STM JOURNALS

Journal of
Telecommunication, Switching Systems and Networks

ISSN: 2454-6372
Volume 13, Issue 1, 2026
January–April
DOI (Journal): 10.37591/JoTSSN

https://journals.stmjournals.com/jotssn

Review JoTSSN

Overview of AI-Driven Antenna Technologies and Privacy-Preserving Methods for Next-Generation 6G Wireless Systems

Rinkesh Mittal[1,*], Mohit Srivastava[2], Pooja Sahni[3], Nidhi Chahal[4], Preeti Bansal[5]

Abstract

The next-generation of wireless communications, 6G, will be built on the convergence of artificial intelligence (AI) and advanced antenna systems. AI-driven antennas are poised to address the unprecedented requirements for data rate, reliability, adaptability, and ubiquity in future networks. An overview of current advancements in AI-enabled antenna systems for 6G networks is provided in this study. From traditional base station deployments to distributed, cell-free, and user-centric frameworks, it examines architectural progress. Advanced beamforming methods that improve spectrum efficiency and interference mitigation—such as hybrid, dynamic, and AI-assisted beam management strategies—are given special attention. Massive Multiple Input, Multiple Output (MIMO) and cell-free MIMO systems are also discussed, emphasizing how machine learning methods enhance mobility management, resource allocation, and channel estimation in extremely crowded and diverse situations. By integrating learning and decision-making skills straight into the physical layer, AI-powered antenna technologies bring about a paradigm shift. These intelligent systems continuously evaluate channel conditions, user mobility patterns, interference characteristics, and ambient dynamics to maximize performance in real time, as opposed to depending just on preset signal processing algorithms. Emerging 6G applications, such as immersive extended reality (XR), holographic communications, autonomous transportation systems, smart cities, remote healthcare, digital twins, and large-scale industrial automation, depend on this kind of flexibility. AI-driven antennas greatly improve spectral efficiency and network resilience by enabling adaptive waveform design, intelligent interference suppression, and predictive beam steering. This paper presents a synthesized account of recent developments, focusing on architectural evolution, beamforming techniques, massive and cell-free MIMO, integrated AI-empowered management, and comparison of privacy-preserving methods.

***Author for Correspondence**
Rinkesh Mittal
E-mail: rinkeshin@gmail.com

[1]Professor and Head, Department of Electronics and Communication Engineering, Chandigarh Engineering College, Mohali, Punjab, India
[2]Dean. Department, Department of Electronics and Communication Engineering, Chandigarh Engineering College, Mohali, Punjab, India
[3]Professor, Department of Electronics and Communication Engineering, Chandigarh Engineering College, Mohali, Punjab, India
[4]Faculty, Department of Electronics and Communication Engineering, Chandigarh Engineering College, Mohali, Punjab, India
[5]Assistant Professor, Department of Electronics and Communication Engineering, Chandigarh Engineering College, Mohali, Punjab, India

Received Date: February 25, 2026
Accepted Date: February 27, 2026
Published Date: March 10, 2026

Citation: Rinkesh Mittal, Mohit Srivastava, Pooja Sahni, Nidhi Chahal, Preeti Bansal. Overview of AI-Driven Antenna Technologies and Privacy-Preserving Methods for Next-Generation 6G Wireless Systems. Journal of Telecommunication, Switching Systems and Networks. 2026; 13(1): 28–34p.

