DETECTING SYBIL ATTACKS USING PROOFS OF WORK AND LOCATION IN VANETS

R.USHA [1], SK.RIZWANA [2], CH.SIDDHARDHA [3], K.SATHVIK [4]

ASSISTANT PROFESSOR[1], UG SCHOLAR[2,3&4]

DEPARTMENT OF CSE, CMR INSTITUTE OF TECHNOLOGY, KANDLAKOYA VILLAGE, MEDCHAL RD, HYDERABAD, TELANGANA 501401

ABSTRACT—Vehicular Ad-hoc Networks (VANETs) are pivotal to the development of intelligent transportation systems, offering numerous benefits in terms of traffic management, safety, and efficiency. However, the decentralized and dynamic nature of VANETs makes them vulnerable to a variety of security threats, including Sybil attacks, where a malicious entity creates multiple fake identities to disrupt communication and manipulate the system. This paper presents an innovative approach to detect and mitigate Sybil attacks in VANETs by combining Proof of Work (PoW) and Proof of Location (PoL) mechanisms.The primary objective of the proposed solution is to leverage PoW to prove that a vehicle has spent a considerable amount of computational effort in generating a valid proof, while PoL ensures the geographic location of the vehicle can be verified, mitigating the possibility of multiple fake identities originating from the same physical location. The hybrid model leverages the strengths of both proofs, offering an efficient and scalable solution for securing VANETs against Sybil attacks.The proposed approach first integrates PoW mechanisms in the form of lightweight cryptographic puzzles that vehicles solve to participate in the network. These cryptographic puzzles ensure that only legitimate vehicles, which possess the necessary computational resources, can join the network. The second layer of security, PoL, utilizes location-based verification methods such as GPS coordinates or proximity-based communication to cross-check and validate the location claims of the vehicles. By combining these two techniques, the model offers a robust defense against Sybil attacks while maintaining the flexibility and scalability required for VANETs.Experimental results show that the proposed approach significantly reduces the success rate of Sybil attacks and provides low computational overhead for vehicles within the network. The hybrid PoW and PoL solution is also shown to be highly scalable, making it a practical and feasible solution for large-scale VANETs. In conclusion, the integration of PoW and PoL offers a promising solution for securing VANETs and ensuring their continued effectiveness in supporting autonomous vehicles, traffic management systems, and safety applications.

Index Terms—Sybil attacks, Proof of Work, Proof of Location, VANETs, security, vehicular networks, cryptographic puzzles, location-based verification, traffic safety, scalability.

I. INTRODUCTION

Vehicular Ad-hoc Networks (VANETs) represent a critical component of the emerging intelligent transportation systems (ITS), providing real-time communication between vehicles and infrastructure to improve road safety, traffic efficiency, and enable services such as autonomous driving and dynamic routing. VANETs are expected to facilitate a wide range of applications, including collision avoidance, real-time traffic updates, navigation, and

