

Security and Privacy in Vehicular Digital Twin Networks: Challenges and Solutions

Chao He, Tom H. Luan, Rongxing Lu, Zhou Su, and Mianxiong Dong

***Abstract*—With the flourishing and advancement of autonomous vehicles, the vehicular digital twin (VDT) has become an emerging paradigm, consisting of inter-twin communication and intra-twin communication. VDT can effectively address the current shortcomings of the autonomous vehicle and provide enhanced and scalable services to the users. Nevertheless, strict security and privacy concerns arise, as VDT collects a wide range of privacy-sensitive information of the users in real-time and is exposed to an open network environment in both physical and virtual horizons. In this article, we investigate the security and privacy of VDT. We first describe the vehicular digital twin network architecture in detail and then investigate some VDT-related applications. After that, we discuss the security and privacy issues in VDT. Finally, we put forward several potential countermeasures and open research issues for VDT from the perspective of security and privacy. We expect this work will bring more attention to further investigation on security and privacy solutions for vehicular digital twin networks.**

***Index Terms*—Vehicular digital twin, security and privacy, autonomous vehicle**

I. Introduction

With the rapid advance in artificial intelligence and communication technologies, autonomous vehicles with sensing, computing, and communications have received worldwide attention from the industry and academia. As reported that 75% of the world's new cars will be autonomous by 2040 [1]. In the future, autonomous driving will undoubtedly promote the revolution of human transportation and shape the future of cities.

While with significant sensing and processing facility onboard, autonomous vehicles are still suffering from the following problems.

- *Myopic sensing range*: Vehicle-mounted equipment can only sense the sight range, resulting in the perception range of autonomous vehicles being limited. For example, the sensing range of LiDAR is 200 meters, and the sensing range of the millimeter-wave radar is around 250 meters. Meanwhile, the radars are susceptible to bad weather and light conditions, and are difficult to perform robust perception.
- *Limited local processing capacity*: The processing capacity of autonomous vehicles is essential to ensure safety and future development. The current data processing is carried out by the onboard computing platform, which requires extraordinarily high computing capacity to cope with complex traffic conditions, and is therefore very costly. As a result, autonomous vehicles would need to seek for external computing capacity to assist data processing.
- *Barriers in communications*: The autonomous vehicles can obtain nearby information (traffic environment and service recommendation, *etc.*) by the inter-vehicular communications. However, the existing communication network is difficult to ensure the security requirements of safety and reliability, which causes autonomous vehicles to be reluctant to communicate with each other and unable to realize efficiently cooperative driving.

Chao He is with the School of Cyber Engineering, Xidian University; Tom H. Luan and Zhou Su are with the School of Cyber Science and Engineering, Xi'an Jiaotong University; Rongxing Lu is with the Faculty of Computer Science, University of New Brunswick; Mianxiong Dong is with the Department of Sciences and Informatics, Muroran Institute of Technology.

The advancement and flourishing of the digital twin shed light on tackling the above issues of autonomous vehicles. Digital twin, as a virtual representation on the cloud or MEC server, is designed to reflect the state and lifecycle of the physical object accurately. The *vehicular digital twin* is defined as the digital representation of the physical vehicle on the cloud, which synchronizes the vehicle's real-time sensing data via wireless communication. As an example shown in Fig. 1, by introducing the digital twin technique, the autonomous vehicle can upload the perception data and vehicle status information to the digital twin through intra-twin [2] communication. The digital twin can process these massive data relying on cloud computing, thereby alleviating the limitation of insufficient local processing capabilities of autonomous vehicles. In addition, through inter-twin communication [2], data sharing can also be performed between digital twins to help autonomous vehicles obtain more real-time information and broaden the perception range of autonomous vehicles. To summarize, by using the combination of intra-twin and inter-twin communication, the vehicles which are difficult to communicate at the physical layer can be conveniently connected to the digital twin layer for information and AI sharing.

With its two-layer structure, the vehicular digital twin network however suffers from the security and privacy threats from both the physical layer and the digital twin layer. Specifically, for the intra-twin communication to connect the physical layer and digital twin layer, malicious attackers may take replay or message tampering attack to manipulate the perception data (from the vehicle) or decision-making results (from the digital twin), thereby affecting the decision-making and control of the vehicular digital twin, and threatening the passenger's safety. For the inter-twin communication at the digital twin layer, an attacker could launch Sybil attack or DDoS attack, providing false information or paralyzing the

