Digital Twin-Based Cybersecurity Framework for Real-Time Threat Prediction in Smart Transport Environments: A Technical Review

Farhinbanu Pathan
School of Computing, Engineering, and Creative Industries
University of Bedfordshire
Park Square, Luton, LU1 3JU, UK
farupathanfaru@gmail.com

Md Israfil Biswas
School of Computing, Engineering, and Creative Industries
University of Bedfordshire
Park Square, Luton, LU1 3JU, UK
mdisrafil.biswas@beds.ac.uk

Xiaohua Feng
School of Computing, Engineering, and Creative Industries
University of Bedfordshire
Park Square, Luton, LU1 3JU, UK
xiaohua.feng@beds.ac.uk

***Abstract*—The review identifies substantial potential for behavioural monitoring, security experimentation, anomaly detection, and predictive cyber defence. However, existing evidence remains predominantly based on industrial applications, small-scale prototypes, simulated environments, and restricted datasets, limiting confidence in the scalability and generalisability of current approaches to dynamic, city-scale transportation systems. Key challenges include synchronisation errors, context-dependent DT fidelity, limited AI explainability, attacks against DT components, privacy exposure, data poisoning, false alarms, and concept drift. Furthermore, existing research focuses primarily on detection, with comparatively limited attention to prediction, adaptive response, recovery, and end-to-end cyber resilience. The review concludes that DTs provide a credible foundation for predictive and resilient smart transport cybersecurity, but operational adoption requires secure-by-design architectures, privacy-preserving analytics, trustworthy AI, context-sensitive fidelity, realistic multimodal datasets, and rigorous validation through operationally representative test environments.**

Keywords*—*Cyber-physical systems, intelligent transport systems, smart transport, threat prediction, cybersecurity, digital twin, real-time synchronisation.

I. Introduction

Smart transport environments integrate automated and connected vehicles, traffic management centres (TMCs), emergency services, roadside units (RSUs), Internet of Things (IoT) sensors, and cloud–edge computing platforms within a distributed Cyber-Physical System (CPS). As illustrated in Fig. 1, these heterogeneous components continuously exchange operational and contextual data to support autonomous decision-making, adaptive traffic management, cooperative mobility, and real-time road-safety services [1]. In this environment, Vehicle-to-Vehicle (V2V) communication enables vehicles to exchange information such as position, speed, acceleration, heading, and safety warnings to support cooperative collision avoidance and traffic coordination. Vehicle-to-Network (V2N) communication connects vehicles with TMCs, RSUs, edge platforms, and cloud services, enabling the exchange of traffic conditions, navigation information, road-event notifications, and control information for centralised and distributed traffic management. Vehicle-to-Pedestrian (V2P) communication extends this ecosystem to pedestrians and other vulnerable road users through connected mobile or wearable devices, supporting pedestrian detection, collision-risk prediction, and safety warnings. The integration of V2V, V2N, and V2P therefore creates an interconnected transport CPS in which cyber communications are increasingly interdependent with physical transportation processes.

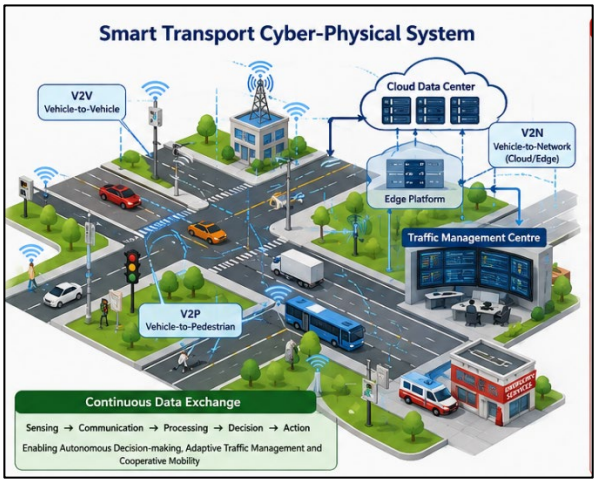

Fig. 1. Smart transport cyber-physical system.

