Review

Not peer-reviewed version

Cyber Security Education by integrating Digital Twins and Generative AI

Atharv S. Avhad *

Posted Date: 18 November 2025

doi: 10.20944/preprints202511.1203.v1

Keywords: cybersecurity; Cyber-Physical Systems (CPS); Digital Twins (DTs); Generative Artificial Intelligence (Gen AI); Large Language Models (LLMs); Internet of Things (IoT); Operational Technologies (OT); Generative Adversarial Networks(GANs); Intrusion Detection Systems (IDS); Security Operations Center(SOC); PentestGPT; hacking; malware; phishing attacks; cyber attacks

 doi:10.20944/preprints202511.1203.v1

Review

Cyber Security Education by Integrating Digital Twins and Generative AI

Atharv S. Avhad

Department of Information Technology, Pune Institute of Computer Technology (PICT), India; avhadatharv587@gmail.com

Abstract

Cybersecurity is the practice of protecting digital system from cyber threats such as hacking, malware, and phishing attacks. It helps in protecting from the Cyber-attacks through different strategies like Antivirus software etc. Cyber Physical Systems (CPS) rely on advanced communication. Cyber Physical Systems (CPS) control technologies to efficiently manage d evices. It also helps the flow of information in the system. However, it has limitations with respect to modifying physical configuration and difficulty to s cale. Cyber Physical Systems (CPS) is controlled through offline mode by different experts for different Cyber attacks on Cyber Physical Systems (CPS). Cyber attacks are getting more advanced and lethal. Traditional pedagogical approaches often struggle to simulate real-world cybersecurity challenges, limiting experiential learning. To overcome this shortcoming , using the Digital Twins (DTs) and Generative Artificial Intelligence (Gen AI).The rapid advancement in Digital Twins (DTs) and Generative Artificial Intelligence (Gen AI). Integration of Digital Twins (DTs) and Generative Artificial Intelligence (Gen AI). cybersecurity management is Particularly in fields that require analytical reasoning and regulatory compliance. enhancing standards to support cybersecurity, and ensuring Digital Twins (DTs) and Generative Artificial Intelligence (Gen AI) can be fully integrated in Cybersecurity. The developed twin has advanced features compared to any equivalent system in the literature When coupled with Generative Artificial Intelligence (Gen AI) models for C ybersecurity. Large Language Models (LLMs) further enhance the experience by generating threat narratives, adaptive feedback, and role-based attack defense scenarios.

Keywords: cybersecurity; Cyber-Physical Systems (CPS); Digital Twins (DTs); Generative Artificial Intelligence (Gen AI); Large Language Models (LLMs); Internet of Things (IoT); Operational Technologies (OT); Generative Adversarial Networks(GANs); Intrusion Detection Systems (IDS); Security Operations Center(SOC); PentestGPT; hacking; malware; phishing attacks; cyber attacks

1. Introduction

As cyber threats become more complex in today's digital world, cybersecurity education needs to move from just teaching theory to providing hands-on, practical learning, which helping to learner in getting the cybersecurity education using real life scenarios, results in increasing the cyber security. Traditional teaching methods often do not prepare students for real-life cyberattacks, which are becoming more sophisticated and multidimensional [3,4]. As cyber-physical systems (CPS), Internet of Things (IoT) networks and operational technologies (OT) continue to integrate, it is becoming increasingly important to create training environment that are immersive, flexible, repeatable and scalable to meet evolving security needs which is a challenge for cybersecurity education [2,5].

Digital Twins (DTs) technology which offers a solution by creating virtual replica of physical systems. These twins enable real-time monitoring, simulation, and analysis of cyber environments, allowing learners to engage with realistic attack scenarios without compromising actual infrastructure of physical system [7,8]. Digital Twins (DTs) have been successfully applied across industries from manufacturing, smart cities to healthcare and energy systems for predictive maintenance applied in

 doi:10.20944/preprints202511.1203.v1

nuclear power house and chemical factories by anomaly detection and system optimization [10,15]. In cybersecurity education, Digital Twins (DTs) provide a safe and controlled platform for simulating threats, testing defenses and rehearsing incident response strategies in safer way than traditional education in cybersecurity [9,24].

Complementing Digital Twins (DTs) is the rise of Generative Artificial Intelligence (Gen AI), particularly through Large Language Models (LLMs) and Generative Adversarial Networks(GANs). These models can interpret system behaviors and generate threat narratives and also provide adaptive feedback to learners. It offers real-time visibility into the system's operations. Tools like PentestGPT and PentestAgent show how large language models (LLMs) can help to automate penetration testing, find security weaknesses and support red/blue team exercises. [6,23].Large Language Models (LLMs) make cybersecurity learning easier by turning complex technical data into simple, easy to understand information. This helps learners better understand how systems work, think more critically and make smarter decisions in changing cyber environments helps in education [11,13].

Together, Digital Twin (DT) and Generative Artificial Intelligence (Gen AI) redefine the core pillars of cybersecurity education detection, response and prevention. This synergy enables learners to engage in realistic, scenario based training that bridges the gap between theoretical knowledge and operational readiness, ultimately cultivating a new generation of cybersecurity professionals equipped for the digital age.

2. Digital Twins (DTs) and Generative Artificial Intelligence (Gen AI) in Cybersecurity

In cybersecurity education, Digital Twins (DTs) provide immersive environments that replicate information technology(IT) and Operational Technologies (OT) infrastructures, enabling learners to engage with simulated cyberattacks such as phishing, ransomware and zero-day exploits without risking real systems [3,4].Generative Artificial Intelligence (Gen AI) enhances this experience by tailoring attack complexity to learner skill levels and generating contextual feedback using LLMs. These models interpret system behavior, generate threat narratives and support red/blue team exercises. The red team acts like attackers to test a system defenses, while the blue team works to detect and stop those attacks. [11,19].

