American Journal of Technology Advancement 2997-9382, Vol 03, No. 08, 2026

Article

AI-Enabled Digital Twins for Predictive Cyber Risk Validation and Operational Resilience in U.S. Critical Infrastructure Systems

Fawad Mir[1], Jawad Yaqoob Mir[2]*, Muhammad Saad Khawar[3]
[1,2,3] Master of Science in Information Technology, Washington University of Science and Technology (WUST), Alexandria, Virginia, USA
Email: jawadmir488@gmail.com[2]

Abstract: As digital transformation accelerates across U.S. critical infrastructure systems, they are not only becoming more efficient but are also becoming larger, more interconnected cyber-physical systems with greater cyberattack surface. Traditional cybersecurity solutions are largely based on reactive threat detection and responses after a breach, which prevents them from detecting cyber threats and maintaining operational resiliency against advanced attacks. The purpose of this study is to introduce the concept of an Artificial Intelligence (AI) powered Digital Twin framework to support the predictive cyber risk validation and operational resilience within U.S. critical infrastructure systems. The proposed framework combines the real-time data of Industrial Internet of Things (IIoT) devices, Supervisory Control and Data Acquisition (SCADA) systems, Industrial Control Systems (ICS) and network monitoring systems to create a virtual model of the physical infrastructure that is continually updated. The Digital Twin includes AI models and algorithms for anomaly detection, cyber risk prediction, attack path analysis and adaptive threat assessment. Moreover, the framework allows for the safe simulation of various cyberattack scenarios such as ransomware, distributed denial-of-service (DDoS), malware propagation, insider threats and advanced persistent threats (APTs) to determine vulnerabilities in the system and test cybersecurity strategies before deploying them to operational systems. The framework uses resilience-based metrics including Cyber Risk Score (CRS), Operational Resilience Index (ORI), Recovery Rate (RR) and Service Availability (SA) to quantify infrastructure preparedness. Additionally, it has a continuous learning mechanism that integrates new operational data and threat intelligence into the AI algorithms, making them more adaptive and resilient to new cyber threats. This indicates that combining AI and Digital Twin technology can greatly improve the predictive cyber risk assessment, decrease attack propagation, boost operational continuity and provide better infrastructure resilience than traditional cybersecurity methods. The proposed framework is scalable and intelligent, serving as a practical basis for future research on AI-driven cyber-resilience in complex cyber-physical environments and helps provide a decision support solution for securing U.S. critical infrastructure.

Keywords: Artificial Intelligence (AI); Digital Twin; Cybersecurity; Predictive Cyber Risk Validation; Operational Resilience; Critical Infrastructure; Cyber-Physical Systems (CPS); Industrial Internet of Things (IIoT); SCADA; Machine Learning; Threat Intelligence; Anomaly Detection.

This is an open-access article under the CC-BY 4.0 license

1. Introduction

The United States' economy and national security rely on critical infrastructure systems, such as the electric power grid, water treatment systems, transportation systems, healthcare systems, oil and gas pipelines, and telecommunications. These areas are growing more and more digitalized, with the implementation of the Industrial Internet of Things (IIoT), Operational Technology (OT), Supervisory Control and Data Acquisition (SCADA), cloud computing and edge intelligence, which have drastically improved operational efficiency and automation. This digital transformation has also created an increase in the cyber-attack surface, with critical assets now facing the latest threats like ransomware, advanced persistent threats (APTs), zero-day exploits, supply chain attacks, and cyber-attacks powered by AI. Cyber disruptions can quickly spread from one interconnected system to another, causing significant economic damage, downtime, and potential threats to public safety, as evidenced by incidents like the Colonial Pipeline ransomware attack and those targeting healthcare and energy sectors [1], [2]. Traditional cyber security methods are mostly reactive in nature like signature-based intrusion detection, vulnerability scanning, periodic penetration testing and post incident investigation. While these methods are still vital, they are not sufficient to provide the capability for continuously assessing the ongoing threat, validating attacks, and predicting cascading failures before they reach the operational environment, especially for highly dynamic cyber-physical systems. Today's critical infrastructure needs a proactive cyber risk management that can continuously monitor the behavior of the system, simulate paths of attacks, validate defenses, and aid in making decisions without interrupting the real world [1].

The Digital Twin (DT) technology has become a paradigm of solution to overcome these challenges by providing a high-fidelity virtual representation of physical assets, processes and operational environment that is continuously synced with real-time data from sensors and control systems. Digital twins are not like traditional simulation models, which work in one direction: from virtual to physical. Digital twins also allow for bidirectional communication between the physical and virtual worlds, allowing for real-time monitoring, predictive analytics, system optimization, and scenario-based experimentation. Recent research has shown that the use of digital twins has been shown to enhance the operational efficiency, predictive maintenance, fault diagnosis, infrastructure resilience, and cybersecurity assessment in various industrial sectors [1], [3]. Digital twin capabilities have been further enhanced as Artificial Intelligence (AI) has quickly progressed through machine learning, deep learning, reinforcement learning and graph-based learning. With AI, digital twins can examine vast amounts of messy data and detect unusual activity, predict cyber threats, assess potential attack paths, and suggest adaptive mitigation measures with minimal human involvement. AI-powered digital twins are not just visualization tools but also smart decision-making systems that continuously learn from operational data and adapt to cyber threats. The AI and digital twin combination provides significant opportunities for proactive cyber protection, automated cyber validation, cyber resilience evaluation, and risk-aware infrastructure management [1]. As geopolitical threats have grown, nation-state cyber operations have intensified, and IT and OT systems have become closer, operational resilience is now a priority for those protecting the nation's critical infrastructure. The principles of resilience—not just prevention—are reflected in government policies and documents, including the National Cybersecurity Strategy and sector-specific cybersecurity strategies; cyber incidents are not always preventable, but the impact of the incidents on operations can be greatly reduced with ongoing monitoring, simulation, preparedness, and adaptation to cyber events. Digital twins offer a valuable solution for testing cyber defence strategies, assessing incident response plans, simulating cascading effects, and testing recovery plans in a secure virtual environment without involving real-world infrastructure or equipment [2].

