



AI-Enabled Digital Twins for Smart Grids: Real-Time Monitoring, Predictive Control, Cybersecurity and Future Research Directions



Jennifer Ikeoluwa Ade-moomiyo, Micheal Abimbola Oladosu*, Moses Adondua Abah,
Ugonna Stanley Nwani, Ifechukwu Victor Muoghalu, Anyan Adebayo Anyan

Abstract: Digital twin (DT) technology combined with artificial intelligence (AI) is becoming a key enabler for resilient and self-optimising electrical power networks that are increasingly digitalised. A digital twin is a continuously updated virtual representation of a physical grid asset or network that uses real-time sensor, phasor measurement unit (PMU), and Internet of Things (IoT) data to closely mirror its physical counterpart. Digital twins become predictive, prescriptive, and self-healing decision-support systems when machine learning (ML) and deep learning (DL) algorithms are integrated into this virtual-physical feedback loop. This review aims to bring together the recent literature (2020-2025) on the field of AI-powered digital twins under four thematic areas: (i) architectural foundations and enabling technologies, (ii) real-time monitoring and state estimation, (iii) predictive control and maintenance, and (iv) cybersecurity monitoring and threat mitigation. Tables summarise enabling technologies, predictive-control case studies, and case studies of cyber-threat countermeasures reported in the literature. The review also pinpoints open research challenges such as interoperability standards, federated and privacy-preserving learning, explainability of AI-driven decisions on the grid, and quantum-assisted twin computation. It suggests a research roadmap for further work. The synthesis signals that while AI-powered digital twins can tangibly reduce unplanned downtime, improve forecasting precision, and boost cyber-physical attack resilience, standardisation, data governance, and trustworthy AI remain to be addressed to enable widespread adoption.

Keywords: Digital twin, Artificial Intelligence, Smart Grid, Real-time Monitoring, Predictive Control, Cyber Security, Machine Learning, Power Systems.

Nomenclature:

DT: Digital Twin
AI: Artificial Intelligence
PMU: Phasor Measurement Unit
DL: Deep Learning
IoT: Internet of Things
DOI: Digital Object Identifier
GRU: Gated Recurrent Units
RNN: Recurrent Neural Networks
STLF: Short-Term Load Forecasting
LSTM: Long Short-Term Memory

I. INTRODUCTION

The electrical power grid is shifting from a centralised, bidirectional system to a decentralised system with high penetration of distributed renewable energy resources, electric vehicles, and distributed generation. This shift, known as the smart grid paradigm, requires technologies that can handle ever-growing complexity, variability and cyber risk. The digital twin has been proposed as a useful solution, providing a virtual representation of the grid's assets that can be interrogated, simulated, and optimised in real time without interrupting physical grid operations [1]. The digital twin concept, coupled with AI, extends beyond 3D visualisation to predictive and prescriptive capabilities: AI models informed by historical and real-time operating data can anticipate future states, suggest control actions, and identify anomalies that indicate equipment degradation or tampering [2].

Three closely related key grid functions are especially significant for the impact of AI and digital twins. First, deep learning frameworks such as recurrent and convolutional neural networks increasingly combine multiple disparate measurement streams into a comprehensive grid state over time, even when the data is incomplete or corrupted.[3] Second, predictive control and maintenance use artificial intelligence (AI) to anticipate asset degradation, load and renewable generation, and proactively schedule maintenance and optimise asset dispatch to minimise unplanned outages and maximise asset life [4-6]. Third, a cybersecurity monitoring system provides a safe, high-fidelity environment to train, test, and continuously validate cybersecurity use cases such as intrusion detection and anomaly detection models for developing cyber-physical threats that affect the operational grid without risking harm to the real grid [7,8]. Although it is gaining popularity, the literature is still divided and

Manuscript received on 05 August 2026 | First Revised Manuscript received on 14 August 2026 | Second Revised Manuscript received on 06 September 2026 | Manuscript Accepted on 15 September 2026 | Manuscript published on 30 September 2026

Jennifer Ikeoluwa Ade-moomiyo, Department of Electrical and Information Engineering, Landmark University, Faculty of Engineering, Omu-Aran, Kwara State, Nigeria. Email ID: jenniferikeoluwa@gmail.com, ORCID ID: [0009-0000-9916-0749](https://orcid.org/0009-0000-9916-0749)

Micheal Abimbola Oladosu*, Department of Chemical Science, Anchor University, Ayobo, Lagos, Nigeria. Email ID: mikeoladosu@gmail.com, ORCID ID: [0009-0000-5098-1247](https://orcid.org/0009-0000-5098-1247)

