applied sciences

MDPI

Article

Personal vs. Non-Personal Data Privacy in 6G Networks: Mechanisms, Compliance, and Architectural Patterns

Maryam Almarwani * and Reem Almarwani

Department of Cybersecurity, College of Computer Science and Engineering, Taibah University, Madina 42453, Saudi Arabia; rmarwani@taibahu.edu.sa
* Correspondence: mmmarwani@taibahu.edu.sa

Abstract

Sixth-generation (6G) networks are expected to provide ubiquitous connectivity, AI-native orchestration, and seamless integration across terrestrial and non-terrestrial infrastructures. However, these capabilities introduce new privacy challenges related to the classification and protection of personal, quasi-personal, and non-personal data in complex data-driven environments. This paper presents a systematic review of 78 peer-reviewed studies published between 2019 and 2025. Following a PRISMA-based methodology, this review analyzes privacy-enhancing technologies (PETs), regulatory compliance frameworks, and architectural patterns for privacy preservation in 6G networks. The findings show that differential privacy (DP) and federated learning (FL) dominate current research, accounting for nearly 52% of the reviewed studies. Blockchain auditing and zero-knowledge proofs (ZKPs) collectively represent approximately 30%, while the remaining mechanisms, including physical-layer security (PLS), trusted execution environments (TEEs), homomorphic encryption (HE), secure multi-party computation (SMPC), and anonymization, account for roughly 18%. These mechanisms exhibit varying levels of privacy strength, utility preservation, latency, and energy cost. At the same time, evolving regulatory frameworks, including GDPR, PDPL, CCPA/CPRA, LGPD, and PIPL, increasingly extend privacy obligations to quasi-personal and aggregated data. Building on these findings, this paper proposes a unified taxonomy that clarifies the boundary between personal and non-personal data. It also provides a cross-layer mapping between PETs and compliance requirements across the Core/SBA, RAN, Edge/MEC, and NTN layers. Finally, this paper presents a forward-looking roadmap for 2025–2030, highlighting hybrid PET pipelines, post-quantum auditability, and AI-driven compliance automation as key directions for privacy-preserving 6G standardization.

Keywords: 6G networks; data privacy; privacy-enhancing technologies; personal data; non-personal data; federated learning; differential privacy; edge computing; compliance frameworks; blockchain auditing

Check for updates

Academic Editor: Paolo Renna

Received: 4 April 2026
Revised: 27 April 2026
Accepted: 30 April 2026
Published: 7 May 2026

Copyright: © 2026 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license.

1. Introduction

Sixth-generation (6G) networks enable ubiquitous connectivity, AI-driven automation, and immersive services such as digital twins, holographic communication, and safety-critical cyber-physical systems. However, these capabilities introduce a fundamental privacy challenge: protecting *personal data* (e.g., identity, health, and behavioral information) while managing *non-personal data* (e.g., telemetry, aggregated analytics, and network logs)

that can still enable re-identification when combined with auxiliary datasets. Earlier network generations focused mainly on personal data protection. In contrast, 6G architectures are highly data-driven and span multiple domains, blurring the boundary between personal and non-personal data. As a result, distinguishing between these data types becomes both technically complex and legally critical [1–4]. These blurred boundaries are further amplified by emerging paradigms such as quantum-secure networking, compliance-aware orchestration, and blockchain-based auditability. These paradigms create new opportunities. However, they also introduce additional regulatory complexities [5–10]. Beyond general frameworks, several concrete mechanisms have recently appeared:

- **Zero-trust O-RAN access control** via *TrustORAN*: Smart-contract-based onboarding and least-privilege tokens for verifiable RAN control [5].
- **Lightweight decentralized AIoT orchestration** using *SCOPE*: energy-aware analytics for constrained devices with auditable orchestration metadata [6].
- **Privacy-preserving inter-slice communication**: Zero-knowledge proofs (ZKPs) for minimal-disclosure verification across administrative domains [10].
- **Quantum-secure blockchain with STARK-like attestations**: Post-quantum auditability without raw data leakage [9].

In parallel, **edge computing and large language models (LLMs) offloading** have become privacy-critical domains in 6G. For example, Badidi et al. propose *privacy-preserving vehicular LLM offloading* with adaptive PETs [11]. These techniques mitigate leakage risks identified in recent analyses of federated LLMs [12] and align with collaborative edge–cloud solutions that protect both model integrity and user data during distributed inference [13,14]. Together, they demonstrate how 6G's AI-native vision creates new classes of sensitive "model–data flows", where PETs and compliance tools must operate jointly. Existing surveys and white papers recognize privacy as a fundamental design requirement in 6G systems [15–17]. However, most of these studies do not explicitly connect the distinction between personal and non-personal data with operational compliance and orchestration mechanisms.

Recent work has started to address this limitation. For example, Shen et al. proposed privacy models tailored for AI-native architectures [18], while Zhou et al. examined cross-domain privacy risks in satellite-enabled 6G environments [19]. Kumar et al. analyzed reconfigurable intelligent surface (RIS)/terahertz (THz) communications as both privacy enablers and potential risk sources [20].

Other works focus on enforcement and verification mechanisms. Chen et al. explored the use of zero-knowledge proofs (ZKPs) for multi-domain verification [21], whereas Zhang et al. and Kashif et al. investigated blockchain-based auditing and adaptive differential privacy-preserving techniques for privacy-preserving orchestration [22,23]. Complementary studies provide user-centric and edge-focused perspectives, highlighting that privacy risks and protections in 6G depend on data type, architectural placement, and compliance context [24,25]. This study provides a structured synthesis of **78 peer-reviewed works** and introduces a unified cross-layer taxonomy linking privacy-enhancing technologies with regulatory compliance across 6G systems.

The main contributions of this paper are summarized as follows:

- **Systematic synthesis:** We provide a PRISMA-based analysis of 78 peer-reviewed studies, ensuring methodological consistency and reproducibility across diverse 6G privacy research directions.
- **Cross-layer taxonomy:** We develop a unified taxonomy that explicitly distinguishes between personal and non-personal data, linking privacy-enhancing technologies (PETs) to compliance requirements across Core/SBA, RAN, Edge/MEC, and NTN layers.

- **Threat-mitigation mapping:** We present a structured mapping between multi-layer threat models and corresponding privacy-preserving mechanisms, enabling clearer alignment between attack surfaces and deployed PETs.
- **Cross-layer integration insight:** We analyze the complementary roles of physical-layer security (PLS) and higher-layer techniques (DP and FL), highlighting their trade-offs and the need for hybrid privacy-preserving architectures.
- **Forward-looking roadmap:** We identify key research gaps and outline future directions, including hybrid PET pipelines, AI-driven privacy orchestration, and post-quantum compliance mechanisms.

These contributions directly address the research questions (RQ1–RQ3) by linking privacy mechanisms, compliance frameworks, and emerging challenges in 6G systems.

- **RQ1:** What are the dominant privacy-enhancing mechanisms (cryptographic, differential privacy, federated learning, LLM offloading, anonymization, physical-layer security, etc.) applicable to personal and non-personal data in 6G networks?
- **RQ2:** How do regulatory and compliance frameworks (GDPR, PDPL, 3GPP SA3, ISO/IEC standards) influence privacy enforcement and accountability across 6G architectural layers?
- **RQ3:** What are the open research gaps, challenges, and future directions for achieving scalable, compliant, and privacy-preserving 6G architectures?

The rest of this paper is organized as follows: Section 2 describes the study selection and PRISMA-based methodology. Section 3 provides the background and contextual framework for 6G privacy. Section 4 then presents the taxonomy of privacy-enhancing mechanisms and compliance hooks across 6G layers. Section 5 outlines the threat models and attack taxonomy. Section 6 provides the comparative analysis of PETs. Section 7 evaluates readiness and data governance maturity. Section 8 discusses challenges and future research trends. Finally, Section 9 concludes the paper and discusses future research directions.

2. Study Selection and Methodology

To address the identified research gaps and ensure reproducibility, this section describes the systematic study selection and review methodology adopted in this study, including data sources, screening criteria, and synthesis procedures aligned with PRISMA guidelines.

2.1. Search Strategy and Sources

The review adopts a PRISMA-based methodology to ensure transparency, traceability, and reproducibility. The initial corpus was collected from four major digital libraries: **IEEE Xplore**, **ACM Digital Library**, **Elsevier/ScienceDirect**, and **SpringerLink**, covering the period 2019–2025.

These sources were selected because they represent the primary venues for high-quality research in networking, cybersecurity, and distributed systems. IEEE and ACM provide strong technical coverage, Elsevier supports multidisciplinary research, and SpringerLink includes standardization-oriented and protocol-focused studies. This selection supports technical depth and coverage of compliance and architectural aspects.

The search queries combined privacy-, compliance-, and orchestration-related keywords to capture cross-layer developments such as privacy-preserving LLM offloading, blockchain auditability, and IoT authentication. The representative Boolean patterns were the following:

- (“6G” OR “beyond-5G”) AND (privacy OR “personal data” OR “non-personal data”).
- (“federated learning (FL)” OR FL OR “split learning”) AND (“differential privacy (DP)” OR DP).

- (blockchain OR "distributed ledger technology (DLT)" OR DLT) AND (audit* OR compliance OR accountability).
- ("edge computing" OR "multi-access edge computing (MEC)") AND ("large language model (LLM)" OR LLM OR prompt* OR offload*).
- ("zero-knowledge proof (ZKP)" OR ZKP) AND (audit* OR attest* OR compliance).
- ("Internet of Things (IoT)" OR IoT OR "vehicular") AND (authentication OR authorization OR access control).
- ("physical layer security (PLS)" OR PLS OR "wiretap channel") AND ("6G" OR "beyond-5G").
- ("low signal-to-noise ratio (SNR)" OR "imperfect channel state information (CSI)" OR "channel estimation") AND ("secrecy" OR "physical layer security").
- ("extremely large multiple-input multiple-output (XL-MIMO)" OR "massive MIMO" OR "beamforming" OR "artificial noise") AND ("privacy" OR "secrecy").
- ("reconfigurable intelligent surface (RIS)" OR RIS OR "terahertz (THz)" OR THz) AND ("security" OR "eavesdropping" OR "physical layer security" OR privacy).
- ("over-the-air federated learning (OTA-FL)" OR OTA-FL) AND ("privacy" OR "differential privacy" OR "physical layer").
- ("non-terrestrial network (NTN)" OR NTN OR "satellite") AND ("security" OR "physical layer security").
- ("semantic communication" OR "semantic-aware communication") AND (privacy OR security OR data protection).
- ("space-air-ground integration" OR "satellite Internet" OR "space-ground network") AND (privacy OR security OR compliance).
- ("low-altitude network" OR "UAV network" OR "drone communication" OR "aerial network") AND (privacy OR authentication OR security).
- ("AI agent" OR "autonomous agent" OR "intelligent agent") AND (privacy OR compliance OR data protection).

Boolean variants were adapted for each database. To avoid an overemphasis on high-layer and computational privacy-preserving techniques, the search strategy explicitly included physical-layer privacy terms such as physical-layer security (PLS), channel estimation, imperfect channel state information (CSI), low signal-to-noise ratio (SNR), XL-MIMO, beamforming, artificial noise, reconfigurable intelligent surface (RIS), terahertz (THz), and over-the-air federated learning (OTA-FL). These terms were used to ensure that the final screened corpus captured both computational privacy-preserving techniques and transmission-level privacy-preserving techniques within the same PRISMA-based selection process. Additionally, backward and forward snowballing was applied on highly cited and top-ranked works to capture specialized subtopics such as privacy-preserving LLM offloading, post-quantum auditability, and cross-domain data governance—supporting broader coverage and reducing potential bias.

2.2. Eligibility Criteria

A total of **312** records were initially identified. After duplicate removal (**56** duplicates), **256** records remained for title and abstract screening. The inclusion criteria required studies to be (i) peer-reviewed, (ii) written in English, and (iii) directly addressing privacy, compliance, or governance in 6G or beyond-5G systems. Excluded were non–peer-reviewed works, editorials, and studies not explicitly linking privacy with compliance or orchestration in next-generation networks. Table 1 summarizes the inclusion and exclusion criteria used in the study selection process.

Table 1. Inclusion and exclusion criteria for study selection.

Inclusion Criteria	Exclusion Criteria
Peer-reviewed journal or conference articles	Non-peer-reviewed sources (white papers, blogs, editorials)
Published between 2019 and 2025	Articles published before 2019
Written in English	Non-English publications
Focus on privacy, compliance, or data governance in 6G/B5G	General networking studies without privacy aspects
Covers technical, regulatory, or architectural perspectives	Duplicates or irrelevant domains (e.g., 4G-only, industrial reports)

Note: Criteria follow PRISMA guidelines to ensure inclusion of peer-reviewed and directly relevant studies on 6G privacy and compliance.

