Global Research Journal in Engineering, Science, Technology and Management (GRJESTM)
Volume 02, Issue 01 (January-February) 2026, pp. 272-279
GRJESTM :: An odaswa™ Journal
ISSN : 3107-3611 (Online)

REVIEW ARTICLE

Neuromorphic Digital Twin Architectures for Adaptive Cybersecurity in Smart Infrastructure

Brian Otieno*[1], Wanjiku Njeri[2], and Daniel Kiptoo[2]

Abstract. The rapid adoption of smart infrastructure has significantly increased the complexity and connectivity of critical systems, including smart cities, intelligent transportation, healthcare networks, industrial automation, and smart energy grids. While digital transformation improves operational efficiency and automation, it also expands the cyberattack surface, making conventional security approaches increasingly inadequate against sophisticated and evolving threats. Neuromorphic computing and Digital Twin technologies have recently emerged as promising solutions for developing adaptive, intelligent, and energy-efficient cybersecurity systems. Neuromorphic computing emulates the information-processing mechanisms of the human brain through event-driven architectures and Spiking Neural Networks (SNNs), enabling real-time anomaly detection with low power consumption. Digital Twins provide virtual representations of physical assets that continuously synchronize with real-world systems, allowing proactive monitoring, threat simulation, and predictive security management. This review examines the integration of neuromorphic computing and Digital Twin architectures for adaptive cybersecurity in smart infrastructure. The paper discusses the principles of neuromorphic intelligence, Digital Twin technology, adaptive cyber defense, enabling technologies, and future research directions. The review highlights how brain-inspired intelligence and real-time virtual modeling can improve cyber resilience, operational reliability, and sustainable security management in next-generation smart infrastructure.

Keywords: Neuromorphic computing, digital twin, adaptive cybersecurity, smart infrastructure, spiking neural networks, cyber resilience

1* Department of Computer Science, Kenyatta University, Kenya
2 School of Computing and Information Technology, Jomo Kenyatta University of Agriculture and Technology, Kenya

Published By **odaswa**. Published in Chennai, Tamil Nadu, India

1. Introduction

Smart infrastructure has become a cornerstone of digital transformation by integrating sensing technologies, communication networks, cloud computing, artificial intelligence (AI), and Internet of Things (IoT) devices into critical infrastructure systems. Applications such as smart cities, intelligent transportation systems, healthcare facilities, industrial control systems, and smart power grids continuously exchange enormous volumes of data to support autonomous monitoring, predictive maintenance, and intelligent decision-making [1], [2]. Although these interconnected environments improve operational efficiency and service quality, they also introduce new cybersecurity challenges arising from increased connectivity, heterogeneous devices, and continuously evolving cyber threats.

Traditional cybersecurity mechanisms primarily rely on signature-based detection, predefined security rules, and centralized monitoring systems. While effective against known attacks, these approaches often struggle to identify previously unseen threats, zero-day vulnerabilities, and sophisticated multi-stage cyberattacks that evolve dynamically over time [3]. Furthermore, conventional security systems frequently require substantial computational resources, limiting their deployment in resource-constrained edge devices commonly found in smart infrastructure.

Artificial intelligence has significantly enhanced cybersecurity by enabling automated threat detection, anomaly identification, malware classification, and predictive risk assessment. Machine learning and deep learning algorithms can analyze large volumes of network traffic and system logs to recognize suspicious behavioral patterns more effectively than conventional rule-based approaches [4]. However, many AI models remain computationally intensive, require large training datasets, and often operate as "black-box" systems, making real-time deployment difficult in latency-sensitive environments.

Neuromorphic computing has emerged as a promising alternative for intelligent cybersecurity by mimicking the computational principles of the biological brain. Introduced by Carver Mead, neuromorphic engineering combines neuroscience, microelectronics, and artificial intelligence to develop energy-efficient computing systems that process information using artificial neurons and spike-based communication [5]. Unlike conventional processors, neuromorphic systems perform asynchronous, event-driven computation, allowing information to be processed only when significant events occur. This approach substantially reduces energy consumption while enabling rapid responses to abnormal system behavior.

Spiking Neural Networks (SNNs), the primary computational model of neuromorphic computing, naturally process temporal information and continuously adapt to changing environments through biologically inspired learning mechanisms such as Spike-Timing-Dependent Plasticity (STDP) [6]. These characteristics make neuromorphic architectures particularly suitable for cybersecurity applications involving continuous monitoring of network traffic, sensor data, and industrial control systems, where rapid anomaly detection and low-latency responses are essential.

