International Research Journal of Education and Technology
Peer Reviewed Journal
ISSN 2581-7795

MULTIDOMAIN PRIVACY-PRESERVING AUTHENTICATION IN VEHICULAR AD-HOC NETWORKS USING BLOCKCHAIN TECHNOLOGY

Manish R C
Department of Artificial Intelligence and Data Science
Bannari Amman Institute of Technology
Tamil Nadu, India
manish.ad20@bitsathy.ac.in

Suriya Narayanan R
Department of Artificial Intelligence and Data Science
Bannari Amman Institute of Technology
Tamil Nadu, India
suriyanarayanan.ad20@bitsathy.ac.in

Sanjithkumar J
Department of Computer Science and Engineering
Bannari Amman Institute of Technology
Tamil Nadu, India
sanjithkumar.cs20@bitsathy.ac.in

Kiruthiga R
Department of Artificial Intelligence and Data Science
Bannari Amman Institute of Technology
Tamil Nadu, India
kiruthigar@bitsathy.ac.in

ABSTRACT

In the field of vehicle ad-hoc networks (VANETs), the integration of vehicular wireless communication technologies has substantially improved driving safety and facilitated intelligent transportation applications. However, current authentication techniques are primarily concerned with vehicle security inside a single administrative domain, ignoring the overarching oversight required in the complex intelligent transportation system. In response, this research proposes a unique multidomain vehicle authentication architecture that uses blockchain technology to generate distributed trust and promote cross-domain information sharing across various administrative domains. Our suggested pseudonym-based privacy-preserving authentication mechanism assures anonymity and traceability, meeting the demand for increased security in the intelligent transportation ecosystem. To improve authority monitoring and key escrow robustness, we propose a two-phase pseudonym distribution mechanism that is conducted cooperatively with the help of a roadside unit (RSU) proxy. Our scheme's effectiveness and practicality in multidomain scenarios are demonstrated through thorough security analysis and compared evaluations with existing methods. The feasibility and effectiveness of the suggested blockchain-based multidomain authentication strategy are further demonstrated by real-world experiments, which also highlight the scheme's potential influence on improving the security and privacy environment in automotive communication networks.

Index Terms— Multidomain Authentication, Privacy-Preserving Authentication, vehicular ad-hoc network (VANET), Blockchain Technology, Security Analysis.

I. INTRODUCTION

The integration of Vehicular Ad-Hoc Networks (VANETs) has brought about a new era of intelligent transportation systems and driving safety in the ever-changing landscape of modern transportation. In addition to improving traffic safety, the development of cutting-edge vehicle wireless communication technology has opened the door for a wide range of intelligent transportation applications. The necessity for strong vehicular authentication systems has been highlighted by the growing complexity of vehicle manufacture and the wide range of intelligent transport terminals. Authentication systems that are now in place, however, have mostly been concerned with maintaining security within certain administrative domains, which has resulted in a deficiency in the oversight of authorities and entities within the larger intelligent transportation system. Recognizing this gap, we propose a cutting-edge multidomain vehicle authentication architecture to solve the limits of current authentication methods. This revolutionary system uses blockchain technology to generate distributed trust and facilitate smooth cross-domain information sharing across various administrative domains. The value of this multidomain strategy stems from its capacity to bridge gaps between various entities, resulting in a comprehensive and secure intelligent transportation environment. To protect user privacy in this networked vehicle network, we present a

pseudonym-based privacy-preserving authentication technique. This solution assures not only anonymity but also traceability, which aligns with the increased security requirements of intelligent transportation systems. In response to the necessity for authority monitoring and resilience to key escrow issues, our study proposes a two-phase pseudonym distribution system. This technique works in conjunction with a roadside unit (RSU) proxy, which strengthens the authentication process.

We perform a thorough security study and compare our suggested system with previous efforts to demonstrate its superiority in order to validate its effectiveness. To show the effectiveness and viability of the blockchain-based multidomain authentication technique in a variety of circumstances, real-world tests are implemented. Our introduction lays the groundwork for a more thorough examination of the complex issues and potential solutions surrounding vehicular authentication, opening the door to improvements in privacy and security for intelligent transportation networks.

