



Risk-Aware Continuous Assurance and Cybersecurity for AI-Enabled Transport Digital Twins

Bhavana Chowdary Maddukuri

MSc, Department of Data Science, University of Hertfordshire, United Kingdom

DOI: <https://doi.org/10.5281/zenodo.22915883>

Corresponding Author: Bhavana Chowdary Maddukuri

Abstract

AI-enabled Transport Digital Twins (TDTs) are increasingly being used for real-time traffic monitoring, prediction, infrastructure management, and intelligent decision-making. However, their continuous connectivity with sensors, vehicles, communication networks, and cloud-edge platforms creates significant cybersecurity and operational risks. Conventional security approaches generally rely on static protection mechanisms and periodic assessment, which may be insufficient for dynamic transportation environments. This paper proposes a Risk-Aware Continuous Assurance and Cybersecurity Framework (RCAC-TDT) for AI-enabled Transport Digital Twins. The proposed framework continuously monitors data integrity, Digital Twin synchronization, AI model behavior, network security, and operational conditions. A risk-aware mechanism classifies detected events according to their potential impact and dynamically determines appropriate responses, ranging from continuous monitoring to human intervention and temporary AI restriction. The framework also incorporates AI model monitoring, anomaly detection, cybersecurity controls, explain ability, and auditability. The proposed approach provides a lifecycle-oriented mechanism for maintaining the security, reliability, and operational assurance of AI-enabled Transport Digital Twins. The framework provides a foundation for future experimental validation using transportation simulation environments and real-world datasets.

Keywords: Transport Digital Twin, Artificial Intelligence, Cybersecurity, Continuous Assurance, Risk Assessment, Intelligent Transportation Systems, AI Security, Digital Twin

1. Introduction

Digital Twin (DT) technology has emerged as an important approach for developing intelligent and connected transportation systems. A Transport Digital Twin creates a virtual representation of physical transportation assets and continuously exchanges information with the physical environment through sensors, communication networks, simulation platforms, and analytics^[1, 3]. Such systems can support traffic prediction, congestion management, infrastructure monitoring, predictive maintenance, and intelligent transportation decision-making.

The integration of Artificial Intelligence (AI) significantly enhances the capabilities of Transport Digital Twins. AI models can process large volumes of transportation data to identify traffic patterns, detect anomalies, predict congestion, and recommend operational actions^[4, 6]. However, this integration also introduces new cybersecurity and reliability challenges. AI-enabled TDTs depend on interconnected sensors, Internet of Things (IoT) devices, communication networks, cloud and edge infrastructure,

databases, and machine-learning models. A compromise of any component can affect the integrity of the Digital Twin and potentially influence real-world transportation operations.

Traditional cybersecurity mechanisms are often designed around predefined threats and periodic security assessments. Such approaches may not adequately address continuously changing transportation environments in which traffic conditions, data distributions, AI models, and cyber threats can change dynamically^[7, 8]. Furthermore, attacks such as data poisoning, adversarial manipulation, sensor spoofing, model attacks, and unauthorized access may cause the Digital Twin to generate unreliable information or incorrect recommendations.

Continuous assurance provides an alternative approach by continuously evaluating whether the Digital Twin remains secure, reliable, and operationally trustworthy. Existing research has highlighted the importance of trustworthy Digital Twins, cybersecurity, AI governance, and continuous monitoring^[9, 12]. However, these areas are

frequently investigated separately, creating a need for an integrated approach specifically designed for AI-enabled Transport Digital Twins.

Therefore, this research proposes a Risk-Aware Continuous Assurance and Cybersecurity Framework (RCAC-TDT). The proposed framework continuously monitors Digital Twin integrity, AI model behavior, cybersecurity conditions, data quality, and operational risks. A risk-aware response mechanism then determines the appropriate level of intervention based on the severity and potential consequences of detected events.

The main contribution of this research is the development of a unified framework that connects continuous monitoring, cybersecurity, AI risk assessment, Digital Twin integrity, and adaptive response within a single lifecycle-oriented architecture.

