Research on the Security Assessment of Cloud Communication in Intelligent Connected Vehicle

Shihao Xue[1,2,a] ,Yuqiao Ning[1,2,b], Yang Chen[1,2,c], Qingyang Wu[1,2,d], Shiwen Shen[1,2,e], Quanrui Huo[1,2,f]

[1]CATARC Intelligent and connected technology Co.,LTd.
[2]China Automotive Technology&Research Center Co.,Ltd.
Tianjin, China

[a]xueshihao@catarc.ac.cn,[b]ningyuqiao@catarc.ac.cn
[c]chenyang2022@catarc.ac.cn,[d]wuqingyang@catarc.ac.cn
[e]shenshiwen@catarc.ac.cn,[f]huoquanrui@catarc.ac.cn

Abstract. This paper introduces a theory and method for vehicle Telematics BOX (T-BOX) communication security assessment. The exponential growth of data generated in vehicles now raises a great deal of data leakage security risks, while there are a large number of data interaction scenarios. This paper will analyse and explain how to conduct security assessment for intelligent connected vehicles cloud communication from various aspects such as inter-platform communication security and vehicle terminal communication security, including the tools needed, evaluation methods and how to evaluate and judge the results, with the aim of ensuring the safe operation of intelligent connected vehicles, preventing accidents caused by security issues, and protecting the lives and properties of vehicle users and the public.

Keywords: intelligent connected vehicles, information security, vehicle terminals, cloud security

1 Introduction

The automotive industry is rapidly iterating, but at the same time the industry lacks a security baseline. There are data security issues such as transmission of important data, leakage of personal information, tampering or replaying of vehicle control type data in the vehicle terminal and cloud, which seriously affects driving safety, personal safety and privacy security[1]. On the other hand, the data interaction scenarios of intelligent connected vehicles show explosive growth, such as data management platform systems, information service system platforms, over the air (OTA) platform systems, and connected vehicle monitoring and management platform systems, all of which retain a large amount of various types of data[2].

In recent years, with the introduction of regulations and policies and continuous strengthening of supervision, many vehicle companies have been carrying out data security-related capacity building work and gradually building data security protec-

A. Rauf et al. (eds.), *Proceedings of the 3rd International Conference on Management Science and Software Engineering (ICMSSE 2023)*, Atlantis Highlights in Engineering 20,
https://doi.org/10.2991/978-94-6463-262-0_15

tion capabilities, but the regulatory standard system has not yet been perfected and there are difficulties in data compliance practices.

It is extremely difficult to build a complete systemic security solution as there are policy, financial and capacity barriers for enterprises to carry out technological research and application implementation. It is common for automotive companies to strengthen their own security protection capabilities by digging into the point pattern of vulnerabilities and following the research methods and assessment techniques described in this paper.

2 Research Background

As a product of the deep integration of multiple industries such as automotive, transportation, electronics and information and communication, the Internet of Vehicles has now become the focus of attention in the field of information security[3]. As an Internet service provided by the Internet of Vehicles industry based on cloud computing and big data, the Internet of Vehicles cloud platform greatly enhances the functionality of Internet of Vehicles applications and improves the user's business experience, but also introduces the security issues of cloud computing technology itself into the Internet of Vehicles, such as cloud computing virtualization, multi-tenancy, cloud computing data security, privacy protection, virtual resource scheduling and management issues, etc., which makes the Internet of Vehicles inevitably face security risks caused by vulnerabilities in the application service itself. For example, some general application such as Web Server programs, FTP service programs, etc. have their own security vulnerabilities, and hackers will face the risk of large volume of vehicle information leakage from the cloud platform and vehicle control by exploiting cloud platform vulnerabilities and interface injection vulnerabilities, or attempting APP injection[4]. On the other hand, as the central node of the Internet of Vehicles application service, attackers use security vulnerabilities to implement attacks such as invasion and control of the application service platform by using intelligent terminals or communication networks as entry points, thus leading to a large number of vehicels being illegally controlled, while threatening the information security and privacy leakage of the entire network[5]. Possible security vulnerabilities in the operating system of the Internet of Vehicles cloud platform, as well as the vulnerability of the operating system itself, affect the security of the cloud service platform. In addition, security threats due to improper configuration can also lead to a degradation of the overall Internet of Vehicle security performance.

