Scalable Computing: Practice and Experience, ISSN 1895-1767, http://www.scpe.org
© 2024 SCPE. Volume 25, Issues 3, pp. 1287–1300, DOI 10.12694/scpe.v25i3.2064

HAZARDOUS CHEMICALS LOGISTICS INTERNET OF VEHICLES BASED ON ENCRYPTION ALGORITHM

YUJIAN TANG[*], YA CHEN[†], AND HOEKYUNG JUNG[‡]

Abstract. With the advancement of information and communication technology, vehicles role in people's lives is not just for transportation but also equipment for the carrier of mobile communication. The new direction is provided by the Internet for the automobiles development and upgrading. Internet of Vehicles (IoVs) includes smart vehicles, Autonomous Vehicles (AVs) as well as roadside units (RSUs) that communicate for providing the enhanced transportation services such as high traffic efficiency and reduced congestion and accidents. In the hazardous chemical logistics sector, the integration of Internet of Vehicles (IoVs) introduces significant security, privacy, and trust challenges. Vulnerabilities to cyberattacks, such as hacking and data manipulation, threaten the integrity of sensitive information regarding hazardous cargo, while concerns about location privacy and data minimization arise due to the tracking of vehicle movements. Ensuring authentication, authorization, and compliance with regulatory standards is essential for building trust within the IoV ecosystem, as any compromise in supply chain integrity could lead to safety hazards or legal liabilities. Robust encryption algorithms like AES and RSA play a crucial role in securing data transmission, but proper implementation and key management practices are necessary to prevent cryptographic weaknesses. Addressing these issues comprehensively is vital for safeguarding the transportation of hazardous chemicals and ensuring the safety of both the environment and the public. IoVs, suffer from security, privacy and trust issues. In order to solve the problem of hazardous chemical logistics of encryption algorithm, the author proposed a research on the information security of the Internet of Vehicles. Firstly, the information characteristics of dangerous chemicals vehicles are analyzed, then analyze the Data Encryption Standard (DES) algorithm. Advanced Encryption Standard (AES) algorithm is analyzed in the symmetric cryptosystem and then RSA algorithm is analyzed in the public key cryptosystem. Finally, the performance of the algorithm and the characteristics of vehicle information are comprehensively analyzed. The security of Internet of Vehicle's data transmission is efficiently improved by the proposed method.

Key words: Encryption algorithm; hazardous chemicals; Internet of Vehicles; vehicle logistics; security research; Autonomous Vehicles; Roadside units

1. Introduction. Internet of Vehicles at home and abroad With the continuous improvement of sensing technology, network communication technology, and data analysis and computing technology, in-vehicle system networks, cyber-physical systems and automotive Internet of Things are also gradually developing. But for the security risks brought by intelligent connected cars, it is still a major problem that scholars need to break through. The safety of vehicle network transportation of hazardous chemicals logistics vehicles is important and the current situation of hazardous chemicals transport vehicles in the Internet of Vehicles is analyzed, encrypt the information of hazardous chemicals transport vehicles, the concealment of vehicle information is guaranteed, and traffic accidents caused by the theft of hazardous chemicals can be prevented to a certain extent. The AES and RSA hybrid encryption algorithm is used to encrypt vehicle information, realize the concealment of vehicle information. On the basis of the original remote monitoring system for hazardous chemicals transport vehicles (Hazardous chemicals vehicle networking), according to the project's requirements for vehicle information encryption, using information encryption technology, the key information of the Internet of Vehicles is encrypted and transmitted, in order to achieve the purpose of information security of the Internet of Vehicles for hazardous chemicals [1].

To this end, the author aims at the network security problems existing in the existing vehicle networking of hazardous chemicals logistics vehicles, combined with the specific needs of the project, an encryption algorithm suitable for the information security of the Internet of Vehicles in the logistics of hazardous chemicals is designed,

[*] Department of information technology, GuangXi Police College, Nanning, GuangXi, 530028, China (yujiantang00234@yahoo.com).

[†] Department of information technology, GuangXi Police College, Nanning, GuangXi, 530028, China (YaChen39@163.com).

[‡] Department of Computer Engineering, PaiChai University, Daejeon, 35345 China (HoekyungJung@163.com).

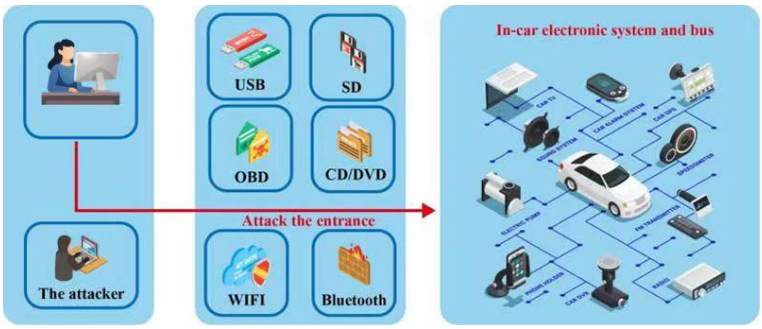

Fig. 1.1: The Internet of Vehicles for Logistics Vehicles

and the encryption algorithm is applied to the Internet of Vehicles in the logistics of hazardous chemicals to realize the confidential communication of the Internet of Vehicles(See Figure 1.1).

The National Highway Traffic Safety Administration (NHTSA) published a proposition for all new manufactured vehicles. Aside from vehicles, it is also essential for 5G communications. The vehicles achievement is the functionality aim by sharing vehicle driving-related information. The security is the design and privacy foundation and it is a priority. Unfortunately, relevant research is scarce concerning in the vehicular communication field. The quantum computers emergence will disrupt traditional cryptographic communications, which will increasingly require physical layer security needs in communications. The possibility of V2V communications suggested by the study and utilizing a secrecy capacity defined as the confidential data. They investigated secrecy capacity limited to vehicle communication and confirm that security parameters that can be controlled. Existing studies have attempted for secrecy capacity calculation by the system model but these efforts have failed for providing meaningful information. The vehicle secrecy capacity is defined with only Signal-to-Noise Ratio values provided in existing wireless communications to perform vehicle communication using the vehicle's defined secrecy capacity. The secure vehicle communication defined by the vehicle secrecy capacity within a security cluster.

