Advanced International Journal for Research
E-ISSN: 3048-7641 editor@aijfr.com
Volume 6, Issue 3 (May-June 2025)

Leveraging Blockchain for Secure Secret Key Generation in Vehicular Networks

Balamurugan K[1], Pooja Bagga[2], Viraj Kale[3]

[1,2,3]Research Scholar, Dept. of Electronics and Tele-Communication, JSM College of Engineering, Pune Maharashtra

Abstract:

A groundbreaking blockchain-based trust management approach is revolutionizing location privacy in Vehicular Ad Hoc Networks (VANETs), a vital part of Intelligent Transportation Systems (ITS). This solution tackles the persistent security issues in VANETs, particularly for Location-Based Services (LBS). Now, vehicles can request LBS while their personal data remains secure through a verified process and the establishment of anonymous zones. An advanced trust management algorithm also governs vehicle behavior. The integration of blockchain technology significantly strengthens data security, leading to a highly robust and impenetrable system. Rigorous testing confirms the system's ability to withstand various trust-based attacks, highlighting its effectiveness in safeguarding vehicle privacy and its practical application in real-world VANET environments. This innovation points to a promising future for secure and private ITS.

Keywords: Conditional Privacy-Preserving Authentication (CPPA) for Vehicular Ad-Hoc Networks (VANETs).

1. Introduction

1. Vehicular Ad Hoc Networks (VANETs)

Vehicular Ad Hoc Networks (VANETs) promise substantial advancements in traffic management, road safety, and transportation efficiency, fostering greater connectivity and data exchange between vehicles and roadside infrastructure. However, to protect sensitive data transmitted across these networks, robust security and privacy measures are imperative. A novel solution has emerged to address these challenges: Effective Conditional Privacy-preserving Blockchain Technology.

Advanced International Journal for Research
E-ISSN: 3048-7641 editor@aijfr.com
Volume 6, Issue 3 (May-June 2025)

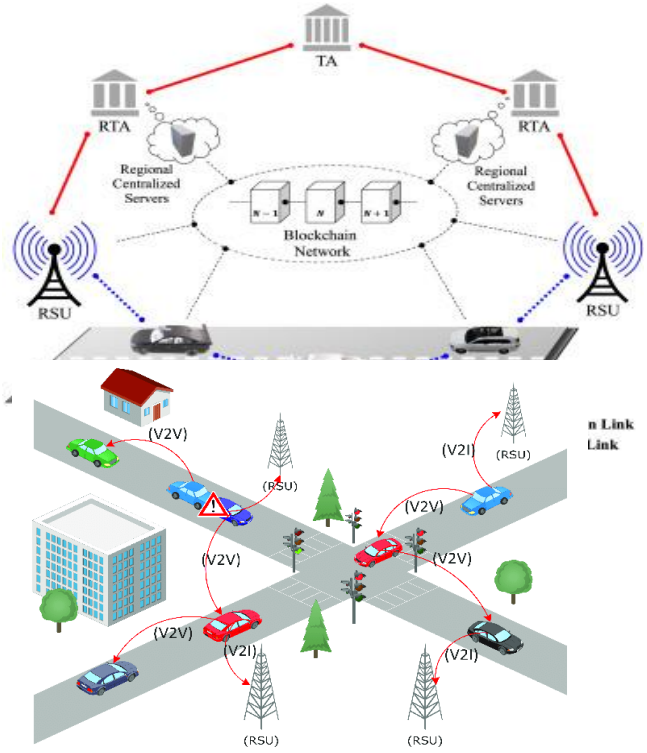

Figure.1. VANETs Architecture

1.1 Vehicular Ad Hoc Networks (VANETs)

Modern transportation systems are at the forefront of innovation with Vehicular Ad-hoc Networks (VANETs), combining wireless networking and vehicle communication. VANETs enable seamless connectivity between vehicles and roadside infrastructure, forming dynamic ad hoc networks during travel. Key components include Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) communication, revolutionizing interactions on the road. Equipped with Roadside Units (RSUs) and On-board Units (OBUs), these networks facilitate real-time information exchange, enhancing traffic management, road safety, and overall driving experience. As smart technologies become increasingly essential, VANETs play a pivotal role in developing intelligent transportation systems, boosting efficiency and paving the way for safer, more interconnected roads ahead.
Figure.2. Overview of message Transmission using VANETs

1.2 Conditional Privacy-Preserving Authentication (CPPA)

Conditional Privacy-Preserving Authentication (CPPA) introduces a novel approach to secure digital interactions, particularly in privacy-sensitive environments. At a time when safeguarding personal information is paramount, CPPA prioritizes user privacy by adapting authentication based on predefined conditions. Unlike traditional methods that often require disclosing sensitive information, CPPA ensures that users access services and systems only under specific circumstances, preserving their privacy. Whether granting conditional access to critical documents, online platforms, or financial transactions, CPPA enhances digital security through privacy-preserving protocols and cryptographic techniques. This approach empowers users with greater control and confidence as they navigate today's interconnected digital landscape.

