

Research on Technical Challenges and Development Trends in Automotive Data Security

Yuchen Jia

(Shanghai Motor Vehicle Testing and Certification Technology Research Center Co., Ltd., Shanghai 201804, China)

Abstract: With the rapid advancement of automotive intelligence and connectivity, data security in vehicles faces numerous technical challenges within today's increasingly complex and interconnected automotive industry environment. Automotive data security has become a critical issue for the industry, while also revealing promising future development trends. By analyzing the current state and challenges facing the automotive data security sector, as well as examining existing technological solutions, this paper explores the future trends in automotive data security. It first highlights the importance of automotive data security, then discusses the main threats currently confronting it, followed by an introduction to key technological solutions in the field, and finally provides forward-looking analysis and evaluation of the future direction of automotive data security.

Keywords: automotive data security, smart vehicles; cybersecurity; data protection; development trends

1 Introduction

The development of the automotive industry is inextricably linked to data security. As automotive technology continues to advance—particularly with the accelerated trends toward intelligence, connectivity, and electrification—the volume of data generated by the industry has grown explosively. This data encompasses not only basic information such as vehicle operating status and driving habits, but also sensitive personal details including user identities and payment records. Consequently, the importance of automotive data security has become increasingly evident. In the process of intelligent automotive development, data security cannot be overlooked, as it carries profound implications for individuals, enterprises, and society as a whole. First, for individuals, automotive data security directly affects the protection of personal privacy. With the rise of smart and connected vehicles, vast amounts of personal information—such as driving patterns and travel routes—are stored within cars. If this data falls into the hands of malicious actors, it could be exploited for illegal activities like theft or fraud. Therefore, ensuring automotive data security is an essential requirement for safeguarding individual privacy. Second, for businesses, data security serves as a critical safeguard for corporate reputation and credibility. If a company experiences a breach in automotive data security resulting in customer data leaks or misuse, its image and reputation could suffer severe damage, potentially leading to legal actions and substantial fines. Thus, automotive data security is a matter that companies must take seriously and address proactively through effective protective measures. Finally, for society at large, automotive data security forms a vital foundation for ensuring traffic safety and public security [1]. As automobiles remain a crucial mode of transportation in modern life, their safety directly impacts people's lives and property. A failure in automotive data security could lead to vehicles being hacked or remotely controlled, potentially triggering traffic accidents or public safety incidents. Hence, securing automotive data is a necessary condition for maintaining both road safety and broader public security.

2 Current Status of Automotive Data Security Development

2.1 Types and Sources of Automotive Data

Automotive data is a broad concept encompassing various types of information generated throughout a vehicle's

entire lifecycle—from manufacturing and sales to usage and disposal. The main categories of automotive data include: first, vehicle identification data, which includes basic information such as the vehicle identification number (VIN), license plate number, model, and color. This data typically comes from vehicle manufacturers or registration authorities. Second, performance data, covering aspects like vehicle weight, fuel consumption, acceleration, and braking distance. These metrics can be collected via onboard sensors or diagnostic tools, and for some models, performance data can also be remotely retrieved through over-the-air (OTA) transmission. Third, driving data, involving route traveled, driving duration, and distance covered. This information can be obtained through global positioning systems (GPS) or in-vehicle navigation systems. Fourth, driver behavior data, including driving habits, reaction times, and levels of distraction. Such data can be gathered using onboard cameras, sensors, and similar devices. Fifth, maintenance data, consisting of records related to repairs, routine servicing, and replacement parts. This data is usually documented by repair shops or recorded manually by vehicle owners. Sixth, fault data, generated when a vehicle experiences malfunctions, including fault codes and descriptions. This information can be accessed through the vehicle's onboard diagnostic system [2].

2.2 Collection and Use of Automotive Data

As mentioned above, automotive data is primarily collected from vehicle manufacturers, onboard systems, third-party service providers, and user feedback. Vehicle manufacturers gather extensive data during the manufacturing and testing phases to assess vehicle performance and identify potential issues, such as onboard systems, sensors, and GPS positioning systems. During vehicle operation, they continuously collect data on vehicle status, driving routes, and driver behavior. Third-party service providers, such as repair shops and insurance companies, also collect data including maintenance records and insurance histories. Additionally, user feedback serves as a significant source of automotive data, which can be obtained through surveys, online reviews, and other methods to capture insights regarding vehicles and driving behaviors.