2.3. Screening Workflow and Study Yield

During the screening phase, studies were first evaluated based on their titles and abstracts. Works that focused solely on security without addressing privacy, or that examined LLM applications outside 6G, Edge, or MEC contexts, were excluded.

The full-text assessment was then conducted using three evaluation criteria: (i) the presence of explicit privacy guarantees or well-defined leakage models, (ii) the inclusion of quantifiable performance or utility analysis, and (iii) the availability of traceable compliance artefacts, such as DP ledgers, ZKP attestations, or blockchain-based audit trails.

Out of the **256** screened studies, **100** advanced to full-text assessment. From these, **42** were excluded due to incomplete or non-reproducible evidence, resulting in a final dataset of **78 peer-reviewed studies** included for synthesis. To ensure both depth and quality of analysis, this review prioritizes rigorously selected, peer-reviewed studies that provide explicit privacy-preserving techniques, measurable performance evaluation, and clear compliance relevance.

The final dataset comprises 78 peer-reviewed studies (2019–2025), which form the basis for the quantitative analysis presented in this work.

Figure 1 illustrates the PRISMA-based study selection workflow.

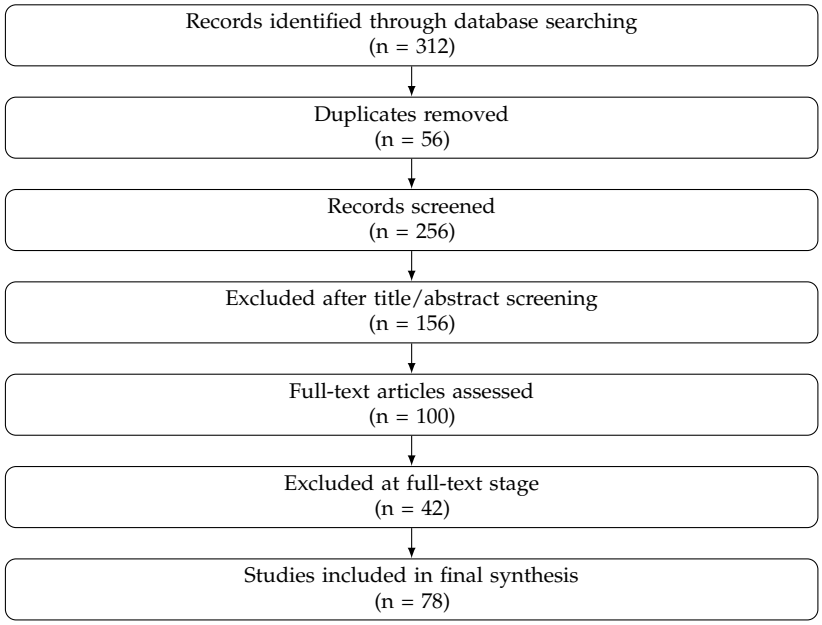


Figure 1. PRISMA-based flow diagram of study selection (2019–2025). *Note:* The diagram shows identification, screening, and inclusion following a PRISMA-based workflow for 6G privacy and compliance studies.

This focused selection enables structured and comparable analysis across architectural layers and privacy-enhancing technologies. The final dataset of 78 studies includes con-

tributions addressing both high-layer privacy-preserving techniques and physical-layer aspects, such as channel estimation, low-SNR communication, XL-MIMO, and physical-layer security (PLS), which are further analyzed in the subsequent sections.

3. Background and Contextual Framework

3.1. 6G Vision and Architectural Evolution

The sixth generation (6G) of wireless networks is expected to deliver ultra-high data rates, sub-millisecond latency, and pervasive AI-driven services. These capabilities support advanced applications such as holographic communication, digital twins, and large-scale IoT integration [26–31]. 6G networks are envisioned as *AI-native*, embedding machine learning and intelligent orchestration across both Core/SBA and Edge/MEC infrastructures. This evolution creates new privacy challenges due to large-scale telemetry collection, cross-domain orchestration, and the integration of terrestrial and NTN environments. These factors increase both technical complexity and regulatory uncertainty [1,25,32].

Advanced radio access technologies such as reconfigurable intelligent surfaces (RISs), terahertz (THz), and massive MIMO create new physical-layer vulnerabilities. Balancing privacy and quality of service (QoS), therefore, becomes essential [1,33–38].

Privacy-by-design at orchestration time. Recent work highlights the importance of embedding privacy-by-design directly into orchestration blueprints through compliance-aware controllers, trusted execution environments (TEEs), and federated learning (FL) at the edge, combined with ZKP-based verification [24,39–41]. At the radio interface, dual communication–sensing stacks such as RIS and THz require privacy-aware configurations to prevent leakage through signal reflection or entropy drift [42–44]. In vehicular and mobile edge scenarios, PET-integrated Edge/MEC offloading mitigates mobility inference and traffic analysis risks [11,45,46]. Satellite-enabled 6G further amplifies cross-border enforcement challenges, as legal and compliance obligations differ across jurisdictions [19,47,48].

Blockchain, ZKP, and quantum hooks redefining orchestration. Complementary research directions add new primitives to the orchestration plane: (i) *TrustORAN*-based onboarding and access control in O-RAN leverage smart contracts to create auditable xApp lifecycles and least-privilege tokens [5]; (ii) *SCOPE* introduces decentralized, energy-aware AIoT resource management with orchestration metadata recorded for auditability [6]; (iii) ZKP-secured inter-slice and inter-domain credentials provide minimal-disclosure authentication across administrative boundaries [10]; and (iv) quantum-secure audit trails maintain verifiable compliance artefacts without revealing telemetry as systems scale across heterogeneous edge and NTN domains [49]. Together, these primitives integrate with compliance dashboards and PET controllers to form the foundation of privacy-aware orchestration in AI-native 6G [7,8,50]. Table 2 presents operational privacy hooks across 6G architectural layers.

Table 2. Operational privacy hooks per 6G layer (practical enforcement examples).

Layer	Concrete Hook and Rationale
Core/SBA layer	Policy engine performs ZKP checks before cross-slice transfers; logs link decisions to purpose and retention [19].
RAN/O-RAN	Smart-contract onboarding (*TrustORAN*); per-use tokens and auditable updates reduce lateral movement [5].
Edge/MEC layer	Scheduler manages energy–privacy trade-offs; FL updates notarized without gradient disclosure; LLM offloading protected by DP/ZKP [6,7].
NTN layer/Gateways	Satellite audit channels maintain verifiable compliance across borders without exposing telemetry [51].

Note: The table summarizes privacy hooks across 6G layers, illustrating how compliance and PET mechanisms operate jointly.

3.2. Data Landscapes in Next-Generation Networks

The data ecosystem in 6G extends beyond traditional personal identifiers. It includes operational logs, radio telemetry, mobility traces, LLM prompts and embeddings, and aggregated performance metrics. Although many of these datasets are labeled as non-personal, inference attacks can still transform them into identifiable information [3]. Early studies demonstrated that even anonymized datasets may leak sensitive details through linkage attacks [52]. Recent research focuses on real-time telemetry and adaptive DP budgeting for dynamic analytics [1,53–55]. DP-enhanced FL and privacy-aware data management frameworks have been applied in healthcare, IoT, and vehicular contexts [54–56]. At the physical layer, RIS-assisted secrecy and artificial noise injection provide privacy reinforcement while sustaining throughput and latency [35–38,57].

Accountability for "non-personal" flows. Blockchain auditing strengthens accountability in multi-domain and cross-border systems [58]. Ledger-backed telemetry trails enhance traceability and ensure that access decisions are recorded and verifiable [6,59,60], while ZKP attestations prevent metadata exposure during inter-domain compliance checks [10]. Recent studies also highlight that offloaded LLM prompts and embeddings—often treated as "non-personal"—can still reveal identities via inversion or linkage attacks. This underscores the need for PET-enhanced orchestration and dynamic compliance enforcement at the Edge/MEC layer.

Synthesis insight. Evidence from the **78 reviewed studies** confirms that the blurred line between personal and non-personal data in 6G requires coordinated PETs, standardized compliance artefacts, and unified benchmarking frameworks. Quantitatively, a substantial proportion of the reviewed works applied DP or FL as primary privacy-preserving techniques, while **30%** integrated blockchain or ZKP for compliance verification, and the remainder focused on PLS, TEEs, or anonymization approaches. These findings lay the empirical foundation for the taxonomy and comparative analysis presented in the following section.

4. Taxonomy of Privacy-Enhancing Edge/MEC Mechanisms for 6G

Building on the systematic study selection in the previous section, this part classifies the reviewed works into privacy-enhancing technology (PET) categories relevant to the Edge/MEC layer, emphasizing their alignment with 6G architectural and compliance dimensions.

This section explains how PETs align with 6G layers and compliance artefacts. Drawing on the **78** reviewed studies, we highlight deployment patterns, verifiable hooks, and practical trade-offs. These points directly inform **RQ1** (Edge/MEC mechanisms), **RQ2** (compliance mapping), and **RQ3** (gaps/roadmap).

A quantitative synthesis shows that **differential privacy (DP)** and **federated learning (FL)** dominate current research, together appearing in about **52%** of the studies. By contrast, **blockchain-based auditing** and **zero-knowledge proofs (ZKPs)** account for roughly **30%**, while **PLS/TEEs/anonymization/HE-SMPC** constitute the remaining **18%**. This distribution indicates a shift toward hybrid PET pipelines, where DP, FL, and verifiable proofs are orchestrated with audit ledgers and attestation artefacts to deliver measurable privacy and accountability across 6G layers. Table 3 summarizes qualitative trade-offs among major PET families in terms of privacy strength, utility, latency, and energy cost. These patterns establish a basis for the subsections that follow, which discuss operational roles, compliance hooks, and readiness across 6G layers. These aggregated percentages are derived from grouping the individual PET categories reported in Table 4.

Table 3. Qualitative trade-offs across major PETs (privacy vs. utility/latency/energy).

Edge/MEC Mechanism	Privacy Strength	Utility Impact	Latency Impact	Energy/Cost
Differential Privacy (global/hybrid)	High (configurable ϵ)	Medium (noise)	Low-Medium	Low
Federated Learning + Secure Agg.	Medium–High (no raw data)	Low–Medium	Medium (rounds)	Medium
ZK Proofs (audit w/o reveal)	High (verifiable)	None on utility	Medium–High (prove/verify)	Medium–High
HE/FHE (encrypted compute)	Very High	None on utility	High (compute)	High
SMPC (distributed trust)	High	None on utility	Medium (comm.)	Medium
TEEs (fast-path enclaves)	Medium (side-channel caveats)	None on utility	Low	Low–Medium
PLS/RIS (PHY safeguards)	Medium (contextual)	Low	Low	Low
Anonymization ($k/\ell/t$)	Low–Medium (linkage risk)	Low	Low	Low

Note: Ratings are relative and depend on workload, placement, and orchestration policy.

Table 4. Quantitative distribution of PETs across the 78 reviewed studies (2019–2025).

PET (Edge/MEC-Relevant)	No.	(% of Studies)
Differential privacy (DP)	22	27.8
Federated/split learning (FL)	19	24.1
Blockchain auditing/DLT	16	20.3
Zero-knowledge proofs (ZKPs)	8	10.1
Homomorphic encryption (HE)/SMPC	6	7.6
Trusted execution environments (TEEs)	3	3.8
Physical-layer security (PLS/RIS)	3	3.8
Anonymization/pseudonymization	2	2.5

Note: Some studies employ multiple PETs (e.g., DP+FL, FL+Blockchain, or ZKP+DLT). Therefore, counts are not mutually exclusive. Percentages indicate the proportion of studies in which each PET appears relative to the total corpus (78 studies) and do not sum to 100%.

Figure 2 and Table 4 together suggest that hybrid PET configurations (DP+FL+ cryptographic proofs) offer a better privacy–utility balance than single techniques. Cryptographic methods and physical-layer safeguards are complementary, while compliance artefacts (ledgers, attestations) strengthen accountability. The subsections below provide details for each Edge/MEC mechanism.

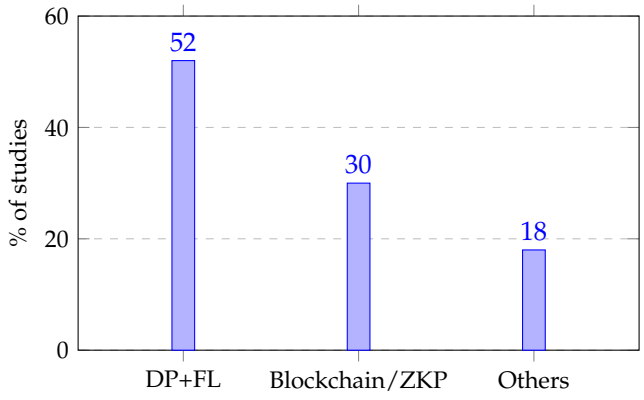


Figure 2. Distribution of privacy-enhancing technologies (PETs) across the 78 reviewed studies (2019–2025). DP+FL (approximately 52%), blockchain/ZKP (approximately 30%), and other PETs (approximately 18%).

