Enabling Cyber Security Education through Digital Twins and Generative AI

[1]G.Prabhakar, Associate Professor , CSE, gantelaprabhakar@gmail.com
Swarna Bharathi institute of science and technology,
Khammam

[2] N.Savitha, Assistant Professor, CSE(DS), savitha.natuva@gmail.com
Swarna Bharathi institute of science and technology,
Khammam

[3]Ameena nasreen, Assistant Professor, CSE(AIML),
amena.nasreen.md@gmail.com
Swarna Bharathi institute of science and technology,
Khammam

Abstract:

Digital Twins (DTs) are gaining prominence in cybersecurity for their ability to replicate complex IT (Information Technology), OT (Operational Technology), and IoT (Internet of Things) infrastructures, allowing for real-time monitoring, threat analysis, and system simulation. This study investigates how integrating DTs with penetration testing tools and Large Language Models (LLMs) can enhance cybersecurity education and operational readiness. By simulating realistic cyber en- vironments, this approach offers a practical, interactive framework for exploring vulnerabilities and defensive strategies. At the core of this research is the Red Team Knife (RTK), a custom penetration testing toolkit aligned with the Cyber Kill Chain model. RTK is designed to guide learners through key phases of cyber-attacks including reconnais- sance, exploitation, and response—within a DT-powered ecosystem. The incorporation of Large Language Models (LLMs) further enriches the experience by providing intelligent, real-time feedback, natural language threat explanations, and adaptive learning support during training ex- ercises. This combined DT–LLM framework is currently being piloted in academic settings to develop hands-on skills in vulnerability assessment, threat detection, and security operations. Initial findings suggest that the integration significantly improves the effectiveness and relevance of cybersecurity training, bridging the gap between theoretical knowledge and real-world application. Ultimately, the research demonstrates how DTs and LLMs together can transform cybersecurity education to meet evolving industry demands.

Keywords: Cyber Social Security · Penetration Testing · Cybersecurity Education · Human-AI Responsive Collaboration.

Introduction:

Traditional cybersecurity has historically focused on protecting technical infras- tructures, systems, and computer networks. However, the evolution of the threat landscape has highlighted how the human element often represents the weakest link in the security chain. Therefore, Cyber Social Security emerges as a disci- pline that studies the intersection between social factors, human behaviors, and information security, recognizing that many of the most sophisticated attacks exploit psychological and social vulnerabilities

rather than exclusively techni- cal ones. The advent of Generative Artificial Intelligence has revolutionized this scenario, significantly amplifying attackers' capabilities to conduct large-scale social engineering operations. In this context, Digital Twins (DTs) are increas- ingly recognized as powerful assets in cybersecurity, offering real-time monitor- ing, detailed system analysis, and high-fidelity emulation capabilities [19]. By creating accurate virtual replicas of hardware, software and firmware compo- nents, DTs enable organizations to proactively identify vulnerabilities and mit- igate cyber threats with greater precision [19], [14]. While their application has demonstrated significant value in sectors such as manufacturing, construction, automotive, agriculture, and transportation, the cybersecurity implications of DT integration remain underexplored [14].When embedded within a Cybersecurity Mesh architecture, DTs can improve threat prediction, streamline incident response, and improve systemic resilience [20]. The integration of Large Language Models (LLMs) into this ecosystem further amplifies these benefits. LLMs can support automated interpretation of system behaviors, assist in real-time threat analysis, and generate human- readable explanations of complex security events, making the DT environment more accessible and intelligent. This synergy enables more adaptive and respon- sive cybersecurity operations.

Building on this perspective, the objective of this research is to explore how current technologies––—specifically Digital Twins, LLMs, and penetration test- ing tools——can deepen our understanding of cyber attacks and their broader context. approach enables a redefinition of key security functions [3]:

1.Detection. DTs and LLMs together redefine detection by enabling real-time simulation, analysis, and intelligent interpretation of cyber-physical environ- ments. While DTs mirror IT, OT, and IoT infrastructures to enhance sit- uational awareness, LLMs support the detection process through advanced natural language understanding and threat intelligence extraction from un- structured data sources, such as *OSINT* and dark web forums. This synergy improves the identification of critical events and behavioral patterns across human, social, cultural, and political dimensions.

