Computers, Materials & Continua

Tech Science Press

Doi:10.32604/cmc.2025.070684

REVIEW

A Comprehensive Survey on Blockchain-Enabled Techniques and Federated Learning for Secure 5G/6G Networks: Challenges, Opportunities, and Future Directions

Muhammad Asim[1,*], Abdelhamied A. Ateya[1], Mudasir Ahmad Wani[1,2], Gauhar Ali[1], Mohammed ElAffendi[1], Ahmed A. Abd El-Latif[1] and Reshma Siyal[3]

[1]EIAS Data Science Lab, College of Computer and Information Sciences, and Center of Excellence in Quantum and Intelligent Computing, Prince Sultan University, Riyadh, 11586, Saudi Arabia

[2]College of Computer and Information Sciences, Imam Mohammad Ibn Saud Islamic University (IMSIU), Riyadh, 11432, Saudi Arabia

[3]School of Computer Science and Engineering, Central South University, Changsha, 410083, China

*Corresponding Author: Muhammad Asim. Email: masim@psu.edu.sa

Received: 21 July 2025; Accepted: 13 November 2025; Published: 12 January 2026

ABSTRACT: The growing developments in 5G and 6G wireless communications have revolutionized communications technologies, providing faster speeds with reduced latency and improved connectivity to users. However, it raises significant security challenges, including impersonation threats, data manipulation, distributed denial of service (DDoS) attacks, and privacy breaches. Traditional security measures are inadequate due to the decentralized and dynamic nature of next-generation networks. This survey provides a comprehensive review of how Federated Learning (FL), Blockchain, and Digital Twin (DT) technologies can collectively enhance the security of 5G and 6G systems. Blockchain offers decentralized, immutable, and transparent mechanisms for securing network transactions, while FL enables privacy-preserving collaborative learning without sharing raw data. Digital Twins create virtual replicas of network components, enabling real-time monitoring, anomaly detection, and predictive threat analysis. The survey examines major security issues in emerging wireless architectures and analyzes recent advancements that integrate FL, Blockchain, and DT to mitigate these threats. Additionally, it presents practical use cases, synthesizes key lessons learned, and identifies ongoing research challenges. Finally, the survey outlines future research directions to support the development of scalable, intelligent, and robust security frameworks for next-generation wireless networks.

KEYWORDS: 5G/6G; blockchain; federated learning; edge computing; security

1 Introduction

Wireless communication has been a vital means to enable pervasive connectivity, enabling instant information exchange between user devices and infrastructures [1,2]. Owing to the growing demand for real-time processing in wireless networks, traditional cloud computing architectures cannot meet their requirements [3,4]. To overcome the limitations of cloud computing, edge computing (EC) has been proposed, which is viewed as a groundbreaking paradigm in the field of distributed computing. It offers unmatched promise for low-latency processing, real-time data analysis, and enhanced scalability [3,5]. EC is capable of overcoming the limitations of cloud computing due to edge decentralized computation, especially in the application scenarios where response and processing are required swiftly, such as autonomous vehicles, industrial automation, and smart cities.

In spite of the EC benefits, it also poses a new range of security threats to user devices [6]. EC frameworks are more susceptible to threats like data breaches, unauthorized access, and advanced cyberattacks, because of Its decentralized nature and resource-constrained edge nodes [7]. In contrast to centralized cloud architecture, EC necessitates lightweight, distributed, and dynamic security functions in order to protect the data confidentiality, integrity, and availability [8]. With the advent of 5G and 6G networks, the deployment of EC has been pushed even further, enabling ultra-reliable, low-latency, and high-throughput communication services to a huge spectrum of intelligent systems, including the Internet of Things (IoT), autonomous mobility, and future industrial use [9]. But the same decentralized and extensive nature of these networks imposes large security and privacy threats.

Federated learning (FL) and blockchain (BC) subsequently became prominent technologies to support security and trust enhancement in 5G/6G edge-based infrastructure [10]. BC offers tamper-evident data exchange and decentralized access control [11], and FL supports cooperative model learning without raw data sharing while preserving privacy in distributed environments. This work presents a comprehensive survey of their contributions towards wireless network security enhancement. We will examine some of the security challenges that manifest in the edge environments, investigate existing solutions available, and find newer research advancements in this important field. Moreover, this paper will provide guidelines on securing EC for the future with a focus on new innovative strategies to address the evolving threat landscape. This review aims to inform an effort to improve the EC systems against future threats to security by synthesizing current evidence and highlighting gaps in the literature.

1.1 State-of-the-Art in Wireless Communication Technologies

The evolution of wireless communication has led to the development of 5G and 6G networks [12]. 5G focuses on enhanced mobile broadband (eMBB), ultra-reliable low-latency communications (URLLC), and massive machine-type communications (mMTC) [13]. In contrast, 6G introduces Artificial Intelligence (AI)-driven networking and quantum-safe communication technologies to enhance network security and efficiency.

With speed, connection, and latency advances, 5G networks have completely changed the wireless communication scene [14,15]. IoT, smart grids, and real-time applications have all benefited from the quick adoption of massive machine-type communication (mMTC) and eMBB, according to recent research by Popovski et al. [16]. In terms of 6G, Yang et al. [17] and Nguyen et al. [18] forecast the arrival of AI-driven networking and terahertz communication, opening up possibilities for uses like smart healthcare and holographic communication. These networks will need strong security frameworks to safeguard sensitive data in these high-performance settings.

Ahmad et al. [19] highlight the underlying advanced threat profile encompassing 5G networks and draw attention to security vulnerability heterogeneity in the new technology paradigms underlying 5G implementation. The authors provided a structured explanation of the overriding security concerns, ranging across data privacy and authentication threats, DoS attacks, and virtualized infrastructure vulnerabilities, to emphasize the need for robust security at both architectural and operational dimensions. In tackling these obstacles, the research surveys existing mitigation strategies and recognizes proactive approaches, including the use of artificial intelligence to detect anomalies, blockchain to handle decentralized trust, and the design of next-generation cryptographic primitives.

The increasing use of EC and accepting open architectures create new cyberattack risks. Furthermore, there is a greater chance of data leakage, privacy breaches, and unauthorized access due to the vast number of linked devices. According to work by Ramezanpour and Jagannath [20] and Chen et al. [21], a move toward decentralized security procedures is necessary to secure the enormous and intricate 5G and 6G networks. These mechanisms are essential for real-time threat detection and mitigation in highly dispersed networks.

The deployment of 5G and 6G technology brings forward a variety of security issues. For example, Alnaim [22] highlight how software-defined networking (SDN) and network function virtualization (NFV) are essential components of 5G design, but they also provide vulnerabilities in the control plane. In their work, they investigated how such technologies expose networks to new attack paths like resource exhaustion and virtual network function (VNF) attacks while promoting flexibility and resource handling.

Similarly, Shehab et al. [23] had conducted an extensive analysis to examine the role of 5G networks as an enabling pillar of sustainability in the context of smart cities. Their work demonstrates how the advanced features of 5G can provide the technology backbone required to accommodate sustainable urban development. The review gives an overview of the 5G communication network architecture and characteristics, emphasizing their ability to support the wide variety of smart city applications like intelligent transport systems, energy-efficient infrastructure, and massive IoT installations. From the examination of a number of important 5G technologies, the authors demonstrate how these developments work towards optimizing resource use, lowering the energy footprint, and enhancing the efficiency and resilience of city systems as a whole, thus furthering long-term sustainability objectives.

This work attempts to investigate how FL techniques and BC technology can be adapted to address the new security issues of 5G and 6G communication. While BC offers tamper-proof and open records, FL allows distributed ML without the need for centralized storage of data, both technologies offer decentralized solutions to improving network security. The following will be the main topics of this paper:

- How BC technology may reduce risks such as DDoS assaults, illegal access, and data manipulation.
- FL's function in intrusion detection and privacy-preserving data analysis.
- Current research has focused on integrating FL and BC technology into 5G and 6G networks to safeguard against advanced threats and provide secure communication.

This paper systematically explores the security issues and creative solutions related to 5G and 6G wireless networks, with particular emphasis on cutting-edge methods like FL and BC. Several major components make up the paper, as seen in Fig. 1.

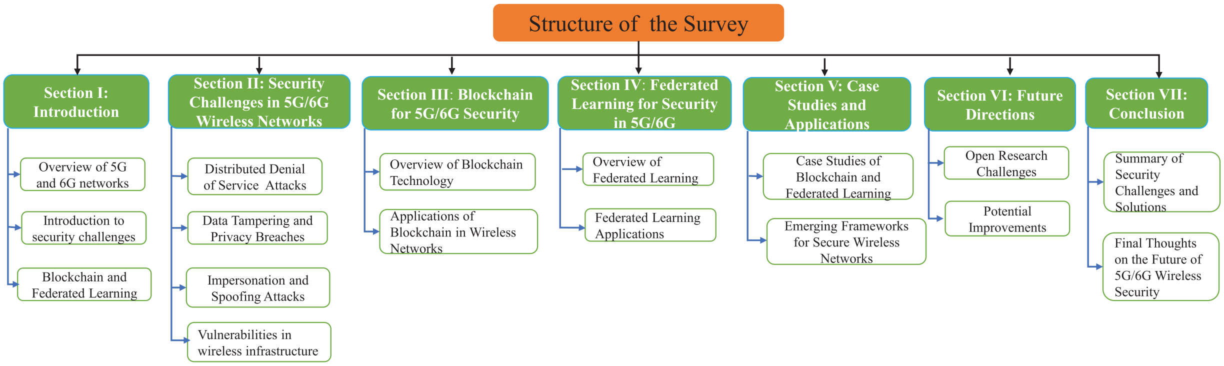
Structure of the Survey
Section I: Introduction
Overview of 5G and 6G networks
Introduction to security challenges
Blockchain and Federated Learning
Section II: Security Challenges in 5G/6G Wireless Networks
Distributed Denial of Service Attacks
Data Tampering and Privacy Breaches
Impersonation and Spoofing Attacks
Vulnerabilities in wireless infrastructure
Section III: Blockchain for 5G/6G Security
Overview of Blockchain Technology
Applications of Blockchain in Wireless Networks
Section IV: Federated Learning for Security in 5G/6G
Overview of Federated Learning
Federated Learning Applications
Section V: Case Studies and Applications
Case Studies of Blockchain and Federated Learning
Emerging Frameworks for Secure Wireless Networks
Section VI: Future Directions
Open Research Challenges
Potential Improvements
Section VII: Conclusion
Summary of Security Challenges and Solutions
Final Thoughts on the Future of 5G/6G Wireless Security

Figure 1: Structure of the survey

1.2 Scope of the Study

This work primarily serves as a comprehensive survey of existing research on the applications of FL and BC for addressing security issues in 5G/6G. While it does not present original experimental data or case studies, the manuscript systematically reviews state-of-the-art approaches, highlights key challenges, and discusses potential future directions. Relevant experimental findings from prior studies are cited where appropriate to illustrate the potential effectiveness of these technologies. The objective is to provide a solid foundation for subsequent empirical research and practical implementations in this rapidly evolving area.