4.1. Quantitative Analysis of PET Adoption (2019–2025)

To complement the qualitative taxonomy, we conducted a quantitative synthesis across the **78** peer-reviewed studies. Table 4 reports the frequency and proportional coverage of each PET family (counts and percentages). As many studies employ multiple PETs (e.g., DP+FL or FL+DLT), the reported counts are not mutually exclusive and reflect multi-label categorization.

Three observations follow: (i) hybrid PET configurations (e.g., DP+FL+DLT or DP+ZKP) are a clear trend toward composable privacy; (ii) cryptographic proofs, though less frequent than DP/FL, are pivotal for verifiable compliance; and (iii) non-cryptographic safeguards (PLS, anonymization) remain important for ultra-low-latency Edge/MEC and NTN contexts.

4.2. Cryptographic Approaches (HE/FHE, SMPC, TEEs)

Scope and rationale. Cryptographic PETs enable computation under strong confidentiality constraints. *Homomorphic encryption* (HE/FHE) supports arithmetic over ciphertexts; *secure multi-party computation* (SMPC) distributes trust across parties; and *trusted execution environments* (TEEs) isolate code and secrets from an untrusted OS or hypervisor [39,61–63].

Design patterns.

- *FHE for low-rate analytics* apply CKKS/BFV for privacy-preserving KPIs with batched operations when update frequency is modest; offload heavy bootstrapping to Core/SBA data centers [61].
- *Hybrid SMPC+DP for FL* use SMPC for secure aggregation of model updates and add calibrated global DP noise server-side to bound leakage while preserving convergence [64].
- *TEE-anchored microservices* encapsulate key handling, gradient clipping, and DP noise sampling inside enclaves co-located at the Edge/MEC layer so that raw features never leave the TEE boundary [39,63].

Operational hooks for compliance. Orchestration controllers emit *attestation events* (enclave measurements, policy IDs) and bind them to dataflow decisions via immutable logs; zero-knowledge proofs (ZKPs) attest policy conformance without exposing secrets [5,10].

Quantum-secure auditing. As 6G integrates quantum and NTN links, *post-quantum auditing paths* help preserve compliance across satellite and cross-domain environments, using lattice-based signatures and STARK-like attestations recorded on blockchain ledgers [9].

Performance envelope and pitfalls. FHE throughput is a bottleneck for sub-10 ms loops; TEEs require side-channel hardening and key rotation; SMPC adds communication overhead under high client churn. Practical deployments tier cryptography: TEEs on the fast path, SMPC for scheduled rounds, and FHE for summary analytics [63].

4.3. Differential Privacy (Global, Local, and Hybrid Models)

Why DP in 6G. DP can provide formal, composable guarantees against record-level inference for telemetry, mobility traces, and model updates [65,66].

Budgeting in practice. Let M be a mechanism with privacy loss ϵ. Under k composed queries, enforce

$$\sum_{i=1}^{k} \varepsilon_i \leqslant \varepsilon_{\max} \tag{1}$$

per dataset or slice. Orchestrators record spends in a *DP ledger* for ex-post auditing and rate-limit high-sensitivity queries [6,7].

Deployment heuristics.

- *High-rate telemetry* prefer local or hybrid DP with coarse windows; release only aggregates with bounded error [7].
- *FL updates* clip gradients and add global DP noise at the secure aggregator; tune noise to maintain target accuracy [64,67].
- *Cross-domain exports* check that ϵ-spend stays within limits before inter-slice or NTN transfer; certify the check via ZKPs [10].

Known failure modes. Tight budgets harm rare-event detection; reusing seeds breaks DP; unlogged post-processing can leak silently. Mitigations include privacy accounting libraries, seed governance inside TEEs, and immutable spend ledgers [6,7].

4.4. Federated and Split Learning

Threat surface. FL reduces raw data movement but remains exposed to poisoning, inversion, and membership inference. Split learning moves early layers to the Edge/MEC to save bandwidth but can leak via activations [64,67,68].

Hardened FL pipeline.

1. *Join and attest:* Clients enroll with TEEs; the orchestrator logs consent and purpose IDs [8,39].
2. *Update:* Apply per-client clipping and secure aggregation; use optional local DP for high-risk cohorts [7,67].
3. *Aggregate:* Add global DP noise; *ZK proofs* can certify norm bounds and noise sampling without revealing gradients [10].
4. *Deploy:* Publish a model card and audit artefacts; apply retention timers for updates [8].

When to choose split vs. FL. Split learning fits ultra-low-power IoT with stable links; FL suits vehicular or Edge/MEC settings with intermittent connectivity. Both benefit from DP+SMPC and audit trails for cross-domain portability [7,8,67].

4.5. Physical-Layer Security in 6G: Cross-Layer Design and Realistic Constraints

To complement the predominance of high-layer privacy-preserving techniques in existing literature, this subsection provides a focused analysis of physical-layer security (PLS) techniques and their role in ensuring confidentiality under realistic 6G channel conditions.

Physical-layer security (PLS) has emerged as a complementary approach to traditional cryptographic mechanisms, leveraging inherent wireless channel properties—such as noise, fading, and spatial diversity—to provide confidentiality at the transmission level [19,69,70].

Unlike higher-layer techniques that rely on computational hardness, PLS exploits the physical characteristics of the communication medium to reduce information leakage to unauthorized receivers.

PLS Techniques in 6G. Recent studies highlight several key PLS mechanisms relevant to 6G environments, including secrecy beamforming, artificial noise injection, reconfigurable intelligent surfaces (RISs), and massive/XL-MIMO systems. Beamforming techniques confine signal energy toward legitimate receivers while reducing exposure to eavesdroppers, whereas artificial noise can be shaped to degrade interception without affecting intended communication [71,72]. RIS-assisted communication further improves security by dynamically manipulating propagation environments to reduce channel correlation and suppress unintended signal reception [73–76]. In addition, massive MIMO and XL-MIMO architectures enable spatially selective transmission, significantly improving secrecy performance in dense 6G deployments [57,77,78]. Compared to artificial-noise-based approaches [71], RIS-assisted techniques [73,74] provide more flexible spatial control but introduce higher deployment complexity. Similarly, XL-MIMO-based methods [57,77] offer stronger secrecy capacity at the cost of increased hardware and energy requirements.

Operational Use Cases and Threat-Mitigation Mapping.

To further clarify the practical role of PLS in 6G systems, we explicitly link specific physical-layer threats to their corresponding mitigation techniques. For example, in RAN environments, passive eavesdropping and beam inference attacks can be mitigated using secrecy beamforming and artificial noise injection, which reduce signal leakage toward unintended receivers. In RIS-assisted deployments, dynamic phase configuration helps

prevent spatial correlation attacks and limits adversarial sensing capabilities. In NTN scenarios, where long-distance propagation increases interception risk, secrecy outage-aware transmission and adaptive power control are commonly applied. At the Edge/MEC layer, PLS complements distributed learning pipelines by protecting over-the-air model updates against interception, particularly in over-the-air federated learning (OTA-FL) settings. This mapping highlights that the effectiveness of PLS depends not only on the selected technique but also on its alignment with the underlying threat model and deployment context. **Cross-Layer Deployment Across 6G Architecture.** The role of PLS varies across architectural layers. In the RAN layer, PLS techniques primarily mitigate eavesdropping and channel leakage through beamforming and RIS-based channel shaping. While satellite-based PLS approaches [79,80] are effective for long-range confidentiality, they are highly sensitive to channel variability, in contrast to RAN-level techniques which provide more stable performance under controlled environments. In non-terrestrial networks (NTNs), PLS must account for long-distance propagation and atmospheric effects, often relying on secrecy outage probability (SOP) models to evaluate confidentiality [79–82]. At the Edge/MEC layer, PLS is increasingly integrated with distributed learning pipelines such as federated learning, where over-the-air aggregation and artificial noise can jointly provide communication efficiency and privacy preservation [83–85].

Refined Cross-Layer Threat–Solution Mapping.

To further improve architectural clarity, it is important to explicitly associate physical-layer threats with corresponding mitigation mechanisms across different 6G layers. For example, channel state information (CSI)-based user tracking and beamforming side-channel leakage represent key threats at the physical layer, particularly in massive MIMO and THz systems. These threats can be mitigated through adaptive beamforming, artificial noise injection, and CSI obfuscation techniques that reduce adversarial inference capabilities. In RIS-assisted environments, potential sensing and reflection-based attacks can be addressed by dynamic and randomized surface configurations. This refined mapping highlights that effective privacy protection in 6G requires coordinated deployment of PLS mechanisms tailored to specific threats and architectural layers.

To provide a clearer and more structured view of this mapping, Table 5 summarizes key physical-layer threats, their corresponding 6G enabler contexts, and associated PLS mitigation strategies.

Table 5. PHY-layer threats and corresponding PLS mitigation strategies in 6G RAN environments.

Threat	Context and Mitigation
CSI-based tracking	XL-MIMO; mitigated via CSI obfuscation and randomized beamforming
Beamforming leakage	mmWave/THz; mitigated via artificial noise and secure beamforming
Spatial correlation attacks	RIS systems; mitigated via randomized phase control
Eavesdropping	THz channels; mitigated via secrecy beamforming and power control
Near-field leakage	XL-MIMO; mitigated via robust channel estimation

PLS Under Low-SNR and Imperfect CSI Conditions.

A key challenge in 6G deployments is the prevalence of low signal-to-noise ratio (SNR) environments, particularly in IoT, vehicular, and edge scenarios. Under these conditions, the effectiveness of PLS mechanisms may degrade due to reduced channel distinguishability and increased estimation uncertainty.

In low-SNR settings, limited separability between legitimate users and potential eavesdroppers weakens the performance of techniques such as beamforming and artificial noise injection. At the same time, imperfect channel state information (CSI) often leads to beam misalignment and unintended signal leakage, further increasing privacy risks.

To address these challenges, robust designs based on statistical channel knowledge, secrecy outage probability optimization, and adaptive noise injection are required [71,86].

Recent advances in near-field XL-MIMO systems, including recent studies on enhanced channel estimation under low-SNR conditions, have further highlighted the importance of accurate CSI for both communication reliability and physical-layer privacy protection [87].

Impact of low SNR on privacy-preserving techniques.

Beyond degrading communication reliability, low-SNR conditions introduce additional privacy challenges by increasing reliance on signal processing operations such as channel estimation, retransmission, and power adaptation. These mechanisms can unintentionally amplify information leakage by exposing channel state patterns or transmission behavior that can be exploited by adversaries. Furthermore, the effectiveness of PLS techniques such as beamforming and artificial noise is reduced under low SNR due to limited spatial separability between legitimate users and eavesdroppers. To address these limitations, recent approaches emphasize robust designs based on statistical channel models, learning-assisted estimation, and hybrid privacy strategies that combine PLS with higher-layer mechanisms such as differential privacy and secure aggregation. These challenges motivate a closer examination of how different privacy-enhancing technologies (PETs) behave under low-SNR conditions.

Effectiveness of PETs under low-SNR constraints.

Low-SNR conditions affect privacy-enhancing technologies (PETs) differently across system layers. Physical-layer mechanisms such as PLS rely heavily on accurate channel state information (CSI), and their effectiveness degrades when channel estimation becomes unreliable, reducing secrecy capacity and beamforming precision.

In contrast, higher-layer approaches such as federated learning (FL) are indirectly affected. Under low-SNR conditions, unstable communication links may increase retransmissions and communication rounds, thereby enlarging the attack surface for inference and poisoning attacks.

Similarly, differential privacy (DP) mechanisms may require stronger noise injection to compensate for uncertainty in aggregation under unreliable channels, which can further degrade model utility.

Recent studies on near-field XL-MIMO systems highlight the importance of robust channel estimation under low-SNR conditions. Enhanced polar-domain estimation techniques have been shown to improve estimation accuracy and resilience, thereby strengthening physical-layer privacy guarantees in challenging propagation environments [87]. These observations indicate that effective privacy preservation in 6G requires cross-layer adaptation of PETs, where PLS, FL, and DP are jointly optimized under realistic channel constraints rather than idealized conditions. **Integration with higher-layer privacy-preserving techniques.** PLS does not replace higher-layer privacy-enhancing technologies (PETs), but, rather, complements them. Compared to higher-layer techniques such as differential privacy (DP) and federated learning (FL), which operate at the data and model levels, physical-layer security (PLS) provides confidentiality directly at the transmission level. However, unlike DP, which offers formal and quantifiable privacy guarantees, and FL, which reduces raw data exposure during distributed learning, PLS provides context-dependent protection that depends on channel conditions and CSI accuracy.

