IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Ai-Driven Digital Twin Frameworks For Next-Gen 6g V2x Security Solutions

[1]Arjun M Nair, [2]Akhija Lakshmi R

[1]Student, [2]Professor

[1] Computer Science and Engineering (Cyber Security),

[1] St. Joseph's college of Engineering & Technology, Palai, India

Abstract: The arrival of sixth-generation (6G) networks is set to change the Internet of Vehicles (IoV) and Vehicle-to-Everything (V2X) communication. It will provide ultra-low latency, high reliability, and smooth connectivity for future self-driving cars and smart transportation systems. With more artificial intelligence (AI), edge computing, and fast communication, IoV will be the foundation of next-generation mobility services. However, the open, dynamic, and diverse nature of vehicle networks makes them very vulnerable to various cyber threats. Attacks such as Sybil, spoofing, denial-of-service (DoS), replay, and data manipulation can undermine trust, disrupt services, and even put passenger safety at risk. Traditional cryptography and security protocols are somewhat effective but often face problems with scalability, high overhead, and limited flexibility in highly mobile and resource-limited settings.

Digital Twin (DT) technology has emerged as a promising way to overcome these limitations. It creates smart virtual replicas of vehicles, networks, and environments. These digital counterparts allow real-time monitoring, detect problems, and provide predictive security defense. Recent advancements show the effectiveness of DT-driven security methods. Cyber-Twin- based intrusion detection improves the recognition of anomalies and allows for flexible countermeasures. In the same way, DT- powered data sharing in Open RAN boosts data confidentiality and integrity while cutting down on communication delays. Trust management strategies based on DTs help evaluate vehicle interactions, ensuring reliable decision-making and detection of harmful nodes. Additionally, the combination of federated learning with blockchain technology offers decentralized, privacy- protecting, and tamper-resistant security solutions. This approach helps address issues like data poisoning and reliance on central authorities.

Collectively, DT-enabled frameworks improve detection accuracy, reduce latency, increase scalability, and boost resilience against complex cyberattacks. These advancements show the transformative potential of DTs in securing 6G-enabled vehicular networks. They are essential for creating safe, efficient, and intelligent transportation systems.

Index Terms - 6G, Internet of Vehicles (IoV), Vehicle-to- Everything (V2X), Digital Twin (DT), Cybersecurity, Intrusion Detection, Trust Management, Authentication, Vehicle-to-Grid

I. INTRODUCTION

The quick growth of wireless communication technologies has brought about sixth-generation (6G) networks. These networks promise major improvements like sub-millisecond latency, high data rates, and large device connectivity. These changes are likely to reshape the Internet of Vehicles (IoV) and Vehicle-to-Everything (V2X) communication models. They will serve as the main support for smart mobility, self-driving cars, and intelligent transportation systems (ITS).

6G-enabled vehicular networks connect vehicles, infrastructure, pedestrians, and the power grid, creating a com- plex cyber-physical ecosystem. This integration allows for real-time data sharing and decision-making, which improves road safety, traffic efficiency, and environmental sustainability. However, this

openness also brings serious vulnerabilities. Vehicles can be targeted by attacks such as identity spoofing, false data injection, large-scale denial-of-service (DoS), and privacy breaches. These threats compromise the integrity of individual vehicles and can disrupt entire traffic systems or energy networks.

Traditional security mechanisms, primarily cryptography- based authentication and intrusion detection, struggle to keep up with the high mobility, changing layout, and time delays found in vehicular environments. Centralized architectures also create bottlenecks and single points of failure, which makes it harder to scale and stay resilient. Digital Twin (DT) technology represents a significant change. By reflecting the physical environment in a virtual space, DTs allow for real-time simulation, prediction, and response. In vehicular networks, every vehicle, network segment, or grid element can have a digital replica that constantly learns from data, predicts possible threats, and independently coordinates countermeasures. This means DTs go beyond just detecting issues; they provide proactive, predictive protection.

This paper thoroughly examines how DT-driven designs can strengthen 6G-based vehicular networks. It reviews and compares important studies that focus on intrusion detection, authentication, trust management, and vehicle-to-grid (V2G) protection. The findings show how combining DTs with AI, federated learning, and blockchain technologies creates a new generation of smart, scalable, and flexible vehicular security systems.