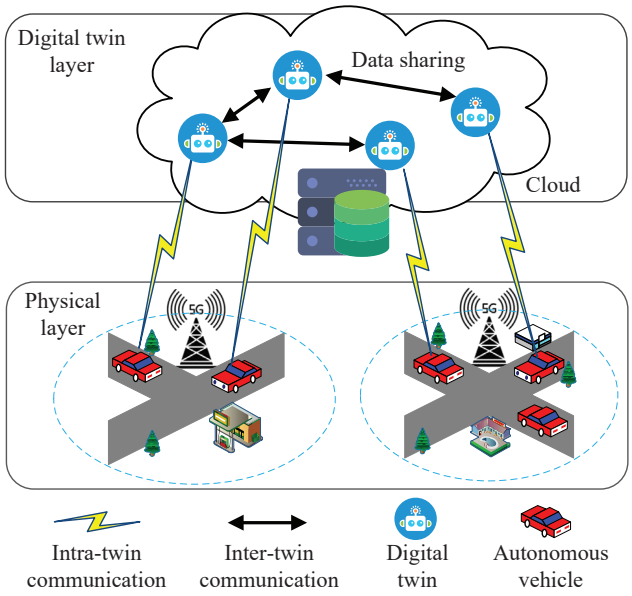


Fig. 1. General architecture of vehicular digital twin network. There are two kinds of communication, inter-twin communication and intra-twin communication.

services of legitimate users to reduce the efficacy of data collected by twins. In addition, the data perceived by the autonomous vehicle uploaded to the digital twin contains sensitive private information, which may be used to infer the user's privacy (location, hobbies, *etc.*). If the security and privacy issues of VDT cannot be well addressed, even with significant convenience brought to the future life, users would not accept it.

The emerging trends motivate our research on the security and privacy issues of VDT. In this article, we have conducted a detailed study of the challenges and attacks faced by vehicular digital twin networks. The structure of this article is as follows. We first introduce the architecture of the vehicular digital twin network. We then investigate the literature and applications related to VDT. After that, we discuss the challenges and security issues of vehicular digital twin network. Finally, we put forward several potential countermeasures and open research issues for VDT from the perspective of security and privacy.

II. Architecture of Vehicular Digital Twin Network

This section describes the vehicular digital twin network architecture from the perspectives of *intra-twin communication* and *inter-twin communication*.

A. Intra-twin communication

The intra-twin communication refers to the communication pipe between the vehicle and its corresponding digital twin at the cloud. Using intra-twin communication, the vehicle uploads the real-time sensing data to its private digital twin through wireless communications (WiFi, 5G cellular networks, *etc.*). In the meantime, the digital twin at the cloud can transmit the information it collects on the cloud to the vehicle using the intra-twin communication.

The intra-twin communication therefore has following features.

- *Consistent communication*: To ensure consistency of information, the digital twin needs to maintain consistent communication with the autonomous vehicle. In this way, the vehicle's sensed data and state information can be continuously uploaded to its private digital twin along the driving trip.
- *Real-time synchronization*: Real-time synchronization between digital twins and autonomous vehicles is required to ensure accurate, secure, compliant data and smooth user experiences.
- *Private and engaged connection*: As a digital collaborator of autonomous vehicles, the goal of digital twins is to help physical autonomous vehicles acquire virtual resources in the cloud. Therefore, the digital twin is private to an autonomous vehicle, and the connection between the digital twin and autonomous vehicle should be also private and engaged for private twin synchronization.

B. Inter-twin communication

The inter-twin communication refers to digital twins on the cloud communicating with each other. Using inter-twin communication, the digital twins on the cloud can share the information, AI learning, and feedback to the vehicle on the ground. As a result, the autonomous vehicle can indirectly communicate with other vehicles outside of their communication range through the relay of inter-twin communication, thereby helping autonomous vehicles obtain global traffic information.

The inter-twin communication is featured from following aspects:

- *Distributed peer-to-peer connection*: In inter-twin communication, each digital twin is an independent individual, and many digital twins form a distributed digital twin network. Each participant (digital twin) in this network will share resources (services or content), so each digital twin is both a resource provider and a resource acquirer.
- *Private data asset*: The digital twin is private to its autonomous vehicle and holds a large amount of data from the autonomous vehicle. These data have a certain value and contain some users' private information, which belongs to the digital twin's private data assets.
- *Multi-agents communication*: As an intelligent, autonomous virtual entity, the digital twin can be treated as an agent. Therefore, we can regard the communication between digital twins as the multi-agents communication.

III. Vehicular Digital Twin Related Applications

Combining the Internet of Things, 5G, big data, cloud computing, virtual reality, and other technologies, digital twins will be an essential part of digital transformation. Their application space is also expanding. As shown in Table I, we provide some application examples related to VDT. In this section, we

TABLE I
SOME APPLICATION EXAMPLES RELATED TO VDT.