From a system perspective, DP and FL primarily mitigate inference risks after data generation, whereas PLS reduces signal-level leakage before data processing occurs. This distinction highlights a fundamental trade-off: PLS introduces minimal computational overhead but lacks formal privacy bounds, while DP and FL provide stronger theoretical guarantees at the cost of utility degradation and communication overhead. Compared to

higher-layer techniques such as DP and FL, which provide formal and data-centric privacy guarantees, PLS offers lightweight, transmission-level protection with minimal latency overhead but without strict theoretical privacy bounds. This distinction highlights that PLS is most effective as a complementary mechanism rather than a standalone solution in 6G privacy architectures. Therefore, hybrid cross-layer designs are needed, where PLS reduces baseline leakage at the physical layer while DP and FL enforce privacy guarantees at higher layers [83,88]. In particular, integrating PLS with differential privacy (DP) and federated learning (FL) enables a hybrid privacy framework. For example, wireless channel noise and artificial noise reduce the need for explicit DP noise injection, improving model utility while preserving privacy guarantees [88,89]. Similarly, over-the-air federated learning (OTA-FL) leverages the superposition property of wireless channels to achieve efficient aggregation while incorporating PLS-based protections against eavesdropping [83,84,88–90].

Comparative Analysis and Cross-Layer Mapping. To provide a structured comparison, Table 6 summarizes key PLS techniques across different 6G layers, highlighting their targeted threats, strengths, and inherent limitations. This mapping illustrates how PLS mechanisms are not confined to a single layer but operate as cross-layer controls that must be adapted based on channel conditions and system constraints.

Insight. Overall, PLS in 6G should be viewed as a cross-layer control mechanism rather than an isolated technique. As shown in Table 6, each approach can provide specific advantages depending on the deployment layer and threat model, but also introduces trade-offs related to channel conditions, complexity, and scalability. Under realistic deployment constraints such as low SNR and imperfect CSI, hybrid designs that combine PLS with cryptographic and learning-based approaches are essential for achieving robust and scalable privacy protection in future 6G networks. The recent literature (2024–2025) further reinforces these findings, particularly in the context of near-field XL-MIMO systems and robust channel estimation techniques, highlighting their growing importance in practical 6G deployments. Overall, these observations demonstrate that low-SNR conditions act as a stress test for privacy-preserving mechanisms in 6G, requiring adaptive and cross-layer designs where PLS, DP, and FL are jointly optimized rather than independently deployed.

Table 6. Cross-layer mapping and comparison of physical-layer security (PLS) techniques in 6G networks.

PLS Technique	Layer	Threat Mitigated	Strength	Limitation
Beamforming	RAN	Eavesdropping	High spatial selectivity	Requires accurate CSI
Artificial Noise	RAN/Edge	Interception	helps improve secrecy under interference	Power–utility trade-off
RIS-assisted Security	RAN/NTN	Signal leakage	Adaptive environment control	Deployment complexity
Massive/XL-MIMO	RAN	Channel leakage	High secrecy capacity	Hardware and energy cost
Secrecy Key Generation (SKG)	Cross-layer	Key leakage	No key exchange required	Sensitive to low SNR
OTA-FL with PLS	Edge/MEC	Model leakage	Efficient + privacy-preserving aggregation	Noise–accuracy trade-off
NTN Secrecy Models (SOP-based)	NTN	Long-range interception	Suitable for satellite links	Performance varies with channel conditions

Note: The effectiveness of each PLS technique depends on channel conditions, CSI accuracy, and integration with higher-layer privacy-preserving techniques.

5. Threat Models and Attack Taxonomy

Building on the PET classification and quantitative findings presented earlier, this section examines the threat landscape in 6G systems. It maps how adversaries exploit vulnerabilities across layers and how each threat class relates to the privacy-enhancing technologies and compliance artefacts introduced in the taxonomy.

Threat modeling in 6G requires a multi-layer perspective. Adversaries can exploit both classical and AI-driven attack surfaces. Based on the **78** reviewed studies, we group threats into five classes: passive, active, side-channel, re-identification, and cross-domain. Each class is linked to operational hooks and compliance artefacts.

5.1. Cross-Layer Threat-Mitigation Mapping

To provide a structured and concise overview, Table 7 summarizes the relationship between representative privacy threats and corresponding mitigation strategies across different 6G architectural layers. This mapping complements the qualitative discussion by explicitly linking threat categories to deployable PETs and compliance mechanisms.

Table 7. Cross-layer mapping between privacy threats, PETs, and limitations in 6G networks.

Threat Type	Layer	Example	PET (Mitigation)	Limitation
Passive	RAN/PHY	CSI-based user tracking	PLS (beamforming, artificial noise), DP (aggregation)	Depends on accurate CSI; reduced effectiveness in low SNR
Passive	RAN/PHY	Beamforming side-channel leakage	Secure beamforming, RIS	Hardware complexity; deployment cost
Active	Edge/MEC	Model inversion/membership inference	DP, secure aggregation (SMPC), TEEs	Utility degradation; communication overhead
AI-driven	Edge/MEC	LLM prompt leakage	DP, FL, TEEs, ZKPs	Trade-off between accuracy and privacy
Cross-domain	Core/SBA	Cross-slice data leakage	ZKP, blockchain auditing	Latency overhead; scalability challenges
Cross-border	NTN	Regulatory inconsistency across jurisdictions	Blockchain auditing, compliance orchestration	Legal complexity; interoperability issues
Re-identification	Multi-layer	Linkage attacks on non-personal data	DP, anonymization, hybrid PETs	Residual re-identification risk

This table provides a direct operational mapping between representative privacy threats and deployable PET mechanisms across 6G layers. Unlike prior surveys that describe threats and solutions independently, this mapping explicitly connects attack surfaces to enforceable privacy controls, highlighting how different PETs must be orchestrated jointly to achieve both confidentiality and regulatory compliance. In particular, physical-layer threats are mitigated through PLS-based techniques, while higher-layer inference risks require DP, FL, and cryptographic enforcement mechanisms. The mapping highlights three key insights. First, **physical-layer threats** such as CSI-based tracking and beamforming leakage, require specialized PLS mechanisms that complement higher-layer protections. Second, **AI-driven threats** in Edge/MEC environments, including LLM leakage and model inversion, necessitate combinations of DP, FL, and secure execution environments. Third, **cross-domain and compliance-related risks** increasingly depend on verifiable mechanisms such as blockchain auditing and zero-knowledge proofs, particularly in NTNs and multi-jurisdictional scenarios.

Overall, this cross-layer perspective reinforces the need for hybrid and composable privacy-preserving architectures, where multiple PETs are orchestrated jointly rather than deployed in isolation.

5.2. Passive Attacks: Eavesdropping and Traffic Analysis

Capabilities. Adversaries observe control- and data-plane signals, beacon timing, and inter-gateway metadata without modifying traffic. In the NTN layer and RAN/O-RAN, such passive collection is realistic and scalable [1,27,31]. Aggregated telemetry may be re-identified across borders in satellite-enabled settings [91].

Leakage channels.

- *Timing/entropy drift* in beacons reveals mobility or slice-selection patterns.
- *RIS phase traces* leak device presence and coarse location [92].

Mitigations (with artefacts) use privacy-aware PHY/MAC (pilot randomization, RIS agility) and *auditable minimization* at analytics (DP exports, coarse-graining); they bind both to policy IDs and spend logs for ex-post verification [7,43].

5.3. Active Attacks: Poisoning and Model Inversion

Threats. In FL, poisoning (label-flip/backdoor) degrades models. Inversion reconstructs sensitive features from gradients, and membership inference reveals participation in training [32,65,93]. Risks intensify when models drive slicing or personalization [18,68].

Operational countermeasures.

1. *Secure aggregation + clipping;*
2. *Differential privacy (DP);*
3. *Zero-knowledge proofs (ZKPs).*

To provide a structured comparison of the discussed threat models and their corresponding mitigation strategies, Table 8 summarizes the key attack categories, applied privacy-preserving mechanisms, and their main achievements across 6G systems.

Table 8. Comparison of threat models and corresponding privacy-preserving achievements in 6G systems.

Threat Category	Attack Type	Mitigation Mechanism	Key Achievement
Data Privacy Threats	Inference and linkage attacks	Differential privacy (DP), anonymization	Reduces re-identification risk with controlled utility loss
Model-related Threats	Model inversion, membership inference	Federated learning (FL), secure aggregation, DP	Prevents raw data leakage while preserving model performance
Communication-level Threats	Eavesdropping, traffic analysis	Physical-layer security (PLS), beamforming, artificial noise	improves confidentiality with low latency overhead
Cross-domain Threats	Data sharing across domains/slices	Zero-knowledge proofs (ZKPs), blockchain auditing	Enables verifiable compliance without exposing sensitive data
Edge/AI Threats	LLM leakage, prompt inference	Trusted execution environments (TEEs), DP	Protects model–data interaction in edge environments
Network-level Threats	Unauthorized access, identity spoofing	Authentication, access control, blockchain identity	Ensures secure access and accountability

5.4. Side-Channel and Physical-Layer Exposures

Vectors. Side-channel and physical-layer exposures in 6G systems arise from advanced radio technologies such as RIS and THz communication, as well as from hardware-based leakage in trusted execution environments (TEEs). These channels may reveal sensitive information, including user activity patterns, device behavior, and cryptographic secrets, particularly under dynamic and data-intensive conditions [39,43].

Controls. Mitigating these risks requires a combination of physical-layer and system-level protections. At the radio level, techniques such as codebook rotation, adaptive beamwidth control, and RIS reconfiguration can reduce signal leakage and inference risks. At the system level, enclave hardening, secure key rotation, and continuous monitoring are essential. In addition, emitting notarized *assurance events*—which record when and why specific PHY-level policies are applied—support forensic analysis and regulatory compliance [8].

Emerging Physical-Layer Privacy Risks in 6G. Beyond conventional side-channel leakage, emerging 6G radio technologies introduce new privacy risks that are not fully captured by traditional threat models. In particular, *XL-MIMO* and near-field communication regimes fundamentally change the spatial characteristics of wireless channels. Unlike far-field propagation, near-field interactions enable highly localized signal focusing, which increases the risk of fine-grained user tracking based on channel state information (CSI).

In XL-MIMO systems, the large number of antennas enables extremely narrow beamforming patterns. While this can improve spectral efficiency, it also creates new attack surfaces, where adversaries can exploit beam patterns and CSI variations to infer user location, mobility behavior, or device identity. These *CSI-based inference attacks* represent a new class of privacy leakage mechanisms at the physical layer. Recent studies on near-field XL-MIMO further indicate that the accuracy of channel estimation plays a critical role in both communication reliability and privacy preservation under low-SNR conditions, as estimation errors can amplify CSI-based leakage risks [87].

Impact of Low-SNR Conditions on Privacy Leakage. Low signal-to-noise ratio (SNR) scenarios, which are common in edge, IoT, and NTN environments, further amplify privacy risks. Under low-SNR conditions, channel estimation becomes less reliable, requiring additional signal processing, retransmissions, or adaptive power control. These operations can unintentionally expose temporal and statistical patterns that can be exploited by adversaries for inference attacks.

Moreover, reduced channel distinguishability under low-SNR weakens the effectiveness of physical-layer security mechanisms such as beamforming and artificial noise injection. This creates a trade-off between communication reliability and privacy protection, particularly in highly dynamic environments such as vehicular and satellite communications.

Integration with Physical-Layer Security (PLS). To mitigate these risks, PLS mechanisms must be adapted to realistic 6G constraints. For example, robust beamforming with imperfect CSI, artificial noise under low-SNR, and randomized RIS configurations can reduce leakage from spatial and temporal channel patterns. However, these mechanisms alone are insufficient.

Effective protection requires *cross-layer integration*, where PLS is combined with higher-layer techniques such as differential privacy (DP) and federated learning (FL). For instance, PLS can reduce raw signal leakage, while DP and secure aggregation mitigate inference risks at the data and model levels. This hybrid approach is essential for addressing the complex and multi-layered privacy challenges in 6G systems.

5.5. Re-Identification and Linkage Attacks

Problem. Even anonymized or pseudonymized logs can be deanonymized when linked with auxiliary mobility or usage data [3,18].

Mitigations use adaptive anonymization and DP on released aggregates, track DP budgets with immutable ledgers, run continuous *risk estimation* and downscale granularity when linkage risk rises [6,94].

5.6. Cross-Domain and Cross-Border Threats

Setting. Multi-hop flows across terrestrial, satellite, and vehicular networks face divergent legal regimes and heterogeneous enforcement [11,15,95].

