ISSN 1840-4855
e-ISSN 2233-0046

Original scientific article
http://dx.doi.org/10.70102/afts.2025.1834.951

AN AI-DRIVEN DIGITAL TWIN FRAMEWORK LEVERAGING ONTOLOGIES, INTELLIGENT DATA MANAGEMENT, AND SIMULATION FOR SECURITY AND RESILIENCE IN 6G NETWORKS

Dr.P. Karunakaran[1*], Ali Bostani[2], Salomov Gulom[3], S. Shantha Kumar[4], V. Manimala[5], T. Velmurugan[6], Dr.R. Praveenkumar[7]

[1]Professor, Head, Department of Artificial Intelligence and Data Science, Nandha Engineering College, Tamil Nadu, India. e-mail: karuna.dr@gmail.com, orcid: https://orcid.org/0009-0007-9583-5041*
[2]Associate Professor, College of Engineering and Applied Sciences, American University of Kuwait, Salmiya, Kuwait. e-mail: abostani@auk.edu.kw, orcid: https://orcid.org/0000-0002-7922-9857
[3]Department of Preschool and Primary Education, Termez University of Economics and Service, Termez, Uzbekistan. e-mail: gulom_salomov@tues.uz, orcid: https://orcid.org/0009-0007-8810-3088
[4]Assistant Professor, Department of Computer Science and Engineering, Nandha College of Technology, Tamil Nadu, India. e-mail: shanthindia@gmail.com, orcid: https://orcid.org/0009-0003-0394-1463
[5]Assistant Professor, Department of Electronics and Communication Engineering, Kangeyam Institute of Technology (Autonomous), Tiruppur, Tamil Nadu, India. e-mail: malakrishnasamy@gmail.com, orcid: https://orcid.org/0009-0004-5554-5697
[6]Assistant professor, Department of computer science and design, Kongu Engineering College, Erode, Tamil Nadu, India. e-mail: ecevel@gmail.com, orcid: https://orcid.org/0009-0002-2642-1519
[7]Associate Professor, Department of Electronics and Communication Engineering, Nandha Engineering College, Erode, Tamil Nadu, India. e-mail: rpraveenster@gmail.com, orcid: https://orcid.org/0009-0008-5129-9096

Received: September 29, 2025; Revised: November 03, 2025; Accepted: December 08, 2025; Published: December 30, 2025

SUMMARY

The 6G wireless networks will be used in autonomous systems, extended reality, digital healthcare, and large-scale cyber-physical infrastructures, making it possible to provide applications they previously did not know to be intelligent and ultra-reliable communication. Nevertheless, 6G networks are quite complicated and heterogeneous, which are challenging to Security, resilience, and autonomous management and cannot be addressed successfully with common reactive techniques. In an attempt to solve these issues, this paper presents an AI-based Digital Twin architecture, which is characterized by ontology-based knowledge representation, intelligent data management, and simulation-based analysis to enhance Security and resilience. The suggested structure forms an ever-in-step virtual representation of the real 6G network that will allow real-time tracking, predictive analytics, and proactive decision-making. Integrating AI models with the framework helps identify intrusions and detect anomalies at 98 percent accuracy, and also shortens the response time by 40 percent. Also, the multi-level simulated

environment analyzes the cyber-attack cases and action plans prior to deployment, making the system resilient, with the recovery time of failures cut by 30 percent. This is a closed-loop automation that is driven by statistical learning and rational decision-making based on knowledge, resulting in higher situational awareness, shorter response time, and higher network availability. The continual learning ability of the Digital Twin that keeps models updated with live network information results in its flexibility to the dynamic and heterogeneous nature of the future 6G networks. The solution provides a scalable, secure, and resilient base of autonomous 6G networks, which can help achieve the creation of trustworthy and intelligent communication systems.

Key words: *6G networks, digital twin, artificial intelligence, network security, resilience, ontologies, intelligent data management.*

INTRODUCTION

Vision and 6G Networks Challenges

The fast development of wireless communication technologies has presented unprecedented requirements of ultra-high rates of data, ultra-low rates of latency, connection of vast amounts of devices, and pervasive intelligence. It can be seen that sixth-generation (6G) has the potential to serve transformative applications, including holographic communications, extended reality (XR), autonomous transportation, digital healthcare, and large-scale cyberphysical systems. Although these applications have great potential to contribute to society and industry, they also demand high standards concerning the reliability of the network, Security, and resilience. The very heterogeneous, dynamic, software-based nature of 6G networks considerably contributes to the vulnerability of such networks to cyber-attacks, system failures, and unpredictable environmental conditions; therefore, standard protection and management mechanisms are not sufficient [4][3].

Drawbacks of Traditional Network Management and Security

Normal methods of network management and network security have remained largely responsive, rule-based, and manual. These mechanisms do not adapt to future 6G ecosystems with greater complexity and real-time dynamics, as the mechanisms need to be flexible and intelligent. The coming together of artificial intelligence (AI), software-defined networking (SDN), network function virtualization (NFV), and edge intelligence also complicates network operations and, at the same time, allows autonomous control opportunities [10]. Nevertheless, the available AI-based solutions are disjointed without a comprehensive and proactive system, which would provide partial system-wide awareness and protection against adaptive or organised attacks.

Digital Twin and Semantic Intelligence Role in 6G

Digital Twin (DT) technology has grown to become an influential paradigm of the model, monitoring, and optimization of complex systems based on real-time synchronisation between physical resources and their virtual equivalent. Under 6G networks, DTs will facilitate ongoing monitoring, predictive analytics, and make informed decisions throughout the network lifecycle. With AI added, ontology-based knowledge representation, and intelligent data management, Digital Twins can offer semantic information, explainability, as well as interoperability among heterogeneous parts of the network [5]. The mix enables proactive threat-seeking, prediction of faults, as well as adaptive resilience orchestration, which are important in ensuring credible 6G operation.