Keywords: Artificial intelligence (AI), 6G wireless communications, AI-powered antennas, massive and cell-free MIMO, and privacy-preserving methods

INTRODUCTION

The rapid evolution from the analog 1G era to today's intelligent 5G/6G landscape is characterized by a persistent drive for enhanced connectivity, lower latency, and higher energy efficiency. In 6G, these ambitions coalesce within AI-driven smart antenna systems that blend real-

time environmental awareness, autonomous adaptation, and seamless integration across heterogeneous platforms. These goals come together in 6G networks' AI-powered smart antenna systems, which incorporate autonomous adaptation, real-time environmental sensing, and smooth coordination across a variety of platforms, such as satellite networks, unmanned aerial vehicles (UAVs), terrestrial base stations, and high-altitude platforms. Next-generation smart antennas are anticipated to continuously learn from their environment, anticipate channel fluctuations, and dynamically alter radiation patterns to maximize connection dependability and coverage, in contrast to traditional antenna arrays that depend on static or semi-static designs. In high-frequency bands like millimeter-wave and terahertz spectra, where signal transmission is extremely sensitive to obstruction, mobility, and atmospheric conditions, this evolution is especially important. This change is largely made possible by AI. AI gives antenna systems predictive analytics, adaptive beam management, interference reduction, and intelligent resource allocation capabilities through sophisticated machine learning and deep learning algorithms. By processing enormous amounts of real-time data at the network edge, these systems minimize latency and backhaul congestion while lowering the need for centralized control. Distributed decision-making is further facilitated by edge intelligence, which enables networks to react instantly to changing environmental dynamics, user movement patterns, and traffic demands. This transformation is guided by AI's exceptional capacity for predictive analytics, optimization, and decision-making at the edge [1–4].

ROLE OF AI IN 6G ANTENNA ARCHITECTURES

AI integration in antenna systems manifests through several core innovations:

AI-Optimized Beamforming

Deep learning models dynamically steer beams for coverage maximization and interference reduction, ensuring signal fidelity in dense urban, Internet of Things (IoT), and vehicular scenarios [1–3].

Adaptive and Massive MIMO

Machine learning enables the real-time optimization of massive MIMO and cell-free architecture. Algorithms manage user grouping, resource allocation, and scheduling, thereby boosting spectral efficiency and energy savings.

Self-Configuring Arrays

Federated and reinforcement learning empower antenna modules to autonomously adapt, self-heal, and conduct predictive maintenance across large networks.

ENABLING AND EMERGING TECHNOLOGIES

Key enabling technologies underpinning this shift include:

Deep Neural Networks (DNNs)

For channel estimation, user localization, and environmental sensing in large-scale antenna systems [2, 3].

Edge AI and Distributed Learning

It allows localized, privacy-preserving optimization across decentralized infrastructure, which is essential for meeting latency and security demands [2–4].

Intelligent Reflecting Surfaces (IRS)

AI-guided IRS dynamically shapes and redirects wireless signals, extending coverage and mitigating blockages [1–4].

TECHNICAL GAINS AND CHALLENGES

Documented improvements from AI-driven methods include:

- Up to 30% reduction in interference, 25% gain in signal-to-noise ratio (SNR), and 15–20% boosts in coverage and reliability, compared to traditional methods.
- High computational demands and data privacy remain leading challenges, requiring efficient edge designs, federated learning frameworks, and explainable AI [3, 4].
- Standardization and regulatory frameworks for AI integration are urgently required for large-scale, interoperable deployment [2–4].

KEY PERFORMANCE RESULTS

Beam Forming Accuracy

Deep learning-powered beam forming models enable up to 25% improvement in SNR compared to traditional methods, leading to stronger and clearer connections in dense environments [1, 2].

Interference Mitigation

AI-driven antenna systems achieve a 30% reduction in signal interference, which is vital for urban and crowded deployments [1–3]

Coverage and Adaptability

Real-time AI pattern control in smart antennas expands coverage by approximately 20% and increases connectivity stability by 15%, supporting robust network service in fluctuating real-world conditions [1–3]

Resource Optimization

AI-based algorithms increase resource allocation efficiency by up to 40%, translating to improved network throughput and lower operational costs through dynamic spectrum and power control [1, 2]

Predictive Analytics

Advanced predictive models forecast network demand and traffic patterns with 90% accuracy, enabling proactive network adjustments for optimized experience and reliability [1, 2].