1.3 Research Questions

This work considers the following research questions to guide the analysis of BC and FL for secure 5G/6G networks:

1. What are the main security and privacy challenges in 5G/6G networks?
2. How can BC integration enhance trust, reliability, and incentive mechanisms in 5G/6G networks?
3. How can FL integration enhance trust, reliability, and incentive mechanisms in 5G/6G networks?
4. How to integrate digital twins (DT) for addressing security issues in 5G/6G networks?
5. What are the existing approaches based on BC and FL, trade-offs, and limitations in 5G/6G networks?
6. Which application domains, such as IoT and Internet of Vehicles (IoV), benefit most from BC and FL, and how is its effectiveness evaluated?

These questions provide a structured framework for the categorization, analysis, and discussion throughout this survey.

2 Related Survey Papers

The use of BC technology in Mobile Edge Computing (MEC) systems has drawn considerable interest since it can improve security, privacy, and data integrity. This part consolidates information from recent review and survey papers on the application of BC technology towards securing MEC with emphasis on existing challenges, solutions, and future work.

- **BC for enhancing MEC security and privacy**
  BC's decentralized nature provides robust security characteristics, making it a suitable option to provide data integrity and secure communication in MEC environments. Different survey articles have explored this integration, for example, Mathur et al. [24] showcased a survey on the applications of BC for various IoT applications. Sharma et al. [25] also touched on the application of BC in green IoT and highlighted its advantages in providing secure and open data-sharing platforms. Similarly, Conti et al. [26] conducted a survey of security threats to MEC and proposed BC as an optimal choice for developing secure access control systems, citing the technology's ability to verify devices and keep communications confidential. Furthermore, Tang et al. [27] provides a comprehensive analysis of BC-based FL, highlighting its potential to address the privacy, security, and reliability challenges inherent in traditional FL.
- **Consensus mechanisms in BC-enabled MEC**
  The appropriate consensus mechanisms are crucial to the scalability and performance of BC-enabled MEC systems. Traditional consensus protocols like proof of work (PoW) and proof of stake (PoS) are computationally intensive and thus not best suited for MEC's resource-constrained environments. Jain et al. [28] described a comprehensive overview of light-weight consensus protocols for MEC, namely delegated PoS (DPoS) and practical byzantine fault tolerance (PBFT), and accounted for their reduced computational requirements and decreased latency. Besides, Luo et al. [29] proposed an energy-efficient two-stage computationally efficient consensus mechanism for BC-based MEC.
- **Resource management optimization**
  Integrating BC with MEC introduces significant challenges in resource management, particularly regarding computational power, storage, and bandwidth. Mershad [30] reviewed various BC-based resource allocation schemes that use smart contracts to automate and optimize the allocation of resources, thereby

enhancing the operational efficiency of MEC networks. Additionally, Xue et al. [31] presented an in-depth survey of the integration of EC and IoT. They briefly discussed the architecture of IoT and its challenges. Adam et al. [32] provided an extensive research study on IoT security, privacy, and trust that was structured according to a three-layered IoT architectural model comprising the perception, network, and application layers. The study begins with an overview of the fundamentals of IoT security, privacy preservation, and trust building, emphasizing their essentiality in ensuring reliable and sustainable IoT applications. From this context, the authors present the systematic review of the main security requirements in each layer of the IoT architecture—such as authentication, confidentiality, integrity of data, and access control—along with the discussion of the unique vulnerabilities and threats inherent in resource-constrained IoT environments. Difficulty such as heterogeneity of devices, large-scale connectivity, lack of standardized protocols, along with the compromise between lightweight security solutions and robust protection, are highlighted by the review. Furthermore, the paper explains how privacy-enhancing mechanisms and trust models can be combined with traditional security solutions to enhance end-to-end system resilience.

- **BC for secure data offloading and task scheduling:**
  Integrating BC technology with MEC has garnered significant attention for its potential to address security, privacy, and efficiency concerns in computation offloading and resource management. A comprehensive survey by Moghaddasi and Rajabi [33] explores BC-based offloading methods within MEC, offering a systematic review of current trends, algorithms, and techniques used to enhance the security and privacy of offloading processes. This survey also discusses future directions for BC integration in MEC, underscoring its growing importance in IoT and edge environments.
  Xue et al. [34] provided another essential review on the integration of BC and EC in IoT applications. They highlighted how BC can be leveraged to improve data management, resource allocation, and security in EC systems. Their paper sheds light on the dual role of BC in enhancing both the performance and the privacy of EC by decentralizing trust and offering secure transaction mechanisms.
  The role of BC in resource scheduling for EC is further discussed by Luo et al. [35], who surveyed the challenges and techniques related to resource scheduling in MEC environments. The review covers computation offloading, resource allocation, and provisioning methods, and it emphasizes the need for more efficient solutions to meet the increasing demands of real-time applications. It also highlights the potential of BC to improve fairness and transparency in scheduling decisions.
  Additionally, Mach and Becvar [36] critically summarized the fundamental concepts and decision-making processes of MEC that control whether computation tasks are executed locally on mobile devices or offloaded to proximate edge servers. The survey also delves into the complexities of resource management, wherein latency limitations, energy consumption, and available bandwidth in the network affect offloading decisions. Furthermore, authors discuss mobility management issues that arise in mobile dynamic environments, particularly maintaining service continuity and QoE as users roam across heterogeneous networks. By placing these issues in the broader context of MEC system design, Mach and Becvar offer valuable insights into the potential and limitations of computation offloading and lay the foundation for future work on optimizing edge-enabled mobile applications.
  Mikavica and Kostić-Ljubisavljević [37] presented a survey of BC-based solutions for security, privacy, and trust management in vehicular networks. They aimed to review, classify, and discuss a range of the proposed models in BC-based vehicular networks. They presented a comparison of the available models with their main features and objectives regarding security, privacy preservation, and trust management.

While the existing surveys provide valuable insights into the integration of BC technology with MEC for enhancing security, privacy, and trust, several critical gaps remain. Most of the reviewed papers focus on either the technical feasibility of BC in MEC or on optimizing specific aspects like consensus mechanisms, resource management, or data offloading separately. There is a lack of comprehensive research that systematically addresses the challenges of deploying BC in MEC environments across multiple dimensions, including security, scalability, energy efficiency, and real-time processing. Furthermore, existing studies often overlook the practical implementation scenarios and the interoperability challenges that arise when combining BC with diverse EC infrastructures.

This work aims to fill these gaps by providing a holistic review of BC-assisted technologies for securing MEC, examining integrated solutions that address the multifaceted challenges of MEC environments, and identifying future research directions that can facilitate the seamless adoption of BC in EC. This work will also explore novel BC-based frameworks that can enhance the reliability, efficiency, and scalability of MEC systems, laying a foundation for secure and intelligent EC networks.

2.1 Consensus Mechanisms in Blockchain-Enabled MEC

Consensus mechanisms are fundamental protocols in blockchain technology that ensure all nodes in a distributed network agree on the validity of transactions or data, maintaining the integrity and consistency of the blockchain. In the context of Mobile EC(MEC), consensus mechanisms play a crucial role in enabling secure, decentralized, and trustworthy interactions between edge devices, users, and services.

In MEC environments, where computational tasks and data processing are moved closer to the network edge [3], integrating blockchain requires efficient consensus mechanisms to ensure secure data transactions and resource sharing among edge nodes. The unique characteristics of MEC, such as low latency, high bandwidth, and real-time processing, make the selection of suitable consensus algorithms critical for maintaining performance and security.

Some common consensus mechanisms in Blockchain-Enabled MEC are given in Table 1 and are discussed below:

Table 1: Overview of the work addressing security concerns in wireless communication

No.	Authors	Title	Journal	Year	Key findings
1	Luo et al. [38]	A Trusted Federated Incentive Mechanism Based on Blockchain for 6G Network Data Security	Applied Sciences	2023	Improved security and convergence using BC and smart contracts.
2	Haddad [39]	Enhancing privacy and security in 5G networks with an anonymous handover protocol based on Blockchain and Zero Knowledge Proof	Computer Networks	2024	Forward/Backward secrecy using BC and zero knowledge proof.
3	Maroufi et al. [40]	Lightweight Blockchain-Based Architecture for 5G Enabled IoT	IEEE Access	2023	Enhanced security against data manipulation and fraud using hashing and encryption protocols.

(Continued)

Table 1 (continued)

No.	Authors	Title	Journal	Year	Key findings
4	Yang et al. [41]	An Improved Federated Learning Algorithm for Privacy Preserving in Cybertwin-Driven 6G System	IEEE Transactions on Industrial Informatics	2022	Avoid privacy leakage using FL.
5	Wan et al. [42]	Privacy-preserving blockchain-enabled federated learning for B5G-Driven edge computing	Computer Networks	2022	Differential privacy protection with BC and FL.
6	Lu et al. [43]	Blockchain and Federated Learning for 5G Beyond	IEEE Network	2021	Enhanced the security and privacy by integrating BC into a FL.
7	Asad et al. [44]	Secure and Efficient Blockchain-Based Federated Learning Approach for VANETs	IEEE Internet of Things Journal	2024	Communication efficiency and data privacy
8	Kalapaaking et al. [45]	Blockchain-Based Federated Learning With Secure Aggregation in Trusted Execution Environment for Internet-of-Things	IEEE Transactions on Industrial Informatics	2023	Securing model aggregation
9	Akoramurthy et al. [46]	Blockchain-based federated learning in internet of health things	Federated Learning for Digital Healthcare Systems(Book)	2024	Protecting the privacy of connected health data
10	Azzaoui et al. [47]	Block5GIntell: Blockchain for AI-Enabled 5G Networks	IEEE Access	2020	Secure sharing of information and resources among 5G nodes
11	Liu et al. [48]	A Secure Federated Learning Framework for 5G Networks	IEEE Wireless Communications	2020	Prevent malicious or unreliable participants
12	Du et al. [49]	Federated learning for distributed intrusion detection in IoT networks	Advanced Machine Learning for Cyber-Attack Detection in IoT Networks	2025	Intrusion detection

(Continued)

Table 1 (continued)

No.	Authors	Title	Journal	Year	Key findings
13	Chelghoum et al. [50]	Blockchain and AI for Collaborative Intrusion Detection in 6G-enabled IoT Networks	IEEE 25th International Conference on High Performance Switching and Routing (HPSR)	2024	Intrusion detection
14	Fu et al. [51]	Federated Learning-Based Resource Management with Blockchain Trust Assurance in Smart IoT	Electronics	2023	Trust management and malicious nodes' detection
15	Liu et al. [52]	BFL-SA: Blockchain-based federated learning via enhanced secure aggregation	Journal of Systems Architecture	2024	Secured data aggregation.

2.1.1 Proof of Work (PoW)

PoW is the original consensus mechanism used by Bitcoin, which requires nodes (miners) to solve complex mathematical puzzles to validate transactions. However, due to its high computational requirements and energy consumption, PoW is generally not suitable for MEC environments where devices have limited resources.

2.1.2 Proof of Stake (PoS)

PoS is an alternative to PoW that requires validators to own a certain amount of cryptocurrency to participate in the consensus process. Validators are chosen to create new blocks based on their stake. PoS is more energy-efficient than PoW, but it can still be challenging to implement in resource-constrained edge devices typical of MEC networks.