This table represents an overview of modern digital technologies such as Cyber-Physical Systems (CPS), Digital Twins (DT), Generative Artificial Intelligence (Gen AI), Large Language Models (LLMs), Internet of Things (IoT) and Operational Technologies (OT). It highlights how these technologies are being applied in the field of cybersecurity, demonstrating their roles in enhancing education, threat detection, policy automation and system protection and giving the Applications, Methods, Findings, References format which is giving basic idea about .

This mind map shows key technologies used in modern digital and cybersecurity systems. It includes Digital Twins(DTs), which create virtual models of real systems for testing and monitoring, and Generative Artificial Intelligence (Gen AI), which enhances automation and creativity. It also covers Cybersecurity education, Threat detection, Incident response, LLM augmented Security Operations Center(SOC) operations (using Gen AI in security centers), Component criticality analysis (finding weak parts) and CPS (cyber-physical Systems) that connect digital and physical technologies.

 doi:10.20944/preprints202511.1203.v1

Table 1. Applications of Digital Twins (DTs) and Generative Artificial Intelligence (Gen AI) in Cybersecurity.

Application	Method	Findings	Reference
Cybersecurity Education	Digital Twin (DTs) and Generative artificial intelligence (Gen AI)	Simulates cyber-attacks tailored to learner skill level	Lin et al. (2024) [18]
Threat Detection in Smart Cities	Digital Twins (DTs) and Intrusion Detection Systems (IDS)	Detects anomalies and resource impacts in Internet of Things (IoT) systems	El-Hajj (2024) [8]
Policy Generation security automation	Digital Twins (DTs) and Machine Learning (ML)	Automates security policy creation and also helps in reduces human error	Hammar and Stadler (2023) [36]
Semiconductor lifecycle security	Digital Twins (DTs) and Lifecycle Data for Semiconductor	Detects defective chips and root causes of the defect in semiconductor lifestyle	Shaikh et al. (2022) [37]
Combat Counterfeit Detection	AI-Enabled Digital Twins (DTs) and Blockchain for counterfeit Detection	Prevents counterfeit electronics in Block Chains	Hornik and Rachamim (2024) [38]
Data-aided intrusion detection systems in Internet of Things(IOT)	Digital Twins (DTs), Generative artificial intelligence (Gen AI) and Blockchain for Internet of Things (IOT)	Predicts threats and secures data transmission in Data aided Intrusion Detection Systems (IDS)	Alharbi et al. (2024) [40]
Soar4iot: securing Internet of Things (IOT) assets with digital twins for security management	securing Internet of Things (IOT) assets with digital twins for security management (SOAR4IoT) Framework and Digital Twin(DTs)	Automates response and improves coordination using the Soar4iot	Empl et al. (2022) [42]
Cryptographic Side Channel leakage intelligent measurement and assessment	Simulation-Based Digital Twins (DTs)	Identifies leakage points in crypto systems	Yi et al. (2023) [43]

 doi:10.20944/preprints202511.1203.v1

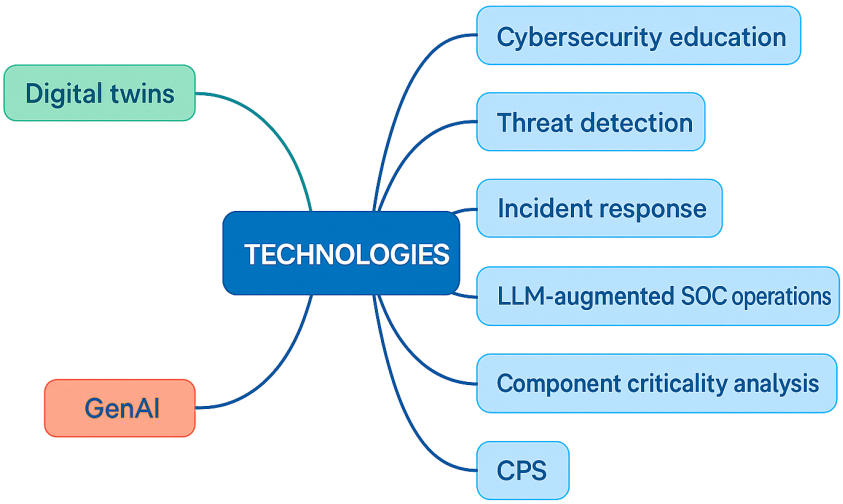

Figure 1. Mind map of Digital Twin (DT) and Generative Artificial Intelligence (Gen AI), Large Language Mode (LLM), and Cyber Physical System (CPS) technologies and their applications

2.1. Digital Twins (DTs) in Cybersecurity Education

Digital Twins (DTs) technology has emerged as a transformative tool in cybersecurity, offering dynamic, real time virtual replicas of physical systems that enable simulation, monitoring and predictive analysis without disrupting operational environments. In cybersecurity contexts, Digital Twins (DTs) are increasingly used to mirror Information Technology (IT), Operational Technologies (OT) and Internet of Things (IoT) infrastructures, allowing organizations to detect vulnerabilities, simulate attack scenarios and evaluate defense mechanisms in a controlled setting in cybersecurity education [4].

One of the most impactful applications of Digital Twins (DTs) is in Cyber security, where they support threat detection, incident response, and forensic analysis. By integrating Digital Twins (DTs) with intrusion detection systems and organizations can visualize system behavior, correlate threat patterns and test mitigation strategies before deploying them in live environments [7,8]. Digital Twins (DTs) also assists shift-left and shift-right security operations, enabling early Security assessment during system design and continuous monitoring during runtime which we are going to discuss in Methodology section [44].