2. Literature Survey

[1] Lu Wei and colleagues discuss the rising importance of Vehicular Ad Hoc Networks (VANETs) in enhancing driving convenience and traffic safety, driven by the proliferation of cars and advancements in wireless communication technology. They emphasize the necessity of a Conditional Privacy-Preserving Authentication (CPPA) method to address VANETs' security vulnerabilities. Traditional CPPA approaches suffer from inadequate communication and storage overheads for ultra-low transmission delay requirements of traffic emergency messages. To tackle these challenges, the authors propose a CPPA signature scheme based on elliptic curve cryptography, ensuring message recovery and reduced communication overhead. They also introduce a secure system secret key (SSK) updating algorithm using Shamir's secret sharing.

[2] Dapeng Wu et al. introduce an energy-efficient data forwarding system (EDFS) aimed at addressing critical issues in Wireless Body Area Networks (WBANs), particularly in healthcare applications. Due to limited energy resources of body sensors in WBANs, effective energy management is crucial to mitigate performance issues such as latency and declining energy efficiency. EDFS employs compressed sensing to minimize physiological data transmission and optimizes relay sensor selection based on factors like sensor relevance, sampling frequency, and remaining energy levels. This adaptive approach adapts to changing WBAN topologies, improving energy conservation and network reliability.

[3] Duan and colleagues underscore the pivotal role of Vehicular Ad Hoc Networks (VANETs) in the autonomous vehicle sector, highlighting emerging security challenges alongside technological advancements in VANETs. They critique weaknesses in the three-factor (3F) authentication strategy proposed by Xu et al., exposing vulnerabilities to dishonest Roadside Units (RSUs) and unauthorized sessions with On-Board Units (OBUs). In response, Duan et al. propose a novel 3F authentication system named TFPPASV, designed to safeguard user privacy and prevent RSUs from bypassing the trusted authority (TA). Their scheme undergoes rigorous formal security analysis using BAN-Logic, supported by informal discussions on its security features and performance comparisons with recent schemes.

[4] Chao Lin et al. address security and privacy concerns in Vehicular Ad Hoc Networks (VANETs), focusing on real-time traffic information sharing among vehicles to enhance driver safety and traffic management efficiency. They critique current conditional privacy-preserving authentication (CPPA) methods and propose a new blockchain-based CPPA (BCPPA) protocol utilizing Ethereum as a public blockchain for secure VANET communication. Their innovative solution includes a key derivation algorithm to reduce the storage burden of private keys for participating vehicles. BCPPA supports batch verification and modified ECDSA or alternative PKI-based signatures for improved verification efficiency. Security requirements are met, and feasibility is demonstrated through implementation on Ethereum's test network.

[5] Jing Zhang et al. introduce a novel system to enhance security and privacy in Vehicular Ad Hoc Networks (VANETs) by addressing limitations of current identity-based vehicular communication protocols. Unlike traditional approaches relying on tamper-proof devices (TPDs), their protocol utilizes the Chinese remainder theorem (CRT) for conditional privacy-preserving authentication. This dynamic CRT-based approach enables trusted authorities (TAs) to generate and distribute group keys without pre-loading master keys on TPDs in vehicles, thereby mitigating side-channel attacks and enhancing system security. The protocol's efficiency is

underscored by reduced computational and communication overheads, supported by rigorous security analysis under the random oracle model.

3. RELATED WORK

Vehicle Ad-hoc Networks (VANETs) offer the potential to streamline traffic management and enhance driver safety. To achieve an optimal balance between traceability, anonymity, and effective key/certificate management in VANETs, blockchain-based conditional privacy-preserving authentication (BCPPA) is recommended. Current BCPPA methods aim to mitigate security and privacy concerns but often at the cost of increased verification and traceability overheads, which fail to meet VANETs' requirements for high mobility, low latency, and real-time performance.

Our proposed solution introduces three foundational components: key derivation (KeyDer), smart contracts, and signatures of knowledge (SoK). This enhanced BCPPA approach, named Efficient Blockchain-based Conditional Privacy Authentication (EBCPA), addresses message authentication, conditional privacy protection, and other critical criteria from the outset. We demonstrate EBCPA's capability to withstand common attacks and highlight its advantages.