2.1.3 Delegated Proof of Stake (DPoS)

DPoS is an extension of the initial PoS consensus algorithm that seeks to promote scalability and efficiency for distributed ledger systems. In this system, network stakeholders vote proportionally to their stake to select a small group of trusted delegates, also referred to as witnesses or validators. These voted delegates are later given the privilege to confirm transactions, generate new blocks, and also keep the overall integrity of the blockchain. DPoS significantly reduces communication overhead, accelerates the time for block confirmation, and also achieves higher throughput than the conventional PoS and PoW systems by restricting the consensus process to a smaller set of nodes. This light-weight nature renders DPoS particularly effective in low-latency and resource-constrained environments such as MEC, where immediate consensus is imperative in facilitating real-time services and applications. Furthermore, the voting mechanism ensures a degree of decentralized control since stakeholders continue to maintain the ability to replace satisfactory or malicious delegates, hence maintaining accountability and responsiveness within the system. DPoS offers scalability and efficiency, which are essential for EC scenarios.

2.1.4 Practical Byzantine Fault Tolerance (PBFT)

PBFT is a consensus mechanism designed to tolerate Byzantine faults (where nodes may act maliciously or fail unpredictably). It achieves consensus through a series of communication rounds among nodes, ensuring that even if some nodes are compromised, the system remains secure. PBFT is efficient in terms of resource consumption, making it well-suited for MEC environments with a smaller number of nodes.

2.1.5 Proof of Authority (PoA)

PoA relies on a limited number of pre-approved validators who are responsible for validating transactions. This approach reduces the computational load and enhances transaction speed, making it suitable for private or consortium blockchains in MEC. PoA offers a balance between decentralization and efficiency, which is crucial for edge-based applications.

2.1.6 Federated Byzantine Agreement (FBA)

FBA, used by systems like Stellar, involves a network of nodes agreeing on a set of trusted nodes to validate transactions. This consensus mechanism is lightweight and can be adjusted to suit the scalability and security needs of MEC environments, where trust relationships can be predefined based on network architecture.

2.2 State-of-the-Art Approaches in Addressing Security Issues

Recent improvements in wireless communication, particularly with 5G and 6G, have revealed the potential of BC and FL to address security concerns. Below is an overview of studies that explore these topics further. For 6G data security, Luo et al. [38] provided a trusted federated incentive mechanism that combines BC and FL. The suggested method makes use of BC and smart contracts to protect user privacy and incentivize edge nodes to engage in secure FL. When compared to conventional algorithms, this method enhances convergence and security. The use of BC technology to improve the decentralization of security protocols in 5G networks is covered by Haddad [39]. Their work focuses on developing an immutable ledger for network transactions to protect data integrity and mitigate distributed denial of service (DDoS) attacks. A lightweight BC-Based architecture is put out by Maroufi et al. [40] to secure 5G-enabled IoT scenarios. Their architecture outperforms conventional 5G (without BC) regarding security against data manipulation and fraud. FL is investigated by Yang et al. [41] for model training on 5G networks while maintaining privacy. Their study demonstrates how FL may be used to cooperatively discover anomalies among various IoT devices while protecting user privacy. In 6G networks, Wan et al. [42] provide BC-enabled FL for B5G-driven EC, where massive data collected from edge devices fuels AI model training. To protect sensitive data while enabling collaborative learning, they propose a hybrid framework combining BC-enabled FL and WGAN-based differential privacy.

Lu et al. [43] enhanced the security and privacy by integrating BC into a FL scheme for maintaining the trained parameters. Asad et al. [44] proposed a secure and efficient BC-based FL approach to ensure communication efficiency and data privacy in vehicular ad hoc networks (VANETs). Their research minimized the long delay while avoiding possible threats and attacks using homomorphic encryption systems. Kalapaaking et al. [45] BC-based FL framework with Intel Software Guard Extension-based trusted execution environment to securely aggregate local models in Industrial IoT. BC-based FL systems are investigated by Akoramurthy et al. [46] as a means of protecting medical IoT data. Their research shows how BC protects privacy while sensitive healthcare data models are being trained federatedly.

Azzaoui et al. [47] presented a comprehensive intelligence and secure data analytics framework for 5G networks based on the convergence of BC and AI named Block5GIntell. Liu et al. [48] presented a BC-based secure FL framework to create smart contracts and prevent malicious or unreliable participants from being involved in FL.

For IoT networks, Du et al. [49] suggested an FL architecture that offers distributed, secure intrusion detection. The application of FL with BC for intrusion detection systems in 5G and 6G networks was investigated by Chelghoum et al. [50]. Their method improves the security of networked devices by identifying anomalous activity in real-time. Fu et al. [51] presented an IoT resource management framework incorporating BC and FL. They proposed a specific FL-based resource management with a BC trust assurance algorithm.

Liu et al. [52] proposed a BC-based FL via enhanced secure aggregation. Their method boosted security and fault tolerance while improving the efficiency of data utilization in the secure aggregation process. Fig. 2 illustrates how FL and BC are integrated to secure wireless networks, especially in 5G and 6G scenarios. The image demonstrates how data moves between edge devices, how FL is used for local model training, and how BC ensures safe data transfers, privacy, and authentication.

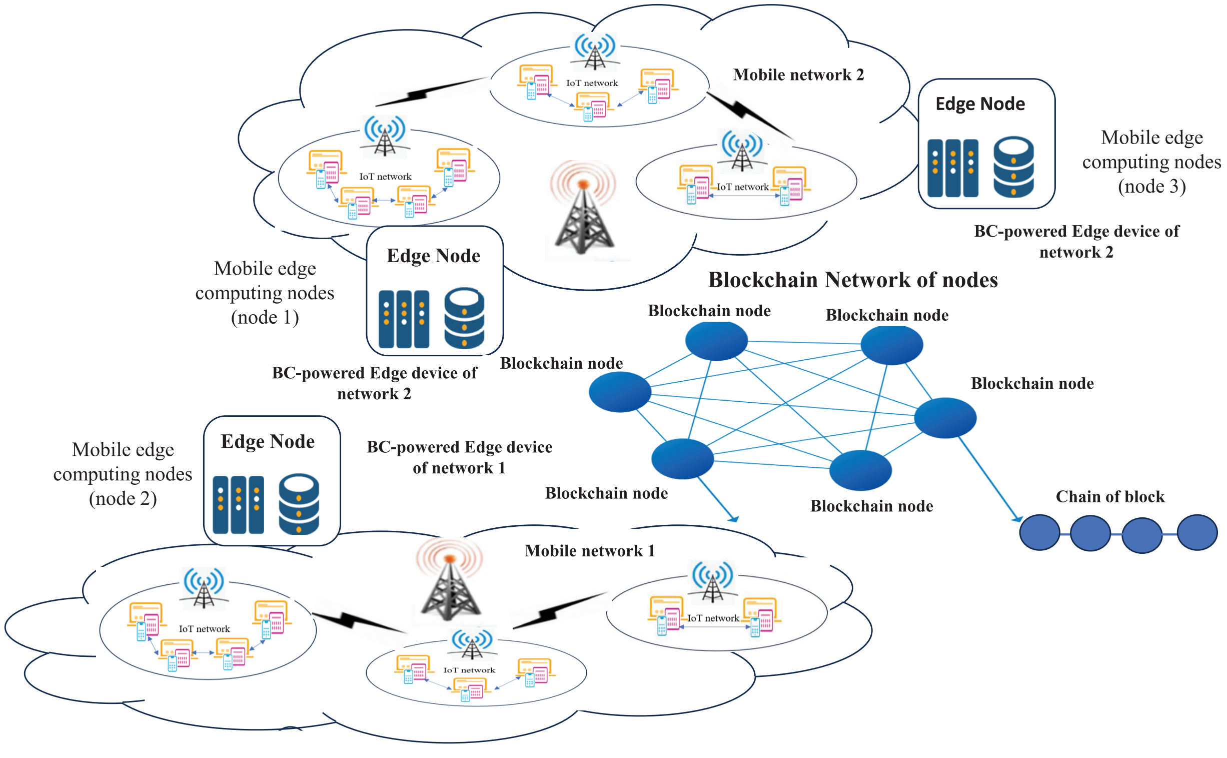
Mobile network 2
IoT network
IoT network
IoT network
Edge Node
Mobile edge computing nodes (node 3)
BC-powered Edge device of network 2
Edge Node
Mobile edge computing nodes (node 1)
BC-powered Edge device of network 2
Blockchain Network of nodes
Blockchain node
Blockchain node
Blockchain node
Blockchain node
Blockchain node
Blockchain node
Edge Node
Mobile edge computing nodes (node 2)
BC-powered Edge device of network 1
Chain of block
Mobile network 1
IoT network
IoT network
IoT network

Figure 2: Generic layered architecture of BC and FL for securing wireless communication networks

2.3 Quantitative Metrics for Security and Privacy

Although this survey primarily provides a qualitative analysis of security mechanisms and privacy-preserving techniques in next-generation wireless networks, quantifiable metrics reported in the literature are included to strengthen the discussion. Prior studies provide numerical insights such as encryption and decryption latency, key size requirements, privacy leakage probabilities, and differential privacy noise parameters relevant to quantum-safe cryptography, Blockchain-based security, and federated learning frameworks [53–55]. These quantitative findings are summarized where appropriate to contextualize the performance of different techniques. Furthermore, the survey emphasizes the need for future empirical evaluations under realistic network environments to establish standardized benchmarks for assessing security and privacy effectiveness in 5G and 6G systems.

3 Notable Case Studies and Applications

The latest advancements in technology witnessed BC and FL showing great potential for providing security in 5G and 6G networks. The section brings forth major real-world applications of the technologies, with emphasis on how they are efficient and scalable for various situations.

3.1 Telecom Italia's BC-Based IoT Security Solution

Telecom Italia has launched a BC-based security solution to protect IoT devices on its 5G network. A decentralized ledger is utilized to record device identities and encrypt data communication. With this BC, Telecom Italia is able to provide immutable records of device interactions, restricting the spoofing and unauthorized access risk. Scalable with the large number of IoT devices, the decentralized nature of the system addresses central bottlenecks but accommodates massive deployment.

3.2 IBM's FL for Privacy-Preserving Data Analytics

IBM uses FL to enable privacy-preserving data analytics on its 5G network. Deployment enables model training collaboratively without the exchange of raw data. FL retains sensitive information locally, thus enhancing privacy and regulatory compliance. FL can support a large number of entities to participate in model training to avoid data centralization issues and scale with the network.

Fig. 3 presents real-world applications of BC and FL in 5G/6G networks, demonstrating significant advancements in securing and scaling modern communication infrastructures. Each case study highlights unique approaches to addressing security challenges, from privacy preservation to scalable data management. The integration of these technologies offers promising solutions to enhance network security and efficiency. Future developments will continue to refine these applications and address emerging challenges in the evolving landscape of wireless communication.

