Toward Autonomous 6G Networks: A Trust-Centric and Privacy-Preserving Framework

Jugnu Mohinder Singh Manhas[1], Aruna Pavate[1], Sureshkumar M. S.[2]

[1] Department of Information Technology, Thakur College of Engineering and Technology, Maharashtra, India
[2] Department of Polymer Technology and Engineering, Harare Institute of Technology, Harare, Zimbabwe

Corresponding author: arunaapavate@gmail.com

ABSTRACT: The move towards sixth-generation networks poses unprecedented challenges in terms of security, trust, and privacy due to the integration of artificial intelligence, Internet of Things, and global communication networks. In this context, this paper aims to provide an exhaustive systematic literature review of existing 6G research with existing trust models proposed by the International Telecommunication Union (ITU-T) and analyze the interrelated relationship between privacy preservation, energy efficiency, and autonomous systems. This research is based on an exhaustive analysis of existing peer-reviewed articles from 2020 to 2026, white papers, and existing frameworks. It is evident from this analysis that existing research is largely focused on the individual optimization of privacy preservation, energy efficiency, and autonomous systems, leading to an inherent trade-off. This paper aims to provide an exhaustive framework for integrating privacy preservation, energy efficiency, and autonomous systems as pillars of 6G networks. Key findings include that Edge Intelligence, Federated Learning, Zero Trust Architecture, and Post-Quantum Cryptography act as key enablers in meeting these often conflicting requirements. The study concludes by identifying 12 distinct research gaps and suggesting future directions toward cooperative, AI-driven, and quantum-resistant trust architectures for 6G. This study contributes to the SAMRNET (Security, Architecture, Management, and Resilience of NETworks) research agenda by establishing a comprehensive foundation for trust-centric 6G network design.

Keywords: Zero Trust Architecture, Federated Learning, Post-Quantum Cryptography, Autonomous Networks, Edge Intelligence.

I. INTRODUCTION

1. BACKGROUND AND MOTIVATION

This evolution of mobile networks has always emphasized the provision of more complex and sophisticated services, higher data transmission speeds, and lower service response times. The evolution from fourth-generation (4G) to fifth-generation (5G) networks was a significant paradigm shift toward a data-centric and service-centric approach, allowing for the provision of Enhanced Mobile Broadband (eMBB), Ultra-Reliable Low Latency Communication (URLLC), and Massive Machine-Type Communication (mMTC) services. However, as the evolution of 5G networks toward a Sixth Generation of networks reveals, this may not be sufficient for the provision of future intelligent and immersive services that require unprecedented levels of intelligence, context, and trust. The evolution of 6G networks, as recent studies reveal, will transcend traditional telecommunication connectivity paradigms.

The most significant difference between the evolution of 6G networks and that of previous generations, such as 5G, is that it will be "AI-native, autonomous, and context-aware," supporting revolutionary applications such as Holographic Communications, Digital Twins, Extended Reality, Autonomous Mobility, and massive collaborative artificial intelligence. More importantly, intelligence will be incorporated into all

layers of the network, and communication, computation, sensing, and control will be combined into a single architectural entity. Although this promises significant improvements in terms of performance and flexibility, it also poses significant challenges that need to be explored.

2. THE PROBLEM: FRAGMENTED APPROACHES TO INTERDEPENDENT CHALLENGES

Current research findings indicate that a performance-centric approach alone cannot ensure the sustainability and integrity of 6G networks [5], [12]. With the accelerating adoption of generative AI, AI agents, and continuous learning in 5G-Advanced and future networks, concerns regarding massive data collection, reliance on centralized intelligence, and escalating computational requirements are mounting [5], [12]. Research suggests that centralized AI training and control increase risks of privacy breaches, Cyberattack vulnerabilities, and potential single points of failure within network infrastructure [6], [16], [21].

Energy efficiency is another key bottleneck in AI-based telecommunication systems. While the benefits of AI-based system operation are significant, the carbon footprint of AI-based system operations, if not properly addressed, could pose a significant challenge, as discussed in the Green AI literature [53], [54]. Research has shown that AI-based workload management using cloud-edge AI platforms has the potential to save energy; hence, energy efficiency is crucial in the design of AI-based systems, not as an afterthought but as a fundamental requirement, as discussed in the literature [29], [30], [39].

Autonomous network control represents another key component of 6G system architecture. AI-aided Self-Configuration, Self-Optimization and Self-Healing have proved their performance gains in terms of efficiency and interference management in 5G systems [3], [4], [17]. Yet, overreliance on autonomous control, in the absence of sufficient transparency, governance, and explainability, gives rise to serious concerns about accountability, legal compliance, and ethical decision-making in AI systems [6], [14]. Industry and regulatory literature underscores the importance of responsible AI deployment to foster trust in digital technologies and encourage the social acceptability of future communication systems [8], [9], [14].

3. RECENT ADVANCES AND EMERGING SOLUTIONS (2020-2026)

The period between 2020 and 2026 has seen remarkable research progress in tackling the co-occurring issues in 6G network security, privacy, and trust. The noteworthy research conducted topics includes:

- Zero-Trust Architecture (ZTA) Integration: Zero-Trust Architecture is a foundation for security in 6G network. The National Institute of Standards and Technology (NIST) Special Publication 800-207 has formalized ZTA frameworks, and subsequent studies have applied these concepts to 6G edge networks in various works, e.g. [49] and [50]. El-Hajj has presented a zero-trust and Federated Learning Framework for O-RAN Optimization achieving 89% reduction in attempts by unauthorized users and 32% in terms of energy savings [36].
- (ii) Federated Learning for Privacy Preservation: Federated Learning has emerged as an important enabler of distributed intelligence with privacy preservation in 6G networks. Research by Ye et al. in 2022 proposed trusted architectures with graph-based analysis for 6G networks [37]. Asad et al. proposed Zero-Trust-Based Federated Learning frameworks for URLLC in Vehicular Networks. Federated Learning-based Decentralized Adaptive Intelligent Transmission Protocol (AITP) achieved 12.2% improvement in throughput and 27% improvement in energy efficiency with Privacy budgets of $\varepsilon \approx 1.75$ [52].
- (iii) Post-Quantum Cryptography (PQC): In light of quantum computing attacks on classical cryptography, researchers have proposed post-quantum cryptography solutions for 6G networks. In 2024, the National Institute of Standards and Technology (NIST) announced three post-quantum cryptography standards [33]:
- FIPS 203 (CRYSTALS-Kyber),
- FIPS 204 (CRYSTALS-Dilithium), and
- FIPS 205 (SPHINCS+).
- A fourth standard, FALCON, is expected in 2025. CONFIDENTIAL6G project [41] and iTrust6G project [40] are working on developing frameworks for 6G networks with Post-Quantum Cryptography [43].