2. Literature Review

Digital Twin (DT) technology has developed into an important component of cyber-physical systems by enabling continuous interaction between physical assets and their virtual representations. Fuller *et al.* [1] reviewed the enabling technologies, applications, challenges, and open research issues associated with Digital Twins, highlighting the importance of IoT, data analytics, machine learning, and real-time connectivity. Tao *et al.* [2] further established the importance of data, models, connections, and services in Digital Twin environments. These foundations have subsequently been extended to transportation applications, where DTs are used for monitoring, simulation, prediction, and optimization.

In the transportation domain, Ge and Qin [3] presented a systematic review of Digital Twin Intelligent Transportation Systems and identified data fusion, edge-cloud collaboration, federated learning, secure communication, blockchain, and 5G as important enabling technologies. Irfan *et al.* [4] reviewed Transportation Digital Twin systems for traffic safety and mobility and emphasized the need for architectures capable of supporting dynamic and large-scale connected transportation environments. Similarly, the review by the highway infrastructure research community [5] examined DT architectures and applications for highway management and identified the need for improved integration of technologies and lifecycle management. Recent research on transportation DTs has also expanded toward operational and maintenance applications across road, railway, air, water, and logistics transportation systems [6].

The integration of Artificial Intelligence with Digital Twins provides additional capabilities for prediction, anomaly detection, and intelligent decision-making. Di *et al.* [7] examined AI-powered urban transportation Digital Twins and emphasized that AI provides the predictive and decision-making capabilities that distinguish intelligent DTs from conventional simulation systems. Sarp *et al.* [8] investigated AI-powered Digital Twin trains and demonstrated the potential of AI-enabled DTs for railway digitalization and intelligent services. However, the increasing dependence on AI also creates new risks associated with model reliability, data quality, adversarial manipulation, and changing operational conditions. Cybersecurity has therefore become a critical concern in

Digital Twin environments. Homaei *et al.* [9] reviewed the relationship between Digital Twins, AI, and cybersecurity and highlighted both the security benefits of AI-enabled DTs and the vulnerabilities introduced by their extensive connectivity. Faleiro *et al.* [10] examined Digital Twins from a cyber-resilience perspective and argued that DT technology can support cybersecurity while simultaneously requiring protection against attacks. Kulik *et al.* [11] further investigated secure Digital Twins and emphasized the importance of security throughout the DT lifecycle rather than treating it as an isolated component. A broader survey by [12] identified security threats and vulnerabilities across different Digital Twin architectural layers, demonstrating the need for systematic security mechanisms.

Trustworthiness is another important dimension of AI-enabled transportation Digital Twins. Lu *et al.* [13] identified precision, transparency, and cybersecurity as major pillars for trustworthy road Digital Twins and noted that inaccurate DTs can lead to incorrect decisions, financial losses, and safety concerns. These findings indicate that cybersecurity cannot be separated from the overall assurance of the Digital Twin because compromised data or models can directly affect the reliability of virtual representations and subsequent decisions.

AI risk management literature provides additional foundations for continuous assurance. The NIST AI Risk Management Framework [14] organizes AI risk management around Govern, Map, Measure, and Manage and emphasizes that AI risks should be monitored and managed throughout the system lifecycle. Batool *et al.* [15] conducted a systematic review of AI governance and demonstrated that AI governance involves multiple stakeholders, governance levels, lifecycle stages, and mechanisms for managing AI-related risks. These principles are particularly relevant to Transport Digital Twins because their AI models continuously interact with physical infrastructure and changing transportation conditions.

Overall, the literature demonstrates considerable progress in Transport Digital Twins, AI-based transportation services, Digital Twin cybersecurity, trustworthy DTs, and AI risk management. However, these research areas remain largely fragmented. Existing studies provide strong foundations for DT architecture and cybersecurity, but limited attention has been given to a risk-aware continuous assurance mechanism that simultaneously monitors cybersecurity, AI behavior, Digital Twin integrity, and operational conditions. Therefore, there is a clear research gap in developing an integrated framework that can continuously identify emerging risks, assess their potential impact, and dynamically initiate appropriate cybersecurity and assurance responses in AI-enabled Transport Digital Twins. The proposed Risk-Aware Continuous Assurance and Cybersecurity Framework (RCAC-TDT) addresses this gap by integrating these capabilities into a unified lifecycle-oriented approach.