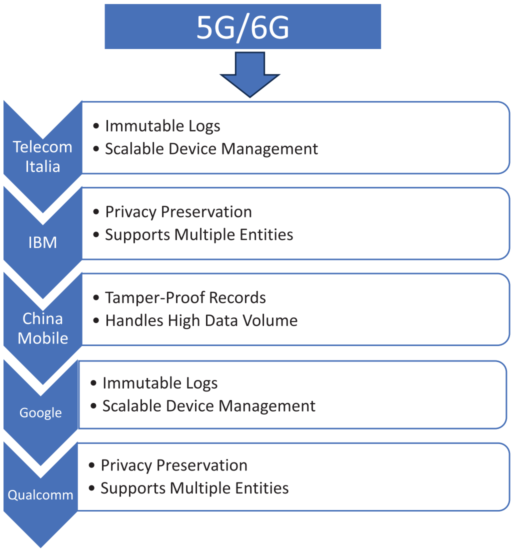

Figure 3: Applications of BC and FL in 5G/6G Networks

3.3 Security Issues in Wireless Communication

Because of the growing number of applications that operate over wireless networks, wireless communication security is essential. All these challenges cover a broad range of issues, such as user privacy, network attack resilience, and confidentiality, integrity, and availability of data. Since wireless networks are broadcast in nature, they are inherently more susceptible to security attacks than wired networks. Some of the principal security concerns include the following.

- Unauthorised users are able to intercept communications over wireless channels, potentially causing data breaches. Encryption protocols must be used to avoid data interception. Current research emphasizes the role of advanced encryption methods in preventing such threats [56].
- Unauthorized attempts at access are feasible in wireless networks. Effective access control and authentication measures must be implemented to prevent access by unauthorized entities. Several techniques for improving access control and authentication in wireless networks have been shown in research [57].
- Data integrity is defined as a promise that information does not get altered during transmission. Methods like digital signatures and cryptographic hashing are utilized to ensure data integrity. Significant surveys summarize significant developments in integrity verification techniques [58].
- Overloading the network with excessive traffic can interfere with services in wireless networks using DoS attacks. Intrusion detection technology and efficient traffic management are required to counter such threats. Comprehensive research on DoS attacks and remedies could be referred to through the literature [59].
- Rogue or unauthorized access points may be installed to deceive users and plunder information. Network monitoring and management are needed to detect and remove rogue access points. Solutions for rogue access point detection and rogue access point control are discussed in recent studies [60].

3.4 Developments in Wireless Protection

Recent developments are intended to overcome these challenges.

- Data wireless transmission is made secure using enhanced encryption techniques. Comparisons of encryption technology and performance of encryption in wireless networks are useful pieces of information [61].
- AI and ML technologies are being used more and more for threat detection and response, making the network more capable of detecting and responding to any security weaknesses. Recent critiques have discussed how AI and ML are applied to improve wireless network security [62].
- BC adds an extra layer of security to wireless networks through the offering of a decentralized way of handling transaction security and access control. The potential of BC technology to improve security is highlighted in papers on its use in wireless networks [63].

Because 5G networks use a service-based architecture (SBA), which divides the control and user planes to provide scalability and flexibility, they significantly improve wireless communication. eMBB, Massive Machine Type Communications (mMTC), and URLLC are some salient characteristics. These characteristics support large numbers of linked devices, low latency, and high-speed communication. 5G's security features include increased authentication techniques like 5G-AKA (Authentication and Key Agreement) and better encryption technologies [19].

With the integration of AI-driven network management, sophisticated network slicing, and seamless satellite network integration, 6G is anticipated to enhance the design of wireless networks significantly. It seeks to enable cutting-edge applications, including quantum and holographic communication technologies, and use Terahertz (THz) communication channels [64]. In order to handle new threats and improve privacy-preserving measures, 6G is expected to include AI-driven security protocols and quantum-safe encryption techniques [65,66].

3.5 Comparison between 5G and 6G Networks

Table 2 and Fig. 4 provide comparisons of key features of 5G and 6G networks. The comparison is mainly based on the following directions.

1. Architecture: 6G builds on 5G's SBA by adding more sophisticated integration and management features.
2. Frequency bands: 6G will use quantum technology and THz bands, whereas 5G uses millimeter waves.
3. Security: While 6G is anticipated to provide quantum-safe encryption and AI-driven security, 5G offers enhanced authentication and encryption [67,68].
4. Threat landscape: New technologies give 5G a larger attack surface, while more advanced threats are expected for 6G [69,70].

Table 2: Comparison of 5G and 6G networks

Aspect	5G	6G
Architecture	Service-Based Architecture (SBA) with separated control and user planes	Advanced SBA with AI-driven management and integration with satellite networks
Frequency bands	Millimeter waves (24 GHz and above)	Terahertz (THz) bands and integration with quantum communication technologies
Key features	eMBB, URLLC, mMTC	Holographic communication, advanced AI/ML, seamless integration with quantum and satellite networks
Security mechanisms	Improved encryption (256-bit), enhanced authentication (5G-AKA), network slicing	Quantum-safe encryption, AI-driven security protocols, advanced privacy-preserving mechanisms
Threat landscape	Expanded attack surface due to new technologies and frequency bands	Anticipated sophisticated threats targeting THz bands, AI-driven attacks, and quantum communication
Network slicing	Initial implementation with isolated security domains	More refined with AI-driven management and enhanced security features
Privacy	Improved but still susceptible to certain breaches	Expected to offer superior privacy mechanisms with better data control and usage

3.5.1 Privacy Breaches

The IoT and increased connectivity in 5G and 6G networks increase the potential of privacy intrusions. Network protocol flaws can be exploited by malicious actors, particularly during network handovers. Common risks include location monitoring, unlawful access to personal information, and communication interception. Important countermeasures include methods like end-to-end encryption, pseudonymization, and privacy-preserving models like differential privacy. Humayun et al. [71] discuss various privacy-preserving techniques in IoT environments over 5G, focusing on challenges like data sharing and access control. Research by Huang et al. [72] highlights privacy-preserving schemes for 5G vehicular networks, where encryption and anonymization techniques play a critical role. Furthermore, Al Ridhawi et al. [73]

outline methods to protect sensitive user data in their proposal for secure communication protocols for 5G-enabled smart cities.

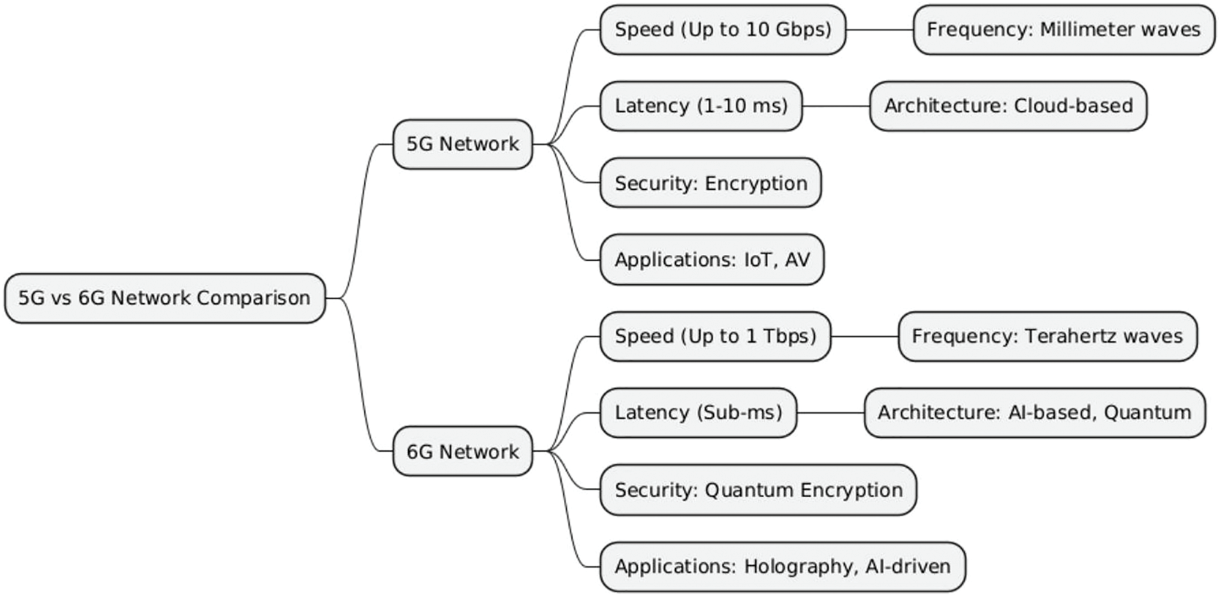
5G vs 6G Network Comparison
5G Network
Speed (Up to 10 Gbps)
Frequency: Millimeter waves
Latency (1-10 ms)
Architecture: Cloud-based
Security: Encryption
Applications: IoT, AV
6G Network
Speed (Up to 1 Tbps)
Frequency: Terahertz waves
Latency (Sub-ms)
Architecture: AI-based, Quantum
Security: Quantum Encryption
Applications: Holography, AI-driven

Figure 4: Comparison of key features between 5G and 6G networks

3.5.2 Distributed Denial of Service (DDoS) Attacks

The dispersed nature of DDoS attacks makes them a huge threat to 5G and 6G networks. Attackers can deny network availability by flooding services with spurious traffic, affecting critical applications like healthcare and autonomous vehicles. In their distributed defense against DDoS attacks in 5G, Hoque et al. [74] highlight the necessity for cooperative detection systems. With emphasis on deep learning methods, Kuadey [75] exhibit excellent results in early detection and prevention of DDoS attacks in 5G-based IoT systems. In order to avoid service interference, Patel [76] presented AI-Powered Intrusion Detection and prevention systems in 5G networks.

3.5.3 Jamming Attacks

Jamming attacks seriously threaten 5G and 6G communication networks since the attackers use interfering signals to interfere. This is particularly important in mmWave networks. Pirayesh and Zeng [77] offered a comprehensive survey on Jamming Attacks and Anti-Jamming Strategies in Wireless Networks. Mpitziopoulos et al. [78] provided a general overview of the critical issue of jamming in WSNs and cover all the relevant work, providing future research directions. Chen et al. [79] provided a comprehensive survey on various multiple-antenna techniques in physical layer security, with an emphasis on transmit beamforming designs for multiple-antenna nodes.

3.5.4 Man-in-the-Middle (MITM) Attacks

In 5G and 6G networks, where attackers may intercept and control messages, MITM attacks pose a serious concern. In their study of machine learning's application to 5G networks, Arul Stephen et al. [80] provided models for anomaly detection based on traffic patterns to identify MITM assaults. Bhushan et al. [81] provided an overview an-in-the-middle attack in wireless and computer networking. In 2022, Conti et al. [82] reviewed the literature on MITM to analyse and categorize the scope of MITM attacks, considering both a reference model, such as the open systems interconnection model.

3.5.5 Spoofing and Impersonation

In 5G and 6G networks, spoofing and impersonation attacks enable hackers to obtain unauthorized access by imitating reputable equipment or users. Babu et al. [83] presented a comprehensive analysis of spoofing. Dasgupta et al. [84] discussed a sensor fusion-based Global Navigation Satellite System spoofing attack detection framework for autonomous vehicles (AVs). Furthermore, it has been determined that certificate-based security and mutual authentication are essential methods for thwarting these kinds of assaults.