For the security of communication between vehicles, there is also a current study by Cheng Huang et al. that proposes a decentralized, accountable, and privacy-protecting architecture for vehicle sharing services (DAPA)[6]. In DAPA, decentralized and dynamic authentication servers are used to help manage the true identity of customers instead of a single trusted authority, which greatly reduces the risk of single point of failure and establishes decentralized trust for customers.

For intelligent transportation, where vehicles interact with signals, etc., in Chaopeng Tan's research[7], it is established that we formulate traffic state estimation and traffic signal control in a way that can effectively integrate the results of privacy-preserving data aggregation mechanisms.

However, although some progress has been made, most of the technical frameworks are not available on a large scale to achieve real implementation, and automotive communication information security still faces many challenges and issues to be addressed. Therefore, this thesis aims to explore and propose new approaches and solutions for automotive communication information security to address evolving security threats and to improve the security and reliability of vehicle communication systems.

3 Assessment of secure communication between intelligent connected vehicle platforms

3.1 Two-way Identity Authentication Security

The intelligent connected vehicle remote service and management system is proposed to need to achieve two-way identity authentication with the server platform prior to platform login on the client platform, so as to achieve meet the requirements of confidentiality, integrity and availability of the transmitted data[8].

The main traffic difference between one-way identity authentication and two-way identity authentication is the authentication process for certificates in the process of establishing a connection in Figure 1. We can operate on the application in the enterprise platform server, using the tcpdump tool for server traffic capture, such as using the command: tcpdump -i any -p -vv -s 0 -w /xxx/capture.pcap, exporting the capture.pcap package, and using the wireshark tool to analyse it to check whether there is a Certificate message after the Server Hello Done request and before the Client Key Exchange, so as to achieve the purpose of two-way identity authentication.

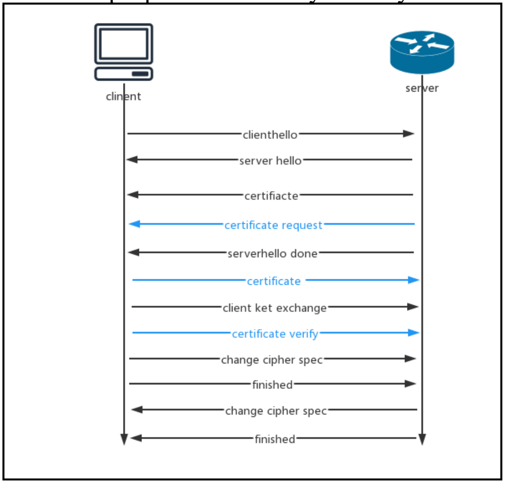
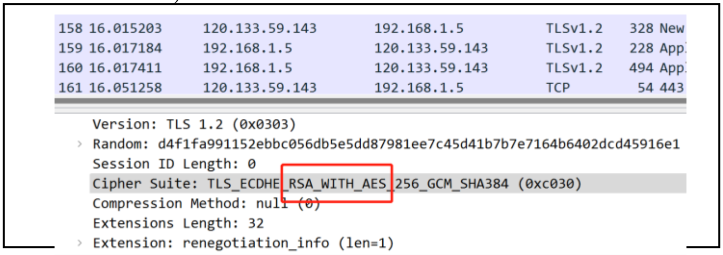


Fig. 1. Two-way authentication traffic characteristics.

3.2 Data Unit Encryption

In the process of data transmission involving the Internet of Vehicles, the key of the encrypted data unit should be different from the key used in the secure communication protocol[9], we can click on the Server Hello data packet to view the cipher suite whose content means: TLS + key exchange negotiation protocol + signature algorithm + WITH + encryption algorithm (key length) (GCM mode) + digest algorithm in Figure 2, we can check whether the type of encryption algorithm in the cipher suite is different from the signature algorithm, where the key used in the secure communication protocol corresponds to the signature algorithm (for authentication) and the key of the encrypted data unit corresponds to the encryption algorithm (for encrypting the content of the transmission).



```
158 16.015203     120.133.59.143      192.168.1.5        TLSv1.2    328 New
159 16.017184     192.168.1.5         120.133.59.143     TLSv1.2    228 App
160 16.017411     192.168.1.5         120.133.59.143     TLSv1.2    494 App
161 16.051258     120.133.59.143      192.168.1.5        TCP         54 443
```

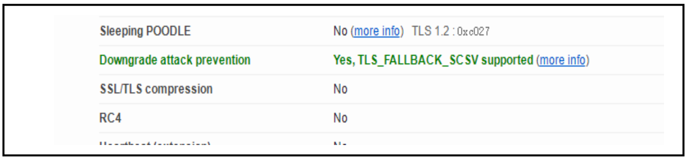
```
    Version: TLS 1.2 (0x0303)
  › Random: d4f1fa991152ebbc056db5e5dd87981ee7c45d41b7b7e7164b6402dcd45916e1
    Session ID Length: 0
    Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)
    Compression Method: null (0)
    Extensions Length: 32
  › Extension: renegotiation_info (len=1)
```

Fig. 2.cipher suite.

