WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Comprehensive Study of Security Challenges and Privacy Issues in 6G Networks

Vinayak Jadhav[1], Arun L. Kakhandki[2]

[1]Department of Electronics and Communication Engineering, AGMRCET, Affiliated to VTU Belagavi, Varur, Karnataka, India-581207
[2]Department of Electronics and Communication Engineering, KLS VDIT, Affiliated to VTU Belagavi, Haliyal, Karnataka, India-581329.
DOI : https://doi.org/10.55248/gengpi.6.0825.3086

ABSTRACT

The upcoming sixth-generation (6G) wireless network envisions a hyper-connected world with massive device connectivity, ultra-low latency (ULL), high energy efficiency, and intelligent edge services. While the technological advancements in 6G promise revolutionary aids, they also impart new and complex security and privacy challenges. This review explores the evolving landscape of 6G security threats and privacy concerns. It critically evaluates the unique vulnerabilities introduced by key 6G technologies such as intelligent surfaces, THz communication, quantum networking, AI-driven infrastructure, and pervasive sensing. The paper also analyses current mitigation strategies and identifies gaps for future research.

Keywords: 6G, security challenges, privacy issues, block chain, AI, quantum computing, THz communication, authentication, and encryption.

1. Introduction

The generation 6G of wireless communication systems is designed to revolutionize the digital landscape by enabling ultra-high-speed connectivity, intelligent automation, and pervasive computing. While 5G introduced breakthroughs in latency, bandwidth, and massive device connectivity, 6G is envisioned as a more transformative paradigm one that flawlessly combined with artificial intelligence (AI), edge computing, terahertz (THz) communications, and quantum technologies into the network infrastructure [1, 2]. In case of expected data speed(rate) up to 1 Tbps, fewer than the millisecond i.e., low latency and the capacity to provide over 10 million users for each square km, 6G is intended to report the connectivity need of upcoming intelligent applications such as holographic communications, real-time digital twins, autonomous drones, and brain-computer interfaces [3, 4].

The AI-native architecture of 6G networks allows AI algorithms to be integrated into control and data planes, handling traffic management, source allocation, service orchestration, and security threat detection. Technologies like quantum-safe encryption, massive MIMO, reconfigurable intelligent environments, and intelligent reflecting surfaces will create a new era of reliable communication [5, 6]. However, the spread of 6G and its addition of edge AI opens up new ways for attackers to enter, as it is faster and more efficient to process data at the edge. Traditional centralized security measures may not be enough, as billions of devices share intelligence and make decisions [7, 8]. The physical layer of 6G is vulnerable, with Terahertz and millimeter wave bands being easy to interfere with, block signals, and listen in on. Safe channel estimation and reliable beamforming are vital for maintaining data integrity [9-10]. The vast amount of context-aware and sensitive data collected by 6G-enabled services increases privacy threats, necessitating changes in privacy-preserving strategies like access restriction and encryption. More advanced models like federated learning, homomorphic encryption, and differential privacy will be needed to confirm that user data remains protected, even while enabling AI-driven personalization and analytics [11].

The AI-centric architecture of 6G introduces further challenges related to algorithmic transparency, fairness, and explainability. Black-box AI models can take decisions about resource allocation, intrusion detection, or user authentication, yet they often lack explainability, making them vulnerable to manipulation or bias. Research in explainable AI (XAI) and interpretable machine learning is beginning to address these concerns, aiming to make AI decisions more transparent and trustworthy. These efforts are mainly important in regulated domains like autonomous vehicles, healthcare, and public safety, where errors or biases could lead to catastrophic outcomes [12, 13].

Trust management is another central issue. With devices dynamically joining or leaving the network, establishing and maintaining trust in such a decentralized environment becomes complex. Blockchain and distributed ledger technologies (DLTs) are being explored for decentralized authentication and identity management, enabling tamper-proof transaction records and consensus-based validation mechanisms [14]. However, their scalability, latency, and energy consumption need to be optimized for real-time 6G operations.

From a regulatory and policy standpoint, the 6G ecosystem will span across multiple jurisdictions and legal regimes. Data sovereignty, compliance with privacy rules and laws like the GDPR, and cross-border data sharing agreements will become increasingly contentious as services become more global and data flows more fluid. Regulatory frameworks must evolve to ensure user rights, data protection, and ethical governance while accommodating the flexibility and scalability that 6G promises [15].

Despite ongoing research, most studies still focus on individual security solutions or specific layers of the network. A unified, end-to-end security architecture that addresses vulnerabilities across the physical, network, and service layers remains largely missing. Moreover, interdisciplinary association between technologists, ethicists, policymakers, and legal experts is critical to addressing the full spectrum of security and privacy risks in 6G.

This paper presents a comprehensive review of security threats and privacy challenges in 6G networks. It analyses vulnerabilities across different layers of the 6G architecture and discusses emerging countermeasures, including AI-based intrusion detection systems, post-quantum cryptography, privacy-preserving computation, and decentralized trust frameworks. The paper also emphasizes the importance of regulatory evolution and global standardization efforts. By identifying research gaps and proposing future directions, this work aims to provide a foundational framework for designing secure, ethical, and privacy-respecting 6G systems.

2. Main Enabling Technologies and Their Security Implications

The emergence of 6G networks is closely tied to the integration of advanced technologies such as Terahertz (THz) communication, intelligent reflecting surfaces (IRS), artificial intelligence (AI), quantum communication, and ubiquitous sensing. While these technologies proposal for transformative capabilities in terms of capacity, speed, and responsiveness, they also introduce novel security and privacy risks that must be addressed from the ground up.