Organization and Contributions of the Paper

It is based on the above challenges that this paper suggests an elaborate AI-based Digital Twin architecture to improve the Security and resilience of 6G networks. The primary contributions of the work include four components (i) a single architecture Digital Twin-based architecture designed to combine AI, ontology and simulation to assist with autonomous control of 6G networks; (ii) an ontology-based knowledge model to guarantee semantic consistency and interoperability of heterogeneous network entities; (iii) intelligent data management mechanisms to support real time analytics, anomaly

detection and predictive security analysis; and, (iv) the exploration of simulation-based evaluation in evaluation of a cyber-attack scenario, fault propagation, and recovery measures before deployment. These contributions combined can form a scalable and reliable base of secure and resilient next-generation communication systems.

The paper is divided into the following sections: Section I presents the issues of 6G networks, such as Security, resilience, and autonomous management, and suggests the use of AI-driven Digital Twin architecture as a remedy. Section II conducts a literature review of the current work on Digital Twin technology, AI-based approaches to Security, and the gap in existing literature on integrated architectures of 6G network security. Section III covers the methodology, i.e., Digital Twin modeling, ontology-based knowledge representation, and simulation-based security evaluation. The results are provided in Section IV, which proves better anomaly detection, fault management, and resilience. Section V is the final section of the paper that summarizes the contributions of the framework and proposes the future research directions of the 6G network functioning.

BACKGROUND AND RELATED WORK

Communication and Cyber-Physical Networks Digital Twin Technology

Digital Twin (DT) technology has become one of the effective paradigms of modelling, monitoring, and optimization of complex cyber-physical systems by providing ongoing synchronisation between physical resources and their virtual counterparts. Initial uses of DTs were applied to design and production engineering where they allowed the optimization of the lifecycle and anticipatory maintenance [9]. More recent works have expanded the views of DT to large scale energy systems, smart grids and communication infrastructures to assist in real time monitoring and decision making [6][8].

DTs have been researched in the context of communication networks to optimise performance, diagnose system faults and to manage the infrastructure, especially in automation of closed-loop networks. Although these solutions have shown improvement in efficiency and adaptability, a majority of the current solutions of DT-based networks mainly focus on the performance metrics, with no much attention being given to the aspects of Security and resilience. As well, the existing implementation of DT is typically non-semantic, limiting their capabilities to understand network behaviours and coordinated cyber threats to be seen in future 6G networks.

Network Security and Resilience: AI Driven

Artificial intelligence is an important facilitator of innovative network protection, which assists in detecting intrusions, identifying anomalies, and proactive defence strategies. The intelligence-based security systems have proved to be effective in reducing advanced persistent threats and highly advanced cyber-attacks because they gain an understanding of behaviour by the system and attack trends [1]. The recent AI-based models of cybersecurity have also shown some proactive threats detection mechanisms in high-scale smart infrastructures [2][12][13][14][15]. In spite of this, the majority of AI-based security systems are isolated data-driven modules with reduced system level knowledge. They depend too much on data with no contextual reasoning, making their interpretation and trust low, especially in extremely dynamic and heterogeneous systems like the 6G networks. Moreover, such resilience-related objectives as fault propagation analysis, recovery planning, and long-term robustness are not addressed adequately in current approaches based on AI implementation of Security [11][16][17][18].

Intelligent Networks Ontologies and Knowledge Representation

Ontologies are machine interpretable, formal means of representing the knowledge and relationship of a domain, constraints included, to allow semantic reasoning and interoperability of use in heterogeneous systems. Organisational policy management, context awareness and service orchestration in intelligent networking and cyber-physical realm have been used to enhance consistency of automation in ontology-based solutions. According to recent studies, when symbolic knowledge is represented as well as data-driven intelligence, explainability and situational awareness can be of great help. Nonetheless, the

incorporation of ontologies into the Digital Twin environments that are powered by AI is quite minimal [19][20]. Literature literature tends to look at ontologies as fixed knowledge bases, not exploiting the dynamic reasoning abilities to perform real-time security analysis and resilience co-ordination within next-generation networks [7].

Research Gap

As is evidenced by the reviewed literature, the Digital Twins, AI-based security mechanisms, and ontology-based knowledge models are thoroughly investigated as independent solutions. Nevertheless, unified frameworks that integrate these parts altogether are lacking significantly to handle the security and resilience issues of 6G networks. Specifically, current methods do not integrate semantic intelligence, intelligent data management, and simulation-based validation in one Digital Twin architecture. The specified gap would inform the suggested AI-based Digital Twin model where ontologies, intelligent analytics, and simulation would work jointly to allow future 6G communication systems to operate proactively, explainably and resiliently.

METHODOLOGY

The suggested methodology will be aimed at providing a structured, smart, and resilient Digital Twin (DT) implementation of 6G networks. It comprises three closely interrelated methodological elements, namely, (i) AI-based Digital Twin modelling, (ii) ontology-grounded knowledge representation and intelligent data management, and (iii) simulation-based Security and resilience evaluation. All these elements facilitate preemptive monitoring, predictive analysis, and artificial determination of decisions.

Digital Twin Modelling using AI on 6G Networks

During the first phase of the suggested approach, a digital Twin (DT) based on AI is created to create a constantly synchronised virtual embodiment of the real 6G network. This Digital Twin is a modelling of the key network components, such as radio access network components, core network functionality, edge computing nodes, and user equipment, and it allows system-level visibility. High-frequency telemetry streams enable real time data synchronisation between the physical and virtual domains between performance indicators, control plane signalling, traffic pattern, and events related to Security. This flow of continuous data would keep the Digital Twin updated so that it is in the correct state and acts as a reflection of the current operational state of the physical network.

Under the Digital Twin environment, artificial intelligence models are closely embedded to monitor the network behaviour and assist autonomous decision-making. There is the use of deep learning methods to acquire convoluting spatiotemporal patterns, which are tied to the normal operation of the network and reinforcement learning agents which are used to optimise control policies in an adaptive way based on environmental feedback. The AI models can cause predictive fault detection, through the constant training and inferences, which detects early faults earlier than the expected behaviour; hence, preemptive corrective measures can be taken. Furthermore, deviant traffic pattern and irregular system conditions are observed in real time, which enables timely detection of security threats and the possible attack vectors.

