Journal of Harbin Engineering University
ISSN: 1006-7043

Vol 45 No. 7
July 2024

Security and Privacy Issues and Solutions in Vehicular Digital Twin Networks

Dheeraj Tiger [1], Anshu Malhotra[1] and Vinod Kumar[2,*]

[1]Department of Mathematics, School of Applied Science, North cap University, Gurugram-122017, India

[2]Department of Mathematics, Shyam Lal College, University of Delhi, New Delhi 110032, India

*: Corresponding author

Abstract

The emergence of the vehicular digital twin (VDT) consists of both intra and inter-twin communication is a result of the growth and development of autonomous cars. In addition to offering consumers improved and scalable services, VDT can successfully address the present drawbacks of autonomous vehicles. However, as VDT is exposed to an open network environment on both physical and virtual horizons and gathers a large range of user privacy-sensitive data in real-time, strict security and privacy problems emerge. We look into the privacy and security of VDT in this article. We first go over the specifics of the vehicular digital twin network architecture before looking into a few applications pertaining to VDT. Next, we talk about VDT's privacy and security concerns. Lastly, from a security and privacy standpoint, we presented a number of viable countermeasures and outstanding research questions for VDT. We anticipate that future research on privacy and security solutions for vehicle digital twin networks will receive attention as a result of our work.

Keywords: Vehicular digital twin, Security, Privacy and Autonomous vehicle

1. Introduction

Lorem In order to address the aforementioned problems with autonomous vehicles, the digital twin's development and thriving provide insight. Accurately reflecting the condition and life-cycle of the actual thing, the digital twin is a virtual representation on the cloud or MEC server. Via wireless communication, the car's real-time sensor data is synchro- nized with the digital version of the actual vehicle on the cloud, known as the vehicular digital twin. The autonomous vehicle can upload perceptual data and vehicle status information to the digital twin through intra-twin communication, as demonstrated in Fig. 1 as an example of the digital twin approach in action. With the use of cloud computing, the digital twin can handle this enormous amount of data, removing the obstacle caused by the autonomous vehicles' limited local processing power. Furthermore, data exchange between digital twins can be accomplished through inter- twin communication, which enables autonomous cars to increase their perception range and receive more real-time information. In summary, vehicle communication that is challenging at the physical layer may be easily bridged to the digital twin layer for information and artificial intelligence sharing through the use of intra-twin and inter-twin communication [1]. Nonetheless, the vehicular digital twin network faces security and privacy risks from both the physical layer and the digital twin layer due to its two-layer architecture. In particular, malicious attackers may use replay or message tampering attacks to manipulate perception data from the vehicle or decision-making results from the digital twin in order to establish an intra-twin communication link between the physical layer and the digital twin layer. This could compromise the safety of the passengers by influencing the vehicular digital twin's control and decision-making. In order to decrease the effectiveness of data acquired by twins, an attacker may use a DDoS or Sybil assault to disrupt genuine users' services or provide fake information for inter-twin communication at the digital twin layer. Further- more, the location, interests, and other private details of the user may be inferred from the data that the autonomous car sensed and transferred to the digital twin. Users would not accept VDT if security and privacy concerns were not adequately handled, even if it meant a huge improvement in future life. Our study on VDT security and privacy issues is driven by these new developments. The difficulties and threats that vehicular digital twin networks must contend with are thoroughly examined in this essay. This essay follows the following format. The vehicular digital twin net- work's architecture is first presented. After that, we look into VDT-related literature and apps. We next go through the difficulties and security concerns with the

vehicle digital twin network. Lastly, we raise a number of pertinent research questions and prospective countermeasures for VDT from a security and privacy standpoint [2].

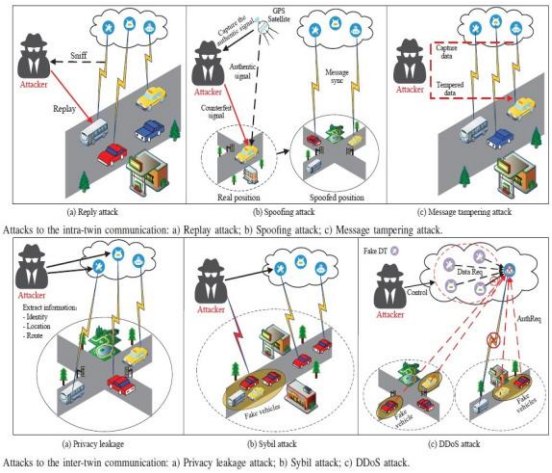

Fig. 1: Threats of the inter-twin communication and intra-twin communication [10]

2. The architecture of digital twin networks for vehicles k

Within-twin and inter-twin communication viewpoints are used to describe the architecture of the vehicular digital twin network in this section.