Furthermore, EBCPA is implemented and evaluated on various platforms including the Hyperledger test network, the Rinkeby test network hosted online by Ethereum, and a VANET simulation environment using VanetMobiSim and NS-2. Computational costs and communication overheads are assessed through comparison with other BCPPA protocols striving for similar security and efficiency goals.

4. METHODOLOGY

We propose the Identity-Based Online/Offline Digital Signature (IBOOS) technique to enhance secure data transmission in Cluster-based Wireless Sensor Networks (CWSNs) and improve Wireless Sensor Networks (WSNs) performance. To achieve energy efficiency, we introduce two new Secure and Efficient Data Transmission (SET) protocols: an enhanced CP-ABE method based on Diffie-Hellman cryptography and IBOOS, which expands on Identity-Based Digital Signature (IBS) techniques. These improvements streamline the architecture, reduce reliance on trusted authorities, and minimize communication overhead between Virtual Controllers (VCs). A central controller is established to integrate content servers, Roadside Units (RSUs), and vehicle information, enabling multiple control servers with RSUs to display accessible content server IDs. Vehicle node details are visible in the RSU interface, facilitating connections with content servers as needed. Additionally, data replication within vehicles is optimized when the nearest RSU is accessible, enhancing data management efficiency.

According to the diagram, vehicle registration using blockchain technology begins with the Registration Authority (RTA), which could be a government department or another authorized entity responsible for vehicle registration. The car owner applies for registration with the RTA, providing details such as manufacturer, model, year, and VIN number. The RTA generates a key pair for the vehicle, comprising a public key for identity confirmation and a private key for transaction signing. The vehicle's registration certificate is then stored on a tamper-resistant distributed ledger known as a blockchain. Upon completion, ownership of the car is transferred to the owner, who can update the blockchain-based registration certificate when the vehicle is sold or transferred.

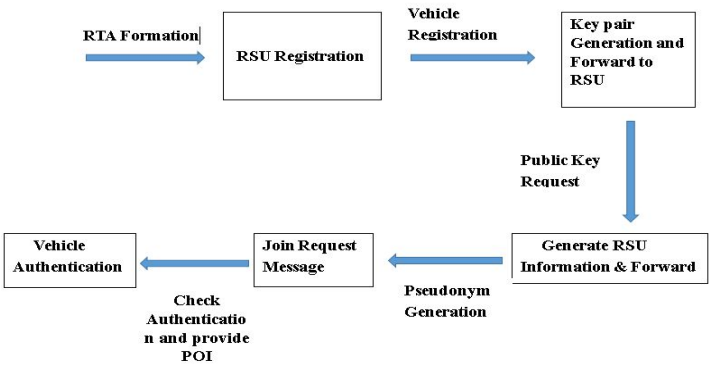

Figure.3. Block Diagram for Wireless Sensor Network

Encryption Module:This proposed lightweight CP-ABE approach for mobile cloud-assisted cyber-physical systems involves three key algorithms. The first algorithm distributes public parameters and securely stores a master secret key. The second algorithm uses these parameters, input data, and access policies to encrypt data before transmitting it to the cloud. Finally, the decryption algorithm ensures that only users meeting the access policy criteria can successfully decode the ciphertext using the master set of attributes.

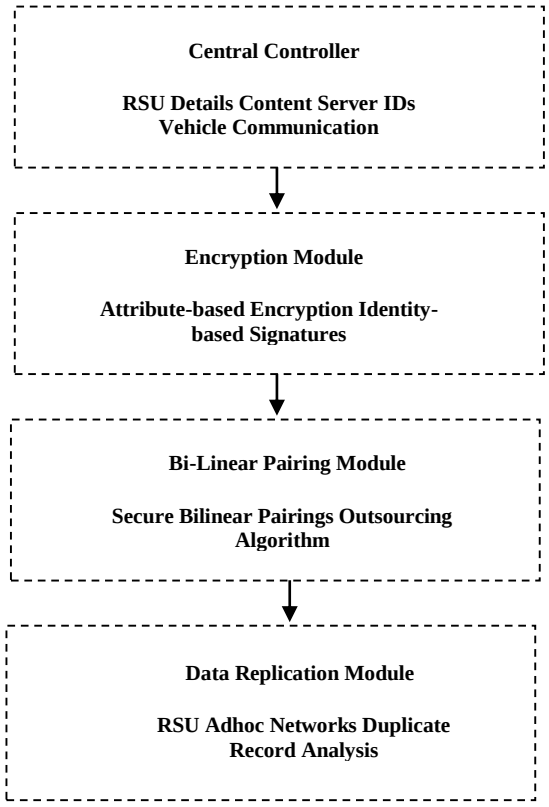

Figure.4. Flow Diagram for Wireless Sensor Network

Central Controller Server: The central controller module serves as the primary hub for managing RSU information, available content server IDs, and facilitating RSU-to-RSU communication with nearby vehicles.