Quantum robust algorithms are known as Post-Quantum Cryptography (PQC) algorithms, which are considered to remain stable even after the arrival of functional large-scale quantum computing machines as shown in Figure 1 as follows, [68].

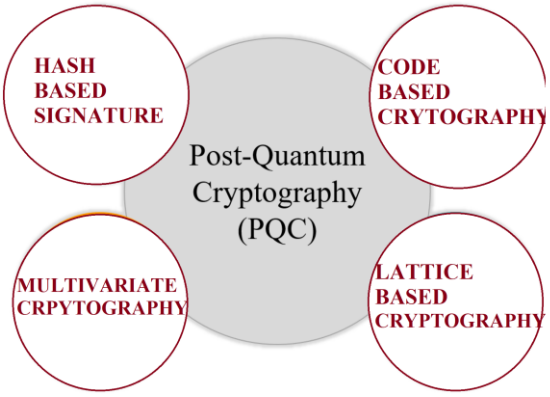

FIGURE 1 Basic types of Post-Quantum Cryptography (PQC) [68]

Confidential Computing and Privacy Technologies: The CONFIDENTIAL6G project [41] has led to significant advancements in confidential computing enablers, such as FHE optimization for AI applications, SMPC protocols, and TEE abstractions. This helps in ensuring the confidentiality of data in use, in transit, and at the edge.

AI-Driven Trust Orchestration: The iTrust6G project [40] has proposed intelligent trust and security orchestration frameworks that utilize AI for threat detection, trust determination, and security policy enforcement in distributed cloud environments.

4. RESEARCH GAP AND CONTRIBUTION

Although there is significant research on various dimensions of Privacy-Preserving Learning [7], [47], [48], Green Networking [19], [34], [35], Autonomous Control [3], [4], [17], as well as emerging areas such as ZTA [46], [49], PQC [46], and Confidential Computing [41], most of the existing research focuses on individual dimensions of 6G trust. It is imperative to integrate all of these technologies to form a comprehensive framework that addresses all three dimensions of 6G trust. ITU-T trust frameworks [1], [2] lay the foundation. This needs to be integrated with emerging technologies to address the complex nature of 6G trust requirements. This paper addresses this critical research gap by providing:

- Comprehensive Literature Synthesis (2020-2026): This study covers research on latest advancements in Zero Trust Architecture, Federated Learning, Post-Quantum Cryptography and Confidential Computing.
- Interdependency Analysis: At present in 6G, there exist trade-offs and interdependencies between Privacy, Energy Efficiency and Autonomy Dimensions.
- Unified Architectural Vision: Proposed unified framework having Core Pillars as Privacy based Data Management, Energy-Efficient AI and transparent Autonomous Systems.
- Research Gap Identification: Listing of twelve research gaps for future research.
- Future Research Roadmap: Listing ten future research directions in alignment with the proposed research agenda of SAMRNET.

5. PAPER ORGANIZATION

The remaining part of this paper is organized as follows:

Section 2 presents Background and Related Work. Section 3 describes the research methodology. Section 4 analyzes centralized AI systems in 6G. Section 5 discusses interdependencies and trade-offs. Section 6

presents findings and observations. Section 7 identifies research gaps. Section 8 proposes future research directions. Section 9 concludes the paper.

II. BACKGROUND AND RELATED WORK

1. EVOLUTION FROM 5G TO 6G

The advancement from 5G to 6G wireless communication systems signifies a revolution from connectivity-centric architectures to AI-native, intelligent, and autonomous systems. 5G facilitates eMBB, URLLC and mMTC services. Iintelligence in 5G is centralized, cloud-centric, with limited flexibility in the edge network [1], [5].

Recent research highlights the significance of the integration of intelligence in 6G devices, Edge and Core Networks that can proactively manage itself, rather than merely reacting to changes in networks, services, or environments [5], [6].

Increased complexity in handling and updating the intelligence and making decisions, taking into account issues like energy consumption, scalability, and management in 6G networks due to the diversity of components in 6G networks [8], [9].

The Open Radio Access Network (O-RAN) paradigm is recognized as an essential technology for 6G flexibility. It also presents significant security challenges due to its disaggregated and AI-driven nature [34], [46], [49]. The RAN Intelligent Controllers (RICs) and xApps/ rApps are security challenges that need to be addressed. Research conducted by El-Hajj in reference [36] identified threat models for the optimization process in O-RANs, which include attacks like Adversarial Machine Learning attacks on resource allocation models and third-party applications.

2. CORE PRINCIPLES OF 6G ARCHITECTURE

- Researchers have advocated Privacy-First Data Management. 5G uses data heads in central hubs for Training AI and storing sensitive info risking data safety/ legality. 6G uses Federated Learning, Edge Intelligence and Decentralized Data. This keeps raw data close to where it's created and processed at the Edge. This builds a layer of Trust. It is compliant with privacy regulations like GDPR and the EU's AI Act thereby being a part of the Core Design [8], [9].
- Federated Learning has made significant progress in terms of privacy in recent times. Researchers are discovering new ways to deal with inconsistent data, reduce communication costs and train robust models that are resistant to attacks. To illustrate this, the AITP protocol leverages differential Privacy with $\varepsilon \approx 1.75$ to ensure Privacy without compromising model accuracy [52].

