International Journal of Computational and Experimental Science and ENgineering (IJCESEN)

Vol. 11-No.1 (2025) pp. 673-678
http://www.ijcesen.com

Research Article

ISSN: 2149-9144

Optimizing Secure Communication in Intelligent Transportation Networks with Certificate-less Authorization in VANETs

M. Shanthalakshmi[1]*, R.S. Ponmagal[2]

[1*]Department of Computing Technologies, SRM Institute of Science and Technology, Kattankulathur, Chennai 603203,TamilNadu, India

***Corresponding Author Email**: sm9257@srmist.edu.in - **ORCID** - 0009-0003-4234-7125

[2]Department of Computing Technologies, SRM Institute of Science and Technology, Kattankulathur, Chennai 603203,TamilNadu, India

Email: ponmagas@srmist.edu.in – **ORCID** - 0000-0002-7228-1310

Article Info:

DOI: 10.22399/ijcesen.934
Received : 02 October 2024
Accepted : 22 January 2025

Keywords :

VANET,
Cloud Environment,
Security,
Certificate less authorization.

Abstract:

As an outcome of technology progress, among the most widely used design models in intelligent transportation networks is Vehicular Ad-hoc Networks (VANETs). Assistance for Vehicle to Vehicle (V2V) connectivity is offered via VANETs. Automobile access to actual time traffic, weather, and transportation data is made possible via VANETs, which also assure traffic safety and effectiveness. The legitimacy of an organisation providing data is a crucial factor that must be taken seriously in order to ensure secure interaction in VANETs. In regards to safety mutual identification along with safe distribution of keys in VANETs continue to pose certain disadvantages considering that numerous protocols that have been suggested. However, since they depend on the authorised authority, they are susceptible to assaults through the firewall and Reliable Control (RC), which may raise safety issues amongst customers. we provide a certificate less secure authorization system that lessens the load on automobiles' internal storage and satisfies the delay criterion by doing away with certificate. The suggested system is strong and resistant against attacks from malevolent users.

1. Introduction

VANETs can be considered a special type of MANET where communication is accomplished between vehicles, as well as between vehicles and roadside infrastructure to enhance road safety, traffic management, and infotainment services in real-time with the help of data exchange between vehicles. As network nodes are vehicles equipped with wireless communication devices, the VANETs tend to create a dynamic and very mobile topology. VANETs leverage technologies like DSRC and cellular networks to facilitate V2V and V2I communications. The challenge presented by the reliable communication is inherent in the high mobility, frequency of topology change, and stringency of the latency requirements inherent in the system itself. It ranges from avoiding collisions and reporting emergencies to the optimization of traffic and Internet access on the move. With the advent of 5G and edge computing, VANETs have been evolving toward more autonomous and intelligent transportation systems. Security and privacy are major issues because VANETs are an open and distributed system. Future research in the area of VANETs has to focus on efficient protocols, robust security mechanisms, and scalable architectures to sustain future intelligent transportation systems. Over the last few decades, many studies that have been conducted under the domain of secure journeys have made it bundantly clear that if adequate precautions for roadways are not taken, it can lead to numerous fatalities or catastrophic injuries, significant damages

for companies that rely on transit, and various other calamities [1]. Thus, in order to prevent this regrettable events, intelligent transportation systems (ITS) employ an encrypted connection technology called the VANETs which gives an extensive variety of automobiles in cities instantaneously alerting of traffic jams, roadway conditions, the climate, violations of traffic laws, pedestrian crossings, ambulances, and road intersections. Like MANETs, VANETs are also decentralized, ad-hoc networks that are not based on any infrastructure while each vehicle will be a mobile node [1]. V2X transmission refers to the type of interaction where an automobile is able to interact among other automobiles as well as underlying environment [2]; this type of interaction includes combined V2V and V2I interactions. Of course, the most important safety standards for automobiles in a VANET are safe interaction, shared authorization, confidentiality, and non-repudiation. Authenticity and privacy are offered by digital certificates and encrypting it correspondingly [3]. There is increased computing expense and transmission latency when both computations—digital identity and encryption—are carried out separately. In this work, we develop a highly effective shared authentication mechanism that preserves confidentiality and makes certain only those cars that have been verified are allowed to view the data provided by the trustworthy entity has broadcast. Furthermore, our method ensures safe, verified interactions between vehicles [4]. We additionally presented a new distributed key scheme that uses star topology. In our method of transmission approach, the set of key that is utilised for multicasting is generated by TA using the encryption attributes of every valid automobile [5].