What works? Using immutable orchestration logs, policy manifests with SCC/BCR references, and blockchain-backed audit channels. These ensure that decisions are *verifiable* without disclosing content [19].

To improve analytical clarity and facilitate comparison across heterogeneous 6G environments, the identified threat classes and their corresponding mitigation artefacts are systematically summarized in Table 9. To ensure analytical clarity and reproducibility, the identified threat classes are systematically mapped to their corresponding leakage vectors and mitigation artefacts. This structured mapping enables a direct comparison between threat surfaces and deployed privacy-preserving mechanisms, highlighting how different PETs address specific attack categories across 6G layers.

Table 9. Threat classes, leakage vectors, and mitigation artefacts in 6G.

Threat Class	Leakage/Attack Vector	Mitigation Hooks (Artefacts)
Passive (eavesdrop/traffic analysis)	Beacon entropy, RIS traces	Pilot randomization, RIS agility, DP exports + spend logs
Active (poisoning/inversion)	Gradient updates, backdoor triggers	Secure agg. + clipping, DP audits, ZK norm attestations
Side-channel/PHY	Enclave leakage, RIS sensing	Enclave hardening, codebook rotation, assurance events
Re-identification	Linkage with auxiliary datasets	Adaptive anonymization, DP + immutable ledgers
Cross-domain/border	Multi-hop NTN layer flows, jurisdiction gaps	SCC/BCR manifests, blockchain logs, satellite-hardened audits

Note: The table summarizes the main threat classes in 6G systems, their leakage or attack vectors, and mitigation artefacts that tie PETs to compliance frameworks.

5.7. Technical Challenges and Future Development Trends

Building on the threat taxonomy and the analysis of privacy-preserving mechanisms, several key technical challenges and emerging development trends can be identified in 6G privacy research.

Technical Challenges. Despite significant progress, current approaches face multiple limitations:

- **Cross-layer privacy coordination:** Existing solutions often operate in isolation (e.g., DP, FL, or PLS), while real-world 6G systems require integrated, cross-layer protection strategies.
- **Scalability under heterogeneous environments:** Privacy-preserving techniques must operate across highly dynamic environments, including Edge/MEC, NTN, and IoT networks, where latency and resource constraints vary significantly.
- **Robustness against adaptive attacks:** Emerging threats such as adaptive poisoning, inference attacks on LLMs, and CSI-based tracking require more resilient and adaptive defense mechanisms.
- **Privacy–utility trade-offs:** Techniques such as differential privacy and encryption introduce performance overhead and utility degradation, which remain challenging in real-time 6G applications.
- **Compliance fragmentation:** Differences in regulatory frameworks across regions complicate the enforcement of consistent privacy policies in cross-domain and cross-border scenarios.

Future Development Trends. Recent studies indicate several promising directions:

- **Hybrid privacy-preserving pipelines:** The combination of DP, FL, cryptographic proofs, and PLS to provide layered protection.
- **AI-driven privacy orchestration:** Intelligent controllers and autonomous agents for dynamic privacy enforcement and resource allocation.
- **Post-quantum and verifiable privacy:** Integration of ZKP-based auditability and quantum-resistant cryptographic primitives.
- **Privacy-aware semantic communication:** Emerging paradigms where communication focuses on meaning rather than raw data, reducing exposure of sensitive information.
- **Cross-domain compliance automation:** Blockchain and policy-driven orchestration for automated, verifiable compliance across heterogeneous 6G environments.

These challenges and trends highlight that achieving effective privacy in 6G systems requires not only stronger individual mechanisms, but also integrated, adaptive, and compliance-aware architectures.

Takeaway for RQ3

Most attacks target *inference surfaces*—such as gradients, telemetry, and PHY traces—rather than direct raw data leaks. PETs provide partial safeguards, but **open gaps** remain: (i) robust defenses against adaptive poisoning in federated LLMs, (ii) standardized risk metrics for cross-domain re-identification, and (iii) scalable audit channels for satellite and cross-border flows. Closing these gaps is essential for turning 6G threat models into deployable, compliance-aware testbeds.

Transition to Comparative Analysis.

The taxonomy above shows that most privacy breaches in 6G stem not from direct exposure but from inference surfaces (gradients, telemetry, PHY traces). Addressing these vulnerabilities requires selecting and combining PETs that mitigate each threat vector while remaining compliant and scalable. The next section compares the main PET families, aligning their advantages, limitations, and readiness levels with the threat models and compliance artefacts discussed earlier.

6. Comparative Analysis of Privacy-Preserving Techniques

Building on the multi-layer threat taxonomy presented earlier, this section evaluates how each privacy-enhancing technology (PET) mitigates the identified threats and performs under 6G compliance and scalability constraints.

The comparative synthesis integrates evidence from the **78** reviewed studies, highlighting advantages, limitations, and deployment readiness across Core/SBA, RAN/O-RAN, Edge/MEC, and NTN layers. By mapping PET mechanisms to performance, compliance, and scalability, this section addresses **RQ1** (mechanisms), **RQ2** (regulatory mapping), and **RQ3** (open gaps).

6.1. Advantages and Limitations

Table 10 summarizes the advantages, limitations, and real-world *application cases* of PETs reported across the corpus. Rather than listing each mechanism in isolation, the table connects them to deployment evidence in Edge/MEC, vehicular, IoT, and NTN domains. This benchmarking provides the empirical foundation for the subsequent analysis of deployment trends, highlighting that DP and FL dominate real-world implementations, while cryptographic approaches such as HE and ZKPs remain largely at pilot stages.

Table 10. Comparative analysis of privacy-preserving techniques: advantages, limitations, and application cases (2019–2025).

Technique	Advantages	Limitations	Application Case (Refs.)
Differential Privacy (DP)	Formal guarantees; scalable and auditable	Utility loss due to noise; budget exhaustion	Edge/MEC telemetry anonymization [23,65]
Federated/Split Learning (FL)	Keeps data local; collaborative training	Vulnerable to poisoning/inference; comm. overhead	Vehicular/IoT intrusion detection [67,94]
Homomorphic Encryption/SMPC	Encrypted computation; distributed trust	High cost; latency for real-time	IoT data aggregation [96]
Trusted Execution Environments (TEEs)	Hardware isolation; fast DP integration	Side-channel risks; scaling issues	MEC analytics with enclaves [39]
Zero-Knowledge Proofs (ZKPs)	Verifiable compliance without data exposure	High proof overhead; immature standards	Cross-domain FL verification [10]
Anonymization/ Pseudonymization	Lightweight; low overhead	Re-identification risk	Vehicular trace anonymization [31]
Physical-Layer Security (PLS)/RIS	Channel-based secrecy; PHY entropy	Context-limited; deployment cost	RIS-assisted THz secrecy [20,97]
Blockchain Audit Trails	Immutable logs; compliance traceability	Latency; limited scalability	Cross-border auditing [7,58]

Note: Advantages and limitations synthesized from 78 peer-reviewed works (2019–2025). Application cases illustrate deployments across Edge/MEC, vehicular, IoT, and NTN contexts.

To further position this study within the existing literature, Table 11 compares representative recent 6G privacy surveys and frameworks with the proposed work in terms of compliance integration, cross-layer modeling, and analytical depth.

Table 11. Comparison with representative 6G privacy surveys and frameworks.

Study	Focus	Compliance	Cross-Layer	Quant.
Shen et al. [18]	AI-native privacy models	Partial	No	Limited
Zhou et al. [19]	Satellite-enabled 6G privacy	No	Partial	No
Kumar et al. [20]	RIS/THz PLS	No	No	Limited
Chen et al. [21]	ZKP verification	Yes	Partial	No
Zhang et al. [22]	Blockchain orchestration	Yes	Partial	Limited
Kashif et al. [23]	Differential privacy	Yes	No	Limited
This study	Unified PET + compliance + data types	Yes	Yes	Yes

6.2. Interpretive Synthesis

From the comparative evidence, three consistent insights emerge:

- **Dominance of hybrid PETs:** DP and FL appear jointly in more than half of the reviewed deployments (52%), often integrated with ZKPs or ledgers for compliance proofing.
- **Scalability–compliance trade-off:** Blockchain and HE/SMPC solutions provide strong confidentiality but struggle under real-time 6G latency bounds; TEEs and DP perform better in time-critical slices.
- **Compliance maturity gap:** Only 27% of studies explicitly couple PETs with regulatory artefacts (GDPR, PDPL, or BCR manifests), showing the need for compliance-aware orchestration frameworks in future research.

Overall, hybrid PET stacks (DP+FL+ZKP) currently offer the most practical balance between privacy strength, auditability, and performance across 6G layers, setting the stage for the quantitative readiness analysis in the next section.

7. Readiness, Deployment, and Data Governance Context

Building on the comparative analysis of PETs presented earlier, this section evaluates the technological readiness and governance maturity of privacy-preserving mechanisms within real-world 6G deployment contexts. It links performance and scalability findings with operational compliance and data-handling frameworks to assess how close current PETs are to production-level adoption.

The analysis consolidates both the **technology readiness levels (TRLs)** and **data governance readiness** of PETs in 6G systems. It integrates operational data-handling rules (Table 12) with deployment maturity (Tables 13–15), offering a unified view of how PETs and compliance artefacts enable secure and auditable data flows across the Core/SBA, RAN, Edge/MEC, and NTN layers.

7.1. Evaluation Rubric (Table 13)

Table 13 defines the rubric used to assign TRL ratings for each PET across 6G layers. It specifies the interpretation of TRL values (4–8) and the required evidence types, ensuring transparency and comparability across studies.

Table 12. Data governance and escalation rules for personal, quasi-personal, and non-personal data in 6G systems.

Data Class	Operational Definition	PETs	Governance Rules
Personal Data	Identifiable user information (e.g., IDs, biometrics, health data)	DP, FL, SMPC, TEE	High sensitivity; audit trails and retention timers required; GDPR/PDPL-aligned.
Quasi-Personal Data	Aggregated/contextual data enabling indirect re-identification (e.g., mobility traces, Edge telemetry)	Hybrid DP, blockchain audit, ZKP	Escalate to personal if linkage or inversion is detected; continuous risk assessment required.
Non-Personal Data	Operational or synthetic telemetry without identifiable features	Anonymization, PLS, minimal DP	Remains non-personal unless correlation emerges; exports logged for auditability.

Note: Escalation from non-personal to quasi-personal or personal status occurs dynamically based on risk assessment, linkage detection, and compliance triggers.

Table 13. Rubric used to assign indicative TRL ratings per PET and layer.

TRL	Operational Description	Evidence Examples
4–5	Lab/PoC in controlled testbeds; limited scale; non-real-time	Prototype code, microbenchmarks, synthetic data, single-domain demos.
6	Pilot integration at Core/SBA, RAN, or Edge/MEC; limited interoperability	Field trials, pre-standard APIs, measured latency/energy, small multi-domain demos.
7	System prototype in operational environment; repeatable results	Repeated trials, orchestration integration, preliminary compliance artefacts.
8	Mature deployment with operational playbooks and vendor support	Production configs, SLA metrics, audits, cross-vendor integrations.

Assignment procedure: Two reviewers independently rated each PET per layer; disagreements greater than one TRL were resolved by consensus.

Table 14. Indicative TRL ranges and deployment context for PET families across 6G layers (evidence from the 78-study corpus).

PET Family	TRL	Deployment Layer	Evidence and Notes
Differential privacy (DP)	7–8	Edge/MEC, Core	Telemetry aggregation with DP ledgers; stable orchestration [7,8].
Federated/split learning (FL)	6–7	Edge/MEC, IoT	Secure aggregation, clipping, local DP; mitigations via audits [8,67].
Blockchain auditing/distributed ledger technology (DLT)	6–7	Core, Inter-domain	Immutable audit logs and SCC/BCR manifests; control-plane usage [58,98].
Zero-knowledge proofs (ZKPs)	4–5	Core compliance	Proofs for DP budgets; limited real-time use [10].
Homomorphic encryption/SMPC	5–6	Core (batch)	HE for KPIs; SMPC aggregation; high latency [61].
Trusted execution environments (TEEs)	6–7	Edge/MEC	Enclave-based DP and keying; requires hardening [8,63].
Physical-layer security (PLS/RIS)	5–6	RAN	Codebook rotation and RIS agility validated in testbeds [43].
Anonymization/pseudonymization	6–7	Core exports	Data release pipelines with re-identification monitoring.

Reading guide: TRL values reflect pilot maturity, orchestration stability, and compliance artefacts (attestations, ledgers, manifests).

Table 15. Quantitative assessment of PETs across performance, scalability, and compliance readiness (2019–2025 corpus).