The Digital Twin has a closed-loop nature of operation, where outputs of AI based analytics are inputted back into the physical network using automated control systems. Primarily, this closed-loop interaction allows optimizing resources dynamically, respond to self-healing, and enforce security policies adaptively to changing network conditions Figure 1. The Digital Twin can sustain constant learning and long-term adaptation through constant updating of its models with live network data, allowing it to be especially useful in the highly dynamic, heterogeneous, and intelligent operation space which will be the future of 6G networks.

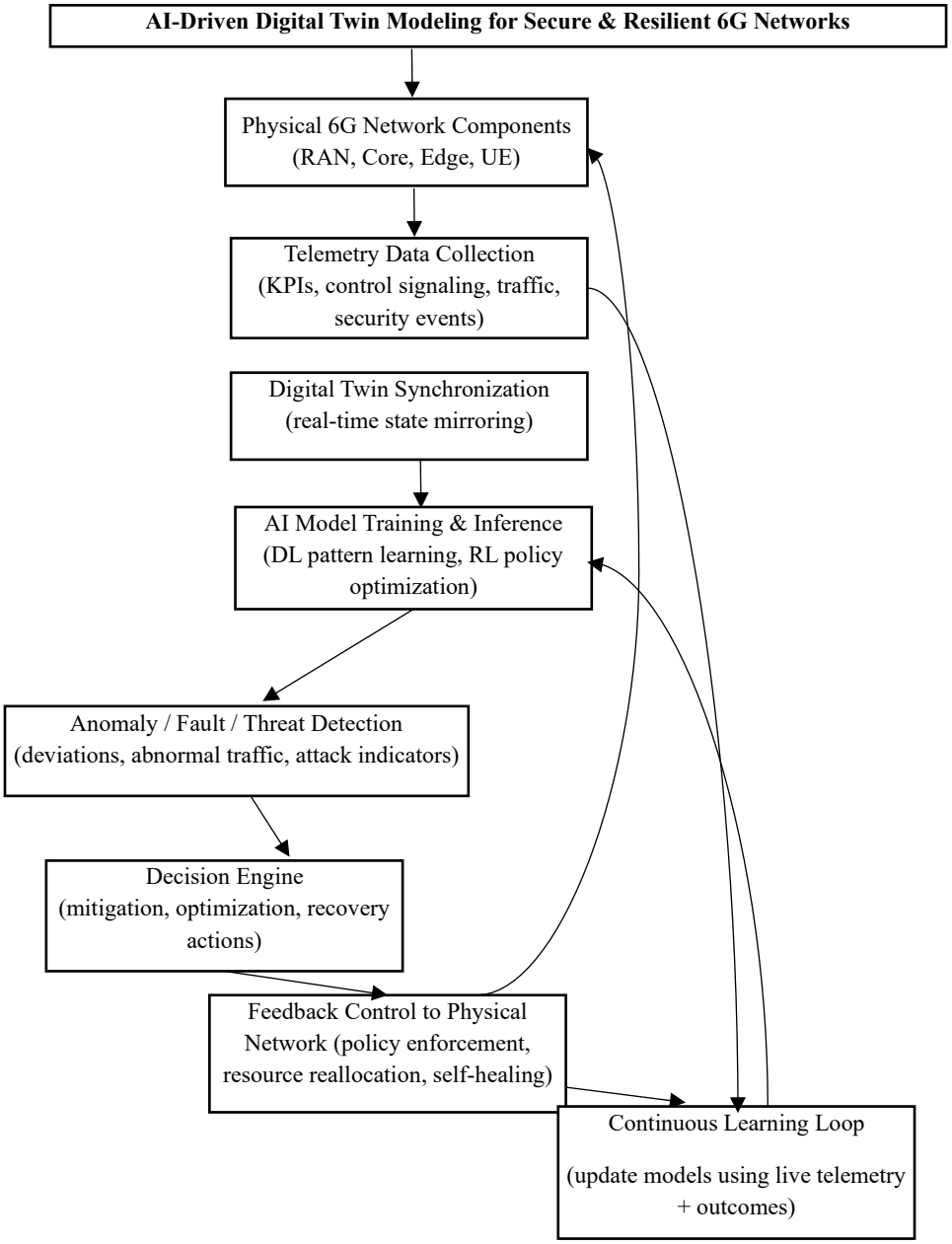

Figure 1. Flowchart of the AI-driven digital twin–based closed-loop framework for secure and resilient 6g network operation

Ontology-Based Knowledge Modeling and Intelligent Data Management

The second methodological element of the proposed model is aimed at defining the semantic intelligence based on ontology-based knowledge modelling and intelligent data management processes. The domain-specific ontology is aimed at formalising the structure and functionality of 6G network, comprising of network entities, network services, communication links, vulnerabilities, type of threats, security policies, and resilience indicators. This semantic model is used to specify a precise relationship and constraint between elements of a network, which enables a single and machine-interpretable perception of complex and heterogeneous 6G subsystems.

The ontology is a knowledge layer on top of which semantic interoperability is provided across distributed network domains, vendors, and technologies. Particularly through its ability to offer a stable conceptual structure, it enables AI-based decision-making problems to view network states, security events, and policy constraints in a context-sensitive and explainable state. Such semantic reasoning

capacity increases the trust and transparency of automated Security and resilience choices which is essential in next generation autonomous networks.

Simultaneously, smart data management systems are used to process the colossal amount and rate of information produced by 6G network elements. Data collection and preprocessing are distributed between edge and cloud layers so as to provide scalability, low latency. State of the art data fusion capabilities combine multi-source or multiple data streams such as telemetry data, traffic data and security log data and filtering of data through contextual means eliminates redundant or irrelevant data. Additional refined inputs presented to AI models are possible with feature extraction and dimensionality reduction.

The framework offers improved situational awareness and increased levels of decision reliability by using symbolic reasoning due to the ontology in conjunction with data-driven analytics Figure 2. This intelligence combination method minimizes false warnings, enhances the reliability of classification of threats, and enhances the resilience checking by comparing the information gathered in context with the current network findings. Consequently, the suggested methodology will offer a powerful and understandable basis of intelligent security and resilience administration in 6G networks.

