

An AI-Enhanced Digital Twin Framework for Experiential Cybersecurity Education

Biju Bajracharya
bajracharya@etsu.edu

Mohammad Moin Uddin
uddinm@etsu.edu

Robert Brown
brownr3@etsu.edu

Eastern Tennessee State University
Johnson City, TN 37614

Abstract

The increasing convergence of Digital Twins (DTs), Cyber-Physical Systems (CPS), the Internet of Things (IoT), and Artificial Intelligence (AI) is transforming critical infrastructure and creating new educational requirements for preparing cybersecurity professionals. Although digital twins and AI have demonstrated significant potential for monitoring, simulation, and intelligent decision support, existing educational platforms typically focus on isolated technologies or implementation-specific solutions without providing a unified framework for integrating these capabilities into cybersecurity education. This paper proposes an AI-enhanced digital twin framework that integrates IoT sensing, digital twin visualization, and AI-assisted analytics within a unified educational environment to support experiential cybersecurity learning and workforce preparation. To facilitate practical adoption, the paper introduces a modular, technology-agnostic reference architecture that separates educational objectives from implementation technologies, enabling the framework to be adapted across diverse hardware platforms, cloud infrastructures, and instructional settings. The feasibility of the proposed framework is demonstrated through a proof-of-concept implementation deployed in an academic building using distributed ESP32 sensing nodes, MQTT-based communication, cloud data management, and Autodesk Platform Services (APS), while establishing the data infrastructure required for future AI-assisted analytics. The proposed framework provides educators with a scalable and extensible foundation for developing immersive cyber-physical learning environments that bridge theoretical cybersecurity concepts with hands-on experimentation, while supporting the preparation of students for securing increasingly intelligent and interconnected cyber-physical systems.

Keywords: Digital Twin, Cyber-Physical Systems, Cybersecurity Education, Artificial Intelligence, Internet of Things, Smart Buildings, Experiential Learning, Workforce Development.

An AI-Enhanced Digital Twin Framework for Experiential Cybersecurity Education

Biju Bajracharya, Mohammad Moin Uddin and Robert Brown

1. INTRODUCTION

The rapid convergence of Digital Twins (DTs), Cyber-Physical Systems (CPS), the Internet of Things (IoT), and Artificial Intelligence (AI) is transforming the design, operation, and security of critical infrastructure, smart buildings, industrial control systems, and intelligent manufacturing environments (Lee et al., 2015; Rajkumar et al., 2010; Atzori et al., 2010; Barricelli et al., 2019; Fuller et al., 2020). Digital twins provide continuously synchronized virtual representations of physical assets, enabling real-time monitoring, simulation, predictive analytics, and operational decision support throughout the system lifecycle (Barricelli et al., 2019; Boje et al., 2020). Advances in AI have enhanced cyber-physical systems through intelligent data analysis, anomaly detection, predictive maintenance, and adaptive decision support (Russell & Norvig, 2021; National Institute of Standards and Technology [NIST], 2023; Zawacki-Richter et al., 2019). As these technologies become increasingly interconnected, cybersecurity professionals must understand not only traditional information systems but also the interactions among physical processes, sensing infrastructure, communication networks, cloud services, digital twins, and AI-enabled analytics (Gubbi et al., 2013). Preparing students for these emerging environments therefore requires educational platforms that integrate these technologies into realistic, hands-on learning experiences.

Traditional cybersecurity laboratories primarily emphasize isolated technical skills such as network defense, penetration testing, digital forensics, and system administration using virtual machines, cyber ranges, or simulated environments (Joint Task Force, 2017; Jones et al., 2020). While these approaches effectively teach foundational cybersecurity concepts, they generally lack the dynamic interaction between cyber and physical components that characterize modern CPS environments. At the same time, digital twins have gained widespread adoption across manufacturing, smart buildings, healthcare, and critical infrastructure for system monitoring, optimization, and predictive analytics (Barricelli et al., 2019; Boje et al., 2020; Fuller et al., 2020). However, their use within cybersecurity education remains relatively limited, with many existing efforts focusing on demonstrating individual technologies or implementation-specific solutions rather than providing an integrated educational framework that supports experiential learning across the cyber-physical system lifecycle (Joint Task Force, 2017; NIST, 2020).

Artificial intelligence expands the educational potential of digital twins by enabling intelligent interpretation of operational data, anomaly detection, predictive modeling, and decision support (Fuller et al., 2020; Grieves & Vickers, 2017). Beyond its operational capabilities, AI is increasingly recognized as an educational assistant that can support guided investigation, personalized learning, and higher-order reasoning while maintaining human oversight and critical evaluation (UNESCO, 2023; Kasneci et al., 2023; Zawacki-Richter et al., 2019). Rather than replacing human decision-making, AI can augment student learning by assisting in the interpretation of complex cyber-physical data while encouraging students to validate AI-generated recommendations using engineering judgment and cybersecurity principles. Integrating AI with digital twin technologies therefore creates opportunities for immersive educational environments in which students can investigate cyber-physical interactions, analyze cybersecurity incidents, and understand the operational consequences of cyberattacks within realistic CPS settings.

Although significant advances have been made in digital twins, cyber-physical systems, AI-assisted analytics, and cybersecurity education, these research areas have largely evolved independently. Existing educational platforms typically emphasize isolated laboratory exercises, while digital twin research primarily targets industrial monitoring and operational optimization (Barricelli et al., 2019; Kasneci et al., 2023; Kolb, 2015). Consequently, there remains a lack of a unified educational framework that integrates CPS, IoT, digital twins, AI-assisted analytics, and cybersecurity experimentation within

a modular architecture that can be adapted across different educational institutions, hardware platforms, and application domains. Addressing this gap requires an approach that clearly separates educational objectives from implementation technologies while maintaining a structured pathway from conceptual framework to practical deployment.

To address these challenges, this paper proposes an AI-enhanced digital twin framework that integrates CPS, IoT, digital twins, and AI for cybersecurity education. This framework integrates cyber-physical systems, IoT technologies, digital twin visualization, and AI-assisted analytics to support immersive, hands-on cybersecurity learning. To facilitate practical adoption, the paper introduces a modular, technology-agnostic reference architecture that supports implementation guidance while remaining adaptable to diverse technologies and instructional environments. Finally, the feasibility of this framework is demonstrated through a prototype implementation that integrates distributed IoT sensing, secure MQTT-based communication, cloud-based data management, Autodesk Platform Services (APS) (Autodesk, 2025), while establishing the data infrastructure required for future AI-assisted analytics.

The primary contributions of this paper are summarized as follows:

- An AI-enhanced Digital Twin Framework that integrates IoT technologies, cyber physical systems, and artificial intelligence into a unified educational platform for cybersecurity education.
- A modular, technology-agnostic reference architecture that offers implementation guidance while remaining adaptable to different hardware platforms, software technologies, and educational environments.
- A proof-of-concept implementation that demonstrates the practical feasibility of the proposed framework through distributed IoT sensing, cloud services, and digital twin visualization, while establishing the infrastructure required for future AI-assisted analytics.
- A scalable educational platform that supports experiential cybersecurity learning and prepares students to design, analyze, and secure modern cyber-physical systems.