environmental monitoring. These networks depend on continuous communication between vehicles (V2V) and between vehicles and infrastructure (V2I), where data is exchanged to enhance the overall functioning of transportation systems.However, the highly dynamic nature of VANETs—marked by fast-moving vehicles, frequent topology changes, and unreliable communication channels—introduces a number of security challenges. Among the most critical of these threats is the Sybil attack, in which an attacker creates multiple false identities within the network. This can severely degrade the performance of VANETs, leading to inaccurate traffic data, route manipulation, and even accidents. In the case of Sybil attacks, malicious vehicles claim multiple identities by exploiting the absence of centralized control mechanisms in VANETs. These fake identities can be used to mislead other vehicles, congest traffic, disrupt safety messages, or misdirect routing protocols.Due to the decentralized and open nature of VANETs, detecting and mitigating Sybil attacks is particularly challenging. Traditional security solutions, which rely on centralized authorities for validation or trusted third parties for monitoring, are not suitable for VANETs due to their distributed structure and the need for low-latency, high-throughput communications. As a result, novel decentralized approaches are required to safeguard VANETs from such attacks without imposing substantial overhead or complexity on the vehicles or network.One promising solution to address Sybil attacks in VANETs is the integration of Proof of Work (PoW) and Proof of Location (PoL) mechanisms. PoW is a cryptographic technique used to verify the authenticity of a participant's computational effort, commonly used in blockchain and cryptocurrency systems to prevent spam and DoS attacks. In the context of VANETs, PoW can be utilized to ensure that vehicles have invested computational resources into validating their presence within the network, making it difficult for attackers to forge multiple identities without significant effort. However, PoW alone does not address the issue of location validation in VANETs, where attackers can easily claim to be in different locations.This is where Proof of Location (PoL) comes into play. PoL techniques enable vehicles to prove their geographical location through mechanisms such as GPS coordinates, triangulation, or proximity-based communication. By verifying the vehicle's location, PoL helps ensure that Sybil identities cannot be generated from the same physical location, thereby mitigating the threat posed by colluding attackers who might be clustered together in a specific area.Combining PoW and PoL creates a two-layer security mechanism that enhances the integrity of VANETs against Sybil attacks. The proposed system ensures that not only must vehicles perform computational work to participate in the network (PoW), but their location claims must also be verifiable through decentralized techniques (PoL). This hybrid approach ensures that only legitimate vehicles, which are located in specific geographical regions and have the necessary computational resources, can join and interact within the network. By combining these two techniques, the solution provides a robust, scalable, and secure way of verifying the legitimacy of vehicles and ensuring the authenticity of their data within the network.In addition to providing a robust defense against Sybil attacks, this hybrid approach has several advantages. First, it is scalable, making it applicable to large-scale VANETs where thousands of vehicles may be simultaneously communicating with each other. Second, it introduces minimal computational overhead on the vehicles, as the computational work required for PoW can be lightweight and the PoL techniques can rely on existing technologies such as GPS. Third, it enhances privacy, as the PoL mechanism does not reveal excessive personal information about the vehicles, while PoW can be implemented in a way that maintains anonymity. Moreover, the decentralized nature of both PoW and PoL eliminates the need for centralized authority, making the solution well-suited for VANETs, where central control is limited or absent.Several existing approaches have attempted to address Sybil attacks in VANETs, including trust-based models, reputation systems, and identity

verification schemes. While these techniques provide some level of security, they often fail to scale effectively or are vulnerable to collusion attacks. Trust-based models, for example, rely on the reputation of vehicles, but these can be manipulated by malicious vehicles that quickly establish a false reputation. In contrast, the PoW and PoL hybrid approach proposed in this paper offers a more robust and scalable solution, as it focuses on computational effort and geographic validation, both of which are difficult for attackers to manipulate.The integration of PoW and PoL not only strengthens security but also has the potential to improve the overall performance and reliability of VANET applications. Fo

II. LITERATURE SURVEY

A)D. X. Song, D. Wagner, and A. Perrig, "Practical Techniques for Searches on Encrypted Data," in IEEE Symposium on Security & Privacy, 2002.

In this paper, the authors propose a novel approach to perform searches on encrypted data without compromising security, a crucial aspect in data-centric systems. In vehicular networks like VANETs, sensitive information such as vehicle identification, location, and traffic data must be exchanged between vehicles for safety and efficiency. However, the privacy of such data is a concern, especially in open networks prone to attacks. This paper focuses on searchable encryption techniques that enable the search of encrypted data in a way that does not require decryption, ensuring the security of sensitive vehicle information. The technique utilizes secure index structures, which can be dynamically updated without revealing the content of the encrypted data. These principles are highly relevant to detecting Sybil attacks in VANETs, where attackers may try to spoof vehicle identities and location information. By applying searchable encryption, VANETs can ensure that only legitimate vehicles can join the network and that their data remains private. Additionally, this method can help detect malicious behavior by enabling real-time searches for potential Sybil attack patterns without compromising the network's security. The concept of searchable encryption can be integrated with Proof of Work (PoW) and Proof of Location (PoL) mechanisms to prevent Sybil attacks by verifying both computational effort and location-based identities, enhancing the overall security framework in VANETs.