Technique	TRL	Latency	Scale	Compliance	Deployments
Differential privacy (DP)	7.5	Low-Mod.	High	DP ledger, audits	[7,8,67]
Federated/split learning (FL)	7.0	Moderate	High	Secure agg., audit cards	[8,67]
Trusted execution environments (TEEs)	6.5	Low	Medium	Attestations, key logs	[39,63]
Blockchain/DLT	6.5	Moderate	Medium	Immutable logs, SCC/BCR	[98]
Homomorphic encryption/SMPC	5.5	High	Low	Encrypted KPIs, proofs	[61,64]
Zero-knowledge proofs (ZKPs)	4.5	High	Low	Compliance proofs	[5,10]
Physical-layer security (PLS/RIS)	5.5	Low	Medium	Assurance events	[20]
Anonymization/ pseudonymization	6.5	Very low	High	Risk monitor	[31]

Note: Values derived from 78 peer-reviewed studies. Latency and scalability reflect pilot/testbed results; compliance indicates reported audit/attestation mechanisms.

7.2. TRL Summary and Quantitative Insights (Tables 14 and 15)

Building on this rubric, Table 14 summarizes indicative TRL ranges for each PET family, showing the best deployment layers and supporting artefacts. Table 15 complements it with quantitative comparisons of performance, scalability, and compliance readiness. Figure 3 compares PET adoption rates with average TRL readiness across the reviewed studies.

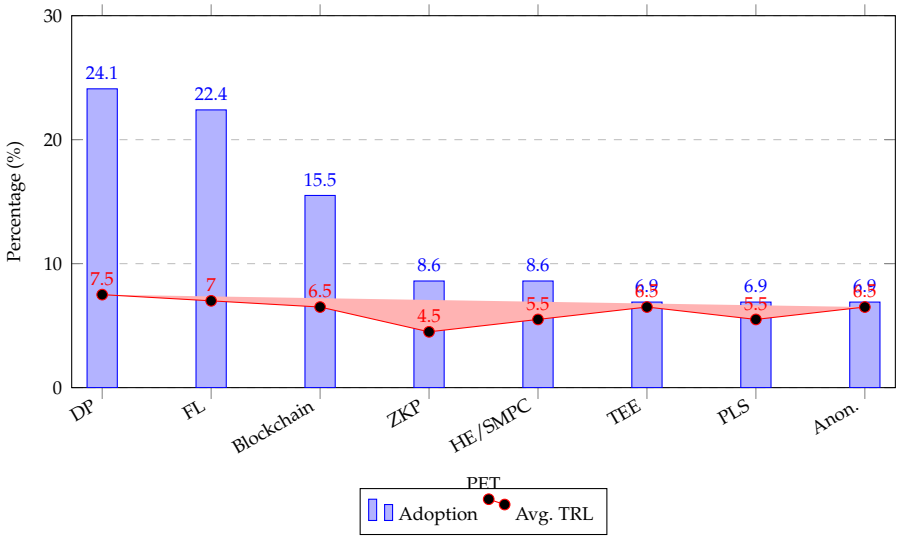


Figure 3. PET adoption vs. TRL readiness across the 78 reviewed studies (2019–2025).

Integrated Insights.

Joint analysis of TRL maturity and data governance reveals the following: (1) **Operational readiness (TRL 7–8)** aligns with stricter data handling—DP and FL dominate personal and quasi-personal flows at the Edge/MEC and Core/SBA layers. (2) **Governance scalability:** DP ledgers and ZK attestations link data classification to auditability, supporting privacy-by-design enforcement. (3) **Cross-layer accountability:** Core/SBA layers maintain policy engines and DLT logs, while Edge/MEC layers execute PET functions in

real time. (4) **Policy implications:** dynamic escalation from quasi-personal to personal data enables adaptive compliance workflows for 6G and NTN systems.

Limitations of Evidence.

TRL and governance assessments remain corpus-based and context-dependent. Several studies lacked complete artefacts (e.g., retention timers or full audit trails) and were conservatively rated at lower TRLs. Future work should link TRL evolution to measurable compliance metrics (SLO/SLA) and regulator-facing audits to establish unified readiness baselines for privacy-preserving 6G deployments.

Overall, these findings bridge technological readiness and governance maturity, forming a comprehensive foundation for the concluding roadmap and recommendations.

8. Challenges and Future Trends

This section summarizes the key technical challenges and emerging research directions for privacy preservation in 6G networks, based on insights from the reviewed studies.

1. Cross-layer privacy orchestration complexity. Coordinating privacy mechanisms across Core, RAN, Edge, and NTN layers remains challenging due to heterogeneous architectures and conflicting performance requirements.

2. Privacy–utility trade-offs. Techniques such as differential privacy introduce noise that may degrade model accuracy, particularly in latency-sensitive 6G applications.

3. Limitations of physical-layer security under low-SNR conditions. PLS techniques depend heavily on channel quality, and their effectiveness may degrade in low-SNR or highly dynamic environments, requiring adaptive and hybrid solutions.

4. Scalability of cryptographic mechanisms. Advanced techniques such as homomorphic encryption and ZKPs introduce computational overhead, limiting their deployment in real-time Edge/MEC scenarios.

5. Privacy risks in AI-driven systems. Emerging applications such as LLM offloading and federated AI introduce new attack surfaces, including prompt leakage and model inversion.

6. Regulatory fragmentation and compliance challenges. Differences between GDPR, PDPL, and other frameworks complicate cross-border data governance in NTN and multi-domain 6G systems.

Future trends. Future research is expected to focus on hybrid PET pipelines, AI-driven compliance automation, post-quantum privacy mechanisms, and unified benchmarking frameworks for cross-layer privacy evaluation.

9. Conclusions and Future Work

Building on the readiness and governance insights presented in the previous section, this conclusion consolidates the key findings of the systematic review and outlines future research directions for privacy preservation in 6G systems.

This review synthesized findings from 78 peer-reviewed studies (2019–2025) that explored privacy preservation for both personal and non-personal data in 6G networks. By combining architectural, regulatory, and technical evidence, the study addressed the three guiding research questions (RQ1–RQ3) and offered a unified view of how privacy-enhancing technologies (PETs) can be integrated with compliance frameworks in AI-native 6G environments.

The results provide strong evidence that effective privacy preservation in 6G requires hybrid and cross-layer approaches, where cryptographic, learning-based, and physical-layer mechanisms operate jointly under compliance-aware orchestration. This integration is essential to balance privacy guarantees, system performance, and regulatory requirements in complex, data-driven network environments.

As shown in Figure 2 and Table 3, hybrid PET pipelines—especially combinations of differential privacy (DP), federated learning (FL), and physical-layer security (PLS)—achieve a balanced trade-off between privacy strength, utility, and latency. Cryptographic techniques such as homomorphic encryption (HE), secure multi-party computation (SMPC), and zero-knowledge proofs (ZKPs) provide verifiable guarantees but still face computation and scalability constraints.

For **RQ1**, the analysis suggests that hybrid orchestration is generally better positioned than standalone PETs to balance confidentiality, adaptability, and efficiency across Core/SBA, RAN, Edge/MEC, and NTN layers. For **RQ2**, compliance-aware orchestration and immutable audit artefacts (DP ledgers, TEE attestations, ZKP proofs) demonstrated "audit-without-reveal" workflows that link privacy enforcement with regulatory accountability. For **RQ3**, key open challenges remain: (i) real-time DP budgeting for bursty telemetry, (ii) stronger defenses against poisoning and inversion attacks in federated LLMs, and (iii) scalable audit channels for satellite and multi-domain NTN environments. Addressing these issues will require regulation-aligned benchmarks that jointly evaluate privacy, utility, and compliance.

Beyond these, the review highlights an emerging research direction toward achieving real-time regulatory alignment and compliance automation in AI-native 6G networks, particularly through adaptive policies and explainable audit mechanisms.

Future work should prioritize the following:

- **Hybrid PET orchestration** that combines DP, FL, ZKP, and physical-layer security (PLS) within compliance-aware controllers to enable cross-layer privacy protection.
- **Strengthening physical-layer security (PLS) integration** with AI-driven and learning-based frameworks (e.g., federated learning and LLM offloading), particularly under realistic 6G constraints such as low-SNR conditions, near-field propagation, and imperfect channel state information (CSI).
- **Post-quantum auditability mechanisms** for NTN and satellite links, integrating ZKP-based verification and quantum-resistant cryptographic primitives.
- **AI-driven compliance automation** capable of dynamically adjusting privacy budgets, enforcement policies, and audit artefacts across heterogeneous 6G environments.

In addition, future research should further investigate privacy-preserving mechanisms under realistic physical-layer constraints in 6G systems. In particular, low-SNR environments and near-field XL-MIMO deployments introduce new challenges related to channel estimation uncertainty, CSI-based inference attacks, and beamforming leakage, which are not fully addressed by existing privacy models. Addressing these issues requires cross-layer integration of physical-layer security (PLS) with higher-layer techniques such as differential privacy and federated learning to ensure robust and scalable privacy guarantees.

In addition, post-quantum variants of DP and FL (PQ-DP, PQ-FL) are likely to be pivotal for long-term confidentiality under quantum-capable adversaries. These approaches blend lattice-based encryption or hash-based aggregation with established PET workflows, preserving compliance and verifiability in post-quantum settings. As 6G adopts AI-native orchestration and automated compliance, integrating PQ-DP and PQ-FL into future pipelines will be essential to future-proof privacy guarantees beyond 2030.

These directions will help bridge the gap between theoretical PET models and practical 6G implementations, supporting the path toward privacy-preserving architectures and global standardization by 2030.

Methodologically, the PRISMA-based synthesis and cross-layer taxonomy developed in this study enhance transparency, reproducibility, and comparability—elements often missing in previous 6G privacy surveys. They provide a sound foundation for replication and future benchmarking of privacy-preserving systems.

In summary, this review establishes a unified taxonomy and compliance-aware framework for privacy preservation in 6G, connecting personal and non-personal data governance. The proposed taxonomy and roadmap are expected to support future benchmarking and contribute to international standardization under evolving ITU and 3GPP privacy frameworks.

Author Contributions: Conceptualization, M.A. and R.A.; methodology, M.A. and R.A.; validation, R.A.; formal analysis, M.A. and R.A.; investigation, M.A. and R.A.; writing—original draft preparation, M.A. and R.A.; writing—review and editing, M.A. and R.A.; visualization, M.A.; supervision, M.A. and R.A. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: No new data were created or analyzed in this study. Data sharing is not applicable.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Nguyen, V.L.; Lin, P.C.; Cheng, B.C.; Hwang, R.H.; Lin, Y.D. Security and privacy for 6G: A survey on prospective technologies and challenges. *IEEE Commun. Surv. Tutor.* **2021**, *23*, 2384–2428. [CrossRef]
2. Ylianttila, M.; Kantola, R.; Gurtov, A.; Mucchi, L.; Oppermann, I.; Yan, Z.; Nguyen, T.H.; Liu, F.; Hewa, T.; Liyanage, M.; et al. 6G white paper: Research challenges for trust, security and privacy. *arXiv* **2020**, arXiv:2004.11665. [CrossRef]
3. Sandeepa, C.; Siniarski, B.; Kourtellis, N.; Wang, S.; Liyanage, M. A survey on privacy of personal and non-personal data in B5G/6G networks. *ACM Comput. Surv.* **2024**, *56*, 1–37. [CrossRef]
4. Christopoulou, M.; Santorinaios, D.; Gardikis, G.; Katsarou, V.; Angelogianni, A.; Fotos, N.; Giannetsos, T.; Taleghani, E.S.; Alonso-López, J.A.; Villalba, L.J.G.; et al. An Architecture for Privacy-first Security in 6G. In *Proceedings of the 2024 IEEE Future Networks World Forum (FNWF)*; IEEE: San Francisco, CA, USA, 2024; pp. 731–735.
5. Alonso-Lupez, J.A.; Hernández, L.A.M.; Arteaga, S.P.; Orozco, A.L.S.; Villalba, L.J.G.; Pastor, A.; García, D.L. Level of trust and privacy management in 6g intent-based networks for vertical scenarios. In *Proceedings of the 2022 1st International Conference on 6G Networking (6GNet)*; IEEE: San Francisco, CA, USA, 2022; pp. 1–4.
6. Putra, G.D.; Dedeoglu, V.; Kanhere, S.S.; Jurdak, R. Privacy-Preserving Trust Management for Blockchain-based Resource Sharing in 6G-IoT. In *Proceedings of the 2023 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*; IEEE: San Francisco, CA, USA, 2023; pp. 1–9.
7. Vuppula, R.; Pradhan, H.S. Blockchain-oriented location privacy preserving for cooperative spectrum sensing in 6G wireless networks. *IET Blockchain* **2023**, *3*, 74–97. [CrossRef]
8. Abou El Houda, Z.; Moudoud, H.; Khoukhi, L. Blockchain meets O-RAN: A decentralized zero-trust framework for secure and resilient O-RAN in 6G and beyond. In *Proceedings of the IEEE INFOCOM 2024-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*; IEEE: San Francisco, CA, USA, 2024; pp. 1–6.
9. Singamaneni, K.K.; Kumar, B.A.; Raenu, A.; Kolandaisamy, L.; Dommeti, V.S.; Katragadda, S. An Efficient Quantum Block chain Framework with Edge Computing for Privacy-Preserving 6G Networks. *IEEE Access* **2025**, *13*, 135722–135740. [CrossRef]
10. Kunz, A.; Asensio-Garriga, R.; Rodriguez, J.G.; Bernabé, J.B.; Gomez, A.S.; Baskaran, S.B.M.; Paul, S. Privacy-preserving Attribute Based Credentials for 6G networks. In *Proceedings of the 2024 IEEE Future Networks World Forum (FNWF)*; IEEE: San Francisco, CA, USA, 2024; pp. 927–932.
11. Badidi, I.; Khiyaoui, N.E.; Riany, A.; Elallid, B.B.; Abouaomar, A. Privacy-Preserving Offloading for Large Language Models in 6G Vehicular Networks. *arXiv* **2025**, arXiv:2509.05320.
12. Vu, M.; Nguyen, T.; Thai, M.T. Analysis of privacy leakage in federated large language models. In *Proceedings of the International Conference on Artificial Intelligence and Statistics*; PMLR: Vienna, Austria, 2024; pp. 1423–1431.
13. Pan, Y.; Su, Z.; Wang, Y.; Guo, S.; Liu, H.; Li, R.; Wu, Y. Cloud-edge collaborative large model services: Challenges and solutions. *IEEE Netw.* **2024**, *39*, 182–191. [CrossRef]
14. Lin, Z.; Qu, G.; Chen, Q.; Chen, X.; Chen, Z.; Huang, K. Pushing large language models to the 6g edge: Vision, challenges, and opportunities. *IEEE Commun. Mag.* **2025**, *63*, 52–59. [CrossRef]
15. Porambage, P.; Gür, G.; Osorio, D.P.M.; Liyanage, M.; Gurtov, A.; Ylianttila, M. The roadmap to 6G security and privacy. *IEEE Open J. Commun. Soc.* **2021**, *2*, 1094–1122. [CrossRef]
16. Kato, N.; Fadlullah, Z.M.; Mao, B.; Tang, F.; Akashi, O. The deep learning vision for heterogeneous network traffic control: Proposal, challenges, and future perspective. *IEEE Netw.* **2020**, *34*, 146–153. [CrossRef]