In dangerous chemical logistics inside Internet of Vehicles (IoVs), encryption algorithms play a basic part in tending to security concerns. These concerns stem from the sensitivity of information related to the transportation and dealing with of dangerous materials. Encryption algorithms guarantee that delicate data, such as vehicle routes and communication between vehicles and central frameworks, is ensured from unauthorized access. Encryption algorithms defend information judgment by encoding it in a way that can as it were be unscrambled by authorized parties with the comparing keys. This anticipates unauthorized access or altering of basic data, decreasing the chance of robbery, attack, or unauthorized get to to dangerous materials. By scrambling information transmitted between vehicles and central frameworks, encryption algorithms ensure the security of people included in unsafe chemical logistics. This guarantees that individual data, such as driver personalities or cargo substance, remains secret and blocked off to unauthorized parties. Encryption algorithms improve the reliability of communication inside IoVs frameworks by avoiding listening in or information control. This guarantees that communications between vehicles, control centers, and other partners stay secure and solid, encouraging secure and productive transportation of perilous chemicals. By and large, encryption algorithms serve as a essential component of security measures in IoVs for perilous chemical logistics, defending delicate information, ensuring security, and improving the reliability of communication channels.

Contribution. The research aims to upgrade the data security of the Web of Vehicles (IoVs), especially concerning dangerous chemical logistics.

1. Firstly, it analyzes the special data characteristics of vehicles transporting unsafe chemicals, taken after by an examination of the Information Encryption Standard (DES) and Advanced Encryption Standard

(AES) algorithms inside the symmetric cryptosystem.

2. Furthermore, it digs into the RSA calculation inside the open key cryptosystem.
3. At last, the consider comprehensively assesses the execution of these calculations and the particular qualities of vehicle data.
4. Moreover, a crossover encryption calculation plot is proposed, wherein AES scrambles vehicle data and RSA is utilized to scramble AES keys.

Experimental outcomes illustrate the adequacy of this strategy in essentially moving forward the security of information transmission inside the Web of Vehicles.

The rest of the paper is organized as follows. Section II provides an overview of the exiting techniques. The research methodology is discussed in section III. Results and discussions are provided section IV and Finally, concluding remarks are provided in Section V.

2. Literature Review. The Internet of Vehicles technology is under the background of the increasingly perfect transportation infrastructure and the increasing difficulty of vehicle management, the concept established on the basis of the Internet of Things is the integration of traditional automobile industry and mobile Internet technology, it can be regarded as a specially optimized mobile ad hoc network. The Internet of Vehicles utilizes the integration of technologies such as GPS, RFID, wireless communication, and sensor networks, through information processing, wireless communication and information sharing between vehicles and X (people, roads, environment, etc.) In this way, it can realize the regulation of vehicles, improve traffic conditions, and at the same time provide users with comprehensive services such as safety and entertainment. The car networking system takes the car as the central node, and connects the car to the network through modern information means, realize the interconnected perception of vehicles and vehicles, vehicles and roads, vehicles and the environment. In today's Internet of Vehicles, the openness of wireless channels and the high-speed mobility of vehicles make vehicle information more vulnerable to attacks, for example, injecting erroneous beacon information into the communication link, tampering with and retransmitting previously broadcast beacon information, etc., can cause harm to the vehicle or driver. For example, Sun, Y, through security and privacy protection protocols and technologies, solve the problems of information security and privacy protection encountered by the Internet of Vehicles in the process of intelligent transportation [2]. Long, N. T. et al. proposed a security protection system for the Internet of Vehicles based on the case of security incidents of the Internet of Vehicles [3]. After analyzing the characteristics of the transmission channel of the Internet of Vehicles, Yu-Mei analyzed vehicle privacy and location privacy, and proposed schemes based on roadside nodes and mutual cooperation between vehicles [4]. Xin-Gang et al. designed a set of intelligent management security positioning system that can perceive in real time, realize precise positioning and security monitoring of data, and ensure the safe transmission of information [5]. Xu, B et al. explored the application of encryption technology in e-commerce in 2009 [6]. Liu, J. et al. studied encryption in aviation in 2009 [7]. In 2002, Wen-Yan conducted energy attack research on the AES algorithm, and the attack complexity ranged from 267 to 2131, which further reduced the scale of the attack [8]. In the same year, Wu, X improved the AES algorithm to make it have Square attack capability and good performance [9]. Based on the current research, the author proposes a research on the information security of the Internet of Vehicles. With the rapid development of intelligent transportation, the Internet of Vehicles as the core has huge development prospects. As a national strategic emerging industry, the safety of the Internet of Vehicles has become the focus, which is the premise and foundation of the development of the Internet of Vehicles. Aiming at the security threat of Internet of Vehicles information transmission, the author proposes a data transmission protection method based on encryption algorithm. Authors discussed the Vehicle-to-Vehicle communications that is suggested to secure in a secure cluster that refers to a vehicles group having a certain level of secrecy capacity. There are problems in secrecy capacity, but vehicular secrecy capacity is defined for the vehicle by SNR. The vehicular secrecy capacity is effective in achieving physical layer and may be changed by antenna related parameters. The vehicle-related parameters are addressed such as vehicle speed, safety distance etc. The vehicle-related secrecy parameters and secrecy capacity through modeling relationship is confirmed in traffic situations. The vehicular secrecy capacity is utilized to achieve secure vehicle communications that enables economic, and effective physical layer security [10]. Author in this paper discussed the Block-chain technology that has been emerged as a decentralized approach. The benefits of trustworthiness and mitigates the problem of single point of failure are offered by Blockchain. Author gives

Blockchain-enabled IoVs (BIoV) on their applications such as crowdsourcing-based applications, and accident avoidance and infotainment and content cashing. In-depth applications federated learning (FL) applications for BIoVs are also presented by the author [11]. Author in this paper presented a three-layer framework through which automotive security can be understood better. The vehicle dynamics and environmental sensors made up the sensing layer for jamming, and spoofing attacks. The communication layer is contained of both in-vehicle and V2X communications and sybil attacks. The sensing and communication layers are targeted by the attacks and affect the functionality and can further compromise the control layer security [12]. Author presented a Cyber Security Evaluation Framework (CSEF) for the evaluation of the security in-vehicle ECUs evaluation. The proposed technique is applied to On-Bord Unit (OBU) for providing a use case. The proposed CSEFis shown is to figure out assets, threats, and vulnerabilities of OBU, playing to conduct security evaluation. Moreover, for the cyber security evaluation, the CSEF can be extended such as the Telematic Box and the gateway [13].