I. LITERATURE REVIEW

A. *2020: A Comprehensive Survey on Authentication Schemes in VANETs [1]*

Idea: This survey reviews authentication schemes in Vehicular Ad-Hoc Networks (VANETs). It identifies vulnerabilities including Sybil, impersonation, replay, and DoS attacks.**Methodology and Results:** Over 50 authentication schemes are examined and grouped into identity-based, group-based, and certificateless methods. The study highlights the trade-offs between computing costs and delays in real-time applications. **Applications:** Offers a foundation for creating 6G-compatible authentication protocols that are optimized for scalability and low latency. **Limitations:** Theoretical in nature, without real- world validation or implementation results.

B. *2021: Cyber-Twin: Digital Twin-Boosted Intrusion Detection [2]*

Idea: Introduces the “Cyber Twin” concept and uses digital twins for autonomous intrusion detection. **Methodology:** Each vehicle has a cyber-twin that uses machine learning models to predict behavior and detect anomalies. **Results:** Achieved a 15 –20% of accuracy for the improvement and reduced false positives. **Challenges:** Synchronization delays and processing overhead in high-mobility scenarios.

C. *2021: Digi-Infrastructure for 6G Smart Cities [5]*

Idea: Proposes a DT-driven network infrastructure that ensures low-latency communication for 6G urban applications. **Results:** Achieved 30% of latency for reduction and improved reliability for critical services. **Applications:** Ideal for emer- gency vehicle coordination and intelligent traffic management. **Limitations:** Chance of high cost and scalability issues for large-scale deployment.

D. *2022: Trust Management for Digital Twins in VANETs [3]*

Idea: Develops trust evaluation models based on DT, using reputation scores and communication history.

Results: Demonstrated the ability to detect 95% of malicious nodes while keeping false positives low. **Limitations:** It is dependent on accurate DT modeling; storage-intensive.

E. *2022: Secure Data Dissemination in DT-Powered O-RAN [4]*

Idea: Introduces a secure data sharing method in Open RAN with the help of lightweight cryptography. **Results:** Latency reduced by 18% and improved packet integrity. **Limitations:** Stability depends on the O-RAN infrastructure; lacks large- scale testing.

F. 2022: Federated Learning and Blockchain for 6G-V2X [6]

Idea: Merges federated learning with blockchain to offer privacy-focused decentralized security. **Results:** Increased resilience to poisoning attacks comes with higher communication costs.

G. 2023: AI-Enhanced Digital Twin Framework (Base Paper) [9]

Idea: Integrates AI-based anomaly detection with DT for real-time cyber resilience. **Results:** Improved detection accu- racy by 20% and reduced latency by 15%. **Limitations:** High AI model complexity; field validation pending.

II. SYNTHESIS

The studies reviewed highlight the important role of digital twins (DTs) in changing vehicular cybersecurity. Early research focused on authentication and theoretical models. Re- cent efforts have moved toward smart, real-time, DT-enabled systems. These systems make use of continuous data exchange between the physical and digital layers, which allows for flexible threat responses.

DTs not only mirror system states; they also predict changes using AI models and reinforcement learning. This ability to predict improves detection accuracy. It lets vehicles proactively isolate compromised nodes or adjust routing as needed. Also, integration with blockchain guarantees secure communication logs, while federated learning shares intelligence across the network, reducing privacy risks.

However, creating smooth interoperability between DTs, vehicular systems, and cloud or edge infrastructures is still a challenge. Issues like synchronization delays, energy consumption, and scalability in ultra-dense networks require new optimization strategies.

III. COMPARATIVE ANALYSIS

A. Discussion

The findings show a shift from traditional rule-based se- curity to cognitive, self-adaptive models. DT-based systems enable:

- Predictive intrusion detection using AI and ML.
- Distributed trust management through DT replicas.
- Integration with blockchain for auditability.
- Low-latency authentication leveraging real-time virtual simulation.

However, there are still important gaps in research related to energy efficiency, real-time synchronization, and multi-layer interoperability.

Paper	Strengths	Limitations
Authentication Survey (2020)	Broad analysis of VANET authentication and attack models.	Theoretical; lacks real-time insights.
Cyber-Twin IDS (2021)	Adaptive DT-based anomaly detection.	High computational cost.
Digi-Infrastructure (2021)	Optimized network slicing and latency reduction.	Scalability and cost issues.
Trust Management (2022)	Reliable trust evaluation with DT.	Storage and modeling complexity.
FL + Blockchain (2022)	Privacy-preserving decentralized model.	Communication overhead.
AI-Enhanced DT (2023)	Combines AI, DT, and FL for real-time security.	Early prototype; untested scalability.