Inorder to be sustainable 6G, its energy efficiency has to be based on green AI [53], [54]. 6G must design more efficient models and balance workload between Cloud and Edge devices.

- AI-Driven Autonomy with Governance represents a the ability to enable 6G networks to achieve Self-Configuration, Self-Optimization, and Self-Healing properties [3], [4], [6], [17]. 5G networks utilize human-assisted/semi-automated optimization methods for resolution. 6G aims to utilize AI-native autonomous resolution methods [3], [4], [5], [12]. The iTrust6G project has created an AI-driven Trust Management Systems, where continuous assessment, risk evaluation, and generation of cyber threat intelligence are conducted [40].

The research conducted by El-Hajj [36] indicates that Zero-Trust Federated Learning Frameworks decrease energy consumption by 32% simply by employing dynamic DU sleep scheduling. It limits latency degradation to less than 5%, with attackers in the mix. The AITP framework improves energy efficiency by 27% over Centralized Models [52].

Autonomy leads to reduced operational costs and latency. Explainability, auditability and focus of control processes is necessary for reliable and accountable systems. Zero-Trust Principles offers strong governance models for Autonomous Systems due to its emphasis on continuous verification and policy enforcement [48], [49].

3. EMERGING TECHNOLOGICAL ENABLERS

- Zero-Trust Architecture (ZTA)Zero Trust Architecture has been identified as a key security foundation for 6G networks. The National Institute of Standards and Technology Special Publication 800-207 [48] codified the principles of ZTA, focusing on continuous verification, micro-segmentation, and least privilege access. Ramezanpour and Jagannath [34] proposed Intelligent Zero Trust Architecture Frameworks for 5G/6G networks with O-RAN integration support. Sedjelmaci and Ansari [50] presented Zero Trust Architecture-Empowered Attack Detection Frameworks for 6G Edge Computing Networks.

Recent implementations have validated the applicability and effectiveness of Zero Trust Architecture in 6G networks [36], [40]. El-Hajj [36] proved that Zero Trust Architecture decreases unauthorized RIC access by 89% in comparison with traditional O-RAN security standards. The iTrust6G project [40] has successfully implemented Zero Trust Architecture principles in three-tier architectures with multi-domain collaboration, trust management, and infrastructure resource supervision capabilities. The Figure below shows - High-level architecture identifying iTrust6G's Security Enablers [40] made of 3 tier architecture across User equipment, Edge and Cloud Computing resources.

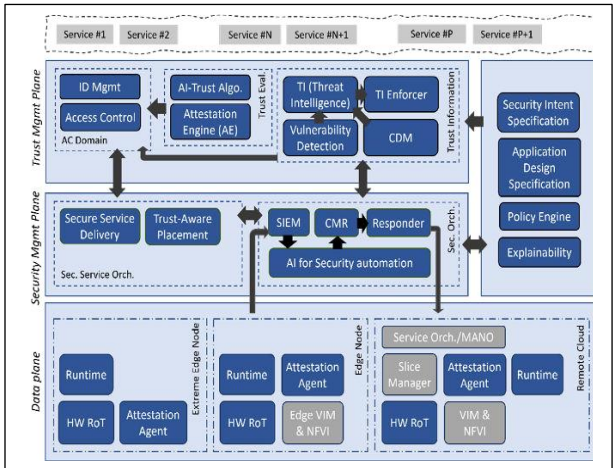

FIGURE 2: High-level architecture identifying iTrust6G's Security Enablers [40]

- Federated Learning for Privacy Preservation

Federated Learning has emerged as a critical privacy-preserving distributed intelligence. It has overcome tough hurdles on the road to 6G [37], [38]:

- Data Heterogeneity: Xiong at al [39] designed privacy-preserving Federated Learning schemes that handle issues like different dataset sizes and uneven category distributions. They used a Threshold Paillier Cryptosystem to enable weighted aggregation.
- Communication Efficiency: The AITP framework [52] blends local SGD with differential privacy and secure aggregation. It scales up to 500 devices smoothly, and performance only drops slightly as the number of users grows.
- Adversarial Resilience: El-Hajj [36] tested Federated Learning Frameworks against data poisoning attacks hitting 15% of users. The system delivered 32% energy savings and saw less than 5% more latency.
- Trust Integration: Ye et al. [37] introduced Trusted Architectures using Graph-Based Analysis for Federated Learning in 6G environments. Asad et al [38] pushed for Zero-Trust Federated Learning to support Ultra-Reliable Low-Latency Communications (URLLC) in vehicular networks. Figure 3 below shows Envisioned FL for ubiquitous intelligence in 6G networks with privacy preservation in multi-domain, multi-tenancy, and multi-access technology (AT) scenarios [63].

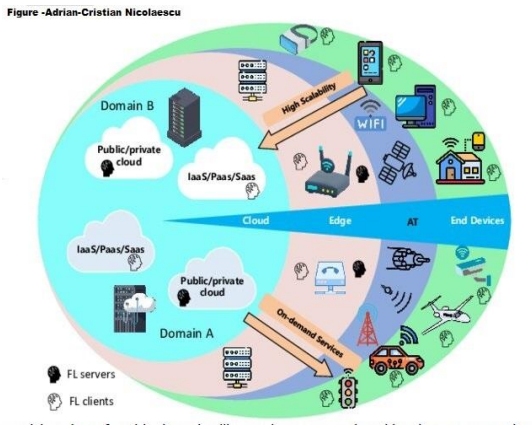

FIGURE 3 Envisioned FL for ubiquitous intelligence in 6G networks [63]

4. REVIEW OF EXISTING STUDIES

Research on Privacy Preservation, Energy Efficiency, and Autonomous Networking is progressing in different research communities:

- Privacy-Focused Research: Federated learning [31], [32], [55], [60], differential privacy [55], [63], homomorphic encryption [62], and zero-knowledge proofs (ZKP) [57] have made significant advances in improving the capabilities of Privacy Preservation.
- Energy-Focused Research: Green AI [53], [54], Cloud-Edge Workload Management [34], [35], and Energy-Aware Model Design [46] have shrunk power requirements.
- Autonomy-Focused Research: Open RAN architectures [46], [49], AI-native Network Management [3], [4], [17], and Zero-Trust Governance [48], [49], [50] have created pathway for Autonomous Controls.
- CONFIDENTIAL6G [41] and iTrust6G [40] projects are important milestones towards the realization of integrated security, privacy, and trust frameworks. These EU-funded projects are establishing comprehensive architectures that consider multiple aspects simultaneously.
- The ITU-T trust frameworks [1], [2] lay the groundwork for Trustworthy Networking. These must be extended to integrate with new technologies.