Moses Adondua Abah, Department of Biochemistry, Federal University of Wukari, Faculty of Pure and Applied Sciences, Wukari, Taraba, Nigeria. Email ID: m.abah@fuwukari.edu.ng, ORCID ID: [0000-0002-9268-1661](https://orcid.org/0000-0002-9268-1661)

Ugonna Stanley Nwani, Department of Computer Engineering, Obafemi Awolowo University, Faculty of Computing, Ile-Ife, Osun State, Nigeria. Email ID: ugonna.nwani@gmail.com, ORCID ID: [0009-0006-1549-9627](https://orcid.org/0009-0006-1549-9627)

Ifechukwu Victor Muoghalu, Department of Mechanical Engineering, University of Coimbra, Portugal, Faculty of Engineering, Paço das Escolas, Coimbra, Portugal. Email ID: muoghaluvictor@gmail.com, ORCID ID: [0000-0002-6659-4636](https://orcid.org/0000-0002-6659-4636)

Anyan Adebayo Anyan, Department of Social Science, College of Management and Human Potential, Walden University, Minneapolis, United States of America (USA). Email ID: anya.anya@walden.edu, ORCID ID: [0009-0006-9494-5313](https://orcid.org/0009-0006-9494-5313)

© The Authors. Published by Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP). This is an open access article under the CC-BY-NC-ND license <http://creativecommons.org/licenses/by-nc-nd/4.0/>

has not been synthesised across domains, especially between power engineering and computer science/cybersecurity. This review brings together recent (2020–2025) peer-reviewed work into a cohesive narrative based on monitoring, control, and security, and ends with a forward-looking research agenda. Section 2 describes the review methodology; Section 3 outlines digital twin architecture and enabling technologies; Section 4 addresses AI-enabled real-time monitoring; Section 5 examines predictive control and maintenance; Section 6 reviews cybersecurity applications; Section 7 discusses open challenges and future research directions; and Section 8 concludes the review.

II. METHODOLOGY

This review used a structured approach based on systematic review patterns and a narrative-synthesis method (e.g., broadly following PRISMA screening logic) to search for, screen, and synthesise peer-reviewed literature on AI-enabled digital twins for smart grids between January 2020 and January 2025.

A. Search Strategy

We collected literature from IEEE Xplore, ScienceDirect (Elsevier), MDPI (Applied Sciences, Energies, Electronics), the ACM Digital Library, and Springer Nature Link, and used citation chaining in Google Scholar to identify recent conference proceedings. Search terms included the core concept "digital twin" AND "smart grid" OR "power system" OR "microgrid", which was then further intersected with domain-specific terms: "artificial intelligence", "machine learning", "deep learning", "real-time monitoring", "state estimation", "predictive maintenance", "predictive control", "federated learning", "cybersecurity", and "intrusion detection". Boolean operators (AND/OR) and truncation broadened the search results, and the publication period was limited to 2020-2025 to ensure the results were current.

B. Inclusion and Exclusion Criteria

Records were considered if they: (i) were published in a peer-reviewed journal or peer-reviewed conference proceedings between 2020 and 2025; (ii) mentioned digital twin technology in the context of smart grids, microgrids or power system elements; (iii) contained an AI, machine learning or deep learning element within the digital twin's monitoring, control or security function; and (iv) included a verifiable digital object identifier (DOI) and full bibliographic metadata. We excluded records that were preprints without peer review, publications not in English,

editorials/opinion pieces lacking technical content, or records whose bibliographic details (authorship, journal, volume, DOI) could not be reproduced independently from data provided by the publisher or the database used for the citation.

C. Screening and Data Extraction

We first screened titles and abstracts for topical relevance to the three thematic pillars of this review (real-time monitoring, predictive control/maintenance, and cybersecurity). We conducted full-text screening for inclusion/exclusion according to the aforementioned criteria. We retrieved the following information for each eligible record: publication year, journal/venue, AI technique(s) used, grid asset or scope addressed, and the main goal or benefit reported. This extraction is the basis for the comparative synthesis in Tables 1–3. After full-text screening and DOI verification, 17 studies that met all inclusion criteria were included in the final synthesis, with no attempt to prioritise or exclude studies based on reference count.

D. Synthesis Approach

Because of the diversity of study design, measurement, and reported outcomes, we used a narrative and thematic synthesis instead of pooling data through meta-analysis. The included studies were organised around the four themes introduced in Section 1 (architecture/enabling technologies, real-time monitoring, predictive control/maintenance, and cybersecurity), and cross-cutting observations were used to identify open challenges and future research directions in Section 8.