The integration of V2V, V2N, and V2P communications significantly expands the attack surface of smart transport systems across vehicle-to-everything (V2X) communications, traffic-control infrastructure, in-vehicle networks, roadside infrastructure, navigation systems, and cloud–edge platforms. The mobility, connectivity, heterogeneity, and geographically distributed nature of these components create multiple opportunities for adversaries to compromise both cyber and physical operations [4]. Potential attacks include data poisoning, malware, false-data injection, spoofing, message manipulation, and denial-of-service (DoS) attacks [4]. For example, manipulation of V2V messages could cause vehicles to respond to false collision warnings, while compromised V2N communications could introduce erroneous traffic information into a TMC or Digital Twin. Existing research offers valuable and fragmented approaches for DT based monitoring, resilience, security testing and intrusion detection. There exists limited evidence on connecting such capabilities in heterogeneous smart transport environments supporting roadside infrastructure, traffic management platforms and real-time prediction of threat across vehicles. Therefore, a transport-specific framework is needed to integrate synchronised system representation, explainable decisions, predictive threat analytics with coordinated response besides protecting DT.

The main contributions of this paper are summarised as follows:

- **A comprehensive synthesis of existing research** on Digital Twin (DT)-enabled cybersecurity within Cyber-Physical System (CPS) environments, with emphasis on DT architectures, security mechanisms, resilience, and threat detection.

XXX-X-XXXX-XXXX-X/XX/$XX.00 ©20XX IEEE

- **A critical comparative analysis** of existing DT-based cybersecurity approaches, covering cyber-resilience mechanisms, intrusion detection, security testing, threat modelling, and attack analysis.
- **An assessment of the applicability of DT-based cybersecurity approaches to smart transport environments**, considering the characteristics of connected vehicles, V2X communications, roadside infrastructure, traffic management centres, and cloud–edge platforms.
- **A systematic analysis of layered DT cybersecurity architectures** for real-time threat prediction, risk assessment, coordinated response, and recovery across heterogeneous transportation CPS environments.
- **Identification of key research gaps and future priorities**, particularly in secure DT synchronisation, model fidelity, trustworthy and explainable AI, scalability, privacy preservation, adversarial resilience, and real-time edge–cloud deployment.

The rest of the paper is organized as follows. A comprehensive background in the context of DT over CPS domain is presented in Section II. Section III covers discussion, challenges and implications on DT security models considering intelligent transport systems. Section IV provides methodologies for DT-Based Cybersecurity for Smart Transport, Section V provides future research directions in this area of research. Finally, Section VI concludes our paper.

II. BACKGROUND

This section briefly describes research works in relation with DT.

A. Digital Twin for Cyber-Physical Security

DT refers to a dynamic visual representation of physical entity, system or process that is updated consistently. Principal components of DT involve physical asset, operational data, virtual model and communication connection linking physical and virtual environments [7]. DT differs from conventional simulation by facilitating automated data exchange and reflecting physical counterpart changes. However, considerable variation in DT maturity makes accurate characterization of systems lacking the automated synchronisation as digital shadows or the digital models. This shows the dependency of DT capabilities on model fidelity, update frequency, data quality instead of merely virtual representation existence.

Digital Twin Architecture: Generic DT architecture consists of physical, application, communication, analytics and virtualisation layers [11]. Sensors, controllers capture the operational states while data transmission and processing are done by IoT, cloud and edge infrastructure. Virtualization layers combine data-driven, behavioural and physical models for system state reconstruction. Subsequently, analytical services support anomaly detection, monitoring, prediction and simulation. Further Gehrmann and Gunnarsson [12] indicated that separation of security analysis and operational equipment can potentially reduce the disruptive interaction with the industrial systems. However, centralising the system knowledge in DT might create high value attack target with critical dependency.

B. Cyber-Physical System (CPS)

CPS integrate physical, computation and communication processes by feedback-based control. CPS observability is extended by DT through heterogeneous operational data conversion into investigation suitable coherent representation without direct physical system altering. Cyber DT frameworks offer controlled environment for attack simulation, defensive action evaluation and security testing [13]. However, evidence is concentrated on industrial control, production systems, limiting its direct generalisation for decentralised mobile transport environments.