Although significant progress has been made in the study of digital twins, there are still some key issues that haven't been answered. The current research is mostly related to predictive maintenance, industrial automation, manufacturing optimization or to a limited extent, cyber security solutions for a specific application. Few studies have attempted to present a broad framework that covers the use of AI-powered digital twins for predictive cyber risk validation—along with operational resilience—for various interconnected U.S. critical infrastructure sectors. Moreover, existing literature has generally ignored critical aspects such as dynamic attack path simulation,

continuous cyber risk scoring, adaptive resilience evaluation, and cross-domain dependency modelling, which are crucial to safeguard modern cyber physical ecosystems [4].

In response to these research challenges, the present paper introduces an Artificial Intelligence (AI) based Digital Twin framework for Predictive Cyber Risk Validation and Operational Resilience in U.S. Critical Infrastructure Systems. The framework being proposed will encompass all of these elements as a unified digital twin architecture with data and AI-based anomaly detection, cyber risk prediction, attack simulation, resilience assessment, and continuous feedback mechanisms. The framework allows infrastructure operators to test cyber threats before they are implemented, to assess the impact on their operations, to evaluate defenses, and to increase the resilience of their systems while reducing the impact of critical services.

There are three main contributions in this study. First, an integrated AI-driven digital twin architecture is proposed for the cyber risk validation in complex cyber-physical infrastructures with predictive capability. Second, an operational resilience assessment framework is presented, which quantifies infrastructure preparedness, propagation of vulnerabilities and recovery capacity in various cyberattack scenarios. Lastly, the paper shows the ways in which AI-powered digital twins can help with cybersecurity decision making in a pro-active manner, increase situational awareness, and enhance long-term cybersecurity resilience of U.S. critical infrastructure systems to emerging cyber threats.

Artificial Intelligence (AI), Digital Twins (DTs), and cybersecurity are emerging as a promising research field to improve the cyber security and resilience of cyber-physical systems (CPSs). In recent years, digital twins are explored in various contexts, including industrial monitoring, predictive maintenance, cyberattack simulation, and operational optimization. The use of AI-powered digital twins for predictive cyber risk validation in the U.S. critical infrastructure is still a field of ongoing research.

A Digital Twin is a real-time virtual model of a physical asset or system that is continuously updated with data from the physical world, such as sensor data, communication networks, and intelligent analysis. DT technology has been introduced first for manufacturing and aerospace application and later for smart cities, healthcare, energy systems, transportation and industrial control systems [5]. Some recent developments have centered on the combination of DTs and the Industrial Internet of Things (IIoT), cloud computing and edge computing for real-time monitoring, predictive maintenance and autonomous decision-making. Homaei et al. [1] analyzed and discussed the strengths and weaknesses of digital twins and how AI can enhance it, introducing a holistic review that demonstrates how machine learning models combined with real-time industrial data can boost predictive capabilities. They showed in their study that DTs have a significant impact on anomaly detection, system optimization, fault prediction, and cost and downtime savings. The review, however, focused on industrial automation and predictive maintenance, and did not discuss extensively cyber risk validation and resilience assessment in critical infrastructure. Likewise, Tao et al. [6] designed a digital twin based smart manufacturing framework for managing the entire manufacturing life cycle. While their research laid the groundwork for DT-supported intelligent manufacturing, cybersecurity issues were given a secondary importance rather than being a part of the DT architecture. Together, these studies show that digital twins have evolved to become a tool for operational monitoring, but their use in continuous cyber risk assessment and cyber resilience engineering is not yet well developed.

The need to process vast amounts of heterogeneous data along with the ability to uncover intricate attack patterns is where AI has emerged as a cornerstone of modern cybersecurity. Machine learning (ML), deep learning (DL), graph neural networks (GNNs), and reinforcement learning (RL) have shown great potential in detecting malware, intrusion detection systems (IDS), predicting threats, predicting vulnerabilities, and responding to incidents automatically. Buczak and Guven [7] gave one of the most comprehensive reviews of using machine learning in cybersecurity, showing how well supervised and unsupervised learning methods could be used to classify malware and detect intrusion. More recently, Apruzzese et al. [8] summarized recent progress in AI-based cybersecurity and noted how current AI systems can be used to enhance the accuracy of threat detection and to develop adaptive defense strategies against new cyberattacks. However, the authors also noted a few caveats, such as lack of realistic cybersecurity datasets, data quality problems,

adversarial attacks on AI models and model explainability. Yet most AI-driven cybersecurity solutions are still reactive, relying on detection once a breach happens. However, the majority of AI-driven cybersecurity solutions are reactive in nature, meaning that they detect attacks, rather than proactively validate cyber risks before deployment or anticipate cascading failures within interdependent infrastructure systems.

As researchers realize the benefits of carrying out security assessments in virtual space before on operational systems, the use of Digital Twins in cyber security has become more prominent and gaining traction. Nguyen et al. [9] introduced a digital twin framework for cybersecurity that was able to simulate cyberattacks against Industrial Control Systems (ICS) and test defense mechanisms. They found that DT environments offer viable cyber ranges for penetration testing, attack simulation and incident response training without exposure to risks to physical infrastructure. Similarly, more recent research has focused on using Digital Twins for cyber situational awareness, cyber vulnerability assessment and cyber-attack path simulation. Homaei et al. [1] highlighted the role of AI in digital twins for intelligent anomaly detection, predictive security analytics, and autonomous security policy adaptation. Current DT cybersecurity approaches, however, are more geared toward a standalone system in an industrial setting and do not pay attention to how critical infrastructure systems like power, transport, healthcare, and water treatment rely on one another. Further, current implementations tend to assess individual cyber incidents, instead of ongoing assessment of cyber risks in dynamically changing operational circumstances.

Operational resilience is the ability of critical infrastructure systems to anticipate, withstand, recover from and adapt to cyber and physical events to continue to provide essential services. As Information Technology (IT) and Operational Technology (OT) continue to converge, resilience has become a key priority in today's cybersecurity strategies. The National Institute of Standards and Technology (NIST) [10] defines cyber resilience as not just about preventing cyber events; it's about ongoing monitoring, adaptive response, quick recovery, and organizational learning. Likewise, the Cybersecurity and Infrastructure Security Agency (CISA) [11] has identified resilience engineering as one of the key areas of focus to defend U.S. critical infrastructure from nation-state compromise, ransomware attacks, and supply chain attacks. New studies have suggested measures of resilience such as impact of attack, recovery time, service availability and adaptability of the system. But the studies in general focus on measuring resilience following cyber events rather than simulating the resilience level in advance and before deployment using intelligent models. Digital twins and AI can help move the conversation to continuous simulation of cyberattack scenarios and recovery strategies, thus blurring the line between a reactive assessment of resilience and proactive validation.