Application examples	Brief descriptions
Data processing	Relying on the computing power of the cloud to process and analyze the data uploaded by autonomous driving vehicles.
Simulation	Simulating driving scenarios and driving conditions of autonomous vehicles, and provide monitoring and prediction services.
Route planning	The digital twins intelligently plan routes for autonomous vehicles according to the obtained information of weather and traffic conditions.
Smart parking	By sharing information between digital twins, free parking Spaces in the city can be obtained.
Vehicle diagnosis	By obtaining the status information of the autonomous vehicle in real time, the vehicle can be diagnosed.
Service recommendation	Some personalized services can be provided to users, recommending food or entertainment according to their preferences.

have investigated some literature related to the application of digital twins in vehicles, which will mainly be elaborated on from three aspects: *help learning and data processing*, *trip simulation*, and *route planning*.

A. Help learning and data processing

Digital twins can transform big data into valuable information through data processing and learning algorithms to provide intelligent services for vehicles, such as monitoring vehicle status, network optimization, and congestion prediction. For example, Chen *et al.* [3] study a UAV-assisted mobile edge computing (MEC) system, which can provide complementary computing resources for the ground mobile edge computing system. The authors establish a digital twin of the MEC system to realize offline training of the proposed proactive deep reinforcement learning (DRL) scheme based on long short-term memory (LSTM) and DRL techniques. For the problems of traffic congestion and chaos. Kumar *et al.* [4] use LSTM-based RNNs technology to build a novel digital twin-centric approach for driver intention prediction and traffic congestion avoidance. Chen *et al.* [5] construct a digital twin model, using decision tree and k-nearest neighbors learning methods to learn the redefined driving environment and driver behavior, so that the digital twin can accurately predict driver's behavior and effectively prevent collisions.

B. Trip simulation

The vehicular digital twin can also perform vehicle condition monitoring and driving assistance through simulation. Xiong *et al.* [6] proposes a DT-assisted method for AV simulation in a car-following scenario. Through real-time simulation, the digital twin can dynamically regulate the physical entities. At the same time, the simulation verification is displayed in the DT scenario to ensure the security of the simulation. Wang *et al.* [7] build a digital twin for advanced driver assistance systems for connected vehicles. By uploading the sensor data acquired in the physical system to the digital twin in the cloud for processing, it provides users with the best driving speed. Venkatesan *et al.* [8] use the digital twin to simulate the performance of the electric vehicle, which can effectively monitor and predict the health of the electric vehicle.

C. Route planning

The most important application of VDT is path planning and traffic congestion management. The digital twin can provide users with personalized route planning services based on information (*e.g.*, destinations, user preferences, and road traffic conditions) while also effectively avoiding traffic congestion. For example, Kumar *et al.* [9] use digital twin, machine learning, edge computing, and other technologies in the intelligent transportation system to analyze the acquired data and create a virtual vehicle model in the digital twin to restore the real traffic scene. Using an artificial intelligence algorithm fed to the digital twin can predict the driver's intention and give the best route decision for drivers. In addition, Jiang *et al.* [9] propose a sustainable urban road planning approach named DT-MCDM-GIS framework based on DT, MCDM, and GIS to assist in urban road planning. The proposed framework alleviates traffic congestion and provides a comfortable route for drivers considering various factors, such as building demolition, land use, traffic congestion, driver habits, air quality, and noise.

IV. SECURITY AND PRIVACY ISSUES IN VDT

Due to the features of intra-twin and inter-twin communications, VDT faces new security requirements and challenges. It not only is exposed to the security threats in the traditional Internet of Vehicles, but also faces new threats specific to the vehicular digital twin network architecture. In this section, we first present some critical challenges faced by VDT. Then, we discuss the VDT security from *intra-twin security* and *inter-twin security*.

Privacy: Privacy is one of the main challenges faced by VDT. In VDT, the vehicle collects information about the traffic environment, vehicle status, and user behavior and habits through various sensors. It transmits these data to the digital twin on the cloud or MEC servers through the 5G cellular network. After receiving the data, the digital twin preprocesses the data, such as filtering, classification, and encoding, and then calculates and analyzes the data through big data and artificial intelligence. The digital twin will also share data to obtain more information. In this series of processes, the user identity and location privacy are vulnerable to being compromised. For example, the vehicle's location information can provide powerful support for vehicle navigation. However, suppose the malicious attacker combines the vehicle's location information with other information. In that case, the attacker can infer and analyze the driver or passenger's interests, hobbies, and living habits. Therefore, while using user information, information sharing and privacy-preserving must be balanced in VDT.

Reliability: In VDT, data reliability is essential to the vehicle's driving safety. We will elaborate on the following three aspects: *sensed data*, *shared data*, and *decision result*. For the sensed data, two reasons may threaten the data reliability. One is that the vehicle collects incorrect data. The other is that it is tampered with by the malicious attacker during transmission. Therefore, the data received by the digital twin will be unreliable or invalid. It will affect the computing result of the digital twin once the incorrect decision feedback to the vehicle leads to major traffic accidents. Besides, the digital twin will also share information to expand their horizons, but the information may be incorrect, which will affect the decision-making results of other digital twins. For example, the digital twin is compromised by an attacker and deliberately sends unreliable information.

