ISSN 1840-4855
e-ISSN 2233-0046

Original scientific article
http://dx.doi.org/10.70102/afts.2025.1834.1006

ARTIFICIAL INTELLIGENCE–EMPOWERED DIGITAL TWINS FOR SIMULATION-DRIVEN SECURITY, PRIVACY, AND RESILIENCY OPTIMIZATION IN 6G NETWORKS

P. Senthilkumar[1*], V. Sheela[2], G.D. Praveenkumar[3], Ali Bostani[4], Nazokat Tukhtaeva[5], Dr.M. Nalini[6], Dr.M. Karpagam[7]

[1]Assistant Professor, Department of Electronics and Communication Engineering, Velalar College of Engineering and Technology, Erode, Tamil Nadu, India.*
e-mail: psenthilkumarece@gmail.com, orcid: https://orcid.org/0000-0002-2377-5269
[2]Assistant Professor, Department of SSCS, CMR University (OMBR Layout), Bangalore, India. e-mail: sheela.v@cmr.edu.in, orcid: https://orcid.org/0009-0002-5732-6485
[3]Assistant Professor, Department of Computer Technology, Kongu Engineering College, Tamil Nadu, India. e-mail: erodegd@gmail.com,
orcid: https://orcid.org/0000-0002-7732-9707
[4]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
[5]Department of Information Technology and Exact Sciences, Termez University of Economics and Service, Termez, Uzbekistan. e-mail: nazokat_tuxtayeva@tues.uz,
orcid: https://orcid.org/0009-0008-7738-4985
[6]Principal, Associate Professor of Mathematics, J.K.K Nataraja College of Arts & Science, Namakkal, Tamil Nadu, India. e-mail: naliniphd77@gmail.com,
orcid: https://orcid.org/0009-0000-9473-1549
[7]Professor, Department of ECE, Sri Krishna College of Engineering and Technology, Coimbatore, Tamil Nadu, India. e-mail: karpagam@skcet.ac.in,
orcid: https://orcid.org/0000-0001-5815-8116

Received: October 01, 2025; Revised: November 05, 2025; Accepted: December 09, 2025; Published: December 30, 2025

SUMMARY

The wireless networks of the sixth generation (6G) are likely to be an AI-native, highly dynamic, and ultra-dense communication eco-system, where the question of security, privacy and resiliency is much more complicated to address than in other generations. Conventional static and prescriptive network management tools cannot scale, be heterogeneous or real-time adaptive to the scale, diversity, and dynamism of 6G systems. In this respect, Digital Twins (DTs) enhancing Artificial Intelligence (AI) have become a potent framework that can help to have high-fidelity virtual models about physical networks to facilitate simulation-based analysis, prediction, and optimization before physical implementation. In this survey, the Digital Twin frameworks based on AI are thoroughly revised in terms of improving the security, privacy, and resiliency of 6G networks, with a specific focus on Digital Twin modelling and prediction algorithms, such as, graph-based, temporal, and representation learning algorithms. Moreover, the paper outlines coherent discussion of machine learning evaluation matrices employed to evaluate DT-enabled security analytics, privacy-conscious learning, and network resiliency, which can be used to benchmark and perform a comparative analysis of performance. The survey also presents an individualised taxonomy of AI-enabled Digital Twin architecture, provides a comparative review of the current modelling methodologies, and reveals several important open research issues and future perspectives concerning scalability, actual-time synchronisation, and standardisation. Digital Twin-enabled frameworks demonstrate a significant advancement in network oversight, achieving a projected detection accuracy of approximately 90% compared to the 75% observed in traditional non-Digital Twin approaches. This work is hoped to be a reference base to the design and implementation of secure, privacy-preserving, and resilient Digital Twin-driven 6G networks by integrating recent progress and identifying the key discrepancies in the research.

Key words: *6G networks, digital twin, artificial intelligence, network security, privacy preservation, resiliency, simulation-driven optimization.*

INTRODUCTION

The continuing development of communication systems in wireless networks within the context of the fifth-generation (5G) systems, to the sixth-generation (6G) systems that have an AI-based nature is necessitated by the need to provide ultra-reliable, low-latency, and smart communication services in dynamic and heterogeneous settings. In contrast to standardised networks in the past, 6G networks are anticipated to support native AI utilization to assist autonomous choices, massive connexon, and real-time adaptation throughout radio access network, core, and edge space [14]. The 6G visionary work focuses on the integration of communication, computing, and intelligence as a design principle and allows using it in the applications of immersive extended reality, autonomous systems, and mission-critical industrial automation [4][11]. Such a fundamental shift in the paradigm has a substantial impact on the complexity of systems and requires new structures capable of modelling, forecasting and optimising the behaviour of networks compared to traditional fixed approaches.

With the growing software-defined nature of 6G networks, their virtualized and data-centric nature, security, privacy and resiliency become first-class design considerations and not second-class ones. The huge size of interconnected devices, the distributed intelligence, and inconsistent trust planes increase 6G infrastructures to advanced cyber threats, privacy leakage risks and cascading failures [20][21]. Conventional perimeter-based security controls, as well as the use of static protection policies, cannot provide security in these practises, especially when machine learning models themselves are in the attack surface. The existence of weak defences to dynamic and adaptive attacks of intelligent and software-defined networks has been accentuated by previous studies, consequently necessitating proactive, predictive, and learning-oriented defences that can ensure all-time availability of services and reliability [10][11]

Older network management techniques founded on fixed rules, fixed optimization and not real-time planning are not as flexible as needed to address the time dynamics of 6G networks. These methods usually work on few observability and reactive control and hence they are not useful in prediction of network anomaly, security breach or performance degradation. In an effort to overcome these limitations, Digital Twin (DT) technology has been growing in popularity as the tool to develop a high-fidelity virtual representation of physical systems that can dynamically develop together with the actual physical system. Digital Twins have first emerged in industrial and cyber-physical systems and allow continuous monitoring and state estimates and predictive analysis using data-driven and hybrid modelling methods [1]. Recent works have applied the DT to the communication networks as they show the potential of real-time simulation, validation and optimization of the 5G and beyond systems [9].

Based on these advancements, AI-powered Digital Twins have become a definite prospect of modelling simulation-based security, privacy, and resiliency optimization in 6G networks. Digital Twins can project network states, test hypothetical situation, and assist in informed decision taking by suggesting the approach based on the advanced machine learning models, including graph-based, temporal, and representation learning, before the actual implementation in the real-world scenario. Although literature in the field has discussed the personal sides of Digital Twins, AI-based modelling, or 6G security, a consistent and additional review uniting the Digital Twin modelling and prediction methods with suitable machine learning testing matrices are not discovered yet. The gap proposed in this paper is that it gives a complete overview of AI-enabling Digital Twin architectures of 6G networks, which provides a comparative analysis of modelling and prediction algorithms, comments on evaluation matrices of security, privacy, and resiliency testing, along with available open research challenges and directions.