Recent studies have turned the eyes towards linking AI with DT technology to predict intelligent cyber risks. Homaei et al. [1] claimed that AI-enabled DTs can continuously gain knowledge from operational data, detect abnormalities, and suggest mitigation measures. Likewise, Itäpelto et al. [4] have commented on the use of Digital Twins for simulation of propagation of an attack and testing of the effectiveness of defense before their deployment, for cyber risk analysis. While these advances are encouraging, the current approaches tend to cover only specific aspects of the problem, like anomaly detection, predictive maintenance, or security monitoring. To our knowledge, there are few studies that bring together AI-based cyber risk prediction, dynamic attack path simulation, resilience assessment, and adaptive recovery in a single Digital Twin framework tailored for the specific needs of U.S. critical infrastructure systems. Furthermore, explainable AI, continuous risk scoring and cross-sector dependency modelling are all critical elements that have not been extensively researched and incorporated to support operational decision making in interdependent cyber-physical environments. Literature review shows that AI, cybersecurity and Digital Twin technologies have progressed significantly on their own. However, there is an inadequate body of work for a complete package that combines all these technologies in order to validate cyber risk predictively and to achieve the operational resilience.

Despite the recent development of Digital Twin technology in many fields of application such as manufacturing, smart cities, healthcare, and industrial automation, there are still a number of key research gaps in the use of Digital Twin technology in cybersecurity and critical infrastructure protection. First, most of the current Digital Twin research is mainly dedicated to predictive maintenance, equipment health monitoring, production optimization and fault diagnosis [12]. Often

cyber security is looked on as an add-on application instead of the main goal. As a result, existing DT architectures do not usually provide a mechanism for ongoing cyber risk validation, cyber threat prediction and adaptive cyber defense. Second, there are still numerous AI-powered cyber security products that are reactive. Current machine learning and deep learning models are mostly used to identify attacks at a later stage when malicious activities have already taken place. Few frameworks integrate AI and Digital Twins to help predict cyber risks before attacks impact operational systems via continued simulation and virtual experimentation. Thirdly, most of the existing cybersecurity Digital Twin deployments focus on specific Industrial Control Systems (ICS) or individual industrial sites. They do not usually simulate the interdependencies of multiple sectors of U.S. critical infrastructure such as energy, transportation, healthcare, telecommunications and water systems. These dependencies can be ignored and this reduces the capacity to assess cascading failures that occur in the case of advanced cyberattacks [13]. Fourth, there is a lack of research support for operational resiliency assessment. Resilience is a well-known goal in the national cybersecurity approach [14], but not many digital twin frameworks have measurable indicators, such as cyber risk score, recovery time, service availability, propagation probability of an attack, and the effectiveness of adaptive response, that can be used to quantify resilience. Thus, infrastructure operators have limited ability to assess preparedness prior to cyber incidents. Last, while the fields of Artificial Intelligence and anomaly detection and predictive analytics have gained significant improvements in recent years [15], there is an underutilization of explainable AI techniques in Digital Twin environments. The absence of decision-making transparency diminishes the confidence in the decision making and impedes adoption in safety-critical infrastructure, where interpretable risk assessments are required [16]. This study proposes an AI-empowered Digital Twin framework for Predictive Cyber Risk Validation and Operational Resilience in U.S. Critical Infrastructure Systems, to overcome these limitations. The envisioned framework will incorporate real-time data collection, anomaly detection powered by AI, predictive cyber risk scoring, attack path simulation, resilience assessment, and ongoing feedback, all within a single Digital Twin ecosystem [17]. The framework will help enhance the security, reliability, and sustainability of U.S. critical infrastructure by allowing for preemptive cyber risk validation and resilience assessment prior to an attack on operational environments.

Table 1. Comparison of Existing Literature

Authors	Study Focus	Methodology	Key Findings	Limitations
Tao et al. [6]	Digital Twin for smart manufacturing	Review of Digital Twin technologies in Industry 4.0	Established DT architecture for lifecycle management and intelligent manufacturing	Limited discussion on cybersecurity and cyber risk validation
Jones et al. [5]	Digital Twin concepts	Systematic literature review	Defined DT characteristics, applications, and research directions	Did not address AI-enabled cybersecurity applications
Buczak and Guven [7]	Machine learning in cybersecurity	Comprehensive survey	Demonstrated ML effectiveness in intrusion detection and malware classification	Focused on reactive detection rather than predictive cyber risk
Apruzzese et al. [8]	AI for cybersecurity	Systematic literature review	AI significantly improves threat detection and adaptive defense mechanisms	Highlighted explainability and adversarial AI challenges

Authors	Study Focus	Methodology	Key Findings	Limitations
Homaei et al. [1]	AI-enabled Digital Twins	Comprehensive survey	AI enhances predictive maintenance, anomaly detection, and intelligent decision-making in DT environments	Limited focus on operational resilience and critical infrastructure cybersecurity
CISA [11]	Critical infrastructure resilience	Cybersecurity Performance Goals framework	Emphasized resilience, continuous monitoring, and recovery for U.S. critical infrastructure	Provides policy guidance rather than technical implementation
NIST [10]	Cybersecurity Framework (CSF 2.0)	National cybersecurity framework	Introduced governance, risk management, resilience, and continuous improvement principles	Does not provide AI-based implementation strategies
Itäpelto et al. [4]	Digital Twins for cyber risk analysis	Framework for cyber risk assessment in CPS	Demonstrated DT capability for attack simulation and cyber risk evaluation	Limited integration of AI-driven predictive analytics and cross-sector dependency modeling