III. DIGITAL TWIN ARCHITECTURE AND ENABLING TECHNOLOGIES

A typical grid digital twin is comprised of three layers: the physical layer consisting of sensors, meters, physics-based models and data-based models replicating the network topology, equipment state and load/generation profile, and the connection layer consisting of communication protocols and middleware that synchronise the physical and virtual layers in near real-time [1,2]. Recent frameworks add a fourth, "cognitive," layer that uses AI models such as forecasting networks, reinforcement-learning agents, and anomaly detectors on the virtual layer's data to produce predictive and prescriptive outputs [3,9]. Table I summarises the main enabling technologies, covering data acquisition, communication, modelling, and AI/analytics.

Table I: Technologies to Enable Smart Grid Digital Twins with AI

Technology Layer	Representative Technologies	Primary Function in the Digital Twin	Key Reference(s)
Physical / sensing	PMUs, smart meters, IoT sensors, SCADA	High-resolution data acquisition for state replication	[1,3]
Connectivity/middleware	5G, MQTT/OPC-UA, edge– cloud architectures	Low-latency, bidirectional physical–virtual synchronisation	[2,9]
Virtual modelling	Physics-based network models, co-simulation platforms, real- time digital simulators	High-fidelity replication of topology and dynamics	[3]
AI/analytics (cognitive layer)	LSTM/GRU/CNN forecasting, reinforcement learning, federated learning	Prediction, optimisation, and privacy-preserving learning	[4,5,10,11]
Security layer	Blockchain, intrusion-detection ML, cyber-range twins	Attack simulation, detection, and resilient response	[7,8,14-16]

The layered architecture can be used at the microgrid scale to demonstrate its practical application: digital twins of

distributed energy resources can be used to co-simulate



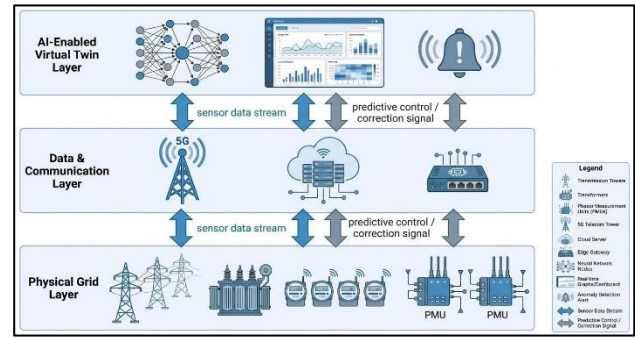
the variability of renewables, storage dispatch, and demand response before resorting to physical control actions, which enables operators to enhance resilience and economic efficiency of an islanded and grid-connected operation [2]. At the transmission and distribution level, a growing number of inverter-based resources are causing faster and more erratic dynamics in the network, and state replication, scalable by using modular and real-time simulator-based twins, is becoming more critical where communication bandwidth or measurement density is limited [3].

IV. AI-ENABLED REAL-TIME MONITORING AND STATE ESTIMATION

Real-time monitoring is the digital twin's bottom-line function. Without an accurate, up-to-the-minute snapshot of how the grid is running, downstream predictive and prescriptive functions cannot be relied upon. However, as modern measurement streams grow in volume, velocity, and, in some cases, incompleteness, classical state-estimation techniques cannot handle this scale of data, motivating the incorporation of deep learning into the state-estimation pipeline [3]. Hybrid architectures that combine convolutional feature extraction with long short-term memory (LSTM) sequence modelling have also shown strong performance in the short-term load forecasting (STLF) problem, which is closely related to real-time monitoring because the forecasting error feeds directly into the state-estimation confidence intervals [4]. Likewise, an ensemble of stacked gated recurrent units (GRU) and recurrent neural networks (RNN) has been applied to jointly predict renewable electricity generation and load for smart grid operation, further enhancing the digital twin's ability to predict short-horizon deviations between predicted and measured states [5].

Beyond forecasting, AI-powered digital twins are now used to estimate grid state even when some measurements are lost or damaged due to communication failures or malicious interference. Attention-based or reinforcement models that fuse data can fill in missing grid data, creating a plausible state from partial observability [3].

This ability is especially useful in distribution networks, where measurement density has historically been lower than in transmission networks and where the rising adoption of distributed generation makes 24/7, high-confidence situational awareness more important. To show the closed-loop information flow between the physical grid, the AI-empowered virtual twin, and the human/automated operator, [Figure 1](#) depicts the data flow between these components.