Parallel to these developments, Digital Twin technology has transformed infrastructure management by creating virtual representations of physical assets that remain synchronized through real-time sensor data. Originally introduced for engineering and manufacturing applications, Digital Twins now support predictive maintenance, operational optimization, infrastructure monitoring, and risk analysis across numerous industrial sectors [7]. In cybersecurity, Digital Twins enable organizations to simulate attack scenarios, evaluate vulnerabilities, assess system resilience, and test defensive strategies without disrupting physical operations.

The convergence of neuromorphic computing and Digital Twin technology offers a new paradigm for adaptive cybersecurity. Digital Twins provide continuous situational awareness by collecting and modeling operational data from physical infrastructure, while neuromorphic processors analyze these data streams using event-driven intelligence capable of detecting subtle behavioral anomalies with minimal computational overhead. This integration enables security systems that continuously learn from changing network conditions, predict potential attacks, and autonomously adapt defensive responses [8].

Adaptive cybersecurity is becoming increasingly important as cyber threats evolve in complexity and frequency. Unlike static security mechanisms, adaptive cybersecurity systems continuously monitor network behavior, identify emerging attack patterns, evaluate system vulnerabilities, and dynamically modify defense strategies in response to changing threat conditions [9]. Such capabilities are particularly valuable in critical infrastructure environments where uninterrupted operation, low latency, and high reliability are essential.

The integration of neuromorphic intelligence with Digital Twin architectures also supports sustainable cybersecurity. Event-driven processing significantly reduces power consumption compared with conventional deep learning systems, making neuromorphic hardware suitable for edge computing, autonomous sensors, and battery-powered devices deployed across smart infrastructure [10]. Combined with real-time Digital Twin simulations, these energy-efficient architectures provide scalable cybersecurity solutions capable of protecting complex distributed systems while minimizing computational costs.

Understanding the principles of neuromorphic Digital Twin architectures is therefore essential for developing the next generation of intelligent cybersecurity systems. The combination of brain-inspired computation, virtual system modeling, adaptive learning, and real-time threat analysis provides a comprehensive framework for enhancing cyber resilience across smart infrastructure.

This paper reviews the fundamental concepts of neuromorphic computing and Digital Twin architectures for adaptive cybersecurity. It discusses neuromorphic principles, Digital Twin technologies, adaptive threat detection, enabling computational frameworks, and the role of these integrated systems in securing future smart infrastructure against evolving cyber threats.

2. Principles of Neuromorphic Digital Twin Architectures for Adaptive Cybersecurity

The convergence of neuromorphic computing and Digital Twin technology provides a new framework for intelligent cybersecurity in smart infrastructure. Neuromorphic systems contribute energy-efficient, brain-inspired intelligence capable of continuous learning, while Digital Twins provide real-time virtual representations of physical infrastructure for monitoring, prediction, and simulation. Together, these technologies enable adaptive cybersecurity systems that continuously analyze operational behavior, detect anomalies, and respond to evolving cyber threats with minimal latency and computational overhead [11].

2.1. Neuromorphic Computing for Cybersecurity

Neuromorphic computing emulates the architecture and information-processing mechanisms of the human brain. Unlike conventional processors that execute instructions sequentially, neuromorphic systems perform massively parallel, event-driven computation using artificial neurons and synapses [5]. Information is transmitted through electrical spikes, allowing computation only when significant events occur, thereby reducing unnecessary processing and energy consumption.

Spiking Neural Networks (SNNs) serve as the computational foundation of neuromorphic systems. Their ability to process temporal information makes them particularly suitable for

cybersecurity applications involving continuous streams of network traffic, sensor measurements, and system logs [6]. Instead of relying solely on predefined attack signatures, SNNs learn normal behavioral patterns and identify deviations that may indicate cyber intrusions, malware activity, or unauthorized access.

Major advantages of neuromorphic computing for cybersecurity include:

- Ultra-low power consumption.
- Real-time anomaly detection.
- Continuous online learning.
- Low-latency event processing.
- Efficient edge deployment.
- Scalability for distributed infrastructure.

These characteristics make neuromorphic processors suitable for protecting IoT devices, industrial control systems, autonomous vehicles, and smart utility networks where rapid threat detection is essential [10].

