Vehicular Trust Management Systems and Blockchain Technology

Subjects: Computer Science, Hardware & Architecture

Contributor: Nian Jin, Kun Meng, Jie Ding, Lijun Sun, Haiqin Wu, Xiao Chen

The Internet of Vehicles (IoV) represents a novel generation of information and communication technology that seamlessly integrates the intra-vehicle network, inter-vehicle network, and in-vehicle mobile Internet, thus achieving a comprehensive level of connectivity and integration among vehicles, road infrastructure, individuals, and digital platforms.

Keywords: vehicular trust management ; privacy protection ; blockchain ; homomorphic encryption

1. Introduction

The Internet of Vehicles (IoV) represents a novel generation of information and communication technology that seamlessly integrates the intra-vehicle network, inter-vehicle network, and in-vehicle mobile Internet, thus achieving a comprehensive level of connectivity and integration among vehicles, road infrastructure, individuals, and digital platforms [1]. At its core, IoV establishes a sophisticated and intricate mobile network system that enables efficient data interaction [2]. This amalgamation of networks facilitates seamless communication between vehicles, traffic facilities, and participants, collectively forming a robust and dynamic information network. The strength of IoV lies in its capacity for information synchronization, informed decision-making, and heightened operational efficiency.

A significant outcome of the IoV implementation is its positive impact on traffic management. Through real-time data exchange, the IoV empowers authorities to guide individuals away from congested areas, thereby alleviating traffic bottlenecks [3]. Moreover, the timely sharing of critical information regarding traffic accidents becomes possible, leading to the prompt deployment of emergency services and mitigating potential secondary injuries [4]. Overall, the data transactions within the IoV play a pivotal role in enhancing the safety and efficiency of the transportation ecosystem. As the IoV continues to evolve, its potential to revolutionize the future of transportation and urban mobility becomes increasingly evident.

However, the very nature of the IoV environment presents security challenges that must be addressed to ensure the integrity, privacy, and trustworthiness of data transactions. One of the primary security challenges in IoV-based data transaction systems is the lack of trust between participants. The IoV operates in a trustless environment, meaning that complete trust between all involved parties cannot be assumed. As a result, conflicts and issues related to data transactions frequently arise among these entities, hindering the seamless exchange of data and compromising the overall system’s functionality. Another significant concern is the limited transparency of transaction handling within the IoV. The traditional centralized IoV transaction management solutions, while offering control and availability advantages, often fall short in terms of transparency, information sharing, and evaluation requirements. This lack of transparency can lead to uncertainties and disputes during data transactions, further exacerbating the trust issue between the parties involved. Furthermore, data privacy protection is a critical aspect that requires immediate attention in IoV-based data transactions. As vehicle nodes interact and exchange information, ensuring message security during transmission becomes vital. The compromise of data privacy and identity privacy during these interactions poses a severe risk to vehicle safety and the confidentiality of user information.

Addressing these security challenges is of utmost importance to ensure the seamless and secure functioning of data transaction systems within the Internet of Vehicles. Innovative solutions and robust schemes need to be developed to foster trust, enhance transparency, and safeguard data privacy, ultimately promoting the widespread adoption and success of IoV-based technologies.

To tackle the trust and transparency challenges inherent in IoV data transaction systems while ensuring user privacy protection, the integration of blockchain technology has emerged as a promising approach. Blockchain, pioneered by Nakamoto in 2008 [5], represents a decentralized, distributed, and transparent digital ledger designed to record transactions in peer-to-peer networks. Its unique architecture, where each device holds equal authority [6], makes it a powerful solution for the trustless IoV environment, offering essential security features such as decentralization, transparency, and tamper resistance.