[Fig.1: Closed-Loop Architecture of an AI-Enabled Smart Grid Digital Twin for Real-Time Monitoring]

Source: Conceptual synthesis based on the three/four-layered digital twin architectures as described in references [1,2,3,9].

V. AI-DRIVEN PREDICTIVE CONTROL AND MAINTENANCE

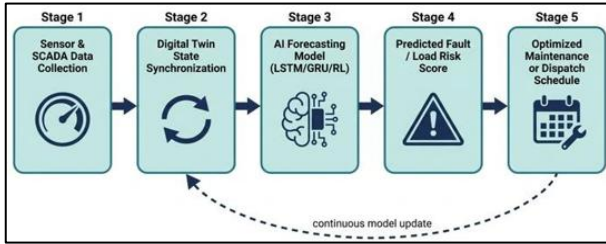
Predictive control takes digital twin monitoring one step further into the temporal plane. It involves planning maintenance, dispatching, and controlling actions before a failure, based on AI-generated predictions. Predictive maintenance based on digital twin technology has been shown to deliver significant improvements over conventional calendar- or threshold-based maintenance, such as increased accuracy of fault diagnosis in manufacturing, power and aerospace sectors, and a decrease in unplanned downtime in the power sector, especially given the critical need to avoid transformer and generator outages in that field due to the high cost of such events [6]. Digital twins of specific renewable assets, such as parabolic-trough solar collector assets, have been used to track thermal and electrical performance against physics-based and data-driven models in real time, to detect performance degradation before it reaches an unplanned degradation state [7].

A specific sub-theme in predictive control that has gained significant interest is deep reinforcement learning (DRL), which enables the digital twin to be used in a safe training and validation environment, where control policies can be learned through simulated trial and error before deployment on the physical asset. To show the twin's ability to act as a forecaster, simulator, and policy trainer in the same closed loop, a recent micro-grid digital twin using DRL and real-time optimisation was shown to deliver better battery scheduling and load-balancing performance than purely rule-based control [9]. Researchers have also developed digital twins of wind turbines, based on machine learning-based predictive modelling, to predict component wear and schedule maintenance tasks under variable wind conditions, minimising maintenance costs and generation losses [8]. [Table II](#) briefly summarises representative predictive-maintenance and predictive-control case studies from the surveyed literature, detailing the AI technique used, the targeted grid asset, and the reported operational gain. [Figure 2](#) shows the AI-powered predictive maintenance and control processes in a digital twin loop.



Table II: A Set of AI-Based Predictive Control and Maintenance Case Studies from Representatives (2020-2025)

Study	Grid Asset / Scope	AI Technique	Reported Benefit
Zhong et al. (2023) [6]	Cross-sector power, manufacturing, aerospace assets	ML/DL-based fault prediction framework (PdMDT)	Improved fault-diagnosis accuracy; framework for predictive maintenance scheduling
Machado et al. (2023) [7]	Fresnel solar thermal collector	Physics-informed data-driven digital twin	Early detection of thermal/electrical performance degradation
Fahim et al. (2022) [8]	Wind turbine components	Machine learning-based predictive modelling	Improved remaining-useful-life estimation and maintenance scheduling
Ozkan, K��k & ��zdemir (2024) [9]	Microgrid battery storage and load balancing	Deep reinforcement learning-supported digital twin (Deep Twin)	Improved energy efficiency and load-balancing over rule-based control
Xia et al. (2021) [5]	Distribution-level renewable and load forecasting	Stacked GRU–RNN ensemble	Improved short-term load and renewable generation forecast accuracy



[Fig.2: AI-Enabled Predictive Maintenance and Control Workflow Within a Digital Twin Loop]

Source: Conceptual synthesis of the predictive maintenance and reinforcement-learning control loops reported in references [6,8,9].