Time-sensitive: Digital twins need to make decision quickly in real-time situations, such as accident avoidance and rapid rescue. Due to the time-varying nature of traffic flow and the timeliness of traffic management, digital twin needs to receive timely, reliable, and accurate traffic information. Its decision-making results also need to be quickly transmitted to the vehicle. However, to satisfy the security requirements of VDT, the strict and complex verification process of the message is required, which will cause a response delay, and thus cannot satisfy the time-sensitive requirements of VDT.

Information synchronization: Data and information need to be continuously synchronized between the digital twin and its physical entity for VDT to ensure information consistency. However, the time and frequency of synchronization will impact the quality of service of VDT. Therefore, when designing the synchronization mechanism of VDT, it is necessary to consider some particular circumstances and provide a reliable synchronization scheme to ensure the low delay and high reliability of the safety message transmission between the vehicle and the digital twin.

In this paper, we divide VDT security issues into *intra-twin security* and *inter-twin security*, and some attacks may exist in both inter-twin communication and intra-twin communication. Fig. 2 and Fig. 3 briefly describe the threats of the inter-twin communication and intra-twin communication. The following two sections discuss the various security and privacy threats of VDT from intra-twin security and inter-twin security.

A. Intra-twin Security

Intra-twin is vulnerable to attacks during communication, which affects the safe operation of VDT. The adversary can use message tampering, eavesdropping, or replay attacks to influence the data flow maliciously, such as sensing data or command messages. These will affect the decision, vehicle control, and user privacy.

In a *replay attack*, the adversary receives and stores information about previous traffic or road conditions, even the command information sent by the digital twin to the vehicle, and attempts to retransmit them soon after to deceive the digital twin and the autonomous vehicle to achieve the adversary's attack intention. The replayed command information may be the control command of the digital twin, which may cause the autonomous vehicle to lose control. For example, the adversary sniffed an acceleration command that the digital twin sends to the autonomous vehicle at a critical moment, and the adversary intercepted and saved this command information. When the road is congested, the adversary resends this message, which will cause a major traffic accident.

In a *message tampering attack*, the adversary monitors the communication data flow between the autonomous vehicle and digital twin. After receiving sensor information or command information, the attacker modifies and resends it. For example, the adversary can make the information invalid by tampering with the perception information, which will significantly impact the decision-making results of digital twin.

In an *eavesdropping attack*, the attacker collects as much information as possible by monitoring network traffic and infers information about the vehicle and user through analysis. It is a passive attack that will compromise the users privacy.

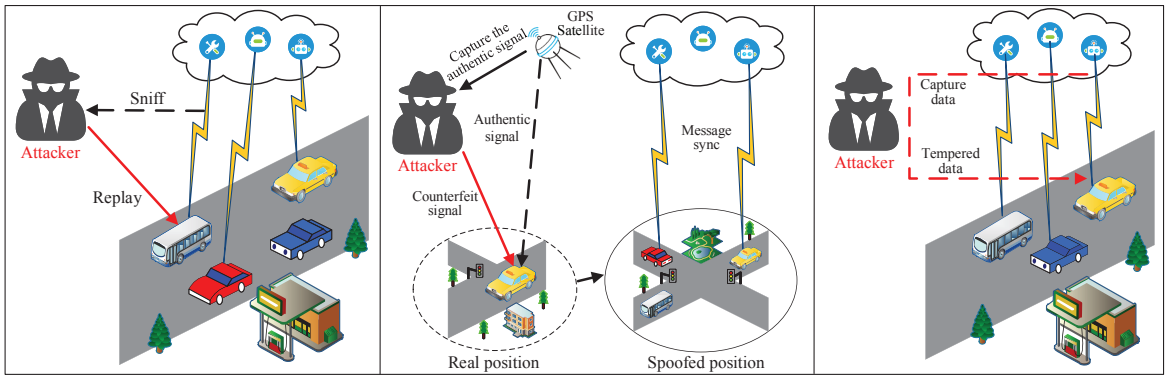
B. Inter-twin Security

The digital twin can obtain more information through mutual information sharing. Hence the vehicle can get the traffic conditions beyond the field of view in advance and improve the service quality. However, information sharing between digital twins may compromise the user's privacy. Besides, since a digital twin is a virtual entity that resides on the cloud, its security largely depends on cloud security. Therefore, it is vulnerable to attacks such as Sybil attack and DDoS attack, resulting in service paralysis.

In a *Sybil attack*, the attacker forges the identity of digital twin to disrupt reliable system operation. There are two main types of such attacks. One generates multiple fake identities and sends multiple false messages to disrupt or deceive other digital twins. And the other is to pretend to be a legitimate digital twin and provide false information. This attack can provide incorrect information about its location by taking advantage of the changing topology and mobility of the vehicle.