2.1 Terahertz (THz) Communication

6G envisions the use of Terahertz frequencies (0.1–10 THz) to support ultra-high-speed applications such as holographic telepresence, extended reality (XR), and real-time tactile internet. However, the unique propagation characteristics of THz namely, high directionality, short-range propagation, and susceptibility to atmospheric absorption—make these links vulnerable to new forms of attacks [16, 17].

Specifically, THz communication is prone to eavesdropping via beam leakage, interception through side lobes, and beam spoofing, wherein attackers imitate or deflect legitimate beams [18]. Despite its narrow beamwidth, reflections or poorly aligned beams can be exploited to compromise link confidentiality. Traditional physical-layer security (PLS) mechanisms, including wiretap coding and artificial noise, become less effective at THz due to high propagation losses [19]. To counteract this, researchers have proposed adaptive beamforming, channel-aware jamming, and artificial noise injection tailored to the THz spectrum [20]. Spectral fingerprinting and ultra-massive MIMO architectures with intelligent beam tracking have also been suggested to strengthen authentication and improve resilience against link spoofing [21].

2.2 Intelligent Reflecting Surfaces (IRS)

IRS play a pivotal role in enabling reconfigurable intelligent surfaces for 6G environments, allowing fine-grained control of electromagnetic wave propagation through passive beamforming elements [22, 23]. However, their passive nature introduces stealthy security threats. Since IRS elements do not emit detectable signals, malicious manipulations such as “disco-IRS” attacks can distort legitimate reflections or redirect traffic without being easily identified [24].

These threats evade conventional security monitoring and necessitate new defense paradigms. Proposed countermeasures include secure reconfiguration protocols, randomized reflection schemes like IRShield, and real-time anomaly detection for control-plane monitoring [25]. Additionally, the integration of IRS with sensing and localization may open up privacy threats where attackers can infer users’ movements or activities without active transmissions [26]. A secure IRS deployment model must incorporate authentication mechanisms, continuous auditing, and tamper detection capabilities.

2.3 Artificial Intelligence Integration

Artificial intelligence is probable to be a foundational layer of 6G architecture, enabling autonomous network optimization, real-time traffic prediction, and intelligent threat response [27, 28]. However, AI integration opens up a wide range of vulnerabilities, particularly in the training and inference stages. Attacks such as adversarial example injection, model poisoning, and data inference can severely compromise the integrity and confidentiality of AI models deployed across 6G environments.

Federated learning (FL), which allows decentralized AI training, mitigates some data-sharing risks but introduces new ones, including backdoor injection and gradient manipulation by malicious participants [29]. To enhance AI reliability, researchers advocate the use of explainable AI (XAI), adversarial robustness training, and secure model aggregation techniques [30]. Tree-based XAI-enhanced intrusion detection systems (IDS), utilizing tools like SHAP and LIME, have shown promise in improving transparency and robustness in AI-driven security frameworks [31].

2.4 Quantum Communication and Post-Quantum Cryptography

Quantum computing presents a serious threat to existing cryptographic standards, particularly those based on RSA and elliptic-curve cryptography. 6G must integrate quantum-resilient communication techniques to counteract this emerging risk [32]. While Quantum Key Distribution (QKD) offers a theoretically secure encryption mechanism, it is constrained by distance, environmental interference, and the vulnerability of trusted relay nodes [33]. These intermediaries are susceptible to denial-of-service and man-in-the-middle attacks.

Moreover, practical implementations of QKD have demonstrated hardware-level attacks such as detector blinding and photon-number splitting [34]. As a result, hybrid security architectures that combine QKD with post-quantum cryptography (PQC) are being developed to safeguard classical and quantum channels [35]. Lightweight PQC algorithms tailored for mobile and edge devices are particularly crucial, ensuring that cryptographic operations remain computationally feasible in resource-constrained environments [36].

2.5 Ubiquitous Sensing and Localization

6G's vision of smart environments is underpinned by pervasive sensing and high-resolution localization technologies. These capabilities enable innovations like digital twins, smart healthcare systems, and brain–computer interfaces (BCIs). However, the widespread collection of location, biometric, and behavioural data raises acute privacy concerns [37, 38].

Accurate localization can be exploited to infer user routines, social patterns, and health conditions, while bio signals from BCIs even when anonymized can be used to reconstruct individual identities or cognitive states [39]. Similarly, digital twins could become a target for behavioural profiling and remote surveillance if adequate protections are not enforced [40].

To counter these risks, privacy-by-design methodologies such as secure multi-party computation (SMPC), edge-based anonymization, and differential privacy (DP) must be embedded into system design [41, 42]. Federated learning plays a pivotal role in protecting user data by enabling collaborative AI training without sharing raw inputs. However, ensuring transparency, fairness, and informed consent in such architectures remains a significant interdisciplinary challenge [43, 44].

3. Security Challenges in 6G Networks

3.1 Attack Surface Expansion

With the proliferation of ultra-dense deployments, intelligent surfaces, UAV-assisted relays, and thousands of edge devices, the 6G network dramatically expands the attack surface [47, 48]. Each physical or logical component, such as edge nodes, RIS (Reconfigurable Intelligent Surfaces), and AI controllers, becomes a potential vulnerability vector. Unlike prior generations, where the core network bore the brunt of attack threats, 6G distributes intelligence and control to the edge and user planes—bringing critical decision-making closer to potentially unsecured endpoints.

The dynamic and programmable nature of 6G also means attackers can exploit reconfigurable network functions, APIs, and software-defined infrastructure. A single compromised node can act as a pivot to disrupt services across the control and data planes. Cross-layer attack propagation is a realistic threat due to tightly coupled interactions between AI models, physical links, and application services [49, 50].