The remainder of this paper is organized as follows. Section 2 reviews related work on digital twins, cyber-physical systems, artificial intelligence, and cybersecurity education. Section 3 presents the proposed AI-enhanced Digital Twin Framework. Section 4 describes technology-agnostic reference architecture. Section 5 presents the prototype implementation and feasibility demonstration. Section 6 discusses the framework's implications, limitations, and future research directions. Finally, Section 7 concludes the paper.

2. RELATED WORK

2.1 Digital Twins for Cyber-Physical Systems

Digital twins have emerged as a key enabling technology for Industry 4.0 by providing continuously synchronized virtual representations of physical systems throughout their operational lifecycle (Grieves & Vickers, 2017; Barricelli et al., 2019; Fuller et al., 2020; Jones et al., 2020; Liu et al., 2021). Coupled with Internet of Things (IoT) sensing, cloud computing, and real-time data analytics, digital twins enable continuous monitoring, predictive maintenance, operational optimization, and informed decision-making across manufacturing, energy systems, healthcare, transportation, and smart infrastructure. Recent advances in digital twin-driven smart manufacturing demonstrate the integration of IoT, cloud computing, and intelligent analytics (Tao et al., 2019). Recent surveys identify digital twins as an essential component of intelligent cyber-physical systems capable of integrating physical assets with computational models for real-time system awareness and control (Fuller et al., 2020; Jones et al., 2020; Barricelli et al., 2019; Liu et al., 2021).

Within smart buildings, digital twins have been combined with Building Information Modeling (BIM), IoT sensor networks, and cloud-based platforms to monitor occupancy, environmental conditions, energy consumption, and facility operations (Boje et al., 2020; Liu et al., 2021). These implementations demonstrate the effectiveness of digital twins for operational management and visualization; however, they primarily target facility optimization rather than cybersecurity education. Consequently, while digital twin research establishes a strong technological foundation, relatively few studies have explored their use as immersive educational environments that promote cybersecurity investigation, cyber-physical experimentation, and workforce preparation.

2.2 Artificial Intelligence in Cybersecurity and Education

Artificial intelligence has become an increasingly important component of modern cybersecurity by supporting anomaly detection, malware analysis, threat intelligence, intrusion detection, behavioral analytics, and automated decision support (NIST, 2023; ENISA, 2023; Russell & Norvig, 2021). More recently, generative AI and large language models (LLMs) have demonstrated considerable potential for assisting cybersecurity analysts by summarizing security events, explaining attack behaviors, generating defensive recommendations, and supporting incident response workflows (Kasneci et al., 2023; UNESCO, 2023). These capabilities have expanded the role of AI from operational automation to intelligent decision support for complex cyber-physical environments.

Beyond cybersecurity operations, AI is also transforming higher education through intelligent tutoring systems, adaptive learning, personalized feedback, and collaborative problem solving (Zawacki-Richter et al., 2019; Kasneci et al., 2023; UNESCO, 2023). Rather than replacing human expertise, current educational research emphasizes human-centered AI that augments student learning while encouraging critical evaluation and evidence-based reasoning. This perspective is particularly relevant for cybersecurity education, where students must learn to interpret complex operational data, validate AI-generated recommendations, and understand the limitations of automated analysis. The integration of AI with digital twin technologies therefore presents an opportunity to create immersive educational environments that combine real-time cyber-physical visualization with intelligent learning support.

2.3 Cybersecurity Education and Educational Cyber-Physical Platforms

Experiential learning has long been recognized as a fundamental component of cybersecurity education because it enables students to apply theoretical concepts through practical investigation and experimentation (Kolb, 2015; Joint Task Force, 2017). Existing educational platforms include cyber ranges, virtual laboratories, industrial control system (ICS) testbeds, capture-the-flag (CTF) competitions, and smart campus environments (NIST, 2020, 2023). These environments expose students to networking, operating systems, industrial protocols, and cybersecurity tools while providing realistic opportunities to develop technical skills.

Recent advances have extended these environments by incorporating IoT devices, cloud computing, and digital twin technologies to create more realistic cyber-physical learning platforms (Boje et al., 2020; Liu et al., 2021; Jones et al., 2020). Smart campus initiatives and digital twin-enabled educational laboratories have demonstrated the value of integrating real-time sensing and visualization into classroom instruction. However, these implementations are typically developed for specific applications or institutional deployments and often lack a generalized educational framework that clearly separates pedagogical objectives, architectural design, and implementation technologies. As a result, adapting these systems to different hardware platforms, cloud infrastructures, or instructional environments often requires substantial redesign.

To better illustrate the current state of the literature, Table 1 compares representative studies across digital twins, cyber-physical systems, artificial intelligence, and cybersecurity education.

2.4 Research Gap and Motivation

Although prior research has advanced digital twins, cyber-physical systems, artificial intelligence, and experiential cybersecurity education, these areas have largely evolved independently. As summarized in Table 1, existing studies typically emphasize one or two aspects of these domains, such as digital twins for industrial monitoring and operational optimization (Barricelli et al., 2019; Fuller et al., 2020; Jones et al., 2020), AI-assisted cybersecurity and intelligent decision support (Buczak & Guven, 2016; National Institute of Standards and Technology [NIST], 2023), or experiential cybersecurity education through cyber ranges and laboratory environments (Joint Task Force on Cybersecurity Education, 2017; NIST, 2020; NIST, 2023). Few studies integrate IoT-enabled cyber-physical systems, digital twins, AI-assisted analytics and decision support, and cybersecurity experimentation within a unified educational framework. Most existing implementations are tightly coupled with specific hardware platforms or software technologies and do not distinguish between educational objectives, architectural design, and implementation, making adaptation to other institutions or application domains more difficult.