Within the domain of high-speed mobility of vehicles, a noteworthy progressions have been made, with later considering the application of encryption algorithms in Internet of Vehicles (IoVs) to address security challenges. For instance, Wang et al. [3,4] proposed an enhancement strategy based on large traveler vulnerability to moderate the impacts of expansive traveler stream on high-speed mobility of vehicle frameworks. Xu, B et al. [6] further explored the application of encryption technology in e-commerce which is further combined with the study of encryption in aviation by Liu, J. et al. [7] Whereas these studies the effectiveness of improving safety and effectiveness, they don't broadly address the security concerns for IoVs. Later progressions in vehicular communication security have presented modern viewpoints on encryption algorithms. Quantum computing and physical layer security have developed as promising domain for supporting the security of vehicular communication systems. Quantum-resistant encryption algorithms offer security against potential dangers postured by quantum computing, ensuring the secrecy and judgment of transmitted information. Also, physical layer security strategies leverage the characteristics of remote communication channels to set up secure communication links, relieving and capturing attempted dangers. In light of these improvements, the proposed crossover encryption algorithm contributes essentially to upgrading the security of information transmission in perilous chemical logistics inside IoVs. By combining the qualities of customary encryption strategies with quantum-resistant procedures and physical layer security components, the crossover encryption algorithm offers vigorous security against different cyber dangers and guarantees the secrecy, integrity, and genuineness of delicate information transmitted over IoVs systems. Moreover, the integration of progressed encryption algorithms in IoVs frameworks upgrades the general strength and dependability of urban rail travel foundation, defending against potential security breaches and guaranteeing the secure and secure transportation of dangerous chemicals. In general, the proposed hybrid encryption algorithm provides a significant advancement in tending to security challenges in IoVs and contributes to the consistent advancement of security and security measures in urban rail travel frameworks.

The author in this paper details the emergence of the Internet that has provided a new direction for the development and upgrading of automobiles. The Internet technology and information technology are combined with existing vehicles for realizing the automobiles intelligent advancement. The developing smart cars goal is to achieve driverless driving and the problems in vehicle information security are increasing gradually. This paper studies the intelligent networking automotive technique and vehicle information security issues based on CAN bus that contributes to the intelligent networked vehicles [14].

Research Gap. Internet of Vehicles at home and abroad With the continuous improvement of sensing technology, network communication technology, and data analysis and computing technology, in-vehicle system networks, cyber-physical systems and automotive Internet of Things are also gradually developing. But for the security risks brought by intelligent connected cars, it is still a major problem that scholars need to break through.

3. Research Methodology.

Research status of the Internet of Vehicles at home and abroad. With the continuous improvement of sensing technology, network communication technology, and data analysis and computing technology, in-vehicle system networks, cyber-physical systems and automotive Internet of Things are also gradually developing. But for the security risks brought by intelligent connected cars, it is still a major problem that scholars need to break through.

Current status of foreign IoV research. Behind the convenience that cars provide people, they also threaten people's safety all the time, the convenience and safety it brings are contradictory [15]. With the increasing number of Internet of Vehicles applications, assisted driving technology, and the birth of the corresponding self-driving cars, have made the existing contradictions even more serious. In 2015, talented American hackers Charlie Miller and Chis hllmlk tested a car for a cyber attack, during the test, the Ucomect in-vehicle system was installed on the vehicle and the car was driven normally, they use remote commands to hack into the vehicle system and try to control the car, after intrusion, they use remote commands to overturn the car, such security threats will seriously affect the safety of the occupants of the vehicle. In October 2016, NHTSA (U.S. Department of Transportation Road Traffic Safety Administration) released the "Best Practices for Cybersecurity in Hyundai Vehicles", this best practice shows that the development of the Internet of Vehicles requires network security, and has good guidance for the development of the Internet of Vehicles enterprises, it clearly proposes to formulate automotive safety standards including cybersecurity, it is used to regulate individuals and organizations such as automobile manufacturing, automobile system or software design, and suppliers, aiming to improve the security of modern vehicle networks, and to guide on-board systems how to prevent and defend against cyber attacks [16]. At the same time, NHTSA also requires Internet of Vehicles companies to conduct network security assessments on in-vehicle assistance systems. Equipment that does not meet security standards cannot be installed on vehicles, and measures should be taken to deal with network threats and network vulnerabilities.

Research status of domestic Internet of Vehicles. My country introduced the concept of Internet of Vehicles in 2010, my country's automobile manufacturers, as well as various automobile technology research institutions, have established the In-Vehicle Information Service Industry Application Alliance (TIAA), committed to the research and application of Internet of Vehicles technology, and promote the development of Internet of Vehicles in my country. The research content of the Internet of Vehicles in the field of transportation is mainly divided into two aspects: highway and urban road traffic safety. Among them, the construction projects of expressways include the national network of expressway ETC, which solves the congestion problem of expressway toll stations in my country and is a major engineering project in China. Implementation of the project, there is no need to manually manage expressway tolls, which improves the operating efficiency of vehicles on expressways, the management department can also check the safety status of the vehicle operation on the highway in real time. In the construction of urban road safety, in order to alleviate traffic congestion and improve road traffic conditions, each city has established a vehicle management system to centrally control and dispatch all vehicles [17]. My country's smart car industry is in a stage of rapid development. In order to promote the development of its smart cars, the goal of the smart vehicle innovation development strategy proposed by the state, it is the six major systems that will eventually establish the Internet of Vehicles industry, and it also attaches great importance to the core technology of smart cars, my country is still in the follow-up stage and needs to establish its own car networking system, build five basic platforms for smart cars, and promote the construction of innovative capacity for smart connected cars [18]. In July 2017, in order to integrate superior resources, promote the development of the standard "Information Security Technology Automotive Electronic System Network Security Guidelines", network security research institutions represented by China Electronics Standardization Institute and University of Electronic Science and Technology of China, combined with China FAW, Shanghai Automobile, and other automobile manufacturers to form a standard preparation working group, jointly promote the first national standard in the field of automotive electronic network security in my country.

