International Journal of Engineering & Extended Technologies Research (IJEETR)

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 4, July- August 2026 |

DOI:10.15662/IJEETR.2026.0804001

# Cybersecurity for Digital Twins

**Dr. Alex Mathew**

Dept. of Cybersecurity, Bethany College, West Virginia, USA

**Publication History**: Received: 07.06.2026; Revised: 28.06.2026; Accepted: 30.06.2026; Published: 03.07.2026.

**ABSTRACT:** Digital twins (DTs), a technology of Industry 4.0 and 5.0, are now playing a pivotal role in the real-time virtual representation of physical assets in manufacturing, aerospace, healthcare, and smart cities. The close coupling of the cyber and physical domains, however, creates a large and novel attack surface that is not well covered by traditional security frameworks. The Secure-AI Twin (SAT) framework is introduced in this paper as an all-encompassing cybersecurity concept for AI-powered digital twins covering four key areas: Vulnerability analysis throughout DT ecosystems, Anomaly detection using AI, Industrial IoT and Industry 5.0 security, and Real-time cyber-physical threat mitigation. The proposed multi-layered defense architecture has been implemented using advances in federated learning, explainable AI, and neural-network-based threat detection, resulting in a 27.4% increase in threat detection accuracy and a 21.2% decrease in latency. The framework tackles the challenges of fidelity, real-time synchronization, and security, known as the "Digital Twin Trilemma," with an integrated solution that includes blockchain-supported federated learning, autoencoder-based anomaly detection, and dynamic incident response. The framework has been proven effective against sophisticated cyber-physical attacks in both industrial control systems and IIoT environments through experimental validation.

**KEYWORDS:** Digital Twin, Cybersecurity, Anomaly Detection, Industry 5.0, Industrial IoT, Federated Learning, Cyber-Physical Systems

## I. INTRODUCTION

Digital twins (DTs) are no longer hypothetical; they are real technologies and solutions transforming the way industrial systems operate, capable of replicating physical systems in real time across sectors such as manufacturing, aerospace, healthcare, and smart cities (Mihai et al., 2022; Sharma et al., 2022). The uses range from patient-specific to planetary scale, such as the European Union's Destination Earth project (Doblas-Reyes et al., 2026). The two-way data flow and the strong connection between cyber and physical components that allow DTs to also lead to a different attack surface, where a malicious actor can exploit a twin to learn about system behaviour, send fake telemetry data, or influence operations parameters with real-world consequences (Airehenbuwa et al., 2025; Stergiou et al., 2023). These facts are highlighted by the Colonial Pipeline, NotPetya, and Stuxnet attacks, which demonstrate how cyber-physical compromise can lead to catastrophic effects on critical infrastructure, especially given the increased importance of DTs in Industry 5.0 (Ahmed et al., 2023; Piras et al., 2024). Security systems are fragmented, and many are 'black boxes' that are hard to scale, keep up with new threats, and are trusted by stakeholders (Empl et al., 2024). In this paper, we present the Secure-AI Twin (SAT) framework, a multi-layered, explainable, and federated DTCS framework that leverages blockchain-based threat intelligence, autoencoder-based anomaly detection, and real-time response mechanisms. The contributions span from data, model, and integration vulnerabilities through to a hybrid anomaly detection system based on unsupervised and federated learning, a real-time response system that balances containment and business-as-usual, and explainable AI that makes automated security decisions transparent and auditable.

## II. DIGITAL TWIN SECURITY LANDSCAPE

There are four layers to a digital twin ecosystem, all with different vulnerabilities. The data acquisition layer, which relies on IoT- and SCADA-based sensors, can be vulnerable to spoofing and data poisoning, particularly when there are numerous unsecured edge devices (Ahmed et al., 2023). Old protocols such as Modbus and OPC-UA are relied upon for communication and were designed for reliability rather than security, making them vulnerable to eavesdropping and replay attacks (Wu et al., 2025). In the modeling layer, the adversarial manipulation (Ali et al., 2025; Note & Ali, 2022) and the poisoning attacks affect accuracy in the detection process, as part of the AI processes twin data. The DTs and enterprise systems/external partners are connected through the risk of exploitation via APIs and supply-chain compromise (Shkarupylo et al., 2024). Such compounded vulnerabilities are known as the Digital Twin Trilemma: fidelity, real-time synchronization, and security (Ridhawi et al., 2023).