Key Contributions

Based on the provided text, the key contributions of the research are as follows:

- A complete overview of AI-enabling Digital Twin architectures specifically tailored for 6G networks is provided.
- The paper offers a comparative analysis of modeling and prediction algorithms, focusing on techniques such as graph-based, temporal, and representation learning.
- Evaluation matrices for security, privacy, and resiliency testing are commented upon to establish a framework for benchmarking performance.
- Available open research challenges and future directions are identified to guide subsequent studies.
- The work highlights significant performance improvements, illustrating that Digital Twin-enabled approaches can reach a 90% detection accuracy compared to 75% for non-Digital Twin methods.

The structure of the paper is organized as follows to provide a systematic exploration of AI-empowered Digital Twins in 6G networks: Section 1: Introduction: Establishes the necessity of AI-native 6G systems and introduces the role of Digital Twins in addressing security, privacy, and resiliency. Section 2: Background and Enabling Technologies: Discusses 6G architecture, the evolving threat landscape, and the foundational concepts of Digital Twin technology and AI intelligence. Section 3: Taxonomy of AI-Empowered Digital Twin Architectures: Provides a classification based on deployment models (centralized, distributed, hierarchical) and functional roles (monitoring, predictive, prescriptive). Section 4: Digital Twin Modeling and Prediction Algorithms: Analyzes specific AI methods such as Graph Neural Networks, temporal models (LSTM/GRU/Transformers), and representation learning. Section 5: Simulation-Driven Optimization: Details how virtual replicas are used for "what-if" security simulations and the generation of synthetic data for model training. Section 6: ML Evaluation Matrices: Defines a unified framework for benchmarking performance using metrics for security (precision/recall), resiliency (MTTR/MTTD), and system overhead. Section 7: Case Studies and Representative Use Scenarios: Examines practical applications such as secure network slicing and privacy-preserving traffic analytics. Section 8: Open Challenges and Research Gaps: Identifies critical barriers including scalability, real-time constraints, and data trustworthiness. Section 9: Future Research Directions: Outlines emerging frontiers like cognitive Digital Twins, cross-layer optimization, and federated learning integration. Section 10: Conclusion: Summarizes the core findings, emphasizing the 90% detection accuracy achieved by DT-enabled frameworks compared to 75% for non-DT methods.

BACKGROUND AND ENABLING TECHNOLOGIES

6G Network Architecture and Threat Landscape

Sixth generation (6G) Of wireless networks the sixth generation (6G) of wireless networks is proposed as an AI-native framework, in which intelligence is introduced throughout the radio access network (RAN), the core network, and edge computing layers to allow autonomous operation and real-time optimization [2][5]. Unlike other generations, 6G implements artificial intelligence as an in-built network feature to uphold adaptive spectrum management, smart mobility management, and smart context-based service provisioning [8]. Such interaction of communication, computing, and intelligence enables ultra-low latency and high connectivity at the same time as it adds complexity and interdependent networks among network elements to the architectural complexity and the architectural interdependency [4][11]. A broader threat range is presented in the 6G systems with the adoption of ultra-dense deployments, software-defined networking, and network slicing, and distributed edge intelligence [17][18]. Decision-making pipelines where AI is utilised as well as virtual functions in networks become appealing targets of adversarial attacks, data poisoning, and inference-driven privacy leakage [19]. Further, constant exchange of telemetry information over edge-cloud structures provokes concerns on data confidentiality, integrity and trust. The issues are forcing the need to implement proactive security tools and the resistance-sensitive design that can foresee the potential failures and reduce attacks prior to their spreading across the network [10][11].

Digital Twin Concept in Communication Networks

Digital Twin (DT) technology has come out as a potent thought construct to comprehend and operate cyber-physical systems to solve the growing complexity and dynamism of the next-generation networks. It is possible to identify a network Digital Twin as the high-fidelity virtual representation of a real-life communication network, constantly updated with the real-time data about the operational status, behaviour, and performance of the underlying system [1][3]. The data collection, model assembly, and synchronisation, simulation and feedback-based optimization are often the stages of lifecycle of a Digital Twin, which allows making informed decisions regarding the functioning of the network. Digital Twins may be in offline or real-time mode in communication networks [12][15]. Design-time analysis, performance analysis, as well as what-if scenario testing are the most common applications of offline DTs, whereas the online monitoring and adaptive control of the physical network are conducted with the help of real-time DTs. Digital twins that are real-time are based on a pair of feedback loops: virtual simulation results are sent back to the real network so as to inform configuration changes, allocation of resources, and fault management. Such a close integration between the physical and virtual world is essential to delivering predictive and resilient network functionality in 6G networks [9][16] (Table 1).

Table 1. Summary of digital twin definitions, enabling technologies, and network characteristics

Aspect	Traditional Communication Networks	AI-Native 6G Networks with Digital Twins
Digital Twin Definition	Not explicitly supported; limited to offline network planning and static simulations	High-fidelity virtual replica of the physical network that evolves synchronously using real-time data and supports continuous analysis and optimization
Operational Mode	Offline, design-time analysis and reactive management	Hybrid offline and real-time operation with closed-loop feedback control
Intelligence Paradigm	Rule-based control and heuristic optimization	Embedded artificial intelligence enabling learning-driven decision making
Key Enabling Technologies	Centralized cloud computing, predefined protocols	AI/ML models, edge intelligence, cloud–edge collaboration, Digital Twin frameworks
State Estimation	Limited observability and delayed analytics	Learning-based state estimation using data-driven and hybrid models
Prediction Capability	Minimal or non-predictive	Proactive prediction of traffic, anomalies, and security incidents
Security and Privacy Handling	Reactive security mechanisms and static policies	Simulation-driven evaluation of security, privacy, and resiliency strategies
Adaptability and Resiliency	Low adaptability; manual reconfiguration	Self-adaptive and resilient operation through DT-assisted optimization

Role of AI in Digital Twin Intelligence

The concept of artificial intelligence can be used to optimise the intelligence and efficacy of Digital Twins by facilitating the learning-based state estimation process, predictive modelling, and decision service. Digital Twins can be represented by machine learning models that include graphs neural networks, temporal sequence models, and representation learning models that enable the model to capture challenging spatial-temporal relationships in large-scale communication networks. The AI models are used to support precise estimation of concealed state of the network, prompt recognition of variability, and prediction of the traffic behaviour or security occurrences which is crucial in the proactive management of the network [6][7][13]. Moreover, AI integration in Digital Twins can be used to employ the paradigm of optimization triggered by simulations such that it is possible to explore alternative network designs and control systems in the virtual realm before the real implementation. This solution will greatly minimise the operational risk and enhance the level of security robustness, privacy security, and network resilience. In order to illuminate the background conceptualizations presented in this section, (Table 1) lists some of the significant definitions of Digital Twins, enabling technologies, and the defining features between conventional networks and AI-native 6G, which will serve as a cursory reference in the later sections. With AI intelligence applied to high-fidelity Digital Twin models, next-generation networks will be able to change their approach to managing networks toward being not reactive to changes but predictive and self-optimising.

