International Journal of Communication Networks and Information Security
ISSN: 2073-607X, 2076-0930
Volume 15 Issue 03 Year 2023

# Research on Internet Technology Innovation and Information Security Challenges in New Vehicle Energy Sector

**Wenjie Lu**
*Ph.D. Candidate, School of Business Administration, Krirk University, Bangkok,Thailand, 10220*
*18664364931@163.com*
**Ximing Sun***
*Professor, School of Business Administration, Krirk University, Bangkok, Thailand, 10220*
*xmsun65@163.com*

***Article History***

Received: 15 October 2023
Revised: 18 November 2023
Accepted: 05 December 2023



***Abstract***

With the rapid proliferation and advancement of new energy vehicles, Internet technology has garnered significant attention and application in this field. This study focuses on innovations in Internet technology in the domain of new automotive energy and the associated information security challenges. The innovations in Internet technology relevant to new energy vehicles, including Telematics, intelligent driving, and remote control, are initially explored. Subsequently, the information security challenges brought about by these innovations are analyzed, encompassing various aspects such as data privacy breaches, remote attacks, and malware infections. The significance of information security in the development of new energy vehicles is emphasized. Solutions and suggestions, including the strengthening of encryption technology, the establishment of a robust security framework, and the enhancement of user education and awareness, are put forward. In conclusion, the current state of research on Internet technology innovation and information security challenges is summarized, and it is suggested that future research should delve deeper into the trajectory of Internet technology development in the field of new energy vehicles, along with the attendant information security challenges, to provide theoretical and practical support for promoting the healthy development and secure application of the new energy vehicle industry.

***Keywords: New Energy Vehicles, Internet Technology, Privacy Protection, Information Security***

## 1. Introduction

With the development of technology and environmental changes, new energy vehicles, as clean, efficient, and energy-saving transportation tools, are increasingly favored and concerned by people. New energy vehicles are primarily powered by new or traditional powertrain systems while integrating advanced vehicle control strategies and driving methods [1]. The primary new energy vehicles are pure electric vehicles, hybrid electric vehicles, fuel cell vehicles, solar-powered vehicles, etc.

The development of new energy vehicles can only be done with the support and innovation of internet technology. Internet technology can provide intelligent, networked, and informationized

services and functions for new energy vehicles, such as intelligent charging, remote control, vehicle networking, and intelligent travel. Internet technology can improve new energy vehicles' performance, safety, convenience, and comfort, enhancing user experience and satisfaction [2]. Internet technology can also promote the coordinated development of the new energy vehicle industry, forming an industrial, innovation, and value chain.

However, internet technology has also brought information security challenges and risks to new energy vehicles. Due to the large amount of data transmission, storage, and processing involved in new energy vehicles and various network communication and interfaces, they may face threats such as hacker attacks, virus infections, and data leakage [3]. These threats may lead to functional failure, performance degradation, and even accidents of new energy vehicles, endangering users' personal and property safety and privacy rights. Therefore, how to ensure information security in the field of new energy vehicles is an urgent problem to be solved [4].

In order to deal with cybersecurity threats in the field of new energy vehicles, some effective optimization measures need to be developed. For example, it is necessary to establish sound laws, regulations, and standards to standardize and regulate cybersecurity in the field of new energy vehicles; to strengthen cybersecurity education and training in the field of new energy vehicles to enhance the cybersecurity awareness and capabilities of users and practitioners, and to adopt advanced encryption and firewall technologies to guarantee data security and cybersecurity in the field of new energy vehicles.

This paper studies the cyber technology innovation and cyber security challenges in the field of new energy vehicles and analyzes the types and impacts of cyber security threats. Some effective optimization measures are proposed based on security risks and their impacts, aiming to provide some references and lessons for network technology innovation and network security challenges in the field of new energy vehicles.

## 2. Related Works

### *2.1 Current Situation of New Vehicle Energy*

With the development of the new automotive energy sector, Internet technology innovations have profoundly impacted the automotive industry. Figure 1 shows the sales volume and market share of new vehicle energy, showing an increasing trend year by year.

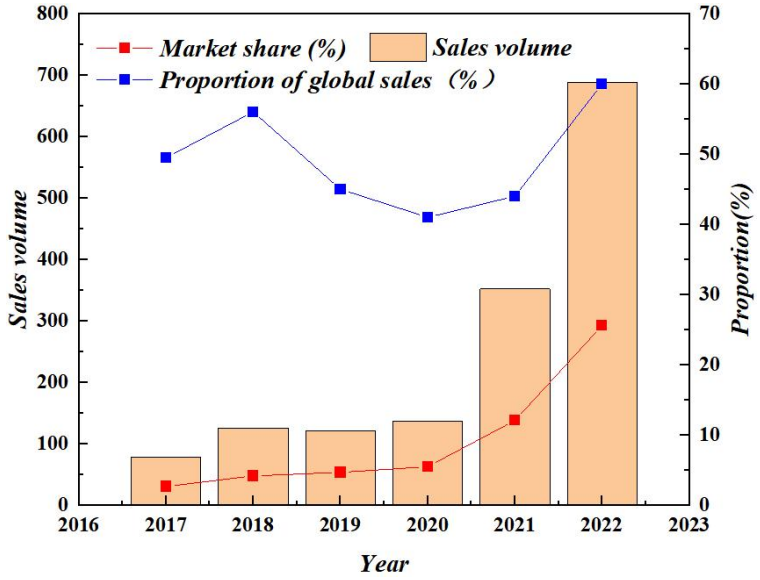


*Figure 1. Risk Threats of New Vehicle Energy*

Internet technology innovation and information security research in the field of new automotive energy face multiple challenges, which require careful study and resolution to ensure the safety and reliability of automotive systems. Here are some main challenges:

(1) Remote Intrusion and Control: Internet-connected automotive systems can be a target for hackers, who can attempt to remotely intrude into a vehicle's control system and threaten driving safety. This includes manipulating critical functions such as braking, accelerating, and steering. The

following table shows sample data from a car owner who experienced a remote intrusion. Table 1 shows sample data of a car experiencing a remote intrusion.