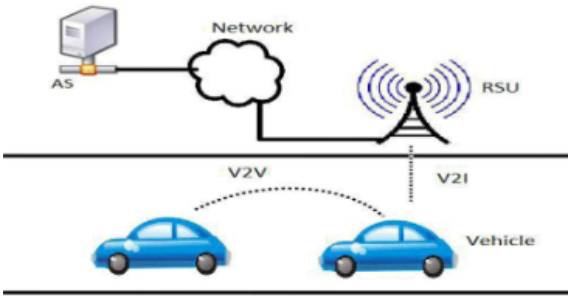


Fig: vehicle communication

Vehicle-to-Vehicle (V2V) Communication: Within a network, V2V communication is the direct sharing of data between cars. V2V communication is essential to our suggested system's ability to support intelligent transportation applications and improve driving safety. Vehicles can exchange real-time information about their position, speed, and other pertinent data through vehicle-to-vehicle (V2V) communication. This facilitates cooperative awareness between cars, enabling them to react as a group to possible threats, traffic situations, or other important occurrences. Even in a dynamic vehicle-to-vehicle communication environment, trust and privacy are established using the blockchain-based multidomain authentication architecture, which guarantees the secure and authenticated exchange of information between vehicles.

Vehicle-to-Infrastructure (V2I) Communication: This type of communication is information sharing between cars and roadside infrastructure elements, including RSUs. Collaboration with RSU proxies facilitates V2I communication in our proposed system. Serving as middlemen, the RSUs contribute to the overall security of the authentication process by helping to carry out the two-phase pseudonym distribution mechanism. A more reliable and well-coordinated intelligent transportation system is ensured by the interaction between cars and infrastructural elements. It enables the transmission of data, including traffic conditions, road updates, and possible hazards, from the infrastructure to automobiles. By including V2I communication, the multidomain authentication technique becomes more dependable and efficient overall, strengthening the vehicular network's resilience and interconnectivity.

II. RELATED WORK

Lei Zhang, Member, Chuanyan Hu, Qianhong Wu [1] a message collector, such as a traffic management authority, can re-aggregate the aggregated signatures. Our hierarchical aggregation technique considerably reduces the transmission/storage overhead of cars and other parties. Furthermore, conventional batch verification systems in vehicular ad hoc networks need vehicles to wait for a sufficient number of messages before performing batch verification. In contrast, we expect that vehicles will generate messages (and related signatures) in specific time intervals, allowing them to begin the batch verification procedure after only a brief delay. Simulation demonstrates that a vehicle can validate received messages with very low latency and a quick response.

Fengzhong Qu, Senior Member, Zhihui Wu [2] vehicular ad hoc networks (VANETs) have sparked attention in both academic and industrial settings because, once deployed, they will provide drivers with a novel driving experience. However, communicating in an open-access environment raises security and privacy concerns, which may jeopardize the large-scale adoption of VANETs. Researchers have offered numerous solutions to these problems. We begin this study by presenting background information on VANETs and categorizing security vulnerabilities that affect VANETs. After defining the requirements that suggested solutions to security and privacy challenges in VANETs must meet, we explain the general secure procedure and identify the authentication mechanisms used in these processes.

Ei Mon Cho, Maharage Nisansala Sevwandi Perera [3] the security and privacy concerns associated with internet-connected cars have gained traction due to the Internet of Vehicles (IoV) research trend. To minimize the expense of safely validating certificates, we concentrate on certificate administration. In this work, we address the management and distribution of the

Certificate Revocation List (CRL) in vehicle public key infrastructure (PKI) using blockchain technology. Activation codes are used in our proposed approach to validate the certificate based on the time to non-revoked vehicle for blockchain mechanism. Our goal is to lower the verification expenses and automatically erase the cars' inactive certificates.