3.2 Threats to AI-driven Control Systems

AI will underpin many control functions in 6G, including beam management, resource scheduling, mobility prediction, and anomaly detection. However, these AI models are vulnerable to a suite of attacks that exploit their statistical and opaque nature:

- **Adversarial Examples**: Minor perturbations to input data can mislead deep learning models. In the context of 6G, adversarial signals could manipulate intrusion detection systems or force incorrect spectrum allocation [51].
- **Poisoning Attacks**: In federated or online learning, malicious data inputs can degrade model performance or embed logic bombs, rendering AI controllers unreliable [52].
- **Model Inversion and Extraction**: Attackers can reconstruct training data or extract sensitive parameters of AI models, particularly those deployed on shared or edge resources.

The opacity of AI ("black-box" behaviour) makes it difficult to audit, debug, or validate decision outcomes in real-time, increasing the risk of undetected compromise. This makes Explainable AI (XAI) and trustworthy ML critical components of future 6G security strategies.

3.3 Security of Edge and Distributed Intelligence

In 6G, computation and intelligence migrate from centralized data centers to edge nodes—closer to end users and devices. While this improves latency and contextual awareness, it exposes the network to:

- **Device-level compromise**: Edge devices may lack tamper-resistant hardware, making them easier to exploit physically or remotely.

- **Insecure model updates**: In federated learning, global model updates aggregated from potentially untrusted edge nodes may introduce poisoned gradients or backdoors [52].
- **Lack of centralized oversight**: Without a centralized trust anchor, managing secure key distribution, trust establishment, and policy enforcement becomes highly challenging.

Techniques like Secure Enclaves, Blockchain-based Identity, and Zero Trust Architectures are being explored to embed resilience in decentralized intelligence systems [53].

3.4 Physical Layer Vulnerabilities

The shift to higher-frequency communications, including THz and mmWave bands, introduces unique security vulnerabilities not encountered in sub-6 GHz systems:

- **Beam Spoofing**: Attackers can imitate or manipulate directional beams to intercept or redirect communications.
- **Jamming**: THz signals, due to their narrow beams and susceptibility to blockage, are highly vulnerable to focused jamming attacks [46].
- **RIS Exploits**: Malicious access or physical tampering with intelligent surfaces could allow attackers to distort signal paths or redirect traffic for surveillance or disruption [50].

These vulnerabilities call for Physical Layer Security (PLS) techniques such as channel-aware key generation, artificial noise injection, and secure beamforming algorithms to be integrated into the PHY stack [50].

3.5 Privacy Leakage in Human-Centric Services

6G envisions human-centric services like holographic communication, digital twins, brain-computer interfaces (BCI), and ambient intelligence. These applications depend on real-time collection of deeply sensitive information:

- **Location and Biometric Data**: Continuous sensing and AI inference expose users to location tracking, gait analysis, emotional profiling, and identity inference.
- **BCI and Digital Twins**: These technologies may reveal neural activity patterns, behavioural preferences, or even subconscious responses, requiring unprecedented levels of privacy protection.
- **Cross-domain Data Aggregation**: With 6G supporting multi-service fusion (e.g., healthcare + navigation + social), correlating data across domains can enable powerful re-identification attacks, even on anonymized datasets.

To mitigate these risks, 6G must adopt Privacy by Design principles, integrating Differential Privacy, Federated Learning, and Decentralized Identifiers (DIDs) into service architectures [45].

3.6 Security of Quantum and Post-Quantum Systems

While Quantum Key Distribution (QKD) offers theoretically unbreakable encryption, its practical deployment is not free from vulnerabilities:

- **Detector Blinding and Photon Splitting**: Exploits in physical QKD hardware can be used to compromise key generation [45].
- **Relay Node Attacks**: Intermediate trusted nodes may become points of failure in quantum repeater chains, leading to denial-of-service or key exposure.

Simultaneously, the rise of quantum computing threatens RSA, ECC, and other widely used cryptosystems. Post-Quantum Cryptography (PQC) is being rapidly researched, but integrating these algorithms into resource-constrained edge and IoT environments poses significant computational and energy challenges [45].

3.7 Network Slicing and Isolation Risks

6G will implement fine-grained network slicing, where multiple virtual networks operate on shared physical infrastructure. This architecture introduces unique risks:

- **Cross-slice Contamination**: Improper slice isolation can allow attackers to leak or infer information from adjacent slices [54].
- **Slice Hijacking**: Misconfigurations or privilege escalation can enable unauthorized users to access sensitive or privileged slices.
- **Denial of Service (DoS)**: An attacker may overload a non-critical slice to induce cascading failures across shared resources [55].

Secure slicing demands hypervisor-level isolation, inter-slice monitoring, and dynamic access control mechanisms made directly into the 6G orchestration layer.

3.8 Evolving Attack Models and Zero-Day Exploits

The diversity and novelty of technologies used in 6G make traditional threat models obsolete. AI-generated malware, dynamic polymorphic attacks, and malicious synthetic agents in metaverse environments can all evade static defense mechanisms. Furthermore, zero-day vulnerabilities in AI models, ML pipelines, or cross-layer APIs are inevitable.

As threats evolve, **Proactive Cyber Resilience**—including autonomous threat hunting, AI-enabled remediation, and collaborative threat intelligence sharing—will be critical to maintaining robust 6G operations [56, 57].

4. Privacy Challenges in 6G Networks

Privacy preservation in 6G networks presents an unprecedented challenge due to the system's deeply immersive, intelligent, and hyper-connected nature. Unlike previous generations, where privacy concerns primarily revolved around user metadata or application-layer encryption, 6G introduces radically new vectors for privacy leakage—ranging from real-time biometric surveillance to inference attacks on AI decision-making. These threats are exacerbated by ubiquitous sensing, edge intelligence, cross-domain data aggregation, and tight human-machine symbiosis that characterize 6G environments [58, 59].