*Table 1. Sample Data of Cars Experiencing Remote Intrusion*

| Feature | Describe | Data example |
|---|---|---|
| Attack IP Addresss | IP address used by the attacker | 192.168.1.100 |
| Attack Type | Types of intrusion or control | Malicious software, port scanning [5] |
| Attack Time | Date and time of attacks | 2023-09-28 14:30:00 |
| Victim IP Address | IP address of the victim system | 192.168.1.200 |
| Attack Tool | Tools or software used by attackers | Metasploit，Nmap |
| Attack Target | The goals of the victim system or network | Web server, database |
| Attack Result | As a result of attack, whether to successfully invade or control | Success, failure |
| Attack Method | The method or loopholes used by the attacker | SQL injection, remote execution code [6] |

(2) Data privacy leakage: Vehicles transmit large amounts of sensitive data over the Internet, including location information, driving habits, and owner identity. Inadequately protected data can be stolen or misused, involving privacy issues for vehicle owners.

(3) Vehicle cyber-attacks: Vehicle internal networks and electronic control units are at risk from malware and cyber-attacks. Table 2 shows the statistics of cyber attacks on a vehicle.

*Table 2. Statistics of Cyber Attacks on Vehicles*

| Attack type | Attack description | Number of attacks |
|---|---|---|
| Remote Invasion | Hacker remote access to vehicle control system | 15 |
| Malicious Software Infection | Mysterious software Infection Vehicle Electronic Control Unit | 10 [7] |
| CAN Bus Attack | Interference in the attack controller area network bus | 8 |
| Wireless Signal Interference | Drives the wireless communication of the vehicle, such as the remote key signal | 5 |
| Data Tamper | Modify the vehicle sensor data to mislead the driving system | 12 |

(4) Supply chain security: Automakers often rely on multiple suppliers in the supply chain to provide electronic and software components. An insecure supply chain can introduce malicious code or backdoors threatening the entire vehicle system. Automakers and related stakeholders must adopt stringent information security measures, including enhanced network security, data encryption, vulnerability remediation, and access control, to ensure the safety and trustworthiness of connected vehicle technologies. At the same time, drivers must maintain information security awareness and avoid using insecure connections or applications to reduce potential risks. Table 3 shows the statistics of threats to supply chain security.

*Table 3. Threat Statistics for Supply Chain Security*

| Threat | Describe | Influence |
|---|---|---|
| Supplier Data Leakage | Suppliers accidentally or malicious leakage sensitive data | Customer data is lost, reputation is damaged |
| Counterfeit Products | Manufacturers pretend to be legitimate suppliers to provide counterfeit products | Customer security risk increases, and the brand is damaged |
| Malicious Software Injection | The malware is injected into the product through supply chain channels | Customer data leakage, system damage |
| Logistics Interruption [8] | Natural disasters or bad weather lead to logistics interruption | Supply delay, production line discontinued production |
| Internal Threat | Internal employees leak sensitive information or conduct malicious behaviors | Data leakage, production interruption [9] |

(5) Software Updates and Vulnerability Management [10]: Maintaining the security of automotive systems requires the timely patching of potential vulnerabilities and providing secure software updates. However, this may also face challenges, such as ensuring that all vehicles are updated and promptly installed the latest patches. Human error and social engineering attacks: It's not just technological threats that present a challenge but also the human factor. Employee negligence or social engineering attacks can lead to information leakage or system compromise.

(6) Consumer education: Consumers need to understand the potential risks of connected vehicles to take appropriate precautions, including solid password settings, regular software updates, and avoiding unsecured Wi-Fi networks.

### *2.2 Connected Car Technology of New Automotive Energy*

The development of Telematics technology enables automobiles to realize real-time data transmission, remote monitoring, and intelligent driving [11], [12], [13]. While the rapid growth of connected vehicle technologies has brought drivers many conveniences and intellectual experiences, it is also accompanied by a series of potential risks and security challenges. First, hacking poses a severe threat, as they may try to invade the vehicle's interconnection system through the network to gain control of the car, which may lead to dangerous situations of remote control of the vehicle, significantly threatening the driver's life safety. Secondly, personal data privacy leakage is another prominent issue. With the development of connected vehicle systems, they collect a large amount of sensitive information, such as driving data, location information, and personal preferences, which will severely violate drivers' privacy if these data are maliciously obtained or leaked. In addition, malware and virus infections are risks that cannot be ignored. Internet connectivity makes vehicle systems more susceptible to malware and virus infections, which can lead to loss of vehicle control or data theft. Network instability may also threaten the security of connected car technology. Network interruptions or delays may lead to the failure of remote control, navigation functions, etc., increasing driving risks. Additionally, supply chain attacks are a potential risk factor, where malicious manufacturers or suppliers may embed backdoors in a vehicle's hardware or software to gain unauthorized access or control. Finally, there is the issue of legal and ethical liability, which can become complicated when connected vehicle technologies cause accidents involving disputes between manufacturers, drivers, and ISPs.