Table 1. Comparison of Representative Studies Related to Digital Twins, Cyber-Physical Systems, AI, and Cybersecurity Education

Reference	Primary Focus	IoT	Digital Twin	AI-Assisted Analytics	AI-Assisted Learning	Cyber security	Educational Focus	Modular Framework	Reference Architecture
Lee et al. (2015)	CPS architecture for Industry 4.0	✓	X	X	X	X	X	✓	✓
Tao et al. (2019)	Digital twin-driven smart manufacturing	✓	✓	Partial	X	X	X	Partial	X
Fuller et al. (2020)	Digital twin survey	✓	✓	Partial	X	X	X	X	X
Jones et al. (2020)	Digital twin taxonomy	✓	✓	X	X	X	X	Partial	X
NIST CPS Framework (2018)	CPS reference framework	✓	X	X	X	✓	X	✓	✓
NIST AI RMF (2023)	AI risk management	X	X	✓	X	✓	X	✓	X
ACM/IEEE Cybersecurity Curricula (2017)	Cybersecurity curriculum guidance	X	X	X	X	✓	✓	Partial	X
NICE Workforce Framework (2020)	Workforce competency framework	X	X	X	X	✓	✓	X	X
This work (Proposed Framework)	AI-enhanced Digital Twin Framework for cybersecurity education	✓	✓	✓	✓	✓	✓	✓	✓

To address these limitations, this paper proposes an AI-enhanced Digital Twin Framework that separates three complementary perspectives: (1) a conceptual educational framework that defines the learning process, (2) a modular, technology-agnostic reference architecture that guides system design, and (3) a prototype implementation that demonstrates practical feasibility. This separation enables institutions to adopt the framework using different sensing technologies, communication infrastructures, cloud platforms, digital twin solutions, and AI services while preserving a consistent educational foundation.

The framework is designed to support scalable deployment for integrating cyber-physical systems, digital twins, and AI into immersive cybersecurity education and workforce preparation.

3. AI-ENHANCED DIGITAL TWIN CYBER-PHYSICAL SYSTEMS FRAMEWORK

The AI-enhanced Digital Twin Framework provides a modular and extensible experiential learning environment designed to prepare students for securing modern intelligent cyber-physical systems. Rather than functioning solely as a technical platform, the framework serves as an educational model that integrates cyber-physical systems, digital twin technology, artificial intelligence (AI), and hands-on cybersecurity experimentation into a cohesive learning ecosystem. As illustrated in Figure 1, the framework comprises seven interconnected educational components that collectively guide students through an experiential cybersecurity learning process. Beginning with a physical operational environment, learners acquire real-time operational data, interact with a synchronized digital twin, conduct cybersecurity experiments, apply AI-assisted analytics to interpret system behavior, investigate and respond to cybersecurity incidents, and ultimately develop workforce competencies through reflection and assessment. Because the framework is modular and technology-agnostic, it can be integrated into existing cybersecurity, networking, cloud computing, Internet of Things (IoT), artificial intelligence, scripting, and systems administration courses without requiring the development of a standalone digital twin curriculum.

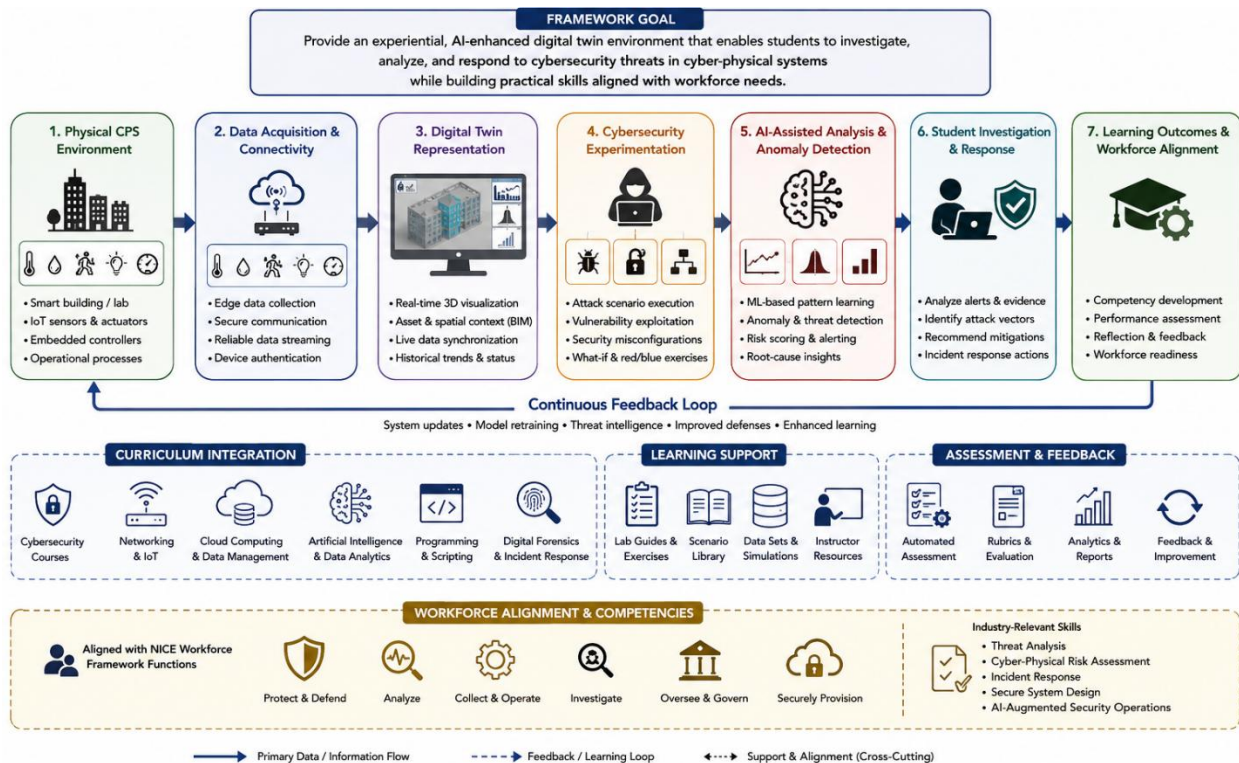


Figure 1: AI-Enhanced Digital Twin Framework for Experiential Cybersecurity Education

3.1 Physical Cyber-Physical System Layer

The Cyber-Physical System (CPS) Environment provides the physical context in which cybersecurity learning activities occur. This component represents the operational infrastructure commonly found in intelligent buildings, industrial automation, smart campuses, healthcare facilities, and other connected environments. Physical assets consist of embedded controllers, IoT sensors, actuators, environmental monitoring devices, and network-connected equipment that continuously generate operational data describing the state of the physical environment (Gubbi et al., 2013; Joint Task Force, 2017).

Compared with software-only cybersecurity laboratories, the framework allows students to understand how cyberattacks can directly influence physical processes. Learners observe relationships between sensor measurements, device behavior, and system operations while developing an appreciation for the unique security challenges associated with cyber-physical environments. This component therefore serves as the foundation for realistic cybersecurity experimentation throughout the framework.

3.2 Data Acquisition and Connectivity

The Data Acquisition and Connectivity component enables reliable collection, transmission, and synchronization of operational data between physical devices and digital services. Sensor observations are continuously acquired by distributed edge devices and transmitted through secure communication services to the digital twin environment. This component abstracts the underlying communication technologies while emphasizing secure messaging, authentication, device management, and reliable data exchange across distributed cyber-physical systems (Jones et al., 2020).

From an educational perspective, students investigate how communication protocols, authentication mechanisms, encryption, and network services influence the security and reliability of cyber-physical environments. Representative laboratory activities include analyzing communication traffic, evaluating authentication mechanisms, investigating message integrity, and exploring attacks targeting connected IoT devices.