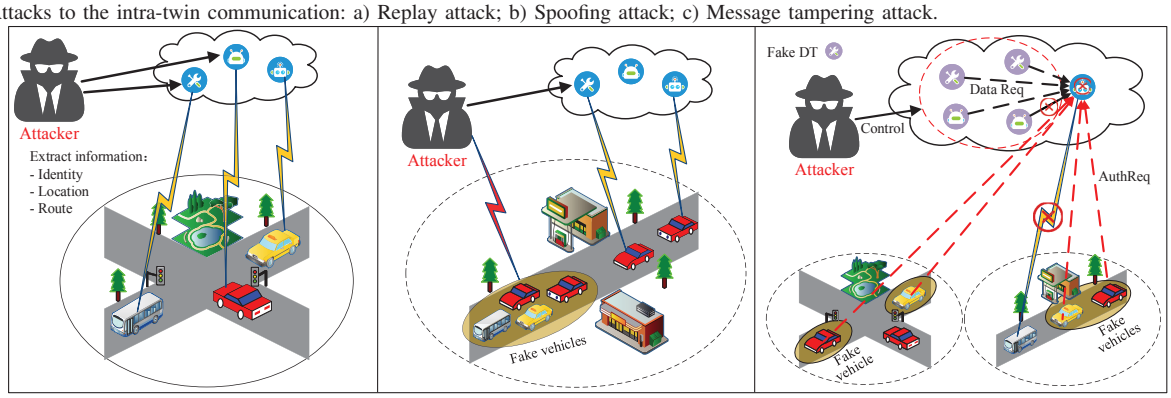
In a *privacy leakage attack*, information sharing between digital twins may compromise user privacy. For example, the adversary can ask the digital twin about the traffic situation at the current location. The adversary can infer the target vehicle's location if the digital twin can answer correctly. When the adversary combines the location information with other information, can further infer the driver's or passenger's hobbies or behaviour habits.

In a *distributed denial of service (DDoS) attack*, the adversary consumes system resources such as bandwidth and memory, causing the system to be paralyzed and unable to provide services to legitimate users, thereby achieving the purpose of the attack. There are two main types of DDoS attacks in VDT. The adversary keeps requesting a connection to the identical digital twin by controlling multiple vehicles. Furthermore, the other is that the adversary continuously requests information from the identical digital twin by controlling the digital twin on the cloud, thereby launching a DDoS attack.



(a) Reply attack (b) Spoofing attack (c) Message tampering attack

Fig. 2. Attacks to the intra-twin communication: a) Replay attack; b) Spoofing attack; c) Message tampering attack.



(a) Privacy leakage (b) Sybil attack (c) DDoS attack

Fig. 3. Attacks to the inter-twin communication: a) Privacy leakage attack; b) Sybil attack; c) DDoS attack.

V. Potential Countermeasures and Open Research Issues for VDT

To ensure the security and privacy of VDT, balanced and pragmatic countermeasures are desired. In this section, we present several potential countermeasures from the aspects of identity authentication, privacy protection and blockchain, but not limited to these. We also discuss several open research issues for VDT.

A. Potential Countermeasures

*1) **Authentication**:* Reliable identity authentication is the first step in establishing a secure VDT. Herein, we divide the authentication into *inter-twin authentication* and *intra-twin authentication* according to the architecture of the vehicular digital twin networks. Specifically, intra-twin authentication means that the vehicle and the digital twin authenticate, and inter-twin authentication means that the authentication between the digital twins.

- **Authentication in intra-twin communication.** As mentioned above, since the communication between the vehicle and the digital twin relies on the public wireless network (5G, *etc.*), it is vulnerable to various attacks. If there is no mechanism to ensure secure communication, the information transmitted between the vehicle and the digital twin will be no security guarantees. In [10], Xu *et al.* propose an authentication scheme based on bilinear mapping and secret handshake protocol, which realized the mutual authentication between the autonomous vehicle and digital twin. Considering the migration of Cybertwin caused by vehicle mobility, Li *et al.* [11] propose a handover authentication scheme to create a new Cybertwin between vehicle and edge server based on proxy ring signature technique. However, the autonomous vehicle and the digital twin are frequently required to communicate with each other, which will generate authentication overhead. But for some time-sensitive services, this will reduce the user experience. Therefore, it is necessary to propose a lightweight cryptographic authentication scheme to meet the security requirements and characteristics of the vehicular digital twin. To tackle the above challenge, continuous authentication is promising to realize lightweight and secure authentication between autonomous vehicles. However, the existing continuous authentication schemes are mainly divided into two categories [12], *user-to-device models* and *device-to-device models*, which are not suitable for VDT scenarios. Therefore, it is significant to design a continuous authentication scheme for VDT.
- **Authentication in inter-twin communication.** We assume that the digital twins reside on the cloud or MEC servers and broaden the vision of autonomous vehicles by information sharing. However, because the cloud or MEC servers is vulnerable to attack, digital twins cannot ensure security and reliability. For example, a compromised digital twin may steal the data of the target digital twin, which will bring severe threats to the security and privacy of the vehicle owner. Therefore, before communicating

between digital twins, it is necessary to perform identity authentication. However, the digital twin network has distributed, virtual, and vast nodes. How to achieve mutual authentication between digital twins is a challenge.