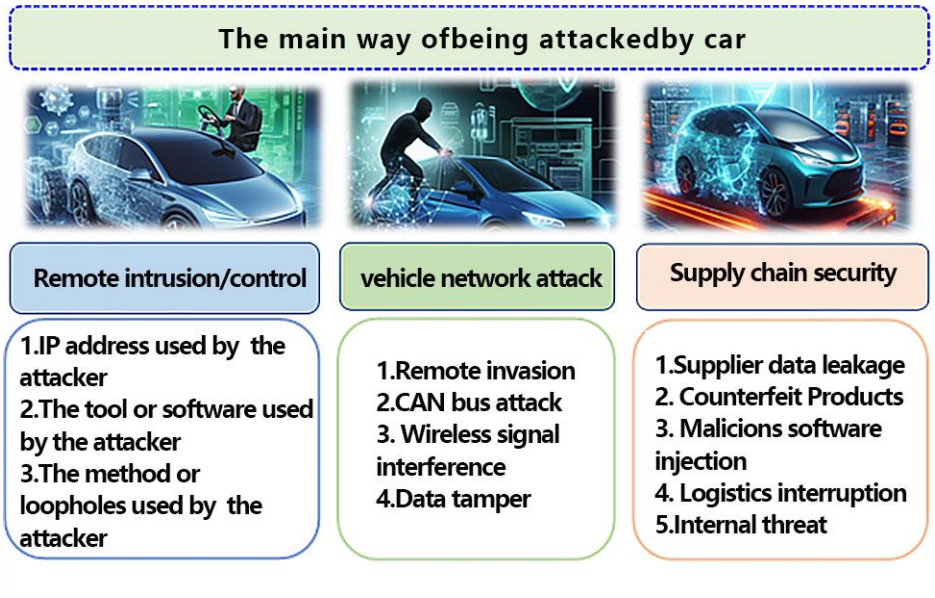


*Figure 2. Main Sources of Automotive Safety Threats*

Figure 2 shows a schematic of the primary sources of automotive security threats. Attackers may attempt to disrupt the regular operation of the vehicle or access internal vehicle data. In summary, automakers and related stakeholders need to adopt stringent information security measures, including enhanced network security, data encryption, vulnerability remediation, and access control, to ensure the safety and trustworthiness of connected vehicle technologies. In contrast, drivers need to maintain an awareness of information security and avoid using insecure connections or apps to minimize potential risks [14].

### *2.3 New Vehicle Energy Intelligent Transportation System*

Intelligent transportation systems integrate vehicles, roads, and urban infrastructure, improving transportation efficiency. The widespread application of intelligent transportation system connectivity technology has provided convenience for urban traffic management and travel, but it also comes with a series of potential risks. Firstly, cybersecurity threats are one of the most prominent issues. Hackers may invade intelligent transportation systems, disrupt traffic signals, surveillance cameras, and vehicle communication, leading to traffic chaos and security issues. Therefore, network security must be strengthened.

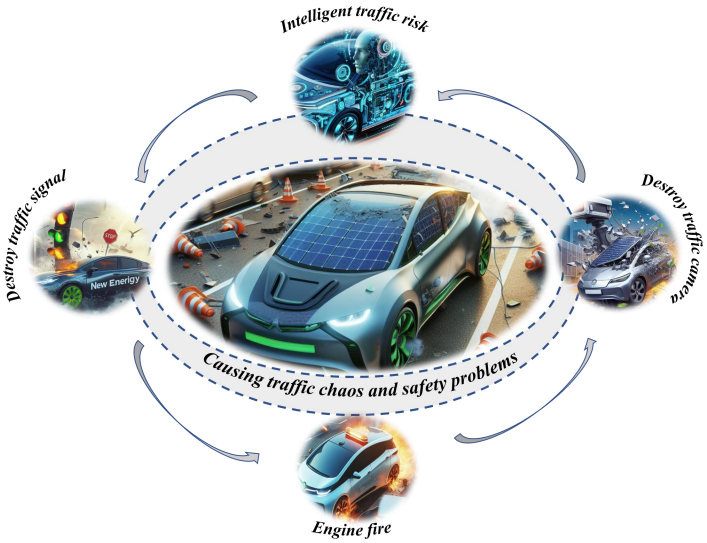


*Figure 3. Schematic Diagram of Cyber Risk in ITS*

Figure 3 shows the network risks faced by intelligent transportation systems. To address these risks, measures must be taken to strengthen network security, data encryption, system failure

recovery, network stability, and developing laws and regulations to ensure the credibility and sustainability of intelligent transportation system connectivity technology. At the same time, users and relevant stakeholders must also actively participate in maintaining their personal information security and road safety.