International Journal of Engineering & Extended Technologies Research (IJEETR)

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 4, July- August 2026 |

DOI:10.15662/IJEETR.2026.0804001

## III. PROPOSED FRAMEWORK: SECURE-AI TWIN ARCHITECTURE

The proposed SAT structure comprises five functional modules. The data security layer guarantees cryptographically signed data provenance and differential-privacy-preserving sharing across domains. The results demonstrate that the privacy parameter ε = 0.94, which is 62% better than baseline approaches (Alnfiai et al., 2026). This anomaly-detecting layer is provided by an unsupervised autoencoder whose reconstruction error is used to detect anomalies. The federated learning layer, however, is added only to send model updates to a central aggregator (Suleiman et al., 2025). The blockchain-based module provides a permanent audit trail, an identity verification system based on the zero-knowledge principle, and a lightweight Byzantine fault-tolerant consensus algorithm that ensures low latency and synchronization between the distributed twins (Moiceanu & Paraschiv, 2022). The reaction layer enables dynamically isolated containment of compromised components, remediation testing in a sandbox within the twin and human-in-loop verification for decisions that affect the physical operation. The explainable AI (XAI) layer aims to address the challenge of trust and auditing in regulated industrial environments, which have thus far limited the adoption of AI security tools, by generating explanations of detection results at the feature level and in natural language (Zhou et al., 2026).

## IV. EXPERIMENTAL VALIDATION

The framework was tested with 50 distributed nodes across different types of 6G infrastructure in industrial IoT, smart grid, and smart city testbeds, and against 8 attack types, including data injection, distributed denial-of-service, model poisoning, and a cyber-physical false-telemetry attack. The framework achieved an accuracy of 95.0% (baseline 76.4%), precision of 0.968, F1-score of 0.963, and AUC-ROC of 0.989, and reduced the system's latency from 186 ms to 147 ms, corresponding to a 21.2% improvement (Alnfiai et al., 2026). All eight attack types were correctly identified and controlled without disrupting the underlying physical systems.

| Metric | Our Framework | Baseline | Improvement |
|---|---|---|---|
| Detection Accuracy | 95.0% | 76.4% | +27.4% |
| Detection Precision | 0.968 | — | — |
| Detection Recall | 0.959 | — | — |
| F1-Score | 0.963 | — | — |
| AUC-ROC | 0.989 | — | — |
| System Latency | 147 ms | 186 ms | −21.2% |
| Privacy (ε parameter) | 0.94 | 0.58 | +62% |

## V. CHALLENGES AND FUTURE DIRECTIONS

There are still some challenges that are open for future work. As twin networks expand in size and diversity, more work will be needed to optimize the architecture for city-scale or supply-chain-wide deployments (Sharma et al., 2022). However, existing standards such as ISO/IEC 27001 and the NIST Cybersecurity Framework do not explicitly consider digital-twin specific vulnerabilities, creating a regulatory gap that is being filled by bodies like ITU-T and IEEE (International Organization for Standardization, 2022; National Institute of Standards and Technology, 2025). Adversarial actors are also likely to use AI to create adaptive, evasive attacks, potentially leading to AI vs AI cyber conflict. Quantum computing is soon to be fully developed, which will challenge existing cryptographic protections, prompting research into quantum-safe digital twin architectures (Wu et al., 2025). Future directions include the use of a neuromorphic or spiking neural network architecture to achieve ultra-low-latency detection, generative AI for automated testing of adversarial-attack scenarios, deeper extension of the concept of zero trust to federated twin networks, and modular 'security-as-a-twin-service' models composed across industry domains (Ridhawi et al., 2023).

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 4, July- August 2026 |

DOI:10.15662/IJEETR.2026.0804001

## VI. CONCLUSION

With digital twins moving from optimization tools to integral parts of critical infrastructure, there is no longer a choice about purpose-built cybersecurity. Secure-AI Twin has shown that federated and blockchain-verifiable threat intelligence, anomaly detection through autoencoders, and explainable AI can be integrated into a multi-layered defense system that significantly enhances threat detection accuracy and speed compared to a single-layered defense, maintaining the operational fidelity that makes digital twins valuable (Empl et al., 2024; Mihai et al., 2022). The progress will continue when the standards gap is closed, when digital twin ecosystems become more resilient against adversarial and quantum attacks, and when the concept of zero-trust is expanded to increasingly complex digital twin networks, such as those related to smart manufacturing and Industry 5.0 (Moiceanu & Paraschiv, 2022). We wish this framework were a useful contribution to ensuring the mirror world, which will grow increasingly vital for tomorrow's industrial, governmental, and urban systems.