Energy Efficiency

Machine learning and adaptive optimization reduce energy consumption in MIMO arrays and massive antenna setups by dynamically tuning active elements, crucial for low-power and sustainable network operation.

Latency Reduction

AI-enabled real-time beam switching and data-driven decision-making support ultra-reliable, low-latency communications required for industrial robotics, healthcare, and AR/VR [2, 3]

TECHNICAL BENEFITS AND USE CASES

Robustness to Channel Variations

AI-enhanced antennas maintain high accuracy and reliability in complex propagation environments, such as mmWave or terahertz bands and high-mobility scenarios. Rapid changes in channel conditions necessitate incredibly quick adaptation in high-mobility scenarios, such as high-speed trains, autonomous vehicles, unmanned aerial vehicles (UAVs), and crowded urban traffic environments. To avoid connection drops, AI models are able to foresee link deterioration, estimate user paths, and proactively modify beam patterns. This predictive ability lowers delay brought on by repeated beam alignment processes and greatly improves link reliability [2, 3].

Self-Healing and Automation

Lifelong learning and zero-touch maintenance allow for automated identification of transmission anomalies and routine optimization, minimizing downtime and manual intervention. By automating standard operational chores like configuration changes, defect detection, performance optimization, and

resource reallocation, zero-touch maintenance enhances lifetime learning. AI systems can spot transmission anomalies including signal deterioration, unexpected latency spikes, hardware issues, or unusual traffic congestion through real-time monitoring and predictive analytics before they become serious problems. Then, automated corrective actions, such as load balancing, adaptive beam adjustment, or traffic rerouting, can be carried out immediately [1–3].

Secure Communications

AI-driven anomaly detection protects networks from jamming and spoofing, thereby adding resilience against security threats. In wireless communication environments, jamming attacks aim to disrupt legitimate transmissions by introducing intentional interference, while spoofing attacks attempt to impersonate authorized devices or manipulate location and identity information. AI-driven anomaly detection systems can recognize subtle irregularities in signal strength, timing, modulation characteristics, or access behavior that may indicate such threats (Figure 1). Once detected, automated mitigation strategies—such as dynamic frequency hopping, adaptive beamforming, power control adjustments, or isolation of suspicious nodes—can be deployed in real time to maintain service continuity [3].

CURRENT REAL-WORLD OUTCOMES

- Industrial deployments and test beds have validated these gains, with CNN channel estimators and reinforcement-learning-powered resource allocations consistently outperforming classical approaches in simulation and field trials from Figure 1.
- Active field studies show that AI-matched antennas excel in real-time adaptation (crucial for IoT, autonomous vehicles, and smart city infrastructure demands) and resource-constrained deployments.