## 3. Methodology

### *3.1 Remote Intrusion and Control of New Vehicle Energy*

Remote intrusion and control technology is a technology that utilizes network connections to illegally access and manipulate computer systems, network devices, or intelligent devices. It poses serious security risks to individuals, organizations, and society [15], [16]. Generally speaking, there are several common ways to control a vehicle without contact:

(1) Vehicle entertainment system vulnerability. The car entertainment system is a crucial target of hacker attacks. Previous cases have confirmed that hackers can access a malicious webpage through the car entertainment system's browser, exploit browser vulnerabilities to control the car entertainment system, and thus control the entire vehicle. In addition, hackers may directly establish a network connection to the entertainment domain through the WIFI hotspot of the car entertainment system. If other devices in the entertainment domain have vulnerabilities, hackers may establish control over specific components and attempt to enter the network of other vehicle parts by exploiting these vulnerabilities.

(2) Update hijacking. Automotive electronic components, like mobile phones and other products, also require software upgrades. Suppose hackers can hijack communication data during vehicle upgrades through technical means. In that case, they may insert a backdoor code during the upgrade process and establish remote control of the vehicle after the update.

(3) OBD peripherals. Nowadays, some car owners may purchase third-party peripherals to remotely access the car's condition or unlock it through their phones. These devices often require the car owner to plug into the vehicle's OBD interface to ensure the peripherals can be connected to the car's internal network. Hackers can use the vulnerabilities of such peripherals to send control commands to the car network, thereby remotely controlling the car. Generate the training sequence waveform with known symbols transmitted from the transmitter to the receiver.

### *3.2 Privacy Disclosure of New Vehicle Energy*

As new energy vehicles use the latest technology to help human beings realize various conveniences, in the process, they have also inevitably exposed the problems of most of the enormous leakage [17], [18]. Internet connectivity has enabled many new energy vehicles to have Internet connectivity, allowing them to communicate with external networks. This provides a potential intrusion channel for hackers who may exploit vulnerabilities to access the vehicle's systems and data. Data collection and storage take advantage of the sensors and data logging devices that new energy vehicles are typically equipped with to collect and store various vehicle-related data, such as driving behavior, energy consumption, and vehicle performance. If these data are not correctly protected, unauthorized persons may access or steal them. New energy vehicles' communication protocols and data transmission methods may have security vulnerabilities that allow hackers to intercept or tamper with information. This could lead to leakage of sensitive data or remote attacks on the vehicle. Third-party applications and services: Some new energy vehicles support integrating third-party applications and services, such as remote monitoring of vehicle information and Telematics platforms. If these third-party applications and services do not have strict privacy protection measures, it may lead to vehicle data misuse or leakage.

Vehicles transmit large amounts of data over the Internet, including location, driving habits, etc., and data privacy breach technology poses a severe security risk that threatens individuals, businesses, and society. This technology allows unauthorized access, collection, and exploitation of an individual's sensitive information, leading to serious privacy violations, identity theft, financial loss, and reputational damage. Hackers can steal an individual's identity information, including name, date of birth, social security number, etc., and use it for illegal activities such as opening a bank account, applying for a loan, committing cyber fraud, placing a heavy financial burden and psychological stress on the victim. Secondly, business secrets, customer data, and partner information can be obtained illegally, which may lead to loss of competitive advantage, financial

loss, and damage to reputation. They may even threaten the survival and development of an organization. Figure 4 is a schematic diagram of data privacy.

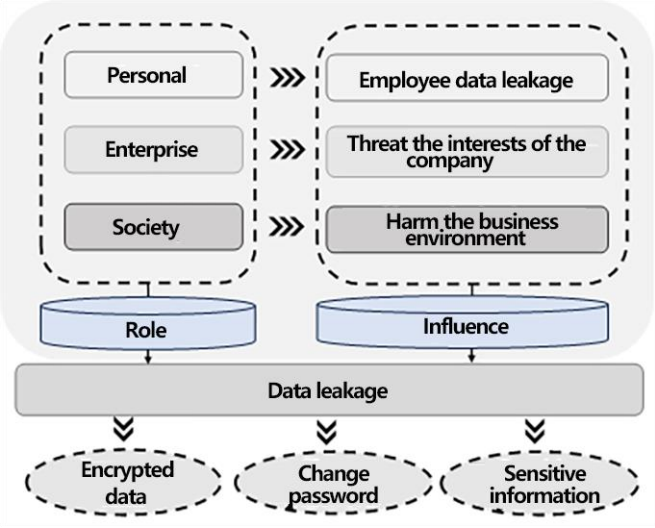


*Figure 4. Schematic Representation of Data Privacy*

The public sector stores large amounts of sensitive information, including citizens' health records, financial information, and government secrets. If these data are compromised, it could lead to social instability, crisis of confidence, and political problems. Table 4 shows the specific statistics of privacy breaches suffered by vehicles.

*Table 4. Specific Statistics of Privacy Breaches Suffered by Vehicles*

| Leakage Type | Describe | Data Type | Revelation Reason | Affected Party |
|---|---|---|---|---|
| Employee Data Leakage | Personal information leakage of employees, such as social security numbers and contact information | Personal identity information | Internal data leakage, social engineering attack | Employees and company reputation are damaged |
| Customer Data Leakage | Customer account information is accessed by hackers | Customer account information | Database vulnerability Unauthorized access | The reputation of the client company is damaged |
| Regulatory Compliance Issues | The company failed to process customer data in accordance with regulations | Customer data | Unrecommended regulations, improper data management | Customer, legal issues |

Common privacy breaches include Location Tracking: New automobiles are often equipped with Global Positioning Systems (GPS), meaning vehicle location information can be collected and recorded. If this information is accessed or misused by unauthorized people, it can lead to privacy breaches and personal security concerns. Driving Data Collection: Vehicles can collect and store driving data such as speed, acceleration, and braking conditions. This data may contain personal driving habits and behavioral patterns that may be used to identify or analyze criminal activity. Personal Information: New vehicles may require the owner or driver to provide personal information such as name, address, and contact information. If unauthorized persons access this information, it

could trigger identity theft and other forms of fraud. Remote Control and Data Transfer: Many new cars feature remote control and data transfer capabilities that enable owners to remotely operate their vehicles from their smartphones or other devices. Such connections may have security vulnerabilities that allow hackers to remotely control the car or access sensitive data in the vehicle's systems. Privacy protection is an evolving area that requires serious attention from multiple parties.