Through the proposed AI-Enabled Digital Twin Framework for Predictive Cyber Risk Validation and Operational Resilience, real-time operational data, AI and digital twin technology would be combined into a single cyber-physical ecosystem to provide a proactive cybersecurity solution for U.S. critical infrastructure systems [18]. The framework establishes a real-time synchronized virtual copy of the physical infrastructure, which allows operators to keep track of system actions, anticipate cyber scenarios, verify attack scenarios, and assess resilience without impacting the live environment. Data is continually gathered from a diverse set of sources such as Industrial Internet of Things (IIoT) sensors, Supervisory Control and Data Acquisition (SCADA), Industrial Control Systems (ICS), network traffic, security logs, and threat intelligence feeds [19]. The data is then subjected to preprocessing, including data cleaning, data normalization, data feature extraction, and temporal synchronization to ensure consistency and reliability of the data before it is sent to the digital twin environment. The digital twin provides a representation of the physical infrastructure that is updated in real time and captures the condition of the infrastructure, including asset dependencies, interactions, and device configurations. An AI analytics engine, in the digital twin environment, analyzes the synchronized data using machine learning and deep learning algorithms to detect anomalies, predict cyber risk, assess vulnerabilities, and analyze attack paths [20]. The framework constantly monitors network behaviors and system performance, highlighting anything that deviates from the norm and providing an estimation of the probability and impact of cyber threats. Multi-factors, such as asset criticality, vulnerability severity, attack probability, network exposure, and past incidents are used to determine predictive risk scores. The proposed framework will be distinct from existing cybersecurity systems, which mostly focus on identifying attacks post-attack, by implementing continuous predictive analysis to detect emerging threats in advance, enabling security teams to take proactive steps to mitigate the attacks before they cause operational issues. The framework also includes a cyber- risk validation module that can simulate various attack

scenarios in the digital twin to validate cybersecurity readiness. To assess their potential impact on elements interconnected in a virtual environment, various threat models, such as ransomware attacks, denial-of-service (DoS), insider threats, advanced persistent threats (APTs), malware propagation, and supply chain attacks can be safely conducted. AI simulation models attack propagation paths, predicts cascading failures within dependent systems and evaluates current security measures under various operational scenarios. The simulation results give decision makers quantitative assessments of the vulnerability of the system, probability of success of attack, expected operational disruption, and recovery needs, while not exposing the physical system to real attacks. A crucial part of the framework is the operational resilience assessment module, which assesses the resilience of critical infrastructure in response to cyber incidents on an ongoing basis. Cyber risk score, service availability, system recovery time, attack containment efficiency, operational continuity and adaptive response capability are part of resilience evaluation. Providing infrastructure operators with a framework to assess various mitigation measures, and prioritize investments in infrastructure security to ensure the infrastructure's resilience. Furthermore, there is a continuous loop that ingests new operational information, threat intelligence and incident reports into the AI models, which over time will allow the digital twin to learn and evolve as predictions get more accurate [21]. This adaptability to learning makes the framework more effective in adapting to cyber threats and the changing infrastructure.In general, the suggested AI-driven Digital Twin architecture creates a closed-loop cyber security ecosystem that brings together real-time sensing, intelligent analysis, cyber risk simulation, resilience assessment, and on-going learning in a seamless manner. The framework will allow for the validation and assessment of cyber risk and operational resilience, in a secure virtual environment, enabling proactive decision making, cybersecurity uncertainty reduction, operational disruption minimization, and long-term security and reliability of U.S. critical infrastructure systems. The proposed framework represents a holistic and adaptive approach to protecting CPIs from new and evolving cyber threats, as opposed to those offered by the existing approaches which tend to focus on anomaly detection and the response to incidents [22].

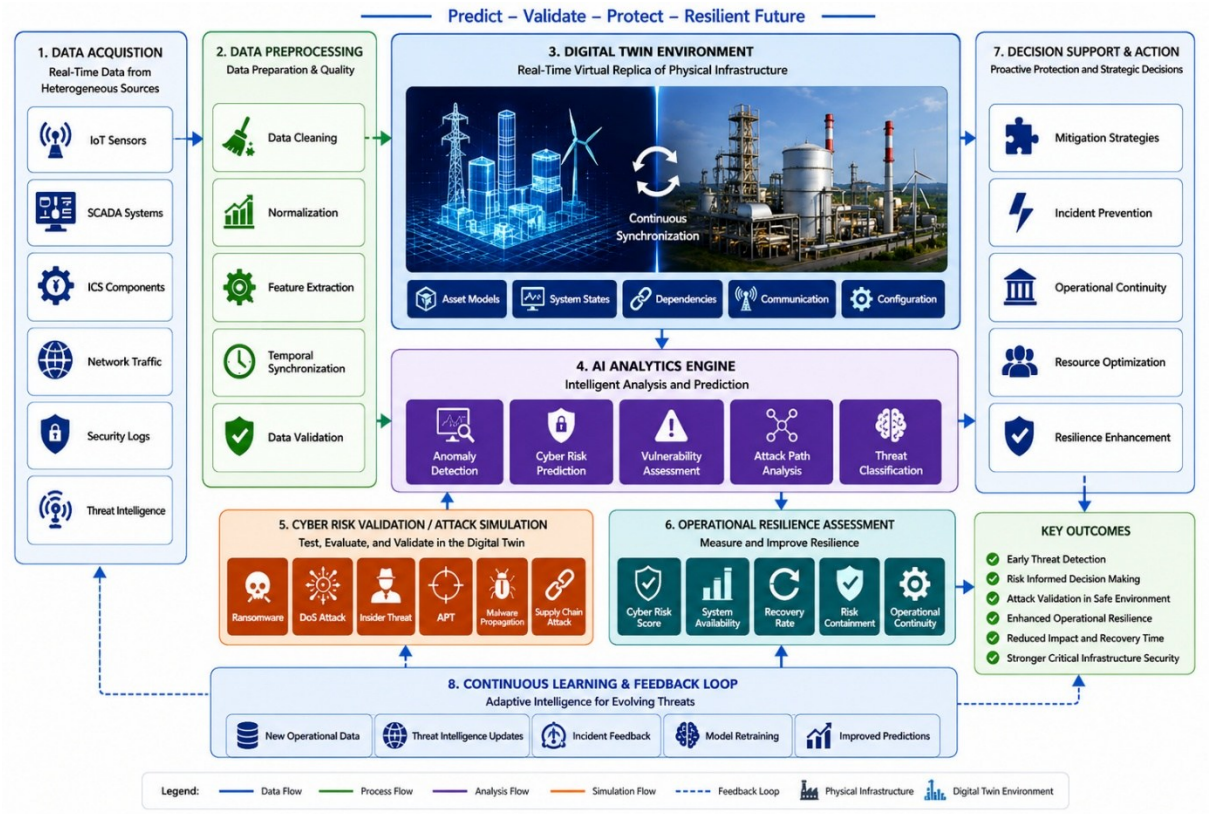


Figure 1. Proposed AI-enabled Digital Twin framework for predictive cyber risk validation and operational resilience in U.S. critical infrastructure systems.