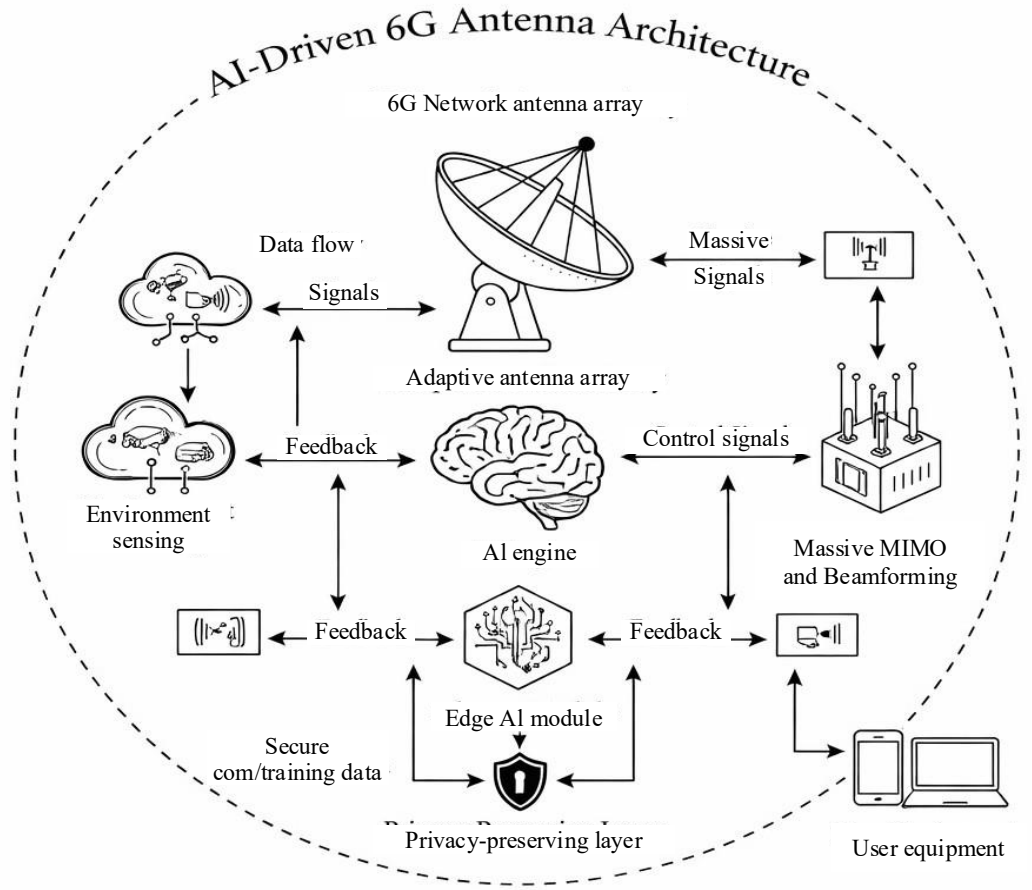

Figure 1. AI-driven antenna communication.

ONGOING CHALLENGES

Despite these results, real-time computational demands and data privacy issues remain areas for further research, where federated learning and privacy-preserving AI methods can offer future solutions.

Recent research articles on privacy-preserving AI methods highlight several essential techniques, including differential privacy, homomorphic encryption, secure multiparty computation, federated learning, and hybrid approaches. These methods protect sensitive data while supporting effective AI model development in the healthcare, telecom, and IoT sectors. By adding precisely calibrated noise to datasets or model outputs, differential privacy prevents the identification of specific records while maintaining overall statistical usefulness, offering mathematically verifiable privacy assurances. Secure outsourced processing in cloud or edge contexts is made possible by homomorphic encryption, which allows computation on encrypted data directly without the need for decryption. Sensitive data is kept locally safe by secure multiparty computation, which enables cooperative model training among several participants without disclosing their private inputs.

By decentralizing model training, federated learning further improves privacy by lowering exposure risks by sharing and aggregating just model updates or gradients rather than sending raw data to a central server. Particularly in large-scale distributed networks, hybrid systems combine these strategies to strike a compromise between model accuracy, communication cost, computational performance, and privacy guarantees. These privacy-preserving measures are particularly important in industries with extraordinarily high data sensitivity, like healthcare, telecommunications, smart cities, finance, and the IoT. AI systems used in healthcare are dependent on genomic information, medical imaging, and electronic health records—all of which must be kept strictly secure. AI-driven resource allocation, mobility forecasting, and user behavior analytics in 6G and telecommunications networks require ongoing subscriber data processing.

Similar to this, IoT ecosystems produce detailed behavioral and environmental data that, if managed carelessly, may result in data misuse or surveillance threats. These industries can profit from advanced analytics while abiding by ethical norms, legal frameworks, and cybersecurity best practices thanks to privacy-preserving AI techniques.