VI. CYBERSECURITY MONITORING AND RESILIENCE

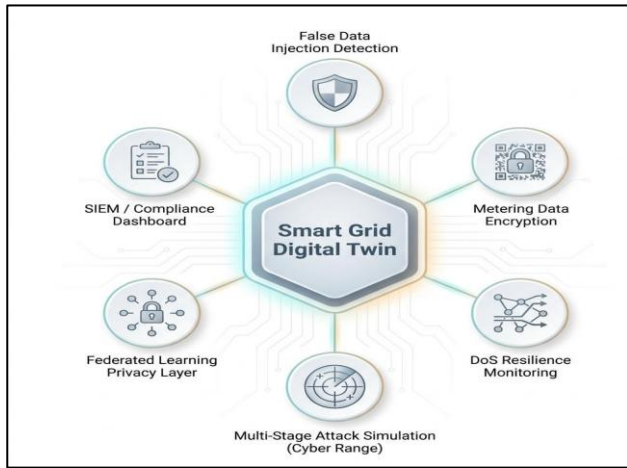
This real-time connectivity that enables digital twin functionality also increases the smart grid's cyber-attack surface, prompting a growing body of work to use the digital twin itself as a cybersecurity tool. Federated learning is one of the most significant enabling techniques, as it allows AI models used to predict loads and detect anomalies to be trained collaboratively on edge devices without sending raw consumer energy data to the central server, which would otherwise create high communication loads and privacy risks [10,11]. Edge–cloud collaborative federated learning frameworks have been shown to preserve forecasting accuracy similar to centralised training while significantly reducing the risk of individual household energy-consumption data breaches [10], and communication-efficient federated schemes have extended this private-by-design paradigm to energy-prediction tasks relevant to digital twin synchronisation [11].

On the detection side, recurrent neural network-based classifiers have been applied to detect false data injection attacks in a DC microgrid, detecting tampered electrical measurements based on their temporal correlation in the electrical sensor data and setting the tampered ones aside to prevent the digital twin state estimation from being incorrect [12]; at the same time, cryptographically secured metering-data aggregation protocols offer complementary protection from tampering during transmission from the smart meters to the data layer of the digital twin [13]. A few recent studies directly use the digital twin as a cyber-physical test range by creating a digital twin instrumented with open-source security information and event management tooling to continuously monitor the cybersecurity of a distribution system, compliant with the EU NIS2 directive [14] (FIWARE-based architecture); and by using the same digital twin to specifically evaluate the detection accuracy for cyber-attack scenarios reproduced in the virtual environment [15].

Complementary work in the field of hardware-in-the-loop digital twin designs an explicit digital twin to test and evaluate a grid's detection countermeasures under realistic attack conditions before they are implemented on the operational grid [16]; meanwhile, digital twin-based resilience studies show how resilient microgrid control is against denial-of-service conditions and how maintaining an accurate virtual state helps control systems maintain acceptable performance when communication channels are actively degraded by an adversary [17]. Table III shows the main cyber threat categories and corresponding AI/digital twin-based cyber countermeasures from the reviewed literature. Figure 3 presents the cybersecurity monitoring framework for smart grids using a digital twin.

Table III: Cyber-Physical Risks and Countermeasures to Smart Grids Using AI/Digital Twin Technology

Threat Category	Attack Vector / Description	AI/Digital Twin Countermeasure	Key Reference(s)
False data injection (FDI)	Manipulation of sensor/measurement values to corrupt state estimation	RNN-based temporal anomaly classifiers; twin-based cross-validation of measurements	[12]
Metering data tampering	Interception or alteration of smart-meter data in transit	Cryptographic batch-verification and secure aggregation protocols	[13]
Denial-of-service (DoS)	Disruption of communication channels supporting twin synchronization	Digital twin-sustained state estimation and resilient microgrid control during degraded connectivity	[17]
Multi-stage / advanced persistent threats	Coordinated intrusion across IT/OT boundaries	Cyber-physical digital twin test ranges for detection-rule validation and countermeasure evaluation.	[15,16]
Privacy leakage from consumption data	Exposure of granular household energy-use patterns	Federated and edge–cloud collaborative learning without raw data centralisation	[10,11]
Regulatory / infrastructure-wide monitoring gaps	Fragmented visibility across distributed critical infrastructure	FIWARE-based digital twin with integrated SIEM for continuous compliance-aligned monitoring	[14]



[Fig.3. Digital Twin-Enabled Cybersecurity Monitoring Framework for Smart Grids]

Source: Conceptual synthesis of digital twin cybersecurity monitoring approaches reported in references [10-17].

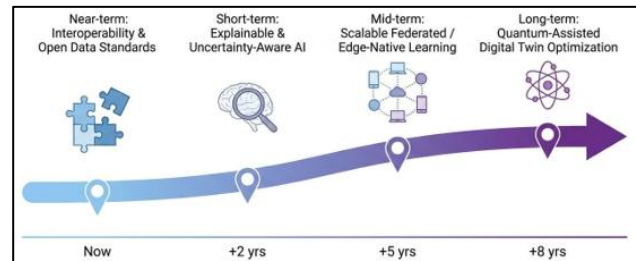
VII. CHALLENGES AND FUTURE RESEARCH DIRECTIONS