3.5.6 Vulnerabilities in Wireless Communication Infrastructure

The core network, which handles resource allocation, user authentication, and data management, acts as the foundation of 5G and 6G communication networks. The attack surface has grown dramatically since network slicing and virtualization were introduced. Some of the key security threats in 5G and 6G networks are given in Fig. 5.

- Vulnerabilities in Virtualization: Misconfigurations or vulnerabilities in Hypervisors can compromise Virtualized Network Functions (VNFs). Attackers could use these flaws to break into networks or obtain unauthorized access.
- Network Slicing: This technique presents customized networks for certain use cases (autonomous cars, IoTs, etc.). Cross-slice attacks, which enable attackers to travel laterally across slices, are a possibility if one slice is compromised.
- Signaling Storms: The likelihood of signaling storms, which may overwhelm the network and cause denial-of-service (DoS) circumstances, is increased by the high density of connected devices in 5G and 6G networks.

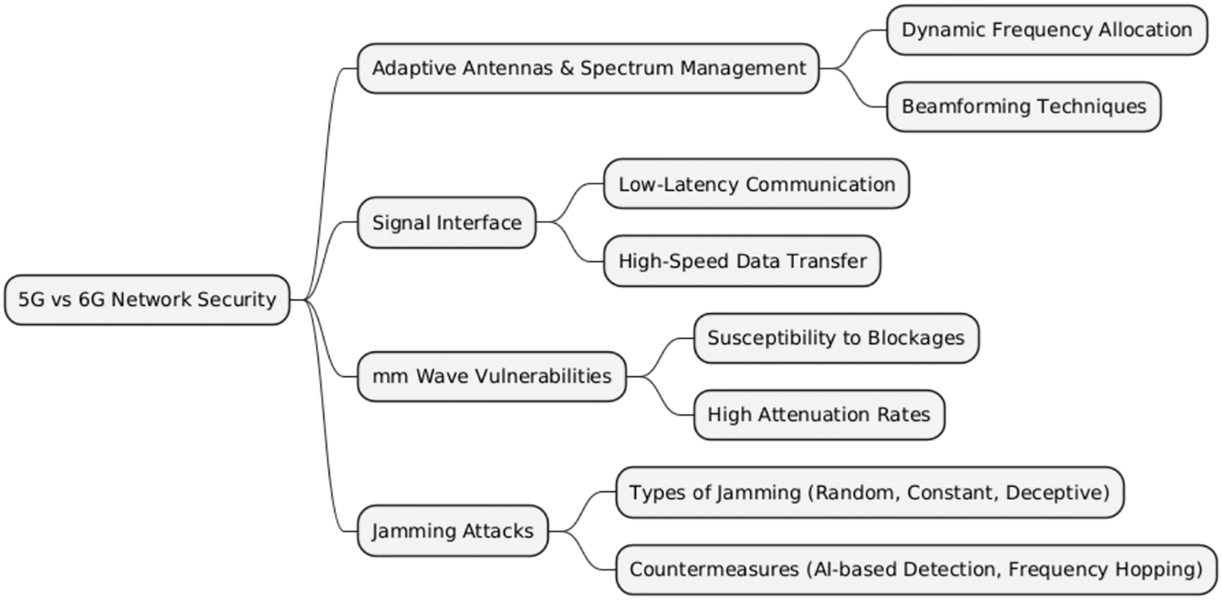
5G vs 6G Network Security
Adaptive Antennas & Spectrum Management
Dynamic Frequency Allocation
Beamforming Techniques
Signal Interface
Low-Latency Communication
High-Speed Data Transfer
mm Wave Vulnerabilities
Susceptibility to Blockages
High Attenuation Rates
Jamming Attacks
Types of Jamming (Random, Constant, Deceptive)
Countermeasures (AI-based Detection, Frequency Hopping)

Figure 5: Key security threats in 5G/6G networks

3.6 6G Threat Landscape

To provide a clearer and more structured understanding of the emerging 6G security landscape, this section presents specific examples of anticipated threats and their potential implications. Key risks include AI-driven automated attacks, ultra-low-latency eavesdropping enabled by enhanced sensing, UAV-assisted denial-of-service attacks, and supply-chain vulnerabilities affecting 6G hardware and software components. Where available, qualitative and quantitative indicators of threat likelihood and severity from recent studies are included to contextualize their impact. Table 3 summarizes major threat categories, the associated network elements, expected impact, and supporting references, offering a concise foundation for risk assessment in next-generation wireless networks.

Table 3: Illustrative 6G threat landscape and risk indicators

Threat type	Affected component	Impact/Severity	References
AI-powered network attacks	Base stations/Edge nodes	High; may disrupt network management	[85,86]
Ultra-low-latency eavesdropping	URLLC links	Moderate; compromises confidentiality	[87]
UAV-assisted DoS attacks	RAN/Backhaul	High; service unavailability	[88]
Supply-chain attacks	Network hardware/Firmware	Critical; may affect entire network	[89]

3.7 Overview of BC in the Wireless Communication

Decentralized ledger technology, or BC, keeps transactions safely on a distributed network. Because it can enhance security, transparency, and data integrity, its application in wireless communication networks, particularly 5G and 6G, is gaining increasing importance. BC offers ways to protect the many devices most susceptible to hacking, data manipulation, and privacy violations in forthcoming wireless networks. BC is a distributed ledger technology (DLT) that maintains a ledger of transactions in a decentralized environment on several devices. With the ability to handle gigantic amounts of data on billions of networked devices securely, with surety, and with less overhead, it has its application in wireless communication, particularly in next-generation wireless networks like 5G and 6G. Due to its decentralized design, free from a point of failure, BC technology is an important asset in protecting wireless networks against any cyber attacks, ranging from data tampering, DDoS attacks, and privacy violations.

BC's capability in lowering single points of failure, network integrity, and trustless interaction allows BC to be useful for wireless communications. BC is the technology that needs to be used for applications like smart cities, autonomous vehicles, and large IoT deployments because it is decentralized to process data in millions of devices securely and enables wireless networks to securely process data in millions of devices. BC-enabled MECs are particularly useful for managing network resources, encrypting data at the edge, reducing latency, and improving real-time decision-making. BC technology was also used in wireless communications to solve data privacy issues, device authentication, and spectrum control. For instance, eliminating middlemen by BC will enhance security for IoT devices and achieve optimal utilization of resources. Furthermore, it is important to manage 5G networks through network slicing because BC provides confidentiality and isolation of various virtual networks from a common shared physical infrastructure. The key features of BC include the following.

1. Decentralization: BC is immune to single-point failures due to the fact that it depends on a decentralized network. The decentralization of wireless communication enhances the security of dispersed edge devices and limits attack avenues on centralized servers. Decentralized authentication, spectrum management, and resource allocation are some of the important uses of BC in this field.
2. Immutability: Once committed to a BC, information can't be erased or altered. This protects the network records of device identifiers, resource reservation, and transaction logs from being tampered with or deleted. It has implications for spectrum management, sensitive data protection, and network slicing compliance.
3. Transparency: BC enables data exchanges and transactions to be traceable by all members of a wireless network. Decentralization's transparency enhances accountability and allows trust building in the management of spectrum resources, device authentication, and data consistency among multiple nodes.

In recent years, using BC integration for wireless networks has been investigated to improve efficiency, security, and transparency. Among the pioneer works, published in 2023 and 2024, are those that describe the promises of BC technology for wireless communication. Li et al. [90] studied a BC-based privacy-preserving and accountable MEC framework for the Metaverse, termed Meta-BMEOC. Zhang et al. [91] investigated a directed acyclic graph BC-enhanced user-autonomy spectrum sharing model.

Haddad et al. [92] investigated a novel, efficient and secure authentication and key agreement protocol for 5G networks using BC. Their security analysis illustrated that the proposed scheme is secure and withstands the known attacks; DOS, DDOS, MITM, hijacking and compromising attacks.

Wijethilaka et al. [93] designed a BC-based secure authentication and authorization framework for robust 5G network slicing. Li et al. [94] investigated BC-based data security for AI applications in 6G networks.

Rishiwal et al. [95] researched a Exploring Secure vehicle-to-everything (V2X) Communication Networks for Human-Centric Security and Privacy in Smart Cities.

Furthermore, Valitabar et al. [96] investigated efficient resource allocation for BC-enabled MEC: a joint optimization approach.

In 2024, Padmavathy and Goyal [97] presented a BC based secure cross layer design for wireless sensor networks. Alzubi et al. [98] investigated BC-enabled security management framework for MEC. The study demonstrated how BC enhances data integrity and privacy protection by securing data transfers between edge devices, cloud servers, and IoT sensors. Moreover, Table 4 presents overview of some recently published works and the key metrics in BC technologies for securing MEC.

Table 4: Overview of key metrics in BC technologies for securing MEC

Study reference	Security level	Latency	Throughput	Energy efficiency	Scalability	Data integrity	Privacy preservation	Computation overhead
Li et al. [90]	Yes	Yes	No	No	No	Yes	Yes	Yes
Zhang et al. [91]	Yes	No	Yes	Yes	No	No	No	No
Haddad et al. [92]	Yes	No	No	No	Yes	Yes	No	No
Wijethilaka et al. [93]	Yes	Yes	Yes	No	No	Yes	No	No
Li et al. [94]	Yes	Yes	Yes	Yes	Yes	No	No	No
Rishiwal et al. [95]	Yes	Yes	No	No	No	Yes	Yes	No
Valitabar et al. [96]	Yes	Yes	Yes	Yes	Yes	No	No	Yes
Padmavathy et al. [97]	Yes	Yes	No	No	Yes	Yes	No	No
Alzubi et al. [98]	Yes	Yes	Yes	No	No	Yes	No	No

3.8 Overview of FL Techniques in Wireless Communication

FL is a machine learning paradigm that permits cooperative model training by several edge devices or dispersed data sources, all while maintaining localized data. This addresses privacy concerns and bandwidth constraints since there is no need to move big or sensitive datasets to a centralized server [90,93].

EC allows data to be stored and computed closer to the point of demand, i.e., at the network edge instead of a central data center. This aids in bandwidth optimization, real-time processing improvement, and latency reduction [91,94]. FL was intended mainly to solve privacy issues in applications with extremely sensitive user data, such as mobile devices and healthcare settings. Google first introduced it in 2016 by McMahan et al. [99]. In the context of 5G/6G networks, where vast volumes of data are created across many IoT devices, FL has become increasingly important by separating data from the core training process. FL gathers just model changes, such as gradients, on a central server, iteratively improving the model rather than centralizing data from all devices. This structure is especially appropriate for 5G and 6G networks, where a wide range of IoT devices produce copious amounts of sensitive data Kairouz et al. [100].