The convergence of Digital Twins (DTs) with Generative Artificial Intelligence (Gen AI) and Large Language Models (LLMs) further enhances cybersecurity capabilities. Large Language Models (LLMs) provide natural language threat interpretation, automate penetration testing workflows, and generate adaptive response strategies [6,23]. This integration supports intelligent Security Operations Center (SOC) workflows and personalized cybersecurity education, bridging the gap between theoretical knowledge and practical application [18].

As cyber threats grow in complexity, Digital Twins (DTs) offer a scalable, intelligent framework for proactive defense, resilience testing, and operational readiness. Their ability to simulate diverse attack vectors and system responses makes them indispensable in modern cybersecurity ecosystems [10,11].

2.2. Generative Artificial Intelligence (Gen AI) in Cybersecurity Education

Generative Artificial Intelligence (Gen AI) is quickly changing the world of cybersecurity. There are many Generative Artificial Intelligence (Gen AI) technologies which are developing for cybersecurity. It helps make security work smarter by using automation, finding new types of threats, and responding faster to attacks. Generative Artificial Intelligence (Gen AI) models especially Large Language Models (LLMs) can write text like humans, understand computer system logs and even

 doi:10.20944/preprints202511.1203.v1

create fake attack situations for testing. This makes them very useful for both protecting systems and studying how hackers might attack them [6,23].

In Security Operations Centers (SOCs),Generative Artificial Intelligence (Gen AI) assists analysts by summarizing alerts, correlating threat indicators and generating contextual explanations of incidents. This reduces cognitive load and accelerates decision-making during high-pressure events [13]. Generative Artificial Intelligence (Gen AI) also supports automated penetration testing workflows, where tools like PentestGPT and PentestAgent use large language models (LLMs) to plan attacks, identify vulnerabilities and suggest strategies [6,23].

Generative Artificial Intelligence (Gen AI) also improves threat intelligence by finding useful information from messy data sources like the internet, dark web forums and social media. It can create fake phishing emails, ransomware and social engineering tricks to help companies test and strengthen their security systems [45].In education,Generative Artificial Intelligence (Gen AI) helps create personalized learning by adjusting cybersecurity education to match each student's skill level and giving instant feedback to help them improve. [18].

Despite its benefits,Generative Artificial Intelligence (Gen AI) also introduces risks. Adversaries can exploit Generative Artificial Intelligence (Gen AI) to automate malware generation, craft convincing phishing campaigns and bypass traditional security filters. Because of this, organizations need to use Generative Artificial Intelligence (Gen AI) carefully. They should include ethical rules and have humans monitor its use to make sure it's safe and used the right way [46].

As cybersecurity threats evolve, Generative Artificial Intelligence (Gen AI) offers a scalable and intelligent framework for proactive defense, continuous monitoring and strategic resilience in education.

2.3. Integration Digital Twins (DTs) and Generative Artificial Intelligence (Gen AI) in Cybersecurity

The integration of Digital Twins (DTs) technology and Generative Artificial Intelligence (Gen AI) is making revolution in cybersecurity by enabling intelligent, adaptive, and scalable security operations which helps in cybersecurity education. Digital Twins (DTs) are virtual representations of physical systems that mirror real-time behavior, allowing for simulation, monitoring and predictive analysis of Cyber-Physical Systems (CPS) [2]. When combined with Generative Artificial Intelligence (Gen AI) particularly Large Language Models (LLMs) these systems evolve from static simulations into dynamic platforms capable of generating realistic threat scenarios and guide for responsive decision making in cyber education [13,18].

Operationally, Digital Twins (DTs) embedded within cybersecurity mesh architectures improve threat detection and incident response by mirroring system behavior and enabling proactive risk modeling [20]. Generative Artificial Intelligence (Gen AI) agents such as PentestGPT and PentestAgent automate penetration testing workflows, assist in vulnerability analysis and simulate attacker tactics through natural language interfaces [6,23]. These agents analyze unstructured data sources including OSINT and dark web forums to extract actionable intelligence and simulate evolving threat landscapes.

The integration between Digital Twins (DTs) and Generative Artificial Intelligence (Gen AI) supports a shift-left and shift-right paradigm in cybersecurity. Shift-left focuses on design time security enhancements, allowing early testing, simulation and vulnerability identification using Generative Artificial Intelligence (Gen AI) [24]. Shift-right emphasizes runtime security operations, where Digital Twins (DTs) continuously monitor system behavior and Generative Artificial Intelligence (Gen AI) agents provide real-time threat analysis and adaptive response strategies [35]. This dual approach ensures that both pre-deployment and operational phases of critical systems are secured and resilient.

Moreover, Digital Twins (DTs) and Generative Artificial Intelligence (Gen AI) are being applied in specialized domains such as ,Internet of Things(IoT) security, supply chain integrity and cryptographic systems. For instance, counterfeit detection in electronics supply chains is being addressed using AI-enabled Digital Twins (DTs) and blockchain technologies [37]. In Internet of Things(IoT) environments, frameworks like SOAR4IoT integrate Digital Twins (DTs) with automated response systems to manage

 doi:10.20944/preprints202511.1203.v1

large-scale device networks securely [41]. In cryptographic systems, Digital Twins (DTs) are used to simulate side channel leakage and thermal attacks, enabling preemptive mitigation strategies [42,43].

This use of Gen AI not only makes systems stronger but also makes cybersecurity learning easier for everyone by giving students and professionals access to advanced tools. It helps train a new generation of cybersecurity experts who have both strong technical skills and smart strategies to handle complex cyber threats confidently and effectively.