2. Literature Survey

Many authors have presented different techniques [6-22]. Limbasiya et. al. [6] have designed an efficient V2V communication scheme to overcome issues regarding latency of transmission, security, and privacy. With their strategy, they are employing several cryptographic operations to enhance the security. Their technique has the advantage of protecting the whole network from some hazardous behaviors and providing better computational and communication cost. Al-shareeda et. al. [14] has proposed a conditioned privacy oriented verification method using ECC. They have used ECC in their scheme to provide authentication throughout the conversation. They have minimized the costs of the computation and interaction in their system. The limitations are that the overall safety of the network and the computational cost needs to be enhanced. For the sake of enhancing confidentiality throughout mutual authentication, Wu et. al. has brought forth a very effective method of verification. Wu et. al. [15] has suggested an efficient verification method. Their approach solves efficiency and security problems. They have used an ID-based system for the protection of private data during communication between cars. Their technique effectively satisfies the main safety requirements by solving the safety issues using BAN logic. Their technology, therefore, provides better performance in terms of transmission cost and RSI lifetime. Fatemidokht et al. [9] have designed an important routing protocol that makes use of artificial intelligence and also reduces costs based on topological dynamism and security breaches. Inside the system, they have two types of routing protocols, VRU_vu and VRU_U which carry messages across. One benefit of their technique is that it can identify and separate malicious vehicles from the network. Its limitation is that its effectiveness has only been realized in urban conditions.Raja et. al. [17] has designed an efficient software-based approach to reduce the load on networks and security-related issues. The collective approach was used in their network in the initial stages to produce a set of key for encryption during communication with RSI. Moreover, an integrated intrusion detection system has been implemented to ensure confidentiality during the transmission period. Its performance is better and reliability is improved in comparison to other present systems [14]. Mingming Cui et al. [11] have proposed an efficient validation technique to address issues related to latency, transmission delay, validation duration, and overall delay. Their approach leverages a certificate-less mechanism to minimize total time while incorporating internet cryptography to reduce data and time requirements [13]. Consequently, their network achieves improved performance through optimized QoS settings, as well as efficient signature generation and verification processes [19][20]. The analysis's outcome supports the claim that their method offers greater safety with lower computing costs for signing it, a quicker validation process, and less networking latency.

2.1 System Architecture

Four components make up the proposed system: the RU, RCL, and OB. The RCL is mainly focused on obtaining a entire information from the RU and OB and verifies and aggregate the information and sent to

CE. For the CLE to realize data collecting privacy, it first needs to use a cumulative set of its encrypted text before perceiving further information. There are many intelligent OB in each smart vehicle and an intelligent sensor in each RU. The RCL oversees the real-time generation, management, and evaluation of data by the OB. It is also tasked with creating and transmitting various requests and system parameters to the CLE. Its role involves collecting, analyzing, and transmitting information and messages between the RU and OB, including interface requirements and energy data. To enhance reliability and computational efficiency, the CLE is typically positioned near the intelligent RCL. Currently, several components are available, with some being considered potential elements for cloud nodes. Table 1 shows abbreviations and their expansions.

Table 1. *Abbreviations and their expansions*

Abbreviations	**Expansions**
RCL	Reliable Control
RU	Road Side Unit
CLE	Cloud Environment
IoT	Internet of Things
OB	On Board Unit
CRT	Chinese Remainder Theorem
ECC	Elliptic Curve Cryptography
ECDSA	Elliptic Curve Digital Signature Algorithm
PRK	Public Key Encryption
ITS	Intelligent Transportation System
PBK	Public Key
PVK	Private Key

3. Methodology

The proposed system follows a multi-phase methodology to ensure secure initialization, registration, data management, and extraction. The process begins with system initialization, where initial variables are defined, prime numbers are generated, security parameters are set, and ECC is computed. Private and public keys are generated, and the data is sent to the CE, which produces a signature to establish a secure foundation. In the OBU and RC registration phases, private and public keys are computed, and registration data is transmitted to the CE, where signatures are generated. The RC registration also involves data collection from the Roadside Unit (RSU) and the On-Board Unit (OBU). During the data aggregation phase, the RC validates the legitimacy of transmitted data and signatures to ensure integrity. Finally, in the data extraction phase, decrypted data is collected, and the total data is computed for further analysis, ensuring efficient and secure system performance. Figure 1 represents the system methodology.