This section explores the key privacy challenges inherent in 6G networks, highlighting both technological risks and regulatory gaps, while discussing emerging countermeasures.

4.1 Human-Centric Data Exposure

One of the defining features of 6G is its human-centric design philosophy, where networks are not only user-aware but also contextually and emotionally responsive. Technologies such as Extended Reality (XR), Brain-Computer Interfaces (BCIs), digital twins, and holographic communication necessitate the continuous collection and processing of highly sensitive data—such as brain signals, facial expressions, speech tone, emotional states, gestures, and even subconscious reactions [60, 62].

Such intimate data, if leaked or misused, can lead to irreversible harm such as psychological profiling, behavioural manipulation, or biometric identity theft. Existing privacy protections (e.g., consent forms or user agreements) are inadequate for such high-resolution, real-time, non-verbal data collection. Furthermore, many of these data types are non-revocable—unlike passwords, a person's gait or neural signature cannot be changed once compromised.

4.2 Federated Learning and Data Inference Risks

6G will rely heavily on federated learning (FL) to support edge AI while preserving data locality. However, FL introduces unique privacy risks even when raw data remains on the device. Attackers can:

- Infer private attributes from model updates (e.g., user's gender, age, or location) using gradient leakage attacks [63].
- Launch membership inference attacks, determining whether a specific data point was used during training.
- Use property inference attacks to deduce underlying characteristics of training datasets.

Although differential privacy and secure aggregation can mitigate some risks, they often reduce model accuracy or increase system complexity, which creates tension between performance and privacy [64].

4.3 Lack of Transparency and Explainability in AI

AI systems deployed in 6G environments will make real-time decisions affecting everything from resource allocation to user behaviour analysis. These models often operate as "black boxes," making decisions that are difficult to interpret or contest. As a result, users may not know:

- What data is being collected.
- How it is being used or shared.
- Whether decisions made about them (e.g., QoS assignment, threat detection, access prioritization) are biased or erroneous.

This opacity raises serious algorithmic accountability and transparency issues, especially under regulations like the General Data Protection Regulation (GDPR), which mandates a "right to explanation" for automated decisions [58, 65]. In response, Explainable AI (XAI) techniques such as LIME and SHAP are being incorporated into privacy frameworks to provide post-hoc interpretability, though their scalability and reliability in real-time 6G settings remain under debate [66].

4.4 Cross-Domain Data Aggregation and Linkage Attacks

The 6G architecture is expected to support seamless integration across domains—healthcare, finance, smart cities, education, and entertainment—through converged services. However, this integration facilitates data linkage attacks, where even anonymized datasets from one domain can be cross-referenced with others to re-identify users [61].

For example, combining movement data from a smart transportation slice with behavioural data from a healthcare slice may reveal the identity and habits of a specific individual. These risks are intensified when data is processed by third-party AI providers or stored across geographically distributed cloud-edge nodes with varying jurisdictional protections [62].

4.5 Weak Identity and Consent Mechanisms

Current identity management systems, such as username-password pairs or device tokens, are insufficient for privacy-preserving authentication in a hyper-dense, mobile 6G network. The challenge intensifies with:

- Ephemeral interactions (e.g., drone-to-drone or vehicle-to-network communication).
- Context-aware services that require continuous background data capture.
- Delegated devices (e.g., wearables, smart implants) transmitting personal information without explicit user initiation.

Moreover, traditional consent models break down in such environments. Asking users to "opt-in" for every data interaction is impractical; yet omitting consent introduces legal and ethical violations. Emerging approaches such as Self-Sovereign Identity (SSI) and Decentralized Identifiers (DIDs) aim to return control to users, allowing cryptographically verifiable, revocable, and fine-grained control over personal data [67].

4.6 Challenges in Enforcing Regulatory Compliance

With 6G's global reach and distributed intelligence, enforcing compliance with regulations like GDPR, CCPA, or upcoming AI Acts becomes exceedingly difficult. Specific challenges include:

- **Data residency**: Edge nodes may temporarily cache or process personal data outside the user's jurisdiction.
- **Algorithmic auditing**: AI models may evolve continuously, making post-deployment audits difficult or obsolete.
- **Legal fragmentation**: Differing regional definitions of "personal data," "consent," and "profiling" hinder uniform privacy enforcement in global 6G deployments [58].

To address these, 6G architecture must natively incorporate privacy governance frameworks, including embedded auditing hooks, regulatory tagging of data, and AI compliance checkers [59].

4.7 Privacy in Collaborative and Ambient Intelligence

Ambient intelligence systems in 6G are designed to perceive, learn, and adapt to users silently in the background. This introduces "invisible surveillance" risks, where users may be unaware of being monitored. Additionally, collaborative AI models (e.g., in swarm robotics or vehicular platoons) often share local observations for joint decision-making, creating challenges in:

- Ensuring that shared insights do not violate individual privacy.
- Preventing information leakage across collaborative agents.
- Managing consent in multi-user settings, such as public spaces or smart classrooms.

Mitigation strategies include context-aware privacy policies, multi-party privacy-preserving computation, and location-sensitive data tagging for collaborative settings [59].

4.8 Evolving Privacy Threats from Synthetic Media and Digital Twins

As digital replicas and metaverse experiences become common in 6G, privacy threats extend to the synthetic self. Unauthorized cloning of avatars, imitation of user behaviour, or reconstruction of voice and gestures from leaked data could facilitate:

- Identity theft in immersive environments.
- Behavioural mimicry attacks to bypass authentication systems.
- Reputation damage by creating fake but convincing user actions or communications [60].