3. Methodology

This section outlines the methodological framework adopted to explore the integration of Digital Twins (DTs) and Generative Artificial Intelligence (GenAI) in cybersecurity operations and education. The approach combines architectural modeling, simulation-based validation, and AI-assisted instructional design.

3.1. Digital Twins (DTs) Based Cybersecurity Modeling

Digital Twins (DTs) technology provides a virtual representation of physical systems, enabling real-time monitoring, simulation and predictive analysis. The Shift Left Shift Right (SLSR) paradigm in cybersecurity emphasizes proactive and reactive security operations across the system lifecycle. In the context of Digital Twins (DTs), this approach enables both design-time and runtime protection of Cyber-Physical Systems (CPS).

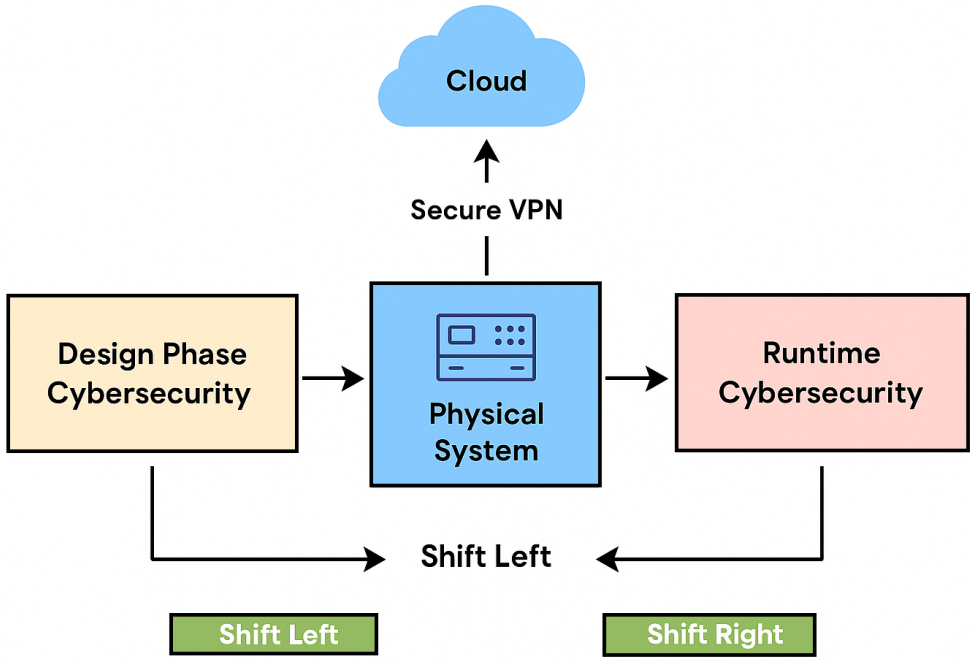

Figure 2. Shift Left Shift Right (SLSR) Paradigm in Digital Twins for Cybersecurity Adapted from [44].

The "Shift Left" aspect focuses on early stage security integration during system design for educational purposes we use it as basics of early stage security. Digital Twins(DTs) simulate system behavior, allowing developers to identify vulnerabilities, test configurations and validate security policies before deployment. This reduces the risk of latent flaws and improves resilience from the outset. The "Shift Right" component addresses runtime security by continuously monitoring live systems through synchronized Digital Twins(DTs). These Security Digital Twins (SDTs) collect real time data from physical assets and simulate attack scenarios, enabling dynamic threat detection, forensic analysis, adaptive responses and strategies.combination of both perspectives, the SLSR paradigm ensures that cybersecurity is embedded throughout the lifecycle—from initial architecture to operational defense.

 doi:10.20944/preprints202511.1203.v1

This dual-phase methodology enhances situational awareness, reduces response latency, and supports continuous improvement of security postures [44].

Security Digital Twins (SDTs) are instantiated to mirror components of Cyber-Physical Systems (CPS),Industrial Internet of Things(IIoT) devices. These Security Digital Twins (SDTs) receive real time data from Virtual Component (VC) hosted on edge or cloud environments, allowing for continuous threat simulation and vulnerability assessment without disrupting live operations [4].

The Digital Twins(DTs) framework supports component criticality analysis and patch prioritization by simulating attack scenarios and evaluating system responses. For example, Benelhaouare et al. demonstrated how thermal digital twins can enhance hardware-level security in 3D-SiP systems by identifying thermal anomalies [43]. The architecture also integrates with supervisory control systems and SOC workflows, allowing for seamless threat detection and forensic analysis. This modeling approach ensures that cybersecurity operations are proactive, scalable, and adaptable to evolving threat landscapes.

3.2. Generative Artificial Intelligence (Gen AI) Integration for Threat Simulation

Generative Artificial Intelligence (Gen AI), particularly Large Language Models (LLMs) is integrated into the Digital Twins (DTs) ecosystem to automate penetration testing, threat modeling and incident response toward cyberattacks and cyber defense.

