Utilizing Crowdsourced Data from Multiple Lidar-Equipped Vehicles to Update the Point Cloud Layer of High-Definition Maps

DR. V. SINDHU[1], KARTHIK M P[2], KEERTHANA M[3], MATTUVAR KUZHALI L[4]
[1]*Assistant Professor, Department of Information Technology, Sri Krishna College of Engineering and Technology, Coimbatore, India*
[2, 3, 4]*Student, Department of Information Technology, Sri Krishna College of Engineering and Technology, Coimbatore, India*

Abstract- ***Reliable communication and safety in Vehicular Ad Hoc Networks (VANETs) depend on effective and secure authentication. This paper presents a new architecture that combines Roadside Units (RSUs) and SHA-256 with pseudonym-based authentication to overcome these issues. Utilizing the cryptographic power of SHA-256, the suggested approach creates a strong mechanism for managing and extracting secret keys. In order to facilitate safe communication via a blockchain-based consortium network in which RSUs serve as trustworthy nodes, a distinct pseudonym is provided at vehicle registration. In order to guarantee data integrity and message validity, these RSUs work together to produce and distribute cryptographic keys. While the blockchain ledger preserves an unchangeable record of authentication events, improving transparency and traceability, the pseudonym method improves privacy by routinely altering vehicle identities as well. Even if this decentralized architecture reduces single points of failure, there is still room for improvement in terms of scalability and latency. By improving VANET security, the suggested solution creates a foundation for safer and more effective vehicular communication.***

Indexed Terms- ***Pseudonym-Based Authentication, SHA-256 Encryption, Blockchain Security, Vehicular Ad Hoc Networks (VANETs)***

I. INTRODUCTION

For vehicles and infrastructure components to communicate safely and effectively, vehicular ad hoc networks, or VANETs, are necessary. As the number of connected cars continues to rise, maintaining data integrity and authentication becomes more challenging. Traditional centralised authentication systems are less effective in dynamic vehicle contexts due to scalability issues and single points of failure. To address these issues, this paper proposes a decentralised authentication framework that combines pseudonym-based authentication, the SHA-256 algorithm, and blockchain technology. Roadside Units (RSUs) are reliable nodes that offer secure cryptographic key management and message validation. By regularly changing pseudonyms, the solution makes use of the openness and immutability of the blockchain to enhance security, prevent unauthorised access, and safeguard privacy. This tactic provides access to a more secure and improved communication reliability and strengthened VANET security to create a more efficient intelligent transportation environment.

A privacy augmentation strategy called pseudonym-based authentication was developed to enhance data privacy through the provision of user anonymity in notification networks, particularly in even further ad hoc networks (VANETs). To keep away from tracking and other illegal methods like spying, a vehicle gets a new set of temporary pseudonyms that are changed at regular intervals instead of using the same permanent identify. This method ensures that only authorized authorities, such as trusted network nodes and Roadside Units (RSUs), can authenticate legitimacy of a vehicle making sure the vehicle's true identity is never exposed. Identity spoofing and replay attacks are the main hacking techniques that are stopped using this pseudonym-based authentication method that employs strong cryptographic algorithms such as

SHA-256 for a safe message transmitting. Wait, there is one more thing: This technology not only results in vehicle security to be improved but also to keep the network open and acceptable, it provides a perfect, comfortable, and isolated communication within intelligent transportation systems.

Figure 1 Vehicular Ad Hoc Networks

SHA-256 is an example of a cryptographic hashing method that is secure and gives data integrity in digital communication networks. This kind of encryption, secure hash algorithm (SHA) is unbreakable to manipulation and collisions due to it getting a set hash greater than or equal to 256 bits from an input no matter the size. This technology is the basis of safe key management, authentication, and digital signatures by means of making every input data different through hash computations. Thus, it offers robust and secure the VANET system.

