Blockchain Technology as a Defense Mechanism Against Data Tampering in Smart Vehicle Systems

Khasanboy Kodirov, HoonJae Lee, and Young Sil Lee(✉)

Dongseo University, Busan, Republic of Korea
hjlee@gdsu.dongseo.ac.kr, youngsil.lee0113@gmail.com

Abstract. Smart vehicle systems, integrated with cutting-edge technology, have evolved to become a crucial element of modern transportation. They are leading us into a fresh era of mobility, offering the potential for increased efficiency, upgraded safety, and enhanced user satisfaction. According to a study by Statista, in terms of IoT-related revenue, the automotive IoT market is expected to reach 23.6 billion US dollars in 2025 [1]. However, their reliance on data-driven technologies also exposes them to the ever-present threat of data tampering. In response to these emerging threats, the imperative to fortify the cybersecurity posture of smart vehicles has never been more pressing. Known for its decentralized, immutable, and transparent nature, blockchain is a promising solution for safeguarding critical vehicle data. As part of this research paper, we look at the fundamentals of blockchain technology and discuss how this technology can be used within smart vehicles to enhance the security and integrity of data generated, stored, and shared. By leveraging the blockchain's security features, stakeholders in the automotive industry can pave the way for safer and more reliable smart vehicle technologies. This research also invites further exploration and collaboration to harness the full potential of blockchain in fortifying the future of smart transportation.

Keywords: Smart vehicle systems · Automotive cybersecurity · Blockchain technology

1 Introduction

During the past few decades, a technological revolution has unfolded, transforming the world. As cloud computing transcended infrastructure, global connectivity was fostered, and the Internet of Things (IoT) connected everyday objects. As these technologies continue to evolve and intertwine, they have collectively woven a complex tapestry that covers the world in an intricate web of innovation and connectivity. It can be summed up by saying that all objects and things are being replaced by their smart substitutes. Smart vehicles are one of these substitutions. Vehicles embedded with cutting-edge technology are ushering in a new era of transportation that promises increased efficiency, enhanced safety, and improved user experiences. As of 2018, there were 330 million connected cars, according to Upstream. Those numbers are expected to rise to 775

B. J. Choi et al. (Eds.): IHCI 2023, LNCS 14532, pp. 20–25, 2024.
https://doi.org/10.1007/978-3-031-53830-8_3

million by 2023. In addition, approximately 25 GB of data will be produced per hour by connected cars by 2025. Those numbers jump to 500 GB an hour for fully autonomous vehicles. Upstream estimates that the automotive industry is projected to lose $505 billion by 2024 to cyberattacks [2]. In response to these emerging threats, the imperative to fortify the cybersecurity posture of smart vehicles has never been more pressing. In an era when smart vehicles are becoming an integral part of daily life, protecting them from cyber threats is not just an option but a critical necessity for their safety and integrity. A fundamental motivation for this research lies in the profound implications smart vehicles have on society, the economy, and public safety. The latest report (Table 1), released in early 2021 illustrates data from 2010 to 2020 and covers over 200 automotive cyber incidents across the world [3]. It is important to understand that smart vehicles are not just mechanical entities. They are intricate cyber-physical systems interacting with hardware, software, sensors, actuators, and external networks. The interplay of these intricate systems has created a range of cybersecurity threats that go beyond the conventional boundaries of automotive engineering.

Table 1. Automotive attack vectors: 2010–2020

#N	Hardware/software	Share of total
1	Cloud servers	32.9%
2	Keyless entry-Key fob	25.3%
3	Mobile app	9.9%
4	ODB port	8.4%
5	Infotainment system	7.0%
6	Sensors	4.8%
7	ECU-TCU-Gateway	4.3%
8	In-vehicle network	3.8%
9	Wi-Fi network	3.8%
10	Bluetooth	3.6%
11	USB or SD port	2.1%

2 Background and Literature Review

Data tampering in the context of smart vehicle systems refers to the unauthorized alteration, manipulation, or compromise of critical data that underpins the functioning and decision-making processes of these vehicles. Whether it involves falsifying sensor data, modifying route information, or tampering with vehicle-to-vehicle (V2V) communications, such attacks pose significant threats to the reliability, safety, and trustworthiness of smart vehicles. The consequences of data tampering incidents in this domain can range from minor inconveniences to life-threatening situations, making it imperative to address this issue comprehensively. Blockchain, the foundational technology behind cryptocurrencies like Bitcoin, has garnered significant attention across various industries due to its unique attributes. It is a decentralized and distributed ledger system that offers transparency, immutability, and trust through cryptographic mechanisms. These qualities position blockchain as a promising solution to secure the integrity of data generated, stored, and communicated within smart vehicle ecosystems. Smart vehicle systems represent a transformative paradigm in modern transportation. These systems integrate cutting-edge technologies, including Internet of Things (IoT) sensors, artificial intelligence (AI), machine learning (ML), and real-time data communication, to create vehicles that are not only intelligent but also interconnected. This convergence of technology promises to revolutionize road safety, traffic management, and overall driving experiences. However, this rapid evolution also introduces new challenges, particularly in terms of data security.