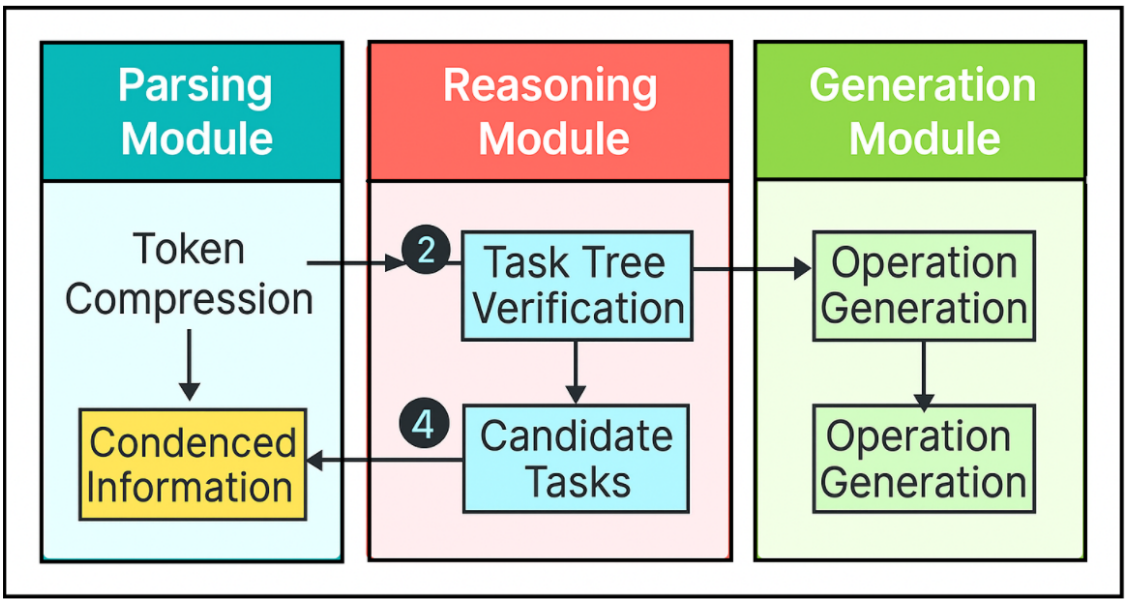

Figure 3. Overview of PENTESTGPT Adapted from [6].

PentestGPT is an automated penetration testing system powered by Large Language Models. It uses three modules—Parsing, Reasoning and Generation to interpret user intent, track vulnerabilities and generate precise attack commands. It maintains a task tree to guide strategic decisions. PentestAgent complements this by simulating attacker behavior using reinforcement learning and LLMs to interact with vulnerable systems dynamically. While PentestGPT emphasizes structured planning and modular execution, PentestAgent focuses on goal-driven exploitation. Together, they enable scalable and intelligent cybersecurity assessments across diverse environments. [6,23]. These models interpret system logs,correlate threat indicators and provide natural language explanations of complex security events for educational purpose in detail with simple way, enhancing analyst efficiency and reducing response time by applying above advantages of the integration of Digital Twins(DTs) and Generative Artificial Intelligence (Gen AI).

By embedding Generative Artificial Intelligence (Gen AI) into the Digital Twins (DTs) framework, organizations can automate complex security task, reduce manual effort and improve threat detection accuracy. This synergy between Digital Twins (DTs) and Generative Artificial Intelligence (Gen AI)

 doi:10.20944/preprints202511.1203.v1

enables continuous learning, real-time adaptation and scalable security operations across diverse infrastructures which help in cyber security education through different departments like Internet of Things (IOT) etc.

3.3. AI Assisted Cybersecurity Education Framework Methodology

To evaluate the educational potential of GenAI in cybersecurity, a two stage instructional framework is implemented using the CLaaS (Cybersecurity Labs as a Service) platform. In the first stage, students interact with AI generated policy drafts during tutorials, refining them using academic research and regulatory frameworks such as NIST and GDPR [47]. This process encourages critical thinking and contextual understanding of cybersecurity principles.

In the second stage, assessments require students to apply Generative Artificial Intelligence (Gen AI) outputs to real-world scenarios, such as developing security policies for financial institutions or designing layered defense strategies. Students analyze gaps in AI-generated content, justify refinements, and present final outputs aligned with industry standards [18]. The CLaaS platform supports this framework by providing browser-accessible virtual machines and integrated Generative Artificial Intelligence (Gen AI) assistance via OCR-to-LLM pipelines [48].

Student feedback is collected to evaluate instructional effectiveness. In a live deployment, students rated Generative Artificial Intelligence (Gen AI) assisted instruction with an average score of 7.83/10, indicating strong pedagogical value [48]. This framework bridges the gap between theoretical knowledge and practical application, preparing students for real-world cybersecurity roles while promoting responsible AI use.

3.4. Validation and Feedback Mechanism

Validation of the Digital Twins (DTs) and Generative Artificial Intelligence (Gen AI) integration is conducted through simulation-based testing and user feedback. SDTs are used to simulate cyberattacks such as command injection, MITM and ransomware, allowing for safe evaluation of system resilience and response strategies [44]. These simulations are mapped to known vulnerability chains using CWE, CAPEC and MITRE ATTACK frameworks, ensuring comprehensive threat coverage.

Educational validation is performed via student feedback collected during Generative Artificial Intelligence (Gen AI)assisted instruction. In a university deployment, 42 students rated the usefulness of simplified AI-generated content, yielding an average score of 7.83/10 [48]. This feedback highlights the effectiveness of enerative Artificial Intelligence (Gen AI) in enhancing comprehension and engagement.

A comparative study between OCR-based and multimodal LLM pipelines is also conducted. While multimodal models like chatGPT 4 offer superior performance on visually dense slides, OCR-based pipelines deliver comparable clarity at lower computational cost [47]. This confirms the feasibility of lightweight Generative Artificial Intelligence (Gen AI) integration for scalable cybersecurity education.

Operational metrics such as detection accuracy, response time and policy compliance are tracked to assess system performance. Feedback from SOC analysts and instructors is used to refine the RTK toolkit and improve scenario realism. These validation mechanisms ensure that the integrated framework is both technically robust and pedagogically impactful.

4. Challenges and Limitations

Despite the promising integration of Digital Twins (DTs) and Generative AI (GenAI) in cybersecurity, several challenges and limitations must be addressed to ensure secure, ethical and scalable deployment. One major concern is the fidelity and synchronization of real-time data between physical systems and their digital counterparts. Inaccurate or delayed data can lead to false positives or missed threats, undermining the reliability of Security Digital Twins (SDTs) [4,44].