The methodology for this study involves a systematic approach to analyzing the characteristics of hazardous chemical information and conducting subsequent encryption algorithm analysis to enhance methodological transparency. Initially, relevant information regarding hazardous chemicals, including their properties, handling requirements, and transportation regulations, will be collected through literature review and consultation with industry experts. This data will then be categorized and classified based on characteristics such as toxicity level, flammability, and health hazards, followed by a comprehensive risk assessment to identify potential vulnerabilities in transportation and handling processes. Subsequently, specific information security requirements related to hazardous chemical logistics will be analyzed, focusing on aspects such as data confidentiality, integrity, availability, and authentication. Based on these requirements, criteria for selecting encryption algorithms will

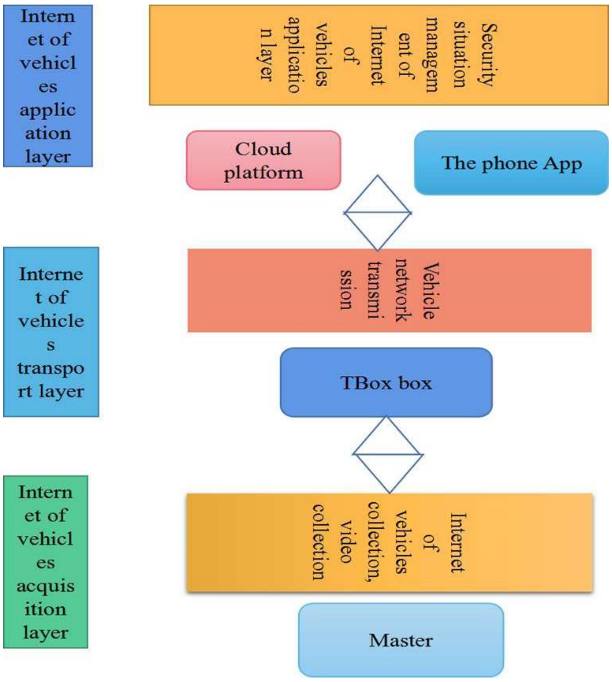
Internet of vehicles application layer
Security situation management of Internet of vehicles application layer
Cloud platform
The phone App
Internet of vehicles transport layer
Vehicle network transmission
TBox box
Internet of vehicles acquisition layer
Internet of vehicles collection, video collection
Master

Fig. 3.1: The structure of the vehicle network system

be defined, considering factors such as encryption strength, computational efficiency, and compatibility with existing systems. Different encryption algorithms will then be evaluated based on their performance against the selection criteria, including practical implementation considerations and security analysis to identify potential vulnerabilities and attack vectors. Integration of findings will involve synthesizing results from the hazardous chemical information analysis and encryption algorithm evaluation to provide recommendations for enhancing information security in hazardous chemical logistics within Internet of Vehicles (IoVs). Through these specific procedures, this methodology aims to ensure methodological transparency and rigor in addressing the research objectives.

3.1. Internet of Vehicles System. The architecture of the Internet of Vehicles is divided into application layer, transmission layer and acquisition layer, as shown in Figure 3.1.

(1) Application layer: Mainly aimed at car users, it provides users with intelligent services through mobile terminals such as mobile phones. It mainly realizes the functions of road condition analysis, vehicle status analysis and vehicle failure analysis, in this process, it achieves information sharing with the urban transportation center, provides convenient services to users, and also provides assistance to urban transportation.

(2) Transport layer: The collected data is transmitted to the application layer by means of 4G, Bluetooth and RFID.

(3) Acquisition layer: Using car sensors, video collectors and audio collectors, etc., to obtain information such as the car's own state and road conditions, and then to the application layer through the transport layer. At this stage, the function of the Internet of Vehicles is still in the monitoring stage, and the unification of people, vehicles and roads has not been effectively realized.

1. Cyber Security Assessment System. Usually like a checklist or a set of rules that specialists utilize to check how secure and secure a computer framework or a organize is. It makes a difference them get it in the event that there are any shortcomings or vulnerabilities that programmers seem abuse to take data or cause issues. By taking after this system, they can make beyond any doubt that the framework is as ensured as conceivable against cyber dangers.

2. Vehicular Communication Vulnerabilities. Envision in the event that vehicles may deliver to each other and share data like where they're going or in case there's something within the road ahead. It might to offer assistance prevent accidents and make driving more secure. But in the event that programmers were able to urge into this communication framework, they seem cause chaos. They could create the things they're not assumed to, like all of a sudden halt or swerve off the road. This might lead to mischances and put people's lives in threat. So, it's truly imperative to form any doubt that the communication between vehicles is secure and ensured from programmers.

Practical Illustrations of Encryption Algorithms in Vehicular Communication and Suggestions of NHTSA's Recommendation:

1. Illustrations of Encryption Algorithms. Encryption algorithms are like secret codes that are utilized to keep data secure when it's being sent from one put to another. For illustration, envision you're sending a message to a companion, but you do not need anybody else to be able to examine it. You may utilize an encryption algorithm to turn your message into a secret code some time recently you send it. At that point, your companion can utilize the same algorithm to turn the code back into the initial message when they get it. This way, indeed in the event that somebody tries to captured the message, they won't be able to get it it since it's all cluttered up.

2. Suggestions of NHTSA's Recommendation for V2V Communication. The National Highway Activity Security Organization (NHTSA) has proposed that modern vehicles should be prepared with innovation called Vehicle-to-Vehicle (V2V) communication. This implies that cars would be able to link each other wirelessly, sharing data about their speed, course, and area. The idea is to assist anticipate mischances by giving drivers notices in the event that there's a hazard of a collision. For illustration, in case one vehicle abruptly brakes, it seem send a flag to adjacent cars to caution them to moderate down. By utilizing encryption algorithms to secure this communication, the NHTSA points to guarantee that the data exchanged between vehicles is secured from programmers who might attempt to alter with it or cause mishaps by sending untrue signals. This would make our roads more secure for everyone.

Within the setting of unsafe chemical logistics, both AES (Advanced Encryption Standard) and RSA (Rivest-Shamir-Adleman) encryption algorithms play a critical parts.

AES Encryption Algorithm. AES may be a symmetric encryption calculation known for its productivity and security. In dangerous chemical logistics inside IoVs, AES can be utilized to encrypt delicate information transmitted between vehicles, control centers, and other partners. AES guarantees information privacy and integrity, ensuring against unauthorized access and altering of basic data such as cargo subtle elements, course plans, and crisis conventions. The strong security and effectiveness of AES make it well-suited for securing communication channels and information exchanges in dangerous chemical logistics scenarios.

RSA Encryption Algorithm. RSA is an asymmetric encryption algorithm commonly utilized for key exchange and computerized marks. In unsafe chemical logistics inside IoVs, RSA can be utilized for secure key trade instruments, empowering encrypted communication channels between vehicles and control centers. RSA gives a secure establishment for establishing trust and realness in IoVs systems, confirming the personality of members and guaranteeing the judgment of transmitted information. Whereas RSA offers solid security ensures, its computational complexity may present proficiency challenges in resource-constrained IoVs situations, requiring cautious consideration of execution trade-offs.