2.1 Intra-twin communication

The communication channel that exists between a vehicle and its cloud-based digital twin is known as intra-twin communication. Through wireless connections (WiFi, 5G cellular, etc.), the vehicle transfers the real-time sensor data to its private digital twin using intra-twin communication. Until then, the intra-twin communication between the digital twin at the cloud and the vehicle allows the latter to get the data it gathers there. Thus, the intra-twin communication has the characteristics listed below.

- **Consistent communication:** The digital twin and the autonomous car must communicate consistently in or- der to guarantee information consistency. This allows the sensed data and state information of the car to be continuously uploaded to its private digital twin while it is being driven.
- **Real-time synchronization:** Accurate, safe, compliant data and seamless user experiences depend on digital twins and autonomous cars synchronizing in real time.
- **Private and engaged connection:** Digital twins are intended to assist physical autonomous vehicles in obtaining virtual resources in the cloud as a digital collaborator of autonomous vehicles. Because of this, an autonomous vehicle's digital twin is private, and in order to synchronize the digital twins, the connection between them needs to be private as well.

2.2 Inter-twin communication

Digital twins conversing with one another on the cloud is referred to as inter-twin communication. The information, AI learning, and feedback from the cloud-based digital twins can be shared with the ground-based vehicle through inter-twin connection. Consequently, by relaying inter-twin communication with other vehicles outside of its communication range, the autonomous vehicle can indirectly communicate and aid in the acquisition of global traffic information by autonomous vehicles. The following factors contribute to the inter-twin communication:

- **Distributed peer-to-peer connection:** A distributed digital twin network is made up of several digital twins, and in inter-twin communication, every digital twin is a separate individual. Since all of the participants in this network—digital twins—will exchange resources, such as services or material, each one of them serves as both a resource supplier and an acquirer.
- **Private data asset:** The digital twin of the autonomous car is exclusive to it and contains a lot of data about it. These data are valuable and include some private user information that is part of the digital twin's private data assets.
- **Multi-agents' communication:** The digital twin may be viewed as an agent since it is a sentient, self-governing virtual being. Consequently, we can refer to the exchange of information between digital twins as multi-agent communication.

3. Specific applications for digital twins in vehicles

Digital twins, which integrate many technologies such as cloud computing, virtual reality, 5G, big data, Internet of Things, and others, will play a crucial role in the digital transformation process. Their range of applications is likewise growing. Here are a few VDT application examples. We have looked into some literature in this section about the use of digital twins in cars. Three primary points of emphasis will be covered: route planning, trip simulation, and assistance with learning and data processing.

- **Data processing and help learning:** By using data processing and learning algorithms, digital twins can convert large amounts of data into useful information. offer vehicles with intelligent services,

such tracking congestion prediction, vehicle status, and network optimization. Chen and colleagues [3] investigate a UAV- assisted A mobile edge computing (MEC) system is able to offer supplementary computer resources for the mobile ground edge computing setup. The writers create a digital twin. of the MEC system to provide offline instruction for the suggested an anticipatory deep reinforcement learning (DRL) system on DRL methods and long short-term memory (LSTM). For the issues of chaos and traffic congestion. A unique digital twin-centric strategy for driver intention prediction and traffic congestion avoidance is developed by Kumar et al. [4] using LSTM-based RNNs technology. In order to build a digital twin that can properly predict driver behavior and successfully prevent crashes, Chen et al. [5] use decision tree and k-nearest neighbours learning techniques to understand the specific driving environment and driver behaviour.