KEY PRIVACY-PRESERVING AI METHODS

Differential Privacy

Injects random noise into datasets and model outputs, ensuring that machine learning models cannot leak individual data points. This technique is widely used in healthcare and large data environments, where statistical guarantees are necessary. This method can be used for data preparation, gradient changes during model training, and result publication, among other phases of the machine learning pipeline. Differential privacy lowers the danger of membership inference attacks and model inversion attacks, which aim to reconstitute private training data in large-scale AI systems, especially those running in distributed or cloud-based contexts.

Homomorphic Encryption

It allows AI models to operate on encrypted data, keeping information confidential throughout the analytic process. Fully homomorphic and partially homomorphic schemes support various computing tasks but often incur higher computational overheads. Partially homomorphic encryption (PHE) and fully homomorphic encryption (FHE) are the two main types of homomorphic encryption. PHE schemes are appropriate for particular, limited AI applications since they only handle a small number of operations, like addition or multiplication. FHE, on the other hand, permits arbitrary calculations on encrypted data, opening the door to more intricate machine learning processes like secure data aggregation and neural network inference [4, 5].

Secure Multiparty Computation (SMPC)

Enables collaborative training on distributed datasets while protecting the privacy of each party's data, using cryptographic protocols such as secret sharing and garbled circuits [6, 7].

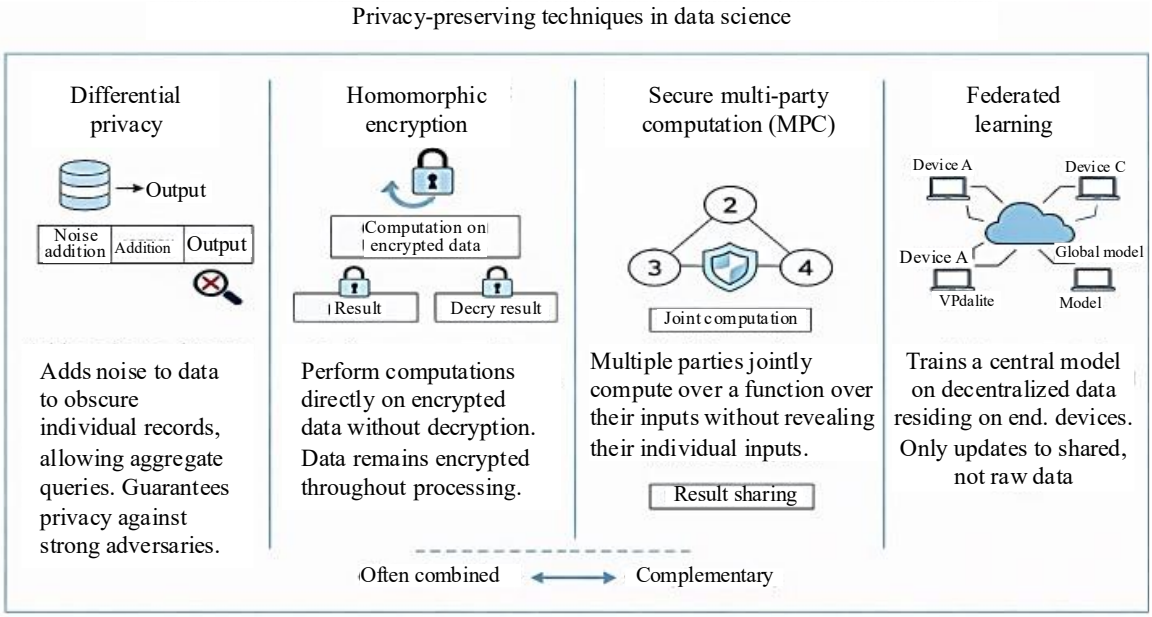

Figure 2. Comparison of privacy-preserving techniques.

Federated Learning

Distributes the model training process across local nodes (e.g., hospitals, IoT devices), aggregating only model updates instead of raw data. This method improves scalability and data protection but faces challenges in network efficiency and full privacy guarantees [8–10].