In this way, both AES and RSA encryption algorithms play basic parts in guaranteeing the security and security of information transmission in dangerous chemical logistics inside IoVs, defending against cyber dangers and unauthorized get to to sensitive data.

3.2. Protection method of data transmission based on encryption algorithm. For the communication transmission link of the Internet of Vehicles, the author designs a transmission link with an encryption algorithm, as shown in Figure 3.2, the T-BOX box in the Internet of Vehicles uses an encryption algorithm to encrypt the original data packets, send encrypted data to the transport channel [19]. After receiving the encrypted data packet in the backend of the Internet of Vehicles, it uses the decryption algorithm to decrypt the encrypted data packet, and performs verification processing on the data, if the data passes the verification, the corresponding instruction is executed; If the data does not pass the verification, the data is discarded.

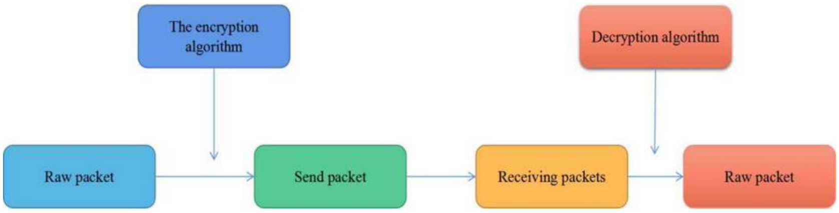

Fig. 3.2: Flowchart of adding encryption algorithm information

(1) Principle of Hybrid Encryption Algorithm. The hybrid encryption algorithm needs to consider the encryption mode, whether to use the AES algorithm or the RSA algorithm to encrypt the vehicle information, not only the characteristics of the algorithm itself, but also the characteristics of the vehicle information should be considered. Combining the previous analysis and the description of the vehicle information, the encrypted data is a series of strings. We know that the RSA algorithm takes a long time to encrypt a small amount of data, so the AES algorithm is used to encrypt plaintext data, generate AES key and ciphertext, and then encrypt the AES key with RSA, which enhances the security of the encryption system; After receiving the data, the receiver first uses the RSA key to decrypt the AES key, uses the AES key to decrypt the ciphertext, and recovers the plaintext information 20.

(2) Development Trend of Hybrid Encryption Algorithms. With the continuous advancement of positioning technology and mobile network technology, promoted the development of location-based applications, in terms of vehicle location privacy protection, schemes based on encryption techniques are commonly used. In the information security of the Internet of Vehicles, the hybrid encryption algorithm is more and more widely used in the field of network information security, and the hybrid algorithm is usually realized by a combination of hardware and software. Due to the fast encryption speed of the symmetric encryption algorithm, the asymmetric encryption algorithm has high security, so the combination of the two is a popular way today, such as DES-RSA, IDEA-RSA, DES-ELGAMAL. In today's information network communication, the hybrid encryption algorithm because of its good encryption performance, in practice, the frequency of use is extremely high. Some of ZTE's high-end products, such as routers, feature hybrid encryption. Choose a combination from symmetric encryption algorithms such as DES, 3DES, IDEA, and asymmetric encryption algorithms such as RSA, ECC, etc, the hybrid algorithm combines the advantages of the two algorithms, will be more widely used in the future.

3.3. The legal development trend of encryption algorithm. With the continuous advancement of positioning technology and mobile network technology, promoted the development of location-based applications, in terms of vehicle location privacy protection, schemes based on encryption techniques are commonly used. In the information security of the Internet of Vehicles, the hybrid encryption algorithm is more and more widely used in the field of network information security, the hybrid algorithm is usually implemented by a combination of hardware and software [21]. Due to the fast encryption speed of the symmetric encryption algorithm, asymmetric encryption algorithms have high security, so the combination of the two is a popular way today, such as DES-RSA, IDEA-RSA, DES-ELGAMAL. In today's information network communication, the hybrid encryption algorithm because of its good encryption performance, in practice, the frequency of use is extremely high. Some of ZTE's high-end products, such as routers, feature hybrid encryption. Choose a combination from symmetric encryption algorithms such as DES, 3DES, IDEA, and asymmetric encryption algorithms such as RSA, ECC, etc. the hybrid algorithm combines the advantages of the two algorithms and will be more widely used in the future [22].

4. Experiments and Research. To validate the adequacy of the proposed encryption strategy, a comprehensive exploratory setup and information examination strategies are vital. The test setup and information examination strategies, besides the insights into the suggestions of encryption algorithm determination on the in general security and effectiveness of Internet of Vehicles (IoVs) in unsafe chemical logistics.

1. Experimental Setup. Create a dataset representing different scenarios in perilous chemical logistics inside IoVs. This dataset ought to incorporate data such as vehicle courses, cargo points of interest, communication messages, and potential security dangers. Execute the proposed encryption strategy, consolidating chosen encryption algorithms (e.g., AES, RSA) into the IoVs communication system. Guarantee that encryption is connected to delicate information transmissions between vehicles, control centers, and other partners.

2. Simulation Environment. Create an environment imitating real-world IoVs scenarios, including vehicle development, communication conventions, and potential security vulnerabilities. Utilize simulation apparatuses such as ns-3 or OMNeT++ for reasonable experimentation. Then design different scenarios speaking to distinctive security dangers and attack scenarios, such as listening stealthily, altering, or information capture attempts. Control parameters to simulate diverse levels of risk escalated and encryption algorithm adequacy. For data analysis, the encryption algorithm, assess the performance of the encryption method by measuring the parameters like encryption/decryption speed, computational overhead, and resource utilization. Then comparing the performance of different encryption algorithms (e.g., AES, RSA) under various scenarios. For evaluating the security effectiveness of the encryption method by analyzing its resilience against common cyber threats and attack vectors. Generally, the determination of encryption algorithms such as AES or RSA in IoVs for dangerous chemical logistics includes trade-offs between security, productivity, and computational overhead. Cautious consideration of these components is basic to guarantee the viability and unwavering quality of encryption strategies in shielding the delicate information transmissions and ensuring against cyber dangers in IoVs situations.

4.1. Process Design of Hazardous Chemical Vehicle Encryption System. The overall process of the remote encryption monitoring system for hazardous chemicals vehicles. First initialize the system, the CPU enters the state of preparing to execute the task, load the AES initial key to the AES-EN port for key expansion, so that the encryption operation can be performed directly when there is vehicle information. Then the Beidou module transmits the obtained positioning data to the built-in CPU of the FPGA through the serial interface, and after analysis and processing, send the vehicle location information to the encryption unit AESand RSA-Core to encrypt the vehicle information to form ciphertext, and send the ciphertext to the communication module through the serial interface, the communication module sends the ciphertext to the measurement and control center through the wireless transmission network, and uses the software to decrypt the ciphertext, the vehicle position information is recovered and stored in the database, and the measurement and control center calls the vehicle information in the database to display on the terminal computer [23].