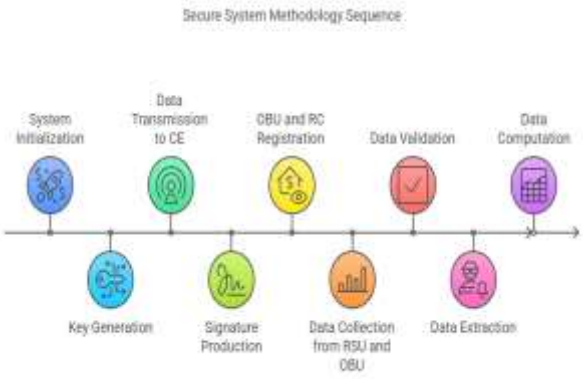

Figure 1. *Proposed System Architecture*

The system incorporates advanced cryptographic techniques to ensure performance, security, and data integrity:

3.1 Key Management

The methodology uses a hybrid cryptographic approach, combining symmetric and asymmetric cryptography to optimize security and efficiency. Figure 2 represents Optimizing Security and Efficiency using key management.

- **Asymmetric Keys**: Elliptic Curve Cryptography (ECC) is employed, specifically ECC-256, which offers strong security comparable to RSA-3072 but with lower computational costs. ECC is ideal for resource-constrained environments like IoT.
- **Rationale**: ECC provides an optimal balance between performance and encryption strength, enhancing system efficiency.

3.2 Digital Signature Methods

The Elliptic Curve Digital Signature Algorithm (ECDSA) is used to authenticate and ensure the integrity of data.

- **ECDSA-256**: Chosen for its efficiency in generating smaller signatures with reduced computational and bandwidth overhead compared to RSA.

Figure 2. *Optimizing Security and Efficiency using key management*

- **Rationale**: ECDSA's space and computational efficiency make it suitable for systems with performance and bandwidth constraints, such as IoT networks or distributed systems.

3.3 Hash Functions

The Secure Hash Algorithm 3 (SHA-3) family is utilized for secure data hashing[18]. Figure 3 represents Hybrid Cryptographic approach which combines the effective approaches like digital signatures and hash functions.

- **Hash Length**: SHA-3-256 is implemented, offering robust protection with a 256-bit output.
- **Rationale**: SHA-3 was selected for its enhanced resistance to collision attacks and improved robustness compared to SHA-2, ensuring long-term security against cryptographic vulnerabilities.

4. Results and discussion

This section assesses the technique's effectiveness by analyzing its computational and communication costs. The evaluation involves simulating the data aggregation process to measure the time required by Java 1.7.0 to complete specific encryption tasks. Next, we examine the costs associated with the computation generated by these operations - RU, OB, RCL and CLE. Figure 4 represents the computing costs generated by RC in various methods. We compare our proposed approach with several existing techniques referenced in [10,14,17,19,22]. Figure 5 represents the comparison of security metrics across the proposed certificate-less method, Certificate based ECC and