Another critical limitation is the interpretability of Generative Artificial Intelligence (Gen AI) models. Large Language Models (LLMs) such as PentestGPT and PentestAgent often function as black

 doi:10.20944/preprints202511.1203.v1

boxes, making it difficult for analysts to trace decision logic or validate outputs [6,23]. This lack of transparency poses risks in regulated environments where explainability is essential for compliance and accountability.

From an educational perspective, over-reliance on Generative Artificial Intelligence (Gen AI) may hinder the development of foundational cybersecurity skills. Students might accept AI-generated outputs without critical evaluation, leading to superficial understanding and reduced problem-solving ability [47]. Additionally, biases embedded in training data can propagate into AI-generated content, potentially reinforcing stereotypes or overlooking edge-case vulnerabilities.

Scalability and resource constraints also present challenges. Multimodal LLMs require significant computational power, limiting their accessibility in low-resource academic or industrial settings [48]. Integrating Digital Twins (DTs) and Generative Artificial Intelligence (Gen AI) into legacy systems may require substantial re engineering, increasing deployment complexity and cost.

Finally, ethical concerns such as data privacy, model misuse, and adversarial manipulation must be proactively addressed. Without robust governance frameworks, these technologies could inadvertently introduce new vulnerabilities into cybersecurity ecosystems.

5. Results and Comparative Summary

The integration of Digital Twins (DTs) and Generative Artificial Intelligence (Gen AI) demonstrated measurable improvements in both cybersecurity operations and education. In operational settings, DTs enabled real time simulation of cyberattacks on virtualized Cyber-Physical Systems (CPS) environments,allowing for safe vulnerability assessment and system hardening. Generative Artificial Intelligence (Gen AI) tools like PentestGPT and PentestAgent automated penetration testing workflows, reducing manual effort and improving threat detection accuracy.

In educational deployments, a twos stage Generative Artificial Intelligence (Gen AI) assisted framework was implemented using the CLaaS platform. Students interacted with AI generated policy drafts and applied them to real-world scenarios. Feedback from 42 participants indicated an average usefulness rating of 7.83/10 for AI-assisted instruction, highlighting its pedagogical value.

A comparative study between OCR-based and multimodal LLM pipelines revealed that while multimodal models offered enhanced visual comprehension, OCR-based systems provided comparable instructional clarity at lower computational cost.

6. Discussion

The convergence of Digital Twins (DTs) and Generative Artificial Intelligence (Gen AI) in cybersecurity introduces a paradigm shift in how threats are modeled, detected and mitigated. Digital Twins (DTs) offer a dynamic simulation environment that mirrors real-world cyber-physical systems, enabling continuous monitoring and predictive analysis. This capability allows organizations to simulate attack scenarios, evaluate system vulnerabilities and test defense mechanisms without compromising operational integrity. By replicating physical components such as PLCs and IoT devices, DTs provide a safe and scalable platform for proactive security operations.

Generative Artificial Intelligence (Gen AI) enhances this framework by automating traditionally manual tasks such as penetration testing, threat modeling, and incident response. Large Language Models (LLM) can interpret system logs, generate attack vectors and suggest remediation strategies in real time. This reduces the burden on security analysts and accelerates decision making processes. The integration of Generative Artificial Intelligence (Gen AI) also supports adaptive learning, allowing systems to evolve based on new threat intelligence and behavioral patterns.

In educational contexts Generative Artificial Intelligence (Gen AI) has shown promise in improving student engagement and comprehension. AI-generated content, when used within virtual lab environments, encourages critical thinking and practical application of cybersecurity principles. Students can interact with policy drafts, refine them using regulatory standards and apply them to simulated scenarios, bridging the gap between theory and practice.

 doi:10.20944/preprints202511.1203.v1

However, successful implementation requires careful consideration of data accuracy, model transparency and ethical safeguards. The effectiveness of this integration depends on continuous validation, interdisciplinary collaboration and a commitment to responsible AI use. When thoughtfully deployed, Digital Twins(DTs) and Generative Artificial Intelligence (Gen AI) offer a powerful, intelligent framework for modern cybersecurity challenges.

7. Conclusion and Future Work

The integration of Digital Twins (DTs) and Generative Artificial Intelligence (Gen AI) presents a transformative approach to cybersecurity, offering both operational and educational advancements. Digital Twins (DTs) enable real-time simulation and monitoring of Cyber-Physical Systems (CPS), allowing organizations to proactively identify vulnerabilities and test defense mechanisms without disrupting live environments. Their ability to replicate infrastructure virtually supports both design time and runtime security operations, enhancing system resilience and threat preparedness.

Generative Artificial Intelligence (Gen AI) complements this framework by automating complex tasks such as penetration testing, threat modeling, and incident response. Large Language Models (LLMs) interpret system behavior, generate attack vectors and provide remediation strategies, significantly reducing the workload on human analysts. In academic settings, Generative Artificial Intelligence (Gen AI) fosters interactive learning by generating policy drafts, guiding scenario-based assessments and supporting personalized instruction. Together, Digital Twins (DTs) and Generative Artificial Intelligence (Gen AI) form a scalable, intelligent cybersecurity ecosystem capable of adapting to evolving threats and educational needs.

Ultimately, the success of Generative Artificial Intelligence (Gen AI) and Digital Twins (DTs) integration depends on continuous validation, ethical oversight and interdisciplinary collaboration. With thoughtful implementation, these technologies can redefine cybersecurity practices and prepare the next generation of professionals for a rapidly evolving digital world.