One of the FL's key advantages is its privacy-preserving data analytics, which makes it extremely relevant to sensitive industries like healthcare and telecommunications. It allows collaborative training without requiring the release of raw data. Niknam et al. [101] proposed a model that makes sure that gadgets, from IoT sensors to smartphones, can improve the accuracy of the global model without running the risk of invading privacy. To improve data safety during model updates, FL systems frequently use strategies like secure multiparty computation (SMPC) and differential privacy Bonawitz et al. [102]. Furthermore, FL provides real-time threat monitoring, allowing nearby devices to monitor any threats and react quickly. These devices can detect abnormalities or assaults by continually evaluating local data; these can then be handled at the network's edge to stop them from spreading further, Amiri and Gunduz [103]. This feature is necessary to keep security in the intricately linked world of contemporary wireless networks.

As shown in Fig. 6, the FL process begins with the FL server initializing the global model parameters and distributing the model to all connected clients through wireless networks. Each client then trains the model locally using its own dataset (e.g., text messages) and subsequently uploads the updated model parameters back to the FL server. The server aggregates these updates from all clients to create a refined global model. This process is repeated iteratively, with the server broadcasting the updated global model to clients until the model reaches convergence.

3.8.1 FL in Privacy Preserving Data Analytics

Conventional machine learning methods involve centralizing data for training, which raises significant privacy problems, especially in industries with highly sensitive data, such as healthcare, banking, and smart cities. FL significantly reduces the risk of data breaches by letting users' data stay on their devices and only exchanging model changes or gradients. Further improvements to privacy are made possible by methods like Differential Privacy and Secure Multi-Party Computation (SMPC), which add noise to model updates and securely compute shared functions without disclosing specific data points. FL has been used in a number of healthcare situations to safeguard private patient data. The following Table 5 summarizes various privacy-preserving techniques used in FL, highlighting the authors, methods, descriptions, and potential applications.

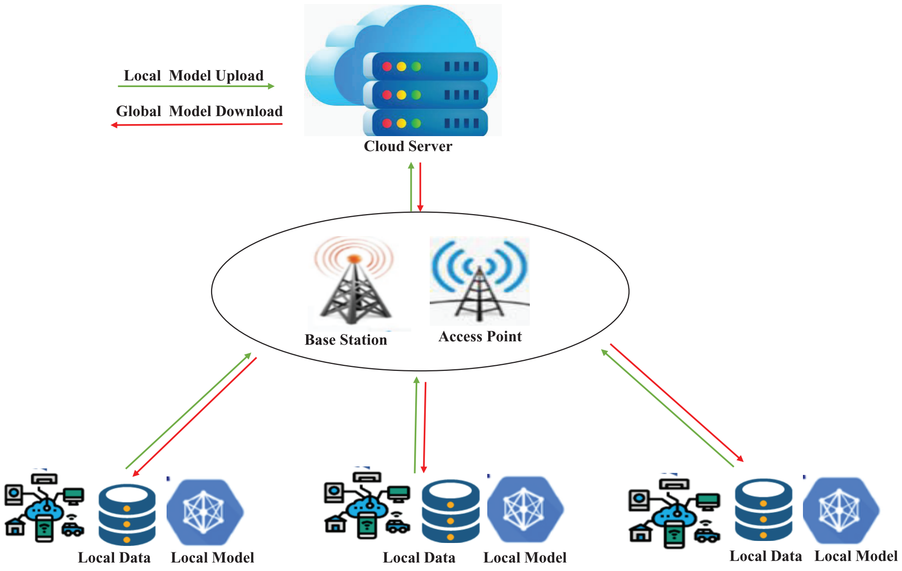

Figure 6: FL in wireless communication

Table 5: Overview of privacy-preserving techniques in FL

Author(s) & Year	Technique	Description	Applications
Bonawitz et al. [104]	FL	Decentralized model training without sharing raw data.	Healthcare, IoT, Finance
Kairouz et al. [100]	Differential Privacy (DP)	Adds noise to ensure individual data privacy.	Healthcare, finance
Yu and Cui [105]	Secure Multi-Party Computation (SMPC)	Private computation across multiple parties.	Healthcare, finance
Abadi et al. [106]	DP-SGD	Adds noise to gradients during training.	Healthcare, sensitive data
Fereidooni et al. [107]	Secure Aggregation	Securely aggregates updates from multiple devices.	Large-scale networks
McMahan et al. [99]	Federated Averaging (FedAvg)	Aggregates local models without raw data sharing.	Healthcare, finance
Fan et al. [108]	Hybrid FL with BC	Secures model updates via BC.	EC, IoT
Huang et al. [109]	Randomized Response, FL	Users submit randomized data for privacy	News recommendation
Hernandez et al. [110]	FL	Malicious Networks	Cloud environment
Liu et al. [111]	Federated Transfer Learning	Combines FL with transfer learning for privacy.	Finance, smart cities

3.8.2 FL in Smart Healthcare Using EC or IoT

The healthcare industry has increasingly adopted cutting-edge machine learning techniques over the past few years to enhance care for patients as well as streamline treatment outcomes. FL, a technique that preserves patient privacy while supporting collaborative model training across decentralized sources of data, is one such approach that has been gaining popularity among these technologies. This is especially important in the healthcare industry because private policies that keep sensitive patient data confidential are very stringent. Patient information security is further augmented in the training process by adding privacy-preserving techniques, such as differential Privacy and secure multi-party computation.

FL allows medical facilities to jointly diagnose diseases securely. For instance, Abbas et al. [112] studied the role of FL in healthcare, highlighting its ability to enable privacy-preserving collaborative model training across institutions and smart health systems using IoT and wearable devices. They discussed major challenges, including security threats, data heterogeneity, and scalability and emphasized emerging privacy-preserving techniques as essential for wider FL adoption and improved healthcare outcomes. Ramesh et al. [113] used FL with EC called as FLEC to process patient data in a decentralized manner, helping in healthcare analytics. This study applies FLEC using simulated healthcare data activating alerts for any defects to observe temperature, heart rate, and SpO2 levels. Lanka and Moodhitaporn [114] used FL and IoT to enhance the security for smart healthcare. They considered different research work for the security-enhancing process using FL in IoT enhanced smart healthcare.

FL enables privacy-preserving real-time data collection in continuous health monitoring. Differential privacy and homomorphic encryption were both used by Das et al. [115] presented a FL-based framework for wearable-enabled personalized healthcare where they addressed its guiding principles, obstacles, and possibilities, showcasing its adaptability and potential to enhance patient insights and health care systems.

To ensure patient confidentiality in remote care settings, Iqbal et al. [116] employed Domain adaptive FL for EC-enabled privacy-preserving MRI analysis. Hakak et al. [117] studied an EC-assisted data analytics framework that used FL to retrain local ML models using user-generated data. Their framework leveraged pre-trained models to extract user-customized insights while preserving privacy and Cloud resources. Ganesh and Ramanaiah [118] delved into the evolution of FL and EC, exploring their convergence in the context of smart healthcare. It examined various applications of FL and EC within healthcare, from remote patient monitoring to predictive analytics and personalized medicine. Jia et al. [119] presented the personalized meta-FL framework for personalized IoT-enabled health monitoring. Ewejobi et al. [120] provided a mini review on homomorphic encryption for Genomics data storage on a federated cloud. This provides secure collaborative genetic dataset analysis for disease research while having strong privacy protection. Yuan et al. [121] proposed an advanced FL framework to train deep neural networks, where the network is partitioned and allocated to IoT devices and a centralized server. Alasbali et al. [122] integrated FL in an IoT-enabled EC for privacy-enhanced skin disease classification. FL was shown to be useful in health monitoring systems by Zhang et al. [123]. They proposed a dropout-tolerable scheme in which the process of FL would not be terminated if the number of online clients is not less than a preset threshold.

Table 6 below summarizes some of the principal research comparing different FL techniques and related privacy measures in health applications. Such research shows how FL can provide data-driven insights without invading the privacy of private health information.

Table 6: Summary of FL techniques and privacy methods in healthcare applications

Author (s)	Application	Privacy technique	Key results
Abbas et al. [112]	Smart Healthcare (IoT devices, wearables, and remote monitoring)	Security risks	Enabled secure training without centralizing patient data.

(Continued)

Table 6 (continued)

Author (s)	Application	Privacy technique	Key results
Ramesh et al. [113]	IoT Healthcare	FL and EC (IoT)	Decentralized patient data processing
Lanka and Mood-hitaporn [114]	Smart Healthcare (IoT)	FL and IoT	Securing the data of IoT-based sensors using FL
Das et al. [115]	Health monitoring	Differential Privacy, Homomorphic Encryption	Secure real-time monitoring of patient data.
Iqbal et al. [116]	MRI analysis	FL and EC	Safeguarding patient privacy
Hakak et al. [117]	Healthcare data analytics	FL and EC	Preserving privacy
Ganesh and Ramanaiah [118]	Smart healthcare systems	FL and EC	Remote patient monitoring
Jia et al. [119]	Health monitoring	FL and IoT-enabled computing framework	Real-world health monitoring
Ewejobi et al. [120]	Genomic analysis	Homomorphic encryption	Secured inter-institution genomic analysis.
Yuan et al. [121]	Healthcare, IoT	FL and IoT	Data privacy and Security
Alasbali et al. [122]	Skin disease classification	FL and IoT-EC	Protect patient sensitive data
Zhang et al. [123]	IoT-Enabled Healthcare	Homomorphic encryption	Private data aggregation from wearables.

3.8.3 FL Applications in Smart Cities

FL, which improves data privacy, scalability, and collaborative learning across urban systems, offers smart cities several advantages. Regarding data privacy, FL permits local data processing, guaranteeing the protection of sensitive data, including individual travel habits and energy use. There is less chance of privacy invasion because just the model parameters are disclosed [100,124]. Moreover, the decentralized structure of FL is scalable and capable of handling big, heterogeneous datasets produced by a variety of city systems, such as energy grids, traffic, and other sensors [125,126].

Real-time learning is essential in dynamic urban situations like traffic management, requiring prompt choices. Without the delay of central systems, FL supports adaptive learning by enabling continuous model updates directly on edge devices [127,128]. According to Zhang et al., [129] and Myakala et al. [130], FL promotes interdepartmental cooperation by enabling municipal agencies to exchange views without disclosing confidential data, strengthening group urban initiatives for traffic reduction and energy saving.

Traffic management is one of the practical uses of FL in smart cities, where information from smart traffic signals and linked cars enhances forecasts and controls congestion while protecting privacy [124,130]. By evaluating dispersed data from citywide sensors, FL facilitates effective resource distribution for energy consumption monitoring, lowering expenses and environmental impact [131]. FL facilitates rapid responses while upholding privacy requirements in public safety by supporting real-time monitoring and incident detection [132,133]. One of the difficulties is data heterogeneity, which leads to consistency problems in model convergence due to different formats from environmental devices, energy meters, and traffic sensors.

This issue is being addressed by continuing research [125,126]. Because sharing model updates across several devices results in substantial data transfer costs, especially in highly populated locations, communication overhead is another issue [129,130].

The security of FL models must be improved by countermeasures such as anomaly detection in updates, even if FL increases data privacy. This is because FL is still susceptible to security risks, including model poisoning and inference assaults [127,131]. These advancements highlight how crucial FL is to facilitating safer, more effective, and cooperative smart city operations. Security issues, such as the possibility of model poisoning, further highlight the necessity for strong countermeasures to guarantee the dependability of FL applications. Table 7 outlines the main uses and difficulties of FL in the context of smart cities, showing how this technology makes collaborative, safe, and scalable urban improvements possible.