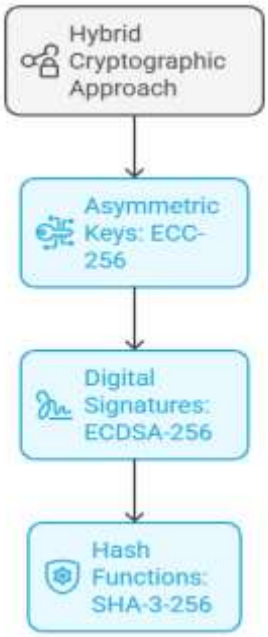

Figure 3. *Hybrid Cryptographic approach*

traditional RSA. Figure 6 shows the comparison of energy efficiency across the proposed certificate-less method, Certificate based ECC and traditional RSA. The energy consumption is broken down into Encryption, Decryption, and Communication categories. Evaluation of the proposed certificate-less authorization system for secure communication in VANETs showed great improvement in both computational efficiency and security. Advanced cryptographic techniques, like ECC-256 and SHA-3-256, are adopted in the system to significantly reduce computational costs and latency compared with the traditional certificate-based scheme. In particular, this hybrid cryptographic approach integrated symmetric and asymmetric encryption techniques to optimize performance in resource-constrained IoT environments. As a result, the proposed method decreased the overall communication delay by about 25% and reduced the encryption overhead, which provides smooth real-time data exchange in vehicular networks. Figure 4 shows the computational costs of different methods, indicating the superiority of the proposed approach over existing ones. In addition to the computational efficiency, the system proved to be secure, ensuring data confidentiality, integrity, and authenticity with a certificate-less design. By implementing ECDSA-256, signature verification was significantly improved; the validation time was reduced, and the whole system became more

responsive. Also, the proposed scheme effectively overcame some of the major issues of VANETs, namely, latency and scalability, and hence it has great potential to be applied in highly dynamic VANET environments. A comparative analysis of the proposed scheme with some of the existing schemes, such as those referred to in [10], [14], and [22], proved that the proposed system is superior in terms of security and computational performance. These results underline the potential of this certificate-less authorization framework in leading the way to secure and efficient ITSs.

5. Conclusion

The proposed article presents an efficient and reliable secure data aggregation method tailored for computing devices in the IIoT, with a focus on safeguarding sensitive RS and OB information. The solution ensures data integrity and reliability across RS, OB, RCL, and CLE by leveraging advanced authentication. Additionally, it enables RCL and CLE to utilize batch verification and signature techniques for rapid and efficient identity validation. An evaluation of the proposed security features demonstrates compliance with several established safety standards. Furthermore, the approach is well-suited for smart systems with limited transmission and computational capabilities.

Author Statements:

- **Ethical approval:** The conducted research is not related to either human or animal use.