3.3 Digital Twin Representation

The Digital Twin Representation serves as the central visualization and situational awareness component of our framework. Operational data collected from the physical environment are synchronized with a virtual representation that continuously reflects the current state of the cyber-physical system. Through interactive visualization, students observe system behavior, monitor device status, examine historical operational trends, and evaluate the effects of cybersecurity events within an intuitive digital environment (Barricelli et al., 2019; Fuller et al., 2020; Jones et al., 2020; Liu et al., 2021).

While traditional dashboards display isolated sensor values, the digital twin integrates spatial information, asset relationships, and real-time operational data into a unified representation of the cyber-physical system. This capability enables students to better understand how cyber incidents propagate across interconnected physical and digital components while providing instructors with an effective platform for demonstrating complex cybersecurity concepts.

3.4 Cybersecurity Experimentation

The Cybersecurity Experimentation component offers a controlled environment in which students investigate realistic attack and defense scenarios involving cyber-physical systems. Laboratory exercises are designed to simulate common security threats including sensor spoofing, false data injection, unauthorized device access, insecure communication channels, denial-of-service attacks, access control violations, and network reconnaissance (NIST, 2023; Rajkumar et al., 2010).

Because experimentation occurs within a controlled educational environment, students can safely observe how cybersecurity incidents influence both physical operations and their corresponding digital twin representations. This experiential approach encourages active learning while allowing instructors to progressively introduce increasingly sophisticated attack scenarios that align with course learning outcomes.

3.5 AI-Assisted Analysis and Anomaly Detection

Artificial intelligence extends the capabilities of the framework by enabling automated analysis of operational and cybersecurity data. AI models continuously analyze system behavior to establish baseline operational patterns, identify anomalies, evaluate cybersecurity alerts, and provide decision-support recommendations (Russell & Norvig, 2021; NIST, 2023; Kasneci et al., 2023; UNESCO, 2023). Rather than replacing human analysis, AI functions as an intelligent assistant that helps students recognize abnormal conditions and interpret complex cyber-physical behaviors.

Students gain practical experience preparing datasets, selecting machine learning techniques, evaluating anomaly detection performance, interpreting AI-generated alerts, and comparing automated predictions with observed system behavior. These activities expose learners to modern AI-assisted cybersecurity techniques increasingly employed in industrial monitoring systems and security operations centers.

3.6 Student Investigation and Response

Following AI-assisted analysis, students transition from automated system outputs to human-centered investigation and decision making. In this phase, learners examine AI-generated alerts, analyze digital twin visualizations, correlate system events across multiple data sources, identify probable attack vectors, and evaluate the potential impact of cybersecurity incidents on both digital and physical system operations. Rather than relying solely on automated recommendations, students are encouraged to validate findings, interpret evidence, and formulate appropriate mitigation and response strategies using established cybersecurity principles.

This component emphasizes critical thinking, analytical reasoning, and collaborative problem solving. Students perform activities such as incident investigation, log and network traffic analysis, root-cause identification, risk assessment, and incident response planning while documenting their observations and recommended actions. By integrating AI-assisted insights with human expertise, the framework reinforces the importance of informed decision making and prepares learners to address the complex challenges encountered in modern cyber-physical environments.

3.7 Learning Outcomes & Workforce Development

The final component translates hands-on cybersecurity experiences into measurable educational outcomes and workforce competencies. Through repeated cycles of observation, experimentation, analysis, investigation, and response, students develop practical skills in cyber-physical system security, digital twin technologies, AI-assisted cybersecurity operations, threat analysis, anomaly detection, and incident response. These experiences foster not only technical proficiency but also critical thinking, communication, collaboration, and evidence-based decision making, all of which are essential for cybersecurity professionals.

The framework is designed to support seamless integration into undergraduate and graduate cybersecurity curricula while aligning laboratory activities with the competencies defined in the NICE Workforce Framework and the Cybersecurity Curricula 2017 guidelines (Joint Task Force on Cybersecurity Education, 2017; NIST, 2020). Because the framework is modular and adaptable, instructors can incorporate individual components or the complete learning cycle into courses covering cybersecurity, networking, Internet of Things (IoT), cloud computing, artificial intelligence, and cyber-physical systems. Hence, our framework extends beyond a technical laboratory platform by providing a structured educational model that prepares graduates for emerging cybersecurity roles involving intelligent, connected, and AI-enabled cyber-physical infrastructures.

While Section 3 introduced the proposed framework from an educational perspective, effective implementation requires an underlying technical infrastructure capable of supporting cyber-physical interaction, real-time data acquisition, digital twin synchronization, AI-assisted analytics, and experiential learning activities. The following section presents a layered reference architecture that operationalizes the framework while remaining modular, extensible, and technology-agnostic.

4. REFERENCE ARCHITECTURE FOR THE AI-ENHANCED DIGITAL TWIN FRAMEWORK

While Section 3 presented the AI-enhanced Digital Twin Framework from an educational perspective, practical deployment requires an underlying architecture capable of supporting real-time data acquisition, secure communication, digital twin synchronization, AI-assisted analysis, and interactive learning activities (Jones et al., 2020; Liu et al., 2021; Gubbi et al., 2013). This architecture draws upon established principles from cyber-physical systems, IoT architectures, cloud-edge computing, digital twin technologies and AI-Assisted analytics (Lee et al., 2015; Rajkumar et al., 2010; Atzori et al., 2010;

Gubbi et al., 2013; Barricelli et al., 2019; Fuller et al., 2020; Jones et al., 2020; Russell & Norvig, 2021; NIST, 2023), while extending these concepts into a unified platform specifically designed to support cybersecurity education and workforce development.

The architecture separates system functionality into seven logical layers that collectively support data acquisition, processing, visualization, cybersecurity experimentation, and educational applications. This layered organization improves modularity, scalability, maintainability, and interoperability by allowing individual components to evolve independently while preserving well-defined interfaces between architectural layers (Gubbi et al., 2013; Atzori et al., 2010). Because the architecture is technology-agnostic, institutions can implement the framework using different hardware platforms, communication protocols, cloud infrastructures, digital twin platforms, and AI services according to their available resources and instructional objectives.

While traditional IoT architectures primarily focus on data collection and system monitoring (Atzori et al., 2010; Gubbi et al., 2013), our architecture is specifically designed to support cybersecurity education. In addition to managing operational data, it facilitates cybersecurity experimentation, AI-assisted analysis, student investigation, and experiential learning while integrating continuous educational feedback throughout the learning process.

Figure 2 also illustrates two cross-cutting elements that span the entire architecture. The Educational Feedback Loop enables continuous interaction between instructors, students, and laboratory activities by supporting observation, experimentation, investigation, reflection, and iterative learning. The Cross-Cutting Security and Operational Considerations ensure that security, privacy, reliability, scalability, monitoring, and system management are incorporated throughout every architectural layer rather than treated as isolated components.