A security-based DT needs to preserve availability, confidentiality and integrity across virtual and physical environments. There is need of authentication, secure interfaces, encrypted communication and authorization for preventing unauthorised manipulation and access [5]. There lies importance of data provenance, integrity validation as corrupted sensor data might produce inaccurate security decisions and virtual states. Therefore, architecture must offer model integrity, privacy protection, resilience synchronisation, explainability and auditability [5]. Finally, there is need of redundancy, graceful degradation so that DT compromise or disconnection doesn't disable physical CPS. This showed the need of embedding cybersecurity across DT lifecycle instead of just adding it to the analytical layer.

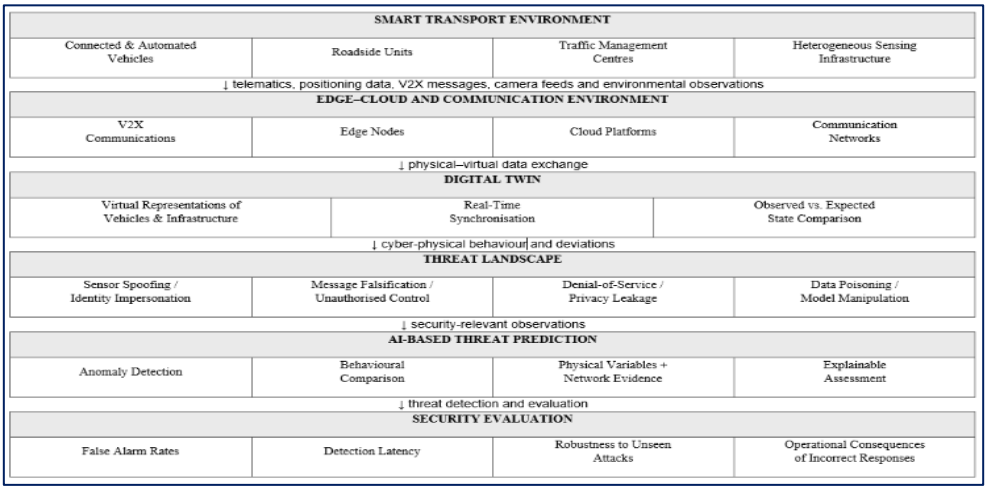

Fig. 2. Digital Twin-based cybersecurity architecture for smart transport environments.

III. Discussion, Challenges and Implications

This section briefly analyses the ongoing research challenges and implications in the area of DT cybersecurity frameworks.

A. Cyber Resilience

Cyber resilience refers to system's capacity of anticipation, withstanding, responding to and recovering from cyber disruption beside maintaining the essential operations. Such capabilities can be strengthened by DT through continuous representation of operational states, behavioural deviation identification and defensive action evaluation without direct disruption of physical assets [12]. ELEGANT adopts DTs for supporting critical infrastructure monitoring and protection [18] while cyber-DT approaches integrate system modelling, attack simulation and security controls [13]. Research on DT driven incident response indicates potential of response strategy evaluation before deployment across physical environment [19]. However, much existing literature operationalizes cyber resilience as mainly monitoring or attack detection. Recovery validation, continuity during compound attacks and graceful degradation are comparatively underdeveloped and thereby limit claims of current frameworks addressing complete life cycle of cyber resilience.

B. Real-Time Intrusion Detection

DT driven intrusion detection compares the observed CPS behaviour with states predicted through trusted virtual model. Such principle is applied by Varghese et al. [8] to industrial control systems, facilitating detection of deviations without exclusively depending on previously specified attack signatures. Historical and real-time CPS data were combined for detecting anomalies and DT-based normal-operation data was used by Castellani et al. [6] along with weak supervision for addressing limited labelled anomalies. Explainable artificial intelligence (AI) is added in ENIGMA for supporting interpretable-based security assessments [10]. Such approaches specify DT potential in improving context-sensitive detection as physical process relationships expose the malicious changes that might be overlooked by network-driven monitoring. However, effectiveness is dependent on trustworthy synchronisation and model fidelity. Also, model error, corrupted telemetry or legitimate operational variation might resemble malicious behaviour and increase false alarms. Moreover, majority of evaluations adopt industrial datasets or controlled testbeds, making scalability and detection latency uncertain across mobile and heterogeneous transport systems.