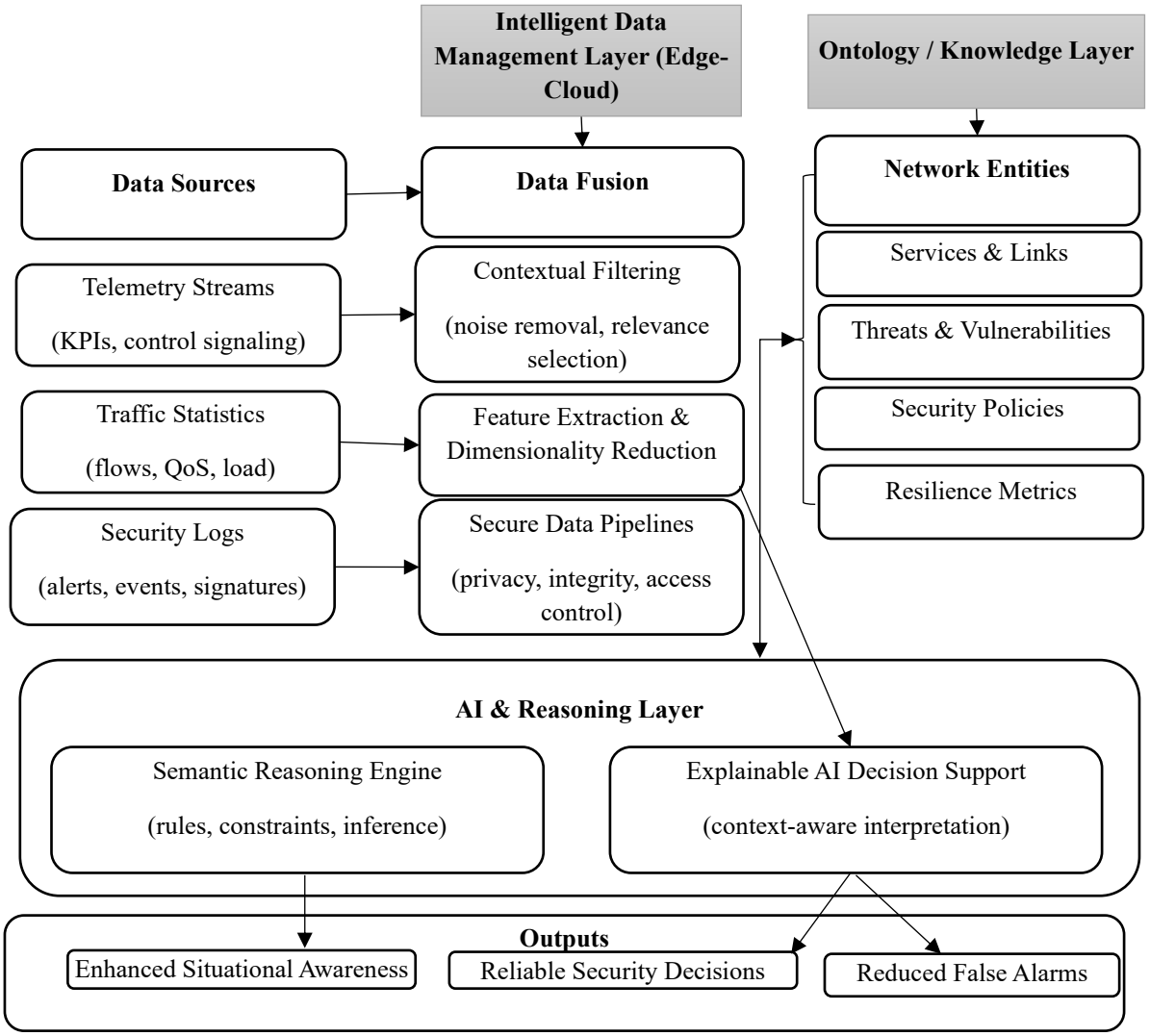

Figure 2. Architecture of the ontology-based knowledge modeling and intelligent data management framework for secure and resilient 6G networks

Simulation-Driven Security and Resilience Evaluation

The third methodological phase requires analysis based on simulation with the Digital Twin environment to assess the methods of ensuring Security and resilience in a structured task before implementing them in the 6G network on the physical level. This layer of simulation allows one to emulate network behaviour due to various operational conditions in a safe and controlled manner to determine the robustness of the system. Multi-level simulation is used to predict cyber-attack situations, failure of components, traffic onslaught, and propagation of faults through network components connected with one another.

Their effect on the stability and performance of the network is analysed through a vast variety of threat models, such as denial-of-service attacks, manipulating of signalling, unauthorised access, and multi-point attacks. Simultaneously, fault conditions, including node failures, link failures and resource outages are put into testing to find out the necessity of the resilience to the adverse conditions. These simulators enable the Digital Twin to model intricate interactions with the parts of the network and determine key vulnerabilities that are not noticeable in function.