3.3 Protocol Version Downgrade Security

An important point in verifying secure communication protocols is whether the protocol used is TLS 1.2 or above and whether downgrading is allowed, for example to TLS 1.1, TLS 1.0 or SSL 3.0, SSL 2.0. If downgrading is supported, there may be a risk of a downgrading attack in which an attacker deliberately causes the system to abandon newer, more secure ways of working and instead use older, less secure ways of working prepared for backwards compatibility, significantly weakening the security of the encrypted communication protocol and enabling an attack that would otherwise not be possible.

Security operators need to ensure that the platform disables both TLS session renegotiation (including server-side secure renegotiation, client-side secure renegotiation, and client-side insecure renegotiation) and TLS compression. Figure 3 shows the results of the ssl protocol detection tool, and we can see that both of these functions are turned off.



Sleeping POODLE	No (more info) TLS 1.2 : 0xc027
Downgrade attack prevention	Yes, TLS_FALLBACK_SCSV supported (more info)
SSL/TLS compression	No
RC4	No

Fig. 3. Protocol version downgrade.

Because of the risk of an Insecure Renegotiation (CVE-2009-3555) insecure renegotiation vulnerability if TLS session renegotiation is turned on, and renegotiation disabling is required for this assessment item.

The TLS session compression case may be affected by a vulnerability of CRIME (CVE-2012-4929), a security risk caused by SSL compression through which private cookies transmitted by the HTTPS protocol can be stolen.

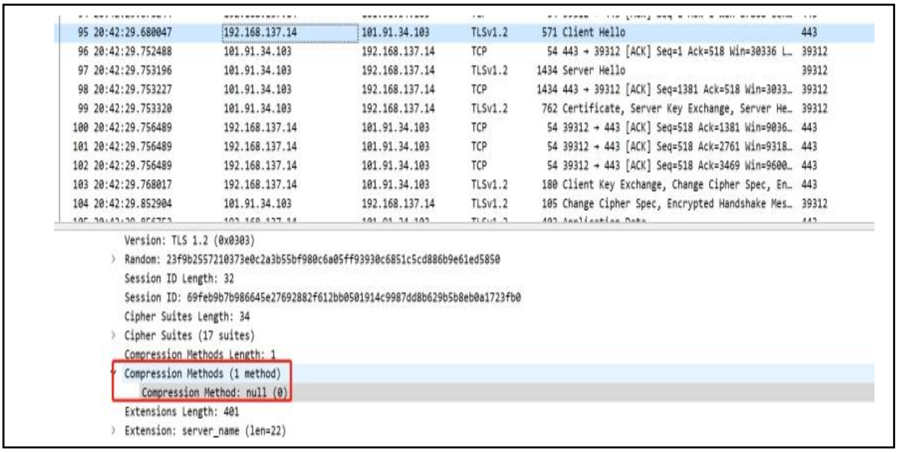
3.4 Certificate Security

Check the encryption algorithm used to determine the level of encryption algorithm, SM2, RSA (length not less than 2048 bits), SM4, AES or the same level and higher encryption algorithms, while the validity period of the certificate should not be greater than 365 days (this validity period refers to the validity period when the certificate is issued, the current CA industry standard validity period is one year, near the expiry of the replacement certificate will be notified, the general situation are in line with) and ensuring key security (The current certificate issuance, renewal and revocation are generally managed by domestic CA authorities, and enterprises may also have their own CA certificate management platform, which can be managed by themselves, and if the certificate is updated, ensure that a secure communication protocol is used when issuing server certificates and CA certificates) .