Blockchain security is the application of cryptographic methods and decentralized consensus algorithms to guarantee the integrity, confidentiality, and immutability of data contained in a blockchain network. Through the use of cryptographic hashing, digital signatures, and distributed ledger technology, blockchain security ensures that unauthorized changes, data breaches, and fraudulent transactions are avoided. In Vehicular Ad Hoc Networks (VANETs), blockchain security is also essential in authentication and secure communication through having a securely immutable record of identity verifications and transactions. Being decentralized, blockchain eliminates single points of failure, reducing the likelihood of cyberattacks. and making the network more resilient. Furthermore, access control systems and smart contracts enhance security even further by enabling automation of data sharing and authentication as well as providing transparency and trust among participants in the network. Such a high-security environment makes blockchain technology a fundamental tool for vehicular network and intelligent transportation system security.

For supporting real-time information exchange between cars and infrastructure points such as Roadside Units (RSUs), Vehicular Ad Hoc Networks (VANETs) are a particular type of Mobile Ad Hoc Networks (MANETs). Supporting safe data sharing for traffic management, collision prevention, and alerts, these networks are crucial to intelligent transportation systems. To enhance road safety and efficiency, VANETs make use of wireless communication protocols to provide cars with the ability to share information regarding road condition, vehicle speed, and potential threats. VANETs pose problems with privacy, security, and authentication due to their high mobility and dynamic nature. Cryptographic approaches such as SHA-256 encryption and blockchain-based authentication schemes are combined in order to address these challenges and provide secure and immutable communication. VANETs enable the development of autonomous car and smart transportation systems by providing a reliable and scalable platform.

Figure 2 Vehicle Communication

II. LITERATURE REVIEW

The significance of vehicular ad hoc networks (VANETs) in boosting driving both safety and traffic

management is becoming more and more significant. However, there are security and privacy concerns issues with wireless vehicle communication. The aforementioned problems can be resolved using the conditional privacy-preserving authentication (CPPA) system; however, the current identity-based CPPA techniques have inherent key escrow problems. In light of this, we provide a lightweight CPPA technique elliptic curve cryptography for address the aforementioned problems. The suggested system overcomes the key escrow problem by using a pseudonym and public/private key pair that are produced automatically by the vehicle. Furthermore, a Low latency, location awareness, and mobility are made possible by this fog computing model is used to suggest a CPPA method for effective vehicular communication. In the suggested technique, two hash chains construct the vehicle's pseudonym in order to efficiently decrease storage overhead, provided that backward security is ensured. Security study demonstrates that the system meets VANET security criteria and is safe under random oracles. The suggested approach performs better than analogous method regarding computational and communication efficiency, according to performance evaluation.

Dapeng Wu [2] et.al Wireless body area networks (WBANs) are mostly used in healthcare for physiological data collection and human body monitoring. Because body sensors have a finite energy supply, their energy depletion will seriously impair network performance, including latency and energy efficiency. The energy consumption rates of body sensors might vary according to their variety. Furthermore, the significant levels of physiological data that are monitored may differ greatly. In order to balance sensor energy consumption and enhance network lifespan and cooperative operations of heterogeneous WBANs, this research proposes an energy-efficient data forwarding method (EDFS) that targets the aforementioned issues. Our primary contributions are as follows: 1) compressed sensing is used to analyze– the original physiological data in order to limit the amount of data that has to be broadcast; and 2) EDFS considers sampling frequency, remaining energy levels, and sensor significance in order to pick the best relay sensor. The EDFS can increase WBAN data transmission's dependability and energy efficiency. Furthermore, our simulation findings show that the suggested EDFS can provide balanced energy consumption and energy efficiency while successfully handling the constantly shifting WBAN topologies.