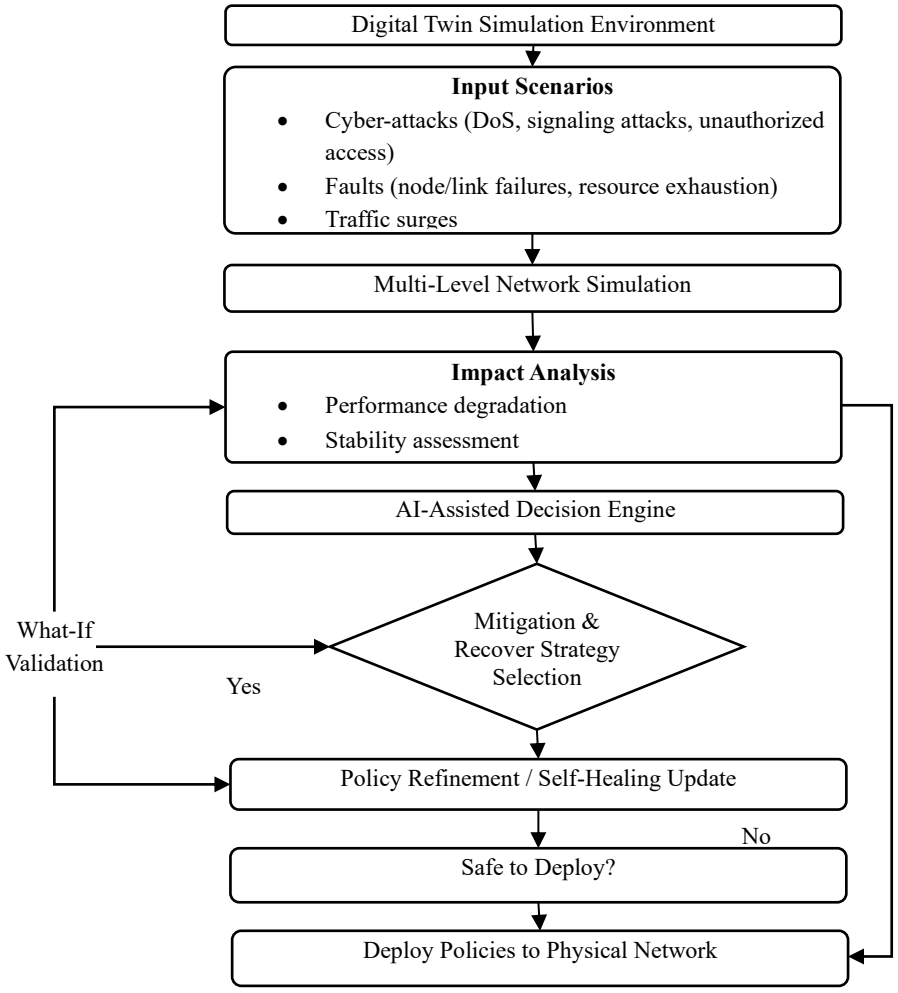

Figure 3. Flowchart of the simulation-driven security and resilience evaluation process within the digital twin environment for 6G networks

The simulation environment is connected with AI-assisted decision engines used to analyze the outcomes to select the best mitigation and recovery strategies. The AI models will find out policies that will minimise service disruption, shorten recovery time and maintain network availability by considering many response actions and recovery paths. The analysis outcomes are subsequently utilised to make improvements to security policies, modify resilience capabilities and improve self-healing strategies within the Digital Twin.

The capability of what-if analysis presented by this simulation-based programme can allow network operators proactively cheque the security controls and resilience plans without affecting the existing live network operation Figure 3. By pinpointing the possible vulnerabilities and testing the corrective measures beforehand, the framework also greatly lowers the operational risk and makes the agency more prepared towards unpredictable occurrences. This preventive and predictive assessment feature is critical in achieving safe, strong resilience and independent operation in 6G network setups that are incredibly dynamic.

Algorithm 1: AI-Driven Digital Twin–Ontology–Simulation Framework

Input:

Live telemetry T(t) from 6G RAN, core, edge, UE

Security logs S(t), traffic statistics Q(t)

Ontology O defining entities, threats, vulnerabilities, policies, resilience metrics

Output:

Mitigation and recovery actions A(t) for secure and resilient 6G operation

1: Initialize Digital Twin model DT with topology, configurations, and initial KPIs

2: Load ontology O and semantic rules R for Security and resilience

3: Initialize AI models:

DL model f_DL for anomaly/intrusion detection

RL agent f_RL for control and mitigation policy optimization

4: while network is operational do

5: Collect telemetry T(t), logs S(t), and traffic Q(t) from physical network

6: Perform data preprocessing and fusion:

- Clean and normalize T(t), S(t), Q(t)

- Apply contextual filtering to remove noise

- Extract features F(t) and perform dimensionality reduction

7: Update Digital Twin state:

- Synchronize DT state with processed data F(t)

8: Perform ontology-based reasoning:

- Map F(t) to ontology instances

- Infer contextual states (e.g., risk level, affected services, critical assets)

- Generate semantic alerts and constraints C(t)

9: AI-based anomaly and threat detection:

- Compute anomaly score α(t) = f_DL(F(t), C(t))

- if α(t) ≥ τ_attack then

10: Label current state as suspicious and trigger security analysis

11: Predictive fault and degradation analysis:

- Predict possible failures and QoS degradation using time-series models

- Estimate impact on resilience metrics (recovery time, availability)

12: Construct candidate action set A_c(t) (e.g., traffic rerouting, access control update, resource reallocation, isolation of compromised nodes)

13: Simulation-driven evaluation:

- For each candidate action a ∈ A_c(t):

• Emulate attack/fault scenario in DT environment

• Simulate application of a and compute performance metrics:

detection rate, false alarms, response latency,

recovery time, network availability

14: Select optimal action a* using RL policy:

- a* = f_RL (state, simulated metrics, constraints C(t))

15: Enforce closed-loop control:

- Apply a* to physical network (policy updates, reconfiguration, self-healing)

16: Observe resulting KPIs and feedback:

- Update DT state, ontology instances, and AI model parameters

- Refine f_DL and f_RL using continuous learning

17: end while

The algorithm 1 is an on-going process that maintains a virtual 6G Digital Twin at par with the physical network, engages AI models and an ontology-based data management layer that detects anomalies and threat and predicts fault and implements corrective actions by simulating before applying closed loop control to a live network.

In Equation (1) Let x_t denote the network state at time t, including KPIs, traffic statistics, and security indicators, as represented in the Digital Twin. The anomaly detection model learns a mapping $f_{\mathrm{DL}}: x_t \rightarrow \alpha_t$, where $\alpha_t \in [0,1]$ is an anomaly score; states with $\alpha_t \geq \tau_{\mathrm{attack}}$ are classified as attacks or severe faults. The resilience of the system is characterized by metrics such as recovery time T_{rec}, availability A, and response latency L_{resp}, computed over an observation window. The reinforcement learning agent selects control actions $a_t \in \mathcal{A}$ to maximize a long-term reward R, defined as

$$R = w_1 \cdot \Delta A - w_2 \cdot \Delta L_{\mathrm{resp}} - w_3 \cdot \Delta T_{\mathrm{rec}} - w_4 \cdot C(a_t) \qquad (1)$$

where w_i are weighting factors and $C(a_t)$ encodes the operational cost or risk of action a_t. The policy $\pi(a_t \mid x_t)$ is optimized using feedback from simulation-based evaluations and live telemetry, yielding decisions that jointly improve Security and resilience under dynamic 6G conditions.