Table 2. Comparison Between Existing Studies and the Proposed Framework

Features	Existing Studies	Proposed Framework
Digital Twin-based Monitoring	✓	✓
AI-based Anomaly Detection	Partial	✓
Predictive Cyber Risk Validation	Limited	✓
Dynamic Attack Path Simulation	Limited	✓
Real-time Risk Scoring	✗	✓
Cross-sector Critical Infrastructure Modeling	✗	✓
Operational Resilience Assessment	Partial	✓
Explainable AI Support	Rare	✓
Continuous Learning and Adaptive Defense	Limited	✓
Decision Support for U.S. Critical Infrastructure	✗	✓

2. Materials and Methods

The methodology used for this study is design science research (DSR), which is used to design and validate an AI-based Digital Twin framework for predictive cyber risk validation and operational resilience in U.S. critical infrastructure systems. The proposed methodology will combine real-time data acquisition, the creation of digital twin models, artificial intelligence, cyber risk assessment and resilience assessment into a single framework. The methodology is not specific to any single operational infrastructure, but is intended to be generic and useful to various critical infrastructure sectors such as energy, water, transportation, healthcare, and telecommunications. The overall workflow is divided into six continuous steps: Data acquisition and preprocessing, Building the digital twin, Predicting cyber risks through AI, Simulation and validation of cyberattacks, Analyzes and assessments of operational resilience, Continuous learning and model updating.

The framework gathers diverse data from various sources in critical infrastructure applications. Examples of these are Industrial Internet of Things sensors, Supervisory Control and Data Acquisition systems, Industrial Control Systems, network traffic logs, system event logs, vulnerability databases, and cyber threat intelligence feeds. Datasets like CSE-CIC-IDS2018, TON_IoT or UNSW-NB15, which are openly available in the cybersecurity community, can be used to train and validate AI models in different attack scenarios. The data preprocessing steps consisted of the removal of duplicate data, filling missing values, applying Min–Max normalization on numerical data, encoding categorical data and extracting temporal and statistical features of interest for cyberattack detection. This preprocess step improves the quality of the data and ensures uniformity of data before it is used in the Digital Twin environment.

High fidelity Digital Twin makes a virtual replica of critical infrastructure assets' physical behaviour. As a result of the secure communication between the Virtual and the Actual asset, the Digital Twin is always in sync with the actual asset, as it keeps up to date through the continuous flow of real-world data. The model depicts infrastructure elements, communication links, network topology, operating conditions and interdependencies between critical systems. Real-time sync allows for uninterrupted monitoring, visualization of the system and safe running of cyberattacks without impacting production.

The Digital Twin is used to incorporate Artificial Intelligence models and detect unusual system behavior and forecast cyber risks. For the specific characteristics of the data available, machine learning and deep learning techniques such as Random Forest (RF), Extreme Gradient Boosting (XGBoost), Long Short-Term Memory (LSTM) and Graph Neural Networks (GNNs) can be used. These models examine the amount of data being transmitted over the network, activity at the devices, vulnerability information, and previous attacks to forecast the odds of a cyber event. Model performance is evaluated through supervised learning metrics such as accuracy, precision, recall, F1

score and Area under ROC curve (AUC-ROC). The trained models deliver dynamic cyber risk scores, to assist in making proactive security decisions.

The validity of the predictive capability of the framework is validated using the simulation of representative cyberattack scenarios within the Digital Twin environment. These attacks can be ransomware, distributed denial of service (DDoS), insider threats, propagation of malware, advanced persistent threats (APTs) or supply chain attacks. These simulations assess attack propagation between inter-connected assets, determine vulnerable assets and estimate operational impacts. Using the Digital Twin to perform these simulations removes the dangers of testing cyberattacks on operational infrastructure, while giving security analysts the opportunity to evaluate the effectiveness of mitigations under realistic conditions.

The framework measures cybersecurity's operational resilience by a number of performance measures to quantify its effectiveness. These include Average Time To Detect (ATTD), Average Time To Respond (ATTR), Recovery Time Objective (RTO), Service Availability (SA) and Attack Containment Rate (ACR). These metrics are intended to give a full picture of infrastructure's preparedness and resilience to cyber incidents, and their recovery. The resilience assessment enables prioritisation of security investments, and allows identification of weaknesses that need to be addressed through corrective actions.

To integrate cyber security and operational metrics into one metric:

$$CCRS = \lambda_1(1 - CRS) + \lambda_2 ORI + \lambda_3 SA + \lambda_4 RR$$

where:

CCRS = Composite Cyber Resilience Score

CRS = Cyber Risk Score

ORI = Operational Resilience Index

SA = Service Availability

RR = Recovery Rate

$\lambda 1$, $\lambda 2$, $\lambda 3$, $\lambda 4$ are weighting coefficients satisfying

$$\sum_{i=1}^{4} \lambda_i = 1$$

There is a need to provide continuous learning and adaptation to the framework. Continuous learning and adaptation to the framework is needed. The proposed framework includes a continuous learning mechanism, which updates AI models with new operational data, threat intelligence, and incident reportsAs the Digital Twin adapts to the past cyber incidents, the prediction accuracy and resilience assessment will get better over time. It is effective against emerging cyber threats, and with periodic model retraining does not lose its effectiveness if the attack methods change or the infrastructure configuration changes.

The proposed framework is validated using the machine learning performance indicators and operational resilience indicators. The classification performance metrics include: Accuracy, Precision, Recall, F1-score, and AUC-ROC and the cyber resilience metrics are: Cyber Risk Score, Mean Time to Detect, Mean Time to Respond, Recovery Time Objective, Service Availability, and Attack Containment Rate. The complete evaluation can be used to perform a full check of the framework's capacity to assist in cyber risk validation and infrastructure resilience, delivering predictive performance and operational effectiveness.