### *3.3 Network Attacks on New Vehicle Energy Vehicles*

Vehicle internal networks may be subject to malware and cyberattacks that can affect the regular operation of cars. Vehicle cyberattack techniques pose serious security risks, threatening transportation safety, personal privacy, and social stability. These attack techniques allow malicious actors to hack and manipulate a vehicle's electronic systems, leading to serious accidents, hijacking, personal information leakage, and road chaos. First, vehicle cyberattacks can lead to traffic accidents and life-threatening situations. Hackers can hack into a vehicle's control systems to interfere with brakes, gas pedals, and steering and even remotely deactivate the car, causing accidents and injuries. This poses a massive threat to the lives of drivers and passengers. Secondly, personal privacy is also threatened. Modern cars have many sensors and wireless connections for collecting and transmitting vehicle and driver data [19], [20], [21]. Hackers can hack into vehicle systems to steal location information, communication records, and driving habits, violate personal privacy, and even misuse this information for criminal activities. Table 5 shows the damage statistics of cyberattacks on vehicles. Hackers can remotely deactivate vehicles, leading to increased traffic congestion and accidents, causing severe damage to urban transportation infrastructure and the economy.

*Table 5. Damage Statistics for Vehicles Subjected to Cyber-attacks*

| Attack type | Influence | Number of Affected Vehicles |
|---|---|---|
| Remote invasion | The control system is accepted by unauthorized access | 8 [22] |
| Malicious software infection | Mysterious software Infection Vehicle Electronic Control Unit | 5 |
| CAN bus attack | The controller area network bus is disturbed | 3 |
| Wireless signal interference | Wireless signal interference remote key signal | 6 [23] |
| Data tamper | Modify the sensor data to mislead the driving system | 4 |

To address these risks, automakers need to strengthen vehicle cybersecurity measures, including encrypted communications, vulnerability remediation, and deployment of intrusion detection systems. Drivers should also remain vigilant by not connecting to untrusted networks at will and updating vehicle software to fix security vulnerabilities. Governments and legal agencies must step up regulation to ensure that the automotive industry complies with cybersecurity standards and penalizes cyber attackers to safeguard road safety and personal privacy. Automakers can take a variety of measures to enhance vehicle cybersecurity. For example, encrypted communications can prevent unauthorized access and data leakage. Vulnerability remediation can fix known security holes promptly, reducing the attack risk. Intrusion detection systems can monitor vehicle networks and detect abnormal activities promptly. Drivers should also avoid connecting to untrusted networks and regularly update their vehicle software to fix security vulnerabilities [24], [25], [26].

Government and legal agencies must also take action to ensure that the automotive industry complies with cybersecurity standards. For example, the U.S. National Highway Traffic Safety Administration (NHTSA) released a guidebook on "Automotive Cybersecurity Best Practices" to help automakers and suppliers develop more secure automotive systems.1 The government should also step up regulation to ensure that the automotive industry adheres to cybersecurity standards and penalizes cyber attackers in order to safeguard road safety and personal privacy.

## 4. Results and Discussion

### *4.1 Optimization of New Vehicle Energy Network Security*

Cybersecurity is one of the crucial issues in today's digital society. To enhance cybersecurity, several measures need to be taken to protect the information assets of individuals, organizations, and countries. The following measures can be taken to enhance the cybersecurity of new automotive energy systems and prevent the risk of privacy breaches:

(1) At the technical level, build strong firewalls and intrusion detection systems to prevent unauthorized access and malicious attacks. Strengthen network monitoring and logging to detect and respond to potential threats promptly.

(2) Operational level: Regularly update operating systems and applications to patch known vulnerabilities and strengthen password management by using complex, unique passwords and changing them regularly. Adopt multi-factor authentication to increase login security and control access to sensitive information to authorized personnel only. Encrypt sensitive data to ensure that it cannot be easily decrypted even if it is stolen.

(3) Social prevention level. Develop and implement cybersecurity policies that clarify how security incidents and violations are handled and establish appropriate penalties. Establish an emergency response program that can act quickly during a cyber attack and back up data to deal with potential data loss situations. Strengthen international cooperation, share threat intelligence, and work with other countries and organizations to combat transnational cybercrime.

Through the multi-layered protection and continuous efforts of the above measures, the digital assets and privacy of the new automotive energy system can be better protected, and the risk of privacy leakage can be reduced. As shown in Figure 5, a schematic diagram of strengthening network security in multiple aspects is provided.

