Abstract

Vehicular Ad-Hoc Networks (VANETs) enable communication between vehicles and infrastructure to enhance road safety, traffic efficiency, and driver experience. However, the dynamic and decentralized nature of VANETs poses significant security and privacy challenges. Traditional authentication methods are often inadequate due to the need for real-time verification, the high mobility of vehicles, and the potential for malicious attacks. In this paper, we propose a secure blockchain-based authentication scheme that ensures conditional privacy preservation in VANETs.

Our approach leverages blockchain technology's immutability and decentralized trust mechanism to provide a robust framework for vehicular communication. By integrating smart contracts and cryptographic techniques, the proposed scheme allows vehicles to authenticate each other in a privacy-preserving manner while maintaining accountability. The authentication process is designed to be lightweight, ensuring efficiency and scalability in VANET environments where low-latency and high-throughput are critical.

We also introduce a conditional privacy preservation mechanism, where vehicles' sensitive data (such as location and travel history) is only disclosed under predefined conditions, such as during an emergency or a security incident. This approach not only reduces the risk of data misuse but also enhances user trust by ensuring that sensitive information is not exposed unnecessarily.

The performance of the proposed scheme is evaluated through simulations, showing significant improvements in terms of security, privacy, and authentication efficiency compared to existing solutions. Our findings suggest that the blockchain-based authentication scheme can effectively address the security and privacy challenges in VANETs, providing a scalable, secure, and privacy-preserving solution for future vehicular communication systems.