- **Trip simulation:** Additionally, the vehicular digital twin can provide driving assistance through simulation and vehicle condition monitoring. A strategy for AV simulation in a car-following scenario with DT assistance is proposed by Xiong et al. [6]. The digital twin has the ability to dynamically control the physical things through simulation in real-time. To guarantee the security of the simulation, the simulation verification is shown in the DT scenario concurrently. A digital twin is created by Wang et al. [7] for connected car advanced driver assistance systems. It gives users the fastest driving speed by uploading the sensor data collected in the physical system to the cloud-based digital twin for processing. By simulating the performance of the electric car, Venkatesan et al. [8] are able to accurately monitor and forecast the health of the electric vehicle.
- **Route planning:** The control of traffic congestion and path planning are the two most significant uses of VDT. In addition to efficiently avoiding traffic congestion, the digital twin can offer consumers individualized route planning services based on data (such as destinations, user preferences, and traffic conditions on the roads). Drivers can choose the optimal path by feeding an artificial intelligence algorithm into the digital twin, which can predict their intentions. To aid in urban road planning, Jiang et al. [9] also suggest a sustainable method called the DT-MCDM-GIS framework, which is based on DT, MCDM, and GIS. By taking into account a number of variables, including land use, building destruction, traffic congestion, driving patterns, air quality, and noise, the suggested framework reduces traffic congestion and gives drivers a comfortable path.

4. Vehicular digital twin security and privacy concerns

VDT has additional security requirements and challenges as a result of the features of intra-twin and inter-twin communications. It faces new risks unique to the architecture of the vehicle digital twin network in addition to the security risks seen in the conventional Internet of Vehicles. We first discuss a few of the major difficulties that VDT faces in this part. Next, we talk on the security of the VDT from both intra- and intertwine perspectives.

- **Privacy:** One of VDT's biggest problems is privacy. With VDT, the car uses a variety of sensors to gather data about user behavior and habits, the traffic environment, and the status of the vehicle. These data are sent over the 5G cellular network to the digital twin hosted on the cloud or MEC servers. Following receipt of the data, the digital twin preprocesses it by encoding, classifying, and filtering it before using big data and artificial intelligence to compute and analyze it. To gather further information, the digital twin will also exchange data. The user's location privacy and identity are susceptible to compromise in this sequence of operations. Vehicle navigation, for instance, can benefit greatly from the location data of the vehicle. But what if the malevolent attacker integrates the vehicle's GPS data with other data? If so, the attacker has the ability to deduce and examine the interests, pastimes, and lifestyle choices of the driver or passenger. As such, VDT must strike a balance between sharing information and protecting user privacy when using user data.
- **Reliability:** The vehicle's driving safety in a VDT depends on the accuracy of the data. We will go into further detail about the sensed data, shared data, and decision outcome. Two factors could jeopardize the dependability of the sensed data. One is that the car gathers inaccurate information. One possibility is that the malevolent assailant modifies it while it is in transit. Consequently, the digital twin will receive erroneous or untrustworthy data. When a vehicle receives erroneous decision feedback and causes significant traffic accidents, it will impact the digital twin's computational outcome. Furthermore, in an effort to broaden their perspectives, the digital twins will also exchange information; nevertheless, erroneous information could have an impact on the choices

made by other digital twins. As an illustration, suppose an attacker compromises the digital twin and sends false information on purpose.

- **Time-sensitive:** In order to prevent accidents and conduct swift rescues, digital twins must make decisions quickly. The requirement for digital twins to collect accurate, dependable, and timely traffic information stems from the time-varying nature of traffic flow and the urgency of traffic management. Additionally, the vehicle must receive the findings of its decision-making rapidly. The stringent and intricate message verification process needed to meet VDT security requirements, however, will delay response times and hence be unable to meet the time-sensitive requirements of VDT.
- **Information synchronization:** In order to achieve information consistency, VDT requires constant synchronization of data and information between the digital twin and its physical entity. Nonetheless, VDT's service quality will be impacted by the synchronization's frequency and timing. In order to guarantee low latency and high reliability of the safety message transfer between the vehicle and the digital twin, it is therefore necessary to take into account some specific scenarios while building the VDT synchronization mechanism and to provide a trustworthy synchronization method. The security concerns related to VDT are separated into two categories in this paper: intra-twin security and inter-twin security. It is possible for both types of assaults to occur. An overview of the risks associated with intra- and inter-twin communication is provided in Fig. 1. the numerous security and privacy risks associated with VDT from both intra- and inter-twin security are covered in the next two sections.