Table 7: Summary of FL applications in smart cities

Aspect	Description	References
Data privacy	FL enables decentralized processing, keeping sensitive data like travel patterns and energy usage local, sharing only model updates.	[100,124]
Scalability	FL handles large, diverse data from traffic, energy, and sensor networks across urban systems.	[125,126]
Real-time learning	Supports adaptive edge learning, enabling fast traffic and service responses without central latency.	[127,128]
Collaborative learning	City departments can collaborate securely, improving strategies in areas like energy conservation without sharing raw data.	[129,130]
Traffic management	Enhances congestion prediction using data from connected vehicles and smart traffic signals while preserving privacy.	[124,130]
Energy monitoring	Aggregates sensor data to optimize energy usage, reduce costs, and lower environmental impacts.	[131,132]
Public safety	Enables real-time surveillance and incident response with built-in privacy protection.	[132,133]
Data heterogeneity	Varying formats across sensors challenge model training; FL requires tailored solutions.	[125,126]
Communication overhead	Sharing frequent updates in dense networks increases data transfer load.	[126,129]
Security risks	FL faces threats like model poisoning and inference attacks; anomaly detection is critical.	[127,131]

3.9 Consensus Algorithms in 5G/6G Networks

Distributed and edge-based 5G/6G networks require low-latency, secure consensus mechanisms. Table 8 summarizes commonly used algorithms.

PBFT is highly suitable for edge/fog deployments due to low-latency deterministic consensus. PoS can be applied in hybrid networks, while PoW is generally impractical [134,135].

Table 8: Consensus algorithms for 5G/6G networks

Algorithm	Mechanism	Advantages	Limitations	Suitability
PoW	Solve computational puzzles	High security	High energy, latency	Low
PoS	Validators by stake	Energy-efficient, lower latency	Risk of centralization	Moderate
PBFT	Voting-based	Low latency, high throughput	Scalability issues	High

3.10 FL Aggregation Techniques

FL aggregates local updates to train a global model without sharing raw data. Two common methods are FedAvg and secure aggregation.

3.10.1 FedAvg (Federated Averaging)

In FL's methodology, the FedAvg algorithm (presented in Algorithm 1) is the most widely adopted aggregation technique. It iteratively updates the global model by averaging locally trained client models, weighted by the proportion of local data. This ensures scalability across heterogeneous client devices while maintaining data privacy.

Algorithm 1: FedAvg aggregation [136]

```
Initialize global model $w_0$
for each round $t = 1, \ldots, T$ do
    Select subset of clients $S_t$
    for each client $k$ in $S_t$ do
        $w_k^t$ = ClientUpdate$(k, w_t)$
    end for
    $w_{t+1} = \sum_{k \in S_t} \frac{n_k}{n} w_k^t$
end for
function ClientUpdate$(k, w)$
    $w_k = w$
    for each local epoch $e$ do
        $w_k = w_k - \eta \nabla L(w_k)$
    end for
    return $w_k$
end function
```

3.10.2 Secure Aggregation

Secure aggregation protects client updates, revealing only the aggregated model. It is essential for privacy-sensitive 5G/6G applications [102].

3.11 Ongoing Standardization Efforts and Interoperability in 5G/6G and AI

Ensuring interoperability and standardization in 5G/6G networks and AI-enabled systems is crucial for large-scale deployment. Several ongoing initiatives aim to harmonize communication protocols, security, and AI governance.

3.11.1 Standards and Regulatory Efforts

- **IEEE:** IEEE 802.11 and 802.15 working groups define wireless communication protocols and interoperability guidelines. IEEE P2413 provides architectural standards for IoT systems, facilitating integration across heterogeneous devices.
- **3GPP:** 3GPP Release 17 and 18 introduce 5G enhancements for URLLC, massive IoT, and AI/ML integration, promoting inter-network compatibility and edge AI support.
- **NIST:** The National Institute of Standards and Technology (NIST) provides guidelines for AI system evaluation, including trustworthiness, robustness, and secure FL frameworks [137].
- **EU AI Act:** The European Union's AI Act proposes risk-based regulatory frameworks to ensure AI transparency, accountability, and interoperability in cross-border applications [138].

3.11.2 Proposed Interoperability Framework

To achieve seamless integration between heterogeneous networks and AI systems, a three-layer interoperability framework can be considered as:

1. **Communication Layer:** Standardized protocols (e.g., 5G NR, IEEE 802.11/15) with secure handover and cross-network compatibility.
2. **Data and AI Layer:** FL and secure aggregation techniques with standardized model representation formats (e.g., ONNX, PMML) to enable cross-platform AI deployment.
3. **Governance Layer:** Alignment with international guidelines such as NIST AI Risk Management Framework and EU AI Act to ensure ethical, transparent, and auditable AI operations.

This framework ensures interoperability across multi-vendor networks, heterogeneous edge nodes, and AI-enabled applications in 5G/6G, supporting global scalability while adhering to emerging regulations.

3.12 Emerging Trends in 5G/6G BC and AI Security

Emerging technologies in 5G/6G networks are evolving at different time scales. For clarity, we categorize these trends into short-term and long-term developments, along with their rationale, as shown in Table 9.

Table 9: Short-Term vs. Long-Term Trends in 5G/6G Blockchain and AI security

Trend Horizon	Key trends	Rationale
Short-Term	Lightweight blockchain frameworks, edge-enabled federated learning, AI-assisted network optimization and anomaly detection.	Focused on immediate deployment needs, ensuring high efficiency, improved privacy, reduced latency, and compatibility with existing 5G infrastructures.
Long-Term	Quantum-safe encryption methods, decentralized AI governance models, and cross-domain interoperability across heterogeneous 6G ecosystems.	Aimed at preparing for quantum-era threats, ensuring long-term scalability, regulatory compliance, and secure integration of ultra-dense and autonomous networks.

3.12.1 Short-Term Trends

Following are some of the short-term trends:

- **Lightweight BC:** Optimized for low-power edge devices and constrained IoT nodes, enabling efficient consensus and data integrity without high computational overhead [139].
- **Edge-Based FL:** Deploying FL at the network edge reduces latency, preserves data privacy, and enables near-real-time analytics.
- **AI-Assisted Network Optimization:** Use of ML for traffic prediction, resource allocation, and anomaly detection in 5G/6G networks.

Rationale: These trends focus on practical deployment in the near term, leveraging existing technologies and standards to enhance efficiency, privacy, and security in edge and IoT-enabled 5G/6G networks.

3.12.2 Long-Term Trends

Following are some of the long-term trends:

- **Quantum-Safe Encryption:** Preparing networks for future quantum threats by developing cryptographic algorithms resistant to quantum attacks.
- **Fully Decentralized AI Governance:** Integration of BC and AI to create autonomous, auditable, and trustless AI ecosystems.
- **Cross-Domain Interoperability Frameworks:** Standardized architectures enabling seamless integration of 5G/6G networks, IoT, and AI across multiple vendors and regulatory regimes.

Rationale: These long-term trends anticipate future technological and regulatory challenges, focusing on scalability, post-quantum security, and global interoperability to ensure sustainable, resilient 5G/6G systems.

3.13 Scalability Analysis of BC in 6G Networks

Scalability is a critical concern for BC integration in 5G/6G networks, particularly due to the massive number of connected devices and high transaction rates. Two main approaches have emerged to improve BC scalability:

- **Sharding:** Divides the network into smaller, parallel-processing shards, reducing the load per node and increasing overall throughput [140].
- **DAG-Based Architectures:** Directed Acyclic Graph (DAG) structures such as IOTA or Tangle allow multiple transactions to be confirmed in parallel without requiring strict sequential block validation, improving TPS and lowering latency [141].

3.13.1 Transaction Throughput vs. Node Count

Table 10 compares the approximate throughput of different BC architectures with varying network sizes, based on recent studies.

Table 10: Comparative analysis: Transactions Per Second (TPS) vs. node count

Architecture	Node count	TPS	Reference
PoW (Bitcoin)	1000	~7	[134]
PBFT	50	~5000	[135]
Sharding-BC	1000	~10,000	[140]
DAG (IOTA)	1000	~100,000	[141]
PoS (Ethereum 2.0)	1000	~1000	[142]

3.13.2 Discussion

As the Table 10 shows, traditional PoW BC suffer from low TPS and limited scalability, making them unsuitable for high-density 6G networks. PBFT provides higher throughput but is limited by the number of nodes due to communication overhead. Emerging solutions such as sharding-based BC and DAG-based architectures can support the massive number of nodes and high transaction rates expected in 6G.

- **Sharding** achieves scalability by processing transactions in parallel shards, suitable for mid-term deployment in 6G edge networks.
- **DAG-Based BC** offers near-linear TPS scaling with the number of nodes and is promising for long-term 6G deployments, especially in IoT-dense environments.

Overall, integrating sharding or DAG-based BC with EC and FL frameworks can ensure secure, scalable, and efficient data processing in future 6G networks.

3.14 Differential Privacy in FL for 5G/6G Networks

FL often requires privacy preservation when aggregating model updates across distributed devices. Differential Privacy (DP) introduces controlled noise to model updates to prevent leakage of sensitive data. However, applying DP can degrade model accuracy, and tuning the privacy budget ϵ is critical.

3.14.1 Empirical Observations

Studies have shown the trade-off between privacy and accuracy, as presented in Fig. 7:

- Lower ϵ (stronger privacy) increases noise, which may reduce model accuracy.
- Higher ϵ (weaker privacy) retains model performance but exposes more information.

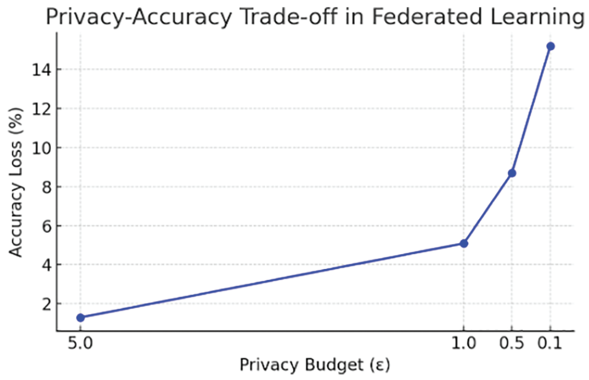

Figure 7: Illustration of the trade-off between privacy budget (ϵ) and model accuracy in FL. Adaptive DP dynamically adjusts noise to minimize accuracy loss

3.14.2 Adaptive Differential Privacy

To mitigate accuracy degradation, adaptive DP techniques dynamically adjust noise levels based on: 1) Model convergence rate, 2) Importance of specific updates, and 3) Sensitivity of the data being aggregated.

3.14.3 Discussion

This discussion highlights key insights and implications derived from our study, with a particular focus on privacy-preserving mechanisms in federated learning for 5G/6G edge scenarios.