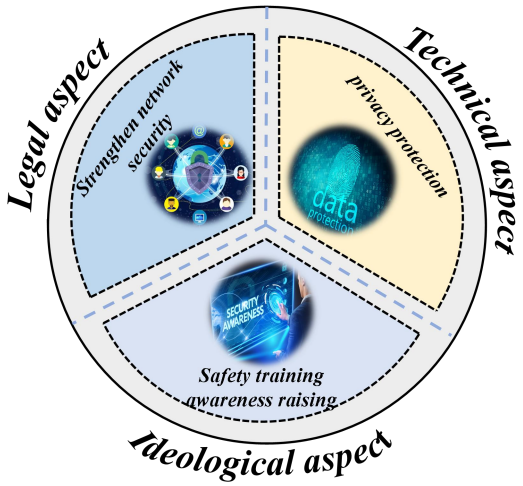


*Figure 5. Schematic Diagram of Multifaceted Cybersecurity Enhancement*

### *4.2 Optimization of Data Encryption and Privacy Protection for New Vehicle Energy*

Adoption of robust data encryption technology and privacy protection policies to protect data transmitted by vehicles. Enhancing data encryption and privacy protection is a crucial task in today's digital age to protect the sensitive information of individuals, organizations, and countries from wrongful intrusion and misuse. First and foremost, it is essential to protect data using strong encryption. This includes using modern encryption algorithms to encrypt data stored on servers, in the cloud, or in transit. It is also vital to ensure that encryption keys are securely stored and managed to prevent them from being leaked or accessed by wrongdoers. Encryption should not only be applied to the transmission and storage of data. Still, it should also include end-to-end communication encryption to protect information when sent and received.

Second, emphasizing user education and privacy awareness is integral to data encryption and privacy protection. Individuals and employees need to understand how to recognize and protect against threats such as phishing, malware, and social engineering and how to protect their privacy [27]. Educate users to use complex passwords, enable two-factor authentication, and share personal information judiciously. At the same time, organizations and governments should increase awareness

and enforcement of privacy regulations to ensure the legality and transparency of data collection and processing.

Third, establishing stringent data access and control measures is crucial to protecting privacy. Only authorized personnel should have access to sensitive data, and access should be strictly monitored and audited. Appropriate destruction or archiving measures should be taken for no longer-needed data to reduce the risk of potential leakage. Figure 6 is a schematic diagram of enhanced data privacy protection.


*Figure 6. Schematic Diagram of Enhanced Data Privacy Protection*

In addition, privacy protection needs to consider the issue of cross-border data transfers [28], [29]. Organizations need to understand and comply with each country's privacy regulations to ensure that they do not violate the relevant laws when transferring data across borders. For example, China's Cybersecurity Law, Data Security Law, and Personal Information Protection Law provide precise requirements for cross-border data transfers. In China, data processors must conduct a security assessment and obtain government approval when providing essential data and personal information collected and generated during their operations in China to foreign countries. In addition, other countries and regions have similar laws and regulations, such as the EU's General Data Protection Regulation (GDPR).

Finally, technological innovations can also support data encryption and privacy protection. Examples include the use of symmetric encryption, asymmetric encryption, hybrid encryption, and blockchain technologies [30] to ensure data immutability and transparency, as well as the use of advanced technologies such as secure multi-party computation to analyze data without revealing sensitive information. Table 6 shows the details of some of the encryption technology types.

*Table 6. Details of Cryptography Types*

| Encryption Technology | Describe | Application Field | Advantage | For Example |
|---|---|---|---|---|
| Symmetric Encryption (AES) | Use the same key to encrypt and decrypt | Data transmission, storage, communication | Fast, efficient, suitable for large-scale data | Data transmission encryption in vehicle communication |
| Asymmetric encryption (RSA) | Use public key encryption and private key decryption | Digital signature, key exchange | High security and digital signature can be achieved | Safe communication between vehicles and cloud servers |
| Hybrid encryption | Combining method of symmetry and | Security communication, key exchange | Combine the advantages of symmetry and | Data transmission of remotely upgraded vehicles |

| | | | | |
|---|---|---|---|---|
| | asymmetric encryption | | asymmetric encryption | |

To enhance privacy protection, we propose the implementation of several crucial measures. Regarding data security, a primary focus lies on robust encryption practices, utilizing financial-grade encryption algorithms for safeguarding vehicle energy data during transmission and storage. Stringent measures will be taken to ensure the secure generation and management of encryption keys, minimizing the risk of key leakage that could compromise data integrity. Access control mechanisms will be established to restrict access to vehicle energy data, allowing only authorized personnel or designated devices to access specific datasets.

In terms of vehicle communication, ensuring routine communication security between the vehicle and the external network is imperative. Countermeasures against potential hackers involve implementing data integrity verification and identity authentication measures, assuring the authenticity of communication parties and safeguarding against data interception or tampering.

Concerning data storage, an optimization of security measures is proposed. This includes the implementation of data partitioning and isolation, segregating sensitive and non-sensitive data to mitigate the risk of data leakage. Regular data backups and encryption protocols will be enforced to prevent data loss and unauthorized acquisition. Additionally, a focus on security updates and vulnerability remediation is emphasized, with manufacturers actively addressing reported security vulnerabilities and promptly providing users with necessary security updates. Users are encouraged to regularly update the software versions of the vehicle system and applications to ensure the timely closure of known vulnerabilities.