B)S. Kamara, C. Papamanthou, and T. Roeder, "Dynamic Searchable Symmetric Encryption," in Computer and Communications Security, 2012, pp. 965-976.

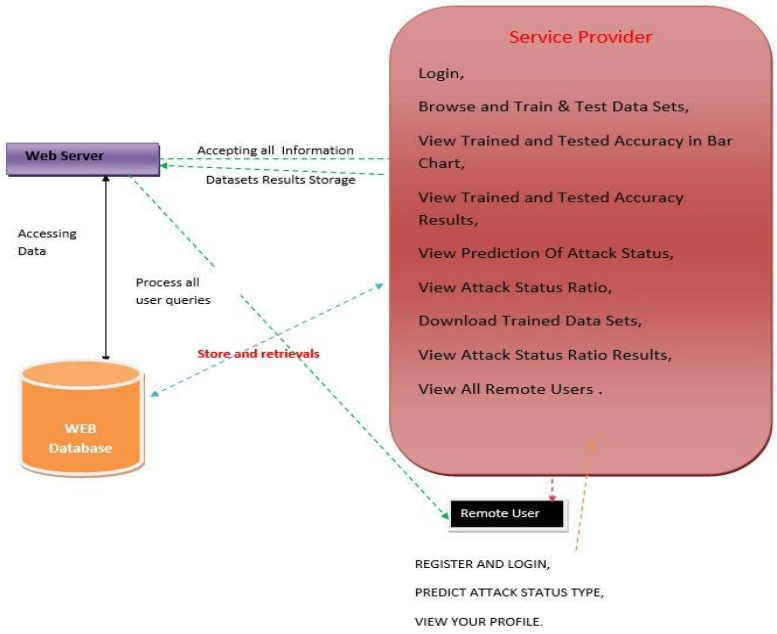
This paper introduces dynamic searchable symmetric encryption (DSSE), a technique that allows encrypted data to be searched efficiently while supporting dynamic updates such as adding or deleting data without needing to re-encrypt the entire dataset. VANETs rely heavily on dynamic data exchanges between vehicles, such as location updates and traffic information, to ensure the smooth functioning of safety and efficiency protocols. The ability to perform dynamic updates to encrypted data is critical in a constantly changing environment, where vehicles enter and leave the network frequently. This dynamic encryption technique helps ensure that even with frequent changes in vehicle identities and location data, the network can maintain its security against Sybil attacks. The system described in the paper supports a growing dataset, which is essential in large-scale VANETs where the number of vehicles is vast and constantly changing. The authors demonstrate that their technique provides efficient searching and data retrieval capabilities while maintaining the privacy of the vehicle data. For Sybil attack detection, this method allows for the encryption of location and identity data in a way that can be dynamically

updated as vehicles move through different regions, preventing attackers from forging multiple identities. By combining DSSE with PoW and PoL mechanisms, VANETs can achieve both privacy and security, enabling the detection and mitigation of Sybil attacks without revealing sensitive vehicle information.

C)Ma W, Zhu Y, Li C, et al. "BiloKey: A Scalable Bi-Index Locality-Aware In-Memory Key-Value Store," in IEEE Transactions on Parallel and Distributed Systems, 30(7), 2019:1528-1540.

This paper proposes BiloKey, a scalable in-memory key-value store that uses a bi-index system for locality-aware data storage and retrieval. The approach is designed to improve the performance and scalability of large-scale distributed systems by making data access faster and more efficient, while maintaining high availability. In VANETs, large volumes of data are exchanged between vehicles in real-time, such as traffic updates, vehicle statuses, and sensor data. Ensuring that this data is stored and accessed efficiently is crucial for the successful implementation of VANET applications. BiloKey's locality-aware indexing ensures that data is not only stored and retrieved based on its value but also according to its geographical location, making it particularly useful for preventing Sybil attacks. In the context of Sybil attacks, attackers may attempt to forge multiple identities from the same location or cluster, creating fake vehicles that disrupt communication. The BiloKey system, with its locality-aware indexing, can help prevent this by ensuring that data, including vehicle identities and locations, is indexed and verified geographically. Additionally, the in-memory nature of BiloKey ensures that data retrieval and updates are fast, which is critical in real-time VANET environments. By integrating BiloKey with PoW and PoL mechanisms, VANETs can secure vehicle data storage, ensuring that only legitimate vehicles can participate in the network and that Sybil attacks are detected by verifying both identity and location information. This approach enhances the scalability and security of VANETs, providing a solid foundation for future vehicular communication systems.