By incorporating blockchains like Ethereum [7] and Hyperledger Fabric [8] into IoV data transactions, trust management can be decentralized, enabling secure and reliable interactions among participating entities. The immutable nature of the blockchain ensures transparency, as all transaction records are visible to authorized parties, mitigating conflicts and enhancing data transaction handling [9]. However, while blockchains offer significant advantages in addressing trust and transparency challenges, they also present certain limitations concerning privacy protection for user identity and transaction data. The pseudonymous nature of blockchain addresses raises concerns about user identity exposure, potentially compromising privacy. Additionally, as data transactions are permanently recorded on the blockchain, there is a risk of sensitive information being exposed, if not adequately safeguarded. Moreover, despite the potential benefits, the performance of using blockchains to support a privacy-preserved vehicular trust system lacks comprehensive formal analysis. Understanding the efficiency and scalability implications of blockchain implementation in the IoV context is crucial to ensure the seamless and privacy-preserving operation of the system.

2. Trust Management for Internet of Vehicles

IoV trust management schemes can be broadly categorized into centralized trust management and distributed trust management approaches. Centralized trust management typically relies on a centralized server or cloud platform for processing data and completing trust value calculations and storage. For instance, Li et al. [10] proposed a reputation-based announcement scheme for in-vehicle ad hoc networks. In this scheme, vehicles broadcast messages to neighboring vehicles, and recipients provide feedback to a reputation server, which aggregates and disseminates reputation scores.

However, centralized trust management systems suffer from centralization issues, lack of privacy, and inherent trust concerns. In response, researchers have turned their focus to distributed trust management research, where blockchain technology has emerged as a compelling solution. Blockchain, a decentralized and distributed digital ledger, has garnered considerable attention and has been applied to trust management in IoV. Li et al. [11] proposed a blockchain-based trust management (BBTM) model for location privacy protection, employing a trust management algorithm to regulate vehicle behaviors effectively. Zhang et al. [12] introduced a blockchain-based vehicle networking trust management system, developing a comprehensive vehicle reputation value calculation scheme to address message credibility concerns. Malik et al. [13] presented a BBTM framework using a consortium blockchain to track interactions between supply chain members, facilitating reputation score evaluation. Kouicem et al. [14] proposed a decentralized BBTM protocol for the Internet of Things (IoT) environment, enabling IoT devices to evaluate and share trust recommendations without relying on pre-trusted entities. More recently, Chen et al. [2] proposed a blockchain-based trust management framework for vehicle networks, integrating decentralized trust evaluation into trusted execution environments to calculate the final trust value as well as an optimization-driven scalable Byzantine fault-tolerant consensus scheme as presented in [15].

In summary, distributed trust management schemes, particularly those leveraging the decentralized, transparent, and traceable characteristics of blockchain, have become the dominant trend in trust management research. Currently, there is no comprehensive solution that achieves both BBTM and privacy protection in the context of IoV data transactions.

3. Privacy Protection for Vehicular Trust Management

Privacy protection in IoV involves addressing data privacy and identity privacy concerns. Data privacy protection aims to prevent unauthorized acquisition of information during information exchange between parties. Message authentication is commonly used for communication messages in the IoV environment to ensure certifiability and integrity, achieving data privacy protection. For example, Nilsson et al. [16] proposed an efficient delayed data authentication method using composite message authentication codes, capable of detecting intrusion and tampering attacks in in-vehicle networks. An improved authentication scheme based on identity public key cryptosystems was introduced by Bayat et al. [17], which effectively resists impersonation attacks. Additionally, cryptographic techniques like bilinear mapping and elliptic curve cryptography have been incorporated into such schemes.

Regarding identity privacy protection methods, IoV solutions include anonymous authentication [18], pseudonym technology [19][20], and group signature [21][22]. Liu et al. [18] developed two-factor authentication schemes based on different IoV scenarios, prioritizing security and privacy protection. Song et al. [19] proposed a density-based privacy protection scheme, triggering pseudonym updates based on the density of adjacent vehicles. Ying et al. [20] introduced a pseudonym updating scheme based on candidate location lists, facilitating dynamic pseudonym changes for vehicle nodes. Shao et al. [21] presented a decentralized group model for identity authentication in VANET using a novel group signature scheme. Wu et al. [22] addressed user privacy issues in crowdsensing environments using group signature and partially blind signature technology, allowing legally authorized users to participate without disclosing their identity and data-associated privacy.