To foster transparency, manufacturers are urged to articulate clear privacy policies, elucidating data collection and processing practices. Users should be empowered with the right to make informed choices regarding data sharing and usage, thereby exercising control over their personal privacy. In summary, the comprehensive adoption of these measures is essential for bolstering privacy protection for both individuals and organizations, concurrently fostering the advancement and innovation of the digital society.

### *4.3 Optimization of New Vehicle Energy Security Training*

Conducting targeted security training for vehicle manufacturers, drivers, and maintenance personnel is imperative to elevate their awareness of information security. A well-informed and vigilant workforce is crucial in safeguarding individuals, organizations, and society from diverse security threats. For enterprises, the establishment of a comprehensive security training program is paramount. This program should encompass training initiatives for employees, users, and stakeholders, emphasizing security best practices. Topics covered should include the identification of malicious emails, the creation of robust passwords, and the adoption of two-factor authentication. Regularly updating training content to align with emerging threats and the latest security technologies is essential.

Promoting security awareness within the enterprise involves organizing simulation exercises and presenting real-world case studies. This approach aids in enhancing individuals' comprehension of potential threats, equipping them with the skills to respond effectively to situations, and fostering the ability to report and address security incidents. Simulating malicious and phishing attacks allows individuals to gain practical experience without exposing the organization to actual risks. An integral aspect of security awareness is embedded within the corporate culture. Establishing a positive security culture is pivotal in cultivating heightened awareness. Organizations should incentivize employees to actively engage in security initiatives, rewarding adherence to safe behaviors and enforcing stringent penalties for violations. A safety culture is further fostered through open lines of communication, providing employees with the freedom to report security issues or propose improvements without the fear of reprisals.

Continual monitoring and feedback play a pivotal role in augmenting security awareness. Organizations can leverage security assessment tools to scrutinize employee security practices, providing constructive feedback and suggestions for improvement based on the assessment outcomes. Simultaneously, regular security alerts and notifications, coupled with the dissemination of

information about the latest security threats, contribute to maintaining vigilance among individuals. Employing technology tools is equally crucial to support security training and awareness initiatives. This encompasses the utilization of online training platforms and simulated attack tools for training and testing purposes. Additionally, the integration of security awareness apps and gamification methods can enhance engagement and facilitate learning of security best practices.

Leadership engagement and modeling are fundamental elements in constructing a robust security culture. Senior executives should proactively endorse security initiatives, embodying security best practices as role models, and regard security as a paramount organizational priority. Elevating safety training and awareness necessitates a multidimensional approach, encompassing structured training programs, simulation exercises, the cultivation of a positive safety culture, continuous monitoring and feedback mechanisms, the integration of technology tools, and unwavering leadership support. Only through this comprehensive effort can we effectively elevate the security awareness of individuals and organizations in the digital age, fortifying defenses against diverse security threats.

## 5. Conclusion

In the realm of new automotive energy, internet technologies like Telematics, Smart Driving, and Remote Control are continuously evolving to offer users greater convenience and enhanced intelligence. Nevertheless, the associated information security risks, including remote intrusion, data privacy breaches, and control vulnerabilities, demand our utmost attention. To comprehensively fortify information security, this paper proposes three optimization strategies across distinct dimensions: in-vehicle network security enhancement, data privacy protection reinforcement, and information security training. By delving deeper into emerging technological trends and advancing robust security solutions, collaboration is fostered among stakeholders to ensure the sustainable and secure adoption of new energy vehicles.

## References


[1] G. Farid, N. F. Warraich, and S. Iftikhar, "Digital information security management policy in academic libraries: A systematic review (2010–2022)," *Journal of Information Science*, p.01655515231160026, 2023.

[2] B. K. Gebremeskel, G.M. Jonathan, and S. D. Yalew, "Information Security Challenges During Digital Transformation," *Procedia Computer Science*, vol. 219, pp. 44-51, 2023.

[3] R. Sun, S. Zhang, Z. Yin, S. Wu, and Y. Chen, "Intelligent Networked Vehicle CAN Network Security," In *2023 Asia-Europe Conference on Electronics, Data Processing and Informatics (ACEDPI)*,pp. 402-408, 2023.

[4] B. S. Bari, K. Yelamarthi, and S. Ghafoor, "Intrusion Detection in Vehicle Controller Area Network (CAN) Bus Using Machine Learning: A Comparative Performance Study," *Sensors*, vol. 23, no. 7, p. 3610, 2023.

[5] S. A. Moqurrab, T. Naeem, M.S. Malik, A.A. Fayyaz, A. Jamal, and G. Srivastava, "UtilityAware: A Framework for Data Privacy Protection in e-Health," *Information Sciences*, p. 119247, 2023.

[6] S. Rajapaksha, H. Kalutarage, M.O. Al-Kadri, A. Petrovski, G. Madzudzo, and M. Cheah, "Ai-based intrusion detection systems for in-vehicle networks: A survey," *ACM Computing Surveys*, vol. 55, no. 11, pp.1-40, 2023.

[7] E. Aliwa, O. Rana, C. Perera, and P. Burnap, "Cyberattacks and countermeasures for in-vehicle networks," *ACM Computing Surveys (CSUR)*, vol. 54, no. 1, pp. 1-37, 2021.

[8] I. Mugarza, J.L. Flores, and J.L. Montero, "Security issues and software updates management in the industrial internet of things (iiot) era," *Sensors*, vol. 20, no. 24, p. 7160, 2020.