While AI-powered digital twins in smart grids have made significant strides, challenges still limit widespread adoption. Although AI-powered digital twins in smart grids have come a long way, they still face several obstacles to widespread adoption. First is the lack of interoperability: virtual models are often built on a particular platform using a specific data schema, making it difficult to integrate with multi-vendor equipment and across transmission–distribution boundaries [1,3]. Second, communication overhead, non-independent and identically distributed (non-IID) data across nodes, and vulnerability to poisoning attacks remain open problems that require new algorithms in federated and privacy-preserving learning approaches [10,11]. Third, explainability of AI-based predictive and control decisions is still not mature enough for safety-critical grid operations: operators should understand the logic behind AI-based predictions and recommendations before they can trust them in safety-critical scenarios. Finally, the cyber security literature shows that digital twins are not merely a defensive measure but also a potential new attack surface; an inaccurate or compromised digital twin can mislead operators, requiring mechanisms to verify twin integrity in addition to threat detection [14-17].

Four research avenues are particularly promising for the future. (ii) Uniform digital twin data models and application programming interfaces would significantly reduce integration costs and facilitate cross-utility benchmarking of AI models. (iii) Explainable and uncertainty-aware AI, such as probabilistic forecasting and interpretable reinforcement learning, would increase operator confidence and regulatory acceptability of AI-recommended control actions.

(iii) Federated and edge-native learning architectures can be scalable and communication-efficient, enabling the training and updating of digital twins across thousands of distributed assets, while maintaining consumer privacy and not overloading the communication infrastructure [10,11]. The quantum-assisted optimisation paradigm and hybrid classical–quantum digital twin system are emerging concepts which may ultimately solve the combinatorial

problem of real-time optimal power flow and contingency analysis at a national grid scale, but are currently physically unfeasible and therefore in a nascent phase. Based on these, Figure 4 outlines a proposed research roadmap that combines these directions into a structured plan.



[Fig.4: Research Roadmap for Next-Generation AI-Enabled Smart Grid Digital Twins (2025–2030+)]

Source: Author's proposed synthesis derived from open challenges discussed across references [1,3,10,11,14-17].

VIII. CONCLUSION

AI-powered digital twins are a developing yet maturing technology for smart grid modernisation, offering a holistic solution for real-time monitoring, predictive control, and cybersecurity resilience. The evidence presented here shows that integrating machine learning and deep learning models into the virtual-physical feedback loop through the digital twin yields measurable operational benefits, such as better forecasting, earlier fault detection, and improved detection of cyber-physical threats. Despite this, challenges of interoperability, explainability, privacy-preserving scalability, and twin-integrity assurance remain unresolved. They will shape research and deployment over the next decade. The value of AI-powered digital twins, as shown in these pilot projects, must be scaled up and integrated into future smart grids through continued cross-disciplinary collaboration among power systems engineers, AI researchers, and cybersecurity experts.

ACKNOWLEDGMENTS

The authors acknowledge the contributions of researchers worldwide whose published work forms the foundation of this review.

DECLARATION STATEMENT

After aggregating input from all authors, I must verify the accuracy of the following information as the article's author.

- **Conflicts of interest:** Based on my understanding, this article has no conflicts of interest.
- **Funding/Grants/Financial Support:** This article has not been sponsored or funded by any organisation or agency.
- **Ethical Approval and Consent to Participate:** The data provided in this article are exempt from ethical approval or participant consent requirements.
- **Data Access Statement and Material Availability:** The adequate resources of this article are publicly accessible.
- **Author's Contribution:** The authorship of this



Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)
© Copyright: All rights reserved.

article is contributed equally to all participating individuals.