2.Response. DTs and LLMs enhance response strategies through dynamic simulations and real-time contextual reasoning. Digital Twins facilitate sce- nario testing and decision-making in crisis situations, while LLMs contribute by generating adaptive response recommendations, analyzing incident re- ports, and enabling more effective communication between technical teams and non-expert stakeholders. Together, they support coordinated responses across civil society, strengthening resilience against cybercrime and cyber terrorism.

3.Prevention. In preventive efforts, DTs and LLMs enable more nuanced risk assessment and proactive threat modeling. DTs simulate critical as- sets—ranging from individuals and communities to infrastructure and soft- ware—while LLMs analyze historical incident data, policy documents, andsocio-political discourse to anticipate emerging threats. This integrated ap- proach allows for a comprehensive security posture that encompasses phys- ical, organizational, and application-level dimensions, while contextualizing cyber risks within legal, economic, and psychological frameworks.

4.The paper is organized as follows: section 2 describes the related works; sec- tion 3 describes the Cyber Kill Chain Model and section 4 the Logical Framework in Cyber Security Education; section 5 conclude the work and explain the future developments.

Related Work:

DTs are playing an increasingly critical role in enhancing cybersecurity across complex, interconnected environments. By creating dynamic virtual replicas of physical systems—spanning IT, OT, and IoT infrastructures—DTs enable orga- nizations to simulate, monitor, and analyze systems in real time. This capability allows for the detection of anomalies, assessment

of vulnerabilities, and rehearsal of threat scenarios in a safe, controlled environment.Integration of digital twins with intrusion detection systems has shown promise in detecting cyberattacks and understanding resource impacts in IoT-based smart city infrastructures [8]. Studies emphasize the importance of addressing cyberse- curity challenges in digital twin deployments, particularly in smart cities, where risks such as unauthorized access and data manipulation are significant concerns. To mitigate these risks, multi-layered security frameworks incorporating encryp- tion, access control, and anomaly detection have been proposed. The integration of digital twins with Building Information Models (BIM) and IoT technologies is seen as crucial for enhancing cybersecurity in the built environment [2]. Overall, digital twins offer a promising approach to improve cyber resilience by enabling real-time monitoring and virtualization of physical systems [9].

cyber Kill Chain

The Cyber Kill Chain is a model that outlines the stages of a cyber-attack, from initial reconnaissance to the final action [27,4]: (i) *Reconnaissance*. The at- tacker gathers information about the target to plan the attack; (ii) *Weaponiza- tion*. Malicious payloads are created to exploit the identified vulnerabilities; (iii) *Delivery*. The attacker transmit the payload to the target environment; (iv) *Exploitation*. Malware code is executed on the target system, exploiting vulner- abilities to gain unauthorized access; (v) *Installation*. Malware or other malicious components are installed on compromised systems; (vi) *Command and Control (C2)*. The attacker establishes communication channels to control compromised systems and execute their plans; (vii) *Actions on Objectives*. The final phase where the attacker achieves their ultimate goal, such as data theft, system con- trol, or disruption. This model has been extensively adopted within the security community as a key framework for understanding and mitigating cyber-attacks. Nonetheless, Khan et al. [16] highlight its shortcomings, especially in confronting sophisticated and persistent threats. To overcome these limitations, they intro- duce an enhanced model that enables simultaneous analysis of multiple threat stages, mirroring the human cognitive process in threat evaluation. Tarnowski[25] also underscores the Cyber Kill Chain's role in strengthening cybersecurity, particularly in safeguarding networks

Digital Twins and Generative AI to **improve Cyber Security Education**

Digital Twins (DTs)—virtual counterparts of physical systems—have found widespread applications across various industries. In manufacturing, they enable real-time monitoring, predictive maintenance, and simulation-based optimization [1,10];in healthcare, they support personalized medicine, precise diagnostics, and ad- vanced treatment planning [1,17]. Agriculture benefits from improved farm man- agement and resource utilization [1,17], while the automotive and aviation sec- tors employ DTs for asset tracking and fault prediction [1]. Urban planning, energy systems, and smart infrastructure also leverage DTs for efficient design, sustainability, and complex system management [17,15]. These applications are enabled by the convergence of IoT, AI, XR, and cloud computing, which bridge the physical and digital realms [1,10].