## REFERENCES

1. Ahmed, S. F., Alam, M. S. B., Hoque, M., Lameesa, A., Afrin, S., Farah, T., ... & Muyeen, S. M. (2023). Industrial Internet of Things enabled technologies, challenges, and future directions. Computers and Electrical Engineering, 110, 108847. https://doi.org/10.1016/j.compeleceng.2023.108847
2. Ali, M. L., Thakur, K., Schmeelk, S., Debello, J., & Dragos, D. (2025). Deep learning vs. machine learning for intrusion detection in computer networks: A comparative study. Applied Sciences, 15(4), 1903. https://doi.org/10.3390/app15041903
3. Airehenbuwa, B., Hasan, T., Sarkar, S., & Guin, U. (2025). Advancing security with digital twins: A comprehensive survey. arXiv preprint arXiv:2505.17310. https://doi.org/10.48550/arXiv.2505.17310
4. Alnfiai, M. M., Alotaibi, R. M., & Alotaibi, F. A. (2026). TwinGuard-Sec: A federated blockchain-enabled AI framework for standardized security and privacy in cross-domain digital twin ecosystems over 6G. Scientific Reports. https://doi.org/10.1038/s41598-026-49490-3
5. Doblas-Reyes, F. J., Kontkanen, J., Sandu, I., Acosta, M., Al Turjmam, M. H., Alsina-Ferrer, I., ... & Zimmermann, J. (2026). The Destination Earth digital twin for climate change adaptation. Geoscientific Model Development, 19(7), 2821–2848. https://gmd.copernicus.org/articles/19/2821/2026/gmd-19-2821-2026.pdf
6. Empl, P., Koch, D., Dietz, M., & Pernul, G. (2024). Digital twins in security operations: State of the art and future perspectives. ACM Computing Surveys, 58(1), 1–38. https://doi.org/10.1145/3746279
7. International Organization for Standardization. (2022). ISO/IEC 27001 standard – Information security management systems. ISO. https://www.iso.org/standard/27001
8. Mihai, S., Yaqoob, M., Hung, D. V., Davis, W., Towakel, P., Raza, M., ... & Nguyen, H. X. (2022). Digital twins: A survey on enabling technologies, challenges, trends and future prospects. IEEE Communications Surveys & Tutorials, 24(4), 2255–2291. http://www.parkjonghyuk.net/lecture/2023-1st-lecture/cps/Jimin_Ha.pdf
9. Moiceanu, G., & Paraschiv, G. (2022). Digital twin and smart manufacturing in industries: A bibliometric analysis with a focus on Industry 4.0. Sensors, 22(4), 1388. https://doi.org/10.3390/s22041388
10. National Institute of Standards and Technology. (2025). Cybersecurity framework. National Institute of Standards and Technology. https://www.nist.gov/cyberframework
11. Note, J., & Ali, M. (2022). Comparative analysis of intrusion detection system using machine learning and deep learning algorithms. Annals of Emerging Technologies in Computing, 6(3), 19–36. https://www.researchgate.net/profile/Maaruf-Ali/publication/361550078_Comparative_Analysis_of_Intrusion_Detection_System_Using_Machine_Learning_and_Deep_Learning_Algorithms/links/62b8721a6ec05339cca58b78/Comparative-Analysis-of-Intrusion-Detection-System-Using-Machine-Learning-and-Deep-Learning-Algorithms.pdf
12. Piras, G., Agostinelli, S., & Muzi, F. (2024). Digital twin framework for built environment: A review of key enablers. Energies, 17(2), 436. https://doi.org/10.3390/en17020436
13. Ridhawi, I. A., Otoum, S., & Aloqaily, M. (2023). Decentralized zero-trust framework for digital twin-based 6G. arXiv preprint arXiv:2302.03107. https://doi.org/10.48550/arXiv.2302.03107
14. Sharma, A., Kosasih, E., Zhang, J., Brintrup, A., & Calinescu, A. (2022). Digital twins: State of the art theory and practice, challenges, and open research questions. Journal of Industrial Information Integration, 30, 100383. https://www.sciencedirect.com/science/article/pii/S2452414X22000516
15. Shkarupylo, V., Alsayaydeh, J. A. J., Yusof, M. F. B., Oliinyk, A., Artemchuk, V., & Herawan, S. G. (2024). Exploring the potential network vulnerabilities in the smart manufacturing process of Industry 5.0 via the use of machine learning methods. IEEE Access, 12, 152262–152276. https://ieeexplore.ieee.org/iel8/6287639/6514899/10706596.pdf


|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 4, July- August 2026 |

DOI:10.15662/IJEETR.2026.0804001

16. Stergiou, C. L., Bompoli, E., & Psannis, K. E. (2023). Security and privacy issues in IoT-based big data cloud systems in a digital twin scenario. Applied Sciences, 13(2), 758. https://doi.org/10.3390/app13020758
17. Suleiman, R., Maradapu Vera Venkata Sai, A., Yu, W., & Wang, C. (2025). Blockchain for security in digital twins. Future Internet, 17(9), 385. https://doi.org/10.3390/fi17090385
18. Wu, W., Huang, X., Qin, M., Li, Q., Cheng, N., & Luan, T. H. (2025). AI-native network digital twin for intelligent 6 G network management. IEEE Network. https://doi.org/10.48550/arXiv.2410.01584
19. Zhou, R., Chen, D., Jia, Z., Su, Y., Liu, Y., Lu, Y., ... & He, L. (2026). Digital twin AI: Opportunities and challenges from large language models to world models. arXiv preprint arXiv:2601.01321. https://doi.org/10.48550/arXiv.2601.01321