(1) Research on encryption algorithms. At present, with the expansion of the operation scope of the logistics industry, the scale of the network of vehicles for hazardous chemicals logistics is gradually expanding, and there is a lot of real-time status information of vehicles. Due to the transparency of the information transmission of the Internet of Vehicles, there is a problem with the safety of vehicle driving. Based on the actual situation and specific needs of the project, the author encrypts the information of the hazardous chemicals logistics vehicle to ensure the safe operation of the vehicle. The second chapter elaborates the encrypted monitoring system for hazardous chemicals vehicles [24]. The positioning data received from the Beidou satellite is analyzed by the CPU to extract the vehicle's driving date, longitude, latitude, altitude and other information data, these vehicle information formats are all ASCII character formats, and the corresponding message message format is designed in combination with the type and characteristics of the data.

(2) Encryption algorithm. After the "Prism" incident in the United States, my country actively promotes domestic encryption algorithms, and proposes to replace foreign encryption algorithms with domestic encryption algorithms to encrypt data, making it difficult for NSA to crack. The block cipher algorithm is a symmetric cipher algorithm, which is mainly used to realize the encryption and decryption of data information. The plaintext, key and ciphertext of the encryption algorithm are all 128 bits, and the same key is used for encryption and decryption [25]. Both the encryption algorithm and the key expansion algorithm are implemented by a

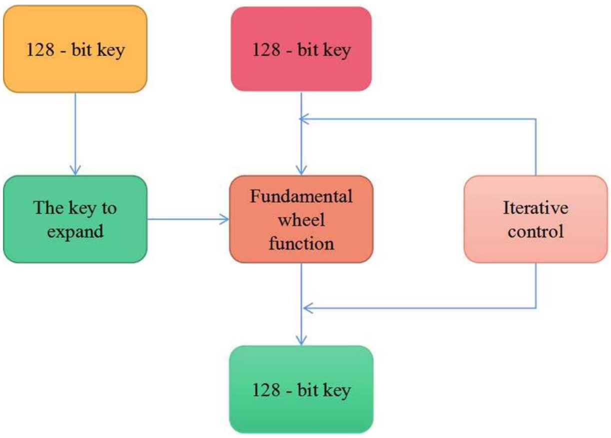

Fig. 4.1: The overall structure of the encryption algorithm

non-linear iterative round function with 32 cycles. The core of the data encryption part is the round function, which combines linear and nonlinear.The basic process is to first divide the 128-bit key into 4 groups according to a 32-bit group, and then generate 32 groups of 32-bit keys according to the key expansion algorithm; Then, the input 128-bit data is also divided into 4 groups according to 32-bit group for circular operation. The overall structure of the encryption algorithm is shown in Figure 4.1.

The plaintext X is 128 bits, rk0 rk32 are 32 sets of round keys, and the synthetic permutation T forms the round function F.

In the formula, L is a linear transformation;   is a nonlinear transformation.The round key rk is generated by the key expansion algorithm. Known encryption key MK= (MK0,MK1,MK2,MK3), system parameter is FK= (FK0,FK1,FK2,FK3), fixed parameter CK= (CK0,...CK1,...CK31).

The output of the encryption transformation is: The decryption transformation of the encryption algorithm has the same structure as the encryption transformation, and the only difference is that the round key is used in the reverse order.

4.2. Performance Analysis of Encryption Algorithms. Through the theoretical analysis of the AES and RSA algorithms, the following is a comparative analysis of the performance of the hybrid encryption algorithm and the single algorithm from the aspects of encryption speed, security and key management [26].

(1) Encryption speed. For the RSA algorithm, to ensure security, its modulus n needs to be at least 1024 bits, then a large number of large integer multiplication and modulo operations are required, the time required for the RSA algorithm to encrypt and decrypt 1M (vehicle information in the Internet of Vehicles) files has been greater than 100s, the following mainly simulates the DES algorithm, the AES algorithm and the AES and RSA hybrid algorithm on MATLAB [27]. The results are shown in Figure 4.2.

As can be seen from Figure 4.2, the encryption speed of AES algorithm is obviously better than that of DES and hybrid encryption algorithm, and the performance of hybrid encryption algorithm and DES algorithm is close, however, in view of the security issues of DES and AES algorithms, hybrid algorithms are widely used in practice, therefore, comprehensive comparison and analysis, the performance of each algorithm, in this paper, AES and RSA hybrid encryption algorithm is selected to encrypt vehicle information [28].

(2) Security. This is the level of secrecy scientists have assigned to their data for a long time. From the previous analysis of DES algorithm, AES algorithm and RSA algorithm, it can be seen that a single encryption algorithm can no longer meet our security requirements, so a hybrid algorithm is proposed.

(3) Key management. From the theoretical analysis of the previous algorithm, it can be seen that RSA belongs to the public encryption system, and the encryption key is distributed in the public form, so the update of the encryption key is very easy, and for different communication objects, only need to keep their own decryption key secret. The AES algorithm belongs to the symmetric cryptosystem, for different communication

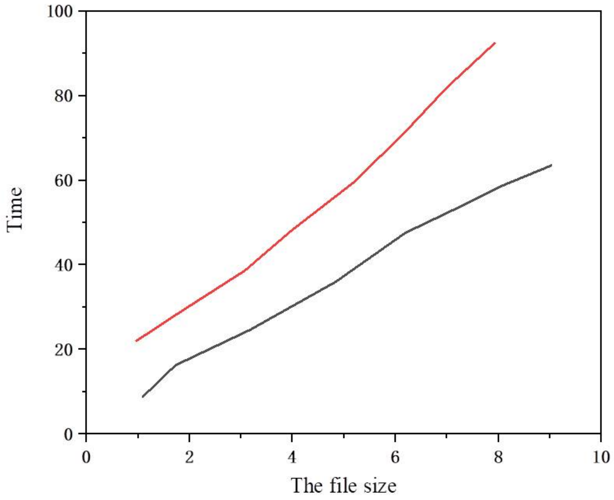

Fig. 4.2: Relationship between encryption and decryption time and file size

objects, AES needs to generate and store different passwords, the key management system has a large overhead, the key must be distributed before the communication, and the key needs to be replaced for different data, the replacement of the key is very difficult. In the hybrid encryption algorithm, the RSA algorithm only needs to encrypt the 128-bit key once, and does not need to generate a key pair, then there is no key management problem, it can be considered that the hybrid encryption algorithm solves the problem of AES and RSA key management. From this, it can be seen that, the AES encryption speed is faster than the RSA algorithm, especially for a large amount of information encryption, it is more advantageous to use the AES algorithm to encrypt. However, the AES algorithm has serious security problems in key management. There is no key transmission problem in the RSA algorithm, because the public key itself is public, and according to the RSA algorithm, it is difficult for a third party to solve the private key. Therefore, the author combines the advantages of the two algorithms, and combines the characteristics of the hazardous chemicals logistics vehicle information, and adopts the scheme of AES encryption of vehicle information and RSA encryption of AES keys.

