C. Sun, X. Liu, X. Huang and C. Fischione, "Layer-wise Efficient Federated Learning with Distributed Clustering and D2D Communications," 2024 IEEE 25th International Workshop on Signal Processing Advances in Wireless Communications (SPAWC), Lucca, Italy, 2024, pp. 831-835, doi: 10.1109/SPAWC60668.2024.10694390.

[22] Y. Jin, J. She, S. Liu and Y. Gao, "Joint Semantic Communication and Output Length Prediction for Efficient Large Language Model Inference," 2025 IEEE/CIC International Conference on Communications in China (ICCC Workshops), Shanghai, China, 2025, pp. 1-5, doi: 10.1109/ICCCWorkshops67136.2025.11148149.

[23] Y. Zhao et al., "Multi-Functional Beamforming Design for Integrated Sensing, Communication, and Computation," in IEEE Transactions on Communications, vol. 73, no. 8, pp. 6322-6336, Aug. 2025, doi: 10.1109/TCOMM.2024.3519551.

[24] D. Wen, Y. Zhou, X. Li, Y. Shi, K. Huang and K. B. Letaief, "A Survey on Integrated Sensing, Communication, and Computation," in IEEE Communications Surveys & Tutorials, vol. 27, no. 5, pp. 3058-3098, Oct. 2025, doi: 10.1109/COMST.2024.3521498.

[25] B. Zhao, T. Yang, H. Xing and L. Xu, "Two-Stage Attention Based Collaborative Inference in Semantic Communication," 2024 International Conference on Ubiquitous Computing and Communications (IUCC), Chengdu, China, 2024, pp. 493-498, doi: 10.1109/IUCC65928.2024.00091.

[26] P. Zhang et al., "Intellicise Wireless Networks From Semantic Communications: A Survey, Research Issues, and Challenges," in IEEE Communications Surveys & Tutorials, vol. 27, no. 3, pp. 2051-2084, June 2025, doi: 10.1109/COMST.2024.3443193.

[27] A. M. Benaya, M. S. Hassan, M. H. Ismail and T. Landolsi, "Aerial ISAC: A HAPS-Assisted Integrated

Sensing, Communications and Computing Framework for Enhanced Coverage and Security," in IEEE Transactions on Green Communications and Networking, vol. 9, no. 4, pp. 2101-2114, Dec. 2025, doi: 10.1109/TGCN.2025.3551395.