*2) **Privacy-preserving**:* Due to the cloud services being *honest-but-curious*, the privacy issues become much more critical in VDT. There are mainly two aspects: *data processing and analysis* and *information sharing*. As shown in Table II, we provide some possible privacy-preserving mechanism for the two aspects, respectively.

- **Data processing and analysis:** The honest-but-curious cloud service may secretly collect the vehicle's sensitive information when the raw data is processed and analysed by the digital twin. We present some privacy-preserving mechanisms to protect the privacy of data processing and analysis in Table II. Among them, random noise is added to the raw data to cover private information for the perturbation-based and differential privacy methods. However, those methods require a balance between data privacy and availability. The trusted computing is a solution that provides privacy computing from the perspective of hardware and architecture, which provides an isolated runtime environment to protect program code and data from being stolen or tampered with by the operating system or other applications. In addition, through homomorphic encryption, the digital twin can send data to cloud service providers for arbitrary processing without worrying about the original information of the data being leaked.
- **Information sharing:** When data is shared between digital twins, the data provider and the requester may expose privacy. To protect privacy in data sharing, we also present some privacy-preserving mechanisms in Table II. Specifically, data anonymization removes personally identifiable information from data to maintain an individual's privacy. Federated learning can enable digital twins to learn a shared model without revealing their raw data collaboratively. However, traditional federated learning requires a centralized controller to maintain a global model over the network, which aggregates information from all the nodes. Due to the peer-to-peer feature of the digital twin network, it is not easy to find a trusted server to maintain the global model. Fortunately, the literature [13] proposes a distributed federated learning system structure that uses graphs to build a peer-to-peer communication pattern between all participating parties. For secure multi-party computing (SMPC) [14], it uses cryptographic tools to enable digital twins to use their data for collaborative computing while ensuring that their data is not leaked to other digital twins. Some of the main techniques are garbled circuit (GC), secret sharing, oblivious transfer (OT) and zero-knowledge proofs (ZKP).

*3) **Blockchain Technology**:* The trust and reliability of data is the key to building VDT, and blockchain is a promising solution with great benefits to enhance the security and reliable data storage and sharing for the digital twin network [15]. Blockchain is a distributed and publicly database that is shared among the nodes, which is characterized by unforgeability, decentralization, transparency, and traceability. It uses cryptography to ensure data security and consensus algorithms to ensure data consistency. As shown in Fig. 4, we envison a blockchain-based secure data storage and sharing model for vehicular digital twin network. In this model, the base stations (BSs) are equipped with MEC server, and have certain computing and storage capabilities. The blockchain is maintained by the BSs, in which the transactions between digital twins are truthfully recorded on the blockchain ledger, facilitate the cooperation between digital twins in data sharing. Through blockchain and smart contract, the secure storage and sharing of data assets in VDT can be achieved. Among them, blockchain can ensure the traceability of data, and smart contract can ensure the security of data sharing through automatic execution. In addition, the trust relationship and data trading between digital twins no longer need to be established by a central organization but is achieved through cryptography, collaboration, and smart contracts.

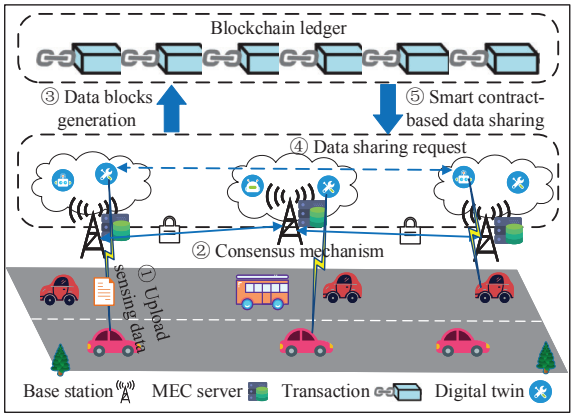


Fig. 4. An illustration of secure data storage and sharing using blockchain in vehicular digital twin network. The workflow is as follows: 1) The vehicle uploads the sensing data to its private digital twin on the MEC server via BS. 2-3) With the help of consensus mechanism, the data and sharing records are verified by the BSs, then added to the blockchain ledger. 4-5) Digital twin data requestor communicates with the data provider for data sharing by the smart contract.