Anusha Vangala , Basudeb Bera , Sourav Saha [4] in this work, we build a new scheme, named BCAS-VADN, for vehicle accident detection and notification in ITS that is supported by blockchain and relies on certificates for authentication. If an accident is observed on the road by any of the vehicles in the BCAS-VADN network, whether its own or a neighboring vehicle(s), each vehicle can securely notify the adjacent Cluster Head (CH) of the transaction through the authentication procedure. The transactions that the CH receives from the cars are then securely sent to its RSU, where they are subsequently safely accepted by the ESs. The ES is in charge of preparing a partial block containing transactions and the Merkle tree root, as well as a digital signature on that information, which it then sends to its associated Cloud Server (CS) in the Blockchain Center (BC) for complete block creation, verification, and addition using the designed consensus process.

M Janani priya, G Yamuna [5] the suggested system focuses on analyzing a cloud integrity auditing model in which the security and privacy of the system are audited, with privacy determined using a machine learning method. The suggested model is built on a hybrid CatBoost algorithm (HCBA), with input data stored in the cloud platform via Bring Your Own Encryption Key (BYOEK). The security of the BYOEK model is assessed and validated against the supplied test model in terms of execution time versus data transfers. Business Associates frequently visit the cloud platform to store and retrieve data pertaining to communications, business model design, and other business-related activities. When looking at cloud storage from a security perspective, data must be extremely secure and accessible only through authentication.

III. PROPOSED SYSTEM

In this is propose a pioneering multidomain vehicular authentication architecture that takes advantage of blockchain technology's transformational powers. The primary goal is to create a decentralized framework that extends beyond specific administrative domains, fostering distributed trust and facilitating smooth information sharing across various parts of the intelligent transportation system. To meet the urgent requirement for increased security and privacy, we use a pseudonym-based authentication mechanism that ensures anonymity and traceability. This unique solution protects user identities while allowing for the surveillance of vehicular activities inside the network. To improve authority monitoring and robustness to key escrow issues, we developed a two-phase pseudonym distribution system. This technique, when used in conjunction with a roadside unit (RSU) proxy, provides an additional layer of protection to the authentication process. Our proposed solution solves the constraints of current identification systems while also laying the groundwork for a more secure and integrated intelligent transportation ecosystem. Our approach's efficiency and feasibility are supported by thorough security analysis and real-world trials, indicating its potential to improve vehicular communication network standards.

3.1 Vehicular ad-hoc networks *(VANET)*

The purpose of vehicular ad-hoc networks, or VANETs, is to improve road safety and transit efficiency through specialized wireless communication networks. Vehicles with communication devices connected to the roadside infrastructure create a dynamic network known as VANETs, which enables real-time information transmission between the vehicles and the infrastructure. Important information like traffic conditions, potential risks on the road, and emergency alerts can be shared thanks to this connection. Through facilitating vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication, VANETs are essential to the operation of intelligent transportation systems. Enhancing traffic flow, lowering accident rates, and facilitating the creation of cutting-edge transportation apps for a safer and more intelligent driving experience are the main objectives of VANETs.

3.1.1VANET structure

The Trust Authority (TA), Key Generation Center (KGC), Roadside Unit (RSU), and On-Board Unit (OBU) are the four fundamental components that make up the structural underpinning of our proposed vehicular ad-hoc network (VANET) architecture. Every entity has a unique and crucial role to play in maintaining the multidomain vehicular authentication system's operation and security.

International Research Journal of Education and Technology
Peer Reviewed Journal
ISSN 2581-7795

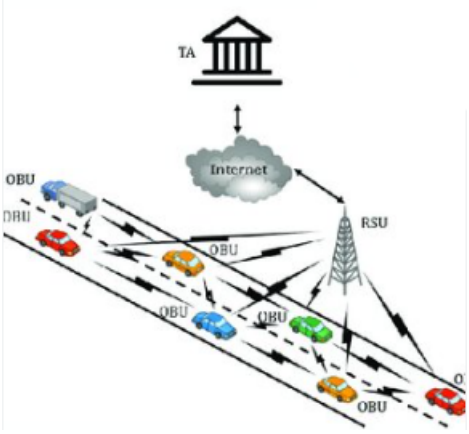


Fig: VANET diagram

The *Trust Authority (TA)* is the key body in charge of supervising and maintaining trust on the VANET. It is critical for assessing entities' validity and managing trust relationships across multiple administrative domains. The TA builds trust and serves as a supervisory entity, ensuring the system's integrity.