2.2. Digital Twin Technology for Cyber Defense

A Digital Twin is a dynamic virtual model that continuously reflects the operational status of a physical asset through real-time data synchronization. Sensors embedded within physical infrastructure collect operational information that is transmitted to the Digital Twin, enabling continuous monitoring, simulation, diagnostics, and predictive analysis [8].

Within cybersecurity, Digital Twins provide a secure virtual environment for evaluating system vulnerabilities without affecting operational infrastructure. Security analysts can simulate attack scenarios, assess the impact of vulnerabilities, evaluate defensive strategies, and optimize security policies before deployment [12].

Digital Twin architectures support cybersecurity by enabling:

- Continuous infrastructure monitoring.
- Vulnerability assessment.
- Attack simulation.
- Predictive risk analysis.
- Incident response planning.
- Security policy validation.

By maintaining synchronized digital representations of physical systems, Digital Twins improve situational awareness and support proactive rather than reactive cybersecurity management.

2.3. Integration of Neuromorphic Computing and Digital Twins

The integration of neuromorphic intelligence with Digital Twin architectures creates adaptive cybersecurity systems capable of learning from continuously changing operational environments. In this framework, IoT sensors collect real-time data from physical infrastructure, Digital Twins organize and simulate system behavior, while neuromorphic processors analyze event streams for abnormal activities.

Instead of processing every incoming data packet continuously, neuromorphic processors respond only to meaningful events. This event-driven computation significantly reduces computational complexity while maintaining rapid detection of suspicious activities such as abnormal communication patterns, unauthorized device behavior, or unexpected control commands [13].

The integration process typically follows these stages:

1. Physical infrastructure generates operational data.
2. IoT sensors collect and transmit system information.
3. Digital Twin continuously updates the virtual model.
4. Neuromorphic processors analyze event streams.
5. AI models detect anomalies and estimate cyber risks.
6. Adaptive security mechanisms initiate appropriate responses.

This architecture enables autonomous cyber defense while maintaining high computational efficiency and operational scalability.

2.4. Adaptive Threat Detection and Response

Traditional cybersecurity systems often rely on predefined attack signatures, making them less effective against previously unknown threats. Adaptive cybersecurity employs continuous monitoring and intelligent learning to identify emerging attack patterns before significant damage occurs [14].

Neuromorphic Digital Twin architectures support adaptive defense through:

- Behavioral anomaly detection.
- Continuous threat learning.
- Predictive attack forecasting.
- Autonomous response generation.
- Dynamic security policy adaptation.

Artificial intelligence analyzes deviations between expected Digital Twin behavior and observed physical system activity. When significant inconsistencies are detected, neuromorphic processors rapidly classify potential threats and recommend mitigation strategies. Since Digital Twins continuously update their models using live operational data, defensive mechanisms evolve alongside changing infrastructure conditions.

This adaptive capability is particularly valuable for critical infrastructure, where uninterrupted operation and rapid threat mitigation are essential.

2.5. Applications in Smart Infrastructure

The combination of neuromorphic intelligence and Digital Twin technology has broad applicability across numerous critical infrastructure sectors.

- **Smart Cities**

Continuous monitoring of transportation systems, surveillance networks, environmental sensors, and municipal services enables early detection of cyber intrusions affecting urban infrastructure [1].

- **Smart Power Grids**

Adaptive cybersecurity protects power generation, transmission, and distribution systems against cyberattacks targeting supervisory control and data acquisition (SCADA) networks and energy management systems [15].

- **Industrial Control Systems**

Manufacturing facilities employ Digital Twins and neuromorphic processors to secure programmable logic controllers (PLCs), robotic production lines, and industrial IoT devices against operational disruptions [16].

- **Healthcare Infrastructure**

Hospitals increasingly depend upon connected medical devices, electronic health records, and telemedicine platforms. Intelligent cybersecurity systems help detect unauthorized access and protect sensitive patient information.

- **Intelligent Transportation**

Autonomous vehicles, railway control systems, and traffic management platforms require continuous cybersecurity monitoring to ensure operational safety and minimize disruptions.

2.6. Summary

Neuromorphic Digital Twin architectures combine brain-inspired intelligence with virtual system modeling to create adaptive cybersecurity solutions for smart infrastructure. Neuromorphic processors enable low-power, event-driven anomaly detection, while Digital Twins provide continuous monitoring, attack simulation, and predictive security assessment. Together, these technologies support real-time threat detection, autonomous adaptation, and resilient cyber defense across critical infrastructure. As smart infrastructure continues to expand, the integration of neuromorphic computing and Digital Twin technology is expected to play an increasingly important role in developing intelligent, scalable, and sustainable cybersecurity systems.