C. DT Testing

DTs offer isolated environment to attack injection, security control assessment and what-if analysis before application of changes for safety critical CPS [15]. However, Somers et al. [15] identified domination of DT driven CPS testing with passive approaches having limited predictive testing. Also, security operations centre integration offers analysis with the simulated evidence and the training scenarios, while gamification, explainable AI are used by ENIGMA for assessing the security decisions [10]. Even though synthetic scenarios can minimise operational risk and compensate for scarce attack data, its validity is based on whether twin can reproduce physical dynamics, timing and communication with proper fidelity. Therefore, testing outcomes from the state of simplified models might create unjustified confidence on controls that have not been validated under the realistic conditions.

D. DT Security Frameworks

Existing DT security frameworks substantially assign different security roles for DT. Security analysis is separated from the operational industrial equipment by Gehrmann and Gunnarsson [12], while integration of system modelling, security services, sensor information and attack simulation was done by Somma et al. [13] in cyber digital twin. It brought monitoring and protection proposed by Jiang et al. [14] for the cyber-physical protection systems. Empl and Pernul [16] have used bidirectional physical-virtual knowledge for IoT-based security analytics. DT is conceptualised by Aziz et al. [17] as proxy controlling the access between the services and the physical assets. These existing architectures help in advancing security isolation and situational awareness; their concentration across IoT, industrial and production settings restricts the direct transfer for smart transport. Additionally, high reliance on DTs creates a high-value target and potential single-point failure unless the incorporation of model integrity, resilient fallback mechanisms and secure synchronisation [5].

Table I shows the comparisons of existing frameworks that emphasise controlled access (AC), monitoring (MO), testing (TE) and intrusion detection (ID) with rare integration of all the four capabilities. Validation of these existing frameworks is highly domain specific, laboratory-based due to the absence of a review framework that comprehensively demonstrates transport-driven real-time synchronisation with assessment of predictive and explainable threat along with coordinated recovery. Such gap offers basis to examine requirements of smart transport in Section IV and provides future directions in Section V.

TABLE I. Comparisons of Existing DT Cybersecurity Frameworks

Studies / Frameworks	Domains	DT Roles	Security Capabilities	Validation Evidence	Main Strengths	Limitations	Capability Mapping
Gehrmann and Gunnarsson [12]	Industrial automation control	Separation of security replica from operational equipment	Monitoring, behavioural comparison	Industrial automation architecture, demonstrator	Limits intrusive interaction with physical environment	No establishment of prediction, transport applicability	MO
Castellani et al. [6]	Industrial facility monitoring	Normal operation training data generation	Weak supervision of anomaly detection	Real-world facility dataset	Addresses labelled anomalous data scarcity	Limited for anomaly detection instead of coordinated response	ID
Varghese et al. [8]	Industrial control systems	Reference to expected physical behaviour	Intrusion detection	ICS experimental evaluation	Deviation detection through physical	Domain-specific evaluation and doesn't establish the transport scale performance	ID

					process behaviour		
ELEGANT [18]	Critical infrastructure	Representation of operational security	Infrastructure monitoring with security assessment	Critical infrastructure use cases	DT capability connected with critical-infrastructure protection	Weak real-time deployment with limited recovery evidence	MO
ENIGMA [10]	General CPS	Environment of offensive security and training	Attack assessment, analyst training	Experiment through gamification, XAI	Supports decisions of explainable and reasoned security	Highly assessment-driven rather than consistent operational response	TE
Somma et al. [13]	General CPS	Cyber DT integrating models, security services	Attack simulation and evaluation of security control	Demonstrating framework	Combines security, modelling and sensor services	Limited evidence on large-scale DT operational validation	TE
Jiang et al. [14]	Cyber-physical production systems	Security monitoring, protection platform	Detection, protection and analysis	CPS-driven implementation, analysis	Addresses cybersecurity functions in an architecture	Manufacturing assumptions can limit direct transferability to transport	MO, ID
Empl and Pernul [16]	IoT	Representation of knowledge and analytics	DT security analytics	Architectural application for IoT security	Bidirectional knowledge usage for contextualising security events	Dependency of effectiveness on adequate DT knowledge, data quality	MO
Aziz et al. [17]	Industrial CPS	Proxy between service consumers and physical assets	Controlled access, security anchoring, availability	Experimental evaluation on DT as proxy concept	Direct exposure reduced for physical components	Proxy is critical dependency when protected insufficiently	AC
Allison et al. [19]	Cyber-physical systems	Evaluation of incident-response environment	Analysis, response decision improvement	Framework scenario evaluation	DT usage extended beyond detection for incident	Limited real-world evidence on heterogeneous CPS domains	TE