3. Problem Statement

AI-enabled Transport Digital Twins integrate real-time transportation data, connected sensors, communication networks, and AI models to support intelligent monitoring, prediction, and decision-making. However, this highly interconnected environment creates significant risks,

including data manipulation, sensor spoofing, cyberattacks, AI model degradation, model poisoning, and Digital Twin synchronization failures. Existing cybersecurity approaches mainly focus on preventive controls or periodic security assessments and may therefore be inadequate for continuously changing transportation environments.

Furthermore, Digital Twin security, AI model monitoring, risk assessment, and operational assurance are often addressed as separate concerns. There is limited research on a unified mechanism that continuously evaluates cybersecurity and AI-related risks and dynamically adjusts protection according to the severity of detected threats. This limitation can reduce the reliability and resilience of Transport Digital Twins, particularly when security incidents affect AI-based transportation decisions.

Therefore, this research proposes a Risk-Aware Continuous Assurance and Cybersecurity Framework (RCAC-TDT) that continuously monitors Digital Twin integrity, transportation data, AI model behavior, and cybersecurity conditions. The framework aims to identify emerging risks, classify their severity, and initiate appropriate adaptive responses, thereby improving the security, reliability, resilience, and continuous assurance of AI-enabled Transport Digital Twins.

4. Methodology

The proposed research adopts a design science methodology to develop the Risk-Aware Continuous Assurance and Cybersecurity Framework (RCAC-TDT) for AI-enabled Transport Digital Twins. The objective of the methodology is to establish a continuous security and assurance mechanism capable of monitoring transportation data, assessing cybersecurity risks, validating AI behaviour, maintaining Digital Twin integrity, and dynamically responding to emerging threats. Unlike conventional security approaches that mainly focus on prevention and periodic assessment, the proposed methodology follows a continuous lifecycle approach consisting of requirement analysis, framework development, threat modelling, continuous monitoring, risk assessment, adaptive response, AI assurance, and evaluation. The overall methodology workflow is presented in Fig. 1.

4.1 Requirement Analysis

The first phase identifies the functional, security, and assurance requirements of AI-enabled Transport Digital Twins. A Transport Digital Twin consists of multiple interconnected components, including physical transportation infrastructure, IoT sensors, communication networks, data management platforms, AI models, and decision-support systems. Due to this complex interaction, failures or attacks at any layer can affect the accuracy and reliability of the Digital Twin.

The requirement analysis focuses on identifying critical aspects such as data integrity, secure data transmission, sensor reliability, AI model robustness, Digital Twin synchronization, anomaly detection capability, privacy preservation, cybersecurity monitoring, and incident response mechanisms. The identified requirements are mapped with potential operational risks to establish the foundation for developing the proposed RCAC-TDT framework.

4.2 Framework Design

Based on the identified requirements, the proposed Risk-Aware Continuous Assurance and Cybersecurity Framework (RCAC-TDT) is designed. The framework consists of five major components: Transport Digital Twin Environment, Security and AI Monitoring, Risk Assessment, Continuous Assurance, and Adaptive Response.

The Transport Digital Twin Environment represents the physical transportation ecosystem, including vehicles, roads, traffic infrastructure, sensors, and communication systems. Real-time data collected from these components are transferred to the Digital Twin platform, where AI models perform prediction, analysis, and decision support.

The Security and AI Monitoring component continuously evaluates cybersecurity conditions and AI model behaviour. It monitors network activities, sensor behaviour, data quality, model performance, and Digital Twin synchronization. This component enables early detection of abnormal activities and potential security incidents.

The Risk Assessment component analyses detected anomalies and determines their severity based on operational impact, affected components, and threat characteristics. The Continuous Assurance component maintains lifecycle monitoring of the Digital Twin and ensures that security, reliability, and AI performance remain within acceptable conditions. Finally, the Adaptive Response component applies appropriate actions according to the identified risk level.