TAXONOMY OF AI-EMPOWERED DIGITAL TWIN ARCHITECTURES

There are broad categories of AI-enabled 6G network Digital Twin architectures, categorised by the deployment model, which defines the instantiations and synchronisation of the virtual twin to the real network. The core of a Digital Twin architecture is a centralised system in which a centralised cloud or core network agent or central node has a global replica and provides full visibility of the systems and optimal optimization features. Although centralised DTs are more straightforward to use to both analyse globally and to coordinate systems-wide, they can potentially include scalability constraints and high latencies when used to ultra-dense 6G systems. In order to mitigate such problems, Architectures of distributed or edge assisted digital twins have been suggested, and partial twins move closer to the network edge allowing low latency monitoring and localised intelligence as well as quicker reaction to dynamic network states. Contexts in 6G environments in large-scale 6G environments, centralized and distributed DTs are hierarchical and form multi-layer structures enabling coordinated optimization of edge, core, and cloud space and balancing between scalability, responsiveness and the efficiency of computation. In addition to deployment considerations, the Digital Twin architectures could be grouped on their functional role in the network management and optimization pipeline. Monitoring Digital Twins are emphasised on observation of current state in real-time, aggregation of telemetry, and presentation of performance, which offers situational awareness on network conditions. Predictive Digital Twins help the models further by taking on the use of machine learning models to predict traffic patterns, identify anomalies, and anticipate a security threat or performance degradation. On a more advanced level of intelligence, prescriptive or control-oriented Digital Twins actively suggest or perform reconfiguration actions on the network depending on the monthly results of the simulation and optimization goals. Such functional categories do not form mutually exclusive groups, and they can be all combined into a single DT architecture to support a sustained monitoring, forecasting, and adaptive control of AI-native 6G systems.

The mapping of Digital Twin functionalities to security, privacy, and resiliency objectives is a critical aspect of proposed taxonomy because it is among the core requirements in 6G networks. Digital twins can run DT-aided diagnostics that improve analytics of attack advisory simulations, evaluation of threat spread, and threat evaluation defences without putting the physical network at risk in real life. Through predictive models, DTs can observe abnormal behaviour in advance and realise mitigation of cyber threats before they happen. Simultaneously, privacy-concerned Digital Twin synchronisation algorithms are suggested to reduce the exposures of sensitive data in the twin-network interactions through the implementation of privacy-friendly methods, including federated learning, data abstraction, and selective state sharing, without violating privacy requirements but maintaining a high level of modelling accuracy.

Reproductive Resiliency DT-driven control loops allow networks to shift to reactively based fault recovery to proactively based self-healing operation. Through the further appraisal of what-if situations in the virtual world, Digital Twins will have the ability to determine the influence of failures, attacks, or traffic outbursts and suggest the most appropriate recovery strategies before the service deterioration takes place. The interaction between the physical network and its Digital Twin is closed and enables AI-native 6G systems to self-adapt to unforeseen conditions and ensure service continuity during unfavourable conditions. In summary, the entire taxonomy of AI-enabled Digital Twin systems i.e. deployment models, functional roles as well as security-privacy-resiliency mapping is summarised graphically in (Figure 1) offering a controlled overview of how various DT design options serve the purpose of intelligent, secure and resilient operation of 6G networks.

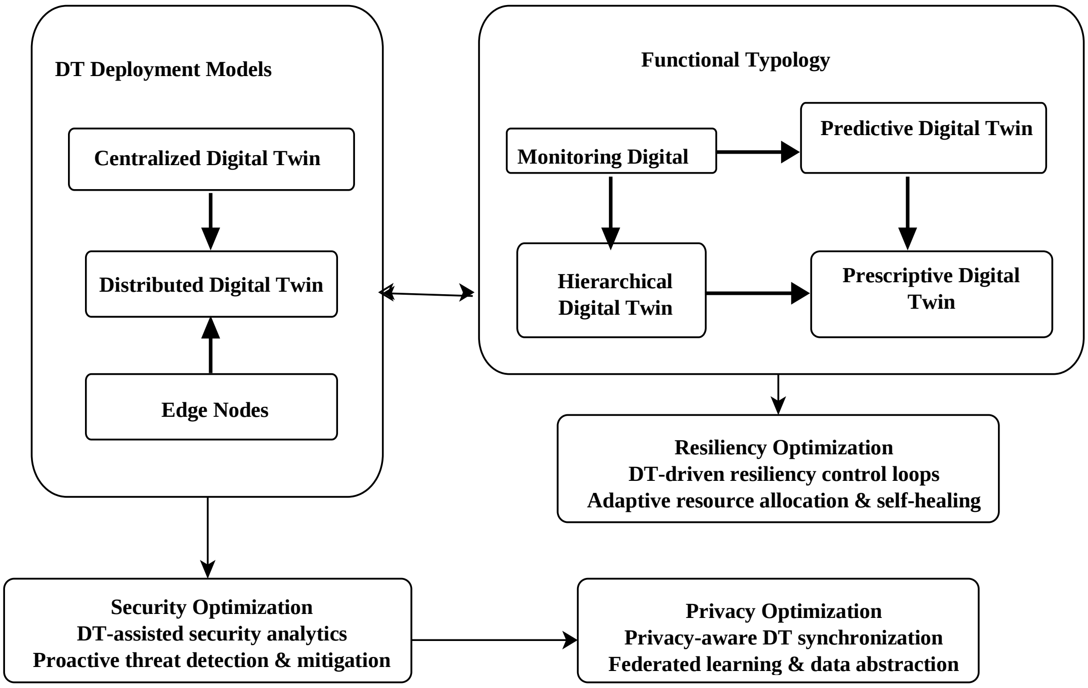
DT Deployment Models
Centralized Digital Twin
Distributed Digital Twin
Edge Nodes
Functional Typology
Monitoring Digital
Predictive Digital Twin
Hierarchical Digital Twin
Prescriptive Digital Twin
Resiliency Optimization
DT-driven resiliency control loops
Adaptive resource allocation & self-healing
Security Optimization
DT-assisted security analytics
Proactive threat detection & mitigation
Privacy Optimization
Privacy-aware DT synchronization
Federated learning & data abstraction

Figure 1. Taxonomy of AI-empowered digital twin architectures for security, privacy, and resiliency optimization in 6G networks

DIGITAL TWIN MODELING AND PREDICTION ALGORITHMS

The effectiveness of AI-native 6G networks depends heavily on the Digital Twin (DT) modeling and prediction algorithms applied to network topology and operational states. Graph-based models, specifically Graph Neural Networks (GNNs), are prominent for representing structural dependencies between base stations, users, and slices. These models enable the discovery of spatial properties and interference dynamics in ultra-dense radio access networks (RAN). Furthermore, dynamic graph learning allows the DT to adjust to evolving 6G topologies and mobility-aware behaviors.

Beyond spatial modeling, temporal sequences are captured via Long Short-Term Memory (LSTM) and Gated Recurrent Units (GRU) to forecast congestion and provide early warnings for anomalous patterns. Recent Transformer-based architectures further enhance predictive power by encoding long-range dependencies and complex correlations on a multi-horizon basis, which is essential for proactive security.