It enables users to access and generate location IDs and RSU IDs within the content server, as well as overseeing data replication within vehicles as part of its operational function. Network administrators can utilize SDN programming to configure, administer, secure, and optimize network resources, leveraging the programmable nature of software-defined networks (SDNs).

Bilinear Pairing Module:To reduce the computational overhead associated with bilinear pairings in pairing-based cryptography protocols, this study presents an innovative outsourcing strategy. Our secure and efficient outsourcing technique operates under the two untrusted server model, sparing the outsourcer from resource-intensive operations like exponentiations or point multiplications. This method serves as a key subroutine in enabling secure identity-based encryptions and signatures, even when outsourced.

Data Replication Module: Enhanced RSU accuracy in vehicle ad-hoc networks enables effective data replication. Each RSU utilizes an ad-hoc model specifically designed to detect and analyze duplicate information, facilitating the data replication process by identifying matching records with other RSUs. Each RSU unit manages its own vehicle ad-hoc network, utilizing the Database Replication module to import data from existing databases, including complex mappings across multiple tables.

5. Result Analysis

The proposed method demonstrates significantly higher accuracy compared to the current system. Specifically, the new algorithm achieves an accuracy of 88%, marking a notable improvement over the 80% accuracy of the previous approach. This substantial enhancement underscores the effectiveness of the proposed solution in addressing existing challenges and enhancing the overall operational efficiency of Wireless Sensor Networks. These advancements underscore the potential of the proposed approach in facilitating secure and energy-efficient data transmission within Cluster-based Wireless Sensor Networks. This is particularly evident through the implementation of Secure and Efficient Data Transmission (SET) protocols and the Identity-Based Online/Offline Digital Signature (IBOOS) algorithm, both of which contribute to superior performance.

Scheme	BCPPA	IBOOS
RSU's Computation cost	13.5175 ms	6.8364
Vehicle Computation cost	5.5696	2.4415

Here are the computation costs for the BCPPA and IBOOS schemes:

- BCPPA:
  - RSU's Computation Cost: 13.5175 ms
  - Vehicle's Computation Cost: 5.5696 ms

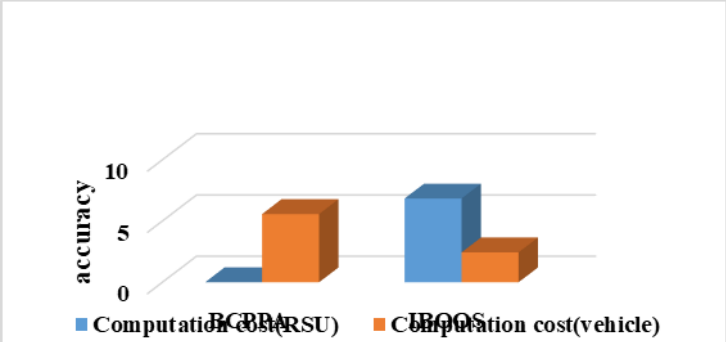

Figure.5. Comparison Graph of BCPPA and IBOOS

- IBOOS:
  - RSU's Computation Cost: 6.8364 ms
  - Vehicle's Computation Cost: 2.4415 ms

6. Future Work

Improving IBOOS and SET protocol performance: Both IBOOS and SET protocols are currently under development, leaving room for enhancements in various aspects such as data encryption and decryption efficiency, message signing, and message verification.

Reducing overhead in IBOOS and SET protocols: While certain computational and communication overhead is inevitable with IBOOS and SET protocols, efforts can be made to minimize this overhead by developing more efficient protocols and algorithms.