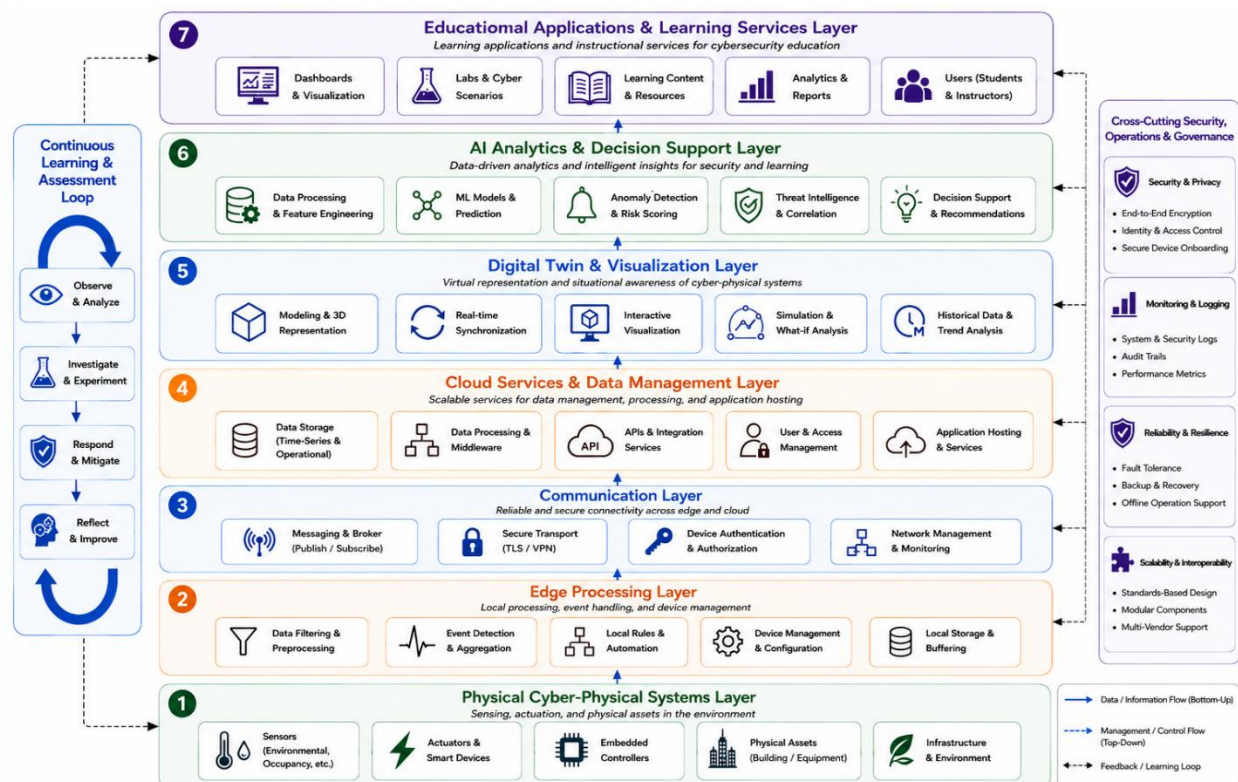


Figure 2: Layered Reference Architecture Supporting the Proposed AI-Enhanced Digital Twin Framework

4.1 Physical Cyber-Physical Systems Layer

The Physical Cyber-Physical Systems layer represents the operational environment in which cybersecurity learning activities take place. This layer includes physical assets such as embedded controllers, sensors, actuators, industrial devices, environmental monitoring systems, and other network-connected equipment commonly found in modern cyber-physical infrastructures (Rajkumar et al., 2010; Lee et al., 2015). These devices continuously generate operational data that reflects the current state of the physical environment and provides the foundation for cybersecurity experimentation. By interacting with physical devices rather than simulated datasets alone, students gain a deeper understanding of how cybersecurity incidents affect real-world operational systems and their associated digital infrastructure.

4.2 Edge Processing Layer

The Edge Processing layer performs local processing of sensor data before transmission to higher architectural layers. Typical responsibilities include data filtering, preprocessing, event detection, local decision making, temporary buffering, and device management. Performing selected computations near the physical devices reduces communication overhead (Gubbi et al., 2013), improves responsiveness, and enables efficient operation under distributed deployment conditions.

From an educational perspective, this layer allows students to investigate edge computing concepts while exploring how local processing influences system performance, security, and resilience.

4.3 Communication Layer

The Communication layer provides reliable and secure information exchange between distributed system components. Its primary responsibilities include message transport, authentication, encryption, device connectivity, and communication monitoring. By abstracting communication services from higher-level applications, the architecture remains independent of any specific networking technology or messaging protocol. Students can use this layer to investigate communication security, protocol behavior, authentication mechanisms, message integrity, and network-based cyberattacks targeting connected cyber-physical systems.

4.4 Cloud Services and Data Management Layer

The Cloud Services and Data Management layer provides centralized computing resources responsible for data storage, middleware services, application programming interfaces (APIs), user management, and system integration. This layer aggregates operational data from distributed edge devices while supporting long-term storage, historical analysis, and coordination among multiple educational services. By separating cloud services and data management from lower architectural layers, the architecture allows computing, storage, and application services to be extended independently as deployment requirements evolve. This separation is designed to support expansion from small laboratory environments to larger educational deployments without requiring changes to the underlying educational framework.

From an educational perspective, this layer enables students to examine how operational data are collected, stored, processed, and accessed across distributed cyber-physical environments. It also provides opportunities to investigate cloud security concepts such as authentication, access control, API security, data protection, logging, and monitoring within the broader context of cyber-physical system security.

4.5 Digital Twin and Visualization Layer

The Digital Twin and Visualization layer maintains a synchronized virtual representation of the physical cyber-physical environment. Operational data collected from physical devices are continuously integrated into the digital twin, allowing students and instructors to monitor system status, visualize device behavior, examine historical trends, and observe the impact of cybersecurity incidents within an interactive environment. Rather than serving as a standalone visualization tool, the digital twin functions as an educational interface that bridges physical infrastructure with cybersecurity analysis, enabling

learners to correlate cyber events with physical system behavior.

4.6 AI Analytics and Intelligence Layer

The AI Analytics and Intelligence layer extends the framework by providing intelligent analysis of operational and cybersecurity data. Machine learning and artificial intelligence techniques analyze system behavior to establish operational baselines, detect anomalies, identify suspicious activities, support predictive analysis, and generate decision-support information.

AI functions as an educational assistant rather than replacing student decision making. Learners critically evaluate AI-generated insights, compare automated predictions with observed evidence, and investigate discrepancies to develop a deeper understanding of AI-assisted cybersecurity operations.