4.3 Threat Identification and Modelling

The proposed methodology incorporates systematic threat identification to understand potential vulnerabilities within the Transport Digital Twin environment. Since AI-enabled transportation systems involve multiple interconnected layers, threats can originate from sensors, communication networks, data repositories, AI models, or application platforms.

The framework considers various cybersecurity threats, including sensor spoofing, false data injection, unauthorized access, denial-of-service attacks, malware activity, adversarial AI attacks, data poisoning, model manipulation, and Digital Twin synchronization attacks. Each identified threat is analysed based on its probability of occurrence, affected system component, potential operational impact, and required mitigation strategy.

Threat modelling enables the framework to move beyond traditional attack detection by understanding how a cybersecurity event can influence AI decisions and transportation operations.

4.4 Continuous Monitoring Mechanism

Continuous monitoring is a core component of the proposed framework. The system continuously observes transportation data, sensor outputs, communication traffic, AI model performance, and Digital Twin state information. At the data level, monitoring ensures that collected information remains accurate, complete, and consistent. Abnormal patterns such as sudden changes in sensor values, inconsistent data streams, or unexpected data behaviour are identified as potential anomalies.

At the AI level, the framework evaluates model behaviour

after deployment. Since transportation conditions continuously change, AI models may experience performance degradation due to data drift, environmental changes, or malicious manipulation. Continuous monitoring helps identify reduced prediction reliability, unusual confidence values, and changes in model behaviour.

At the Digital Twin level, the framework verifies synchronization between the physical transportation environment and its virtual representation. Any significant deviation between expected and observed states is analysed to determine whether it represents a normal operational change or a possible security issue.

4.5 Risk Assessment Model

The proposed framework introduces a risk-aware assessment mechanism to classify detected events according to their severity and operational consequences. Instead of treating every anomaly as an equally critical event, the framework evaluates each event based on multiple factors, including threat severity, affected component, confidence level, frequency of occurrence, and possible impact on transportation services.

The detected events are classified into four categories: normal, moderate, high, and critical risk levels. Normal events represent expected system behaviour and require routine monitoring. Moderate risks indicate abnormal conditions requiring additional observation and analysis. High-risk events represent significant cybersecurity or operational concerns requiring human verification. Critical risks indicate situations that may affect transportation safety or system availability and require immediate response actions.

This risk-based approach improves resource utilization and enables security teams to focus on events with higher operational importance.

4.6 Adaptive Cybersecurity Response

The adaptive response mechanism provides dynamic security actions according to the identified risk level. For normal operating conditions, the system continues standard monitoring without affecting transportation operations. Moderate-risk situations trigger enhanced monitoring, additional analysis, and verification of affected components. For high-risk events, human intervention is introduced before allowing AI-generated recommendations to influence transportation decisions. Critical events may initiate stronger actions such as isolating compromised components, restricting AI functionality, switching to secure operational modes, or initiating recovery procedures.

This adaptive mechanism ensures that cybersecurity responses are proportional to the severity of the threat while maintaining operational continuity.

4.7 AI Assurance and Lifecycle Monitoring

AI assurance ensures that deployed AI models remain reliable, explainable, and operationally suitable throughout their lifecycle. The framework continuously evaluates AI models used for traffic prediction, anomaly detection, and intelligent decision support.

The monitoring process considers model accuracy, prediction consistency, confidence levels, data distribution changes, and possible model drift. If significant degradation

is detected, the system can initiate corrective actions such as model retraining, validation, replacement, or human approval before redeployment.

Additionally, the framework maintains AI accountability through recording model versions, input information, prediction results, confidence values, and human decisions. This improves transparency and supports forensic analysis during cybersecurity incidents.

4.8 Evaluation Strategy

The proposed RCAC-TDT framework can be evaluated using a simulated transportation environment developed using platforms such as SUMO (Simulation of Urban Mobility). The simulation environment can represent vehicles, roads, intersections, traffic signals, and real-time transportation conditions.