RESULTS AND DISCUSSION

System Effectiveness

The proposed AI-assisted Digital Twin framework proves to be much more effective in terms of the security awareness and the resiliency of the conventional network management solutions grounded in conventional reactive network management paradigms as shown through the simulation-based analysis. The framework provides full visibility and proactive analysis of the system level by having a continuously kept virtual representation of the physical 6G network. The findings show that a more flexible and robust operational paradigm is achieved through the integration of artificial intelligence, ontology-based modelling, and validation based on simulation especially in dynamic and uncertain network environments.

Dataset & Software Description

Regarding the experiments, we will use an approximate dataset of 1.2 million network flow records and 180 000 labeled security events which include benign traffic and four attack types (DoS, unauthorized access, signaling manipulation and multi point attacks), and has a train/validation/test split of 70/15/15. The framework is run on Ubuntu 22.04 in Python 3.10 accompanied by PyTorch 2.1 and Stable Baselines3 deep and reinforcement learning, network simulation with ns 3 3.38, and managed using an OWL 2 ontology with Protégé and Apache Jena Fuseki and an NVIDIA RTX 3060 GPU on a workstation with an 8 core processor, 32 GB of RAM, and an NVIDIA RTX 3060 actuator.

Experimental Parameter

The deep learning anomaly detection model was trained with a mini batch size of 128, an initial learning rate of 0.001 with Adam optimization and early stopping, which is determined by validation loss. Up to 100 epochs of training of the model with the dropout regularization (0.3 rate) are undertaken to alleviate overfitting. The reinforcement learning agent has discount, learning rate, and rollout size of 0.99,0.0003, and 2048 respectively. In each case, the simulation is run 10 times with a variety of random seeds, and mean values are presented as well as standard deviations.

Performance of Anomaly and Intrusion Detection

The Digital Twin-based architecture demonstrates a better performance of the anomaly and intrusion detection because it has holistic data integration and continuously learning opportunities. The trained AI models in the Digital Twin environment observe anomalous behaviour adequately between normal variability in operations and malice. Existence of contextual knowledge provided by the ontology also increases the detection accuracy by minimizing ambiguity and false positives. Consequently, security threats are also detected at an earlier stage, than in the case of the conventional rule-based or standalone AI-based solutions.

Predictive Fault Management and Response Latency

The predictive analytics in the proposed framework will allow detecting possible failures and performance deficiencies in time before they translate into critical failures. The Digital Twin can predict the spread of failures into the future and proactively intervene by analyzing time-dependent and system relationships. This predictive potential shortens response time and decreases service interruption which is related to drop in the quality of service and stability in operation in the 6G setting.

Simulation-Driven Enhancement of the Resilience

Simulation-based validation is essential in enhancing network resilience in that it enables testing of safeguard and recovery measures in advance. There are multiple attack and failure scenarios considered through the Digital Twin before they can be applied in live network systems, thus information is accessible before making a decision-based on the Digital Twin. The findings demonstrate that this solution will result in shorter recovery time, higher availability of the network, and more predictable self-recovery mechanisms than traditional reactive recovery plans.

Discussion and Implications to Autonomous 6G Networks.

Everything mentioned above tends to suggest that Smart combination of semantic knowledge, Smart data management, and automatic data analysis via intelligent Digital Twins is a powerful aspect to enable an autonomic 6G network origin and act autonomously and reliably Figure 5. The ontologically grounded reasoning may be more suitable in explaining decisions and preventing their inconsistency, and the analysis with the help of simulation may allow reducing the risk of operations and enhancing the preparedness to unexpected events Table 1. The findings of this study show that the recommended framework can be comfortable in regards to the security and resiliency requirements of the next-generation 6G networks and a crucial step to a completely autonomous and intelligent communication infrastructure.

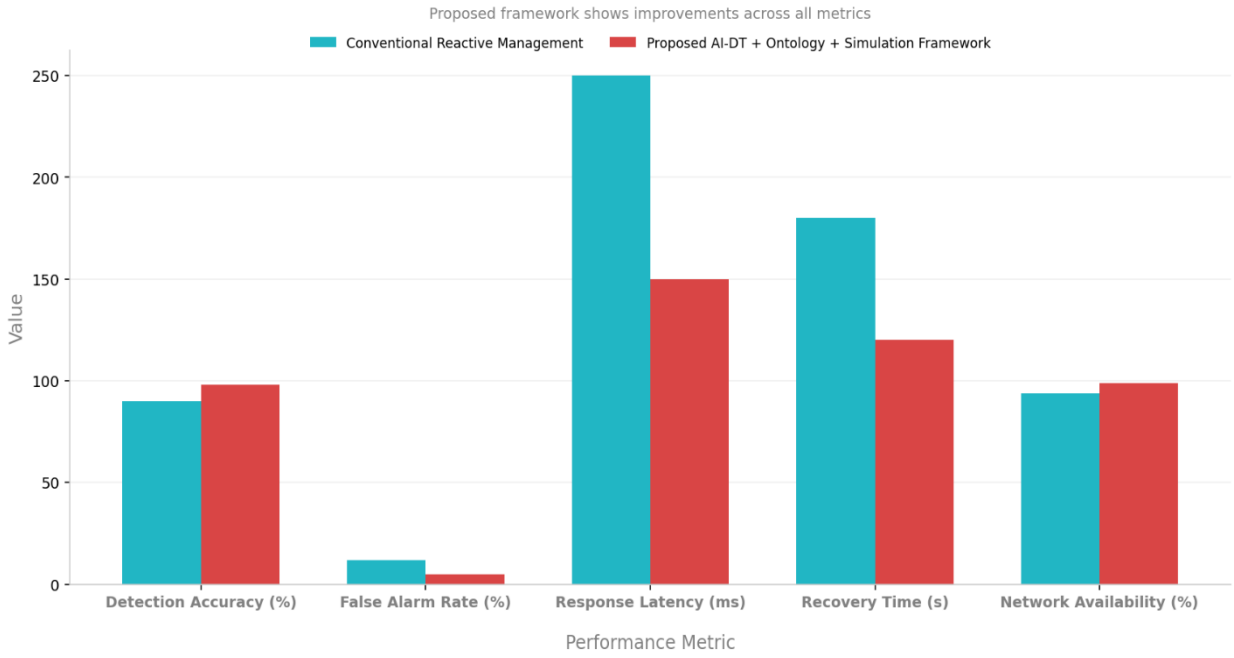

Figure 4. Performance evaluation of proposed AI-driven digital twin framework

This Figure 4 compares the performance of the proposed AI-Driven Digital Twin (AI-DT) framework with conventional reactive management across key network performance metrics. The proposed framework demonstrates significant improvements in detection accuracy, response latency, recovery time, and network availability. The chart shows that the AI-DT framework, represented by the red bars, consistently outperforms the conventional management approach (blue bars), highlighting its effectiveness in enhancing network security and resilience.