In order to trade off data-driven with robustness, hybrid modeling combines machine learning with classical control-theoretic algorithms, including Kalman and particle filters. These hybrids provide the estimation of the state in the presence of noisy or partially observable conditions, which is crucial to mission-critical applications because the quantification of uncertainty is needed. Lastly, the learning of normal network behavior in latent spaces is made possible by representation learning, such as Autoencoders (AE), and Variational Autoencoders (VAE). This helps the DT to know when there is an intrusion or a fault that does not conform to the learned norms and at the same time allows privacy conscious modeling due to abstracting sensitive data. The workings logic of these modeling schemes are realized through the following prediction monitoring and representation learning algorithms:

Algorithm 1: Hybrid State Estimation & Predictive Monitoring

```
ALGORITHM HybridPredictiveMonitoring:

    INPUT: Real-time network telemetry (topology, traffic, signal metrics)

    OUTPUT: Network State Estimate, Anomaly Alert (Target: 90% Detection Accuracy)
```

```
INITIALIZE Digital Twin with physical layer constraints and protocol logic
    WHILE network is operational:
        1. DATA ACQUISITION: Collect high-dimensional data from 6G edge nodes
        2. SPATIAL MODELING (GNN):
           Represent nodes and edges; capture interference and connectivity
        3. TEMPORAL PREDICTION (LSTM/Transformer):
           Analyze traffic patterns; predict multi-horizon network states
        4. HYBRID STATE ESTIMATION (Kalman/Particle Filter):
           Combine ML prediction with control-theoretic filters for noise reduction
        5. ANOMALY EVALUATION:
           IF Predicted_State deviates from Physical_State > Threshold:
               Trigger Security/Resiliency Protocol (vs. 75% accuracy in non-DT systems)
        6. SYNCHRONIZATION: Update virtual model to match physical reality
    END WHILE
END ALGORITHM
```

This algorithm 1 will act as the active brain of the Digital Twin to combine data-driven AI and classical mathematical control. Whereas Graph Neural Networks (GNNs) and Transformers discover pattern features present in 6G traffic, the Kalman or particle filters are used to add extra refinement to these forecasts by eliminating signal noise and addressing lost information. The synergy enables the system to detect anomalies in the network with a 90 percent accuracy even in a very dynamic or volatile network environment. It makes sure that there is a perfect synchronization of the virtual model with the physical network so that the system can intervene before the performance deterioration happens.

Algorithm 2: Privacy-Aware Representation Learning

```
ALGORITHM PrivacyAwareDetection:
INPUT: High-dimensional raw network data
OUTPUT: Latent Representation, Reconstruction Error
TRAIN Autoencoder (AE/VAE) on "Normal" network behavior:
ENCODER: Compress raw data into a privacy-preserving latent space
DECODER: Reconstruct original data from latent representation
FOR EACH incoming network state:
 1. FEATURE ABSTRACTION: Generate latent representation to hide sensitive data
2. RECONSTRUCTION: Re-create the network state from latent space
```

```
3. ERROR CALCULATION: Compute (Original_Data - Reconstructed_Data)
4. DETECTION LOGIC:
IF Reconstruction_Error > Threshold:
Report "Intrusion/Fault Detected" (Maintaining 90% accuracy bound)END FOR
END ALGORITHM
```

This algorithm 2 is meant to be used in monitoring network security without interfering with privacy of sensitive data. It makes use of Autoencoders (AE/VAE) to represent large volumes of raw network traffic in a simplified latent space. This is a good process that conceals certain identifiable information and the main operational aspects required in the monitoring process are preserved. Security This is done by computing reconstruction error: the Digital Twin trains on what normal network behavior should look like in this compressed representation, and an error that is very large (large error) indicates a possible intrusion. The solution gives a high-fidelity security layer that does not violate privacy limits in the 6G infrastructure.

Table 2. Comparison of digital twin modeling and prediction algorithms for ai-native 6G networks

Algorithm	**Input Data Type**	**Prediction Capability**	**Security / Privacy Relevance**	**Computational Complexity**
Graph Neural Networks (GNNs)	Network topology graphs, node/link states, traffic flows	Topology-aware state prediction, interference and slice behavior modeling	Enables attack propagation analysis, secure routing, and slice isolation assessment	High (graph construction and message passing overhead)
LSTM / GRU	Time-series traffic data, control signals, telemetry logs	Short- and mid-term traffic forecasting, anomaly and attack trend prediction	Early detection of abnormal traffic patterns and intrusion attempts	Medium (sequential processing overhead)
Transformer Models	Multivariate time-series, cross-layer network features	Long-horizon prediction, complex temporal dependency modeling	Proactive threat anticipation and resilience planning	High (self-attention and memory requirements)
Auto encoders (AE / VAE)	High-dimensional network telemetry and feature vectors	Representation learning and deviation-based anomaly detection	Privacy-aware modeling through latent abstraction and anomaly detection	Low to Medium (depends on network depth and latent size)

In addition to the services brought up by Digital twin, representation learning methods are used to come up with compact and meaningful latent representation of the high-dimensional data of the network. Auto encoder (AE) and Variational Auto encoder (VAE) can be used to have Digital Twins to learn normal network behaviour on latent spaces that an abnormality, an intrusion, or a fault should deviate more severely than the one the Digital Twin has learned. Privacy-aware modelling can also be done in latent-space representations, as they help to abstract sensitive information without compromising critical operational characteristics. The key Digital Twin modelling and prediction algorithms are briefly described with input data types, predictions made, and in relation to security and privacy goals, and their computational costs in (Table 2), a systematic source of information on the use of the models in 6G Digital Twin deployment in simulations.

Digital Twin Modeling and Prediction Algorithms

The effectiveness of AI-native 6G networks depends heavily on the modeling and prediction algorithms applied to network topology and operational states. The mathematical foundation for these models is detailed below, followed by a consolidated table of parameter initializations.

Graph State Update Equation

$$h_v^{(k+1)} = \sigma(W^{(k)} \cdot \text{AGGREGATE}\{h_u^{(k)}: u \in N(v)\}) \quad (1)$$

This equation (1) represents the core message-passing mechanism of Graph Neural Networks (GNNs) used to model the 6G network topology. It defines how a node $\boldsymbol{v}$(base station or user) updates its hidden state $\boldsymbol{h}$by aggregating information from its neighbors $N(v)$. This allows the Digital Twin to capture spatial interference and connectivity dynamics across ultra-dense radio access networks.

Scaled Dot-Product Attention (Transformer)

$$\text{Attention}(Q, K, V) = \text{softmax}\left(\frac{QK^T}{\sqrt{d_k}}\right)V \quad (2)$$

The attention mechanism from Equation (2) allows the Digital Twin to identify long-range temporal dependencies in multivariate 6G time-series data. By calculating the similarity between Queries (Q) and Keys (K), the model assigns weights to Values (V), enabling high-precision forecasting of congestion or security threats on a multi-horizon basis.