[9] M. Alloghani, M.M. Alani, D. Al-Jumeily, T. Baker, J. Mustafina, A. Hussain, and A.J. Aljaaf, "A systematic review on the status and progress of homomorphic encryption technologies," *Journal of Information Security and Applications*, vol. 48, p. 102362, 2019.

[10] M. Aydar, S.C. Cetin, S. Ayvaz, and B. Aygun, "Private key encryption and recovery in blockchain," *arXiv preprint arXiv:1907.04156*, 2019.

[11] S. Kaur, G. Kaur, and M. Shabaz, "A secure two-factor authentication framework in cloud computing," *Security and Communication Networks*, vol. 2022, pp. 1-9, 2022.

[12] J. Yang, C. Wang, B. Jiang, H. Song, and Q. Meng, "Visual perception enabled industry intelligence: state of the art, challenges and prospects," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 3, pp. 2204-2219, 2020.

[13] J. Gwak, J. Jung, R. Oh, M. Park, M.A.K. Rakhimov, and J. Ahn, "A review of intelligent self-driving vehicle software research," *KSII Transactions on Internet and Information Systems (TIIS)*, vol. 13, no. 11, pp. 5299-5320, 2019.

[14] A.A. Abd El-Latif, B. Abd-El-Atty, W. Mazurczyk, C. Fung, and S.E. Venegas-Andraca, "Secure data encryption based on quantum walks for 5G Internet of Things scenario," *IEEE Transactions on Network and Service Management*, vol. 17, no. 1, pp. 118-131, 2020.

[15] I. Sharafaldin, A.H. Lashkari, S. Hakak, and A.A. Ghorbani, "Developing realistic distributed denial of service (DDoS) attack dataset and taxonomy," *In 2019 International Carnahan Conference on Security Technology (ICCST),* pp. 1-8, 2019.

[16] K.B. Virupakshar, M. Asundi, K. Channal, P. Shettar, S. Patil, and D.G. Narayan, "Distributed denial of service (DDoS) attacks detection system for OpenStack-based private cloud," *Procedia Computer Science*, vol. 167, pp. 2297-2307, 2020.

[17] V.J. Richardson, R.E. Smith, and M.W. Watson, "Much ado about nothing: The (lack of) economic impact of data privacy breaches," *Journal of Information Systems*, vol. 33, no. 3, pp. 227-265, 2019.

[18] B. Murdoch, "Privacy and artificial intelligence: challenges for protecting health information in a new era," *BMC Medical Ethics*, vol. 22, no. 1, pp. 1-5, 2021.

[19] J. Feng, Y. Wang, J. Wang, and F. Ren, "Blockchain-based data management and edge-assisted trusted cloaking area construction for location privacy protection in vehicular networks," *IEEE Internet of Things Journal*, vol. 8, no. 4, pp. 2087-2101, 2020.

[20] X. Jia, L. Xing, J. Gao, and H. Wu, "A survey of location privacy preservation in social internet of vehicles," *IEEE Access*, vol. 8, pp. 201966-201984, 2020.

[21] A. Karale, "The challenges of IoT addressing security, ethics, privacy, and laws," *Internet of Things*, vol. 15, p. 100420, 2021.

[22] A. Gohar, and G. Nencioni, "The role of 5G technologies in a smart city: The case for intelligent transportation system," *Sustainability*, vol. 13, no. 9, p. 5188, 2021.

[23] S. Kaffash, A.T. Nguyen, and J. Zhu, "Big data algorithms and applications in intelligent transportation system: A review and bibliometric analysis," *International Journal of Production Economics*, vol. 231, p. 107868, 2021.

[24] C. Togay, A. Kasif, C. Catal, and B. Tekinerdogan, "A firewall policy anomaly detection framework for reliable network security," *IEEE Transactions on Reliability*, vol. 71, no. 1, pp. 339-347, 2021.

[25] S. Prabakaran, R. Ramar, I. Hussain, B.P. Kavin, S.S. Alshamrani, A.S. AlGhamdi, and A. Alshehri, "Predicting attack pattern via machine learning by exploiting stateful firewall as virtual network function in an SDN network," *Sensors*, vol. 22, no. 3, p. 709, 2022.

[26] V. Tkachov, M. Hunko, and V. Volotka, "Scenarios for implementation of nested virtualization technology in task of improving cloud firewall fault tolerance," *In 2019 IEEE International Scientific-Practical Conference Problems of Infocommunications, Science and Technology (PIC S&T)*, pp. 759-763, 2019.

[27] Z. Allam, and D.S. Jones, "On the coronavirus (COVID-19) outbreak and the smart city network: universal data sharing standards coupled with artificial intelligence (AI) to benefit urban health monitoring and management," *In Healthcare* ,vol. 8, no. 1, p. 46, 2020, February.

[28] W.G. Voss, "Cross-border data flows, the GDPR, and data governance," *Wash. Int'l LJ*, vol. 29, p. 485, 2019.

[29] D. Coyle, and D. Nguyen, "Cloud computing, cross-border data flows and new challenges for measurement in economics," *National Institute Economic Review*, vol. 249, pp. R30-R38, 2019.

[30] A.S. Rajasekaran, M. Azees, and F. Al-Turjman, "A comprehensive survey on blockchain technology," *Sustainable Energy Technologies and Assessments*, vol. 52, p. 102039, 2022.