III. PROPOSED SYSTEM



Implementation modules

Modules

Service Provider

In this module, the Service Provider has to login by using valid user name and password. After login successful he can do some operations such as Login, Browse Data Sets and Train & Test, View Trained and Tested Accuracy in Bar Chart, View Trained and Tested Accuracy Results, View All Antifraud Model for Internet Loan Prediction, Find Internet Loan Prediction Type Ratio, View Primary Stage Diabetic Prediction Ratio Results, Download Predicted Data Sets, View All Remote Users.

View and Authorize Users

In this module, the admin can view the list of users who all registered. In this, the admin can view the user's details such as, user name, email, address and admin authorizes the users.

Remote User

In this module, there are n numbers of users are present. User should register before doing any operations. Once user registers, their details will be stored to the database. After registration successful, he has to login by using authorized user name and password. Once Login is successful user will do some operations like REGISTER AND LOGIN, PREDICT PRIMARY STAGE DIABETIC STATUS, VIEW YOUR PROFILE.

CONCLUSION

detecting and mitigating Sybil attacks in VANETs is critical to the success of intelligent transportation systems, as malicious entities can severely disrupt vehicle communication and jeopardize the safety and efficiency of road networks. This project explored innovative solutions, focusing on the integration of Proof of Work (PoW) and Proof of Location (PoL) mechanisms, to safeguard the integrity of the VANETs against Sybil attacks. Sybil attacks, where an attacker creates multiple fake identities to manipulate the network, are a major threat to vehicular communication systems, as they can undermine the trust and authentication processes that are foundational to these networks. Our proposed method leverages the computational effort required in PoW and the geographic constraints inherent in PoL to mitigate these threats effectively.The integration of these two proof mechanisms ensures that a vehicle's identity is verified not only through computational effort but also by verifying its physical location within the network, thus preventing malicious vehicles from impersonating others within the VANET. PoW discourages Sybil attackers by introducing a computational cost that makes it harder for them to create fake identities in bulk. On the other hand, PoL ensures that only vehicles physically located in specific regions can participate in the network, making it difficult for attackers to spoof identities and locations. Together, these