B. Open Research Issues

Apart from the above-discussed security and privacy issues, there are several other security issues that we must tackle for vehicular digital twins.

Knowledge based security mechanism. A key feature of VDT is the consistent intra-twin communication along the driving path of vehicles. As a result, the shared information and knowledge between vehicles and their digital twins can be explored to resist potential attacks. Lifelong machine learning is appropriate to apply, which continuously learns and accumulates the knowledge learned in the past to help the problem-solving in the future. In VDT, utilizing lifelong learning can make the digital twin more knowledgeable and better in learning ability, which will provide flexible solutions to various problems that the vehicle may encounter during driving. However, the correctness and applicability of lifelong learning knowledge may change due to factors such as the

TABLE II
PRIVACY-PRESERVING MECHANISM FOR VEHICULAR DIGITAL TWIN.

	Technique	Advantage	Disadvantage
Data processing and analysis	Perturbation	Different attributes are preserved separately. Do not need information about other records.	Very little privacy preservation. Reconstruction of original data is not possible.
	Differential Privacy	High computing and communication efficiency. Flexible privacy needs. Wide range of applications.	Sacrificing computational precision. Scalability level is still a question.
	Trust computing	High level of security and commonality.	May exist some unknown vulnerability. Security highly depends on hardware manufacturers.
	Homomorphic Encryption	High level of security. Non-interactive.	High computational and communication overhead. Low computation efficiency. Limited computing capacity.
Data sharing	Anonymization	Individual's privacy is maintained.	Linking attack. Heavy loss of information.
	Federated learnig	Protect user privacy. Solve the problem of isolated data island.	High communication overhead. Heterogeneity of system and data.
	SMPC	High level of security. Transformed data are exact and protected.	Complicated(more than two parties are involved). Expensive.

driver's preference and vehicle mobility. Therefore, maintaining the effectiveness of lifelong learning in the ever-changing road environment is a challenge.

Data effectiveness. VDT is vulnerable to false data injection during the data sensing and sharing stages. In the data sensing stage, digital signature technology cannot prevent data from being tampered with before collection. Therefore, the adversary can inject false data through sensors. Besides, the malicious digital twin can inject invalid data into other digital twins in the data sharing stage. For this reason, detecting false data quickly and correctly is a challenging issue.

Secured data trading. A vital advantage of the digital twin is the data-sharing among digital twins using inter-twin communication. In this manner, vehicles can obtain real-time information from inter-twin communications to assist its driving. However, data privacy should be well protected. However, paying too much attention to users' privacy will reduce the service efficiency of VDT, which brings a bad user experience. Therefore, maintaining a balance between protecting user privacy and ensuring service efficiency is challenging. Although vehicles are distributed in the city, their digital twins are connected as a data trading market. In this scenario, the game theory and blockchain based data trading scheme is effective in punishing the malicious digital twins.

VI. CONCLUSION

The vehicular digital twin is a promising paradigm in future transportation. In this article, we first introduced the architecture of vehicular digital twin networks. Then, we investigated the literature related to the vehicular digital twin. In addition, we analyzed the vehicular digital twin's security threats from intra-twin and inter-twin communication, respectively. Finally, we presented some potential countermeasures from identity authentication, privacy-preserving and blockchain, and several open research issues are also discussed.

We hope this article sheds more light on the security and privacy of vehicular digital twins. In the future, we will make more research efforts along this emerging line.

REFERENCES

[1] Z. Su, Y. Hui, and T. H. Luan, "Distributed Task Allocation to Enable Collaborative Autonomous Driving With Network Softwarization," *IEEE J. Sel. Areas Commun.*, vol. 30, no. 10, 2018, pp. 2175-2189.

[2] T. H. Luan *et al.*, "The Paradigm of Digital Twin Communications," 2021, pp. 1-7, [Online]. Available: http://arxiv.org/abs/2105.07182.

[3] X. Chen *et al.*, "Resource Awareness in Unmanned Aerial Vehicle-Assisted Mobile-Edge Computing Systems," *IEEE Veh. Technol. Conf.*, 2020, pp. 1-6.

[4] S. A. P. Kumar *et al.*, "A novel digital twin-centric approach for driver intention prediction and traffic congestion avoidance," *J. Reliab. Intell. Environ.*, vol. 4, 2018, pp. 199-209.

[5] X. Chen *et al.*, "Digital behavioral twins for safe connected cars," *Proc. 21st ACM/IEEE Int. Conf. Model Driven Eng. Lang. Syst. Model*, 2018, pp. 144-154.

[6] H. Xiong *et al.*, "Design and Implementation of Digital Twin-Assisted Simulation Method for Autonomous Vehicle in Car-Following Scenario," *J. Sens.*, 2022, pp. 1-12.