3. Conclusion

The rapid expansion of smart infrastructure has significantly increased the need for intelligent, adaptive, and energy-efficient cybersecurity solutions. Traditional security mechanisms, although effective against known threats, are often

inadequate for defending highly connected cyber-physical systems against sophisticated, dynamic, and zero-day attacks. The convergence of neuromorphic computing and Digital Twin technology offers a promising solution by combining brain-inspired intelligence with real-time virtual system modeling. This integrated approach enables continuous monitoring, adaptive learning, predictive threat analysis, and autonomous cyber defense while maintaining low computational and energy requirements.

Neuromorphic computing introduces event-driven processing through Spiking Neural Networks (SNNs), allowing cybersecurity systems to analyze temporal data efficiently and detect abnormal behavior with minimal latency. Unlike conventional AI models that require substantial computational resources, neuromorphic architectures support real-time inference and continuous learning using significantly lower power. These characteristics make them highly suitable for deployment in IoT devices, edge computing platforms, industrial control systems, and other resource-constrained environments.

Digital Twin technology complements neuromorphic intelligence by providing synchronized virtual representations of physical infrastructure. Through continuous integration of sensor data, Digital Twins enable organizations to monitor system performance, simulate cyberattack scenarios, evaluate vulnerabilities, and validate security strategies before deployment. This proactive capability improves cyber resilience by allowing security teams to anticipate potential risks rather than merely responding after attacks occur.

The combination of these technologies creates an adaptive cybersecurity framework capable of responding dynamically to evolving threats. The major contributions of Neuromorphic Digital Twin architectures can be summarized as follows:

- **Provides continuous real-time monitoring** of smart infrastructure through synchronized Digital Twins.
- **Enables ultra-low-power cybersecurity** using event-driven neuromorphic processors.
- **Detects behavioral anomalies** through Spiking Neural Networks rather than relying solely on attack signatures.
- **Supports predictive threat intelligence** by combining AI analytics with Digital Twin simulations.
- **Improves cyber resilience** through adaptive learning and continuous security updates.
- **Reduces response latency** by deploying neuromorphic intelligence at edge devices.
- **Allows safe cyberattack simulation** without affecting operational infrastructure.
- **Enhances scalability** for large distributed IoT and cyber-physical systems.
- **Minimizes computational overhead**, making deployment feasible for resource-constrained environments.
- **Supports sustainable cybersecurity** through energy-efficient computing architectures.

Despite these advantages, several challenges remain before large-scale deployment becomes practical. Standardized Digital Twin architectures for cybersecurity are still evolving, while interoperability among heterogeneous infrastructure systems continues to present technical difficulties. Additional challenges include securing Digital Twin communication channels, protecting sensitive operational data, ensuring AI explainability, reducing false-positive detections, and integrating neuromorphic hardware into existing cybersecurity infrastructures. Furthermore, regulatory compliance, cybersecurity governance, and workforce expertise will play important roles in successful implementation.

Future research should focus on improving neuromorphic hardware platforms, developing explainable Spiking Neural Networks, integrating

federated learning for distributed cyber defense, and combining Digital Twins with large-scale edge intelligence for autonomous security management. Emerging technologies such as quantum-safe cryptography, 6G communication networks, intelligent autonomous agents, and self-healing cyber-physical systems are expected to further strengthen adaptive cybersecurity capabilities in future smart infrastructure.

In conclusion, Neuromorphic Digital Twin architectures represent a transformative direction for next-generation cybersecurity by integrating brain-inspired computing with real-time virtual modeling. Their ability to provide adaptive learning, predictive threat detection, low-power computation, and autonomous decision support makes them highly suitable for protecting critical smart infrastructure. As research in neuromorphic hardware, Digital Twin technologies, and artificial intelligence continues to mature, these integrated architectures are expected to become a fundamental component of resilient, scalable, and sustainable cybersecurity systems.

Acknowledgement

The authors sincerely thank the faculty members of their institution for their continuous guidance and encouragement throughout this study. They also express their gratitude to the library and research staff for providing essential resources. Special appreciation is extended to colleagues and peers for their valuable feedback and support.