IV. Methodologies of DT-Based Cybersecurity for Smart Transport

This section presents DT-Based cybersecurity methodologies for threat prediction with intelligence.

A. AI-Based Threat Prediction Methodologies

AI can extend DT-driven cybersecurity beyond conventional signature matching by learning normal cyber-physical relationships and predicting whether observed deviations represent malicious attacks, legitimate operational variations, equipment faults, or transient communication anomalies. This capability is particularly relevant to smart transport environments, where system behaviour changes continuously with traffic density, vehicle mobility, weather conditions, road configurations, communication quality, and heterogeneous vehicle populations. Weakly supervised and semi-supervised learning are therefore particularly promising because representative labelled datasets of real-world cyber-attacks are scarce, while continuously changing transport conditions can reduce the generalisability of fully supervised models [6]. Behavioural comparison between DT-generated expected states and observations from physical assets has demonstrated value for intrusion identification and anomaly detection across CPS and industrial domains [10]. Such approaches can be transferred to smart transport by jointly analysing network-level evidence, vehicle behaviour, traffic conditions, sensor measurements, and physical-system states, rather than treating cybersecurity solely as a communication-level classification problem.

Several complementary DT-based cybersecurity methodologies and frameworks can strengthen this predictive capability. Security-Enhancing Digital Twins (SEDTs) provide structured approaches for identifying security requirements, determining appropriate model fidelity, integrating security mechanisms during operation, and managing DT security throughout the system lifecycle [1]. Real-time anomaly detection combines DT-generated predictions with deep-learning, statistical, or physics-based models to identify discrepancies between expected system behaviour and live physical telemetry [9]. Twin-enabled penetration testing further extends DT functionality by enabling non-destructive simulation of attacker tactics, techniques, and procedures (TTPs) against a virtual replica before security controls are deployed or tested against operational transport infrastructure. This provides an opportunity to evaluate system resilience while reducing the safety and availability risks associated with testing directly on live transportation systems.

Security of the digital thread and DT connectivity layer is equally important. The bidirectional communication channels linking vehicles, RSUs, sensors, edge platforms, cloud infrastructure, and their corresponding digital representations must be protected against interception, manipulation, replay, and data poisoning. Secure synchronisation, authentication, integrity protection, low-latency communication, and appropriate bandwidth management are therefore fundamental requirements for trustworthy DT operation. In addition, DT environments can provide safe experimentation and training environments for AI and reinforcement-learning agents, allowing autonomous agents to explore potential attack scenarios, evaluate defensive strategies, and develop adaptive countermeasures without directly affecting physical transportation operations. These capabilities collectively suggest that DT cybersecurity should be considered as a multi-

layered security architecture encompassing secure data acquisition, protected synchronisation, behavioural modelling, AI-based prediction, virtual security testing, and coordinated response.