Protecting the integrity of synthetic identities, along with watermarking and authentication of user-generated content, will be crucial in defending against these emerging threats.

5. Mitigation Strategies and Future Directions

To effectively mitigate the rising spectrum of threats in 6G networks, a comprehensive, multi-layered security architecture is indispensable. At the forefront are AI-driven intrusion detection systems (IDS) that leverage machine learning to detect anomalous behaviours in real-time, even in highly dynamic and heterogeneous environments [68]. Given the anticipated rise of quantum computing, lightweight post-quantum cryptography (PQC) is being researched to ensure cryptographic resilience without overburdening resource-constrained devices [69]. Simultaneously, blockchain-based trust management frameworks offer decentralized and tamper-resistant mechanisms for authentication, identity management, and transaction validation in multi-party 6G ecosystems [70]. These are particularly critical in scenarios involving device-to-device (D2D) and edge-cloud interactions [71].

To protect sensitive data during processing and training phases, privacy-preserving computation techniques such as secure multi-party computation (SMPC), homomorphic encryption, and trusted execution environments (TEE) are being integrated into the 6G stack [72]. Moreover, context-aware access control systems are being discovered to dynamically adapt security policies based on user roles, locations, and threat levels [73]. Despite these technical advancements, there is growing consensus that regulatory and policy frameworks must evolve in parallel to address the decentralized, borderless, and data-intensive nature of 6G [74]. International collaboration will be critical in defining standardized security protocols and privacy benchmarks, ensuring interoperability while maintaining sovereignty and compliance [75].

6. Conclusion

The beginning of 6G marks a radical transformation in wireless communication, driven by AI-native architectures, terahertz (THz) communications, and intelligent, decentralized edge-cloud ecosystems. While the potential benefits are enormous—ranging from immersive XR experiences to autonomous systems and holographic communications—these capabilities simultaneously expose the network to an unprecedented spectrum of security threats and privacy risks.

Throughout this review, we explored the multifaceted vulnerabilities that permeate the 6G stack across the physical, network, and application layers. From beamforming attacks on THz links to adversarial threats targeting AI-driven control systems and the privacy implications of ubiquitous sensing, it is evident that conventional security models are insufficient for the hyper-connected, dynamic, and intelligent landscape of 6G.

To counteract these challenges, research has proposed a variety of layered defense strategies. These include AI-powered intrusion detection systems, lightweight post-quantum cryptographic protocols, blockchain-enabled trust management, and privacy-preserving computation through homomorphic encryption and secure multi-party computation. Additionally, context-aware access control, explainable AI (XAI) models, and zero-trust frameworks are being integrated into the 6G design stack to enhance robustness, transparency, and trustworthiness.

However, technical solutions alone are not enough. The decentralized and global nature of 6G demands coordinated efforts in regulatory alignment, standardization, and policy formulation. Cross-border collaboration is essential to ensure interoperability, data sovereignty, and ethical AI deployment across heterogeneous and geopolitically diverse environments.

Looking ahead, there is a clear need for security and privacy to be embedded by design- not as an afterthought in 6G networks. This will require a convergence of multiple research domains, including AI security, quantum-safe cryptography, secure hardware design, and human-centric privacy engineering. Only through such multidisciplinary collaboration can we ensure that 6G not only delivers on its promise of hyper-connectivity and intelligence but does so in a secure, resilient, and privacy-respecting manner.

Data availability statement

All data that support the findings of this study are included within the article (and any supplementary files).

Competing interests

All authors have no conflicts of interest to declare that are relevant to the content of this article.

Funding details

The authors did not receive support from any organization for the submitted work.

References

[1] Zhang, Z., Xiao, Y., Ma, Z., Xiao, M., Ding, Z., Lei, X., Karagiannidis, G. K., & Fan, P. (2019). 6G Wireless Networks: Vision, Requirements, Architecture, and Key Technologies. IEEE Vehicular Technology Magazine, 14(3), 28–41. https://doi.org/10.1109/MVT.2019.2921208

[2] Saad, W., Bennis, M., & Chen, M. (2020). A Vision of 6G Wireless Systems: Applications, Trends, Technologies, and Open Research Problems. IEEE Network, 34(3), 134–142. https://doi.org/10.1109/MNET.001.1900287

[3] You, X., Wang, C. X., Huang, J., Gao, C., Zhang, Z., Wang, M., Huang, Y., Zhang, Y., & Tan, Y. (2021). Towards 6G wireless communication networks: Vision, enabling technologies, and new paradigm shifts. Science China Information Sciences, 64(1), 1–74. https://doi.org/10.1007/s11432-020-2955-6

[4] Dang, S., Amin, O., Shihada, B., & Alouini, M.-S. (2020). What Should 6G Be? Nature Electronics, 3(1), 20–29. https://doi.org/10.1038/s41928-019-0355-6

[5] Chen, S., & Zhao, J. (2020). The Requirements, Challenges, and Technologies for 6G Mobile Wireless Networks. IEEE Communications Magazine, 58(3), 36–42. https://doi.org/10.1109/MCOM.001.1900413

[6] Jiang, W., Han, B., & Schotten, H. D. (2021). Artificial Intelligence for Wireless Networks: A Tutorial on Neural Networks. IEEE Communications Surveys & Tutorials, 23(2), 1224–1244. https://doi.org/10.1109/COMST.2020.3048805

[7] Alsabah, M., Alazab, M., Awad, A. I., & Baker, T. (2021). Anomaly Detection Framework for Internet of Things Networks: A Machine Learning Approach. Journal of Parallel and Distributed Computing, 159, 13–24. https://doi.org/10.1016/j.jpdc.2021.09.005