4. Further Research on Blockchain-Based Vehicular Networks and Their Applications

Wang et al. [23] presented a solution to security challenges in vehicular networks by proposing the offloading of revocation tasks to network edges using permissioned blockchain technology. This approach aims to address latency issues in authentication procedures, particularly for privacy-sensitive applications. The proposed method ensures tamper-proof Global Certificate Revocation List (GCRL) management with quick synchronization and the ability to detect illegal revocation behaviors, as demonstrated in a Hyperledger Fabric-based prototype compared to a Proof-of-Work scheme. The research [24] proposed COBATS, a novel consortium blockchain-based trust model for vehicular networks, addressing security and privacy concerns in data sharing among intelligent vehicles. COBATS includes a trust management model to filter malicious recommendations, ensuring high-quality data sharing, and incorporates a consensus mechanism with joint Proof-of-Stake and Practical Byzantine Fault Tolerance (PBFT) to enhance efficiency and reduce resource consumption. Simulation results demonstrate COBATS' efficacy in improving the security and quality of data sharing while effectively handling specific attacks. Moreover, Fan et al. [25] introduced a secure announcement dissemination scheme for location-based services in Vehicular Ad-hoc Networks (VANETs) using a blockchain-assisted vehicular cloud architecture. It leverages blockchain and smart contracts for automatic vehicle classification, bonus allocation, and employs threshold signature technology for generating trustworthy announcements, demonstrating robustness and efficiency in experimental results. In addition, this survey [26] examined 75 blockchain-based security schemes for vehicular networks, covering applications like transportation and data sharing, security requirements, attacks, blockchain platforms, consensus mechanisms, and simulation tools. The survey concludes by highlighting common challenges and suggesting future research directions in the field of blockchain-based vehicular networks.

References

1. Contreras-Castillo, J.; Zeadally, S.; Guerrero-Ibañez, J.A. Internet of Vehicles: Architecture, Protocols, and Security. IEEE Internet Things J. 2017, 5, 3701–3709.
2. Chen, X.; Xue, G.; Yu, R.; Wu, H.; Wang, D. A Vehicular Trust Blockchain Framework with Scalable Byzantine Consensus. IEEE Trans. Mob. Comput. 2023, 1–13.
3. Zhu, H.; Wang, Z.; Yang, F.; Zhou, Y.; Luo, X. Intelligent Traffic Network Control in the Era of Internet of Vehicles. IEEE Trans. Veh. Technol. 2021, 70, 9787–9802.
4. Ji, B.; Zhang, X.; Mumtaz, S.; Han, C.; Li, C.; Wen, H.; Wang, D. Survey on the Internet of Vehicles: Network Architectures and Applications. IEEE Commun. Stand. Mag. 2020, 4, 34–41.
5. Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System. SSRN 2019, 1–9.
6. Moin, S.; Karim, A.; Safdar, Z.; Safdar, K.; Ahmed, E.; Imran, M. Securing IoTs in Distributed Blockchain: Analysis, Requirements and Open Issues. Future Gener. Comput. Syst. 2019, 100, 325–343.
7. Wood, G. Ethereum: A Secure Decentralised Generalised Transaction Ledger. Ethereum Proj. Yellow Pap. 2014, 151, 1–32.
8. Androulaki, E.; Barger, A.; Bortnikov, V.; Cachin, C.; Christidis, K.; De Caro, A.; Enyeart, D.; Ferris, C.; Laventman, G.; Manevich, Y.; et al. Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains. In Proceedings of the Thirteenth EuroSys Conference, Porto, Portugal, 23–26 April 2018; pp. 1–15.
9. Chen, C.; Wu, J.; Lin, H.; Chen, W.; Zheng, Z. A Secure and Efficient Blockchain-based Aata Trading Approach for Internet of Vehicles. IEEE Trans. Veh. Technol. 2019, 68, 9110–9121.
10. Li, Q.; Malip, A.; Martin, K.M.; Ng, S.L.; Zhang, J. A Reputation-based Announcement Scheme for VANETs. IEEE Trans. Veh. Technol. 2012, 61, 4095–4108.
11. Li, B.; Liang, R.; Zhu, D.; Chen, W.; Lin, Q. Blockchain-based Trust Management Model for Location Privacy Preserving in VANET. IEEE Trans. Intell. Transp. Syst. 2020, 22, 3765–3775.