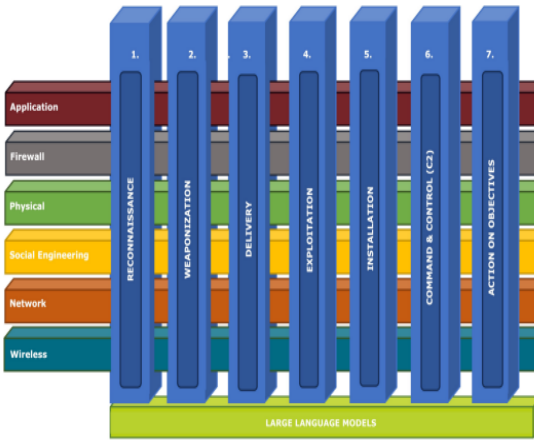
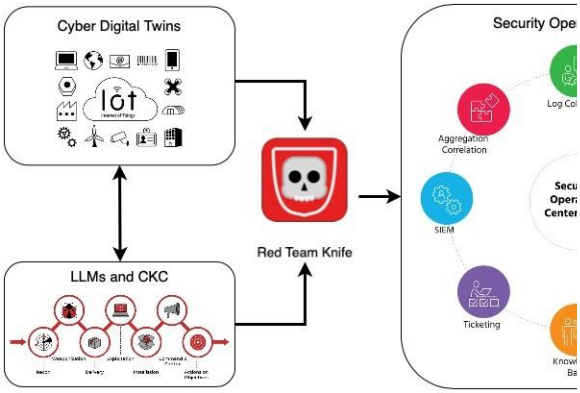


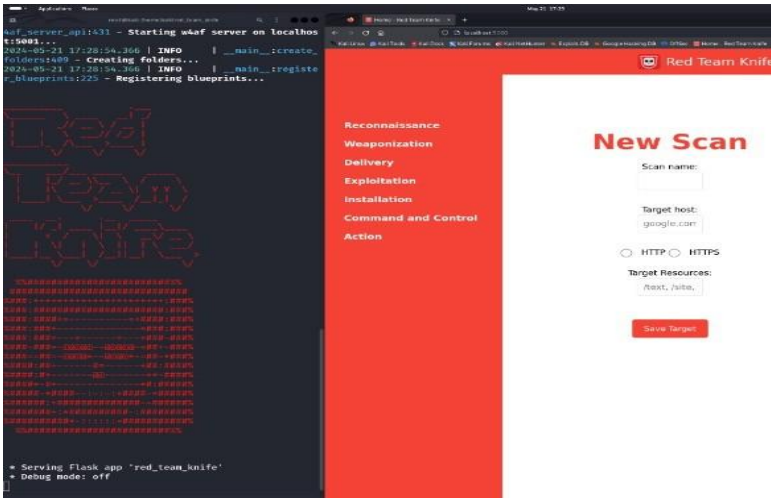
Fig. 1. Logical Architecture: Cyber Digital Twin to improve Securit

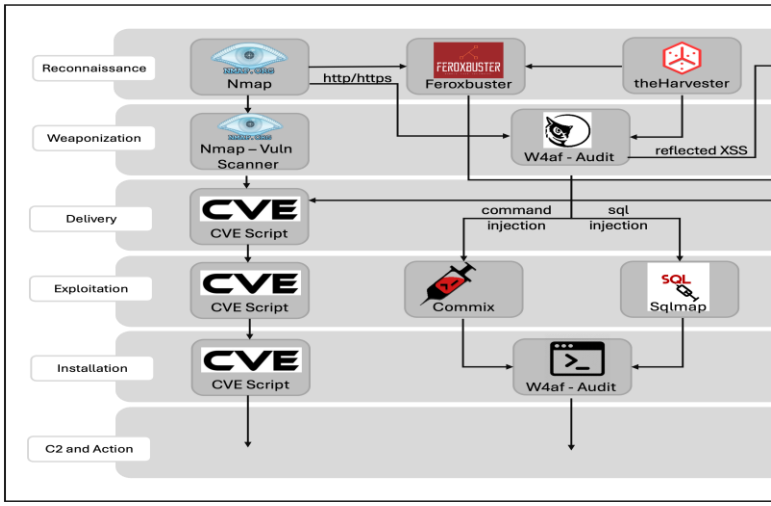
In the proposed architecture, LLMs and a Red Team Knife (RTK) play a key role for Cyber Security Education. The goal is to help perform the various activities to identify threats and vulnerabilities in the various systems through suggestions and guidelines in applying the results obtained from the various tools implemented. An example is shown in Figure 2: RTK identify vulnerabilities like SQL injection, XSS, CSRF, data exposure, etc. of the Cyber Digital Twins analyzed; thanks to the support of the "LLMs and CKC" it is possible to be able to acquire penetration testing competencies and improve the Blue Team activities like in the Secure Operation Center.