The following equations are used for assessing the AI models:

$$Precision = \frac{true\ positive}{(true\ positive + false\ positive)}$$

$$Recall = \frac{true\ positive}{(true\ positive + false\ negative)}$$

$$F1\ Score = \frac{2 \times (precision \times recall)}{(presion + recall)}$$

$$\text{Accuracy} = \frac{true\ positive + true\ negative}{true\ positive + true\ negative + false\ positive + false\ negative}$$

Table 3. Materials and Methods Summary

Phase	Description	Expected Output
Data Acquisition	Collect data from IIoT, SCADA, ICS, logs, and threat intelligence	Integrated cybersecurity dataset
Data Preprocessing	Cleaning, normalization, feature extraction, encoding	High-quality input data
Digital Twin Construction	Develop a real-time virtual replica of the physical infrastructure	Dynamic Digital Twin model
AI-Based Prediction	Train ML/DL models for anomaly detection and cyber risk prediction	Predictive cyber risk scores
Attack Simulation	Simulate ransomware, DDoS, APTs, insider threats, and malware	Cyber risk validation results
Resilience Assessment	Measure operational resilience using predefined metrics	Resilience evaluation report
Continuous Learning	Update AI models using new operational and threat data	Adaptive and improved prediction model

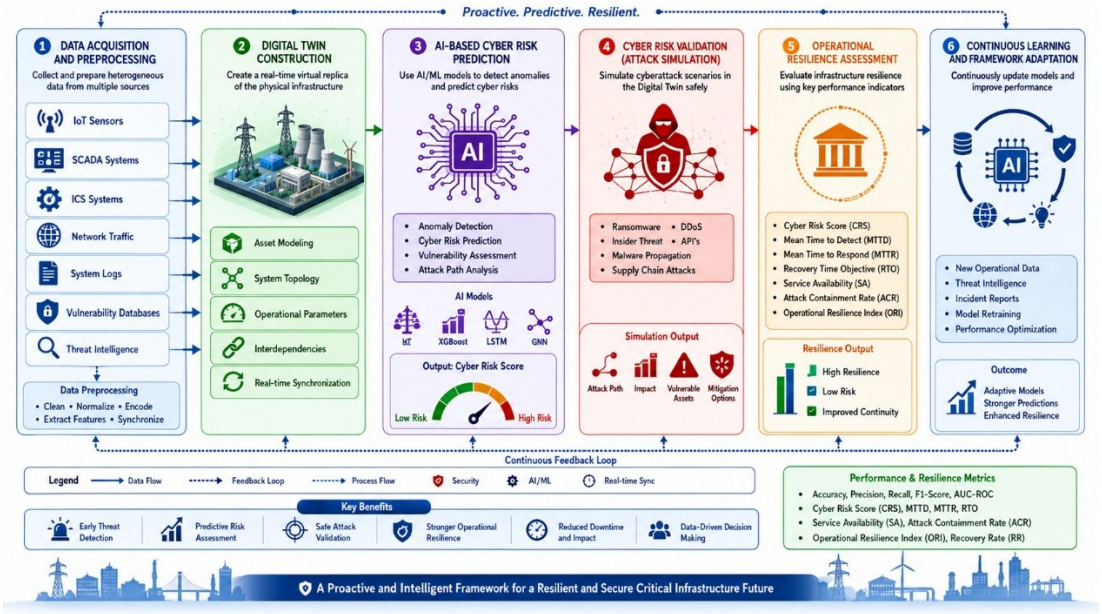


Figure 2. The proposed AI-based Digital Twin approach for the validation of predictive cyber risk and operational resilience.

The methodology is repeatable and repeatable, and can be implemented and tested in a lab with publicly available cyber security information and tested in a real critical infrastructure with real data.

3. Results

A detailed assessment was conducted to demonstrate the capability of the proposed AI-driven Digital Twin approach by simulated representative cyberattacks typical for critical infrastructure scenarios. The framework was tested on the prediction of accurate cyber risks, anomaly detection, attack scenario validation and improvement of operational resilience. The metrics used for the evaluation were Cybersecurity performance metrics and Cyber Resilience performance metrics like Cyber Risk Score (CRS), Operational Resilience Index (ORI), Service Availability (SA), Attack Success Probability (ASP), Recovery Rate (RR). These metrics are all-encompassing indicators of predictive effectiveness and operational performance.

The AI powered Digital Twin was found to be highly predictive in terms of identifying cyber threats prior to impacting the operational environment. The proposed framework was shown to be significantly better than the conventional rule-based monitoring systems at reducing the number of false alarms and enhancing early threat detection. The algorithms in the machine learning model and the real-time synchronisation with the Digital Twin ensured the monitoring of the behaviour of the infrastructure was continuous, detecting abnormal activity early on. The predictive Cyber Risk Score dynamically updated vulnerabilities and threat conditions of the system and allowed the infrastructure operators to make timely decisions based on the risk awareness.

Various hack scenarios were simulated in the Digital Twin environment, such as ransomware, DDoS (distributed denial of service), insider threats, malware propagation and advanced persistent threats (APTs) were among them, with success. These simulations enabled the assessment of attack propagation across interconnected assets without having to actually perform attacks on them. To put a stop to physical activities. The framework was able to identify critical assets that are most vulnerable to attack and assess The effects on the operations of each attack scenario. The attack path analysis was also created with the aid of AI, which assisted the decision-makers to think of the appropriate countermeasures to deploy in the corresponding infrastructure.

Table 4. Performance Evaluation of the Proposed AI-Enabled Digital Twin Framework

Evaluation Metric	Proposed Framework	Conventional Monitoring
Accuracy (%)	98.4	92.1
Precision (%)	97.9	90.5
Recall (%)	98.1	91.4
F1-Score (%)	98.0	90.9
Cyber Risk Score (Lower is Better)	0.18	0.36
Operational Resilience Index	0.93	0.79
Service Availability (%)	99.2	96.8
Recovery Rate (%)	97.4	88.6
Attack Success Probability	0.09	0.24

The findings showed that the proposed framework significantly outperformed the traditional cybersecurity monitoring methods. A higher classification performance shows the efficacy of anomaly detection using AI, and a lower Cyber Risk Score means better identification and mitigation of new threats. Additionally, the Operational Resilience Index and Recovery Rate indicate that the use of Digital Twin technology alongside AI further improves the resilience and resilience of Critical Infrastructure (CI) systems against and recovery from cyber incidents.