3.5 Session Renegotiation and TLS Compression

Verify that TLS session renegotiation and TLS compression are disabled for secure communication protocols. TLS session renegotiation (including server-side secure renegotiation, client-side secure renegotiation, client-side insecure renegotiation) and TLS compression should be disabled at the same time. The TLS session renegotiation on case may be at risk from the Insecure Renegotiation (CVE-2009-3555) insecure renegotiation vulnerability.If the protocol supports secure renegotiation, it will generally not be affected by this vulnerability, but renegotiation needs to be disabled for this assessment. TLS session compression may be vulnerable to CRIME (CVE-2012-4929), a security vulnerability caused by SSL compression, through which private cookies transmitted by the HTTPS protocol can be stolen.

Open it with wireshark, find the TLS packet in PROTOCOL and also look for the packet with INFO content clienthello, click on the packet to view the Compression field: the client can submit one or more methods that support compression. The default compression method is null, which means no compression. TLS compression has been disabled as analyzed in Figure 4.



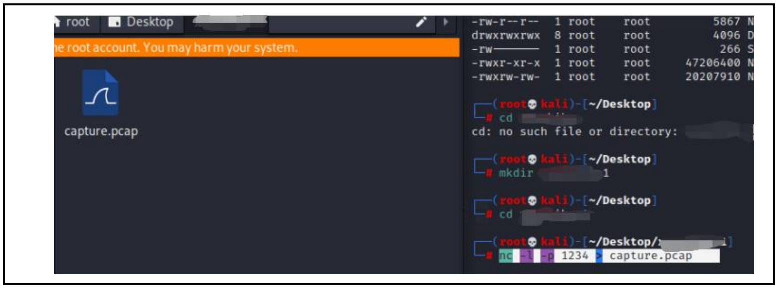
```
 95 20:42:29.680047   192.168.137.14   101.91.34.103    TLSv1.2   571 Client Hello                                    443
 96 20:42:29.752488   101.91.34.103    192.168.137.14   TCP        54 443 → 39312 [ACK] Seq=1 Ack=518 Win=30336 L…   39312
 97 20:42:29.753196   101.91.34.103    192.168.137.14   TLSv1.2  1434 Server Hello                                    39312
 98 20:42:29.753227   101.91.34.103    192.168.137.14   TCP      1434 443 → 39312 [ACK] Seq=1381 Ack=518 Win=3033…  39312
 99 20:42:29.753320   101.91.34.103    192.168.137.14   TLSv1.2   762 Certificate, Server Key Exchange, Server He…   39312
100 20:42:29.756489   192.168.137.14   101.91.34.103    TCP        54 39312 → 443 [ACK] Seq=518 Ack=1381 Win=9036…  443
101 20:42:29.756489   192.168.137.14   101.91.34.103    TCP        54 39312 → 443 [ACK] Seq=518 Ack=2761 Win=9318…  443
102 20:42:29.756489   192.168.137.14   101.91.34.103    TCP        54 39312 → 443 [ACK] Seq=518 Ack=3469 Win=9600…  443
103 20:42:29.768017   192.168.137.14   101.91.34.103    TLSv1.2   180 Client Key Exchange, Change Cipher Spec, En…   443
104 20:42:29.852904   101.91.34.103    192.168.137.14   TLSv1.2   105 Change Cipher Spec, Encrypted Handshake Mes…   39312

    Version: TLS 1.2 (0x0303)
  > Random: 23f9b2557210373e0c2a3b55bf980c6a05ff93930c6851c5cd886b9e61ed5850
    Session ID Length: 32
    Session ID: 69feb9b7b986645e27692882f612bb0501914c9987dd8b629b5b8eb0a1723fb0
    Cipher Suites Length: 34
  > Cipher Suites (17 suites)
    Compression Methods Length: 1
  v Compression Methods (1 method)
        Compression Method: null (0)
    Extensions Length: 401
  > Extension: server_name (len=22)
```

Fig. 4. Protocol compression.