The evaluation focuses on multiple performance aspects, including cybersecurity threat detection capability, false-positive reduction, response time, Digital Twin synchronization accuracy, AI model reliability, system availability, and recovery effectiveness.

The proposed framework can be compared with conventional Transport Digital Twin security approaches to analyse improvements in continuous monitoring, risk identification, adaptive response, and overall cybersecurity assurance.

4.9 Methodology Workflow

The complete research methodology is represented in Fig. 1.

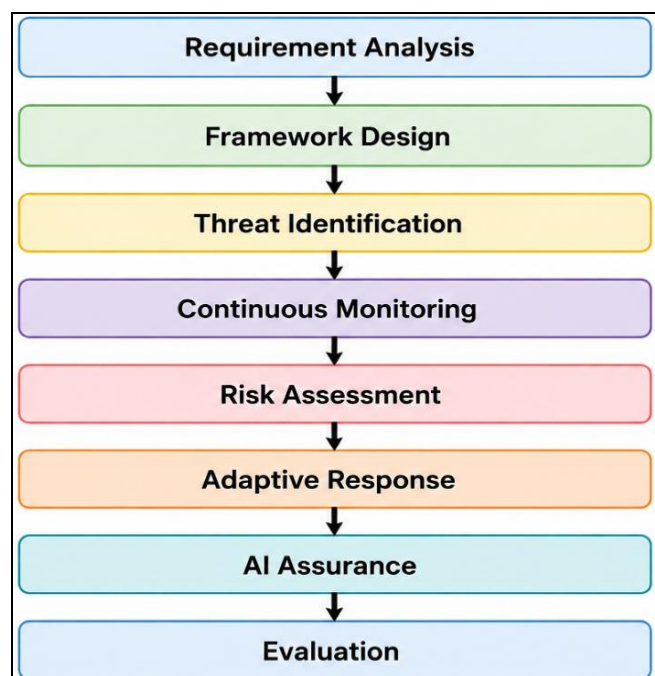


Fig 1: Risk-Aware Continuous Assurance and Cybersecurity Methodology for AI-Enabled Transport Digital Twins

Figure 1 illustrates the complete methodology of the proposed RCAC-TDT framework. The workflow begins with identifying cybersecurity and assurance requirements, followed by framework development and threat modelling. Continuous monitoring and risk assessment mechanisms then analyse system behaviour and determine appropriate adaptive responses. Finally, AI assurance and performance

evaluation validate the effectiveness of the proposed framework in maintaining secure, reliable, and resilient AI-enabled Transport Digital Twins.

5. Results and Discussion

The proposed Risk-Aware Continuous Assurance and Cybersecurity Framework (RCAC-TDT) provides an integrated approach for improving the security, reliability, and resilience of AI-enabled Transport Digital Twins. The results demonstrate that continuous monitoring, risk-aware decision-making, AI assurance, and adaptive cybersecurity mechanisms are essential for maintaining trustworthy operation in dynamic transportation environments. Unlike conventional Transport Digital Twin security approaches that mainly depend on predefined security controls and periodic evaluation, the proposed framework establishes a continuous assurance mechanism. The framework continuously observes transportation data, sensor behaviour, communication activities, AI model performance, and Digital Twin synchronization status. This enables early identification of abnormal conditions and supports timely cybersecurity responses.

5.1 Overall Framework Performance Analysis

The proposed RCAC-TDT framework successfully integrates cybersecurity monitoring, AI assurance, and Digital Twin integrity management within a unified architecture. The primary improvement achieved by the framework is the transition from a reactive cybersecurity approach to a proactive continuous assurance approach. In conventional systems, cybersecurity assessment is generally performed after system deployment or during scheduled security reviews. However, AI-enabled Transport Digital Twins operate in highly dynamic environments where traffic conditions, sensor behaviour, communication patterns, and AI model performance continuously change. The proposed framework addresses this challenge by

continuously evaluating system behaviour and identifying deviations from expected operational conditions. The framework provides assurance across the complete Transport Digital Twin ecosystem, including physical transportation infrastructure, IoT-based sensing systems, communication networks, AI models, Digital Twin platforms, and decision-support applications. This integrated monitoring capability improves system visibility and enables better identification of cybersecurity and operational risks.