References

1. A. P. J., A. Shankar, A. N. J. R., K. Koliparthy, V. N. Badiger, and V. Shivakumar, "Exploring the applications and challenges of digital twins in various industries," in *Proc. 2024 IEEE 9th Int. Conf. for Convergence in Technology (I2CT)*, pp. 1–7, 2024. doi:10.1109/I2CT61223.2024.10543818.
2. K. Alshammari, T. Beach, and Y. Rezgui, "Cybersecurity for digital twins in the built environment: Current research and future directions," *J. Inf. Technol. Constr.*, vol. 26, pp. 159–173, 2021.
3. M. T. Baldassarre, V. S. Barletta, D. Caivano, D. Raguseo, and M. Scalera, "Teaching cyber security: The hack-space integrated model," vol. 2315, 2019.
4. V. S. Barletta, D. Caivano, M. Calvano, A. Curci, and A. Piccinno, "Craste: Human factors and perception in cybersecurity education," vol. 3713, pp. 75–81, 2024.
5. S. Biffl, M. Eckhart, A. Lüder, and E. Weippl, *Introduction to Security and Quality Improvement in Complex Cyber-Physical Systems Engineering*, Springer, Cham, 2019.
6. G. Deng, Y. Liu, V. Mayoral-Vilches, P. Liu, Y. Li, Y. Xu, T. Zhang, Y. Liu, M. Pinzger, and S. Rass, "PentestGPT: An LLM-empowered automatic penetration testing tool," 2024. Available: https://arxiv.org/abs/2308.06782.
7. M. Dietz, M. Vielberth, and G. Pernul, "Integrating digital twin security simulations in the security operations center," in *Proc. 15th Int. Conf. on Availability, Reliability and Security (ARES)*, ACM, 2020.
8. M. El-Hajj, "Leveraging digital twins and intrusion detection systems for enhanced security in IoT-based smart city infrastructures," *Electronics*, vol. 13, no. 19, 2024. doi:10.3390/electronics13193941.
9. R. Faleiro, L. Pan, S. R. Pokhrel, and R. Doss, "Digital twin for cybersecurity: Towards enhancing cyber resilience," in *Proc. Int. Conf. on Broadband Communications, Networks and Systems*, pp. 57–76, Springer, 2021.
10. J. Guo and Z. Lv, "Application of digital twins in multiple fields," *Multimedia Tools and Applications*, vol. 81, no. 19, pp. 26941–26967, 2022. doi:10.1007/s11042-022-12536-5.
11. M. Guven, "A comprehensive review of large language models in cyber security," *Int. J. Comput. Exp. Sci. Eng.*, vol. 10, no. 3, Sep. 2024. doi:10.22399/ijcesen.469.
12. E. Hadar, D. Kravchenko, and A. Basovskiy, "Cyber digital twin simulator for automatic gathering and prioritization of security controls' requirements," in *Proc. 2020 IEEE 28th Int. Requirements Engineering Conf. (RE)*, pp. 250–259, 2020. doi:10.1109/RE48521.2020.00035.

 doi:10.20944/preprints202511.1203.v1

13. M. Hassanin and N. Moustafa, "A comprehensive overview of large language models (LLMs) for cyber defences: Opportunities and directions," 2024. Available: https://arxiv.org/abs/2405.14487.
14. D. Holmes, M. Papathanasaki, L. Maglaras, M. A. Ferrag, S. Nepal, and H. Janicke, "Digital twins and cyber security–solution or challenge?," in *Proc. 2021 6th South East Europe Design Automation, Computer Engineering, Computer Networks and Social Media Conf. (SEEDA-CECNSM)*, pp. 1–8, 2021.
15. R. P. Joshi, S. Gulati, and A. K. Kar, "Digital twin for industrial applications–a literature review," in *Transfer, Diffusion and Adoption of Next-Generation Digital Technologies*, Springer Nature, Cham, 2024.
16. M. M. S. Khan, J. A. Giraldo, and M. Parvania, "Real-time cyber-physical analysis of distribution systems using digital twins," in *Proc. 2022 IEEE Int. Conf. on Communications, Control, and Computing Technologies for Smart Grids (Smart-GridComm)*, pp. 34–39, 2022.
17. L. Latorre, E. Rego, L. De Leo, and M. Gutierrez, "Tech report: Digital twins," 2024. doi:10.18235/0013166.
18. Y. Z. Lin et al., "Transforming engineering education using generative AI and digital twin technologies," 2024. Available: https://arxiv.org/abs/2411.14433.
19. J. Luzzi, R. Naha, A. Arulappan, and A. Mahanti, "SoK: A holistic view of cyberattacks prediction with digital twins," in *Proc. 2024 2nd Int. Conf. on Emerging Trends in Information Technology and Engineering (ICETITE)*, pp. 1–7, 2024.
20. K. L. McLaughlin, "The power of digital twins in the cybersecurity mesh," *EDPACS*, vol. 68, no. 6, pp. 35–39, 2023.
21. G. Rossetti et al., "Y Social: An LLM-powered social media digital twin," 2024. Available: https://arxiv.org/abs/2408.00818.
22. M. Sasikala, Y. M. Mahaboob John, B. Jothi, S. N., and S. S. K., "Integrating digital twins with AI for real-time intrusion detection in smart infrastructure networks," in *Proc. 2024 Int. Conf. on Intelligent Algorithms for Computational Intelligence Systems (IACIS)*, pp. 1–6, 2024.
23. X. Shen et al., "PentestAgent: Incorporating LLM agents to automated penetration testing," 2025. Available: https://arxiv.org/abs/2411.05185.
24. A. Somma et al., "A cyber digital twin framework to support cyber-physical systems security," in *Proc. 2023 IEEE Smart World Congress (SWC)*, pp. 1–10, 2023.
25. I. Tarnowski, "How to use cyber kill chain model to build cybersecurity?," *Eur. J. Higher Educ. IT*, 2017.
26. S. A. Varghese et al., "Digital twin-based intrusion detection for industrial control systems," in *Proc. 2022 IEEE Int. Conf. on Pervasive Computing and Communications Workshops (PerCom Workshops)*, pp. 611–617, 2022.
27. T. K. Yadav and A. M. Rao, "Technical aspects of cyber kill chain," *arXiv preprint arXiv:1606.03184*, 2015.
28. L. Yang, S. Luo, X. Cheng, and L. Yu, "Leveraging large language models for enhanced digital twin modeling: Trends, methods, and challenges," 2025. Available: https://arxiv.org/abs/2503.02167.
29. B. R. Barricelli, E. Casiraghi, and D. Fogli, "A survey on digital twin: Definitions, characteristics, applications, and design implications," *IEEE Access*, vol. 7, pp. 167653–167671, 2019.
30. M. Grieves and J. Vickers, "Digital twin: Mitigating unpredictable, undesirable emergent behavior in complex systems," *Transdisciplinary*, pp. 85–113, 2017.
31. M. W. Grieves, "Digital twins: Past, present, and future," in *The Digital Twin*, Springer, pp. 97–121, 2023.
32. B. Bothwell, "Science & Tech Spotlight: Digital Twins—Virtual Models of People and Objects," Tech. Rep. GAO-23-106453, U.S. Government Accountability Office, 2023.
33. A. B. Shitole et al., "Real-time digital twin of residential energy storage system for cyber-security study," in *Proc. IEEE 2nd Int. Conf. on Smart Technologies for Power, Energy and Control*, pp. 1–6, 2021.
34. E. C. Balta, M. Pease, J. Moyne, K. Barton, and D. M. Tilbury, "Digital twin-based cyber-attack detection framework for cyber-physical manufacturing systems," *IEEE Trans. Autom. Sci. Eng.*, vol. 21, no. 2, pp. 1695–1712, 2023.
35. K. Hammar and R. Stadler, "Digital twins for security automation," in *Proc. IEEE/IFIP Network Operations and Management Symposium*, pp. 1–6, 2023.
36. H. A. Shaikh et al., "Digital twin for secure semiconductor lifecycle management: Prospects and applications," *arXiv preprint arXiv:2205.10962*, 2022.
37. J. Hornik and M. Rachamim, "Leveraging AI-enabled digital twins to combat counterfeit brands," *J. Forensic Sci. Crim. Invest.*, pp. 1–8, 2024.
38. G. Cathey, J. Benson, M. Gupta, and R. Sandhu, "Edge centric secure data sharing with digital twins in smart ecosystems," in *Proc. 3rd IEEE Int. Conf. on Trust, Privacy and Security in Intelligent Systems and Applications*, pp. 70–79, 2021.