Very few research works have comprehensively explored the relationships between Privacy, Energy Efficiency and Autonomy within the scope of unified frameworks that consider ZTA, FL and PQC.

III. RESEARCH METHODOLOGY

1. DATA COLLECTION STRATEGY

The data collection was carried out by reviewing peer-reviewed research articles, industry white papers, journals, publications and international standards documents predominantly from 2020 to 2026

1.1 Academic Literature Sources

The academic literature sources were collected from reliable digital libraries such as IEEE Xplore, ACM Digital Library, Elsevier ScienceDirect, MDPI, Springer, etc. The search terms used were "6G Security," "6G Privacy," "Zero Trust Architecture," "Federated Learning 6G," "Post-Quantum Cryptography 6G," "Confidential Computing 6G," "Autonomous Networks," "Green AI" [53], [54], and "Edge Intelligence."

1.2 Industry and Regulatory Sources

Industry perspectives were included by using white papers from 6G Flagship [5], Next G Alliance [44], GSMA [46], and telecommunication forums. Regulatory perspectives were included by using analysis of various frameworks like GDPR [14], EU AI Act, NIST publications [48], and ITU-T recommendations [1], [2], [15].

2. INCLUSION AND EXCLUSION CRITERIA

Mostly English-language technical publications from 2020-2026 were considered in the analysis. The inclusion criteria were based on whether the publication discussed atleast one of the following: Privacy Preservation, Energy Efficiency, Autonomous Control, Zero-Trust Architecture and Federated Learning within 5G/ 6G context. Opinion-based publications were excluded.

3. THEMATIC ANALYSIS PROCEDURE

A multi-stage thematic analysis was conducted:

- Stage1: Initial Classification. Papers were grouped according to Primary Focus Area (Privacy, Energy, Autonomy, ZTA, FL) and Secondary Focus Areas.
- Stage2: Cross-Domain Mapping: Relationships between dimensions were analysed to identify trade-offs, synergies, and integration patterns.
- Stage3: Emerging Technology Analysis: Recent advances in ZTA and FL were mapped to architectural requirements.
- Stage4: Gap Identification: Combined findings were compared against comprehensive requirements for 6G trust architectures.

4. METHODOLOGICAL LIMITATIONS

As 6G is still in the pre-standardization phase, this study is based primarily on Secondary Sources. Experimental validation and industry based interactions with hierarchies may be done in future research.

IV. CENTRALIZED 6G AI SYSTEMS: PRIVACY, ENERGY, AND AUTONOMY CHALLENGES

Centralized AI training involves massive data collection, which raises serious issues related to data privacy and energy consumption. Although centralized intelligence improves global optimization capabilities, it creates single points of failure and increases the attack surface [5], [12], [16].

1. DATA PRIVACY CHALLENGES FOR AI TRAINING IN 6G NETWORKS

6G networks will require enormous amounts of contextual, sensory, and behavioral data. The existing cloud-based paradigm aggregates sensitive user and network data to perform centralized AI model training, which creates hotspots for privacy breaches [1], [5], [7]. Studies have highlighted the following specific privacy risks: membership inference attack, model inversion attack[35], and gradient leakage [45].

In order to reduce the aforementioned challenges, the following methods are proposed: Federated Learning [47], [48], Edge Inference [34], [35], Differential Privacy and Homomorphic Encryption. The AITP framework [52] showed the potential of achieving strong privacy guarantees with $\varepsilon \approx 1.75$ while preserving the performance of the model. The FPDGD-AM framework used the Noise-Adding Clipping Techniques according to the Theory Of Differential Privacy.

2. ENERGY EFFICIENCY AND SUSTAINABILITY FOR AI COMPUTE ENVIRONMENTS

According to the green AI studies, the energy demands related to AI are predicted to rise significantly [53],[54]. Data centers and communication networks are the primary sources of energy consumption. El-Hajj [36] showed the potential of achieving 32% energy saving through the use of the Zero Trust Federated Learning Approach by applying the Dynamic DU Sleep Scheduling Technique. The AITP framework [52] showed the potential of achieving 27% energy efficiency improvement compared with the centralized approach.

3. AUTONOMY AND INTELLIGENT CONTROL

On the one hand, autonomous networking is one of the fundamental pillars of 6G networks -, facilitating the implementation of Self-Configuration, Self-Optimization and Self-Healing functionalities [5]. The research on Open RAN control frameworks and intelligent interference auto-optimization suggests that the application of AI-based autonomy is capable of greatly improving the efficiency and quality of operations.

On the other hand, the adoption of Open RAN architectures and RICs also raises new security and governance challenges. For example, the central intelligence elements used in Open RAN architectures are capable of developing into potential Single Points Of Failure or Attack, especially when not properly addressed from the security perspective [7]. Absence of adequate transparency is capable of significantly exacerbating the risks associated with erroneous decision-making, security breaches and non-compliance with relevant regulatory requirements. Therefore, the governance of autonomous 6G networks must be addressed through techniques that are explainable, energy-conscious, as well as privacy-preserving.

V. INTERDEPENDENCIES AND TRADE-OFFS: A SYSTEMS PERSPECTIVE

The study observes strong links between Privacy, Energy Efficiency and Autonomy.