Reference

1. Pokhrel S.R., Choi J., "Secure and lightweight conditional privacy-preserving authentication for securing traffic emergency messages in VANETs", IEEE Transactions on Communications, Vol. 68, no. 8, pp. 4734-4746, Aug. 2020.
2. Baza M., Nabil M., Lasla N., Fidan K., Mahmoud A., Abdallah M., "An energy-efficient data forwarding technique for heterogeneous WBANs", In Proceedings of IEEE Wireless Communications and Networking Conference (WCNC), pp. 1-7, April 2019.
3. Shrestha R., Nam S.Y., Bajracharya R., Kim S., "A three-factor security safeguarding validation scheme for VANETs", Sensors, Vol. 9, no. 9, p. 1338, Aug. 2020.
4. Jiang X., Tong F.R., Leung V.C.M., "A blockchain-based conditional privacy-preserving authentication protocol for vehicular ad hoc networks", IEEE Internet of Things Journal, early access, doi: 10.1109/JIOT.2020.3026354, Sep. 2020.
5. Ayvaz S., Cetin S.C., "Conditional privacy-preserving authentication scheme based on Chinese remainder theorem for VANETs", International Journal of Intelligent Systems and Applications, Vol. 7, no. 2, pp. 72-87, Apr. 2019.
6. Guo R., Gao S., Zheng D., Jing C., Wang L., "An accessible authentication method for blockchain that is traceable and protects privacy in VANETs", IEEE Access, Vol. 11, pp. 7716–7726, 2019.
7. Zeadally S., Feng Q., He D., Liang K., "BPAS: Vehicle Ad Hoc Network Privacy-Preserving Authentication System Assisted by Blockchain", IEEE Transactions on Industrial Informatics, pp. 4146-

4155, 2020.
8. Cui., Zhang., Zhong., Liu., "Comprehensive conditional privacy protection authentication system for secure vehicular networks in a multi-cloud environment", 2020.
9. Zheng Z., Zhang Y., Dai H., "A survey on blockchain and the Internet of Things", IEEE Journal of Internet of Things, 6(5), pp. 8076–8094, 2020.
10. Xu Jin H., Xu J., Liang W., Li K., "An Internet of Vehicles key agreement protocol and authentication system based on blockchain for roadside units", Journal of Parallel and Distributed Computing, pp. 29–39, 2020.
11. Wellens M., Westphal B., Mahonen P., "Performance evaluation of IEEE 802.11-based WLANs in vehicular scenarios", Proceedings of the 65th IEEE Vehicular Technology Conference (VTC007), pp. 1167-1171, 2020.
12. Cottingham D., Wassell I., Harle R., "Performance of IEEE 802.11 a in vehicular contexts", IEEE Vehicular Technology Conference, pp. 854-858, 2007.
13. Wellens M., Westphal M., Mahonen P., "Performance evaluation of IEEE 802.11-based WLANs in vehicular scenarios", Proceedings of the 65th IEEE Vehicular Technology Conference (VTC007), pp. 1167 1171.
14. Jaballah M., Conti M., Lal C., "Security and Design Requirements for Software-defined VANETs", Computer Networks, vol. 169, March 2020.
15. Al-shareeda M., Anbar M., Manickam S., Hasbullah I. H., "An Efficient Identity-Based Conditional Privacy-Preserving Authentication Scheme for Secure Communication in a Vehicular Ad Hoc Network", Symmetry, vol. 12, October 2020.
16. Ramabadran R., Afanasyev P., Malone D., Leeser D., McCarthy D., Brien B. O., et al., "A Novel Physical Layer Authentication with PAPR Reduction based on Channel and Hardware Frequency Responses", IEEE Transactions on Circuits and Systems, Vol. 67, no. 2, pp. 526-539, February 2020.
17. Bottarelli M., Karadimas P., Epiphaniou P., Kbaier D., Ismail B., Maple B., "Adaptive and Optimum Secret Key Establishment for Secure Vehicular Communications", IEEE Transactions on Vehicular Technology, Vol. 70, no. 3, pp. 2310-2321, March 2021.
18. Li J., Choo KR., Zhang W., Kumar S., Rodrigues J., Khan MK., Hogrefe D., "Efficient EPA-CPPA: An Efficient, Provably-Secure, and Anonymous Conditional Privacy-Preserving Authentication Scheme for Vehicular Ad Hoc Networks", Vehicular Communications, 2018; 240.
19. Sutrala A.K., Bagga P., Das A.K., Kumar N., Rodrigues J.J.P.C., Lorenz P., "On the design of conditional privacy preserving batch verification-based authentication scheme for Internet of Vehicles deployment", IEEE Transactions on Vehicular Technology, 69(5), pp. 5535–5548, 2020.
20. Vijayakumar P., Azees M., Kozlov S.A., Rodrigues J.J.P.C., "An anonymous batch authentication and key exchange protocols for 6G enabled VANETs", IEEE Transactions on Intelligent Transportation Systems, 2020.