APPLICATIONS AND CHALLENGES

- These privacy-preserving techniques have been substantially deployed in healthcare, where compliance with regulations (HIPAA, GDPR) is crucial. They are also increasingly adopted in telecom and IoT networks, helping safeguard highly distributed and sensitive data from Figure 2.
- Hybrid systems that combine federated learning with differential privacy or cryptographic protocols are among the most promising directions, offering improved scalability and stronger privacy guarantees.
- Ongoing challenges involve balancing privacy, computational efficiency, and predictive accuracy—tradeoffs continue to define the choice and configuration of privacy-preserving AI for real-world applications.

CONCLUSION

- AI-driven sixth-generation (6G) antenna systems promise transformative gains in wireless performance, resilience, and automation. By merging advanced antenna technology with intelligent algorithms, these systems will form the backbone of future ubiquitous, secure, and adaptive networks, enabling revolutionary applications across smart cities, autonomous vehicles, immersive media, and beyond. Ongoing research must address energy efficiency, trust, and transparency to realize the full vision of intelligent wireless communication.
- In summary, AI-driven 6G antenna systems deliver substantially higher accuracy, coverage, adaptability, efficiency, and reliability, firmly positioning them as transformative technologies essential for the future of wireless connectivity and intelligent applications.

REFERENCES

1. Sasirekha B, Gunavathi C. Systematic review on privacy-preserving machine learning techniques for healthcare data. J Cyber Secur Technol. 2025;10:1-26. doi:10.1080/23742917.2025.2511145.

2. Torkzadehmahani R, Nasirigerdeh R, Blumenthal DB, Kacprowski T, List M, Matschinske J, et al. Privacy-preserving artificial intelligence techniques in biomedicine. Methods Inf Med. 2022;61(Suppl 1):e12-e27. doi:10.1055/s-0041-1740630. PMID: 35062032.
3. Srinivas K, Sateesh R, Vadivukarassi M, Sathya P, Aandi S, Swapna M. Privacy-preserving federated learning for fault detection in distributed manufacturing. In: Proceedings of the 5th IEEE International Conference on ICT in Business Industry & Government (ICTBIG); 2025. p. 1-6. doi:10.1109/ICTBIG68706.2025.11323921.
4. Khang A, Singh Y, Barak D. Review of the literature on using machine and deep learning techniques to improve IoT security. In: Khang A, Abdullayev HV, Litvinova E, Musrat GE, Avramovic ZŽ, editors. Revolutionizing Automated Waste Treatment Systems: IoT and Bioelectronics. Hershey (PA): IGI Global Scientific Publishing; 2024. p. 273-300. doi:10.4018/979-8-3693-6016-3.ch018.
5. Mareedu A. Hybrid AI models in network security: Combining ML, DL, and rule-based systems. Int J Emerg Res Eng Technol. 2024;5:109-121.
6. Tok YE, Toprak AG, Karahan SN, Mercan OB, Aydin HM, Altintas M. Artificial intelligence for next-generation 6G technologies and networks. Discov Netw. 2026;2(1):3. doi:10.1007/s44354-026-00016-3.
7. Zhao H. Research on privacy protection and performance optimization of 6G communication network based on the fusion of federated learning and edge computing. Discov Artif Intell. 2025;6. doi:10.1007/s44163-025-00687-x.
8. Lorincz J, Klarin Z, Begusic D. Advances in improving energy efficiency of fiber-wireless access networks: A comprehensive overview. Sensors (Basel). 2023;23(4):2239. doi:10.3390/s23042239. PMID: 36850836.
9. Akinsiku AM. Federated learning techniques for privacy-preserving AI in distributed networks: A review. TechSphere J Pure Appl Sci. 2025;2(1):69-83.
10. Sabir B, Yang S, Nguyen D, Wu N, Abuadbba A, Suzuki H, et al. Systematic literature review of AI-enabled spectrum management in 6G and future networks. arXiv [Preprint]. 2024. arXiv:2407.10981.