Zongtao Duan [3] et.al The autonomous car business depends on vehicular ad hoc networks (VANETs), and as VANET technology advances, security risks are rising quickly. An intelligent security protocol that offers unbreakable security is necessary for the mitigation of these risks. The centralised Trusted Authority (TA), which is in charge of allocating criteria for authentication throughout the process of car registration and authentication is dependent upon these parameters, is used by a number of three-factor authentication solutions for VANET that have been released recently. The flaws of the most current three-factor (3F) authentication technique introduced by Xu et al. are first explained in this paper. Our study demonstrates that an RSU may simply initiate a session with OBU and avoid the TA if it is dishonest. Additionally, in order to prevent RSU from evading the TA and to protect user privacy, this study proposes a novel technique that offers 3F authentication for VANETs (TFPPASV). The suggested plan satisfies the VANET's performance and security criteria. In addition to the unofficial conversation on security features, we conduct a rigorous security analysis of the suggested architecture using BAN-Logic analysis. Lastly, we contrast the performance and security of the suggested TFPPASV with a few new and similar methods.

Chao Lin [4] et.al has proposed in this system Security and privacy are two persistent problems that need to be resolved even though Vehicular Ad-hoc Networks (VANETs) have the potential to increase driver safety and traffic management effectiveness (for example, by promptly exchanging traffic status among cars). As a result, security fixes have been suggested, including conditional privacy-preserving authentication (CPPA) methods. Due to issues like unsolvable private key update in ID-based protocols or limits in management of keys and certificates in protocols based on PKI. CPPA protocols are often far from being prepared for deployment in VANETs. Even though several blockchain-based CPPA (BCPPA) protocols have been put out to address these issues, several obstacles still remain, such as the need for hardware, frequent

contacts, or the ability to revoke the private key. We are therefore inspired to provide a fresh BCPPA procedure in this study that does not have these problems. on particular, we introduce a PKI-based solution based on Ethereum (a public blockchain) that enables secure communication on VANETs by utilizing a standard digital signature mechanism, such ECDSA. To put it another way, we implement an efficient certificate management system by combining blockchain technology with a key derivation process. As a result, participating automobiles don't need to have as many private keys. Our BCPPA supports either implementing additional PKI-based signatures with batch verification directly or substituting modified ECDSA for batch validation to do so to lower the cost of verification time. We show the security criteria that our BCPPA protocol is capable of fulfilling along with the physical design. We next put BCPPA into practice on the Ethereum test network, Rinkeby, and demonstrate its viability (in milliseconds) with simulations using Vanet MobiSim and NS-2.

Jing Zhang [5] et.al has proposed in this system in order to accomplish conditional privacy-preserving, the majority of the current identity-based and security-based vehicular communication protocols used in Vehicular Ad-hoc Networks (VANETs) depend on a tamper-proof device (TPD), which is a piece of ideal hardware that is put in automobiles.. It is often difficult to achieve quick authentication throughout the message verification process using such schemes, and the ensuing overheads further limit their speed. This work suggests a unique conditional privacy-preserving authentication strategy for secure vehicle authentication that is based on the Chinese remainder theorem (CRT) in order to overcome such issues. The suggested methodology does away with the necessity of loading the master key into the car's TPDs beforehand and simply calls for realistic TPDs. When creating and disseminating new group keys for network's cars, the trusted authorities (TAs) can benefit dynamically from the Chinese remainder theorem.et.al has proposed in this system. The suggested approach guarantees a greater degree of protection for the whole system and addresses the leakage issue during side channel assaults. Furthermore, even with a rising number of signatures, the suggested technique achieves quicker verification by avoiding the need involving map-to-point hash and bilinear pairing operations throughout the verification process. Additionally, the performance study demonstrates that our suggested scheme is effective in lowering computing as well as overheads in communication and the security analysis shows that our proposed scheme is safe in the case of random oracles.

III. RELATED WORK

Real-time connection between vehicles and everything is made possible by the new technology known as systems for intelligent transportation. Therefore, in vehicular ad-hoc networks (VANETs), protecting and authenticating data packets for communication within and between vehicles are essential security services. Nonetheless, signature-based authentication frequently uses public-key cryptography ($P\ KC$), which uses a lot of processing power and transmission bandwidth for key distribution and signature creation and verification. Therefore, by taking use of the randomness and reciprocity characteristics of wireless channels, physical layer-based secret key extraction has become a viable option for key agreement. However, current reconciliation methods have serious communication costs and security problems, and the poor channel reciprocity results in differences in the derived key. This study uses $P\ KC$-based authentication to exchange authenticated probing packets and identify initial validity. In light of this, we provide a blockchain-based reconciliation method that enables the trusted third party ($T\ T\ P$) to publish the mismatched bit repair sequence through a smart contract transaction.