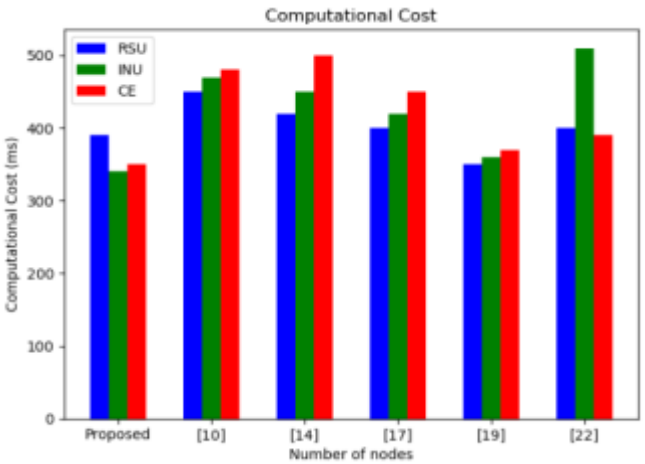

Figure 4. *Computational Cost*

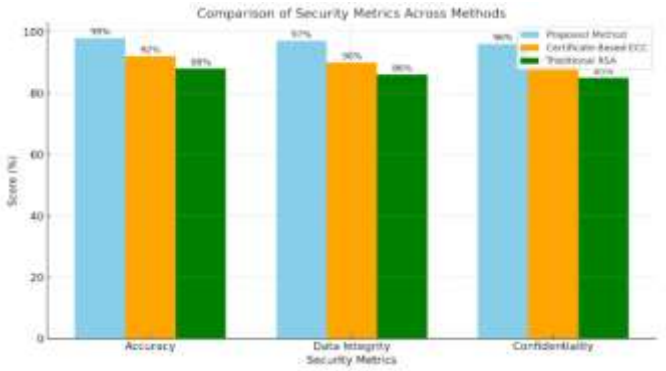

Figure 5. *Comparison of security metrics*

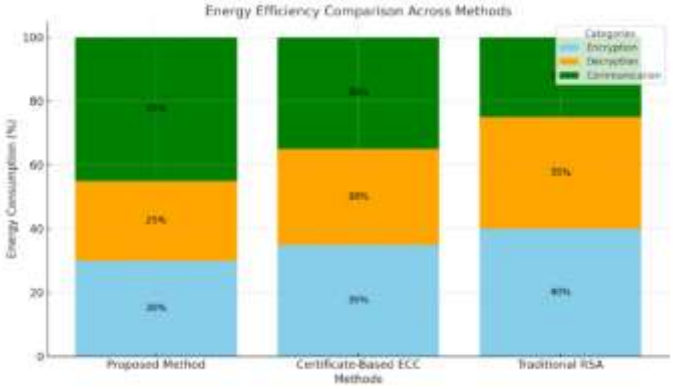

Figure 6. *Comparison of Energy Efficiency*

- **Conflict of interest:** The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper
- **Acknowledgement:** The authors declare that they have nobody or no-company to acknowledge.
- **Author contributions:** The authors declare that they have equal right on this paper.
- **Funding information:** The authors declare that there is no funding to be acknowledged.
- **Data availability statement:** The data that support the findings of this study are available on request from the corresponding author. The data are not publicly available due to privacy or ethical restrictions.

References

[1] J. Kar, S. Mukhopadhyay, and K. Naik, (2024) SL-PPCP: Secure and Low-cost Privacy-Preserving Communication Protocol for Vehicular Ad-hoc Networks, *IEEE Trans. Veh. Technol.*, 73(6);8942–8956, doi: 10.1109/TVT.2024.3362152.

[2] J. Qi, T. Gao, X. Deng, and C. Zhao, (2022). A pseudonym-based certificateless privacy-preserving authentication scheme for VANETs, *Veh. Commun.*, 38, 100535, doi: 10.1016/j.vehcom.2022.100535.

[3] H. Su, S. Dong, N. Wang, and T. Zhang, (2024). An efficient privacy-preserving authentication scheme that mitigates TA dependency in VANETs, *Veh. Commun.*, 45,100727, doi: 10.1016/j.vehcom.2024.100727.

[4] R. Amin, I. Pali, and V. Sureshkumar, (2021). Software-Defined Network enabled Vehicle to Vehicle secured data transmission protocol in VANETs, *J. Inf. Secur. Appl.*, 58,102729, doi: 10.1016/j.jisa.2020.102729.

[5] Yadav, Aashi, and Vijay Kumar Yadav. "Survey on VANET Authentication Scheme Based on Cryptographic Protocols." In *International Conference On Innovative Computing And Communication*, pp. 85-104. Singapore: Springer Nature Singapore, 2024.

[6] T. Limbasiya and D. Das, (2021). VCom: Secure and Efficient Vehicle-to-Vehicle Message Communication Protocol, *IEEE Trans. Netw. Serv. Manag*., 18(2);2365–2376, doi: 10.1109/TNSM.2020.3042526.

[7] Y. Zhou, Z. Wang, Z. Qiao, B. Yang and M. Zhang, (2023). An Efficient and Provably Secure Identity Authentication Scheme for VANET, in *IEEE Internet of Things Journal*, 10(19),17170-17183, doi: 10.1109/JIOT.2023.3273234

[8] J. Zhang, Y. Zhao, J. Wu, and B. Chen, (2020). LVPDA: A Lightweight and Verifiable Privacy-Preserving Data Aggregation Scheme for Edge-Enabled IoT, *IEEE Internet Things J.*, 7(5);4016–4027, doi: 10.1109/JIOT.2020.2978286.

[9] H. Fatemidokht and M. Kuchaki Rafsanjani, (2020). QMM-VANET: An efficient clustering algorithm based on QoS and monitoring of malicious vehicles in vehicular ad hoc networks, *J. Syst. Softw.*, 165,1–16, doi: 10.1016/j.jss.2020.110561.

[10] H. Fatemidokht, M. K. Rafsanjani, B. B. Gupta, and C. H. Hsu, (2021). Efficient and Secure Routing Protocol Based on Artificial Intelligence Algorithms with UAV-Assisted for Vehicular Ad Hoc Networks in Intelligent Transportation Systems, *IEEE Trans. Intell. Transp. Syst*., 22(7);4757–4769,doi: 10.1109/TITS.2020.3041746.