REFERENCES

- Sifat MMH, Choudhury SM, Das SK, Ahamed MH, Muyeen SM, Hasan MM, et al. Towards an electric digital twin grid: technology and framework review. *Energy AI*. 2023; 11:100213. DOI: [10.1016/j.egyai.2022.100213](https://doi.org/10.1016/j.egyai.2022.100213)
- Bazmohammadi N, Madary A, Vasquez JC, Bazmohammadi H, Khan B, Wu Y, et al. Microgrid digital twins: concepts, applications, and future trends. *IEEE Access*. 2022; 10:2284-302. DOI: [10.1109/ACCESS.2021.3138990](https://doi.org/10.1109/ACCESS.2021.3138990)
- Arraño-Vargas F, Konstantinou G. Modular design and real-time simulators toward power system digital twins' implementation. *IEEE Trans Ind Inform*. 2023;19(1):52-61. DOI: [10.1109/TII.2022.3178713](https://doi.org/10.1109/TII.2022.3178713)
- Rafi SH, Al-Masood N, Deebea SR, Hossain E. A short-term load forecasting method using integrated CNN and LSTM network. *IEEE Access*. 2021; 9:32436-48. DOI: [10.1109/ACCESS.2021.3060654](https://doi.org/10.1109/ACCESS.2021.3060654)
- Xia M, Shao H, Ma X, de Silva CW. A stacked GRU-RNN-based approach for predicting renewable energy and electricity load for smart grid operation. *IEEE Trans Ind Inform*. 2021;17(10):7050-9. DOI: [10.1109/TII.2021.3056867](https://doi.org/10.1109/TII.2021.3056867)
- Zhong D, Xia Z, Zhu Y, Duan J. Overview of predictive maintenance based on digital twin technology. *Heliyon*. 2023;9(4): e14534. DOI: [10.1016/j.heliyon.2023.e14534](https://doi.org/10.1016/j.heliyon.2023.e14534)
- Machado DO, Chicaiza WD, Escañó JM, Gallego AJ, de Andrade GA, Normey-Rico JE, et al. Digital twin of a Fresnel solar collector for solar cooling. *Appl Energy*. 2023; 339:120944. DOI: [10.1016/j.apenergy.2023.120944](https://doi.org/10.1016/j.apenergy.2023.120944)
- Fahim M, Sharma V, Cao TV, Canberk B, Duong TQ. Machine learning-based digital twin for predictive modelling in wind turbines. *IEEE Access*. 2022; 10:14184-94. DOI: [10.1109/ACCESS.2022.3147602](https://doi.org/10.1109/ACCESS.2022.3147602)
- Ozkan E, Kök İ, Özdemir S. DeepTwin: a deep reinforcement learning supported digital twin model for micro-grids. *IEEE Access*. 2024; 12:196432-41. DOI: [10.1109/ACCESS.2024.3521124](https://doi.org/10.1109/ACCESS.2024.3521124)
- Su Z, Wang Y, Luan TH, Zhang N, Li F, Chen T, et al. Secure and efficient federated learning for smart grid with edge-cloud collaboration. *IEEE Trans Ind Inform*. 2022;18(2):1333-44. DOI: [10.1109/TII.2022.3095506](https://doi.org/10.1109/TII.2022.3095506)
- Badr MM, Mahmoud MMEA, Fang Y, Abdulaal M, Aljohani AJ, Alasmary W, et al. Privacy-preserving and communication-efficient energy prediction scheme based on federated learning for smart grids. *IEEE Internet Things J*. 2023;10(9):7719-36. DOI: [10.1109/JIOT.2022.3230586](https://doi.org/10.1109/JIOT.2022.3230586)
- Habibi MR, Baghaee HR, Dragičević T, Blaabjerg F. Detection of false data injection cyber-attacks in DC microgrids based on recurrent neural networks. *IEEE J Emerg Sel Top Power Electron*. 2021;9(5):5294-310. DOI: [10.1109/JESTPE.2020.2968243](https://doi.org/10.1109/JESTPE.2020.2968243)
- Ding Y, Wang B, Wang Y, Zhang K, Wang H. Secure metering data aggregation with batch verification in industrial smart grid. *IEEE Trans Ind Inform*. 2020;16(10):6607-16. DOI: [10.1109/TII.2020.2965578](https://doi.org/10.1109/TII.2020.2965578)
- Coppolino L, Nardone R, Petruolo A, Romano L. Building cyber-resilient smart grids with digital twins and data spaces. *Appl Sci*. 2023;13(24):13060. DOI: [10.3390/app132413060](https://doi.org/10.3390/app132413060)
- Coppolino L, Nardone R, Petruolo A, Romano L, Souvent A. Exploiting digital twin technology for cybersecurity monitoring in smart grids. In: *Proceedings of the 18th International Conference on Availability, Reliability and Security (ARES 2023)*. New York: ACM; 2023. DOI: [10.1145/3600160.3605043](https://doi.org/10.1145/3600160.3605043)
- Sen Ö, Bleser N, Ulbig A. Digital twin for evaluating detective countermeasures in smart grid cybersecurity. In: *2023 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm)*. Piscataway: IEEE; 2023. DOI: [10.1109/SmartGridComm57358.2023.10333871](https://doi.org/10.1109/SmartGridComm57358.2023.10333871)
- Abdelrahman MS, Kharchouf I, Hussein HM, Esoofally M, Mohammed OA. Enhancing cyber-physical resiliency of microgrid control under denial-of-service attack with digital twins. *Energies*. 2024;17(16):3927. DOI: [10.3390/en17163927](https://doi.org/10.3390/en17163927)