Nevertheless, existing evidence does not yet establish dependable, real-time threat prediction at the scale and complexity of large transportation networks. Many studies report strong detection performance using simulations, bounded testbeds, or historical datasets in which class distributions and operating conditions are substantially more controlled than those encountered in live mobility systems. Dataset imbalance, insufficient representation of emerging attacks, adversarial manipulation of training data, and concept drift can significantly degrade model performance following deployment. Furthermore, a prediction without an interpretable rationale may be unsuitable for safety-critical interventions, where operators need to understand why a vehicle, communication link, or traffic-control component has been classified as potentially compromised. Explainable AI techniques such as LIME can improve the interpretability of anomaly assessments, while C-ITS research demonstrates the potential of combining machine-learning detection with threshold-based and trust-based mechanisms. Future evaluations should therefore report not only accuracy-based metrics but also false-alarm rates, detection latency, robustness against previously unseen attacks, explainability, computational overhead, and the operational consequences of incorrect security decisions.

The effectiveness of a transport DT is also fundamentally dependent on temporal consistency between the physical transportation environment and its digital representation. Timely and trustworthy synchronisation enables the DT to compare observed and expected system states, identify deviations, simulate potential attack consequences, and evaluate response strategies before corrective actions are transferred to physical assets. However, dynamic transport environments introduce additional synchronisation challenges. Vehicle mobility, heterogeneous sensing rates, clock discrepancies, intermittent connectivity, network congestion, edge-cloud latency, and rapidly changing traffic conditions can produce divergence between the physical system and its DT. Such synchronisation divergence may result in either missed attacks or false alarms if security decisions are based on outdated or inaccurate twin states.

The systematic review by Somers et al. [15] indicates that DT-based research has developed more extensively around monitoring and testing than around predictive, runtime-driven security applications. Similarly, the cyber-resilience review by Pavao et al. [20] highlights the insufficient treatment of resilience mechanisms across existing transport cybersecurity research. These findings reinforce the need to move from isolated DT-based monitoring and intrusion detection towards integrated architectures that combine secure synchronisation, predictive analytics, virtual security testing, explainable AI, and coordinated response. Overall, the literature demonstrates substantial potential for DT-enabled cybersecurity in smart transport, but there remains limited empirical evidence demonstrating scalable, continuously synchronised, explainable, and operationally validated real-time threat prediction across heterogeneous transportation networks. Addressing this gap represents an important research direction for developing resilient Digital Twin-based cybersecurity frameworks for next-generation intelligent transport systems.

V. Future Research Directions

In this section, we present future research directions acquired from this study.

A. Context-Dependent Digital Twin Fidelity

The effectiveness of DT-driven cybersecurity depends strongly on the extent to which the virtual representation captures security-relevant behaviour of its physical counterpart. Future research should therefore move from a general concept of DT fidelity towards context- and task-dependent fidelity requirements. The required fidelity should be determined by the cybersecurity objective, risk level, and operational context. For example, a DT used for V2X message validation requires accurate representations of vehicle mobility, communication protocols, network conditions, and message-generation processes. In contrast, a DT supporting vehicle anomaly detection may require more detailed representations of sensor, actuator, controller, and vehicle-dynamics relationships. Future frameworks should consequently develop adaptive fidelity mechanisms that dynamically increase model resolution when security risks or system uncertainty increase. Research should also establish measurable fidelity metrics linking model accuracy and synchronisation quality directly to threat-prediction performance.

B. Scalability and Distributed Deployment

Most existing DT cybersecurity solutions have been evaluated using industrial testbeds, simulation environments, limited datasets, or isolated devices. Future research should therefore evaluate DT cybersecurity under realistic transportation conditions, including variable vehicle densities, high mobility rates, network congestion, intermittent connectivity, packet loss, heterogeneous communication technologies, and cross-jurisdictional operation. Scalable architectures should support hierarchical or federated DTs in which local edge-level twins collaborate with regional and city-level representations while maintaining security and state consistency. Importantly, scalability should no longer be evaluated solely through conventional classification accuracy. Future studies should report DT update latency, synchronisation divergence, detection-performance degradation, event-processing throughput, communication overhead, memory and computational consumption, and response latency as primary scalability indicators.