The *Key Generation Centre (KGC)* is responsible for the creation and distribution of cryptographic keys required for safe communication within the VANET. It works with the TA to make sure that keys are transferred securely and efficiently. The KGC plays a critical role in building a secure foundation for communication between automobiles and infrastructure components.

Roadside Units (RSUs) are strategically placed infrastructure devices that enable communication between automobiles and the larger intelligent transportation system. They serve as middlemen in the authentication process, enabling the secure flow of information and facilitating the dissemination of pseudonyms. RSUs improve the overall efficiency and dependability of the vehicle communication network.

Vehicle-specific embedded communication devices are called *On-Board Units (OBUs)*. They are essential to carrying out the suggested privacy-preserving authentication approach based on pseudonyms. OBUs exchange cryptographic keys and pseudonyms with one another using V2V communication to provide safe and anonymous exchanges. The OBUs actively engage in the authentication procedure, enhancing the VANET's overall security stance.

In the system architecture involves collaborative efforts to overcome the issues of multidomain vehicular authentication through the novel integration of blockchain technology and advanced cryptographic methods.

3.2 Privacy-preserving authentication

Privacy-preserving authentication is an important component in safeguarding communication systems, especially in situations where user anonymity and sensitive information are vital. This notion entails implementing authentication systems that allow users to authenticate their identity or authority without disclosing unneeded information about themselves. In the context of vehicular ad-hoc networks (VANETs) or other communication systems, privacy-preserving authentication ensures that information, such as cryptographic credentials or pseudonyms, is exchanged in a way that respects the user's confidentiality. In a vehicle network, for example, privacy-preserving authentication mechanisms frequently make use of pseudonyms or temporary IDs. Instead of revealing a vehicle or user's true identity, pseudonyms are used to allow entities to interact and verify without providing sensitive information. Cryptographic approaches, such as zero-knowledge proofs or homomorphic encryption, can help to improve privacy by allowing credentials to be verified without revealing their real content. Privacy-preserving authentication seeks to achieve a balance between the necessity for safe communication and the protection of individual privacy. Implementing these strategies allows communication systems to authenticate entities while reducing the leakage of personal information, promoting a safe and privacy-conscious environment for users.

3.3 Pseudonym-Based Privacy-Preserving Authentication

Pseudonym-based privacy-preserving authentication is a technique for enabling secure communication while protecting user privacy in systems such as vehicular ad hoc networks (VANETs). Instead of using permanent and personally identifiable information for authentication, this technique assigns entities temporary and pseudonymous identifiers. These pseudonyms serve as surrogates for actual identities, allowing entities to communicate securely while retaining sensitive personal information.

In the context of VANETs, cars are allocated pseudonyms that change on a regular basis, making it difficult for unauthorized entities to track or identify specific vehicles over time. This dynamic pseudonym assignment protects user anonymity while also preventing hostile actors from persistently tracking specific automobiles. In the entities utilizing pseudonyms exchange cryptographic credentials or proofs as part of the authentication procedure. By doing this, it is made possible for the entities to confirm one another's legitimacy without revealing their true identities. To accomplish secure and privacy-preserving authentication,

International Research Journal of Education and Technology
Peer Reviewed Journal
ISSN 2581-7795

methods such as digital signatures, zero-knowledge proofs, or other cryptographic algorithms are frequently used. Systems can achieve a balance between the requirement for secure communication and the protection of user privacy by implementing pseudonym-based privacy-preserving authentication, particularly in settings where maintaining anonymity is essential. By reducing the dangers connected with the disclosure of personally identifiable information, this strategy helps to increase confidence in communication networks.