Red team Knife:

A penetration test (or pentest) is a simulated cyberattack on a computer system, conducted to assess its security posture. The purpose of a pentest is to uncover weaknesses or vulnerabilities that could be exploited by unauthorized actors to access system functionalities or sensitive data. This process enables a thorough risk assessment of the system.





Conclusion

This paper explores the cybersecurity landscape and investigates how digital twins and LLMs can enhance individuals' competencies in penetration testing. Specifically, it introduces a dual-dimensional approach to cybersecurity educa- tion: the horizontal dimension, represented by various digital twins simulating different asset types; and the vertical dimension, aligned with the stages of the Cyber Kill Chain, which together support the development of layered function- alities within the Red Team Knife (RTK) and LLMs.

References:

1.A P, J., Shankar, A., J R, A.N., Koliparthy, K., Badiger, V.N., Shivakumar, V.: Exploring the applications and challenges of digital twins in various industries. In: 2024 IEEE 9th International Conference for Convergence in Technology (I2CT).

pp. 1–7 (2024). https://doi.org/10.1109/I2CT61223.2024.10543818

2.Alshammari, K., Beach, T., Rezgui, Y.: Cybersecurity for digital twins in the built environment: Current research and future directions. Journal of Information Technology in Construction 26, 159–173 (2021)

3.Baldassarre, M.T., Barletta, V.S., Caivano, D., Raguseo, D., Scalera, M.:Teaching cyber security: The hack-space integrated model. vol. 2315 (2019), **https://www.scopus.com/inward/record.uri?eid=2-s2.0-85061370504&partnerID=40&md5=e8da8bde8df7b4a276e5517e34136832**

4. Barletta, V.S., Caivano, D., Calvano, M., Curci, A., Piccinno, A.: Craste: Human factors and perception in cybersecurity education. vol. 3713,

p. 75 – 81 (2024), https://www.scopus.com/inward/record.uri?eid=2-s2.0-85198753881&partnerID=40&md5=35f9b858e583d214bb7a53c0a7dbf0da

5.Biffl, S., Eckhart, M., Lüder, A., Weippl, E.: Introduction to Security and Quality Improvement in Complex Cyber-Physical Systems Engineering, pp. 1–29. Springer International Publishing, Cham (2019)

6.Deng, G., Liu, Y., Mayoral-Vilches, V., Liu, P., Li, Y., Xu, Y., Zhang, T., Liu,Y., Pinzger, M., Rass, S.: Pentestgpt: An llm-empowered automatic penetration testing tool (2024), https://arxiv.org/abs/2308.06782

7.Dietz, M., Vielberth, M., Pernul, G.: Integrating digital twin security simulations in the security operations center. In: Proceedings of the 15th International Conference on Availability, Reliability and Security. ARES '20, Association for Computing Machinery, New York, NY, USA (2020)

8.El-Hajj, M.: Leveraging digital twins and intrusion detection systems for enhanced security in iot-based smart city infrastructures. Electronics 13(19) (2024). https:

//doi.org/10.3390/electronics13193941

9.Faleiro, R., Pan, L., Pokhrel, S.R., Doss, R.: Digital twin for cybersecurity: Towards enhancing cyber resilience. In: International Conference on Broadband Communi- cations, Networks and Systems. pp. 57–76. Springer (2021)

10. Guo, J., Lv, Z.: Application of digital twins in multiple fields. Multimedia Tools and Applications **81**(19), 26941–26967 (2022). https://doi.org/10.1007/s11042-022-12536-5, https://doi.org/10.1007/s11042-022-12536-5