Kalman Filter State Estimation (Hybrid Model)

$$\boldsymbol{\hat{x}_{k|k} = \hat{x}_{k|k-1} + K_k(z_k - H\hat{x}_{k|k-1})} \quad \textbf{(3)}$$

This equation (3) describes the correction step of the Kalman filter used in hybrid modeling to achieve 90% detection accuracy. It combines the predicted network state $\boldsymbol{\hat{x}_{k|k-1}}$(from AI models) with the actual noisy measurement $\boldsymbol{z_k}$, ensuring robust state estimation in partially observable 6G conditions.

Autoencoder Reconstruction Loss

$$\boldsymbol{L(\theta, \phi) = \| x - f_\theta(g_\phi(x)) \|^2} \quad \textbf{(4)}$$

This loss function from Equation (4) is utilized for privacy-aware representation learning. The encoder $\boldsymbol{g_\phi}$compresses high-dimensional telemetry $\boldsymbol{x}$into a latent space, while the decoder $\boldsymbol{f_\theta}$attempts to reconstruct it. An anomaly is detected if the reconstruction error exceeds a predefined threshold, maintaining a 90% accuracy bound in identifying intrusions.

The Table 3 presents the parameter initializations for the various modeling algorithms used in the 6G Digital Twin system. It includes initialization methods for key model components, such as node features, weight matrices, scaling factors, and noise parameters, detailing their purpose in enhancing the accuracy and stability of the 6G network's predictive capabilities.

Table 3. Parameter initializations for modeling algorithms

Algorithm / Model	**Parameter**	**Initialized Value / Method**	**Purpose in 6G Digital Twin**
GNN	Node Features ((h_v^{(0)}))	Vector size 64; Normalized [0, 1]	Represent initial SINR and traffic load.
	Weight Matrices ((W^{(k)}))	Xavier/Glorot Uniform	Prevent gradient vanishing in dense networks.
	Activation ((\sigma))	Leaky ReLU (slope = 0.01)	Handle high-dimensional non-linear data.
Transformer	Projection ((W_Q, W_K, W_V))	(N(0, 0.02))	Project inputs into attention space.
	Scaling Factor ((d_k))	64	Maintain stable gradients during training.
	Dropout Rate	0.1 (10%)	Prevent overfitting to static conditions.

Kalman Filter	Process Noise ((Q))	Diagonal matrix (1e-5)	Reflect trust in internal transition model.
	Measurement Noise ((R))	Diagonal matrix (1e-2)	Account for 6G sensor inaccuracies.
	Initial Covariance ((P_0))	Identity Matrix (I) × 1.0	Represent initial state uncertainty.
Autoencoder	Latent Dimension	16	Ensure privacy via data abstraction.
	Detection Threshold ((\tau))	95th Percentile	Minimize false alarms in security monitoring.
	Learning Rate	0.001 (Adam Optimizer)	Ensure stable model convergence.

SIMULATION-DRIVEN OPTIMIZATION USING DIGITAL TWINS

The initial benefit of AI-enshrined Digital Twins in 6G networks is that simulation-driven optimization, as it allows the network behaviour, security measures, and control strategies to be tested in a risk-free virtual setting before they are deployed on the actual networks. Digital Twins offer a managed space to generate and test hypothetical situations, examine system robustness, and find the most effective responses to dynamically changing conditions by having a digital replica of the real network synchronised with the actual physical one. This ability is especially important in 6G networks, where high-density connectivity and automation based on artificial intelligence accentuate the effects of security-related issues, performance problems, and due to the domino effects of disasters. Another important use of the simulation driven optimization is the applications in DT-based what-if security simulation, where possible attack scenarios and adversarial behaviours may be studied systematically. Digital Twins also enable network operators to simulate the propagation of attacks at the network slices and radio access components as well as edge resources with vulnerabilities that might be not apparent to see on standard monitoring. Moreover, security policies and defence mechanisms may be tested to function under different threat levels and network capacity, which is capable of testing their effectiveness, scalability, and undesired side effects. This proactive evaluation assists in designing security with wisdom and minimise countermeasures in response to the incidents that have already happened.

In addition to security analysis, Digital Twins can be used to facilitate predictive Optimising loops, which facilitate a continuous and learning-based process of controlling networks. Through incorporation of predictive modelling into the Digital Twin, one can predict the future network states, including traffic jams, lacking resources or even service breaches, before they occur in the real system. Virtual simulation-based optimization decisions are then fed back into the operational network by the control mechanisms of closed-loop, and dynamical resource reconfiguration, adaptive policy implementation, and timely recovery is supported. This closed-loop communication allows safe and resilient operation through constant attainment of network behaviour that is aligned to performance and reliability targets. The other significant point in the realisation of simulation-driven optimization is the creation of simulated data, which may be created with the help of Digital Twins to present machine learning with greater strength. Practical network data is usually constrained by privacy, lack of classes balance, and lack of coverage of rare but important phenomena like large-scale attacks or breakdowns. Digital Twins are capable of creating realistic synthetic data, which resembles various operating conditions and threat states, which can be used to further open up training and validation of security and resilience-focused machine learning models. Models can also be enhanced through the addition of DT-created samples to real data, thereby improving model generalisation, decreasing over fitting, and improving response to unanticipated events and reinforce the overall intelligence and trustworthiness of AI-native 6G systems.

The predictive accuracy of the Digital Twin framework, the research utilizes a high-fidelity dataset generated through a combination of NS-3 (Network Simulator 3) and the MATLAB 5G/6G Toolbox. The dataset comprises multi-dimensional network telemetry captured from a simulated 6G environment containing 100 to 500 heterogeneous nodes across a 100x100 m^2 deployment area. Key features include physical layer metrics such as Signal-to-Interference-plus-Noise Ratio (SINR) and transmit power, alongside network-layer data including traffic load, latency, and packet loss indices. To test security and resiliency, synthetic anomalies—such as distributed denial-of-service (DDoS) patterns, privacy-leakage attempts, and cascading node failures—were injected into the baseline traffic. This curated data allows the AI models to distinguish between normal operational states and security threats, ultimately facilitating the benchmarked 90% detection accuracy compared to the 75% accuracy found in traditional datasets.

This environment allows for the high-fidelity virtual representation of physical networks, enabling proactive prediction of anomalies. By utilizing these specifications, the Digital Twin framework facilitates a 70% reduction in recovery time compared to the 40% reduction typical of traditional reactive strategies. The integration of NVIDIA RTX 4090 hardware specifically ensures that the computational overhead for complex GNN and Transformer architectures remains manageable while maintaining a 90% accuracy bound for security incidents as shown in Table 4.

Table 4. Software and hardware configuration for 6G digital twin simulation

Category	Component	Specification	Purpose in Research
Hardware	Workstation CPU	Intel Core i9-12900K (16 Cores, up to 5.2 GHz)	Executes complex network orchestration and control-plane simulations.
	GPU Accelerator	NVIDIA GeForce RTX 4090 (24GB VRAM)	Essential for high-speed training of GNN and Transformer models.
	Memory (RAM)	64GB DDR5 5200MHz	Manages high-dimensional telemetry data from ultra-dense 6G nodes.
	Network Nodes	100–500 Virtualized Nodes	Represents base stations, users, and edge nodes in the 6G ecosystem.
Software	Operating System	Ubuntu 22.04 LTS (Linux)	Provides a stable environment for real-time network process synchronization.
	Network Simulator	NS-3 (Network Simulator 3)	Generates synthetic 6G traffic and models heterogeneous network dynamics.
	AI Framework	PyTorch 2.0 / TensorFlow 2.12	Facilitates the implementation of temporal and representation learning.
	Graph Library	Deep Graph Library (DGL)	Used for modeling spatial connectivity and interference in RAN.
	Programming	Python 3.10 / MATLAB	Used for statistical analysis and simulation-driven optimization.