IV. METHODOLOGY

The proposed method ensures vehicle communication in VANETs through the integration of the SHA-256 algorithm and pseudonym-based authentication. Roadside Units (RSUs) are used as trusted nodes for generating and distributing cryptographic keys in a consortium network using blockchain technology. Vehicles are assigned unique pseudonyms during registration to enable repeated changes in identification for enhanced privacy. Cryptography is utilized by the system to ensure message integrity and authenticity, and authentication events are eternally stored on the blockchain ledger. A decentralized

design is implemented in order to overcome scalability and latency problems and minimize single points of failure.

Figure 3 System Flow Diagram

A. Encryption Module

This module is responsible for securing data transmitted throughout the system. This module ensures that confidential information is encrypted in a manner that cannot be decrypted by unauthorized entities using advanced cryptographic techniques such as SHA-256. Through the encryption of messages prior to sending and decryption upon receipt, it provides secure end-to-end data transfer and plays a significant role in maintaining vehicular communication confidentiality and integrity.

B. Central Controller Module

As the primary coordinator of the system, the central controller module manages and oversees all operations pertaining to data flow and authentication. This module oversees the issuance of cryptographic identities, keeps the blockchain network synchronised, and enables secure communication between automobiles and RSUs. By monitoring and controlling system activity, it enhances the VANET architecture's overall efficacy and reliability.

C. Bi-linear Pairing Module

This module is intended to facilitate sophisticated cryptographic functions that are necessary for safe key management and authentication. Through the generation and verification of keys between cars and RSUs, it makes it possible to create secure communication channels. By limiting network participation to authorized organizations, this module offers a strong basis for safe vehicle communication and authentication procedures.

D. Data Replication Module

This module is in charge of preserving data availability and consistency throughout the blockchain-based consortium network. This module guarantees data redundancy and guards against loss from node failure by distributing authentication records and other important data among several nodes. It improves the fault tolerance and dependability of the system, guaranteeing secure vehicle operations and continuous access to authentication records.

Figure 4.1 LIDAR

V. ALGORITHM DETAILS

SHA-256 is a secure hashing technique used in the latest invention for VANET pseudonyms authentication. Fixed-size 256-bit hash value provision by SHA-256 for every transaction, on the one hand, protects data integrity with its tamper and collision resistance. The function has, therefore, been worn as a means to produce and hash a unique pseudonym during vehicle registration which is then used for signing and authenticating of messages. Roadside Units (RSUs) authenticate cars and help them communicate safely by using pseudonyms that they agreed on with a hash. By storing these hashed pseudonyms on the blockchain ledger, no identities could be linked back, thus, the implementation results in a transparent and incorruptible system. In vehicular networks, this methodology extends to security, privacy, and authentication reliability.

1. Implement a protocol based on blockchain that RSUs' trust the nodes.
2. Vehicle Registration:
   a. assign a unique vehicle identification number (VID).
   b. name the vehicle as the name (P).
   c. Set the hashed identity as H(P) = SHA-256(P) and save it to the blockchain database.
   d. Include H(P) in the blockchain.
3. Key Distribution:
   a. RSUs use H(P) to check the car's identity.
   b. Once it is correct, the system creates a session key (SK) for a secure conversation two nodes.
   c. Encode the session key and send it to the vehicle.
4. Secure Communication:
   a. The car applies H(P) to authenticate with every message.
   b. After the H(P) of that message has been hashed and then compared to the one in the blockchain, the RSU knows the origin of the message.
   c. The received message's validation is done: If it is correct, it is accepted; otherwise, it is rejected.
5. Update the pseudonym:
   a. Create a new one, P', at predetermined intervals.
   b. Update the blockchain after computing the updated H(P') = SHA-256(P').
   c. To protect privacy, invalidate the outdated pseudonym H(P).