4.3. Design of Encryption Algorithm Level Table. According to the mixed criticality of automotive electronic systems, information security is related to functional safety, different functions require different information security levels, the encryption algorithm is related to the information security level, different information security levels require different security encryption algorithms. The encryption algorithm level table reflects the corresponding relationship between key functions, information security levels and encryption algorithms. The security of encryption algorithms is quite different. High-level algorithms should ensure high encryption strength, at the same time, it meets the real-time requirements of the system, for example, once the car brake control function is cracked and exploited by an attacker, it is very likely to cause car crashes, so we must focus on protection, you can choose high-level encryption algorithms such as AES algorithm, ensure message security; While satisfying a certain encryption strength, low-level algorithms should occupy as little system resources as possible, save encryption and decryption time, and improve system efficiency, for example, if the window control function is cracked by an attacker, it will not pose a fatal risk to personnel. Lightweight encryption algorithms such as TEA are suitable choices. According to the ASCII level and the risk classification of automobile information security, the encryption algorithm level table is designed in combination with the security of the encryption algorithm, as shown in Table 4.1.

Table 4.2, from top to bottom, corresponds to the information security level, encryption algorithm, and

Table 4.1: The relationship between the security level and each algorithm

Security level	Symmetric dense length	key length	Confidentiality period
90	9	1036	2011
100	113	2038	2020
170	189	3312	2030

Table 4.2: Parameter settings

enter	din[127:0]=1 8720563580201 60101 1023456276731 key[127:0]=000102030405060708090a0b0c0d0e0f
output	dout[I 97-01-3 38hac077 fa 2 hfdla u489.70h0adh

the corresponding algorithm identification and ID range from low to high according to functional security requirements. In the CAN protocol, the frame ID is used to identify the priority of the CAN data frame. The smaller the frame ID value, the higher the frame priority. The higher the criticality of the vehicle function, the more timely the message needs to be transmitted. In order to transmit the message of the high critical function in time, the priority of the message ID should be assigned higher. According to the standard frame ID value range 0x000-0x7FF, the author assumes the ID range in Table 4.1 according to the security level. The design also combines encryption algorithms of different security levels to form an algorithm library, and assigns an algorithm identifier to each encryption algorithm, which is used as a unique characteristic value to realize the dynamic scheduling of encryption algorithms.

4.4. Analysis of AES Simulation Results. First, initialize the parameters of the designed BD2 encryption system. Combined with the project requirements, the input data is part of the vehicle information. The PLL generates the clock signal for each module in the system to work normally, the input clock signal is 50MHz, and the output clock signal c. For the frequency of 75MHz, the phase of 600 drives the SDRAM chip to work; q is a 75MHz drive encryption module; c2 is a 75MHz drive control module, such as CPU and peripheral modules. The pin UART-rxd is connected to the BD2 receiving module, and the UART-txd sends the cipher text to GPRS, and sends the cipher text to the monitoring center through the wireless transmission network, the monitoring terminal uses software to decrypt the ciphertext to recover the vehicle location information, for the relevant personnel to dispatch and manage vehicles. Table 5.1 is the setting of related parameters. This system uses Modelsim to simulate, the pins dout-a and dout-r[of the AES and RSA encryption modules have outputs, and the CPU is connected to the pins such as enc and clk, controls when encryption and key entry start. The positioning data of BD2 is input from UART-rxd, through the encryption module to the dout pin to the control module, here, the ciphertext is sent to the GPRS module via the UART-txd pin. According to the requirements of the project team, we only encrypt and decrypt the vehicle's terminal ID, positioning time, longitude and latitude. The file names are all named AES. as shown in Table 4.2.

First, use the AES encryption module alone, input din and key, and output the data doout through the AES encryption module, it is sent to the monitoring center through the wireless transmission network and decrypted by software.

5. Conclusion. To advance encryption algorithms for Internet of Vehicles (IoVs) in hazardous chemical logistics, several promising avenues warrant exploration. Firstly, the development of quantum-resistant cryptography is essential to withstand potential future threats posed by quantum computers, ensuring the longevity of IoV security. Additionally, investigating the application of homomorphic encryption could enable secure computation on encrypted data, enhancing privacy without compromising data analysis capabilities. Dynamic key management techniques tailored to the dynamic nature of IoV environments could bolster security by facilitating real-time distribution and updating of encryption keys. Moreover, staying abreast of post-quantum cryptography standards and adopting emerging techniques resilient to quantum attacks is paramount for IoV security. Furthermore, research into secure multiparty computation methods and their integration with IoV systems could enable secure collaboration and data sharing among vehicles and infrastructure. Thus, exploring the integration of blockchain technology with encryption algorithms has the potential to enhance transparency, accountability, and data integrity in hazardous chemical logistics within IoVs. The author deeply analyzes the status quo of the vehicle networking of hazardous chemicals logistics vehicles, aiming at the privacy protection of the vehicle's location, this paper proposes and designs a hybrid encryption algorithm for the vehicle networking of hazardous chemicals logistics vehicles, and completes the design and implementation of each module in the hybrid encryption system. Based on the system architecture of the Internet of Vehicles, the author proposes a protection method based on an encryption algorithm for the low security of the data of the Internet of Vehicles. Finally, the performance of the algorithm and the characteristics of vehicle information are comprehensively analyzed, and a hybrid encryption algorithm scheme is proposed, that is, AES encrypts vehicle information, technical scheme for encrypting AES keys with Rivest-Shamir-Adleman encryption (RSA). The benefit of encryption algorithm is analyzed from the security and realization of encryption algorithm. Finally, the experimental results show that the use of encryption algorithms can effectively protect the transmission data and increase the protection capability of the Internet of Vehicles information transmission. By advancing encryption algorithms in these directions, IoV systems can be fortified against evolving security threats, ensuring the robust protection of sensitive data and critical operations.