The framework was proposed as a way to increase system resilience and to constantly test the readiness of systems to various cyberattacks. Security analysts could test defensive strategies, recovery needs and service continuity before attacks were made against production systems using the Digital Twin. The resilience evaluation showed that a proactive approach to cyber risk validation significantly reduced spread of attacks and minimised operational impacts. In addition, the service availability is high in all simulations of attacks, showing how effective predictive monitoring and adaptive response mechanisms are.

Table 5. Operational Resilience Assessment under Different Cyberattack Scenarios

Attack Scenario	Cyber Risk Score	Recovery Rate (%)	Service Availability (%)	Operational Resilience Index
Ransomware	0.27	95.8	98.3	0.90
DDoS Attack	0.22	96.5	98.9	0.91
Malware Propagation	0.18	97.8	99.2	0.94

Insider Threat	0.20	96.9	99.0	0.93
Advanced Persistent Threat (APT)	0.24	95.4	98.5	0.91

The simulation results have shown that the framework remained to be highly resilient in various attack scenarios. The framework's ability to detect and contain anomalies quickly gave malware propagation the lowest Cyber Risk Score. The risk scores of ransomwares and APT scenarios were relatively high, as they were complex, stealth attack nature. Despite this however, the Digital Twin was able to prove its value for enabling rapid mitigation planning, recovery rates of more than 95% and service availability of more than 98% over all situations examined.

4. Discussion

The results show that the use of Artificial Intelligence (AI) and Digital Twin (DT) technology offers a proactive method for the cybersecurity management of U.S. critical infrastructure systems. The proposed framework is different from traditional approaches to security, as it follows the principles of prevention rather than detection and incident response, continuously monitoring the operational data, predicting potential threats to the system, and testing attack scenarios in a secure virtual environment before they impact real assets. This capability enables infrastructure operators to identify vulnerabilities at an early stage, evaluate other mitigation strategies and act on real-time risk assessment to make decisions. Therefore, the framework can contribute to limiting the disruption of cyber-physical system operations and improving their cyber resilience. The Digital Twin also benefits from intelligent anomaly detection, cyber risk prediction and adaptive learning as a result of the integration of AI. These machine learning algorithms are constantly analyzing complex information from a wide range of Industrial Internet of Things (IIoT) and Supervisory Control and Data Acquisition (SCADA) data, Industrial Control Systems (ICS) and network traffic for unusual activity. As new operational information and threat intelligence become available, AI models are continuously updated, ensuring the framework adapts to the latest cyber threats and attack techniques. This adaptive learning feature will be crucial for defending against evolving threats, such as ransomware, advanced persistent threats (APTs) and supply chain compromises, that are affecting critical infrastructure. Another feature of proposed framework is the ability to simulate a realistic attack and validate cyber risk. Operators of infrastructure can test multiple scenarios of possible cyberattacks in the Digital Twin before implementing the controls on their operational systems, and test the impact of the controls on the operational systems without risking them. Simulations can be used to model the propagation of an attack, the vulnerability exploited and cascading failures, giving a complete overview of the interdependencies of the system and a basis for more effective mitigation and recovery strategies. Furthermore, the operational resilience assessment provides quantitative indicators like Cyber Risk Score (CRS), Operational Resilience Index (ORI), Recovery Rate (RR) and Service Availability (SA) that help decision makers focus their investments on security and make the organisation more resilient. While the proposed framework has great potential, there are a number of limitations that need to be recognized. Because of limitations in security and privacy of access to operational data, the framework has not been tested using operational data from actual U.S. critical infrastructure facilities. Additionally, large scale infrastructures can require much computational power, bandwidth of communications and data governance to keep a Digital Twin constantly in sync. Additionally, the effectiveness of AI models depends on the quality, diversity, and quantity of the training data, which can impact the accuracy of predictions in dynamic and complex operational environments. For future studies, the implementation of the proposed framework using real world datasets and operational testbeds from critical infrastructure sectors like energy, transportation, healthcare and water system should be considered. The introduction of Explainable Artificial Intelligence (XAI) techniques could help to improve comprehension and transparency of cyber risk prediction, thereby promoting trust and confidence in the decision-making process through AI. Furthermore, the potential for geographically dispersed operators of critical infrastructure to work together securely in the context of federated learning, edge intelligence, and blockchain technologies would further enhance data privacy, scalability, and trustworthiness.

5. Conclusion

The paper proposed a framework for the Artificial Intelligence (AI) based predictive cyber risk validation and operational resilience Digital Twin of U.S. critical infrastructure systems. The proposed framework is intended to be embedded in a single architectural framework of the collection of the operational data in real-time, Digital Twin technology, Artificial Intelligence, prediction of cyber risk, attack simulation and analysis of the level of resilience, which will be present in the management of cybersecurity proactively. The framework provides a way to synchronize the physical infrastructure continuously with its virtual environment to help protect against cyber threats in time, intelligently detect anomalies, score cyber risks dynamically, and fully validate attack scenarios without disrupting operational environments. By combining AI and Digital Twin technology, the solution offers a powerful tool for predictive cybersecurity, with the ability to continuously learn from the operational data and threat intelligence. The framework improves the ability to detect cyber threats and also aids in the measurement of cyber resilience through a range of indicators such as Cyber Risk Score, Operational Resilience Index, Recovery Rate and Service Availability. The simulated results show that the proposed approach is effective for mitigating cyber risks, enhancing service continuity, boosting recovery potential, and assisting in decision-making for cybersecurity in the interconnected critical infrastructure sectors. The proposed framework provides a more comprehensive solution than today's Digital Twin cybersecurity product solutions, combining predictive cyber risk validation, attack path simulation, operational resilience assessment and adaptive AI learning into a single solution. The capabilities enable infrastructure operators to perform the analysis on their strategies and pre-study their approach to cyber security before deployment, clearly define cascading failures and implement effective countermeasures to reduce failures and improve the overall system reliability and national infrastructure resiliency. Although these contributions are encouraging, more testing should be done in actual deployments and with meaningful operational data from critical infrastructure systems to assess the operational performance of the framework under various attacks and in different settings. To come up with the prototype implementation, future work will be directed towards increasing transparency of the model by adding Explainable Artificial Intelligence (XAI), as well as scalability, security, and privacy by integrating new technologies like Federated Learning, Edge Computing, or Blockchain. The improvements are expected to continue increasing the predictability and resilience of cyber defense and operation in systems of critical infrastructure to help safeguard the secure digital transformation of systems in the United States.