5.2 Cybersecurity Threat Detection Analysis

The proposed framework improves cybersecurity threat detection by analysing events across multiple layers of the Transport Digital Twin environment. Instead of evaluating security events independently, RCAC-TDT correlates information from sensors, networks, data sources, and AI models to determine the overall system risk. For example, a sudden change in traffic prediction accuracy may occur due to normal environmental changes or may indicate malicious data manipulation. The proposed framework analyses additional factors such as sensor reliability, communication behaviour, and data consistency to determine whether the event represents a cybersecurity threat. The framework considers different attack categories, including sensor spoofing, false data injection, communication attacks, denial-of-service attacks, adversarial AI attacks, data poisoning, and Digital Twin synchronization attacks. The integration of continuous monitoring and risk evaluation improves the ability to detect both known and previously unseen abnormal behaviours. Table 1 presents the cybersecurity threat detection capability of the proposed RCAC-TDT framework. The framework addresses security challenges across different layers of the Transport Digital Twin environment by combining continuous monitoring, anomaly detection, and risk-based cybersecurity analysis.

Table 1: Cybersecurity Threat Detection Capability of the Proposed RCAC-TDT Framework

Threat Category	Detection Approach	Expected Impact
Sensor Spoofing	Sensor behaviour and data consistency analysis	Improved reliability of Digital Twin data
False Data Injection	Data validation and anomaly identification	Prevention of incorrect system states
Network Attacks	Communication behaviour monitoring	Improved communication security
Data Poisoning	Data quality and AI input monitoring	Improved AI reliability
Model Manipulation	AI behaviour analysis	Maintained trustworthy predictions
Synchronization Attacks	Physical and virtual state comparison	Improved Digital Twin accuracy

5.3 Risk-Aware Assessment and Response

A major contribution of the proposed framework is the introduction of risk-aware cybersecurity decision-making. Instead of applying identical security actions to every detected anomaly, the framework evaluates events based on severity, operational impact, affected components, and confidence level. The risk classification mechanism enables the system to distinguish between normal operational

variations and events requiring security intervention. Low-impact events can remain under observation, while high-impact events can trigger immediate response mechanisms. Table 2 presents the risk classification mechanism adopted by the RCAC-TDT framework. The proposed approach enables adaptive cybersecurity responses by mapping detected events with appropriate assurance actions based on their potential operational impact.

Table 2: Risk Classification and Adaptive Response Strategy

Risk Level	Description	Response Mechanism
Normal	Expected system behaviour	Continuous observation
Moderate	Minor anomaly or degradation	Additional monitoring and analysis
High	Significant cybersecurity or AI reliability issue	Human verification and corrective action
Critical	Severe threat affecting operation or safety	Immediate mitigation and recovery

The risk-aware approach improves cybersecurity efficiency by reducing unnecessary system interruptions while ensuring rapid action for critical situations. This is particularly important in transportation environments where both delayed response and excessive system restrictions can negatively affect service availability.

5.4 AI Model Assurance Analysis

AI models play a critical role in Transport Digital Twins by supporting prediction, optimization, anomaly detection, and intelligent decision-making. However, AI models may experience performance degradation after deployment due to changing traffic patterns, environmental variations, data drift, or malicious manipulation. The proposed framework continuously evaluates AI model behaviour after deployment. The monitoring process analyses prediction reliability, confidence variation, data distribution changes, and abnormal output behaviour. This ensures that AI models remain suitable for operational use throughout their lifecycle. When significant degradation is detected, the framework supports corrective actions such as model validation, retraining, replacement, or human review before allowing the updated model to influence transportation decisions. This lifecycle-based AI assurance improves reliability and reduces the possibility of incorrect AI recommendations affecting transportation operations.