Data tampering, or the unauthorized alteration and manipulation of data, has emerged as a critical concern in the realm of smart vehicle systems. These systems rely heavily on data for various functions, including:

1. Sensors and telemetry: Smart vehicles use sensors to collect data on road conditions, weather, vehicle performance, and the environment. This data informs real-time decisions for navigation and safety.
2. Communication networks: Vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication networks enable vehicles to share critical information. Tampered data in these networks can lead to accidents or disruptions in traffic management.
3. Automated decision-making: Many smart vehicles incorporate autonomous or semi-autonomous features that rely on data for decision-making. If this data is compromised, it can lead to incorrect or unsafe actions.
4. Fleet management: In commercial settings, fleet management relies on accurate data for route optimization, fuel efficiency, and maintenance scheduling. Tampered data can result in inefficiencies and increased costs.

In recent years, the convergence of blockchain technology and smart vehicle systems has gained substantial attention, with several noteworthy studies shedding light on the dynamic landscape of applications and innovative approaches. Notable among these are: (1) Smith et al. (2023), who introduce a blockchain-based communication framework designed to enhance secure vehicle-to-vehicle (V2V) communication in smart vehicles, thus ensuring data integrity and privacy[4]. (2) Brown and Lee (2022), whose comprehensive survey provides insights into diverse blockchain applications within the automotive industry, particularly emphasizing cybersecurity. This survey encompasses the latest trends in safeguarding smart vehicle systems against data tampering and cyber threats [5]. (3) Gupta et al. (2022), who explore scalable blockchain solutions for managing the burgeoning data volumes generated by smart vehicles [6]. These recent contributions illustrate the ongoing evolution of blockchain technology within smart vehicle systems, underscoring its potential in revolutionizing security, data management, and communication in the realm of connected and autonomous transportation.

3 Data Tampering in Smart Vehicle Systems

Data tampering in smart vehicle systems encompasses a range of malicious activities, including the unauthorized alteration, manipulation, or compromise of critical data. The consequences of such tampering are multifaceted and potentially severe:

1. **Safety risks:** One of the foremost concerns is the potential compromise of safety-critical data. For instance, tampering with sensor data, such as those responsible for collision avoidance or lane-keeping, can lead to incorrect decisions by autonomous driving systems, resulting in accidents and endangering lives.
2. **Traffic disruption:** Data tampering can disrupt the coordination and communication between smart vehicles. In V2V and V2I communication networks, altered data can mislead vehicles, leading to traffic congestion or collisions.
3. **Financial implications:** In commercial applications, data tampering can have financial repercussions. Fleet management relies on accurate data for route optimization, fuel efficiency, and maintenance scheduling. Tampered data can result in inefficiencies and increased operational costs.
4. **Privacy concerns:** Smart vehicles collect vast amounts of data, including location, behavior, and preferences. Unauthorized access or tampering with this data can lead to privacy breaches, identity theft, and misuse of personal information.

Before delving into further discussion, let's examine common data tampering incidents in smart vehicle systems in Table 2 [7].

Table 2. Common of data tampering incidents in smart vehicle systems

#N	Incident type	Description	Consequences
1	GPS spoofing	Falsification of GPS signals	Misleading navigation
2	Sensor manipulation	Altered LiDAR and radar data	Unsafe driving decisions
3	Communication disruption	Interference with V2V and V2I systems	Traffic congestion, accidents
4	Data theft	Unauthorized access and theft of data	Privacy breaches

Addressing data tampering in smart vehicle systems necessitates innovative and robust security measures. Blockchain technology emerges as a promising solution, offering inherent features that can help fortify the integrity of data and enhance trust among stakeholders. In the following sections, we will explore how blockchain technology can be leveraged to counter data tampering risks effectively within the context of smart vehicles.

4 Blockchain Technology as a Solution in Smart Vehicle Systems

Blockchain technology, when applied to smart vehicle systems, represents a robust and sophisticated approach to addressing data tampering vulnerabilities and ensuring the integrity of critical data and communications. In this section, we examine the technical aspects of how blockchains can be implemented within smart vehicle ecosystems, focusing on specific use cases, protocols, and underlying cryptography.

4.1 Technical Foundations of Blockchain in Smart Vehicle Systems

Blockchain technology has a lot to offer in the context of smart vehicles, but it's important to establish a technical foundation before looking at practical implementations. Key principles and components include:

- **Distributed ledger architecture**: Blockchain operates as a distributed ledger as shown in Fig. 1 [8], which consists of a network of nodes (computers) that collectively maintain a synchronized record of transactions. This architecture ensures redundancy and eliminates single points of failure.