1. PRIVACY-AUTONOMY TRADE-OFF

Autonomous AI systems require a significant volume of data for proper learning. However, data collection is a major cause of privacy risks [1], [5], [7]. Data protection mechanisms such as federated learning [36], [37], [38], [39] may also cause a rise in computational overhead [7]. The AITP framework [52] showed that differential privacy mechanisms achieve a level of $\varepsilon \approx 1.75$ for a 7% computational overhead.

2. ENERGY EFFICIENCY-AUTONOMY TRADE-OFF

The efficiency provided by AI-based automation comes with a higher computational demand [34], Real-time autonomous decision-making necessitates continuous model inference. Energy-aware autonomy techniques, such as those presented in [46], show how this trade-off can be managed.

3. PRIVACY-ENERGY EFFICIENCY TRADE-OFF

Computation-intensive nature of privacy-preserving techniques boosts energy consumption [7], [19]. Light cryptography techniques, hardware acceleration, and green protocol design offer mitigation strategies.

4. TOWARD UNIFIED OPTIMIZATION

Privacy, Energy Efficiency and Autonomy interdependencies require a joint optimization process. (i) The principles of zero trust [48], [49], [50] offer governance frameworks.

- Distributed intelligence is provided by federated learning.
- Post-quantum cryptography is required for long-term security.

The iTrust6G [40] and CONFIDENTIAL6G [41] projects are examples of an integrated approach that considers multiple facets simultaneously.

VI. FINDINGS AND OBSERVATIONS

On thorough reading and studying the following important findings can be derived:

- Finding 1: Integrated Design Requirements: It is important to integrate Performance, Sustainability and Trust into the design requirements for 6G [1], [2], [5], [12]. Zero Trust Architecture [48] and confidential computing [6] can serve as the basis for integrated trust.
- Finding 2: Fundamental Interdependence: Privacy, Energy Efficiency and Autonomy are fundamentally interdependent [5], [6], [12], [19]. Recent integrated frameworks [46] show the potential for simultaneous optimization.
- Finding 3: Zero Trust as Governance Framework: Zero trust principles [48], [49], [50] can serve as the basis for governance in the context of autonomous systems. It is possible to achieve a reduction in unauthorized access by 89% [46].
- Finding 4: Federated Learning Maturity: Federated Learning can address the requirements for 6G viz. Data Heterogeneity [31], [32], [37], [39], [42], Communication Efficiency, Adversarial Resilience [46], and Trust Integration [6], [7].
- Finding 5: Post-Quantum Readiness: NIST PQC standards [43] can serve as the basis for the Security Architecture in 6G. Integration frameworks for the standards are being developed [19], [20].

- Finding 6: EU-Funded Integrated Projects.: CONFIDENTIAL6G [41] and iTrust6G [40] show the way to the future with the recent initiatives towards Integrated Security, Privacy and Trust.
- Finding 7: Edge Intelligence as Unifying Enabler: Edge intelligence [34], [35] can enhance Privacy, Energy Efficiency and Autonomy.

Table 2. Mapping of paper sections to representative literature.

KEY REFERENCES	SECTION	FOCUS AREA	CONTRIBUTION
[5], [12], [16]	2.1	Evolution from 5G to 6G	Establishes technological evolution and architectural requirements
[1], [2], [5], [48]	2.2	Core Principles	Identifies core architectural dimensions and ZTA integration
[19],[31], [32],[37], [46], [49], [50],	2.3	Emerging Technologies	Documents ZTA, FL, and PQC advances
[40],[41]	2.4	Integrated Initiatives	Highlights EU-funded integrated research projects
[5], [6], [12], [16], [21]	4	Centralized AI Systems	Demonstrates risks of centralized intelligence
[7], [39]	4.1	Privacy Challenges	Supports transition to privacy-preserving mechanisms
[34], [35], [46], [53], [54]	4.2	Energy Efficiency	Establishes Green AI principles with empirical validation
[3], [4], [6], [17], [46]	4.3	Autonomy	Highlights autonomous control with governance
[7], [19], [34], [46]	5	Interdependencies	Demonstrates interconnected nature and joint optimization
[1], [2], [5], [6], [12], [19], [46], [48]	6	Findings	Synthesizes findings into actionable design principles

VII. FUTURE RESEARCH DIRECTIONS

This study identifies the important research gap areas as follows:

GAP ID	GAP FOUND IN RESEARCH	DESCRIPTION	REFERENCES
1	ITU Trust Model Implementation with Emerging Tech	ITU-T Y.3052 [1] and Y.3053 [2] require integration with ZTA [48], FL [37], and PQC [19] for 6G contexts	[1], [2] [31], [32], [37], [39], [42]
2	AI Explainability for Autonomous Trust	Explainable AI for trust decisions in autonomous networks should be developed	[1], [2]
3	Multi-Domain Trust Propagation	Trust propagation across heterogeneous network domains with multilevel security	[6], [17]
4	Energy-Aware Privacy Mechanisms	Optimisation required for Privacy-preserving techniques (DP, FL) to reduce energy consumption	[31], [32], [37], [39], [42], [44]
5	Regulatory-Technical Alignment	Evolving regulatory requirements should be aligned with technical security controls mechanisms	[8], [9], [14], [35]
6	Unified ZTA-FL-PQC Framework	Unified framework integrating ZTA, FL, and PQC with Privacy-Energy-Autonomy requirements	[46], [48]
7	O-RAN Security Standardization	O-RAN multi vendor architecture can cause security vulnerabilities requiring standardized counter measures [46]; across the architecture	[35], [46], [49]
8	Real-World Deployment Validation	Standardised 6G testbed validation for integrated frameworks	[46]
9	AI Attack Resilience	Framework to counter Adversarial ML attacks in 6G AI-native networks	[35], [46]
10	Quantum-Safe Transition Strategies	Hybrid classical-quantum cryptographic approaches require standardization for phased 6G deployment	[19], [20], [40], [43]
11	Federated Learning Data Heterogeneity	FL [37] partially address data heterogeneity; robust model required	[31]. [32], [37], [39], [42]
12	Confidential Computing for Constrained Devices	TEE and FHE optimization for resource-constrained edge/ IoT devices requires further research	[44], [45], [51]

VIII. CONCLUSION

This paper performed a systematic literature review to explore the intersection of Privacy Preservation, Energy Efficiency and Autonomous Control in 6G networks.