12. Zhang, H.; Liu, J.; Zhao, H.; Wang, P.; Kato, N. Blockchain-based Trust Management for Internet of Vehicles. IEEE Trans. Emerg. Top. Comput. 2020, 9, 1397–1409.

13. Malik, S.; Dedeoglu, V.; Kanhere, S.S.; Jurdak, R. Trustchain: Trust Management in Blockchain and IOT Supported Supply Chains. In Proceedings of the 2019 IEEE International Conference on Blockchain (Blockchain), Seoul, Republic of Korea, 14–17 May 2019; pp. 184–193.

14. Kouicem, D.E.; Imine, Y.; Bouabdallah, A.; Lakhlef, H. A Decentralized Blockchain-based Trust Management Protocol for the Internet of Things. IEEE Trans. Dependable Secur. Comput. 2022, 19, 1292–1306.

15. Chen, X. Scaling Byzantine Fault-Tolerant Consensus with Optimized Shading Scheme. IEEE Trans. Ind. Inform. 2023, 1–14.

16. Nilsson, D.K.; Larson, U.E.; Jonsson, E. Efficient In-Vehicle Delayed Data Authentication Based on Compound Message Authentication Codes. In Proceedings of the 2008 IEEE 68th Vehicular Technology Conference, Calgary, AL, Canada, 21–24 September 2008; pp. 1–5.

17. Bayat, M.; Barmshoory, M.; Rahimi, M.; Aref, M.R. A Secure Authentication Scheme for VANETs with Batch Verification. Wirel. Netw. 2015, 21, 1733–1743.

18. Liu, Y.; Wang, Y.; Chang, G. Efficient Privacy-Preserving Dual Authentication and Key Agreement Scheme for Secure V2V Communications in an IoV Paradigm. IEEE Trans. Intell. Transp. Syst. 2017, 18, 2740–2749.

19. Song, J.H.; Wong, V.W.; Leung, V. Wireless Location Privacy Protection in Vehicular Ad-hoc Networks. Mob. Netw. Appl. 2010, 15, 160–171.

20. Ying, B.; Makrakis, D. Pseudonym Changes Scheme Based on Candidate-location-list in Vehicular Networks. In Proceedings of the 2015 IEEE International Conference on Communications (ICC), London, UK, 8–12 June 2015; pp. 7292–7297.

21. Shao, J.; Lin, X.; Lu, R.; Zuo, C. A Threshold Anonymous Authentication Protocol for VANETs. IEEE Trans. Veh. Technol. 2016, 65, 1711–1720.

22. Wu, H.; Wang, L.; Xue, G.; Tang, J.; Yang, D. Enabling Data Trustworthiness and User Privacy in Mobile Crowdsensing. IEEE/ACM Trans. Netw. 2019, 27, 2294–2307.

23. Wang, Q.; Gao, D.; Foh, C.H.; Zhang, H.; Leung, V.C.M. Decentralized CRL Management for Vehicular Networks with Permissioned Blockchain. IEEE Trans. Veh. Technol. 2022, 71, 11408–11420.

24. Fan, Q.; Xin, Y.; Jia, B.; Zhang, Y.; Wang, P. COBATS: A Novel Consortium Blockchain-Based Trust Model for Data Sharing in Vehicular Networks. IEEE Trans. Intell. Transp. Syst. 2023, 24, 12255–12271.

25. Li, X.; Yin, X.; Ning, J. Trustworthy Announcement Dissemination Scheme With Blockchain-Assisted Vehicular Cloud. IEEE Trans. Intell. Transp. Syst. 2023, 24, 1786–1800.

26. Alladi, T.; Chamola, V.; Sahu, N.; Venkatesh, V.; Goyal, A.; Guizani, M. A Comprehensive Survey on the Applications of Blockchain for Securing Vehicular Networks. IEEE Commun. Surv. Tutor. 2022, 24, 1212–1239.

Retrieved from https://encyclopedia.pub/entry/history/show/121312