4.7 Educational Applications and Learning Services Layer

The Educational Applications and Learning Services layer provides the primary interface through which instructors and students interact with the framework. This layer supports laboratory exercises, cybersecurity scenarios, assessment activities, dashboards, reporting tools, and instructional resources that facilitate experiential learning. It enables instructors to design progressively challenging cybersecurity activities while providing students with opportunities to investigate realistic cyber-physical security incidents using operational data, digital twin visualizations, and AI-generated analyses.

By integrating technical infrastructure with educational services, this layer transforms the reference architecture from a conventional cyber-physical system into a comprehensive platform for cybersecurity education and workforce development.

4.8 Continuous Learning & Assessment Loop

A distinguishing feature of the reference architecture is the Continuous Learning and Assessment Loop, which extends across all architectural layers to connect system operation with the educational objectives of the framework. As students interact with physical cyber-physical systems, digital twin visualizations, AI-generated insights, and cybersecurity laboratory activities, the architecture continuously supports iterative cycles of observation, investigation, response, reflection, and improvement. Rather than treating laboratory exercises as isolated events, the framework encourages learners to progressively refine their technical understanding and decision-making skills through repeated interaction with increasingly complex cybersecurity scenarios.

The Continuous Learning and Assessment Loop also enables instructors to monitor student progress throughout the learning process. Laboratory activities, cybersecurity investigations, AI-assisted analyses, incident response exercises, and reflective reports provide multiple opportunities for formative assessment while supporting timely instructional feedback. By embedding continuous learning and assessment throughout this architecture, this component operationalizes the educational framework presented in Figure 1, transforming the underlying technical infrastructure into an active learning environment that promotes experiential learning, critical thinking, and workforce readiness. By integrating security, operational, and governance principles across every architectural layer, the architecture provides students with a realistic representation of modern cyber-physical systems while reinforcing the multidisciplinary competencies required for cybersecurity professionals.

4.9 Cross-Cutting Security, Operations, and Governance

While the functional layers each provide specific system capabilities, the Cross-Cutting Security, Operations, and Governance components represent architectural principles that span and influence every layer of reference architecture. Security mechanisms such as authentication, authorization, encryption, privacy protection, secure communication, and access control are incorporated throughout the architecture rather than implemented as isolated services. Similarly, operational functions—including monitoring, logging, auditing, reliability, resilience, scalability, backup, recovery, and lifecycle management—ensure the framework remains secure, maintainable, and adaptable across diverse deployment environments.

Integrating these concerns across all architectural layers provides students with a realistic

representation of professional cybersecurity practice, where securing cyber-physical systems requires coordinated consideration of technology, operations, and organizational governance rather than isolated technical controls. This holistic perspective reinforces the multidisciplinary nature of cybersecurity while preparing learners to design, operate, monitor, and secure intelligent connected infrastructures in real-world environments.

The architecture provides a modular and technology-agnostic blueprint for implementing the AI-enhanced Cyber-Physical Systems Framework introduced in Section 3. By integrating physical cyber-physical systems, edge processing, secure communication, cloud services, digital twin technologies, AI-assisted analytics, and educational learning services within a unified layered architecture, the framework supports realistic cybersecurity “while supporting interoperability, extensibility, and potential expansion across different deployment environments. The Continuous Learning and Assessment Loop and the Cross-Cutting Security, Operations, and Governance components ensure that educational objectives and cybersecurity best practices remain embedded throughout the architecture. The following section demonstrates how this architecture is realized through the development of a prototype cyber-physical systems testbed and illustrates its application in supporting cybersecurity education and workforce development. The proposed architecture therefore offers the technical foundation for realizing the educational framework presented in Section 3 while remaining modular, scalable, and adaptable to diverse instructional environments.

5. Prototype Implementation and Feasibility Demonstration

To demonstrate the practical feasibility of the AI-enhanced Digital Twin Framework and the supporting reference architecture presented in Sections 3 and 4, a proof-of-concept cyber-physical systems (CPS) platform was developed and deployed within an academic building. As illustrated in Figure 3, the prototype realizes the principal implemented components of the conceptual architecture through the integration of distributed IoT sensing, edge computing, secure communication, cloud-based data management, and digital twin visualization, while establishing the data infrastructure required for future AI-assisted analytics. The prototype demonstrates how the framework can be instantiated using commercially available hardware and software technologies while preserving the modular structure and interoperability of the architecture.

The prototype was intentionally constructed using commercially available, relatively low-cost sensing and edge-computing components. The primary physical components consist of ESP32-based sensing nodes and environmental/ToF sensors, while several software components use cloud or platform services. Although a formal cost-effectiveness analysis was outside the scope of this study, the modular architecture allows institutions to select alternative hardware and service tiers based on available resources. Future deployments will evaluate total implementation and operating costs alongside technical and educational outcomes.

The prototype was designed as an educational cyber-physical environment that enables students to investigate cybersecurity incidents, analyze operational data, interact with a real-time digital twin, and evaluate AI-assisted decision support. The prototype therefore serves not only as a functional CPS platform but also as a hands-on learning environment that supports cybersecurity education and workforce development.



Figure 3: Prototype Implementation of the AI-Enhanced Digital Twin Framework

5.1 Physical Cyber-Physical Infrastructure

The physical cyber-physical environment consists of multiple classrooms equipped with distributed environmental and occupancy sensing nodes. Environmental monitoring is performed using ESP32-based sensing devices capable of measuring temperature, humidity, indoor air quality, equivalent carbon dioxide (eCO₂), total volatile organic compounds (TVOC), and ambient light conditions. To preserve occupant privacy while supporting occupancy analysis, doorway activity is monitored using time-of-flight (ToF) sensors that detect entry and exit events without capturing images or personally identifiable information.

The distributed deployment enables continuous monitoring of classroom conditions while providing realistic cyber-physical assets that students can observe, analyze, and interact with during laboratory exercises. The modular hardware design also allows additional sensing devices and CPS components to be incorporated without modifying the overall framework.

5.2 Edge Processing

Each sensing node performs local data acquisition and edge processing before transmitting telemetry to the cloud infrastructure. Edge processing includes sensor sampling, local filtering, occupancy event detection, timestamp generation, and preliminary data validation. Performing these operations at the edge reduces communication overhead while improving system responsiveness and scalability.

Communication between distributed sensing nodes and cloud services is implemented using the MQTT publish-subscribe protocol through a HiveMQ broker with Transport Layer Security (TLS). The publish-subscribe architecture decouples sensing devices from cloud services, allowing heterogeneous devices to exchange information asynchronously while maintaining secure and reliable communication. This modular communication infrastructure also enables new sensing nodes and CPS devices to be added with minimal impact on the existing system.

5.3 Cloud Services and Data Management

The cloud services layer provides centralized coordination of data processing, storage, authentication, and application services. As shown in Figure 3, Node-RED serves as the middleware platform responsible for integrating incoming MQTT messages, processing sensor data streams, and orchestrating communication among distributed system components.