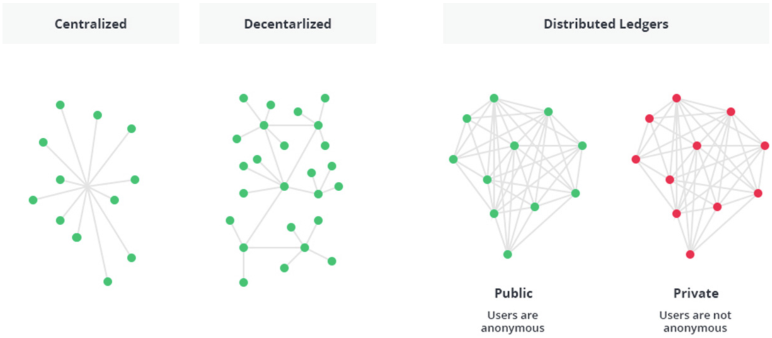

Fig. 1. Distributed Ledger Architecture of Blockchain

- **Consensus mechanisms**: Smart vehicle blockchain implementations often utilize consensus mechanisms like Proof of Work (PoW) or Proof of Stake (PoS) to validate and add new blocks to the chain. The choice of consensus mechanism impacts factors such as security, energy efficiency, and transaction speed.
- **Smart contracts**: Smart contracts are self-executing, programmable scripts deployed on the blockchain. They enable automation of predefined actions when specific conditions are met. In smart vehicle systems, smart contracts can govern agreements related to data access, sharing, and compensation.
- **Public vs. private blockchains**: The choice between public and private blockchains depends on the use case. Public blockchains (e.g., Ethereum) are open to anyone, offering transparency but with potential privacy concerns. Private blockchains provide controlled access, ensuring data privacy, making them suitable for business consortia and organizations.

4.2 Practical Implementations and Prototypes

Smart vehicle systems have been incorporated with blockchain technology in a number of practical implementations and prototypes, demonstrating its potential for enhanced data security and integrity. The initiatives include blockchain-powered data marketplaces for vehicles to share and monetize data securely, secure over-the-air software updates that verify update authenticity, and experimental decentralized autonomous vehicles (DAVs) that use blockchain for consensus on route planning and traffic coordination. Within smart vehicle ecosystems, these real-world endeavors demonstrate blockchain's feasibility and benefits in improving data tampering resistance and trust.

5 Conclusion

In conclusion, incorporating blockchain technology into smart vehicle systems is a pivotal step toward enhancing data integrity and security in the evolving landscape of connected transportation. Blockchain's technical foundations and practical implementations offer promising solutions to combat data tampering risks and establish trust within vehicular ecosystems. While challenges like scalability and interoperability persist, blockchain's potential to revolutionize smart transportation remains undeniable. It emerges as a transformative defense mechanism against data tampering, ushering in a future of safer and more reliable smart vehicles.

Acknowledgment. This research was supported by Korea Institute of Marine Science & Technology Promotion (KIMST) funded by the Ministry of Oceans and Fisheries (20210650).

References

1. Placek, M.: Automotive IoT Market Size 2021–2026. Statista, https://www.statista.com/statistics/423083/iot-units-installed-base-within-automotive-segment/. Accessed 18 Sept 2023
2. Blum, B.: Cyberattacks on Cars Increased 225 Percent in Last 3 Years. Birmingham Times, http://www.birminghamtimes.com/2022/02/cyberattacks-on-cars-increased-225-percent-in-last-3-years/. Accessed 18 Sept 2023
3. Juliussen, E.: Now Your Car is a Cybersecurity Risk, Too. EETimes, https://www.eetimes.com/now-your-car-is-a-cybersecurity-risk-too/. Accessed 20 Sept 2023
4. Smith, J., Author, A.B., Author, C.D.: Blockchain-Based Secure Communication for Smart Vehicles. Journal of Advanced Transportation Technology **28**(3), 123–137 (2023)
5. Brown, A., Lee, S.: A Comprehensive survey of blockchain solutions for automotive cybersecurity. Int. J. Smart Vehicle Syst. **15**(4), 234–251 (2022)
6. Gupta, R.: Scalable blockchain solutions for smart vehicle data management. J. Connect. Vehicles Smart Transp. **10**(2), 87–101 (2022)
7. Trustonic: Top 10 Security Challenges in the Automotive Industry for Connected Cars. https://www.trustonic.com/opinion/top-10-security-challenges-for-connected-cars/. Accessed 26 Oct 2023
8. Lastovetska, A.: Blockchain Architecture Basics: Components, Structure, Benefits & Creation. https://mlsdev.com/blog/156-how-to-build-your-own-blockchain-architecture. Accessed 20 Sept 2023