4 Security assessment of vehicle terminals, vehicle infotainment systems and platform communications

4.1 Vehicle Terminal Traffic Capture Method

Firstly, we should access the vehicle terminal system through Android Debug Brige, ssh, telnet, etc. The vehicle terminal system is usually linux or similar unix system, we can use tcpdump and other tools to capture the traffic of the vehicle terminal T-B0X, and then use the netcat tool to export the captured packets to the local, a traffic packet in the format of pcap can be obtained as shown in Figure 5, or use the adb pull command to export and use wireshark to analyse the traffic.



e root account. You may harm your system.

```
-rw-r--r--   1 root    root         5867 N
drwxrwxrwx   8 root    root         4096 D
-rw-------   1 root    root          266 S
-rwxr-xr-x   1 root    root     47206400 N
-rwxrw-rw-   1 root    root     20207910 N

┌──(root㉿kali)-[~/Desktop]
└─# cd [redacted]
cd: no such file or directory: [redacted]

┌──(root㉿kali)-[~/Desktop]
└─# mkdir [redacted]1

┌──(root㉿kali)-[~/Desktop]
└─# cd [redacted]

┌──(root㉿kali)-[~/Desktop/[redacted]]
└─# nc -l -p 1234 > capture.pcap
```

Fig. 5. Export capture data package.

At the same time, we can have our PC program an open hotspot for the vehicle infotainment system to connect to, and use wireshark to listen to the local NIC and get the packets that the vehicle infotainment system is interacting with the cloud. In the next step, we can obtain the interactive IP address of the data packet through a command similar to tshark -r TBOX.pcap -T fields -e ip.src>TBOX.txt.

4.2 Vehicle Cloud Platform Monitoring and Management

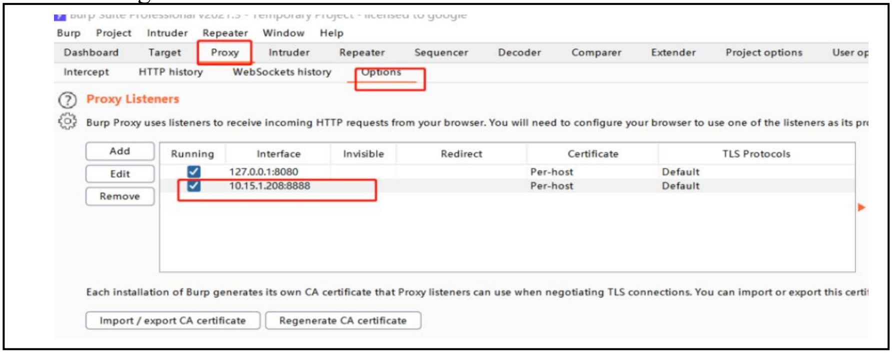
The enterprise platform should monitor and manage the information security of vehicle terminals, and should be able to provide vehicle terminal-related data and traceability means for information security emergency response after information security problems arise in vehicle terminals. Determine whether the enterprise platform has information systems for monitoring the information security status of vehicle terminals, such as IDPS and emergency response centre, as well as using the addition of probes at the vehicle end to report data with the cloud platform, and the cloud platform for unified data management and retention[10].

Login to the corresponding platform or check the relevant functions in the development documents to check if the information security status of the vehicle terminal can be monitored in real time, whether there are corresponding logs, recording comprehensive information, such as: security event records, attacked by xx, attack source IP, whether the attack was successful, the attack was intercepted or blocked IP and other processing. It is necessary to have monitoring means for information security of the vehicle terminal, and at the same time, for the data generated, ensure that the record content is comprehensive and retained for a long time.

4.3 Vehicle Cloud Platform Communication Integrity Assessment

In addition, if the vehicle infotainment system is Android, we can also use the adb shell settings put global http_proxy +IP +PORT command to configure the global proxy for the vehicle infotainment system, and combine it with the burpsuite tool, the data related to the upgrade process and user login authentication process in the vehicle infotainment system was captured for further traffic tampering and replay, where we can configure the proxy in the proxy module, as shown in Figure 6.

The packets from the burpsuite proxy module were modified and replayed in the Repeater module to check if the enterprise platform server on the right responded to the modified packets sent.It is necessary to focus on trying to check if the platform provides integrity protection measures for authentication data, important business data, important audit data, important configuration data and important personal information during transmission for communication with the vehicle terminal.


Burp Suite Professional v2021.3 - Temporary Project - licensed to google
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User op
Intercept HTTP history WebSockets history Options
Add
Edit
Remove
Import / export CA certificate
Regenerate CA certificate

Proxy Listeners

Burp Proxy uses listeners to receive incoming HTTP requests from your browser. You will need to configure your browser to use one of the listeners as its pr

Running	Interface	Invisible	Redirect	Certificate	TLS Protocols
☑	127.0.0.1:8080			Per-host	Default
☑	10.15.1.208:8888			Per-host	Default

Each installation of Burp generates its own CA certificate that Proxy listeners can use when negotiating TLS connections. You can import or export this certi

Fig. 6. Configure local tool proxy.