4.1 Intra-twin Security

The susceptibility of intra-twin communication attacks affects the safe operation of VDT. Replay attacks, eavesdrop- ping, or message tampering are some of the ways the adversary can purposefully change the data flow, for example, by sensing data or command messages. These will affect the user's freedom of choice, control over the vehicle, and privacy.

a) **Replay attack:** In a replay attack, the attacker obtains and records data about past traffic or road conditions- including the commands that the digital twin sent to the vehicle and then tries to re-transmit the data shortly after in an attempt to trick both the autonomous car and the digital twin into carrying out the attacker's intended attack. The repeated command data might be the digital twin's control command, which might make the autonomous car lose control. An instance of this would be if the enemy intercepted and stored the acceleration command that the digital twin sent to the autonomous car at a crucial juncture. An important traffic accident will result from the opponent sending this message again when the road is clogged.

b) **Message tampering attack:** An attacker tampering with messages observes the communication data flow between the digital twin and the autonomous vehicle. Once the attacker obtains sensor or command data, they alter it and resend it. For instance, by manipulating the perceptual data, the adversary can render the information false, which will have a big effect on the digital twin's ability to make decisions.

c) **Eavesdropping attack:** Through network traffic monitoring, the attacker in an eavesdropping assault gathers as much information as possible and uses analysis to deduce details about the vehicle and user. The users' privacy will be jeopardized by this passive attack.

4.2 Inter-twin Security

Mutual information sharing enables the digital twin to get additional data. As a result, the car may enhance service quality by anticipating traffic circumstances outside of its field of vision. The user's privacy could be jeopardized, though, if digital twins share information. A digital twin's security also heavily relies on cloud security because it is a virtual entity that lives on the cloud. This means that it can be the target of assaults like DDoS and Sybil, which can paralyze services.

a) **Sybil attack:** In order to compromise dependable system functioning, an attacker uses a Sybil attack to assume the identity of a digital twin. Such attacks fall into two categories. To trick or disturb other virtual twins, one creates several phony identities and sends numerous bogus communications. The second is to present fraudulent information while posing as an authentic digital twin. Because of the vehicle's fluctuating topology and motion, this assault has the potential to provide false information regarding its whereabouts.

b) **Privacy leakage attack:** Sharing of data between digital twins can jeopardize user privacy in the event of a privacy leakage attack. The opponent may question the digital twin, for instance, about the flow of traffic at the present location. If the digital twin provides an accurate response, the opponent can

deduce the target vehicle's location. The attacker can further deduce the interests or behavioural patterns of the driver or passenger by fusing the location data with additional data.

c) **Distributed denial of service (DDoS) attack:** By consuming system resources like memory and bandwidth, the adversary in a distributed denial of service (DDoS) attack renders the system inoperable and unable to serve legitimate users, fulfilling the assault's objective. In VDT, there are primarily two kinds of DDoS attacks. The opponent controls many cars and continuously requests a link to the same digital twin. Moreover, the other way is for the adversary to take control of the digital twin on the cloud and initiate a DDoS attack by persistently requesting information from the same digital twin.

5. Research issue and possible countermeasures for VDT

Countermeasures that are sensible, well-balanced, and guarantee the security and privacy of VDT are desired. In this section, we offer a number of possible countermeasures that pertain to privacy protection, identity authentication, and blockchain, among other areas. We also go over a few unresolved VDT research questions

5.1 Potential Countermeasures

a) **Authentication** The first step in creating a safe VDT is reliable identity authentication. Based on the design of the vehicular digital twin networks, we separate the authentication process into two categories here: intra-twin authentication and inter-twin authentication. In particular, intra-twin authentication refers to the authentication that takes place within the vehicle and the digital twin, whereas inter-twin authentication is the authentication that takes place between the digital twins.

- Authentication in intra-twin communication
- Authentication in inter-twin communication

2. Blockchain Technology: Building a VDT requires trust and trustworthy data, and blockchain technology is a promising way to improve the security and dependability of data sharing and storage for digital twin networks [11]. Blockchain is a publicly shared distributed database with unforgeability, decentralization, transparency, and traceability among its nodes. Consensus algorithms are used to guarantee data consistency and cryptography to provide data security. Data assets in VDT can be shared and stored securely with the use of blockchain technology and smart contracts. Among these, smart contracts, which execute automatically, can guarantee the security of data sharing and blockchain can guarantee data traceability. Furthermore, smart contracts, cooperation, and cryptography enable the establishment of trust relationships and data exchanges between digital twins without the need for a central organization.