[8] Liu, X., Wang, T., & Xu, Y. (2021). Secure and Efficient Device Authentication in 6G Networks. IEEE Transactions on Network and Service Management, 18(3), 3147–3159. https://doi.org/10.1109/TNSM.2021.3082847

[9] Sarieddeen, H., Alouini, M.-S., & Dawy, Z. (2020). Terahertz-Band Ultra-Massive Spatial Modulation MIMO. IEEE Journal on Selected Areas in Communications, 39(6), 1532–1545. https://doi.org/10.1109/JSAC.2020.3018816

[10] Rappaport, T. S., Xing, Y., Kanhere, O., Ju, S., Murdock, J. N., Wang, E., & Sun, H. (2019). Wireless Communications and Applications Above 100 GHz: Opportunities and Challenges for 6G and Beyond. IEEE Access, 7, 78729–78757. https://doi.org/10.1109/ACCESS.2019.2921522

[11] Aledhari, M., Razzak, R., Parizi, R. M., & Srivastava, G. (2020). Federated Learning: A Survey on Enabling Technologies, Protocols, and Applications. IEEE Access, 8, 140699–140725. https://doi.org/10.1109/ACCESS.2020.3013541

[12] Adadi, A., & Berrada, M. (2018). Peeking Inside the Black-Box: A Survey on Explainable Artificial Intelligence (XAI). IEEE Access, 6, 52138–52160. https://doi.org/10.1109/ACCESS.2018.2870052

[13] Tjoa, E., & Guan, C. (2020). A Survey on Explainable Artificial Intelligence (XAI): Toward Medical XAI. IEEE Transactions on Neural Networks and Learning Systems, 32(11), 4793–4813. https://doi.org/10.1109/TNNLS.2020.3027314

[14] Sharma, P. K., & Park, J. H. (2018). Blockchain Based Hybrid Network Architecture for the Smart City. Future Generation Computer Systems, 86, 650–655. https://doi.org/10.1016/j.future.2018.03.066

[15] Zwickl, P., & Hölbl, M. (2021). Data Sovereignty and GDPR Challenges in 6G-Driven Environments. Computer Law & Security Review, 41, 105542. https://doi.org/10.1016/j.clsr.2021.105542

[16] Chen, S., Li, X., Zhang, Y., & Han, T. X. (2023). “Terahertz Communications for 6G: Prospects and Challenges.” *IEEE Network*, 37(2), 12–18. https://doi.org/10.1109/MNET.123456

[17] Han, C., I, C., & Akyildiz, I. F. (2023). “Propagation and Channel Modeling for Terahertz Wireless Communications.” *IEEE Transactions on Wireless Communications*, 22(1), 1–14.

[18] Koenig, S., Lopez-Diaz, D., Antes, J., et al. (2023). “Wireless Sub-THz Communications for 6G: Opportunities and Threats.” *Nature Electronics*, 6, 112–118.

[19] Alsabah, M., Alenezi, F., & Hassan, N. U. (2024). “Security Threats in Terahertz Communication: A Survey.” *IEEE Access*, 12, 55678–55699.

[20] Wu, Q., & Zhang, R. (2020). “Towards Smart and Reconfigurable Environment: Intelligent Reflecting Surface Aided Wireless Network.” *IEEE Communications Magazine*, 58(1), 106–112.

[21] Basar, E., Renzo, M. D., Rosny, J., et al. (2023). “Reconfigurable Intelligent Surfaces: A Signal Processing Perspective with Wireless Applications.” *IEEE Signal Processing Magazine*, 40(3), 70–88.

[22] Zeng, Y., Zhang, R., & Lim, T. J. (2023). “Wireless Communications With Reconfigurable Intelligent Surface: Path Loss Modeling and Estimation.” *IEEE Wireless Communications Letters*, 10(1), 27–31.

[23] Tang, W., Chen, M. Z., Zhao, J., et al. (2022). “Wireless Communications With Reconfigurable Intelligent Surface: Path Loss Modeling and Analysis.” *IEEE Transactions on Wireless Communications*, 21(12), 10340–10353.

[24] Chen, L., & Zhou, L. (2024). “IRShield: Randomized Beamforming Against IRS-based Spoofing Attacks.” *IEEE Transactions on Information Forensics and Security*, 19, 1234–1246.

[25] Luo, S., Chen, Y., & Zhao, Q. (2023). “Security in IRS-Aided 6G Networks: Threat Models and Mitigation Strategies.” *IEEE Internet of Things Journal*, 10(7), 5544–5556.

[26] Yang, J., Zhang, Y., & Li, X. (2023). "Privacy Implications of Integrated Sensing and Communication in 6G." *Computer Networks*, 224, 109473.

[27] Shlezinger, N., Eldar, Y. C., & Alexandropoulos, G. C. (2022). "Deep Learning for Wireless Communications: Opportunities and Challenges in 6G." *IEEE Signal Processing Magazine*, 39(1), 21–31.

[28] Alsheikh, M. A., Lin, S., Niyato, D., et al. (2023). "Edge Intelligence for 6G: Security and Privacy Challenges." *IEEE Network*, 37(4), 92–98.

[29] Zhao, Y., Ma, X., & Zhang, H. (2024). "Security Risks in Federated Learning for 6G: A Comprehensive Survey." *IEEE Communications Surveys & Tutorials*, 26(1), 89–113.

[30] Rieger, A., & Tutschku, K. (2023). "Explainable AI in 6G Security: Towards Transparent Anomaly Detection." *Journal of Network and Computer Applications*, 206, 103579.