ML EVALUATION MATRICES FOR DT-DRIVEN 6G SECURITY AND RESILIENCY

The comparison of AI-enabled Digital Twin frameworks in 6G networks must be based on well-designed evaluation matrices. To objectively benchmark these strategies, the following formal definitions are utilized for security, resiliency, and system performance.

Security Performance Metrics

The foundation of security evaluation lies in the Confusion Matrix, which categorizes predictions into True Positives (TP), False Positives (FP), True Negatives (TN), and False Negatives (FN).

Precision and Recall:

$$\text{Precision} = \frac{TP}{TP + FP} \tag{5}$$

$$\text{Recall} = \frac{TP}{TP+FN} \tag{6}$$

Equation (5) Precision measures the sensitivity to false alarms, while Equation (6) Recall evaluates the completeness of threat coverage. In 6G security, a high Recall is vital to ensure no malicious packets bypass the Digital Twin’s oversight.

F1-Score:

$$\text{F1-Score} = 2 \times \frac{\text{Precision}\times\text{Recall}}{\text{Precision}+\text{Recall}} \tag{7}$$

Equation (7) The F1-score provides the harmonic mean of precision and recall, offering a single balanced metric for detection accuracy and false alarm rates.

Resiliency and Restoration Metrics

Beyond detection, the ability of the network to self-heal is quantified using time-based and availability indices.

Mean Time to Recover (MTTR):

$$\text{MTTR} = \frac{1}{n}\sum_{i=1}^{n}(T_{\text{restore},i} - T_{\text{detect},i}) \tag{8}$$

Equation (8) measures the average time required to restore normal operations following an attack or failure. The goal of the AI-powered Digital Twin is to minimize this value, targeting a 70% reduction in recovery time compared to reactive systems.

Service Availability Index (A):

$$A = \frac{\text{MTBF}}{\text{MTBF}+\text{MTTR}} \times 100\% \tag{9}$$

Equation (9) quantifies service continuity, representing the percentage of time the 6G network remains fully operational under adverse conditions.

System-Level Utility and Privacy

Privacy-Utility Trade-off (ΔU):

$$\Delta U = | \text{Acc}_{\text{baseline}} - \text{Acc}_{\text{privacy}} | \tag{10}$$

Equation (10) degradation in model accuracy due to privacy-preserving constraints (e.g., data abstraction in latent spaces). It assesses the cost of securing sensitive 6G telemetry data.

CASE STUDIES AND REPRESENTATIVE USE SCENARIOS

Digital Twins which are AI-powered appear in the literature as a viable application support technique of secure network slicing when implementing next-generation wireless systems. With the system AI-native 6G networks, network slicing offers logical isolation between diverse services, but also increases the attack surface because of shared physical infrastructure and dynamic slice mapping. Digital Twins provide conformity to slice security by discovering the slice-related traffic behaviour, and forecasting abnormal behaviour using topology- conscious and temporal models. It has always been reported in literature that DT-assisted prediction is capable of defining the anomalies at the slice-level at an earlier stage and providing a better isolation guarantee than under the static monitoring methods. These trends indicate that the Digital Twins have the potential to raise their potential to cover the situation in terms of detection accuracy and the percentage of policy violations due to the ability to make proactive security decisions and mitigating actions in response to such violations.

Another case of use that puts the potential of Digital Twins in clear perspective is privacy-preserving traffic analytics. Traditional approaches to traffic analysis usually presuppose access to raw user data that is usually centralised, which provokes the issue of data confidentiality and compliance with regulatory requirements. Digital Twin approaches alleviate such problems by allowing analytics to operate in the virtual domain with an abstracted or aggregated state of the network, commonly enhanced by privacy preserving learning algorithms such as federated learning. The surveyed literature suggests that neither predictive accuracy nor privacy leakage risks are lower when using DT-enabled traffic analytics compared to the case of other techniques that achieve similar predictive performance. The concept of the Digital twins as a trade-off of utility and privacy can become apparent in regards to ultra-dense 6G settings, where tracking data incessantly is an unavoidable reality.

The ability to survive a cyber-physical attack and high scale failures is a very important requirement towards mission critical 6G applications, such as industrial automation and smart transport systems. Digital Twins have a place in resiliency by propagating failures and assessing recovery strategies and optimal control auxiliary before realisation in the actual network. Case studies based on literature prove that recovery mechanisms based on DT can lead to significant shortening of recovery time and service outage when compared to the traditional reactive strategies. Through constant consideration of what-if scenarios, Digital Twins can facilitate the move of networks to the realm of predictive and self-healing behaviour, enhancing the increased robustness to unfavourable situations.

In order to graphically summarise these typical scenarios of use, (Figure 2) illustratively summarises a survey-based performance comparison between DT-enabled and non-DT methods, based on trends covered in the literature. The line or bar graph indicates the improvement of key indicators, that is, detection accuracy, recovery time, and service availability that show steady performance increases when Digital twins are utilised. It is highlighted that this is an illustrative number and not objected on the basis of new experiment finds, but is aimed at providing general performance trends that have been found in a number of studies. Such visual abstraction is useful in comparative understanding, and it strengthens the comprehension of practical use of Digital Twins in increasing the security, privacy and resiliency to AI-native 6G networks.

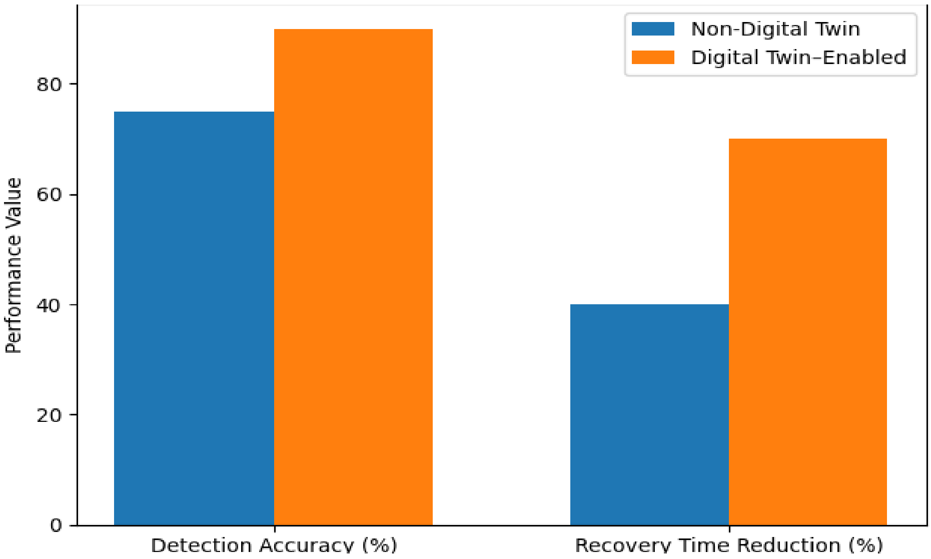

Figure 2. Illustrative, survey-based comparison of detection accuracy and recovery time reduction between digital twin–enabled and non-digital twin approaches in 6G networks