3.Privacy-preserving: The sincere but inquisitive nature of cloud services makes privacy concerns in VDT much more pressing. Information exchange and data processing and analysis are the two key facets. We offer a potential privacy-preserving method for each of the two elements, as indicated in table 1.

- Data processing and analysis
- Information sharing

b) **Open Research Issues**

For vehicular digital twins, there are a number of additional security concerns that need to be addressed in addition to the privacy and security concerns that were previously covered.

- Knowledge based security mechanism
- Data effectiveness
- Secured data trading

6. Conclusion

One promising paradigm for transportation in the future is the vehicular digital twin. We initially covered the architecture of automotive digital twin networks in this paper. Next, we looked into the literature on the digital twin of a vehicle. Furthermore, we examined the security risks posed by intra-twin and inter-twin communication in the context of vehicular digital twins. Lastly, we discussed a few open research topics and offered some possible countermeasures from the privacy-preserving, blockchain, and identity authentication domains. Essentially, the effectiveness of VDT networks depends on the well-coordinated integration of strong privacy and security features. The public, stake- holders, and users all need to be trusted in order for VDT networks to be widely adopted. As technology develops, navigating the potential and problems given by Vehicular Digital Twin networks will require constant cooperation and a proactive approach to security and privacy.

References

[1] T. H. Luan, R. Liu, L. Gao, R. Li, H. Zhou, The paradigm of digital twin communications, arXiv preprint arXiv:2105.07182 (2021).

[2] Z. Su, Y. Hui, T. H. Luan, Distributed task allocation to enable collaborative autonomous driving with network softwarization, IEEE Journal on Selected Areas in Communications 36 (10) (2018) 2175–2189.

[3] X. Chen, T. Chen, Z. Zhao, H. Zhang, M. Bennis, J. Yusheng, Resource awareness in unmanned aerial vehicle-assisted mobile-edge computing systems, in: 2020 IEEE 91st Vehicular Technology Conference (VTC2020-Spring), IEEE, 2020, pp. 1–6.

[4] S. A. Kumar, R. Madhumathi, P. R. Chelliah, L. Tao, S. Wang, A novel digital twin-centric approach for driver intention prediction and traffic congestion avoidance, Journal of Reliable Intelligent Environments 4 (2018) 199–209.

[5] X. Chen, E. Kang, S. Shiraishi, V. M. Preciado, Z. Jiang, Digital behavioral twins for safe connected cars, in: Proceedings of the 21th ACM/IEEE international conference on model driven engineering languages and systems, 2018, pp. 144–153.

[6] H. Xiong, Z. Wang, G. Wu, Y. Pan, Design and implementation of digital twin-assisted simulation method for autonomous vehicle in car- following scenario, Journal of Sensors 2022 (2022).

[7] Z. Wang, X. Liao, X. Zhao, K. Han, P. Tiwari, M. J. Barth, G. Wu, A digital twin paradigm: Vehicle-to-cloud based advanced driver assistance systems, in: 2020 IEEE 91st Vehicular Technology Conference (VTC2020-Spring), IEEE, 2020, pp. 1–6.

[8] S. Venkatesan, K. Manickavasagam, N. Tengenkai, N. Vijayalakshmi, Health monitoring and prognosis of electric vehicle motor using intelligent-digital twin, IET Electric Power Applications 13 (9) (2019) 1328–1335.

[9] F. Jiang, L. Ma, T. Broyd, W. Chen, H. Luo, Digital twin enabled sustainable urban road planning, Sustainable Cities and Society 78 (2022) 103645.

[10] C. He, T. H. Luan, R. Lu, Z. Su, M. Dong, Security and privacy in vehicular digital twin networks: Challenges and solutions, IEEE Wireless Communications (2022).

[11] M. Dai, T. Wang, Y. Li, Y. Wu, L. Qian, Z. Su, Digital twin envisioned secure air-ground integrated networks: A blockchain-based approach, IEEE Internet of Things Magazine 5 (1) (2022) 96–103.