REFERENCES

[1] Yan, R., Lin, C., Zhang, W. F., Chen, L. W., Peng, K. N. , *Research on information security of users' electricity data including electric vehicle based on elliptic curve encryption*, International Journal of Distributed Sensor Networks, 16(11), 155014772096845, 2020.

[2] Sun, Y., Li, X., Lv, F., Hu, B. , *Research on logistics information blockchain data query algorithm based on searchable encryption*, IEEE Access, PP(99), 1-1, 2021.

[3] Long, N. T. , *Research on innovating and applying cryptography algorithms for security routing in service based routing*, Internet of Things and Cloud Computing, 3(3), 33-41, 2015.

[4] Yu-Mei, Y. I. , *Study on location-transportation optimization for hazardous material logistics network*, China Safety Science Journal, 21(6), 135-140, 2011.

[5] Xin-Gang, J. U., Guo, H. O., Liu, Y. , *Research of the security of iris recognition based on composite chaos encryption*, Journal of Henan Normal University(Natural Science), 37(3), 68-70, 2009.

[6] Xu, B., Zhang, L. H., Tan, X. P. , *Two-level emergency centers location model based on the hazardous chemicals' accidents*, Systems Engineering-Theory Practice, 35(3), 728-735, 2015.

[7] Wu, X., Oh, H. C., Akarimi, I., Goh, M., Souza, R. D. , *Tops: advanced decision support system for port and maritime chemical logistics*, The Asian Journal of Shipping and Logistics, 27(1), 143-156, 2011.

[8] Sang-Il, Jo, Jaesung, Lee , *Vehicle detection algorithm for vds by using décalcomanie matching based on histogram*, The Journal of Korean Institute of Communications and Information Sciences, 42(6), 1225-1232, 2017.

[9] Liu, C., Shao, Y., Cai, Z., Li, Y. , *Unmanned aerial vehicle positioning algorithm based on the secant slope characteristics of transmission lines*,IEEE Access, PP(99), 1-1.

[10] Ahn, N. Y., Lee, D. H. *Physical Layer Security of Autonomous Driving: Secure Vehicle-to-Vehicle Communication in A Security Cluster.* arXiv preprint arXiv:1912.06527, 2019.

[11] Hildebrand, B., Baza, M., Salman, T., Amsaad, F., Razaqu, A., Alourani, A. *A Comprehensive Review on Blockchains for Internet of Vehicles: Challenges and Directions.* arXiv preprint arXiv:2203.10708, 2022.

[12] El-Rewini, Z., Sadatsharan, K., Selvaraj, D. F., Plathottam, S. J., Ranganathan, P. *Cybersecurity challenges in vehicular communications.* Vehicular Communications, 23, 100214, 2020.

[13] Zhang, H., Pan, Y., Lu, Z., Wang, J., Liu, Z. *A Cyber Security Evaluation Framework for In-Vehicle Electrical Control Units.* IEEE Access, 9, 149690-149706, 2021.

[14] Chen, C., Zhang, B., Liu, M., Wei, S., Zhang, J., Shen, L. *Research on Intelligent Networking Automotive Technology and Information Security Based on CAN Bus.* In IOP Conference Series: Materials Science and Engineering (Vol. 688, No. 4, p. 044058). IOP Publishing, 2019.

[15] Zhang, H. , *An analysis on vehicular ad-hoc networks: research issues, challenges and applications*, International journal of computational intelligence research, 14(8), 641-655, 2018.

[16] Sari, A., Onursal, O., Akkaya, M. , *AReview of the security issues in vehicular ad hoc networks (vanet)*, International Journal of Communications, Network and System Sciences, 8(13), 552-566, 2015.

[17] Wan, J., Yan, H., Hui, S., Fang, L. , *Advances in cyber-physical systems research*, Ksii Transactions on Internet Information Systems, 5(11), 1891-1908, 2011.

[18] Ae Ger, A., Bimeyer, N., H Stübing, Huss, S. A. , *A novel framework for efficient mobility data verification in vehicular ad-hoc networks*, International Journal of Intelligent Transportation Systems Research, 10(1), 11-21, 2012.

[19] Fishman, S., Ph., D. , *Studies of the upper-extremity amputee* , Artificial Limbs, 5(1), 88, 1958.
[20] Kumar, N. S., Rajakumar, K. , *A study on security for adaptive periodic threshold sensitive energy efficient protocol based on elliptic curve cryptology in wireless sensor network*, International journal of computing information technology, 11(2), 137-147, 2019.
[21] Kumar, N. S., Rajakumar, K. , *A study on security for adaptive periodic threshold sensitive energy efficient protocol based on elliptic curve cryptology in wireless sensor network*, International journal of computing information technology, 11(2), 137-147, 2019.
[22] Council, B. N. , *SThird international symposium on intelligent information technology and security informatics*, Mis Quarterly, 33(4), 1, 2010.
[23] Kai, L. , *Research on adaptive target tracking in vehicle sensor networks*,Journal of Network Computer Applications, 36(5), 1316-1323, 2013.
[24] Qureshi, K. N., Alhudhaif, A., Shah, A. A., Majeed, S., Jeon, G. , *Trust and priority-based drone assisted routing and mobility and service-oriented solution for the internet of vehicles networks*, Journal of Information Security and Applications, 59(5), 102864.
[25] Goel, S., Yuan, Y. , *Emerging research in connected vehicles [guest editorial*, IEEE Intelligent Transportation Systems Magazine, 7(2), 6-9, 2015.
[26] B Ji, X Zhang, S Mumtaz, C Han, C Li, H Wen, *Survey on the internet of vehicles: network architectures and applications*, IEEE Communications Standards Magazine, 4(1), 34-41, 2022.
[27] Schumacher, H. J., Ghosh, S. , *A fundamental framework for network security*, Journal of Network Computer Applications, 20(3), 305-322, 1997.
[28] Nopmongcol, U., Griffin, W. M., Yarwood, G., Dunker, A. M., Maclean, H. L., Mansell, G. , *Impact of dedicated e85 vehicle use on ozone and particulate matter in the us*, Atmospheric environment, 45(39), p.7330-7340, 2011.

Edited by: Pradeep Kumar Singh
Special issue on: Intelligent Cloud Technologies Enabled Solutions for Next Generation Smart Cities
Received: Nov 9, 2022
Accepted: Mar 1, 2024