Formula

Pseudonym Generation:
$P=f(VID, T)$

Hashing for Secure Identity

$H(P)=SHA\text{-}256(P)$

Session Key Generation for Secure Communication

$SK=H(P)\oplus R$

VI. RESULTS AND DISCUSSION

Blockchain technology and SHA-256 encryption are the key attributes used to evolve security and privacy in vehicular ad hoc networks by employing the suggested pseudonym-based authentication solution. The results indicate that the decentralized system works bogus identity monitoring and unwanted access non-violence when research or experiment placed in regards to vibration and noise pollution are conducted through the secure channels by regularly changing pseudonyms while still effectively communicating safely and privately. The immutable nature of blockchain guarantees asked data not to be the subject of manipulations, thereby, reducing the danger of replay and spoofing attacks. The fact that blockchain technology becomes a solution to us made it clear that the weaknesses are addressed and eliminated so fast in comparison to the past. The study of performance lies in the ability of the system to create keys, verify messages, and control the cryptographic identities partly with the small amount of the processor in this work. Nevertheless, it is quite essential to solve these issues with especially the system when the traffic is high, which implies that further optimization should be proceeded.

In the end of all these the outcomes clearly demonstrate that the proposed system is able to offer a perfect and confidential solution for ITS, thus, resulting in a significant boost of vehicle network security.

Precision

$Precision=TP+FP/TP$

Recall

$Recall=TP+FN/\ TP$

F1-Score

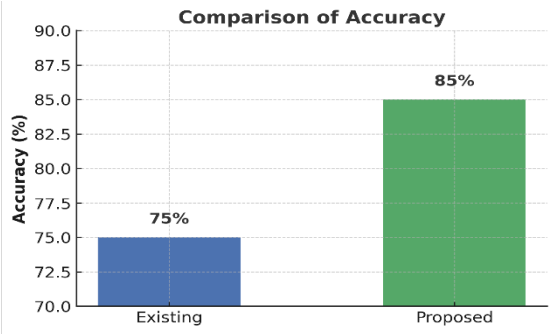
$F1\text{-}Score=2\times Precision+Recall/\ Precision\times\ Recall$

Accuracy

$Accuracy=TP+TN+FP+FN/\ TP+TN$

Algorithm	Accuracy
Existing	75
Proposed	85

COMPARISON TABLE



COMPARISON GRAPH

CONCLUSION

The proposed solution is to have an effective and safe VANET because of the combination of the blockchain-based solution with SHA-256 and a pseudonym-based system of authentication. The system for secure vehicular networks' using Roadside Units (RSUs) for data integrity, privacy, and authentication dependability has been improved by cryptographic key management and regular pseudonym updates. Declaring the fact that no central point of failure jeopardizes the security of the distributed design and still enables transparency with the use of a not mutable blockchain ledger is not enough to say that / Nevertheless, latency and scalability are the main concerns, these problems should not overshadow the potential of the system to assure safe vehicle interactions and also provide a more secure and efficient transportation system.

FUTURE WORK

Subsequent studies will focus on enhancing the proposed system's scalability and performance via computing overhead minimization and blockchain consensus mechanism optimization. Real-time verification can be enhanced further and latency minimized by implementing edge computing and lightweight cryptography strategies. The system can also be made resilient against evolving cyber threats by employing artificial intelligence-based anomaly detection and adaptive security features. The framework will be more relevant in future intelligent transportation networks if it is developed further to ensure compatibility with advanced automobile technologies such as 5G and autonomous driving platforms.

REFERENCES

[1] "Vehicular distributed computing: Architectures, applications, and portability," edited by Boukerche and E. Robson, Computer organisations, vol. 135, pp. 171–189, 2020.