TABLE I: Comparative Evaluation of DT-Based 6G Vehicular Security Studies

IV. RESEARCH GAPS AND FUTURE DIRECTIONS

DT-based vehicular security research has made progress, but it still faces several challenges. These issues need to be re- solved before we can implement it widely in 6G environments.

A. Real-Time Synchronization

Maintaining low-latency synchronization between physical vehicles and their digital counterparts is still a technical challenge. Adaptive update methods that use edge computing and 6G's ultra-reliable low-latency communication (URLLC) can help solve this problem.

B. Energy and Computation Efficiency

DT computation and AI training require a lot of resources. Future research should look into lightweight models, energy- efficient neural structures, and teamwork between edge and cloud computing.

C. Cross-Domain Interoperability

Seamless collaboration among automotive, power grid (V2G), and communication domains is essential. Creating standard data models and interoperability frameworks will enhance consistency and trust among different systems.

D. Secure DT Lifecycle Management

From creation to decommissioning, a DT must keep integrity and confidentiality. Using blockchain-based identity management can ensure traceability and prevent tampering.

E. Privacy Preservation and Legal Compliance

With DTs collecting sensitive vehicle data, it is essential to ensure compliance with privacy standards like GDPR or the upcoming automotive cybersecurity rules.

F. Integration with Quantum-Resistant Cryptography

As quantum computing progresses, traditional cryptographic methods may become weak. We should include quantum-safe cryptographic tools in DT communication pipelines.

G. Multi-Agent Coordination and Swarm Security

In fully autonomous systems, thousands of vehicles will work together through DTs. Research into cooperative, swarm- based defense methods could greatly improve large-scale resilience.

V. CONCLUSION

Digital Twin technology has become a game-changer in securing 6G-enabled vehicular networks. By connecting the physical and cyber worlds, Digital Twins enable real-time monitoring, predictive insights, and flexible security control. Combining Digital Twins with AI, blockchain, and federated learning has been shown to improve how well we detect intrusions, evaluate trust, and ensure data integrity.

Future efforts should focus on lightweight Digital Twin synchronization, decentralized decision-making at the network edge, and standardization for better compatibility. As 6G infrastructure develops, Digital Twin-driven vehicular systems are expected to turn into self-healing, smart networks that can withstand even the most advanced cyber threats.

VII. REFERENCES

[1] M. S. Khan, R. Ahmad, M. H. Alsharif, *et al.*, "A Comprehensive Survey on Authentication Schemes and the Attacks that Threaten It in Vehicular Ad-Hoc Networks," *IEEE Access*, vol. 8, pp. 45279–45296, 2020.

[2] K. Wang, J. Li, L. Gao, *et al.*, "Cyber-Twin: Digital Twin-Boosted Autonomous Intrusion Detection for Vehicular Ad-Hoc Networks," *IEEE Trans. Veh. Technol.*, vol. 70, no. 7, pp. 7043–7055, 2021.

[3] L. Zhao, T. Li, "Trust Management for Digital Twins in VANETs," *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 11, pp. 19945–19958, 2022.

[4] Y. Xu, B. Chen, "Secure Data Dissemination in DT-Powered Vehicular O-RAN," *IEEE Trans. Netw. Serv. Manag.*, vol. 19, no. 1, pp. 567–580, 2022.

[5] P. Rawat, V. Sharma, "Digi-Infrastructure for 6G Smart Cities Using Digital Twin Technology," *Future Internet*, vol. 13, no. 8, pp. 201–215, 2021.

[6] H. Singh, M. Gupta, "Security of 6G-V2X Networks using Federated Learning and Blockchain,"

IEEE Trans. Commun., vol. 70, no. 12, pp. 13567–13580, 2022.
[7] S. A. Malik, R. Hussain, "6G for V2X Communication: Technologies, Challenges, and Opportunities," *IEEE Commun. Standards Mag.*, vol. 5, no. 2, pp. 20–28, 2021.
[8] J. Liu, H. Zhang, "Smart DT-Enabled Security for Vehicle-to-Grid Sys tems," *IEEE Internet of Things J.*, vol. 8, no. 12, pp. 9876–9889, 2021.
[9] S. Sharma, A. K. Sangaiah, M. Khari, *et al.*, "AI-Enhanced Digital Twin Framework for Cyber-Resilient 6G Internet of Vehicles Networks," *IEEE Trans. Intell. Transp. Syst.*, vol. 24, no. 12, pp. 12456–12468, 2023.