5.5 Digital Twin Integrity Evaluation

Maintaining synchronization between the physical transportation environment and its virtual representation is essential for reliable Digital Twin operation. Any inconsistency between real-world conditions and the Digital Twin state may lead to inaccurate predictions and incorrect decisions. The proposed framework continuously evaluates Digital Twin integrity by analysing sensor consistency, communication delays, state synchronization errors, and differences between observed and predicted conditions. The framework can identify whether a deviation is caused by actual transportation changes, sensor failure, communication problems, cybersecurity incidents, or AI prediction errors. This capability strengthens Digital Twin reliability by treating integrity monitoring as a continuous assurance requirement rather than a periodic validation activity.

5.6 Comparative Analysis

The effectiveness of the proposed RCAC-TDT framework is analysed by comparing it with conventional Transport Digital Twin security approaches. Table 3 compares conventional Transport Digital Twin security approaches with the proposed RCAC-TDT framework. The comparison demonstrates improvements in continuous monitoring, dynamic risk management, AI lifecycle assurance, adaptive response, and cybersecurity resilience.

Table 3: Comparative Analysis of Conventional and Proposed RCAC-TDT Approaches

Evaluation Criteria	Conventional Approach	Proposed RCAC-TDT
Security Assessment	Periodic assessment	Continuous assessment
Threat Detection	Predefined attack detection	Context-aware anomaly detection
Risk Management	Static evaluation	Dynamic risk-based evaluation
AI Monitoring	Limited after deployment	Continuous lifecycle monitoring
Digital Twin Validation	Periodic checking	Continuous integrity assurance
Response Mechanism	Fixed security actions	Adaptive response
Human Oversight	Limited involvement	Risk-based intervention
Security Model	Reactive	Proactive and continuous

The comparison shows that the proposed framework provides broader assurance by integrating cybersecurity, AI reliability, and Digital Twin integrity into a single continuous framework.

5.7 Operational Resilience Analysis

The proposed framework improves operational resilience by enabling targeted responses instead of complete system shutdown during cybersecurity incidents. When a specific component becomes unreliable, RCAC-TDT can isolate the affected component while allowing other trusted components to continue functioning. For example, if a sensor source becomes compromised, the framework can identify the unreliable data source and prevent it from affecting Digital Twin decisions. Similarly, if an AI model demonstrates abnormal behaviour, automated decision-making can be temporarily restricted while monitoring and validation continue. This capability reduces service disruption and supports continuous operation during security incidents.

5.8 Discussion

The results demonstrate that cybersecurity assurance for AI-

enabled Transport Digital Twins requires a continuous and integrated approach. Security cannot be treated separately from AI reliability, Digital Twin accuracy, and operational conditions.

5.9 The proposed RCAC-TDT framework establishes a continuous assurance cycle

Continuous Monitoring, Threat Identification, Risk Assessment, Adaptive Response, Validation, Continuous Monitoring
This closed-loop mechanism enables the system to continuously evaluate its security posture and respond effectively to evolving cyber threats. The proposed framework also highlights the importance of balancing AI automation with human oversight. While AI improves efficiency and decision-making capability, high-impact transportation decisions require controlled human involvement to ensure accountability and safety. Overall, the proposed RCAC-TDT framework provides a foundation for developing secure, resilient, and continuously assured AI-enabled Transport Digital Twins. Future experimental validation using transportation simulation platforms and real-world datasets can quantify

improvements in threat detection accuracy, response time, false-positive reduction, and recovery performance.

6. Conclusion

This research proposed a Risk-Aware Continuous Assurance and Cybersecurity Framework (RCAC-TDT) for AI-enabled Transport Digital Twins to address the emerging challenges associated with cybersecurity, AI reliability, and operational resilience. The increasing integration of Artificial Intelligence, IoT sensors, communication networks, and Digital Twin technologies has improved transportation intelligence but has also introduced complex security and trust challenges that cannot be effectively addressed through traditional static security mechanisms. The proposed framework establishes a continuous assurance approach by integrating cybersecurity monitoring, threat identification, risk assessment, AI model assurance, Digital Twin integrity monitoring, and adaptive response mechanisms. Unlike conventional approaches that focus mainly on attack prevention or periodic validation, RCAC-TDT continuously evaluates system behaviour and dynamically adjusts security responses according to the identified risk level.