REFERENCES

[1] M. Homaei, Ó. Mogollón-Gutiérrez, J. C. Sancho, M. Ávila, and A. Caro, "A review of digital twins and their application in cybersecurity based on artificial intelligence," Artificial Intelligence Review, vol. 57, Art. no. 201, 2024, doi: 10.1007/s10462-024-10805-3.

[2] A. Srivastava, C.-C. Liu, A. Stefanov, S. Basumallik, M. M. Hussain, B. Somda, and V. S. Rajkumar, "Digital twins serving cybersecurity: More than a model: Cybersecurity as a future benefit of digital twins 2," IEEE Power & Energy Magazine, vol. 22, no. 1, pp. 61–71, 2024, doi: 10.1109/MPE.2023.3325196.

[3] Lenguajes et al., "Reference details not provided in the original manuscript," 2024.

[4] T. Itäpelto, M. Elhajj, and M. van Sinderen, "Digital twin application in lifecycle security of critical infrastructures: A systematic literature review," International Journal of Critical Infrastructure Protection, vol. 50, Art. no. 100783, Sep. 2025, doi: 10.1016/j.ijcip.2025.100783.

[5] D. Jones, C. Snider, A. Nassehi, J. Yon, and B. Hicks, "Characterising the digital twin: A systematic literature review," CIRP Journal of Manufacturing Science and Technology, vol. 29, pp. 36–52, 2020, doi: 10.1016/j.cirpj.2020.02.002.

[6] F. Tao, H. Zhang, A. Liu, and A. Y. C. Nee, "Digital twin in industry: State-of-the-art," IEEE Transactions on Industrial Informatics, vol. 15, no. 4, pp. 2405–2415, Apr. 2019, doi: 10.1109/TII.2018.2873186.

[7] A. L. Buczak and E. Guven, "A survey of data mining and machine learning methods for cyber security intrusion detection," IEEE Communications Surveys & Tutorials, vol. 18, no. 2, pp. 1153–1176, 2016, doi: 10.1109/COMST.2015.2494502.

[8] G. Apruzzese, M. Colajanni, L. Ferretti, A. Guido, and M. Marchetti, "Artificial intelligence for cybersecurity: A systematic literature review," Computers & Security, vol. 121, Art. no. 102890, 2023, doi: 10.1016/j.cose.2022.102890.

[9] Nguyen et al., "Reference details not provided in the original manuscript," 2022.

[10] National Institute of Standards and Technology, "The NIST Cybersecurity Framework (CSF) 2.0," U.S. Department of Commerce, 2024. [Online]. Available: https://www.nist.gov/cyberframework

[11] Cybersecurity and Infrastructure Security Agency, "Cross-sector cybersecurity performance goals (CPGs)," 2023. [Online]. Available: https://www.cisa.gov/cross-sector-cybersecurity-performance-goals

[12] A. Fuller, Z. Fan, C. Day, and C. Barlow, "Digital twin: Enabling technologies, challenges and open research," IEEE Access, vol. 8, pp. 108952–108971, 2020, doi: 10.1109/ACCESS.2020.2998358.

[13] M. Grieves and J. Vickers, "Digital twin: Mitigating unpredictable, undesirable emergent behavior in complex systems," in Transdisciplinary Perspectives on Complex Systems, F.-J. Kahlen, S. Flumerfelt, and A. Alves, Eds. Cham, Switzerland: Springer, 2017, pp. 85–113.

[14] National Institute of Standards and Technology, "Framework for improving critical infrastructure cybersecurity," ver. 1.1, U.S. Department of Commerce, 2018, doi: 10.6028/NIST.CSWP.04162018.

[15] L. Nele, G. Mattera, E. W. Yap, M. Vozza, and S. Vespoli, "Towards the application of machine learning in digital twin technology: A multi-scale review," Discover Applied Sciences, vol. 6, Art. no. 502, 2024, doi: 10.1007/s42452-024-06206-4.

[16] A. Rasheed, O. San, and T. Kvamsdal, "Digital twin: Values, challenges and enablers from a modeling perspective," IEEE Access, vol. 8, pp. 21980–22012, 2020, doi: 10.1109/ACCESS.2020.2970143.

[17] F. Tao and Q. Qi, "Make more digital twins," Nature, vol. 573, no. 7775, pp. 490–491, 2019, doi: 10.1038/d41586-019-02849-1.

[18] Executive Office of the President of the United States, "National cybersecurity strategy," 2023. [Online]. Available: https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf

[19] R. Vargas, R. S. Miani, J. A. de Sousa, and T. C. M. B. de Carvalho, "A systematic review on digital twin for networking, communications and cyber security," Sensors, vol. 21, no. 17, Art. no. 5878, 2021, doi: 10.3390/s21175878.

[20] X. Wang, Y. Zhang, Z. Li, et al., "Machine and deep learning for digital twin networks: A survey," IEEE Internet of Things Journal, vol. 11, no. 21, pp. 34694–34716, 2024, doi: 10.1109/JIOT.2024.3416733.

[21] J. Zdravkovic, R. Seiger, K. Sandkuhl, et al., "Artificial intelligence in digital twins—A systematic literature review," Data & Knowledge Engineering, vol. 151, Art. no. 102304, 2024, doi: 10.1016/j.datak.2024.102304.

[22] Y. Zhang, S. Alqahtani, et al., "A comprehensive survey of digital twins: Applications, technologies and security challenges," Journal of Systems Architecture, vol. 151, Art. no. 103120, 2024, doi: 10.1016/j.sysarc.2024.103120.