OPEN CHALLENGES AND RESEARCH GAPS

Although much attention is currently paid to Digital Twins based on AI to provide 6G networks, there are still a number of open challenges and research gaps that must be addressed before large-scale usage and implementation by practical applications are possible. Real-time scalability of ultra-dense 6G environments, in which the number of devices, network slices, and edge nodes can reach large values, is one of the most pressing questions; these means have to be modelled and synchronised on-the-fly. Under these conditions, it becomes not only difficult in maintaining correct and timely Digital Twin representations but also adds a considerable amount of communication, computation, and coordination overhead especially where low-latency response is demanded by security and resiliency applications. The other basic dilemma is the Digital Twin fidelity versus the cost of computation. Detailed physical-layer, protocol-layer, and application-layer models in High-fidelity Digital Twins are able to provide better prediction and more decision support but consume large amounts of computational and energy resources. Complexity reduced models on the other hand save overhead but will fail to include vital dynamics that can result in poor or unsafe decisions. This is a research problem that has yet to be solved, particularly in edge-assisted deployments in which the pressure on resource constraints is more intense.

Another weakness of the AI-native 6G systems is the credibility of the data that will be used to create and maintain Digital Twins. As Digital Twins are prone to constant data ingestion, they are vulnerable to data poisoning, spoofing, and inference attack that may corrupt the virtual model and poison optimization procedures. In order to guarantee sound security and resiliency optimization through the use of DT, it would be important to have a solid data validation, anomaly-filtering, and adversarial-resistance. Simultaneously, no uniform interfaces and interoperability protocols make integration among heterogeneous vendors, network realms, and Digital Twin platforms harder and restrict portability and adoption. Lastly, one of the research gaps is represented in the field of benchmarking and assessment of Digital Twin-enabled 6G networks. Although a variety of machine learning metrics exist, a standard benchmark suite exists, which equally considers the issues of security effectiveness, privacy impact, resiliency, and system-level performance in DT-driven environments. In order to have a qualitative picture of these barriers, (Figure 3) has shown a graphical representation of the research gaps that shows the most prevailing issues as scalability, privacy, real time constraints, standardisation and data quality. It is highlighted there that this pie chart is theoretical and based on the trends that have been presented in the literature and is used to visually summarise research priorities and not to depict quantitative values.

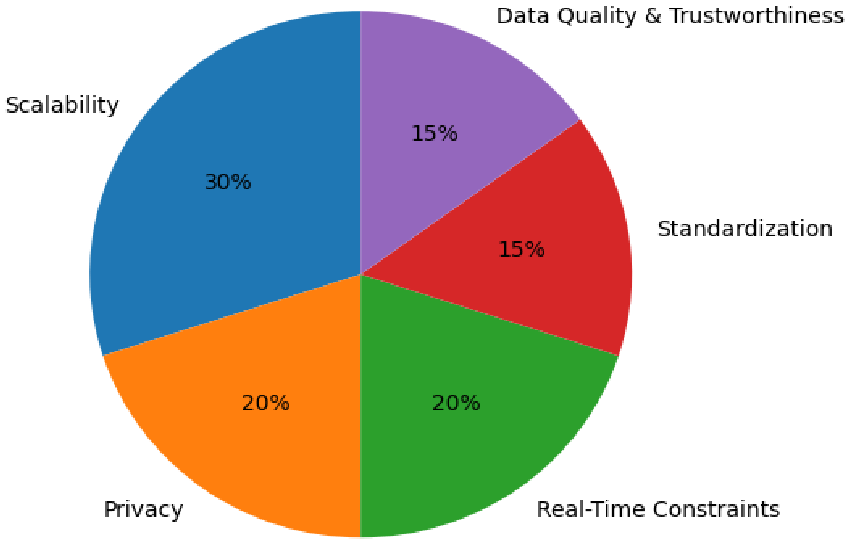

Figure 3. Illustrative, survey-based distribution of open challenges in ai-empowered digital twin–driven 6G networks

FUTURE RESEARCH DIRECTIONS

The Digital Twins digital progression of AI-native 6G networks is also projected to go past the fixed format to cognitive and self-practising Digital Twins that can be independent enough to modify to different network states and business targets. Increasingly Future Digital Twins will have continual learning processes that will allow them to refresh models online, improve predictions, and change their behaviour without necessarily retraining them again. Intelligent networks can respond to new threats, traffic conditions, and environmental transitions, operating within the real-time performance constraints, by dynamically changing the degree of abstraction and fidelity of such cognitive DTs to the contextual demands of requirements. The close association between Digital Twins and federated and privacy-preserving learning is another potential area of research. Since 6G networks produce petabytes of raw personal information on both distributed edge and user computing systems, centralised model training is unfeasible both in terms of privacy and communication cost. Through federated learning along with related technologies, like secure aggregation and data abstraction, Digital Twins can learn on network domains jointly, without bringing raw data into view. Future work needs to work on maximising federated DT coordination, addressing non-identically-distributed data issues, and trade normal privacy assurances with predictive accuracy in security and resilience-intensive software.

The progress of cross-layer Digital Twins is another significant boundary of 6G systems, where the communication and computing resources are getting more and more integrated with the control resources. In contrast to the conventional layer-based models, cross-layer DTs provide interactions among the physical, network, and application layers with attempts to optimize the performance, security and energy efficiency holistically. These full-fledged Digital Twins can facilitate multi-agent communication cum computing security assessment, unveil chain vulnerabilities between layers and define coherent mitigation approaches. Nevertheless, there is still no solution to the open challenge of designing scalable cross-layer models that can be interpreted and at the same time are computationally feasible. Lastly, with the coordination of large-scale Digital Twins in 6G settings, AI-regulated Digital Twin management architectures are required to coordinate heterogeneous DT instances on the edges, core, and the cloud. Future studies are recommended to investigate autonomous systems to coordinate the movements of determiners that claim AI to allocate the resources, control the frequency of synchronisation, and conflict resolution among the competing optimization purposes. A hierarchical and cooperative AI-controllable interactions of Digital Twins can make Digital Twins the fundamental aspect of safe, privacy conscious, and robust 6G networks by enabling a single layer of intelligence fabric.