References

[1] A. Zanella, N. Bui, A. Castellani, L. Vangelista, and M. Zorzi, "Internet of Things for smart cities," IEEE Internet of Things Journal, vol. 1, no. 1, pp. 22–32, 2014.

[2] M. Ammar, G. Russello, and B. Crispo, "Internet of Things: A survey on the security of IoT frameworks," Journal of Information Security and Applications, vol. 38, pp. 8–27, 2018.

[3] S. Mansfield-Devine, "The growth and evolution of cyber threats," Network Security, vol. 2018, no. 10, pp. 5–8, 2018.

[4] I. Goodfellow, Y. Bengio, and A. Courville, Deep Learning. Cambridge, MA, USA: MIT Press, 2016.

[5] C. Mead, Analog VLSI and Neural Systems. Reading, MA, USA: Addison-Wesley, 1989.

[6] W. Maass, "Networks of spiking neurons: The third generation of neural network models," Neural Networks, vol. 10, no. 9, pp. 1659–1671, 1997.

[7] M. Grieves and J. Vickers, "Digital Twin: Mitigating unpredictable, undesirable emergent behavior in complex systems," in Transdisciplinary Perspectives on Complex Systems, Springer, 2017, pp. 85–113.

[8] F. Tao, H. Zhang, A. Liu, and A. Y. C. Nee, "Digital Twin in industry: State-of-the-art," IEEE Transactions on Industrial Informatics, vol. 15, no. 4, pp. 2405–2415, 2019.

[9] S. Jajodia, A. K. Ghosh, V. Swarup, C. Wang, and X. S. Wang, Moving Target Defense: Creating Asymmetric Uncertainty for Cyber Threats. New York, NY, USA: Springer, 2011.

[10] M. Davies et al., "Loihi: A neuromorphic manycore processor with on-chip learning," IEEE Micro, vol. 38, no. 1, pp. 82–99, 2018.

[11] F. Tao and M. Zhang, Digital Twin Driven Smart Manufacturing. London, U.K.: Academic Press, 2019.

[12] E. Jones, S. K. Sharma, and R. Clarke, "Digital twins for cyber situational awareness and resilience," Computers & Security, vol. 115, Art. no. 102603, 2022.

[13] B. Rajendran, A. Sebastian, M. Schmuker, N. Srinivasa, and E. Eleftheriou, "Low-power neuromorphic hardware for signal processing applications," Nature Electronics, vol. 2, no. 10, pp. 1–13, 2019.

[14] R. Mitchell and I. R. Chen, "Adaptive intrusion detection for cyber-physical systems," IEEE Transactions on Dependable and Secure Computing, vol. 12, no. 1, pp. 1–14, 2015.

[15] A. Hahn, A. Ashok, S. Sridhar, and M. Govindarasu, "Cyber-physical security testbeds: Architecture, application, and evaluation for smart grid," IEEE Transactions on Smart Grid, vol. 4, no. 2, pp. 847–855, 2013.

[16] E. A. Lee, "Cyber-physical systems—Are computing foundations adequate?" Position Paper, NSF Workshop on Cyber-Physical Systems, Austin, TX, USA, 2006.

[17] H. He and J. Yan, "Cyber-physical attacks and defenses in the smart grid: A survey," IET Cyber-Physical Systems: Theory & Applications, vol. 1, no. 1, pp. 13–27, 2016.

[18] N. R. Jennings, "Autonomous agents: Theory and practice," The Knowledge Engineering Review, vol. 10, no. 2, pp. 115–152, 1995.

[19] P. A. Laplante, Cyber-Physical Systems Engineering. Boca Raton, FL, USA: CRC Press, 2017.

[20] G. A. Fink, D. M. Nicol, E. D. Edgar, and B. F. Rice, "Tools for cyber security situational awareness," IEEE Computer, vol. 45, no. 4, pp. 22–30, 2012.

[21] A. A. Cárdenas, S. Amin, and S. Sastry, "Research challenges for the security of control systems," Proceedings of the 3rd USENIX Workshop on Hot Topics in Security, San Jose, CA, USA, 2008.

[22] G. E. Hinton, "Deep learning—A technology with the potential to transform cybersecurity," Nature Electronics, vol. 2, no. 1, pp. 44–45, 2019.

[23] NIST, Framework for Improving Critical Infrastructure Cybersecurity, Version 2.0. Gaithersburg, MD, USA: National Institute of Standards and Technology, 2024.