Time-series sensor measurements are stored in InfluxDB to support historical analysis, trend visualization, and long-term data collection. Firebase provides authentication, user management, and metadata storage, while RESTful APIs exposes standardized interfaces that allow web applications and external services to access real-time and historical system information. Separating data acquisition, storage, and application services improves scalability while simplifying future system expansion.

5.4 Digital Twin and AI-Assisted Analytics

The prototype demonstrates the realization of the principal implemented layers of the architecture. ESP32 sensing nodes instantiate the Physical CPS and Edge Processing layers; MQTT and HiveMQ implement the Communication layer; Node-RED, InfluxDB, and Firebase realize the Cloud Services layer; and Autodesk Platform Services provides the Digital Twin and Visualization layer. The resulting data infrastructure also establishes the foundation for future implementation and evaluation of the AI Analytics and Intelligence layer and associated educational applications.

5.5 Educational Applications and Learning Integration

The prototype implementation was specifically designed to support experiential cybersecurity education rather than traditional building management. The prototype is designed to support student interaction across multiple layers of the framework, from physical sensing devices and secure communication networks to cloud services and digital twin visualization, with future extensions incorporating AI-assisted analytics. This end-to-end exposure enables students to understand the relationships among cyber infrastructure, physical processes, and intelligent decision-support systems.

The prototype provides the technical foundation for laboratory activities such as monitoring live CPS operation through the digital twin, analyzing environmental and occupancy data, investigating abnormal sensor behavior, examining communication security, and studying the operational effects of manipulated sensor data. These activities represent intended instructional scenarios supported by the architecture; formal experimental evaluation of attack injection, detection, and response workflows remains part of planned classroom deployment.

From an instructional perspective, the framework also provides instructors with centralized dashboards, system monitoring capabilities, and configurable laboratory scenarios that support classroom demonstrations, guided exercises, and project-based learning. The modular design allows additional AI models, sensing technologies, and cybersecurity exercises to be incorporated as technologies evolve, supporting adaptation to future curriculum needs.

5.6 Proof-of-Concept Implementation Summary

The proof-of-concept implementation demonstrates that the principal technical layers of the proposed reference architecture can be realized and integrated using commercially available hardware and software technologies. The implementation is intended to establish integration feasibility rather than provide comprehensive performance, scalability, cybersecurity, AI, or educational validation. While the architecture presented in Section 4 remains technology-agnostic, the implementation shown in Figure 3 illustrates one practical realization using ESP32 edge devices, HiveMQ, Node-RED, InfluxDB, Firebase, and Autodesk Platform Services.

The prototype demonstrates the realization of the principal implemented layers of the architecture. ESP32 sensing nodes instantiate the Physical CPS and Edge Processing layers; MQTT and HiveMQ implement the Communication layer; Node-RED, InfluxDB, and Firebase realize the Cloud Services and Data Management layer; and Autodesk Platform Services supports the Digital Twin and Visualization layer. The resulting infrastructure provides the foundation for future implementation and evaluation of

AI-assisted analytics and additional educational services. This mapping demonstrates the feasibility of integrating the principal architectural components while preserving the modularity of the overall framework.

6. Discussion and Future Directions

The proposed AI-enhanced digital twin framework extends traditional cyber-physical system laboratories by integrating real-time IoT sensing, digital twin technologies, and artificial intelligence into a unified educational platform. While conventional laboratory environments often focus on isolated cybersecurity concepts or simulated exercises, this framework enables students to investigate security events within a realistic cyber-physical environment where physical processes, sensing infrastructure, cloud services, and intelligent analytics operate as an interconnected system. This integrated approach better reflects the complexity of modern critical infrastructure and industrial cyber-physical systems encountered in professional practice.

Scalability is treated in this study as an architectural design objective rather than an experimentally validated property. Although the layered architecture allows sensing nodes, data services, and educational applications to be extended independently, systematic evaluation of node capacity, message throughput, communication latency, resource utilization, and concurrent users remains necessary to characterize deployment-scale performance.

A key strength of the framework is its modular and layered architecture. By separating the educational framework (Section 3), the technology-agnostic architecture (Section 4), and the prototype implementation (Section 5), our approach allows educational institutions to adopt the framework using different hardware platforms, communication technologies, cloud services, or visualization tools while preserving the overall system design. Individual components, including sensing devices, middleware, digital twin platforms, and AI models can be replaced or extended without requiring substantial modifications to the remaining architecture. This flexibility improves the framework's long-term sustainability as technologies continue to evolve.

The integration of artificial intelligence distinguishes our framework from existing educational cyber-physical system testbeds. Rather than using AI solely for automation, the framework positions AI as a decision-support tool that assists students in interpreting operational data, identifying anomalies, and evaluating potential cybersecurity incidents. This human-centered approach encourages students to critically assess AI-generated recommendations instead of relying exclusively on automated outputs, thereby reinforcing analytical reasoning and professional decision-making skills.

Although the prototype implementation demonstrates the technical feasibility of the framework, several limitations remain. The current deployment has been evaluated within an academic building using a limited number of sensing modalities and cybersecurity scenarios. Additional validation across larger cyber-physical environments, industrial control systems, and smart manufacturing platforms would demonstrate the framework's generalizability. Similarly, while the architecture supports AI-assisted analytics, future work may investigate advanced machine learning models, large language model (LLM)-based instructional assistants, and autonomous cyber-physical threat detection capabilities to enhance both operational performance and educational effectiveness.

The level of abstraction exposed to learners should also be adaptable to their preparation and instructional level. Introductory learners may interact primarily with visualizations, alerts, and guided investigations, whereas advanced undergraduate or graduate students can work directly with device configurations, communication protocols, data models, AI algorithms, and attack-response mechanisms. Such progressive abstraction can support adoption of the framework across different courses and learner populations.

Access to realistic operational data remains an important challenge for digital twin-based cybersecurity education because industrial organizations may be unable or unwilling to share sensitive operational and security data. The prototype addresses this limitation in part by generating operational data within an institutionally controlled academic environment. Such campus-based testbeds can provide realistic time-series and cyber-physical data while avoiding dependence on proprietary industrial datasets. Synthetic and scenario-generated datasets may further complement live data when access to

operational environments is limited.

Near-real-time synchronization also creates opportunities to move cybersecurity learning beyond episodic laboratory exercises toward continuous cyber-risk monitoring and assessment. Students could observe how an enterprise attack surface evolves over time, correlate changes in physical and digital assets with emerging risks, and evaluate defensive decisions as operational conditions change.

Future research will also focus on evaluating the educational impact of the framework through classroom deployment and curriculum integration. Planned studies include the development of structured laboratory exercises, assessment of student engagement and learning outcomes, measurement of cybersecurity competencies, and investigation of how AI-assisted digital twin environments influence problem-solving and workforce readiness. These educational evaluations will provide quantitative evidence regarding the framework's effectiveness in preparing students for careers involving cyber-physical systems, industrial cybersecurity, and critical infrastructure protection.