3.4 Blockchain-based multidomain authentication

This system's suggested blockchain-based multidomain authentication architecture is a ground-breaking method for handling the intricate problems in vehicular ad hoc networks (VANETs). Fundamentally, the design transcends the boundaries of distinct administrative domains by integrating blockchain technology to create a decentralized and distributed trust model. This design facilitates smooth collaboration between the four key entities: Trust Authority (TA), Key Generation Center (KGC), Roadside Unit (RSU), and On-Board Unit (OBU). In order to maintain the integrity of the system as a whole, the Trust Authority manages trust relationships. A crucial part of securely producing and dispersing cryptographic keys is the Key Generation Center. By serving as go-betweens, Roadside Units provide safe communication between automobiles and the larger infrastructure. Through V2V communication, the On-Board Units, implanted within cars, participate in pseudonym-based privacy-preserving authentication. The blockchain functions as an immutable and transparent ledger that records and validates authentication transactions across domains. This architecture not only improves security but also allows for efficient cross-domain information sharing, assuring the durability of the vehicular communication network. Our suggested architecture, which takes advantage of blockchain's decentralized and tamper-resistant characteristics, provides a substantial leap in maintaining the trust, privacy, and security of intelligent transportation systems in a multidomain setting.

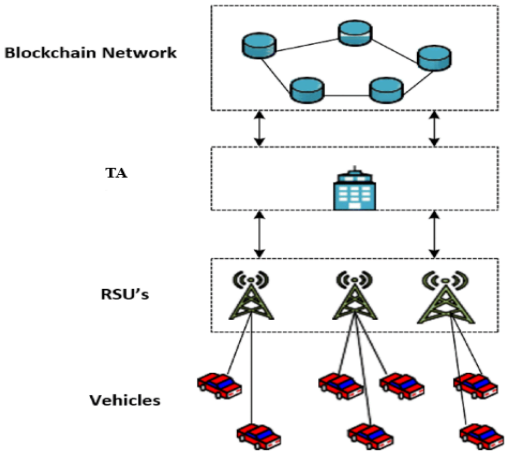
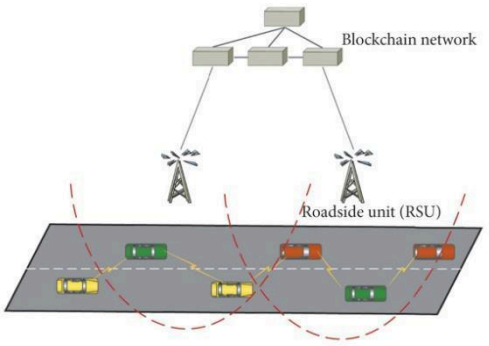


Fig: Blockchain based secure communication

3.4.1 Blockchain-based security methods



A blockchain-based secured data technique makes use of blockchain technology to improve the security and integrity of stored data. This approach organizes data into blocks, with each block including a cryptographic hash of the previous block, resulting in a linked chain of blocks. The blockchain's decentralized and distributed structure assures that data uploaded to the network is tamper-resistant and immutable.

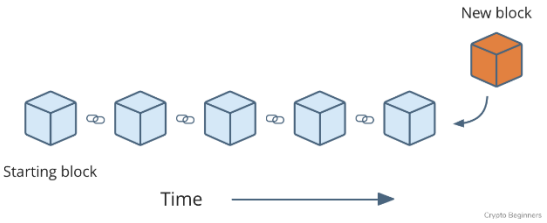


Fig: Blockchain linked new block

The employment of cryptographic techniques improves data security by cryptographically linking each block to the one before it, producing a continuous and secure chain. Public-key cryptography is commonly used

to protect transactions, ensuring that only authorized parties have access to the data. Smart contracts, which are self-executing contracts with the terms of the agreement explicitly put into code, can also be linked into the blockchain to provide further security. These contracts automate and enforce established norms and conditions, lowering the likelihood of fraud or illegal access to data. A blockchain-based secured data approach offers a strong and transparent foundation for data security via decentralization, cryptographic hashing, consensus mechanisms, and smart contracts. This technique protects data integrity while simultaneously ensuring transparency, traceability, and resistance to illegal changes.

IV. CONCLUSION

In conclusion, the multidomain authentication architecture based on blockchain that has been suggested offers a novel way to address the issues with vehicular ad hoc networks. The system creates a decentralized trust model by incorporating blockchain technology, guaranteeing the security and anonymity of communication between various administrative domains. Roadside Units, On-Board Units, the Trust Authority, and the Key Generation Center work together to build a strong framework for privacy-preserving authentication. Pseudonyms, cryptographic keys, and the blockchain's immutability all work to improve data confidentiality and integrity. The architecture shows its efficiency and feasibility through thorough security research and real-world trials, representing a major advancement in the security landscape of intelligent transportation systems in multidomain scenarios.