C. Privacy-Preserving Digital Twins

Smart transport DTs may process highly sensitive information, including vehicle identifiers, trajectories, behavioural patterns, passenger-related information, location data, sensor measurements, and video streams. Future research should therefore investigate privacy-preserving DT architectures that maintain cybersecurity and threat-prediction capabilities without requiring unnecessary centralisation of raw data. Potential approaches include federated learning, distributed analytics, differential privacy, secure multi-party computation, privacy-preserving data aggregation, and selective data sharing. Privacy should be incorporated throughout the DT lifecycle, covering data acquisition, synchronisation, processing, sharing, storage, model training, retention, and deletion. Future evaluations should consider not only the technical effectiveness of privacy mechanisms but also data minimisation, purpose limitation, proportionality of collection, access accountability, and the potential impact of privacy protection on threat-detection performance.

D. Towards End-to-End Cyber-Resilient Digital Twin Frameworks

The reviewed evidence identifies several priorities for advancing DT-based cybersecurity research in smart transport. Future research should investigate how DTs can support the complete cyber-resilience lifecycle, encompassing anticipation, prevention, detection, response, adaptation, recovery, and continuous learning. Current research predominantly concentrates on monitoring, anomaly detection, and security testing, while empirically validated recovery and adaptive response mechanisms remain comparatively underdeveloped. Addressing this gap would enable DTs to evolve from descriptive monitoring and simulation tools into dependable, continuously validated evidence platforms for predictive and resilience-oriented smart transport cybersecurity. Such evolution must nevertheless retain appropriate human oversight, institutional governance, and safety controls to ensure that automated cyber-defence decisions do not introduce additional risks into critical transportation operations.

VI. Conclusions

This review critically examined the role of DT technology in strengthening cybersecurity and cyber resilience within smart transport environments. The analysis demonstrates that DTs provide a promising mechanism for integrating heterogeneous cyber-physical observations from connected vehicles, V2X communications, roadside infrastructure, traffic management centres, IoT sensors, and cloud–edge platforms. By maintaining a dynamic representation of physical transport assets and their operational states, DTs can provide contextual information for anomaly detection, support behavioural modelling, enable security testing in controlled virtual environments, and facilitate threat prediction and risk assessment without directly exposing safety-critical infrastructure to experimental attacks. These capabilities are particularly valuable in smart transportation, where cyber incidents affecting vehicles, traffic-management platforms, V2X communication, or roadside infrastructure can propagate from the digital domain into physical operations and potentially compromise road safety and mobility services.

However, the reviewed literature also reveals that DT-driven cybersecurity has not yet been sufficiently validated as an operational solution for large-scale, heterogeneous, and safety-critical smart transport systems. Much of the existing evidence originates from manufacturing, industrial control, and other CPS domains, with comparatively limited empirical evaluation in dynamic transportation environments. Furthermore, a DT should not be regarded as an inherently trustworthy security authority. Its reliability depends on the integrity of its data sources, synchronisation mechanisms, models, interfaces, and bidirectional communication channels. Compromise of these components could enable adversaries to manipulate the virtual representation and consequently amplify, conceal, or reproduce malicious information within security decisions.

The review further identifies a persistent imbalance between threat detection and broader cyber resilience. Although artificial intelligence and machine-learning techniques can improve the recognition of complex and previously unseen behaviours, their practical deployment remains constrained by limited and unrepresentative datasets, insufficient explainability, concept drift, adversarial manipulation, false positives, and computational requirements. Consequently, future DT cybersecurity research should move beyond isolated intrusion classification towards integrated, predictive, explainable, and resilience-oriented security frameworks. Key priorities include security-aware DT synchronisation, context-dependent model fidelity, interpretable threat prediction, privacy-preserving analytics, trustworthy AI, and scalable edge–cloud architectures.

References

[1] Jafari, M., Kavousi-Fard, A., Chen, T., & Karimi, M. (2023). A review on digital twin technology in smart grid, transportation system and smart city: Challenges and future. *IEEE Access*, *11*, 17471-17484.

[2] Gularte, K. H. M., Da Costa, J. P. J., Vargas, J. A. R., Da Silva, A. S., Santos, G. A., Wang, Y., ... & Schotten, H. D. (2024). Integrating cybersecurity in V2X: A review of simulation environments. *IEEE Access*, *12*, 177946-177985.