Future work should also examine standardized cyber-physical data models that combine asset relationships, telemetry, security events, vulnerabilities, and operational context. Such models could provide richer contextual inputs for defensive AI and enable AI systems to reason across both cyber and physical dimensions of an enterprise attack surface.

Future refinement could also map the proposed architecture to standardized digital twin capability models, such as the Digital Twin Consortium's Periodic Table of Digital Twin Capabilities, to provide a common basis for characterizing and comparing educational digital twin implementations.

Overall, this AI-enhanced digital twin framework establishes a scalable foundation for integrating cyber-physical systems, artificial intelligence, and experiential cybersecurity education within a unified instructional environment. By combining modular system architecture with immersive digital twin technologies and intelligent decision support, the framework offers a practical pathway for modernizing cybersecurity education while supporting the workforce demands of increasingly connected and intelligent cyber-physical systems.

Although the proof-of-concept demonstrates that the principal components of the framework can be integrated within an operational academic environment, the present study does not constitute comprehensive technical or educational validation. The current deployment uses a limited number of sensing modalities and has not yet been subjected to systematic scalability, cybersecurity attack-response, AI-model performance, or concurrent-user evaluation. Accordingly, scalability is treated as an architectural design objective rather than a demonstrated performance characteristic. Future technical evaluation will measure sensor-to-cloud and digital-twin update latency, communication reliability, system uptime, resource utilization, message throughput, and supported sensing-node and user capacity. Controlled cybersecurity experiments will further examine attack injection, observable physical and digital effects, detection, investigation, and response. AI capabilities will be evaluated using model-specific metrics such as detection accuracy, false-positive and false-negative rates, and inference performance. These evaluations will complement subsequent classroom studies assessing student engagement, learning outcomes, and workforce competencies.

7. Conclusion

This paper presented an AI-enhanced Digital Twin Framework for cybersecurity education and workforce development that integrates cyber-physical systems (CPS), Internet of Things (IoT) technologies, digital twin visualization, and artificial intelligence within a unified educational environment. To support practical adoption, the paper introduced modular, technology-agnostic reference architecture and demonstrated its feasibility through a proof-of-concept implementation using ESP32-based sensing nodes, MQTT communication, cloud-based data management, and Autodesk Platform Services, while establishing the data infrastructure required for future AI-assisted analytics. By separating the conceptual framework, reference architecture, and implementation, the proposed approach provides a flexible foundation that can be adapted to diverse educational institutions, technologies, and cyber-physical applications.

The proposed framework advances cybersecurity education by bridging theoretical instruction with hands-on cyber-physical system experimentation through immersive digital twin technologies and intelligent decision support. By integrating conceptual design, reference architecture, and prototype implementation into a cohesive educational platform, the framework provides educators with a practical roadmap for developing experiential learning environments that prepare students to analyze, secure, and manage increasingly intelligent and interconnected cyber-physical systems. As digital twins and AI continue to transform critical infrastructure and industry, this framework offers a scalable foundation for modernizing cybersecurity education and strengthening workforce readiness.

8. REFERENCES

- Atzori, L., Iera, A., & Morabito, G. (2010). The internet of things: A survey. *Computer Networks*, 54(15), 2787–2805.
- Autodesk. (2025). Autodesk Platform Services documentation. Autodesk. <https://aps.autodesk.com/developer/documentation/>
- Barricelli, B. R., Casiraghi, E., & Fogli, D. (2019). A survey on digital twin: Definitions, characteristics, applications, and design implications. *IEEE Access*, 7, 167653–167671.
- Boje, C., Guerriero, A., Kubicki, S., & Rezgui, Y. (2020). Towards a semantic construction digital twin. *Automation in Construction*, 114.
- Buczak, A. L., & Guven, E. (2016). A survey of data mining and machine learning methods for cyber security intrusion detection. *IEEE Communications Surveys & Tutorials*, 18(2), 1153–1176.
- European Union Agency for Cybersecurity. (2023). Artificial intelligence cybersecurity challenges.
- Fuller, A., Fan, Z., Day, C., & Barlow, C. (2020). Digital twin: Enabling technologies, challenges and open research. *IEEE Access*, 8, 108952–108971.
- Grieves, M., & Vickers, J. (2017). Digital twin: Mitigating unpredictable, undesirable emergent behavior in complex systems. In *Transdisciplinary perspectives on complex systems*. Springer.
- Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of things (IoT): A vision, architectural elements, and future directions. *Future Generation Computer Systems*, 29(7), 1645–1660.
- Joint Task Force on Cybersecurity Education. (2017). Cybersecurity curricula 2017. ACM/IEEE Computer Society.
- Jones, D., Snider, C., Nassehi, A., Yon, J., & Hicks, B. (2020). Characterising the digital twin: A systematic literature review. *CIRP Journal of Manufacturing Science and Technology*, 29, 36–52.
- Kasneci, E., et al. (2023). ChatGPT for good? On opportunities and challenges of large language models for education. *Learning and Individual Differences*, 103.
- Kolb, D. A. (2015). *Experiential learning: Experience as the source of learning and development* (2nd ed.). Pearson.
- Lee, J., Bagheri, B., & Kao, H.-A. (2015). A cyber-physical systems architecture for Industry 4.0-based manufacturing systems. *Manufacturing Letters*, 3, 18–23.
- Liu, M., Fang, S., Dong, H., & Xu, C. (2021). Review of digital twin about concepts, technologies, and industrial applications. *Journal of Manufacturing Systems*, 58, 346–361.

- National Institute of Standards and Technology. (2018). Framework for cyber-physical systems (CPS framework) (Version 1.0).
- National Institute of Standards and Technology. (2020). Special Publication 800-181 Revision 1: Workforce framework for cybersecurity (NICE Framework).
- National Institute of Standards and Technology. (2023). Artificial intelligence risk management framework (AI RMF 1.0) (NIST AI 100-1).
- Rajkumar, R., Lee, I., Sha, L., & Stankovic, J. (2010). Cyber-physical systems: The next computing revolution. In Proceedings of the 47th Design Automation Conference (pp. 731–736).
- Russell, S., & Norvig, P. (2021). Artificial intelligence: A modern approach (4th ed.). Pearson.
- Tao, F., Zhang, H., Liu, A., & Nee, A. Y. C. (2019). Digital twin in industry: State-of-the-art. IEEE Transactions on Industrial Informatics.
- UNESCO. (2023). Guidance for generative AI in education and research.
- Zawacki-Richter, O., Marín, V. I., Bond, M., & Gouverneur, F. (2019). Systematic review of research on artificial intelligence applications in higher education. International Journal of Educational Technology in Higher Education, 16, Article 39.