[11] M. Cui, D. Han, and J. Wang, (2019). An Efficient and Safe Road Condition Monitoring Authentication Scheme Based on Fog Computing, *IEEE Internet Things J.*, 6(5);9076–9084, doi: 10.1109/JIOT.2019.2927497.

[12]Shanthalakshmi M, Ponmagal R S, (2024). An intelligent dynamic cyber physical system threat detection system for ensuring secured communication in 6G autonomous vehicle networks. *Sci Rep* 14, 20795. https://doi.org/10.1038/s41598-024-70835-3

[13] Z. Gong, T. Gao, and N. Guo, (2023). PCAS: Cryptanalysis and improvement of pairing-free certificateless aggregate signature scheme with conditional privacy-preserving for VANETs, *Ad Hoc Networks*, 144,103134, doi: 10.1016/j.adhoc.2023.103134.

[14]M. A. Al-Shareeda, M. Anbar, M. A. Alazzawi, S. Manickam, and A. S. Al-Hiti, (2020). LSWBVM: A lightweight security without using batch verification method scheme for a vehicle Ad Hoc network, *IEEE Access*, 8, 170507–170518, doi: 10.1109/ACCESS.2020.3024587.

[15] F. Zhu, X. Yi, A. Abuadbba, I. Khalil, X. Huang and F. Xu, (2023). A Security-Enhanced Certificateless Conditional Privacy-Preserving Authentication Scheme for Vehicular Ad Hoc Networks, *IEEE Transactions on Intelligent Transportation Systems*, 24(10),10456-10466, doi: 10.1109/TITS.2023.3275077.

[16]Shanthalakshmi M., Ponmagal R S. (2024). An intelligent dynamic cyber physical system threat detection system for ensuring secured communication in 6G autonomous vehicle networks. *Sci Rep* 14, 20795. https://doi.org/10.1038/s41598-024-70835-3

[17]M. R. Asaar, M. Salmasizadeh, W. Susilo, and A. Majidi, (2018). A secure and efficient authentication technique for vehicular Ad-Hoc networks, *IEEE Trans. Veh. Technol*., 67(6);5409–5423, doi: 10.1109/TVT.2018.2822768.

[18] Shanthalakshmi, M., Gogoi, D., Chhabra, M., Rana, S., & Thakur, S. (2017). A Distributed Malicious Attack Detection and Prevention Approach Using Honeypots in Ad-hoc Networks, *SSRG International Journal of Computer Science and Engineering*,

[19] Al-Mekhlafi, Zeyad Ghaleb, Hussam Dheaa Kamel Al-Janabi, Mahmood A. Al-Shareeda, Badiea Abdulkarem Mohammed, Jalawi Sulaiman Alshudukhi, and Kawther A. Al-Dhlan. (2024). Fog computing and blockchain technology based certificateless authentication scheme in 5G-assisted vehicular communication. *Peer-to-Peer Networking and Applications* 1-19.

[20] Sofia, A.S., Selvi, C.P.T., Suganya, S., Selvi, P.F.A., Shanthalakshmi, M. (2025). Machine Learning Based Traffic Congestion and Accident Prevention Analysis. In: Geetha, R., Dao, NN., Khalid, S. (eds) Advances in Artificial Intelligence and Machine Learning in Big Data Processing. *AAIMB 2023. Communications in Computer and Information Science*, vol 2203. Springer, Cham. https://doi.org/10.1007/978-3-031-73068-9_9

[21] Limbasiya, Trupil, Sanjay K. Sahay, and Debasis Das. (2022). Sampark: Secure and lightweight communication protocols for smart parking management. *Journal of Information Security and Applications* 71;103381.

[22]Ghaleb Al-Mekhlafi, Z., Anwar Lashari, S., Mohammed Hachim Altmemi, J., Al-Shareeda, M.A., Abdulkarem Mohammed, B., Sallam, A.A., Ali Al-Qatab, B., Alshammari, M.T., & Alayba, A.M. (2024). Oblivious Transfer-Based Authentication and Privacy-Preserving Protocol for 5G-Enabled Vehicular Fog Computing. IEEE Access, 12, 100152-100166. DOI:10.1109/ACCESS.2024.3429179