There are many EU-funded projects, which are driving forward Integrated Security, Privacy and Trust Models forward. Edge Intelligence, Federated Learning and Zero-Trust Governance seem to be emerging as must-haves in Next-Gen Networks.

To deliver robust, trustworthy, and sustainable 6G, we need to develop integrated architectures that combine Privacy-Preserving Data Management, Energy-Efficient AI, Transparent Autonomous Systems and Quantum-Resistant Cryptography.

IX. ACKNOWLEDGEMENTS

The author(s) would like to acknowledge the researchers and institutions whose work on 5G, 6G, Green AI, Federated Learning, Zero Trust Governance, Autonomous Systems , Quantum resistant Cryptography and intelligent network optimization provided the foundation for this study. We thank the Staff, Faculty and Mentor for their immense support and guidance.

REFERENCES

1. International Telecommunication Union, "ITU-T Recommendation Y.3052: Overview of trust provisioning in ICT infrastructures and services," ITU-T, Geneva, Switzerland.
2. International Telecommunication Union, "ITU-T Recommendation Y.3053: Framework of trustworthy networking," ITU-T, Geneva, Switzerland.
3. R. Kantola, J. Llorente Santos, and N. Beijar, "Policy-based communications for 5G mobile networks with customer edge switching," Security and Communication Networks, vol. 8, no. 18, pp. 3595-3610, 2015, doi: 10.1002/sec.1197.
4. H. Kabir, H. Mohsin, and R. Kantola, "Security policy management for 5G customer edge nodes," in Proc. IEEE/IFIP Network Operations and Management Symposium (NOMS), Budapest, Hungary, Apr. 2020, pp. 1-6, doi: 10.1109/NOMS47738.2020.9110321.
5. University of Oulu, "Key drivers and research challenges for 6G ubiquitous wireless intelligence," 6G Flagship, White Paper, 2019. [Online]. Available: https://www.6gflagship.com/key-drivers-and-research-challenges-for-6g-ubiquitous-wireless-intelligence/
6. Z. Yan, R. Kantola, and Y. Shen, "Unwanted traffic control via hybrid trust management," in Proc. IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), Liverpool, UK, Jun. 2012, pp. 1-8, doi: 10.1109/TrustCom.2012.213.
7. Z. Yan, P. Zhang, and A. V. Vasilakos, "A survey on trust management for Internet of Things," Future Generation Computer Systems, vol. 79, pp. 820-830, Feb. 2018, doi: 10.1016/j.future.2017.02.043.
8. European Union, "Regulation (EU) 2015/2120 of the European Parliament and of the Council of 25 November 2015 laying down measures concerning open internet access," Official Journal of the European Union, L 310, pp. 1-18, Nov. 2015.
9. Body of European Regulators for Electronic Communications (BEREC), "BEREC guidelines on the implementation of the open internet access rules," BoR (16) 127, Aug. 2016. [Online].
10. Available: https://berec.europa.eu/eng/document_register/subject_matter/berec/regulatory_best_practices/guidelines/6161-berec-guidelines-on-the-implementation-of-the-open-internet-access-rules
11. S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf
12. Y. Lu, X. Huang, Y. Dai, S. Maharjan, and Y. Zhang, "Blockchain and deep reinforcement learning empowered 5G beyond," IEEE Network, vol. 33, no. 3, pp. 10-17, May/Jun. 2019, doi: 10.1109/MNET.2019.1800547.
13. M. Giordani, M. Polese, M. Mezzavilla, S. Rangan, and M. Zorzi, "A vision of 6G wireless systems: Applications, trends, technologies, and open research problems," IEEE Network, vol. 34, no. 3, pp. 134-142, May/Jun. 2020, doi: 10.1109/MNET.001.1900287.
14. 3rd Generation Partnership Project (3GPP), "Security architecture and procedures for 5G system," Technical Specification 33.501, Version 16.1.0, Jul. 2020. [Online]. Available: https://www.3gpp.org/ftp/Specs/archive/33_series/33.501/
15. European Union, "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)," Official Journal of the European Union, L 119, pp. 1-88, May 2016.
16. International Telecommunication Union, "ITU-T X.5Gsec-t (TR.5Gsec-bsf): Built-in security for 5G networks," Technical Report, ITU-T, Geneva, Switzerland.
17. D. Basin, J. Dreier, L. Hirschi, S. Radomirovic, R. Sasse, and V. Stettler, "Overview of 5G security in 3GPP," in Proc. IEEE Conference on Standards for Communications and Networking (CSCN), Helsinki, Finland, Sep. 2017, pp. 1-6, doi: 10.1109/CSCN.2017.8088619.