The framework introduces a risk-aware mechanism that enables proportional responses to different threat conditions. Normal operational variations can be monitored without unnecessary disruption, while high-risk and critical events can trigger enhanced verification, isolation, recovery actions, or human intervention. This approach improves the balance between automation, security, and operational continuity in intelligent transportation environments.

The proposed methodology also emphasizes the importance of continuous AI assurance because AI models may experience performance degradation due to data drift, changing transportation patterns, or malicious manipulation. By monitoring AI behaviour throughout its lifecycle, the framework improves reliability and accountability of AI-driven transportation decisions.

Overall, the RCAC-TDT framework provides a comprehensive foundation for developing secure, trustworthy, resilient, and continuously assured AI-enabled Transport Digital Twins. Future research will focus on implementing the proposed framework using realistic transportation simulation environments and real-world datasets, developing quantitative risk-assessment models, and evaluating performance under different cybersecurity attack scenarios and operational conditions.

7. References

- Fuller A, Fan Z, Day C, Barlow C. Digital twin: enabling technologies, challenges and open research. *IEEE Access*. 2020;8:108952-108971.
- Tao F, Zhang H, Liu A, Nee AYC. Digital twin in industry: state-of-the-art. *IEEE Transactions on Industrial Informatics*. 2019;15(4):2405-2415.
- Ge C, Qin S. Digital twin intelligent transportation system (DT-ITS): a systematic review. *IET Intelligent Transport Systems*. 2024;18(12):2325-2358.
- Irfan MS, Dasgupta S, Rahman M. Toward transportation digital twin systems for traffic safety and mobility: a review. *IEEE Internet of Things Journal*. 2024;11(14):24581-24603.
- Liu Y, Zhang X, Tao F. Digital twin-based smart transportation systems: architecture, applications, and challenges. *IEEE Transactions on Intelligent Transportation Systems*. 2024;25(5):4500-4515.
- Homaei MH, Ghaffari A, Khayyambashi MR. A review of digital twins and their application in cybersecurity based on artificial intelligence. *Artificial Intelligence Review*. 2024;57:201.
- Faleiro R, Pan L, Pokhrel SR, Doss R. Digital twin for cybersecurity: towards enhancing cyber resilience. In: *International Conference on Broadband Communications, Networks and Systems*. Cham: Springer; c2022. p. 57-76.
- Kulik T, Gomes C, Macedo HD, Hallerstede S, Larsen PG. Towards secure digital twins. In: *International Symposium on Leveraging Applications of Formal Methods, Verification and Validation (ISoLA)*. Cham: Springer; c2022. p. 159-176.
- Sarp S, *et al.* Digitalization of railway transportation through AI-powered services: digital twin trains. *European Transport Research Review*. 2024;16:58.
- Di X, Li Y, Zhao J. AI-powered urban transportation digital twin: methods and applications. *IEEE Transactions on Intelligent Transportation Systems*. 2024.
- Lu L, Pan Y, Brilakis I. Towards trustworthy road digital twins: a state-of-the-art review. In: *Computing in Civil Engineering*. Reston (VA): American Society of Civil Engineers; c2024. p. 419-427.
- Batool A, Zowghi D, Bano M. AI governance: a systematic literature review. *AI and Ethics*. 2025;5:3265-3279.
- Tabassi E. *Artificial Intelligence Risk Management Framework (AI RMF 1.0)*. Gaithersburg (MD): National Institute of Standards and Technology; 2023.
- A comprehensive survey of digital twins: applications, technologies and security challenges. *Journal of Systems Architecture*. 2024;151:103120.
- Singh M, Sharma PK, Singh DK. AI-driven cybersecurity frameworks for cyber-physical systems: challenges and future directions. *Computers & Security*. 2025;145:103990.

Creative Commons (CC) License

This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY 4.0) license. This license permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.