[31] Vyas, V., Rathore, M., & Tripathi, R. (2023). "XAI-Enabled Intrusion Detection Systems in IoT for 6G Networks." *IEEE Access*, 11, 9967–9979.

[32] Kumar, P., & Banerjee, S. (2023). "Quantum Communication in 6G: Opportunities and Challenges." *IEEE Transactions on Quantum Engineering*, 4, 310–324.

[33] Yuan, X., Zhang, Z., & Li, H. (2022). "Quantum Key Distribution and Secure Communication in 6G." *IEEE Transactions on Information Forensics and Security*, 17, 4182–4194.

[34] Lütkenhaus, N., & Braunstein, S. L. (2023). "Security Loopholes in Practical QKD Implementations." *Nature Photonics*, 17(1), 18–24.

[35] Bindra, R., Choudhary, P., & Singh, M. (2024). "Hybrid Post-Quantum Cryptography Frameworks for 6G Networks." *Future Generation Computer Systems*, 154, 812–827.

[36] Azad, M., & Ullah, N. (2023). "Lightweight PQC Algorithms for Edge and IoT Devices in 6G." *Ad Hoc Networks*, 144, 103623.

[37] Zafari, F., Papapanagiotou, I., & Christidis, K. (2022). "Localization for Smart 6G Environments: Techniques and Challenges." *IEEE Communications Surveys & Tutorials*, 24(2), 901–929.

[38] Kim, H., & Lee, S. (2023). "Ubiquitous Sensing in 6G for Smart Healthcare and Digital Twins." *IEEE Internet of Things Journal*, 10(5), 4021–4032.

[39] Li, M., & Li, H. (2023). "Location Privacy in Next-Gen Wireless Networks: A 6G Perspective." *IEEE Transactions on Mobile Computing*, 22(4), 1591–1605.

[40] Ahmad, I., Yousafzai, A., & Zhang, Z. (2024). "Privacy Risks in Brain-Computer Interfaces for 6G." *ACM Computing Surveys*, 56(1), 1–34.

[41] Duan, Y., & Hu, J. (2023). "Digital Twins in 6G Networks: Privacy and Security Challenges." *IEEE Transactions on Industrial Informatics*, 19(2), 1678–1689.

[42] Tang, J., Ni, J., & Lin, X. (2023). "Differential Privacy in 6G-Enabled Smart Environments." *IEEE Transactions on Dependable and Secure Computing*, 20(3), 1425–1439.

[43] Raza, S., Wang, J., & Li, X. (2023). "Secure Multi-party Computation for Federated Learning in 6G." *IEEE Access*, 11, 32445–32459.

[44] Huang, H., Zhang, Q., & Li, F. (2023). "Federated Learning for Privacy Preservation in 6G Networks: A Legal and Technical Review." *Computer Law & Security Review*, 51, 105731.

[45] Zhang, Wei, Long Chen, and Bo Liu. "Privacy-Preserving Federated Learning for 6G Edge Intelligence: Threats and Solutions." *IEEE Network*, vol. 36, no. 3, 2022, pp. 115–121. https://doi.org/10.1109/MNET.011.2100331.

[46] Liu, Jinchuan, and H. Zhao. "Secure and Efficient Patient Data Transmission over THz Links with Blockchain for Auditability." *IEEE Transactions on Industrial Informatics*, vol. 18, no. 11, 2022, pp. 7742–7751. https://doi.org/10.1109/TII.2022.3149210.

[47] Alwis, Chandima N. K., et al. "Survey on 6G Frontiers: Trends, Applications, Requirements, Technologies, Challenges, and Future Research." *IEEE Open Journal of the Communications Society*, vol. 2, 2021, pp. 836–886. https://doi.org/10.1109/OJCOMS.2021.3071659.

[48] Viswanathan, Harish, and Sundar Subramanian. "6G: Vision, Requirements, Architecture and Key Technologies." *Bell Labs Technical Journal*, vol. 25, no. 2, 2020, pp. 1–15. https://doi.org/10.1002/bltj.12337.

[49] Tang, Jian, and Yingying Chen. "Cross-Layer Security Threats in AI-Driven 6G Networks: Challenges and Research Opportunities." *IEEE Wireless Communications*, vol. 30, no. 2, 2023, pp. 100–107. https://doi.org/10.1109/MWC.001.2200152.

[50] Shlezinger, Nir, et al. "Dynamic Reconfigurable Intelligent Surfaces for 6G: Challenges and Opportunities." *IEEE Journal on Selected Areas in Communications*, vol. 41, no. 3, 2023, pp. 763–778. https://doi.org/10.1109/JSAC.2023.3245716.

[51] Li, Jiahui, and Bo Wang. "Adversarial Machine Learning in Wireless Communications: Threats and Defenses in 6G Era." *IEEE Communications Surveys & Tutorials*, vol. 25, no. 1, 2023, pp. 78–104. https://doi.org/10.1109/COMST.2023.3249120.

[52] Xie, Can, et al. "Generalized Federated Learning with Poisoning Attacks in Edge-Enabled 6G." *IEEE Transactions on Mobile Computing*, 2022. https://doi.org/10.1109/TMC.2022.3171346.

[53] Sun, Xuefeng, et al. "Blockchain-Empowered Secure Federated Learning for Intelligent 6G Edge." *IEEE Transactions on Industrial Informatics*, vol. 19, no. 2, 2023, pp. 1362–1372. https://doi.org/10.1109/TII.2022.3154887.

[54] Parvez, Imran, et al. "Network Slicing for 6G: Opportunities and Challenges." *IEEE Network*, vol. 35, no. 2, 2021, pp. 147–155. https://doi.org/10.1109/MNET.011.2000440.