 doi:10.20944/preprints202511.1203.v1

39. O. Alharbi, R. A. Shaikh, and R. Asif, "Data-aided intrusion detection systems: Leveraging AI, blockchain and digital twin technology," in *Proc. IEEE Int. Conf. on Big Data (BigData)*, pp. 8214–8215, 2024.
40. S. Pirbhulal, H. Abie, and A. Shukla, "Towards a novel framework for reinforcing cybersecurity using digital twins in IoT-based healthcare applications," in *Proc. IEEE 95th Vehicular Technology Conf. (VTC2022 Spring)*, pp. 1–5, 2022.
41. P. Empl, D. Schlette, D. Zupfer, and G. Pernul, "SOAR4IoT: Securing IoT assets with digital twins," in *Proc. 17th Int. Conf. on Availability, Reliability and Security*, pp. 1–10, 2022.
42. H. Yi, R. Lin, H. Song, C. Li, and X. Lin, "Experimental study of cryptographic algorithm based on digital twin technology side channel leakage intelligent measurement and assessment," *Rev. Adhesion Adhesive*, vol. 11, no. 25, pp. 856–880, 2023.
43. A. Z. Benelhaouare, A. Oukaira, M. Oumlaz, and A. Lakhssassi, "Enhancing thermal security of 3D-SiP systems through thermal digital twin (TDT)," in *Proc. IEEE Canadian Conf. on Electrical and Computer Engineering*, pp. 20–24, 2024.
44. A. Mohsin, H. Janicke, S. Nepal, and D. Holmes, "Digital Twins and the Future of their Use Enabling Shift Left and Shift Right Cybersecurity Operations," *arXiv preprint arXiv:2309.13612*, 2023. Available: https://arxiv.org/abs/2309.13612
45. A. Fitzgerald, "How Can Generative AI Be Used in Cybersecurity? 15 Real-World Examples," *Secureframe Blog*, Jun. 2025. Available: https://secureframe.com/blog/generative-ai-cybersecurity
46. SentinelOne, "What is Generative AI in Cybersecurity?," *SentinelOne Cybersecurity 101*, May 2025. Available: https://www.sentinelone.com/cybersecurity-101/data-and-ai/generative-ai-cybersecurity/
47. M. Elkhodr and E. Gide, "Integrating Generative AI in Cybersecurity Education: Case Study Insights on Pedagogical Strategies, Critical Thinking, and Responsible AI Use," *arXiv preprint arXiv:2502.15357*, 2025. Available: https://arxiv.org/abs/2502.15357
48. K. Patel, Y.-Z. Lin, G. Raul, B. P.-J. Shih, M. W. Redondo, B. S. Latibari, J. Pacheco, S. Salehi, and P. Satam, "Integrating Generative AI into Cybersecurity Education: A Study of OCR and Multimodal LLM-assisted Instruction," *arXiv preprint arXiv:2509.02998*, 2025. Available: https://arxiv.org/abs/2509.02998