[2] "A first glance at personality the board plans on the blockchain," by P. Dunphy and F. A. Petitcolas, IEEE Security and Privacy, vol. 16, no. 4, pp. 20–29, 2021.

[3] "Blockchain advances for the web of things: Research issues and difficulties," IEEE Internet of Things Journal, vol. 6, no. 2, pp. 2188–2204, 2020; M. A. Ferrag, M. Derdour, M. Mukherjee, A. Derhab, L. Maglaras, and H. Janicke.

[4] "Privacy preserving client character in Identity-as-a-Service," presented by T. H. Vo, W. Fuhrmann, and K.-P. Fischer-Hellmann at the 21st Conference on Innovation in Clouds, Internet and Networks and Workshops (ICIN) in 2018. IEEE, 2021, 1–8 pages.

[5] X. Zhu and Y. Badr, "Character the executives' frameworks for the Internet of Things: A study towards blockchain arrangements," Sensors, vol. 18, no. 12, p. 4215, 2021.

[6] Cui, J., Zhang, J., Zhong, H., Xu, Y.: SPACF: Secure privacy-preserving authentication for VANETs using a cuckoo filter. IEEE Trans. Veh. Technol. 66(11), 10283–10295 (2017).

[7] Nakamoto, S.: Bitcoin: A decentralized peer-to-peer electronic cash system. Consulted (2008).

[8] Wood, G.: Ethereum: A secure, decentralized, and generalized transaction ledger. Ethereum Project Yellow Paper 151(2014), 1–32 (2014).

[9] Tzeng, S.-F., Horng, S.-J., Li, T., Wang, X., Huang, P.-H., Khan, M.K.: Strengthening

security and privacy in identity-based batch verification for VANETs. IEEE Trans. Veh. Technol. 66(4), 3235–3248 (2017).

[10] Malhi, A., Batra, S.: Privacy-focused authentication framework leveraging bloom filters for secure vehicular communication. Springer-Verlag (2016).

[11] Sun, C., Liu, J., Xu, X., Ma, J.: Privacy-preserving mutual authentication with resistance to DoS attacks in VANETs. IEEE Access 5, 24012–24022 (2017).

[12] He, D., Chan, S., Guizani, M.: An efficient, accountable, and privacy-enhancing authentication framework for wireless networks. IEEE Trans. Veh. Technol. 65(3), 1605–1614 (2016).

[13] Rajput, U., Abbas, F., Eun, H., Oh, H.: Hybrid privacy-preserving authentication for VANETs. IEEE Access 5, 12014–12030 (2017).

[14] Vo, T.H., Fuhrmann, W., Fischer-Hellmann, K.-P.: Privacy preserving client character in Identity-as-a-Service. In: 21st Conference on Innovation in Clouds, Internet and Networks and Workshops (ICIN), pp. 1–8. IEEE, (2021).

[15] Wu, T.-Y., Yang, L., Lee, Z., Chu, S.-C., Kumari, S., Kumar, S.: A three-factor authentication protocol for wireless sensor networks with provable security. Wirel. Commun. Mob. Comput. 2021, 15 pages (2021).

[16] Zhu, X., Badr, Y.: Character the executives' frameworks for the Internet of Things: A study towards blockchain arrangements. Sensors 18(12), 4215 (2021).

[17] Menezes, J., Vanstone, S.A.: Implementation and applications of elliptic curve cryptosystems. J. Cryptol. 6(4), 209–224 (1993).

[18] Cheng, J., Chen, M., Zhou, M., Gao, S., Liu, C., Liu, C.: Detecting change-points in overlapping communities within evolving networks. IEEE Trans. Big Data 6(1), 189–200 (2020).

[19] Chaudhry, S.A.: Remarks on a secure, privacy-preserving, and lightweight authentication protocol for VANETs. IEEE Sens. J. 22(13), 13763–13766 (2022).

[20] Chuang, M.-C., Lee, J.F.: TEAM: An extended trust-based authentication mechanism for VANETs. IEEE Syst. J. 8(3), 749–758 (2013).