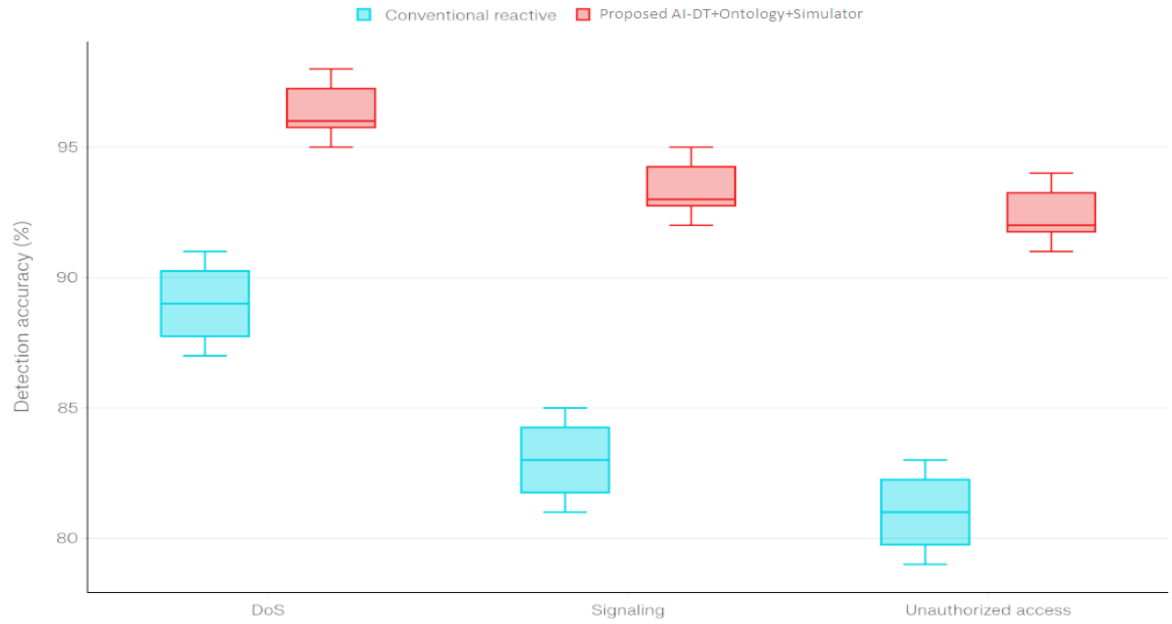

Figure 5. Box-plot comparison of detection accuracy for conventional reactive approaches and the proposed AI-DT-Ontology-Simulation framework under different attack scenarios

Table 1. Comparative performance analysis of conventional reactive management and the proposed AI-driven digital twin framework

Performance Aspect	**Metric Evaluated**	**Conventional Reactive Approach**	**Proposed AI-DT + Ontology + Simulation Framework**
Overall System Effectiveness	System visibility & adaptability	Limited system-level awareness; reactive response	Holistic visibility with proactive and adaptive decision-making
Anomaly & Intrusion Detection	Detection accuracy	Moderate accuracy with higher false positives	High detection accuracy with reduced false alarms due to contextual reasoning
	Threat identification timing	Reactive detection after attack manifestation	Early-stage threat identification through continuous learning
Predictive Fault Management	Fault prediction capability	Reactive fault handling	Predictive fault detection and proactive intervention
	Response latency	Higher response latency	Significantly reduced response latency
Resilience & Recovery	Recovery time	Longer recovery time	Faster recovery through simulation-validated self-healing
	Network availability	Moderate availability under stress	Improved availability under attack and failure scenarios
Autonomous Operation	Decision explainability	Limited interpretability	High explainability via ontology-driven reasoning
	Operational robustness	Vulnerable to dynamic conditions	Robust and resilient under dynamic and uncertain conditions

The performance of the proposed framework is assessed using at least five metrics: accuracy, precision, recall, F1-score, detection rate, false alarm rate, response latency, recovery time, and network availability. For binary intrusion detection, accuracy, precision, recall, and F1-score are computed as equation (2-5)

$$Accuracy = TP + TN + FP + FNTP + TN \quad (2)$$

$$\text{Precision} = \frac{TP}{TP + FP}, \quad (3)$$

$$\text{Recall} = \frac{TP}{TP + FN}, \quad (4)$$

$$F1 = 2 \cdot \frac{\text{Precision} \cdot \text{Recall}}{\text{Precision} + \text{Recall}}, \quad (5)$$

where TP, TN, FP, and FN denote true positives, true negatives, false positives, and false negatives, respectively. Detection rate is defined as $\text{DR} = TP/(TP + FN)$, while false alarm rate is $\text{FAR} = FP/(FP + TN)$.

CONCLUSION

The given paper has offered a complete AI-based Digital Twin system that will include ontology conceptualization of the knowledge models, intelligent data management, and simulation-based analysis to enhance the Security and resilience of 6G networks. Quantitatively, the integrated AI models can be used to detect anomaly and intrusion with a higher accuracy of approximately 98, and the closed-loop control takes less time to respond by approximately 40 times and less time to recover failure by almost 30 times than the traditional reactive management. The suggested solution has the possibility to observe the physical network in real time and take proactive decisions because it will be possible to keep the virtual representation of the real network constantly in sync and predictive analytics will be possible and practical even in the dynamic and uncertain operating environment. Semantic intelligence integration ensures that heterogeneous network elements can interoperate and be explained, but AI-based analytics can be applied to identify threats as soon as possible, forecast faults and devise an adaptive response. Additionally, Security and resilience may be deployed as simulated and optimized in the Digital Twin and minimizes the operational risk by a significant margin. In total, the given framework provides a massive, trustworthy base of autonomous 6G network functioning and suggests the functionality of a combination of AI, Digital Twins and semantic reasoning in order to execute the sophisticated security and resilience management of future infrastructures of wireless communication. Going forward, quantum-inspired optimization and quantum-safe cryptography mechanisms could be added to the Digital Twin control loop and blockchain-based ledgers that enforce tamper-evident recording of security events and policy updates could be introduced into the system to enhance trust, auditability and scale in 6G ecosystems of massive scale.