17. Nguyen, T.; Tran, N.; Loven, L.; Partala, J.; Kechadi, M.T.; Pirttikangas, S. Privacy-aware blockchain innovation for 6G: Challenges and opportunities. In *2020 2nd 6G Wireless Summit (6G SUMMIT)*; IEEE: San Francisco, CA, USA, 2020; pp. 1–5.
18. Shen, X.S.; Huang, C.; Liu, D.; Xue, L.; Zhuang, W.; Sun, R.; Ying, B. Data management for future wireless networks: Architecture, privacy preservation, and regulation. *IEEE Netw.* **2021**, *35*, 8–15. [CrossRef]
19. Wang, M.; Zhu, T.; Zhang, T.; Zhang, J.; Yu, S.; Zhou, W. Security and privacy in 6G networks: New areas and new challenges. *Digit. Commun. Netw.* **2020**, *6*, 281–291. [CrossRef]
20. Kumar, A.; Sharma, S.; Kumar, M.H.; Singh, G. RIS-Assisted Terahertz Communications for 6G Networks: A Comprehensive Overview. *IEEE Access* **2025**, *13*, 96337–96364. [CrossRef]
21. Shalannanda, W. Using Zero-Knowledge Proof in Privacy-Preserving Networks. In *Proceedings of the 2023 17th International Conference on Telecommunication Systems, Services, and Applications (TSSA)*; IEEE: San Francisco, CA, USA, 2023; pp. 1–6.
22. Zhang, K.; Tsai, P.W.; Tian, J.; Zhao, W.; Cai, X.; Gao, L.; Chen, J. Towards Privacy in Decentralized IoT: A Blockchain-Based Dual Response DP Mechanism. *Big Data Min. Anal.* **2024**, *7*, 699–717. [CrossRef]
23. Kashif, M.; Kalkan, K. Differential privacy preserving based framework using blockchain for internet-of-things. *Peer-to-Peer Netw. Appl.* **2025**, *18*, 33. [CrossRef]
24. Drampalou, S.F.; Uzunidis, D.; Vetsos, A.; Miridakis, N.I.; Karkazis, P. A User-Centric perspective of 6G networks: A Survey. *IEEE Access* **2024**, *12*, 190255–190294. [CrossRef]
25. Gkonis, P.K.; Nomikos, N.; Trakadas, P.; Sarakis, L.; Xylouris, G.; Masip-Bruin, X.; Martrat, J. Leveraging network data analytics function and machine learning for data collection, resource optimization, security and privacy in 6G networks. *IEEE Access* **2024**, *12*, 21320–21336. [CrossRef]
26. Zaman Chowdhury, M.; Shahjalal, M.; Ahmed, S.; Jang, Y.M. 6G wireless communication systems: Applications, requirements, technologies, challenges, and research directions. *arXiv* **2019**, arXiv:1909.11315. [CrossRef]
27. Tariq, F.; Khandaker, M.R.; Wong, K.K.; Imran, M.A.; Bennis, M.; Debbah, M. A speculative study on 6G. *IEEE Wirel. Commun.* **2020**, *27*, 118–125. [CrossRef]
28. Dang, S.; Amin, O.; Shihada, B.; Alouini, M.S. What should 6G be? *Nat. Electron.* **2020**, *3*, 20–29. [CrossRef]
29. Giordani, M.; Polese, M.; Mezzavilla, M.; Rangan, S.; Zorzi, M. Toward 6G networks: Use cases and technologies. *IEEE Commun. Mag.* **2020**, *58*, 55–61. [CrossRef]
30. Letaief, K.B.; Chen, W.; Shi, Y.; Zhang, J.; Zhang, Y.J.A. The roadmap to 6G: AI empowered wireless networks. *IEEE Commun. Mag.* **2019**, *57*, 84–90. [CrossRef]
31. Fachrurrozi, N.R.; Ramli, K.; Anwar, K. Challenges on Security and Privacy in IMT-2030 (6G) Networks. In *Proceedings of the 2024 IEEE International Conference on Communication, Networks and Satellite (COMNETSAT)*; IEEE: San Francisco, CA, USA, 2024; pp. 691–698.
32. Sun, Y.; Liu, J.; Wang, J.; Cao, Y.; Kato, N. When machine learning meets privacy in 6G: A survey. *IEEE Commun. Surv. Tutor.* **2020**, *22*, 2694–2724. [CrossRef]
33. Saeed, M.M.; Saeed, R.A.; Hasan, M.K.; Ali, E.S.; Mazha, T.; Shahzad, T.; Khan, S.; Hamam, H. A comprehensive survey on 6G-security: Physical connection and service layers. *Discov. Internet Things* **2025**, *5*, 28. [CrossRef]
34. Rajesh, K.; Vetrivelan, P. Comprehensive analysis on 5G and 6G wireless network security and privacy. *Telecommun. Syst.* **2025**, *88*, 52. [CrossRef]
35. Baskar, N.; Selvaprabhu, P.; Unnikrishnan, V.M.; Chandra Babu, V.K.; Kumaravelu, V.B.; Rajamani, V.; Chinnadurai, S.; Sarker, M.A.L. Security and Privacy Issues in RIS-Based Wireless Communication Systems. In *Reconfigurable Intelligent Surfaces for 6G and Beyond Wireless Networks*; Wiley Online Library: New York, NY, USA, 2025; pp. 377–404.
36. Ahmed, M.; Soofi, A.A.; Raza, S.; Li, Y.; Khan, F.; Khan, W.U.; Asif, M.; Han, Z. A Comprehensive Survey on RIS-Enhanced Physical Layer Security in UAV-Assisted Networks. *IEEE Internet Things J.* **2025**, *12*, 32538–32562. [CrossRef]
37. Minh La, T.; Tri Nguyen, H.; Nguyen Phan, K. Examining Physical Layer Security for RIS-Aided Wireless Communication Systems. In *Reconfigurable Intelligent Surfaces for 6G and Beyond Wireless Networks*; Wiley Online Library: New York, NY, USA, 2025; pp. 499–523.
38. Cai, L.; Wang, J.; Zhang, R.; Zhang, Y.; Jiang, T.; Niyato, D.; Wang, X.; Jamalipour, A.; Shen, X. Secure physical layer communications for low-altitude economy networking: A survey. *arXiv* **2025**, arXiv:2504.09153. [CrossRef]
39. Liu, Z.; Wan, L.; Ma, Y.; Guo, J.; Guo, S.; Ma, J.; Ma, J. Establishing Trustworthy and Privacy-Preserving SAGIVNs in 6G: Architectures, Requirements, and Solutions. *IEEE Netw.* **2024**, *38*, 141–147. [CrossRef]
40. Jin, Y.; Wang, T.; Yang, Q.; Shi, L.; Zhang, S. Zero-Knowledge Federated Learning: A New Trustworthy and Privacy-Preserving Distributed Learning Paradigm. *arXiv* **2025**, arXiv:2503.15550.
41. Commey, D.; Appiah, B.; Klogo, G.S.; Crosby, G.V. ZKP-FedEval: Verifiable and Privacy-Preserving Federated Evaluation using Zero-Knowledge Proofs. *arXiv* **2025**, arXiv:2507.11649.
42. Abasi, A.K.; Aloqaily, M.; Guizani, M. 6g mmwave security advancements through federated learning and differential privacy. *IEEE Trans. Netw. Serv. Manag.* **2025**, *22*, 1911–1928. [CrossRef]