Automotive data holds significant value for car manufacturers, service providers, and users alike. Manufacturers can leverage this data to enhance product design and improve quality and performance. For instance, by analyzing vehicle failure data, manufacturers can identify and address potential issues, thereby reducing the rate of vehicle malfunctions. Additionally, such data can be used to develop new safety features and improve overall vehicle safety. Service providers can utilize automotive data to deliver personalized services. For example, insurers can offer customized insurance plans based on drivers' risk profiles derived from their driving behavior data. Repair shops can also use vehicle maintenance records to anticipate required parts in advance, improving repair efficiency. For users, understanding their own driving behavior data helps them better manage their vehicles and enhance driving safety [3]. For example, by reviewing fuel consumption data and travel routes, drivers can adjust their habits, optimize routes, and reduce fuel usage.

However, the collection and use of automotive data also face certain challenges and limitations. First, privacy protection is a critical issue. When collecting and using vehicle data, it is essential to comply with relevant privacy regulations to ensure that users' personal information is not disclosed or misused. Second, data quality is another concern that requires attention. To obtain accurate and useful data, advanced data collection and analysis techniques must be employed, along with thorough data cleaning and validation processes.

3 Challenges Facing Automotive Data Security

With the rapid development of automotive intelligence and connectivity, vehicle data security faces multiple challenges, including both technical and managerial aspects.

On a technical level, automotive data security faces several key challenges. First, there are cybersecurity threats. As vehicles become increasingly connected, the number of connection points to external networks grows, making them more vulnerable to cyberattacks. These attacks—such as malware infections or hacker intrusions—can threaten

both vehicle operation and passenger safety. Second, there are data protection requirements. Modern vehicles store vast amounts of sensitive information, including personal user data, driving habits, and travel routes. Ensuring the security of this data throughout its collection, transmission, storage, and usage is a major challenge for the automotive industry. Third, new technologies introduce additional security risks. Innovations such as autonomous driving and connected vehicle systems bring progress but also new vulnerabilities. For example, autonomous vehicles rely on high-precision maps and sensors, and the security of this data directly impacts driving safety [4].

At the management level, the main challenges facing automotive data security include: first, incomplete security management systems. Some automakers and service providers have inadequate policies and poor implementation in data security management, leading to frequent incidents of data breaches and misuse. Second, insufficient awareness among personnel. Some employees and managers do not sufficiently prioritize data security, lacking necessary awareness and skills, which increases the risk of human errors and violations. Third, ineffective interdepartmental collaboration. Automotive data security involves multiple departments and stages, requiring close coordination between internal teams and external suppliers. However, in practice, inconsistent coordination and poor communication often result in gaps and blind spots in data security management.

To address these challenges, the automotive industry needs to implement a series of measures to strengthen data security management, including enhancing cybersecurity defenses, improving data protection systems, raising employee awareness of security, and strengthening cross-departmental collaboration. At the same time, government agencies at all levels and industry associations should also enhance supervision and guidance to jointly promote improvements in automotive data security.

4 Key Technologies for Automotive Data Security

Automotive data security is a complex and critical technical field. To ensure the security of automotive data, several approaches are generally available.

First, automotive data encryption technology is one of the key methods for ensuring the security of vehicle data. Encryption serves as the foundation for protecting automotive data by using cryptographic algorithms to encode sensitive information, thereby preventing unauthorized third parties from accessing or tampering with it. This technology is particularly critical in the automotive industry, as vehicle data often contains important information such as users' personal privacy and vehicle operational status. If such data is leaked or maliciously exploited, it could result in significant losses and serious security risks for users. Automotive data encryption involves multiple fields and areas of expertise, including cryptography, computer security, and network communications, making its implementation and specific details quite complex.

Secondly, firewalls and intrusion detection systems (IDS) are also crucial tools for ensuring automotive data security, playing a vital role in this field. As the name suggests, an automotive data firewall acts as a barrier, primarily monitoring and controlling data flows entering and exiting the vehicle's network. It can identify and block potential security threats such as unauthorized access or malware, thereby safeguarding the integrity and confidentiality of automotive data. With careful configuration and management, firewalls significantly reduce the risks of data breaches or system attacks. IDS, on the other hand, is a system designed to proactively detect and respond to security threats. By analyzing network traffic, system logs, and other data sources, it identifies and reports potential attacks or security incidents. IDS continuously monitors the network and system status in real time, immediately issuing alerts and initiating appropriate countermeasures upon detecting suspicious behavior or signs of an attack. As a key defense line, IDS helps promptly identify and address potential security threats, ensuring the safety and reliability of automotive data.

Once again, security updates and patch management are crucial aspects that cannot be overlooked in automotive data security. As technology continues to evolve, new security vulnerabilities and threats constantly emerge. Therefore, timely implementation of security updates and patch management for vehicle systems—aimed at fixing

known vulnerabilities and preventing attackers from exploiting them—is essential for safeguarding automotive data security.