[3] Durlik, I., Miller, T., Kostecka, E., Zwierzewicz, Z., & Łobodzińska, A. (2024). Cybersecurity in autonomous vehicles—are we ready for the challenge? *Electronics*, *13*(13), 2654.

[4] Abdo, A., Chen, H., Zhao, X., Wu, G., & Feng, Y. (2023). Cybersecurity on connected and automated transportation systems: A survey. *IEEE Transactions on Intelligent Vehicles*, *9*(1), 1382-1401.

[5] Alcaraz, C., & Lopez, J. (2022). Digital twin: A comprehensive survey of security threats. *IEEE Communications Surveys & Tutorials*, *24*(3), 1475-1503.

[6] Castellani, A., Schmitt, S., & Squartini, S. (2020). Real-world anomaly detection by using digital twin systems and weakly supervised learning. *IEEE Transactions on Industrial Informatics*, *17*(7), 4733-4742.

[7] Fuller, A., Fan, Z., Day, C., & Barlow, C. (2020). Digital twin: Enabling technologies, challenges and open research. *IEEE Access*, *8*, 108952-108971.

[8] Varghese, S. A., Ghadim, A. D., Balador, A., Alimadadi, Z., & Papadimitratos, P. (2022, March). Digital twin-based intrusion detection for industrial control systems. In *2022 IEEE International Conference on pervasive computing and communications workshops and other affiliated events (PerCom workshops)* (pp. 611-617). IEEE.

[9] Xu, Q., Ali, S., & Yue, T. (2021, April). Digital twin-based anomaly detection in cyber-physical systems. In *2021 14th IEEE Conference on Software Testing, Verification and Validation (ICST)* (pp. 205-216). IEEE.

[10] Suhail, S., Iqbal, M., Hussain, R., & Jurdak, R. (2023). ENIGMA: An explainable digital twin security solution for cyber–physical systems. *Computers in Industry*, *151*, 103961.

[11] Tao, F., Qi, Q., Wang, L., & Nee, A. Y. (2019). Digital twins and cyber–physical systems toward smart manufacturing and industry 4.0: Correlation and comparison. *Engineering*, *5*(4), 653-661.

[12] Gehrmann, C., & Gunnarsson, M. (2019). A digital twin based industrial automation and control system security architecture. *IEEE Transactions on Industrial Informatics*, *16*(1), 669-680.

[13] Somma, A., Casola, V., Cavalli, A. R., De Benedictis, A., Mallouli, W., & Valdés, V. E. (2023, August). A cyber digital twin framework to support cyber-physical systems security. In *2023 IEEE Smart World Congress (SWC)* (pp. 1-10). IEEE.

[14] Jiang, Y., Wang, W., Ding, J., Lu, X., & Jing, Y. (2024). Leveraging digital twin technology for enhanced cybersecurity in Cyber–Physical production systems. *Future Internet*, *16*(4), 134.

[15] Somers, R. J., Douthwaite, J. A., Wagg, D. J., Walkinshaw, N., & Hierons, R. M. (2023). Digital-twin-based testing for cyber–physical systems: A systematic literature review. *Information and Software Technology*, *156*, 107145.

[16] Empl, P., & Pernul, G. (2023). Digital-twin-based security analytics for the internet of things. *Information*, *14*(2), 95.

[17] Aziz, A., Schelén, O., & Bodin, U. (2023, January). Digital twin as a proxy for industrial cyber-physical systems. In *Proceedings of the 2023 10th International Conference on Wireless Communication and Sensor Networks* (pp. 85-92).

[18] Sousa, B., Arieiro, M., Pereira, V., Correia, J., Lourenço, N., & Cruz, T. (2021). Elegant: Security of critical infrastructures with digital twins. *IEEE Access*, *9*, 107574-107588.

[19] Allison, D., Smith, P., & McLaughlin, K. (2023, August). Digital twin-enhanced incident response for cyber-physical systems. In *Proceedings of the 18th International Conference on Availability, Reliability and Security* (pp. 1-10).

[20] Pavao, J., Bastardo, R., & Rocha, N. P. (2024). Cyber resilience and intelligent transport systems, a scoping review. *Procedia Computer Science*, *239*, 139-148.