5 Conclusion

Due to the particularity of the vehicle as a human transport device, vehicle information security is closely related to functional security. A breach of a certain link not only means that user data is stolen and information is leaked, but also likely to directly lead to the control of the vehicle's internal bus network and the counterfeiting of information in the vehicle, thus threatening the safety of the occupants themselves.

The current trend of information security incidents of intelligent connected vehicles is increasing year by year, and there have been many attacks of hackers illegally controlling intelligent connected vehicles through remote, effective threat detection and security protection has become the cornerstone of the rapid development of intelligent connected vehicles. The cloud communication security of the Internet of Vehicles is an important element to ensure the healthy development of the Internet of Vehicles industry, and runs through all aspects of the Internet of Vehicles service applications, and is not only an important force to promote the development of intelligent connected vehicles products, but also an important part of the information security industry[11]. With the development and deepening application of the Internet of Vehicles technology, it faces increasingly complex means of network attacks.

The technical approaches described in this paper are relatively basic in their assessment. In a real environment, where hackers are more flexible in their attack methods, providers of the Internet of Vehicles products should build a more secure network infrastructure and configure it correctly to block attacks from the underlying physical network and virtual platform, and rely on professional security operations and maintenance staff to carry out compliance audits, statistical analysis, alarm analysis and other measures to prevent and mitigate security issues arising in business operations.

References

1. Fadi Al-Turjman, Joel Poncha Lemayian, Intelligence, security, and vehicular sensor networks in internet of things (IoT)-enabled smart-cities: An overview, Computers & Electrical Engineering, Volume 87, 2020, 106776, ISSN 0045-7906.
2. B. Ji et al., "Survey on the Internet of Vehicles: Network Architectures and Applications," in IEEE Communications Standards Magazine, vol. 4, no. 1, pp. 34-41, March 2020.
3. A. Nanda, D. Puthal, J. J. P. C. Rodrigues and S. A. Kozlov, "Internet of Autonomous Vehicles Communications Security: Overview, Issues, and Directions," in IEEE Wireless Communications, vol. 26, no. 4, pp. 60-65, August 2019.
4. H. Zhou, W. Xu, J. Chen and W. Wang, "Evolutionary V2X Technologies Toward the Internet of Vehicles: Challenges and Opportunities," in Proceedings of the IEEE, vol. 108, no. 2, pp. 308-323, Feb. 2020.
5. Ioana, Alexandru, Adrian Korodi, and Ioan Silea. 2022. "Automotive IoT Ethernet-Based Communication Technologies Applied in a V2X Context via a Multi-Protocol Gateway" Sensors 22, no. 17: 6382.
6. C. Huang, R. Lu, J. Ni and X. Shen, "DAPA: A Decentralized, Accountable, and Privacy-Preserving Architecture for Car Sharing Services," in IEEE Transactions on Vehicular Technology, vol. 69, no. 5, pp. 4869-4882, May 2020.

7. C. Tan, K. Yang, Privacy-Preserving Adaptive Traffic Signal Control in a Connected Vehicle Environment. In arXiv e-prints, May 2023.
8. P. Bagga, A. K. Das, M. Wazid, J. J. P. C. Rodrigues and Y. Park, "Authentication Protocols in Internet of Vehicles: Taxonomy, Analysis, and Challenges," in IEEE Access, vol. 8, pp. 54314-54344, 2020.
9. C. Feng, K. Yu, M. Aloqaily, M. Alazab, Z. Lv and S. Mumtaz, "Attribute-Based Encryption With Parallel Outsourced Decryption for Edge Intelligent IoV," in IEEE Transactions on Vehicular Technology, vol. 69, no. 11, pp. 13784-13795, Nov. 2020.
10. Subburaj, S.D.R., Vijay Kumar, V.R., Sivakumar, P., Vinoth Kumar, B., Surendiran, B., Neeraja Lakshmi, A. Fog and Edge Computing for Automotive Applications. In: Challenges and Solutions for Sustainable Smart City Development. EAI/Springer Innovations in Communication and Computing. Springer, Cham. 2021.
11. K. Zrar Ghafoor et al., "Millimeter-Wave Communication for Internet of Vehicles: Status, Challenges, and Perspectives," in IEEE Internet of Things Journal, vol. 7, no. 9, pp. 8525-8546, Sept. 2020.