Finally, driver authentication and authorization are also crucial for ensuring automotive data security. By verifying the driver's identity and granting appropriate access rights, only authorized drivers can access and operate vehicle systems, preventing unauthorized access and operations—making this a key technology in safeguarding automotive data.

5 Future Trends in Automotive Data Security

5.1 Applications of Artificial Intelligence in Data Security

With the rapid advancement of artificial intelligence (AI) technology, its applications in the field of data security are expanding steadily, providing strong support for safeguarding automotive data. In the foreseeable future, AI's role in automotive data security will become increasingly prominent, enabling the following technological applications: First, emergency response and root-cause analysis for security incidents. AI can respond swiftly to security events and assist in identifying their origins. Through machine learning and pattern recognition, AI can automatically detect and identify abnormal vehicle behaviors, enabling prompt responses and mitigating potential threats to automotive data security. Second, monitoring security trends. AI can track real-time security developments, including newly discovered vulnerabilities, attack patterns, and threat intelligence. This helps enterprises stay informed about emerging risks and respond promptly, protecting their data and systems from attacks. Third, developing cutting-edge security technologies. Leveraging AI's powerful analytical capabilities, automotive security engineers can accelerate the development of new security solutions, such as advanced encryption algorithms, firewall rules, or intrusion detection systems, thereby enhancing overall data security. Fourth, analyzing and responding to major internet security vulnerabilities. When significant security flaws emerge on the internet, AI can quickly assess the scope of impact and potential risks, offering timely countermeasures to automotive companies. This helps reduce the risk of vulnerability exploitation and protects both businesses and users from potential losses and threats.

5.2 The Potential of Blockchain Technology in Data Security

As vehicles become increasingly intelligent and connected, the application of blockchain technology in automotive data security will grow ever more important. With its decentralized, transparent, and tamper-proof characteristics, blockchain offers innovative solutions for securing vehicle data. First, blockchain can be used to encrypt and store automotive data. By storing vehicle data on a blockchain, data integrity and immutability are ensured, protecting against malicious attacks or unauthorized alterations. Additionally, blockchain's cryptographic algorithms provide an enhanced level of security for vehicle data. Second, blockchain enables access control and identity authentication for automotive data. By establishing a blockchain-based identity verification system, only authorized users can access and manipulate vehicle data, thereby preventing unauthorized access and data breaches. Finally, blockchain supports traceability and auditing of vehicle data. By recording every modification and access event, it becomes possible to track the origin and flow of data, ensuring its completeness and authenticity. This is particularly significant for investigating and tracing automobile accidents.

Although blockchain technology holds great potential for automotive data security, its application in this field is still in the early stages of development and faces several technical challenges and limitations. For instance, issues such as scalability and performance of blockchain, integration with existing systems, and user privacy protection require further research by industry professionals, along with breakthroughs in technological innovation and practical exploration.

6 Conclusion

As automotive technology continues to advance and vehicles become increasingly intelligent and connected,

automotive data has become a valuable asset, yet it also faces unprecedented security challenges. Currently, ensuring the security of automotive data presents serious technical difficulties, whose importance and urgency cannot be overlooked. The security of automotive data directly impacts personal privacy protection and is crucial to vehicle safety. With the growing intelligence and connectivity of vehicles, the challenges and potential risks associated with automotive data security are becoming increasingly evident. Data breaches or misuse could lead to severe social safety incidents and damage automakers' brand image and reputation. Moreover, automotive data security directly affects customer trust in manufacturers. Therefore, protecting automotive data has become an urgent and critical task. Automakers, suppliers, and relevant government agencies must work together to strengthen technological research and development, improve regulations and policies, and enhance overall security awareness to ensure the safety and reliability of automotive data.

References

- [1] Wang Yudian.“Challenges and Development Trends in Safety Management Technology for Power Batteries of New Energy Vehicles” [J]. Automobile and New Powertrain, 2023,(5): 61-64. DOI: 10.16776/j.cnki.1000-3797.2023.05.004.
- [2] Wang Zhenpo, Yuan Changgui, Li Xiaoyu.“Analysis of Challenges and Development Trends in Safety Management Technology for Power Batteries of New Energy Vehicles” [J]. Automotive Engineering, 2020(12): 1606-1620. DOI: 10.19562/j.chinasae.qcgc.2020.12.002.
- [3] Li Yibing, Sun Yueting, Xu Chengliang.“Analysis of Automotive Safety Technology Development Trends Based on Traffic Accident Data”[J]. Journal of Automotive Safety and Energy, 2016(3): 241-253.
- [4] Cai Ying.“Analysis of Challenges and Development Trends in Safety Management Technology for Power Batteries of New Energy Vehicles”[J]. Times Automobile, 2022, (12): 124-125.