AUTHOR'S PROFILE



Jennifer Ikeoluwa Ade-moomiyo is an Electrical Engineering graduate and researcher with a strong interest in artificial intelligence, intelligent systems, human-computer interaction, and digital technologies. She holds a Bachelor's degree in Electrical and Information Engineering from Landmark University, Nigeria. She has gained experience through academic research, engineering practice, and professional training in wireless communication, machine learning, digital systems, and user-centred design. Her research interests include artificial intelligence, digital twins, human-AI interaction, intelligent systems, wireless communication, and the application of emerging technologies to real-world challenges. She is also developing expertise in UI/UX and Product Design, with a particular interest in creating accessible, user-centred, and innovative digital experiences. She is passionate about interdisciplinary research and contributing to technological solutions that improve how people interact with digital and intelligent systems.



Micheal Abimbola Oladosu is an interdisciplinary researcher with a strong academic and research background. He founded Research Hub Nexus Institute, a platform dedicated to research publication, academic writing support, and mentorship for emerging scholars. He currently lectures in the Department of Chemical Sciences (Biochemistry Unit), Anchor University, Lagos, Nigeria. His research interests span the intersections of the life sciences, biomedical sciences, and technology, and he has actively collaborated on multidisciplinary research projects published in reputable peer-reviewed journals. He also reviews for several academic journals and serves on the editorial boards of multiple international scientific journals and publications.



Moses Abah Adondua is a dedicated biochemist and lecturer at the Department of Biochemistry, Faculty of Biosciences, Federal University Wukari, Nigeria. With a strong academic foundation and research interests in molecular biology, enzymology, and metabolic disorders, he is actively involved in both teaching and research, mentoring undergraduate students and contributing to the development of innovative approaches in research in biochemistry. He is currently the Co-Founder of Research Hub Nexus, where he helps advance research, innovation, and academic collaboration. He also participates in scholarly publishing peer review and capacity-building initiatives aimed at strengthening scientific research in Africa and globally, respectively.



Ugonna Stanley Nwani is a Computer Engineering graduate and early-career researcher with interests in artificial intelligence, machine learning, computer vision, and image processing. He has gained industry experience in data science, data engineering, and analytics, working with machine learning workflows, data pipelines, and business intelligence systems. Beyond industry, he has contributed to technical education and community development by teaching programming, data analysis, and machine learning concepts to students and early-career learners. His interests include developing reliable, adaptive AI systems, particularly visual perception technologies that operate effectively in real-world and resource-constrained environments.



Ifechukwu Victor Muoghalu is an engineer and researcher trained in Materials and Metallurgical Engineering at Nnamdi Azikiwe University, Awka, Nigeria, where he obtained his B.Eng., and in Energy for Sustainability at the University of Coimbra, Portugal, where he earned his Master's Degree. His research centres on sustainable energy systems and their application in E-vehicle and smart grid technologies. His current work focuses on AI-enabled digital twins for real-time monitoring, predictive control, and cybersecurity of modern power systems, with an emphasis on resilient, data-driven solutions for the clean energy transition.



Anya Adebayo is a Political Science graduate from Obafemi Awolowo University, Ile-Ife, Nigeria, with interdisciplinary research interests spanning artificial intelligence, robotics, public policy, security studies, sustainable development, and technological innovation. His academic and professional experience spans development research, governance,





strategic analysis, emerging technologies, and policy-oriented research, with particular emphasis on applying Artificial Intelligence, Machine Learning, Robotics, Blockchain, and Internet of Things (IoT) technologies to contemporary development and security challenges in Africa. His research spans diverse interdisciplinary areas, including climate resilience, public health surveillance, sustainable agriculture, waste management, urban security, disaster resilience, electoral integrity, and development policy. His scholarly work examines how emerging technologies and evidence-based policy frameworks can strengthen institutional capacity, improve societal resilience, and support sustainable development outcomes. His current research interests include AI-enabled governance and security, intelligent and autonomous systems, robotics, climate and disaster resilience, public health intelligence, sustainable development, technology policy, and the intersection of emerging technologies with development and security studies. His broader scholarly focus is on advancing interdisciplinary approaches that leverage technological innovation, policy research, and data-driven methodologies to address complex socioeconomic and developmental challenges in Africa.

Disclaimer/Publisher's Note: The statements, opinions, and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of the Publisher /Journal and/or the editor(s). The Publisher /Journal and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions, or products referred to in the content.