43. Chaccour, C.; Soorki, M.N.; Saad, W.; Bennis, M.; Popovski, P.; Debbah, M. Seven defining features of terahertz (THz) wireless systems: A fellowship of communication and sensing. *IEEE Commun. Surv. Tutor.* **2022**, *24*, 967–993. [CrossRef]
44. Ghourab, E.M.; Azab, M.; Gračanin, D.; Alhussein, O.; Al-Qutayri, M.; Muhaidat, S. Extended reality-aware wireless communication networks: A systematic literature review. *IEEE Open J. Commun. Soc.* **2025**, *6*, 7567–7588. [CrossRef]
45. Cevallos-Salas, D.; Estrada-Jiménez, J.; Guamán, D.S. Heuristic Techniques for Assessing Internet Privacy: A Comprehensive Review and Analysis. *Technologies* **2025**, *13*, 377. [CrossRef]
46. Paolone, G.; Paesani, R.; Pilotti, F.; Camplone, J.; Piazza, A.; Di Felice, P. Smart Lighting Systems: State-of-the-Art in the Adoption of the EdgeML Computing Paradigm. *Future Internet***2025**, *17*, 90. [CrossRef]
47. Moro-Visconti, R. The Impact of Emerging Technologies on Patent Valuation. In *Patent Valuation: Economic, Financial, and Market Approaches*; Springer: Berlin/Heidelberg, Germany, 2025; pp. 561–602.
48. Yang, M.; Qu, Y.; Ranbaduge, T.; Thapa, C.; Sultan, N.; Ding, M.; Suzuki, H.; Ni, W.; Abuadbba, S.; Smith, D.; et al. From 5g to 6g: A survey on security, privacy, and standardization pathways. *arXiv* **2024**, arXiv:2410.21986. [CrossRef]
49. Xenos, E.; Dang, S.; Armour, S.; Austin, A.; Beach, M.A. *Robust and Ubiquitous Connectivity Enabled by Unified Integrated and Secure NTN*; University of Bristol: Bristol, UK, 2025, *preprint*. [CrossRef]
50. Papageorgiou, A.; Bobev, T. *MOZAIK D5.2 Legal Toolkit*; Technical Report; CiTiP KU Leuven: Leuven, Belgium, 2025.
51. Petrosino, A. Integration of Terrestrial and Non-Terrestrial Technologies in IoT Networks. Master's Thesis, Politecnico di Bari, Bari, Italy, 2024. Available online: https://hdl.handle.net/20.500.14242/64881 (accessed on 3 April 2026).
52. Carminati, B.; Ferrari, E. Trusted Privacy Manager: A System for Privacy Enforcement. In *Proceedings of the 21st International Conference on Data Engineering Workshops (ICDEW'05)*; IEEE: San Francisco, CA, USA, 2005; p. 1195.
53. Lyimo, M.; Mgawe, B.; Leo, J.; Dida, M.; Michael, K. Adaptive Antenna for Maritime LoRaWAN: A Systematic Review on Performance, Energy Efficiency, and Environmental Resilience. *Sensors* **2025**, *25*, 6110. [CrossRef] [PubMed]
54. Kalejaiye, A.N.; Shallom, K.; Chukwuani, E.N. Implementing federated learning with privacy-preserving encryption to secure patient-derived imaging and sequencing data from cyber intrusions. *Int. J. Sci. Res. Arch.* **2025**, *16*, 1126–1145. [CrossRef]
55. Haripriya, R.; Khare, N.; Pandey, M.; Patel, S.; Choudhary, J.; Singh, D.P.; Solanki, S.; Sharma, D. FWFA: Fairness-Weighted Federated Aggregation for Privacy-Aware Decision Intelligence. *IEEE Access* **2025**, *13*, 120417–120436. [CrossRef]
56. Islam, N.; Zulkernine, M. Privacy-preserving machine learning in internet of vehicle applications: Fundamentals, recent advances, and future direction. *arXiv* **2025**, arXiv:2503.01089. [CrossRef]
57. Li, Y.; Khan, F.; Ahmed, M.; Soofi, A.A.; Khan, W.U.; Sheemar, C.K.; Asif, M.; Han, Z. RIS-based Physical Layer Security for Integrated Sensing and Communication: A Comprehensive Survey. *IEEE Internet Things J.* **2025**, *12*, 32444–32468. [CrossRef]
58. Delgado-von Eitzen, C.; Fernández Iglesias, M.J.; Anido Rifón, L.E. A GDPR-Compliant Blockchain Architecture for the Verification of Educational Credentials: Design, Implementation, and Evaluation. SSRN, 2025, *preprint*. Available online: https://ssrn.com/abstract=5366209 (accessed on 3 April 2026).
59. Abdullahi, A.D.; Bahrami, E.; Dargahi, T.; Al-Khalidi, M.; Hammoudeh, M. Interplay between Security, Privacy and Trust in 6G-enabled Intelligent Transportation Systems. *arXiv* **2025**, arXiv:2510.02487. [CrossRef]
60. Rehan, M.W.; Rehan, M.M. Survey, taxonomy, and emerging paradigms of societal digital twins for public health preparedness. *Npj Digit. Med.* **2025**, *8*, 520. [CrossRef] [PubMed]
61. Rezazadeh, F.; Kahvazadeh, S.; Mosahebfard, M. Towards quantum-enabled 6G slicing. *arXiv* **2022**, arXiv:2212.11755. [CrossRef]
62. Zhou, Z.; Chen, X.; Li, E.; Zeng, L.; Luo, K.; Zhang, J. Edge intelligence: Paving the last mile of artificial intelligence with edge computing. *Proc. IEEE* **2019**, *107*, 1738–1762. [CrossRef]
63. Masouros, D.; Soudris, D.; Gardikis, G.; Katsarou, V.; Christopoulou, M.; Xilouris, G.; Ramón, H.; Pastor, A.; Scaglione, F.; Petrollini, C.; et al. Towards privacy-first security enablers for 6G networks: The PRIVATEER approach. In *Proceedings of the International Conference on Embedded Computer Systems*; Springer: Berlin/Heidelberg, Germany, 2023; pp. 379–391.
64. Liu, Y.; Yuan, X.; Xiong, Z.; Kang, J.; Wang, X.; Niyato, D. Federated learning for 6G communications: Challenges, methods, and future directions. *China Commun.* **2020**, *17*, 105–118. [CrossRef]
65. Du, M.; Yang, P.; Liu, Y.; He, X.; Chen, M. Dp-fed6g: An adaptive differential privacy-empowered federated learning framework for 6G networks. *Digit. Commun. Netw.* **2025**, *11*, 1994–2002. [CrossRef]
66. Lin, J.C.W.; Srivastava, G.; Zhang, Y.; Djenouri, Y.; Aloqaily, M. Privacy-preserving multiobjective sanitization model in 6G IoT environments. *IEEE Internet Things J.* **2020**, *8*, 5340–5349. [CrossRef]
67. Hafi, H.; Brik, B.; Frangoudis, P.A.; Ksentini, A.; Bagaa, M. Split federated learning for 6G enabled-networks: Requirements, challenges, and future directions. *IEEE Access* **2024**, *12*, 9890–9930. [CrossRef]
68. Tan, A.Z.; Yu, H.; Cui, L.; Yang, Q. Towards personalized federated learning. *IEEE Trans. Neural Netw. Learn. Syst.* **2022**, *34*, 9587–9603. [CrossRef]
69. Mucchi, L.; Jayousi, S.; Caputo, S.; Panayirci, E.; Shahabuddin, S.; Bechtold, J.; Morales, I.; Stoica, R.A.; Abreu, G.; Haas, H. Physical-Layer Security in 6G Networks. *IEEE Open J. Commun. Soc.* **2021**, *2*, 1901–1914. [CrossRef]

70. Youn, J.; Son, W.; Jung, B. Physical-Layer Security Improvement with Reconfigurable Intelligent Surfaces for 6G Wireless Communication Systems. *Sensors* **2021**, *21*, 1439. [CrossRef]
71. Roth, S.; Sezgin, A. EMF-Constrained Artificial Noise for Secrecy Rates with Stochastic Eavesdropper Channels. *IEEE Wirel. Commun. Lett.* **2023**, *13*, 2407–2411. [CrossRef]
72. Liu, S.; Gao, T.; Liu, Y.; Lu, X. Physical-Layer Public Key Encryption Through Massive MIMO. In Proceedings of the ACM Asia Conference on Computer and Communications Security, Singapore, 1–5 July 2024. [CrossRef]
73. Guo, M.; Lin, Z.; Ma, R.; An, K.; Li, D.; Al-Dhahir, N.; Wang, J. Inspiring Physical Layer Security with RIS: Principles, Applications, and Challenges. *IEEE Open J. Commun. Soc.* **2024**, *5*, 2903–2925. [CrossRef]
74. Khalid, W.; Rehman, M.A.U.; Van Chien, T.; Kaleem, Z.; Lee, H.; Yu, H. Reconfigurable intelligent surface for physical layer security in 6G-IoT: Designs, issues, and advances. *IEEE Internet Things J.* **2023**, *11*, 3599–3613. [CrossRef]
75. Chiti, F.; Degl'Innocenti, A.; Pierucci, L. Secure Networking with Software-Defined Reconfigurable Intelligent Surfaces. *Sensors* **2023**, *23*, 2726. [CrossRef]
76. Katsanos, K.D.; Alexandropoulos, G.C. Spatial Secrecy Spectral Efficiency Optimization Enabled by Reconfigurable Intelligent Surfaces. In Proceedings of the European Signal Processing Conference, Helsinki, Finland, 4–8 September 2023. [CrossRef]
77. Zhang, J.; Du, H.; Sun, Q.; Ai, B.; Ng, D.W.K. Physical Layer Security Enhancement with Reconfigurable Intelligent Surface-Aided Networks. *IEEE Trans. Inf. Forensics Secur.* **2020**, *16*, 3480–3495. [CrossRef]
78. Li, D.; Ma, W. Enhancing NR Physical-Layer Key Generation via Beamwidth Adaptations. In Proceedings of the 7th International Conference on Information Communication and Signal Processing (ICICSP), Zhoushan, China, 21–23 September 2024. [CrossRef]
79. Kumar, R.; Arnon, S. Review of Physical Layer Security in Integrated Satellite–Terrestrial Networks. *Electronics* **2024**, *13*, 4414. [CrossRef]
80. Radojkovic, I.; Anastasov, J.; Milic, D.; Ivanis, P.; Djordjevic, G.T. Secrecy Analysis of LEO Satellite-to-Ground Station Communication System Influenced by Gamma-Shadowed Ricean Fading. *Electronics* **2025**, *14*, 293. [CrossRef]
81. An, J.; Kang, B.; Ouyang, Q.; Pan, J.; Ye, N. Covert Communications Meet 6G NTN: A Comprehensive Enabler for Safety-Critical IoT. *IEEE Netw.* **2024**, *38*, 17–24. [CrossRef]
82. Ben Yahia, O.; Erdogan, E.; Karabulut-Kurt, G.; Altunbas, I.; Yanikomeroglu, H. Physical Layer Security Framework for Optical Non-Terrestrial Networks. In Proceedings of the International Conference on Telecommunications, Alexandria, Egypt, 13–15 July 2021. [CrossRef]
83. Yan, N.; Wang, K.; Zhi, K.; Pan, C.; Chai, K.K.; Poor, H.V. Secure and Private Over-the-Air Federated Learning: Biased and Unbiased Aggregation Design. *IEEE Trans. Wirel. Commun.* **2025**, *24*, 5901–5916. [CrossRef]
84. Xue, X.; Hasan, M.K.; Yu, S.; Kandel, L.N.; Song, M. Over-the-Air Federated Learning with Enhanced Privacy. In Proceedings of the IEEE International Conference on Communications, Rome, Italy, 28 May–1 June 2023. [CrossRef]
85. Li, H.; Li, M.; Lin, Y.; Li, T.; Li, R.; Fan, X. Physical Layer Secure Transmission of AI Models in UAV-Enabled Edge AIoT. *Electronics* **2025**, *14*, 3450. [CrossRef]
86. Miao, R.; Song, Z.; Li, Y.; Li, X.; Liu, L.; Shao, G.; Wang, B. RIS-Aided Physical Layer Security with Imperfect CSI: A Robust Model-Driven Deep Learning Approach. *Entropy* **2026**, *28*, 457. [CrossRef] [PubMed]
87. Wang, H.; Yan, T.; Zhou, N.; Li, X.; Wen, F.; Du, W. Enhanced polar-domain channel estimation for near-field XL-MIMO in low-SNR scenarios. *IEEE Trans. Veh. Technol.* **2025**, *74*, 19407–19419. [CrossRef]
88. Mao, J.; Yin, T.; Yener, A.; Liu, M. Leveraging the Physical Layer for Differential Privacy in Over-the-Air Federated Learning. In Proceedings of the IEEE International Conference on Communications, Denver, CO, USA, 9–13 June 2024. [CrossRef]
89. Seif, M.; Tandon, R.; Li, M. Wireless Federated Learning with Local Differential Privacy. *arXiv* **2020**. [CrossRef]
90. Zhang, H.; Yang, C.; Dai, B. When Wireless Hierarchical Federated Learning Meets Physical Layer Security: A Finite Blocklength Approach. *arXiv* **2022**. [CrossRef]
91. Gonzalez, P.; Alhamed, F.; Shakespear-Miles, H.; Barzegar, S.; Paolucci, F.; Sgambelluri, A.; Olmos, J.V.; Ruiz, M.; Velasco, L. Near-real-time 6G service operation enabled by distributed intelligence and in-band telemetry. *J. Opt. Commun. Netw.* **2025**, *17*, A247–A258. [CrossRef]
92. Bazzi, A.; Chafii, M. Low dynamic range for ris-aided bistatic integrated sensing and communication. *IEEE J. Sel. Areas Commun.* **2025**, *43*, 912–927. [CrossRef]
93. Rasheed, I.; Mostafa, H. Federated learning-based anomaly detection for zero-day attack prevention in 6G network slices. *Comput. Netw.* **2025**, *268*, 111376. [CrossRef]
94. Chen, C.; Liao, T.; Deng, X.; Wu, Z.; Huang, S.; Zheng, Z. Advances in Robust Federated Learning: A Survey with Heterogeneity Considerations. *IEEE Trans. Big Data* **2025**, *11*, 1548–1567. [CrossRef]
95. Larrucea, X.; Moffie, M.; Asaf, S.; Santamaria, I. Towards a GDPR compliant way to secure European cross border Healthcare Industry 4.0. *Comput. Stand. Interfaces* **2020**, *69*, 103408. [CrossRef]
96. S, V.; Manoharan, R.; Ramachandran, S.; Rajasekar, V. Blockchain Based Privacy Preserving Framework for Emerging 6G Wireless Communications. *IEEE Trans. Ind. Inform.* **2022**, *18*, 4868–4874. [CrossRef]

97. Bariah, L.; Mohjazi, L.; Abumarshoud, H.; Selim, B.; Muhaidat, S.; Tatipamula, M.; Imran, M.A.; Haas, H. RIS-Assisted Space-Air-Ground Integrated Networks: New Horizons for Flexible Access and Connectivity. *IEEE Netw.* **2023**, *37*, 118–125. [CrossRef]
98. Han, D.; Liu, Y.; Cao, R.; Gao, H.; Lu, Y. A lightweight blockchain architecture with smart collaborative and progressive evolution for privacy-preserving 6G IoT. *IEEE Wirel. Commun.* **2024**, *31*, 148–154. [CrossRef]

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