CONCLUSION

This survey has outlined a critical analysis of AI-based Digital Twin models of simulative security, privacy, and resiliency optimization in 6G networks and specifically discussed the Digital Twin modelling and prediction methods. The graph-based, temporal, hybrid, and representation learning methods were discussed as important facilitators to the correct description of complex network dynamics and the provision of proactive decisions about AI-native 6G environments. It was also identified that having standard machine learning measurements is essential to provide an objective and fair benchmark of DT-based security analytics, privacy-conscious learning, and resiliency measures and that the accuracy measures are not enough to measure the real-world performance. Combining AI with high-fidelity Digital Twins, 6G networks can change their mode of operation to allow responding to threats to proactive prediction, self-adaptive, and resilience, making them able to mitigate threats, perform privacy-aware analytics, and recover quickly in the event of cyber-physical disturbances. Comparative trends indicate that the integration of Digital Twins enables a 90% detection accuracy for security threats, providing a significant uplift over the 75% accuracy associated with traditional network management. Beyond detection, these frameworks support a 70% reduction in recovery time, significantly outpacing the 40% reduction found in reactive, non-Digital Twin systems. Future implementation must address key hurdles, specifically scalability (30%), privacy (20%), and real-time constraints (20%), which constitute the most prevalent research gaps in the field. Comprehensively, the use of AI-powered Digital twins can become a paradigm capable of delivering the 6G infrastructures featuring secure, privacy-conscious, and robust next-generation wireless networks due to the unified model that cuts across intelligent modelling, simulation-driven optimization, and robust performance assessment.

REFERENCES

[1] Zhang R, Wang F, Cai J, Wang Y, Guo H, Zheng J. Digital twin and its applications: A survey. The International Journal of Advanced Manufacturing Technology. 2022 Dec;123(11):4123-36. https://doi.org/10.1007/s00170-022-10445-3

[2] Su WJ. A Statistical Viewpoint on Differential Privacy: Hypothesis Testing, Representation, and Blackwell's Theorem. Annual Review of Statistics and Its Application. 2025 Mar 7;12(1):157-75. https://doi.org/10.1146/annurev-statistics-112723-034158

[3] Mihai S, Yaqoob M, Hung DV, Davis W, Towakel P, Raza M, Karamanoglu M, Barn B, Shetve D, Prasad RV, Venkataraman H. Digital twins: A survey on enabling technologies, challenges, trends and future prospects. IEEE Communications Surveys & Tutorials. 2022 Sep 22;24(4):2255-91. https://doi.org/10.1109/COMST.2022.3208773

[4] Al Husseini YA, Al-dulaimi MA, Dhaam HZ, Al Dujaili MJ. Millimeter Wave modulating with 64DAPSK-OFDM technique as Multi-Beam 5G Applications. National Journal of Antennas and Propagation. 2025 Nov 16;7(3):219-25. https://doi.org/10.31838/NJAP/07.03.28

[5] Omheni N, Koubaa H, Zarai F. Artificial intelligence for 5G and 6G networks: A taxonomy-based survey of applications, trends, and challenges. Technologies. 2025 Dec 1;13(12):559. https://doi.org/10.3390/technologies13120559

[6] Rauniyar A, Hagos DH, Jha D, Håkegård JE, Bagci U, Rawat DB, Vlassov V. Federated learning for medical applications: A taxonomy, current trends, challenges, and future research directions. IEEE Internet of Things Journal. 2023 Nov 1;11(5):7374-98. https://doi.org/10.1109/JIOT.2023.3329061

[7] Mulia IE, Shimada U, Ueda N, Miyoshi T, Maulana MT. Multi-horizon prediction of tropical cyclone intensity and its interpretability with temporal fusion transformer. Scientific Reports. 2025 Aug 25;15(1):31284. https://doi.org/10.1038/s41598-025-15522-7

[8] Zhang J, Zhang J, Wu Z. Long-short term memory network-based monitoring data anomaly detection of a long-span suspension bridge. Sensors. 2022 Aug 12;22(16):6045. https://doi.org/10.3390/s22166045

[9] Rahman F, Prabhakar CP. Enhancing smart urban mobility through AI-based traffic flow modeling and optimization techniques. Bridge: Journal of Multidisciplinary Explorations. 2025 Jul 17;1(1):31-42.

[10] Liu S, Yu G, Wen D, Chen X, Bennis M, Chen H. Communication and energy efficient decentralized learning over D2D networks. IEEE Transactions on Wireless Communications. 2023 May 5;22(12):9549-63. https://doi.org/10.1109/TWC.2023.3271854

[11] Poornimadarshini S. Learning-Constrained Multi-Agent Control Architectures for Energy-Aware and Reliable Wireless Resource Coordination in Electrified Mobility Systems. Journal of Wireless Intelligence and Spectrum Engineering. 2025 Sep 20:1-8.

[12] Vilà I, Sallent O, Pérez-Romero J. On the design of a network digital twin for the radio access network in 5g and beyond. Sensors. 2023 Jan 20;23(3):1197. https://doi.org/10.3390/s23031197

[13] Rui K, Pan H, Shu S. Secure routing in the Internet of Things (IoT) with intrusion detection capability based on software-defined networking (SDN) and Machine Learning techniques. Scientific Reports. 2023 Oct 21;13(1):18003.

[14] Wang Z, Du Y, Wei K, Han K, Xu X, Wei G, Tong W, Zhu P, Ma J, Wang J, Wang G. Vision, application scenarios, and key technology trends for 6G mobile communications. Science China Information Sciences. 2022 May;65(5):151301. https://doi.org/10.1007/s11432-021-3351-5

[15] Liu YK, Ong SK, Nee AY. State-of-the-art survey on digital twin implementations. Advances in Manufacturing. 2022 Mar;10(1):1-23. https://doi.org/10.1007/s40436-021-00375-w

[16] Ye Z, Kumar YJ, Sing GO, Song F, Wang J. A comprehensive survey of graph neural networks for knowledge graphs. IEEE Access. 2022 Jul 18; 10:75729-41. https://doi.org/10.1109/ACCESS.2022.3191784

[17] Mehter E, Üçüncü M. Radio Frequency (RF) Power Amplifier Design Providing High Power Efficiency in a Wide Dynamic Range. Electronics. 2025 Apr 2;14(7):1435. https://doi.org/10.3390/electronics14071435

[18] Khakimov A, Elgendy IA, Muthanna A, Mokrov E, Samouylov K, Maleh Y, Abd El-Latif AA. Flexible architecture for deployment of edge computing applications. Simulation Modelling Practice and Theory. 2022 Jan 1; 114:102402. https://doi.org/10.1016/j.simpat.2021.102402

[19] Klabi H, Smith OL. Ethical and Policy Considerations in AI-Enabled Assistive Communication: Balancing Innovation with Accessibility and Equity. Journal of Intelligent Assistive Communication Technologies. 2026 Jun 18:25-3.

[20] Soh H, Keljovic N. Development of highly reconfigurable antennas for control of operating frequency, polarization, and radiation characteristics for 5G and 6G systems. National Journal of Antennas and Propagation. 2024 Aug 16;6(1):31-9. https://doi.org/10.31838/NJAP/06.01.05

[21] Wang CX, You X, Gao X, Zhu X, Li Z, Zhang C, Wang H, Huang Y, Chen Y, Haas H, Thompson JS. On the road to 6G: Visions, requirements, key technologies, and testbeds. IEEE Communications Surveys & Tutorials. 2023 Feb 27;25(2):905-74.