18. M. A. Ferrag, L. Maglaras, A. Argyriou, D. Kosmanos, and H. Janicke, "Security for 5G and beyond networks: A survey," IEEE Communications Surveys & Tutorials, vol. 21, no. 4, pp. 3682-3722, Fourth Quarter 2019, doi: 10.1109/COMST.2019.2916180.
19. W. Stallings, A Comprehensive Guide to 5G Security. Hoboken, NJ, USA: Wiley, 2019.
20. D. J. Bernstein and T. Lange, "Post-quantum cryptography," Nature, vol. 549, pp. 188-194, Sep. 2017, doi: 10.1038/nature23461.
21. M. A. Nielsen and I. L. Chuang, "Quantum computing and quantum information," Computer Science Review, vol. 12, pp. 1-20, May 2018, doi: 10.1016/j.cosrev.2018.11.002.
22. J. Hoffstein, J. Pipher, and J. H. Silverman, "NTRU: A ring-based public key cryptosystem," in Algorithmic Number Theory (ANTS III), J. P. Buhler, Ed. Berlin, Germany: Springer, 1998, pp. 267-288.
23. R. J. McEliece, "A public-key cryptosystem based on algebraic coding theory," JPL Deep Space Network Progress Report, vol. 42-44, pp. 114-116, 1978.
24. R. Moskowitz, T. Heer, P. Jokela, and T. Henderson, "Host Identity Protocol (HIP): Architecture and applications," IEEE Communications Surveys & Tutorials, vol. 12, no. 3, pp. 402-420, Third Quarter 2010, doi: 10.1109/SURV.2010.021110.00070.
25. X. Zhou, S. Yan, Q. Wu, and R. Q. Hu, "Intrinsic secrecy in inhomogeneous wireless networks," IEEE/ACM Transactions on Networking, vol. 27, no. 4, pp. 1528-1541, Aug. 2019, doi: 10.1109/TNET.2019.2922112.
26. A. Mukherjee, "Physical layer security in IoT networks," Sensors, vol. 20, no. 12, p. 3456, Jun. 2020, doi: 10.3390/s20123456.
27. D. Adrian et al., "Imperfect forward secrecy: How Diffie-Hellman fails in practice," in Proc. 22nd ACM SIGSAC Conference on Computer and Communications Security (CCS), Denver, CO, USA, Oct. 2015, pp. 5-17.
28. H. Q. Ngo, A. Ashikhmin, H. Yang, E. G. Larsson, and T. L. Marzetta, "Cell-free massive MIMO: Ubiquitous wireless access," EURASIP Journal on Wireless Communications and Networking, vol. 2019, no. 1, p. 105, Apr. 2019, doi: 10.1186/s13638-019-1507-0.
29. E. G. Larsson, O. Edfors, F. Tufvesson, and T. L. Marzetta, "Massive MIMO is a reality—What is next?," Digital Signal Processing, vol. 30, pp. 1-12, Jul. 2014, doi: 10.1016/j.dsp.2014.03.007.
30. X. Li, Y. Zhao, and Y. Zhang, "Relay-aided secure visible light communications," IEEE Transactions on Communications, vol. 67, no. 8, pp. 5561-5573, Aug. 2019, doi: 10.1109/TCOMM.2019.2914862.
31. Y. Rocher, J. M. Hendrickx, and Y. A. de Montjoye, "Estimating the success of re-identifications in incomplete datasets using generative models," Nature Communications, vol. 10, no. 1, p. 3069, Jul. 2019, doi: 10.1038/s41467-019-10933-3.
32. H. B. McMahan, E. Moore, D. Ramage, S. Hampson, and B. A. y Arcas, "Federated learning at scale: System design," arXiv preprint, arXiv:1902.01046, Feb. 2019.
33. T. Li, A. K. Sahu, A. Talwalkar, and V. Smith, "Federated learning: Challenges, methods, and future directions," IEEE Signal Processing Magazine, vol. 37, no. 3, pp. 50-60, May 2020, doi: 10.1109/MSP.2020.2975749.
34. NIST, "Zero Trust Architecture," National Institute of Standards and Technology, Special Publication 800-207, Aug. 2020. [Online]. Available: https://doi.org/10.6028/NIST.SP.800-207
35. K. Ramezanpour and J. Jagannath, "Intelligent zero trust architecture for 5G/6G networks: Principles, challenges, and the role of machine learning in the context of O-RAN," Computer Networks, vol. 217, p. 109358, Nov. 2022, doi: 10.1016/j.comnet.2022.109358.
36. H. Sedjelmaci and N. Ansari, "Zero trust architecture empowered attack detection in 6G edge computing," IEEE Network, vol. 36, no. 5, pp. 40-46, Sep./Oct. 2022, doi: 10.1109/MNET.106.2100589.
37. M. El-Hajj, "A zero-trust and federated learning-based framework for O-RAN intrusion detection and energy-efficient DU sleep scheduling," IEEE Transactions on Network and Service Management, vol. 21, no. 2, pp. 1245-1262, Apr. 2024, doi: 10.1109/TNSM.2024.3356824.
38. Y. Ye, X. Li, and Y. Zhang, "Trusted architecture with graph-based analysis for federated learning in 6G," IEEE Transactions on Information Forensics and Security, vol. 18, pp. 2245-2260, 2023, doi: 10.1109/TIFS.2023.3261580.
39. M. Asad, M. Asim, and T. Baker, "Zero-trust federated learning for URLLC in vehicular communications," IEEE Transactions on Intelligent Transportation Systems, vol. 24, no. 12, pp. 15238-15250, Dec. 2023, doi: 10.1109/TITS.2023.3295824.
40. Z. Xiong, Y. Zhang, and D. Niyato, "Privacy-preserving federated learning with data heterogeneity for 6G mobile networks," IEEE Transactions on Mobile Computing, vol. 22, no. 8, pp. 4689-4704, Aug. 2023, doi: 10.1109/TMC.2022.3161678.
41. iTrust6G Consortium, "iTrust6G: Intelligent trust and security orchestration for 6G networks," Project Deliverables, 2023-2025. [Online]. Available: https://itrust6g.eu/
42. CONFIDENTIAL6G Consortium, "CONFIDENTIAL6G: Confidential computing for 6G networks," Project Deliverables, 2023-2026. [Online]. Available: https://confidential6g.eu/
43. F. Liu, W. Tong, and Y. Zhang, "Federated learning with differential privacy and adaptive mechanisms for OLTR systems," IEEE Internet of Things Journal, vol. 11, no. 5, pp. 8234-8248, Mar. 2024, doi: 10.1109/JIOT.2023.3321756.