[55] Taleb, Tarik, et al. "6G Network Slicing: Secure, Dynamic, and Resilient Isolation of Slices in Multi-Tenant Networks." *IEEE Communications Standards Magazine*, vol. 7, no. 3, 2023, pp. 68–75. https://doi.org/10.1109/MCOMSTD.0001.2300020.

[56] Akyildiz, Ian F., and Chong Han. "Evolution Beyond 5G: Towards 6G with Intelligent Reflecting Surfaces and AI." *Computer Networks*, vol. 198, 2021, 108329. https://doi.org/10.1016/j.comnet.2021.108329.

[57] Zhao, Ming, et al. "AI-Native Proactive Cyber Defense for 6G Networks: A Resilience-Driven Approach." *IEEE Transactions on Network and Service Management*, vol. 19, no. 4, 2022, pp. 567–581. https://doi.org/10.1109/TNSM.2022.3204600.

[58] Razaque, Abdul, and Khaled Elleithy. "Privacy Preservation for Smart Healthcare: Survey of Data Privacy Techniques." *Healthcare* 11, no. 3 (2023): 383. https://doi.org/10.3390/healthcare11030383.

[59] Hitaj, Briland, Giuseppe Ateniese, and Fernando Perez-Cruz. "Deep Models Under the GAN: Information Leakage from Collaborative Deep Learning." In *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, 603–618. ACM, 2017. https://doi.org/10.1145/3133956.3134012.

[60] Nasr, Milad, Reza Shokri, and Amir Houmansadr. "Comprehensive Privacy Analysis of Deep Learning: Passive and Active White-box Inference Attacks against Centralized and Federated Learning." In *IEEE Symposium on Security and Privacy (SP)*, 739–753. IEEE, 2019. https://doi.org/10.1109/SP.2019.00065.

[61] Abadi, Martín, et al. "Deep Learning with Differential Privacy." In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, 308–318. ACM, 2016. https://doi.org/10.1145/2976749.2978318.

[62] Goodman, Bryce. "A Step Towards Accountable Algorithms? Algorithmic Discrimination and the European Union General Data Protection." In *Proceedings of the 29th International Conference on Legal Knowledge and Information Systems*, 3–12. IOS Press, 2016.

[63]. Narayanan, Arvind, and Vitaly Shmatikov. "Robust De-anonymization of Large Sparse Datasets." In *IEEE Symposium on Security and Privacy (SP)*, 111–125. IEEE, 2008. https://doi.org/10.1109/SP.2008.33.

[64] Cameron, Fergal. "Challenges for GDPR Compliance in the Era of Edge Computing and 6G." *Computer Law & Security Review* 49 (2023): 105805. https://doi.org/10.1016/j.clsr.2023.105805.

[65] Rikken, Maurits, Niels den Hartog, and Rianne Dekker. "Digital Twins and the New Frontiers of Privacy." *Technology in Society* 72 (2023): 102202. https://doi.org/10.1016/j.techsoc.2022.102202.

[66] Zwitter, Andrej, and Oskar J. Gstrein. "Big Data, Privacy and COVID-19 – Learning from Humanitarian Expertise in Data Protection." *International Journal of Human Rights* 24, no. 8 (2020): 1321–1338. https://doi.org/10.1080/13642987.2020.1787274.

[67] Sengupta, Saurabh, Debasis Samanta, and Sushmita Ruj. "Digital Avatars in 6G: Identity, Privacy, and Ethical Considerations." *IEEE Network* 37, no. 1 (2023): 207–213. https://doi.org/10.1109/MNET.121.2200191.

[68] Zhang, Yong, et al. "Artificial Intelligence-Enabled Intrusion Detection for 6G Networks: A Survey." *IEEE Internet of Things Journal* 10, no. 6 (2023): 5023–5040. https://doi.org/10.1109/JIOT.2023.3247109.

[69] Chen, Li, et al. "Lightweight Post-Quantum Cryptographic Algorithms for Resource-Constrained Devices in 6G Environments." *IEEE Transactions on Information Forensics and Security* 18 (2023): 2271–2285. https://doi.org/10.1109/TIFS.2023.3283654.

[70] Wang, Jun, et al. "Blockchain-Based Trust Management in 6G: Challenges, Advances, and Future Directions." *IEEE Network* 36, no. 4 (2022): 113–120. https://doi.org/10.1109/MNET.001.2100452.

[71] Elgendy, Islam A., et al. "Decentralized Identity and Trust Models for Edge-to-Edge 6G Communication." *Computer Networks* 226 (2023): 109690. https://doi.org/10.1016/j.comnet.2022.109690.

[72] Zhang, Qi, et al. "Privacy-Preserving Machine Learning for 6G: Federated Learning and Beyond." *IEEE Wireless Communications* 30, no. 2 (2023): 24–31. https://doi.org/10.1109/MWC.2023.1000101.

[73] Hu, Xiaoyang, et al. "Context-Aware Access Control in 6G Networks: Architecture, Challenges, and Opportunities." *IEEE Communications Surveys & Tutorials* 25, no. 1 (2023): 150–175. https://doi.org/10.1109/COMST.2022.3220918.

[74] Ahmed, Noman, et al. "Regulatory and Policy Considerations for Securing 6G Networks." *Telecommunications Policy* 47, no. 1 (2023): 102456. https://doi.org/10.1016/j.telpol.2022.102456.

[75] Badran, Shady, et al. "Global Collaboration for 6G Security Standardization: Towards Unified Privacy and Trust Frameworks." *IEEE Access* 11 (2023): 54678–54693. https://doi.org/10.1109/ACCESS.2023.3276500.