[7] Z. Wang *et al.*, "A Digital Twin Paradigm: Vehicle-to-Cloud Based Advanced Driver Assistance Systems," *IEEE Veh. Technol. Conf.*, 2020, pp. 0-5.

[8] S. Venkatesan *et al.*, "Health monitoring and prognosis of electric vehicle motor using intelligent-digital twin," *IET Electr. Power Appl.*, vol. 13, no. 9, 2019, pp. 1328-1335.

[9] F. Jiang *et al.*, "Digital twin enabled sustainable urban road planning," *Sustain. Cities Soc.*, vol. 78, 2022, pp. 1-20.

[10] J. Xu, C. He, and T. H. Luan, "Efficient Authentication for Vehicular Digital Twin Communications," *IEEE Veh. Technol. Conf.*, 2021, pp. 1-5.

[11] G. Li *et al.*, "SecCDV: A Security Reference Architecture for Cybertwin-driven 6G V2X," *IEEE Trans. Veh. Technol.*, vol. 71, no. 5, 2021, pp. 4535-4550.

[12] Y. H. Chuang *et al.*, "A lightweight continuous authentication protocol for the Internet of Things," *Sensors*, 2018, pp. 1-26.

[13] A. Lalitha *et al.*, "Peer-to-peer Federated Learning on Graphs," 2019, pp. 1-9, [Online]. Available: http://arxiv.org/abs/1901.11173.

[14] F. Horandner and B. Prunster, "Armored twins: Flexible privacy protection for digital twins through conditional proxy re-encryption and multi-party computation," *Proc. 18th Int. Conf. Secur. Cryptogr. SECRYPT 2021.*, 2021, pp. 149-160.

[15] Dai. M *et al.*, "Digital Twin Envisioned Secure Air-Ground Integrated Networks: A Blockchain-Based Approach," *IEEE Internet Things Mag.*, vo. 5, no. 1, 2022, pp. 96-103.

Chao He received his B.E. degree from Zhejiang Gongshang University, Hangzhou, China, in 2018. He is currently pursing his Ph.D. degree with the School of Cyber Engineering, Xidian University, Xi'an, China. His research interests include vehicular digital twin, multi-agent system and internet of vehicles security.

Tom H. Luan received his B.Eng. degree from Xi'an Jiao Tong University, China, the M.Phil. degree from Hong Kong University of Science and Technology, and the Ph.D. degree from the University of Waterloo, Ontario, Canada. He is a professor at the School of Cyber Science and Engineering of Xi'an Jiaotong University, Xi'an, China. His research mainly focuses on content distribution and media streaming in vehicular ad hoc networks and peer-to-peer networking, as well as the protocol design and performance evaluation of wireless cloud computing and edge computing.

Rongxing Lu received the Ph.D. degree from the Department of Electrical and Computer Engineering, University of Waterloo, Canada, in 2012. He is currently a Mastercard IoT Research Chair, a University Research Scholar, and an Associate Professor with the Faculty of Computer Science (FCS), University of New Brunswick (UNB), Canada. He has published extensively in his areas of expertise. His research interests include applied cryptography, privacy enhancing technologies, and IoT-big data security, and privacy. He was a recipient of nine best (student) paper awards from some reputable journals and conferences. He was awarded the most prestigious "Governor General's Gold Medal," when he received his Ph.D. degree. He has won the Eighth IEEE Communications Society (ComSoc) Asia Pacific (AP) Outstanding Young Researcher Award in 2013. He also serves as the Chair of IEEE Communications and Information Security Technical Committee (ComSoc CISTC), and the Founding Co-Chair of IEEE TEMS Blockchain and Distributed Ledgers Technologies Technical Committee (BDLT-TC). He is the Winner of 2016-2017 Excellence in Teaching Award, FCS, UNB.

Zhou Su is an associate editor of IEEE Internet of Things Journal, IEEE Open Journal of the Computer Society, IET Communications, and so on. His research interests include wireless networking, mobile computing, Internet of Things and network security. He served as the track/symosuim chair for several international conferences including IEEE VTC, IEEE/CIC ICCC, WCSP, and so on. He received the best paper award of IEEE ICC2020, IEEE BigdataSE2019, IEEE CyberSciTech2017, and so on.

Mianxiong Dong received his B.S., M.S., and Ph.D. in computer science and engineering from the University of Aizu, Japan. He is the vice president and youngest ever professor of Muroran Institute of Technology. He is a Foreign Fellow of EAJ. He is the recipient of NISTEP Researcher 2018 (one of only 11 people in Japan) in recognition of significant contributions in science and technology, Hokkaido Science and Technology Incentive Award 2019, and the Young Scientists' Award 2021 of MEXT. He was a Clarivate Analytics 2019 Highly Cited Researcher (Web of Science).