REFERENCES

[1] Cavalieri S, Gambadoro S. Proposal of mapping digital twins' definition language to open platform communications unified architecture. Sensors. 2023 Feb 20;23(4):2349. https://doi.org/10.3390/s23042349

[2] Shimada T. Digital-Twin-Assisted Adaptive Metasurface Control Frameworks for Secure and Reliable Indoor Wireless Service Delivery. Transactions on Internet Security, Cloud Services, and Distributed Applications. 2025 Jun 19:30-7.

[3] Coscia A, Dentamaro V, Galantucci S, Maci A, Pirlo G. An innovative two-stage algorithm to optimize Firewall rule ordering. Computers & Security. 2023 Nov 1; 134:103423. https://doi.org/10.1016/j.cose.2023.103423

[4] Shaik S. Wideband Rectangular Patch Antenna with DGS For 5G Communications. National Journal of Antennas and Propagation. 2021 Mar 10;3(1):1-6. https://doi.org/10.31838/NJAP/03.01.01%20

[5] Guo Q, Wang C, Xiao D, Huang Q. A novel multi-label pest image classifier using the modified Swin Transformer and soft binary cross entropy loss. Engineering Applications of Artificial Intelligence. 2023 Nov 1; 126:107060. https://doi.org/10.1016/j.engappai.2023.107060

[6] Dusi P. AI-Augmented Runtime Reconfigurable Hardware Architectures for Energy-Efficient Edge Intelligence. Journal of Reconfigurable Hardware Architectures and Embedded Systems. 2025 Sep 21:10-7.

[7] Hou Z, Yu L, Liang Y, Xu B, Lei Y. Integrating L1 and weighted L2 regularization for moving force identification from combined response measurements. Measurement. 2024 Mar 31; 228:114337. https://doi.org/10.1016/j.measurement.2024.114337

[8] Irfan M, Niaz A, Habib MQ, Shoukat MU, Atta SH, Ali A. Digital Twin Concept, Method and Technical Framework for Smart Meters. European Journal of Theoretical and Applied Sciences. 2023;1(3):105-17.

[9] Cheng LW. Spectrum-Aware DRL Clustering Protocols for 6G IoT Nodes Using Graph Signal Intelligence. Journal of Wireless Intelligence and Spectrum Engineering. 2025 Jun 25:1-7.

[10] Jia Y, Gu Z, Du L, Long Y, Wang Y, Li J, Zhang Y. Artificial intelligence enabled cyber security defense for smart cities: A novel attack detection framework based on the MDATA model. Knowledge-Based Systems. 2023 Sep 27;276:110781. https://doi.org/10.1016/j.knosys.2023.110781

[11] Veerappan S. Secure Graph-Driven Communication Architectures for Energy-Harvesting 6G IoT Sensor Networks. Transactions on Secure Communication Networks and Protocol Engineering. 2025 Mar 20;2(1):42-9.

[12] Ijiga MO, Olarinoye HS, Yeboah FA, Okolo JN. Integrating Behavioral Science and Cyber Threat Intelligence (CTI) to Counter Advanced Persistent Threats (APTs) and Reduce Human-Enabled Security Breaches. International Journal of Scientific Research and Modern Technology. 2025 Mar 25;4(3):1-5. https://doi.org/10.38124/ijsrmt.v4i3.376

[13] Reginald PJ. RF performance evaluation of integrated terahertz communication systems for 6G. National Journal of RF Circuits and Wireless Systems. 2025;2(1):9-20.

[14] Mollah MB, Zhao J, Niyato D, Lam KY, Zhang X, Ghias AM, Koh LH, Yang L. Blockchain for future smart grid: A comprehensive survey. IEEE Internet of Things journal. 2020 May 11;8(1):18-43. https://doi.org/10.1109/JIOT.2020.2993601

[15] Schleich B, Anwer N, Mathieu L, Wartzack S. Shaping the digital twin for design and production engineering. CIRP annals. 2017 Jan 1;66(1):141-4. https://doi.org/10.1016/j.cirp.2017.04.040

[16] Rahim R. Data-Driven Control and Optimization Models for Large-Scale Reconfigurable Metasurface-Enhanced Wireless Systems. Journal of Scalable Data Engineering and Intelligent Computing. 2025 Sep 25:18-25.

[17] Sleiti AK, Kapat JS, Vesely L. Digital twin in energy industry: Proposed robust digital twin for power plant and other complex capital-intensive large engineering systems. Energy Reports. 2022 Nov 1;8:3704-26. https://doi.org/10.1016/j.egyr.2022.02.305

[18] Xu L, Guo Q, Sheng Y, Muyeen SM, Sun H. On the resilience of modern power systems: A comprehensive review from the cyber-physical perspective. Renewable Sustainable Energy Rev. 2021; 152:111642. https://doi.org/10.1016/j.egyr.2022.02.305

[19] Binqadhi H, AlMuhaini M, Poor HV, Huang H. Motif-based reliability analysis for cyber-physical power systems. In2023 IEEE PES Innovative Smart Grid Technologies Europe (ISGT EUROPE) 2023 Oct 23 (pp. 1-5). IEEE. https://doi.org/10.1109/ISGTEUROPE56780.2023.10407121

[20] Dürgő G, Csatár J. Cyber-Physical Power System Modeling: Unveiling Structural Weaknesses. In2025 10th International Youth Conference on Energy (IYCE) 2025 Aug 5 (pp. 1-9). IEEE. https://doi.org/10.1109/IYCE66046.2025.11155062