ISSN: 2633-4828 Vol. 6 No.1, January, 2024

International Journal of Applied Engineering & Technology

ANALYSIS OF SMART ROAD SAFETY USING BLOCKCHAIN

Nikunj Deepak Karolia[1], Dr. Amit Kumar Yadav[2] and Dr. Alam N. Shaikh[3]
[1,2]SRM University, India.
[3]Principal, Vasantdada Patil Pratishthan's, College of Engineering and Visual Arts, Sion, Mumbai, India
[1]ndkarolia2019@gmail.com

ABSTRACT
Our Research "Analysis of Smart Road Safety using Blockchain "is a with the rapid development of the informatization and industrialization of the Internet of Vehicles (IoV), the number and application of connected vehicles are growing rapidly. The safety problem is related to the property and life of human beings, which has attracted extensive attention from academic and industrial circles. Based on the study of high-quality literature published in the past decade and other high-level research works, this paper first analyzes the forms of attack against the Internet of Vehicles from the two aspects of attack mode and target. Then, it summarizes the existing blockchain-based system framework of the Internet of Vehicles (BIoV) and then discusses the security solutions of blockchain-based vehicles from the aspects of authentication, privacy, trust management, access control, and so on, to support the distributed system architecture and solve the security challenges of the Internet of Vehicles. Finally, the technical difficulties and the direction of further research of BIoV are summarized.

Keyword: Analysis, Smart, Road, Safety, Blockchain.

INTRODUCTION
IoV has become the most promising and fastest-growing new network paradigm and has also brought many applications, such as emergency communication of traffic incidents, traffic congestion prediction, and new traffic service modes. So in IoV, the secure transmission of V2X [1] is crucial. Suppose a hacker invades a regular vehicle or interferes with vehicle communications through eavesdropping, jamming, or spoofing attacks. In that case, there is a potential for serious accidents that can damage the vehicle or endanger the lives of passengers. Therefore, the primary safety goal of the Internet of Vehicles is to disseminate critical event information (such as accident reports) in a timely, safe, and accurate manner to ensure safe driving [2]. Most models of IoV are on centralized patterns. But the main problem with centralized mechanisms is the single point of failure problem. Many researchers have proposed distributed model schemes, but due to the dynamic nature of IoV, it has other issues, such as distributed vital management, content distribution, message trust, and data privacy. We should need a security mechanism to ensure that entities in IoV cannot manipulate, alter, or delete critical event messages in VANET. If critical event messages generated by vehicle entities are in a distributed database, all information will be transparent and shared. The security technology-based blockchain can achieve this. Blockchain is a decentralized peer-to-peer network, and nodes do not need to trust each other. It includes data encryption, timestamps, distributed consensus, smart contracts, and other technologies. With the maturity of blockchain technology, it has been deeply integrated with various industries [3, 4], solving the technical bottlenecks unique to multiple industries.

Attack Categories
As early as 2005, Chavez et al. [8] suggested that hackers may attack cars, and identity authentication and encryption should keep cars safe. This section focuses on attack categories and security requirements of the IoV. Firstly, attacks of IoV can be classified into traditional security attacks and exclusive attacks, according to the target and mode. Conventional security attacks include physical control attacks, network layer attacks, identity attacks, forged information attacks, and application attacks. Exclusive attacks are common and seriously impact the IoV but do not exist or be uncommon and have little impact on the traditional network.

Bluetooth Communication

Attackers can hijack traffic between Bluetooth keys and vehicles and tamper with and replay malicious traffic. Not only does it result in vehicle theft, but also it threatens the functional safety of the vehicle. In general, cellular networks are the more secure of the three wireless technologies.

Identity Attacks

There are two main attack entities for identity attacks: vehicles and roadside unit (RSU). In IoV, malicious nodes are often disguised as RSU and attempt to trick users into obtaining their authentication information. The attackers then use their identity to access confidential information, even as an authentication against others. In addition, they can also impersonate the identity of other vehicles. For example, an attacker might mimic an emergency vehicle, which would give them a higher priority in the network and thus reduce congestion.

Fake Information Attacks

The spread of false information [3] also exists in IoV, and it will cause more severe harm. Like Sybil Attacks by Douceur [4], attackers can spread incorrect information about road congestion, effectively forcing other vehicles to divert. They can also lead to traffic jams or sending accident alerts. Because of its low computing cost, falsifying information becomes one of the common attacks. And the distributed feature of IoV will lead to more severe harm.

Blockchain-Based IoV (BIoV)

Most scenarios in IoV are real-time and mobile, generating and exchanging large amounts of data [7]. In particular, many of the classic technology centralized security technologies are unlikely to be suitable for scenarios. Therefore, blockchain can provide a large number of innovative solutions for most application scenarios. So, on the other hand, integrating blockchain into the Internet of Vehicles not only improves the security, privacy, and trust of the Internet of Vehicles but also enhances the performance and automation of the system. To sum up, to accommodate flexibility and handle large amounts of data, we should combine blockchain technology with the Internet of Vehicles. This section will focus on the system model of BIoV.

Security Technology of BIoV

This section will focus on blockchain-based security technologies for the Internet of Vehicles. By keyword retrieval of Internet of Vehicles, blockchain, security technology, and so on, we searched relevant literature since 2010/2023, manually screened the title and abstract of the paper, conducted corresponding screening according to the quality of the article, and sorted out and analyzed as many high-quality papers as possible.