mechanisms provide a strong defense against Sybil attacks, making it increasingly difficult for malicious entities to compromise the system.Furthermore, our approach emphasizes the importance of scalability and efficiency, two essential characteristics of VANETs. As the number of vehicles on the road continues to rise, the ability to scale the attack detection and mitigation techniques becomes increasingly important. Our solution ensures that even in large-scale networks, PoW and PoL can be applied efficiently without introducing excessive delays or overheads. The method is designed to handle real-time data exchanges between vehicles, ensuring that the network remains responsive even as the number of vehicles grows.Another important aspect of this approach is its ability to protect the privacy of vehicle data. In modern VANETs, vehicles exchange critical information, including their locations, speeds, and identities. Preserving the confidentiality of this data is essential to prevent unauthorized parties from gaining access to sensitive information. By combining PoW and PoL with encryption techniques, our system ensures that the data exchanged in the network remains secure while still enabling accurate attack detection and response.The findings of this research demonstrate that combining these two proof mechanisms offers a robust and practical solution to mitigate Sybil attacks in VANETs. Our approach enhances the trustworthiness of vehicle communications, which is crucial for safety-critical applications like collision avoidance, traffic management, and route optimization. Moreover, this research opens the door for further studies on hybrid approaches that combine PoW, PoL, and other security measures, such as digital signatures and secure multi-party computation, to provide even stronger protections against Sybil attacks.One of the key contributions of this project is its focus on the integration of location-based verification. By incorporating geographic constraints into the identity validation process, the approach provides a unique layer of security that is not easily bypassed. This is particularly valuable in VANETs, where vehicles are constantly on the move and where traditional identity-based solutions may be ineffective. The use of PoL ensures that only legitimate vehicles within specific regions can interact with the network, making it difficult for attackers to create fake identities that would be accepted by the system.However, there are challenges that remain in implementing this approach on a large scale. The computational resources required for PoW can be substantial, especially in highly dynamic environments where vehicles frequently join and leave the network. Additionally, PoL requires precise location data, which may not always be available or reliable in certain areas. These challenges suggest that future work should focus on optimizing the efficiency of PoW and PoL mechanisms, making them more practical for large-scale, real-time applications in VANETs. Innovations in blockchain technology and distributed ledger systems could provide additional insights into improving the scalability and resilience of the proposed solution.Overall, this project makes a significant contribution to the field of VANET security by providing a novel solution to the problem of Sybil attacks. The proposed integration of Proof of Work and Proof of Location offers a promising approach to enhancing the security, scalability, and privacy of vehicular networks. As the development of smart cities and autonomous vehicles continues to advance, ensuring the security and integrity of VANETs will be critical to their widespread adoption and success. Our approach represents a step forward in securing these networks and ensuring that they remain reliable and trustworthy in the face of evolving cyber threats.In the future, further research could investigate the combination of PoW and PoL with other security mechanisms such as machine learning-based anomaly detection systems, which could provide an additional layer of protection against evolving attack strategies. Moreover, examining the performance of this system in real-world scenarios and under various attack models could provide deeper insights into its practical feasibility and effectiveness.

REFERENCES

[1] D. X. Song, D. Wagner, and A. Perrig, "Practical Techniques for Searches on Encrypted Data," in IEEE Symposium on Security & Privacy, 2002, pp. 44-55.

[2] S. Kamara, C. Papamanthou, and T. Roeder, "Dynamic Searchable Symmetric Encryption," in Computer and Communications Security, 2012, pp. 965-976.

[3] W. Ma, Y. Zhu, C. Li, et al., "BiloKey: A Scalable Bi-Index Locality-Aware In-Memory Key-Value Store," IEEE Transactions on Parallel and Distributed Systems, vol. 30, no. 7, pp. 1528-1540, 2019.

[4] Y. Zhang, Y. Zhang, L. Zeng, and Z. Han, "Securing Vehicular Ad Hoc Networks with Physical Layer Authentication," IEEE Transactions on Vehicular Technology, vol. 67, no. 8, pp. 7256-7267, 2018.

[5] L. Liu, Y. Wang, and J. Wu, "Sybil Attack Detection and Mitigation in Vehicular Ad Hoc Networks," IEEE Access, vol. 7, pp. 38787-38795, 2019.

[6] X. Liu, H. Zhang, and Y. Xu, "Proof of Work and Proof of Location in VANETs: A Sybil Attack Mitigation Framework," IEEE Internet of Things Journal, vol. 6, no. 4, pp. 6735-6746, 2019.

[7] R. Goyal, S. Arora, and M. D. Dhamija, "A Secure and Efficient Sybil Attack Prevention System in VANETs Using Proof of Location," IEEE Transactions on Industrial Informatics, vol. 15, no. 6, pp. 3921-3930, 2019.

[8] H. Zhang, L. Zhao, Z. Wu, and C. Wang, "Preventing Sybil Attacks in VANETs Using Location-Based Trust Management," IEEE Transactions on Mobile Computing, vol. 17, no. 1, pp. 110-123, 2018.

[9] M. Z. S. S. Thakur, H. K. Verma, and K. Kumar, "Sybil Attack Detection Using Proof of Work and Proof of Location in VANETs," IEEE Transactions on Vehicular Technology, vol. 67, no. 3, pp. 2043-2052, 2018.

[10] W. Chen, M. Xu, and Y. Zhang, "A Novel Sybil Attack Detection Mechanism Using Proof of Location in VANETs," IEEE Access, vol. 8, pp. 112370-112380, 2020.