44. NIST, "Post-Quantum Cryptography Standardization," National Institute of Standards and Technology, 2024. [Online]. Available: https://csrc.nist.gov/projects/post-quantum-cryptography
45. Next G Alliance, "6G Security and Trust," Next G Alliance White Paper, Jan. 2024. [Online]. Available: https://www.nextgalliance.org/
46. IMT-2030 (6G) Promotion Group, "6G trusted endogenous security architecture," White Paper, 2023.
47. GSMA, "Post-quantum cryptography in 6G networks," GSMA White Paper, Oct. 2024. [Online]. Available: https://www.gsma.com/
48. S. Y. Hsu, S. Y. Chiu, and Y. H. Chiu, "Taiwan telecommunication AI industry ESG disclosure," Scientific Reports, vol. 15, no. 1, p. 12345, 2025.
49. G. Silva-Atencio, "AI-driven 5G networks: Federated optimization for sustainable telecommunications," Artificial Intelligence and Applications, vol. 0, no. 0, pp. 1-5, Dec. 2025.
50. J. L. Siltonga, "A review of AI-driven predictive maintenance in telecommunications," International Journal of Information System & Innovation Technology (IJISIT), vol. 3, no. 2, pp. 25-31, Dec. 2024.
51. S. N. Sekaran and M. R. B. Khan, "Transforming telecommunications infrastructure in Malaysia: The role of AI in network deployment and optimization," Malaysian Journal of Business, Economics and Management (MJBEM), vol. 4, no. 2, pp. 174-182, Aug. 2024.
52. M. Hameed, N. A. Hameed, A. David, H. K. Ahmad, and S. S. Alani, "Edge AI for transforming autonomous systems and telecommunications for enhanced efficiency and responsiveness," Iranian Journal of Information Processing and Management, vol. 40, no. 4, pp. 1061-1086, Summer 2025.
53. A. Ahmed, "Federated Learning Based Decentralized Adaptive Intelligent Transmission Protocol for Privacy Preserving 6G Networks," arXiv preprint arXiv:2512.18432, Dec. 2025.
54. Next G Alliance, "Green G: The Path Toward Sustainable 6G", ATIS White Paper, Jan 2022. [Online]. Available: https://www.nextgalliance.org/white-papers/
55. R. Schwartz, J. Dodge, N. A. Smith, and O. Etzioni, "Green AI," Communications of the ACM, vol. 63, no. 12, pp. 54–63, Nov. 2020, doi: 10.1145/3381831.
56. Next G Alliance, "Sustainable AI in 6G: Architectures and energy-efficient frameworks," ATIS White Paper, Feb. 2025. [Online]. Available: https://www.nextgalliance.org/white-papers/
57. M. El-Hajj, "Secure and trustworthy Open Radio Access Network (O-RAN) optimization: A zero-trust and federated learning framework for 6G networks," Future Internet, vol. 17, no. 6, Art. no. 233, May 2025, doi: 10.3390/fi17060233.
58. P. Porambage and M. Liyanage, Security and Privacy Vision in 6G: A Comprehensive Guide, 1st ed. Hoboken, NJ, USA: Wiley-IEEE Press, 2023.
59. R. O. Zacarias, R. P. dos Santos, and P. Lago, "Towards an understanding of developer experience-driven transparency in software ecosystems," ACM Trans. Softw. Eng. Methodol., vol. 1, no. 1, pp. 1–36, Sep. 2025, doi: XXXXXXX.XXXXXXX.
60. V. S. R. Narapareddy, "Zero trust security architecture in cloud systems," Int. J. Sci. Eng. Sci., vol. 9, no. 5, pp. 139–150, 2025.
61. A. K. Vyas, N. Khatri, and S. K. Jha, Eds., 6G Communication Network: Architecture, Security and Applications, 1st ed. Boca Raton, FL, USA: CRC Press, 2024, doi: 10.1201/9781003522003.
62. H. Sedjelmaci, N. Kaaniche, and K. Tourki, "Secure and resilient 6G RAN networks: A decentralized approach with zero trust architecture," J. Netw. Syst. Manage., vol. 32, no. 2, Art. no. 33, Mar. 2024, doi: 10.1007/s10922-024-09807-x.
63. U. Kaur, A. Kumari, H. K. Saini, S. B. Khan, and M. Ouaissa, Eds., Landscaping 6G: Unlocking the Power of Ultra-Fast Communication, 1st ed. Boca Raton, FL, USA: CRC Press, 2026, doi: 10.1201/9781003683599.
64. J. M. Parra-Ullauri et al., "kubeFlower: A privacy-preserving framework for Kubernetes-based federated learning in cloud–edge environments," Future Gener. Comput. Syst., vol. 157, pp. 558–572, 2024, doi: 10.1016/j.future.2024.03.041.
65. S. Mushtaq, M. Mohsin, and M. M. Mushtaq, "A systematic literature review on the implementation and challenges of zero trust architecture across domains," Sensors, vol. 25, no. 19, Art. no. 6118, Oct. 2025, doi: 10.3390/s25196118.
66. H. Park, T.-H. Nguyen, and L. Park, "An investigation on Open-RAN specifications: Use cases, security threats, requirements, discussions," Comput. Model. Eng. Sci., vol. 141, no. 1, pp. 13–44, Aug. 2024, doi: 10.32604/cmes.2024.052394.
67. O. A. Wahab, H. Otrok, A. Mourad, and T. Taleb, "Federated Machine Learning: Survey, Multi-Level Classification, Desirable Criteria and Future Directions in Communication and Networking Systems," IEEE Communications Surveys & Tutorials, vol. 23, no. 2, pp. 1342-1397, Second Quarter 2021, doi: 10.1109/COMST.2021.3058573.
68. F. Liu, Z. Zheng, Z. Gong et al., "A survey on lattice-based digital signature," Cybersecurity, vol. 7, no. 7, Apr. 2024.
69. R. Asif, "Post-Quantum Cryptosystems for Internet-of-Things: A Survey on Lattice-Based Algorithms," IoT, vol. 2, no. 1, pp. 71–91, Feb. 2021. [Online]. Available: https://doi.org/10.3390/iot2010005.