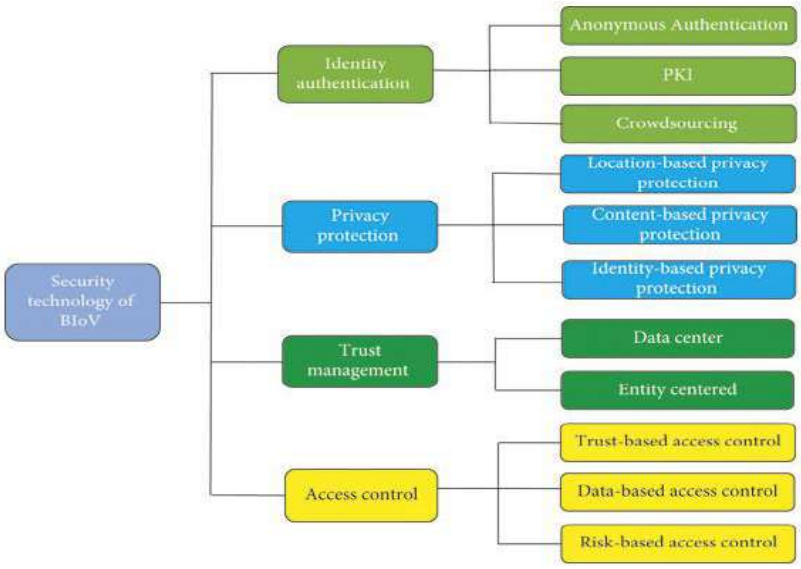

Fig.1: Security technology categories of BIoV.

Security Analysis Methods

Based on thoroughly investigating blockchain-based IoV security technology in the last section, we analyzed that each protocol and scheme's simulation environment and analysis methods differed. This section focuses on security analysis methods and performance parameters in BIoV.

Informal Safety Analysis

Informal security analysis refers to the theory or process analysis of the following security elements according to the characteristics of security protocols proposed in this paper.

RESULTS

Therefore, we should design a lightweight blockchain-based IoV framework or lightweight authentication and privacy protection protocols; (5) combination with existing new technologies. Blockchain can be combined with edge computing to enhance data analytics and improve the security of nodes on the Internet of Vehicles. Blockchain can also be combined with deep learning to build risk prediction models and improve access control security for Internet of Vehicles systems. Blockchain can also be combined with SDN and AI technologies to improve the transparency of the control plane. Therefore, the significance of the research work carried out in this paper is to summarize, classify, and discuss the existing blockchain-based Internet of Vehicles security technology, grasp its development direction, summarize verification and effective evaluation methods, and provide direction and method guidance for the following research work.

Summarization and Prospect

Through the above discussion on various aspects of blockchain-based IoV technology, security and privacy issues in IoV applications have focused on people's attention. We can enhance decentralized privacy protection, traceability, and other types of security by integrating blockchain technology. The research achievements in identity authentication, privacy protection, trust management, access control, and so on have been made. However, the following problems remain unresolved. However, the following issues remain unresolved: (1) development of a blockchain-based IoV security framework, which is different from the traditional IoV network architecture. We can use existing infrastructure to build IoV systems at maximum cost savings; (2) studying new blockchain models.

REFERENCES

1. R. Shrestha, S. Y. Nam, R. Bajracharya, and S. Kim, "Evolution of V2X communication and integration of blockchain for security enhancements," *Electronics*, vol. 9, no. 9, p. 1338, 2023.
2. R. Shrestha and S. Y. Nam, "Regional blockchain for vehicular networks to prevent 51% attacks," *IEEE Access*, vol. 7, pp. 95033–95045, 2023.
3. S. Xie, Z. Zheng, W. Chen, J. Wu, H.-N. Dai, and M. Imran, "Blockchain for cloud exchange: a survey," *Computers & Electrical Engineering*, vol. 81, Article ID 106526, 2023.
4. P. Fraga-Lamas and T. M. Fernandez-Carames, "A review on blockchain technologies for an advanced and cyber-resilient automotive industry," *IEEE Access*, vol. 7, pp. 17578–17598, 2022.
5. R. Shrestha, R. Bajracharya, A. P. Shrestha, and S. Y. Nam, "A new type of blockchain for secure message exchange in VANET," *Digital communications and networks*, vol. 6, no. 2, pp. 177–186, 2022.
6. T. Ali Syed, A. Alzahrani, S. Jan, M. S. Siddiqui, A. Nadeem, and T. Alghamdi, "A comparative analysis of blockchain architecture and its applications: problems and recommendations," *IEEE Access*, vol. 7, pp. 176838–176869, 2022.
7. T. Ali, A. Nadeem, M. Shoaib, M. Nauman, and A. Alzahrani, "Blockchain-based-vehicle-life-cycle-tracking-system," 2019,

8. M. L. Chavez, C. H. Rosete, and F. R. Henriguez, "Security and privacy vulnerabilities of in-car wireless networks: a tire pressure monitoring system case study," in *Proceedings of the 15th International Conference on electronics (2005), communications and Computers*, CONIELECOMP, Berkeley, CA, USA, August 2020.
9. P. Sharma and H. Liu, "A machine-learning-based data-centric misbehavior detection model for internet of vehicles," *IEEE Internet of Things Journal*, vol. 8, no. 6, pp. 4991–4999, 2021.