V. REFERENCE

1. L. Guo, M. Dong, K. Ota, Q. Li, T. Ye, J. Wu, and J. Li, “A secure mechanism for big data collection in large scale internet of vehicle,” IEEE Internet of Things Journal, vol. 4, no. 2, pp. 601–610, April 2017.
2. Y. Liu, W. Guo, C.-I. Fan, L. Chang, and C. Cheng, “A practical privacy-preserving data aggregation (3pda) scheme for smart grid,” IEEE Transactions on Industrial Informatics, pp. 1–1, 2018.
3. C. Lin, D. He, X. Huang, N. Kumar, and K.-K. R. Choo, “BCPPA: A blockchain-based conditional privacy-preserving authentication protocol for vehicular ad hoc networks,” IEEE Trans. Intell. Transp. Syst., early access, Jun. 30, 2020,
4. J. Contreras-Castillo, S. Zeadally, and J. A. Guerrero-Ibañez, “Internet of vehicles: Architecture, protocols, and security,” IEEE Internet Things J., vol. 5, no. 5, pp. 3701–3709, Oct. 2018.
5. J. Wang, J. Liu, and N. Kato, “Networking and communications in autonomous driving: A survey,” IEEE Commun. Surveys Tuts., vol. 21, no. 2, pp. 1243–1274, 2nd Quart., 2019.
6. B. Brecht et al., “A security credential management system for V2X communications,” IEEE Trans. Intell. Transp. Syst., vol. 19, no. 12, pp. 3850–3871, Dec. 2018.
7. Y. Li et al., “Direct acyclic graph-based ledger for Internet of Things: Performance and security analysis,” IEEE/ACM Trans. Netw., vol. 28, no. 4, pp. 1643–1656, Aug. 2020.
8. Y. Yao, X. Chang, J. Mišic, V. B. Miši ´ c, and L. Li, “Bla: Blockchain- ´ assisted lightweight anonymous authentication for distributed vehicular fog services,” IEEE Internet Things J., vol. 6, no. 2, pp. 3775–3784, Apr. 2019.
9. J. Cui, X. Zhang, H. Zhong, Z. Ying, and L. Liu, “RSMA: Reputation system-based lightweight message authentication framework and protocol for 5G-enabled vehicular networks,” IEEE Internet Things J., vol. 6, no. 4, pp. 6417–6428, Aug. 2019.
10. A.K. Sutrala, P. Bagga, A. K. Das, N. Kumar, J. J. P. C. Rodrigues, and P. Lorenz, “On the design of conditional privacy preserving batch verification-based authentication scheme for Internet of Vehicles deployment,” IEEE Trans. Veh. Technol., vol. 69, no. 5, pp. 5535–5548, May 2020.
11. M. Shen et al., “Blockchain-assisted secure device authentication for cross-domain industrial IoT,” IEEE J. Sel. Areas Commun., vol. 38, no. 5, pp. 942–954, May 2020.
12. A. Jolfaei and K. Kant, “Data security in multiparty edge computing environments,” in Proc. Government Microcircuit Appl. Crit. Technol. Conf., Artif. Intell. Cyber Secur., Challenges Opportunities Government, Albuquerque, NM, USA, 2019, pp. 17–22.
13. R. Canetti and H. Krawczyk, “Universally composable notions of key exchange and secure channels,” in Proc. Int. Conf. Theory Appl. Cryptograph. Techn., Amsterdam, The Netherlands, 2002, pp. 337–351.
14. H. Tan and I. Chung, “Secure authentication and key management with blockchain in VANETs,” IEEE Access, vol. 8, pp. 2482–2498, 2020.
15. M. Wazid, A. K. Das, V. Odelu, N. Kumar, and W. Susilo, “Secure remote user authenticated key establishment protocol for smart home environment,” IEEE Trans. Dependable Secure Comput., vol. 17, no. 2, pp. 391–406, Mar. 2020.