- In 5G/6G edge scenarios, adaptive DP allows privacy-preserving FL while supporting latency-sensitive applications.
- The privacy-accuracy trade-off can be tuned per application (e.g., IoT telemetry, autonomous vehicles).
- Combining DP with secure aggregation ensures robust protection against data inference attacks, even when nodes are compromised.

Legal-Technical Co-Design for GDPR Compliance

BC's inherent immutability can conflict with GDPR's "right to erasure" (Article 17), creating legal challenges for storing personal data on-chain. To address this, legal-technical co-design approaches can be employed. Sensitive data can be stored off-chain in encrypted form with only cryptographic hashes maintained on-chain, allowing selective deletion without compromising auditability. Pruning and compression techniques, such as Merkle tree pruning or STARK-based proofs, can reduce on-chain storage requirements while retaining verifiable state. Additionally, selective encryption with key revocation can render personal data inaccessible, effectively achieving GDPR compliance. These strategies enable a balance between regulatory adherence, system performance, and verifiability, particularly benefiting resource-constrained edge nodes [53–55].

4 Interoperability Challenges of FL and BC

While FL and BC can complement each other to enhance security and privacy in 5G/6G networks, their integration poses several interoperability challenges. BC consensus mechanisms can introduce latency that delays FL model aggregation, potentially affecting convergence rates. Lightweight consensus protocols or asynchronous aggregation strategies can mitigate this issue. Additionally, combining decentralized FL with BC can lead to significant storage and computational overhead as the number of participants or model complexity increases. Techniques such as model compression, sharding, and off-chain storage of model parameters can alleviate scalability bottlenecks. Effective co-design of FL aggregation protocols and BC architectures is thus essential to balance latency, throughput, security, and storage efficiency, enabling practical and scalable deployments.

5 Integration of Digital Twins, FL, BC, and EC for Securing 6G Applications

The emergence of 6G networks promises ultra-high data rates, extremely low latency, and pervasive connectivity, enabling revolutionary applications such as autonomous transportation, holographic communications, industrial automation, and intelligent healthcare. However, due to the distributed, heterogeneous, and latency-sensitive nature of 6G services, such developments introduce unprecedented security and privacy challenges. Combining emerging paradigms, including digital twins (DT), FL, BC, and MEC, can provide a synergistic platform to address these challenges. A DT is a virtual replica of a physical system that is refreshed with real-time data. DTs in 6G can model the users' states, networks' states, and environmental states to enable predictive analysis and decision-making in real-time [143,144].

The integration of DT, FL, BC, and MEC forms a multi-layered architecture that is well-adapted to the 6G foundation principles of responsiveness, intelligence, and trust. Fig. 8 presents a framework for this integration. The lowest layer is shrouded by EC, e.g., MEC, which enables distributed data processing near where data is being generated, relieves the burden on centralized cloud resources, and complies with the latency requirements. It is also the foundation on which FL is implemented, which leverages the distributed nature of MEC to facilitate model training without sensitive data centralization.

DTs reside in the middle layer, tightly connected to the edge infrastructure. Each physical device (e.g., user device, intelligent car, or medical sensor) is represented by a digital twin that observes its activity, environmental data, and operational readings. Prediction models complement twins learned using FL to enable anticipatory decision-making (e.g., predicting vehicular traffic or patient deterioration) [145]. BC manages the trust and coordination layer, which secures model update exchanges and transaction history through smart contracts and consensus rules. BC provides non-repudiation, audibility, and tampering resistance. BC is significant in scenarios when edge nodes would be controlled by different administration domains (e.g., factories, traffic control, hospitals). This integration not only deals with security attacks but also enables secure collaboration among heterogeneous nodes.

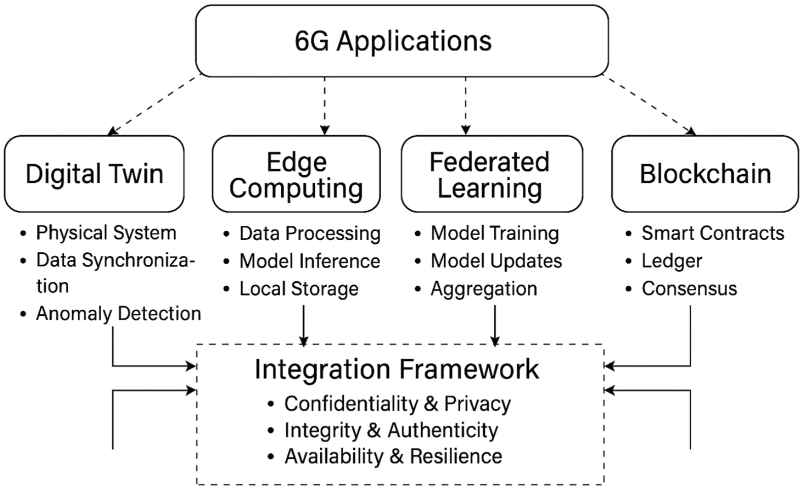

Figure 8: DT, MEC, FL, and BC integrated framework

5.1 Potential Use Cases of the Proposed Integrated Framework

This integration of DT, FL, BC, and EC can be depicted via heterogeneous 6G-enabled applications. This includes the following use cases [145,146].

1. Smart healthcare (Healthcare 5.0)
   DT can represent patient physiological variables such as heart rate, glucose level, and blood pressure, updated in real-time by wearable sensors. Predictive diagnosis is done using the twins. FL makes learning models shift locally in patient data, while keeping it private. BC makes sensitive health data private, grants access control to smart contracts, and audits medical data exchanges. EC performs initial processing (e.g., filtering the ECG signal) at bedside terminals, enabling fast response in case of emergencies.
2. Autonomous driving
   DTs of internal system (e.g., engine, sensors) and external world (e.g., traffic environment) are fitted in vehicles. They facilitate real-time decision-making. Vehicles learn to update their driving models (e.g., path planning, obstacle detection) without sharing raw sensor data via FL. These model updates are recorded via BC for integrity verification and cooperation among several transport authorities and vehicle manufacturers. Embedded edge nodes in vehicles and roadside units supply latency-sensitive computation.
3. Smart cities
   DTs model city infrastructures, including traffic lights, power grids, and water networks. FL offers city-wide prediction, e.g., predicting traffic congestion or power spikes. BC offers open data-sharing across departments (e.g., transport, energy) and verifies the source of control decisions. Edge devices, e.g.,

MEC servers embedded with smart meters and traffic cameras, perform local computation to provide quick feedback and control.

4. Industrial IoT (IIoT)
In manufacturing, DTs simulate production lines and the health status of machines. FL enables on-site learning from the behavior of machines for predictive maintenance and production optimization. BC offers secure supply chain logging of data, authenticity of components, and usage logs of machines. EC helps in real-time quality control and anomaly detection.
5. Immersive media and XR
DTs replicate user motions, environmental dynamics, and device interactions for applications such as holographic communication and interactive gaming. FL allows real-time personalization of immersive experiences. BC supplies ownership and traceability of virtual assets, and EC supplies ultra-low-latency rendering and media synchronization. Table 11 summarizes the key benefits of the integrated technologies for the previously mentioned applications.

Table 11: Role of DT, MEC, FL, and BC in 6G use cases

Use case	Role of DT	Role of FL	Role of BC	Role of MEC
Smart healthcare	Real-time patient monitoring	Local model training on patient data	Secure health record sharing	On-site data processing
Autonomous driving	Virtual vehicle modeling	Collaborative model updates	Tamper-proof logs	In-vehicle edge nodes
Smart cities	Infrastructure modeling	City-wide traffic forecasting	Transparent resource allocation	Real-time control systems
Industrial IoT	Machine state replication	Predictive maintenance models	Supply chain data integrity	On-site fault detection
Immersive media and XR	User/environment modeling	Experience personalization	Digital asset provenance	Low-latency rendering

5.2 *Workflow of the Framework*

Fig. 9 presents a systematic workflow architecture of 6G application security by leveraging the integration of DT, FL, BC, and EC. The workflow describes the processing of sensor data, learning from it, securing it, and utilizing it to enhance the robustness, privacy, and intelligence of 6G systems. The proposed framework consists of the following main layers.

1. Sensor devices (Data collection layer)
In the lowest layer, smart sensor devices such as IoT sensors, wearables, and embedded systems collect real-time information from the physical world. These sensors include biomedical sensors in a healthcare environment, LiDAR, radar, and cameras in autonomous vehicles, utility meters in a smart city, and industrial sensors in a production line. Such sensors continuously send raw data in the form of temperature, movement, audio, and health parameters, which are the sensory backbone of a 6G-enabled system. Data in this layer can be spoofed, tampered with, or subjected to man-in-the-middle attacks when not treated securely.
2. Edge node with EC (Data preprocessing and filtering)
The second stage comprises edge nodes, e.g., mobile base stations, smart gateways, and vehicular edge devices, equipped with EC capabilities. These nodes filter, normalize, and preprocess raw sensor data. Also, this layer extracts useful features for downstream operations and performs latency-sensitive

tasks like real-time detection, event triggering, or local control. EC avoids sending sensitive data unnecessarily across the network, reducing bandwidth usage and exposure risks. Furthermore, it enables confidentiality through local data processing and reduces reliance on centralized cloud servers.

3. Local DT instance (Real-time virtualization)
   A DT is at the edge of each physical thing (e.g., patient, car, smart meter). The twins contain a real-time, synchronized digital copy of the physical system, enabling simulation of future states, predictive diagnostics (e.g., vehicle or patient anomaly detection), and context-aware responses and situational awareness. DTs are equipped with processed data from edge nodes and replicate decision outcomes based on past and current conditions. Also, DTs provide semantic consistency and are essential for anomaly detection of suspicious behaviors that indicate cyber-physical attacks.
4. Training of FL (Coordinated edge model updates)
   The edge nodes and corresponding DTs contribute to FL by training local ML models on preprocessed and contextualized data, avoiding raw data exchange to maintain privacy, and generating encrypted or masked model updates (e.g., gradients or weights). This process takes place among a number of distributed edge devices concurrently, allowing each device to update a global model of intelligence without ever disclosing the user data. FL invokes data sovereignty and differential privacy and guards against model inversion attacks as well as data leakage.
5. BC for model aggregation (Trust infrastructure layer)
   Model updates generated by each node are sent to a BC network that verifies each update with digital signatures, uses consensus algorithms, e.g., proof of stake, practical Byzantine fault tolerance, to validate updates, and cancels smart contracts to automate reward, access, and verification. This prevents tampering, poisoning attacks, and provides a zero-trust architecture for the FL pipeline. BC ensures integrity, traceability, and non-repudiation of model updates and enables decentralized trust management.
6. Global model update (Knowledge fusion)
   Once validated by BC consensus, the model updates are combined into a global model through secure methods, e.g., federated averaging, returned to edge nodes and DTs, and refined iteratively over time through successive rounds of learning. This global intelligence is then put to use at the application level, driving intelligent 6G applications such as autonomous control systems, immersive XR environments, or personalized health diagnostics. Furthermore, this layer facilitates uniform and secure delivery of acquired intelligence, which is crucial for collaborative action in distributed settings. Table 12 summarizes the key functions of each component of the framework.

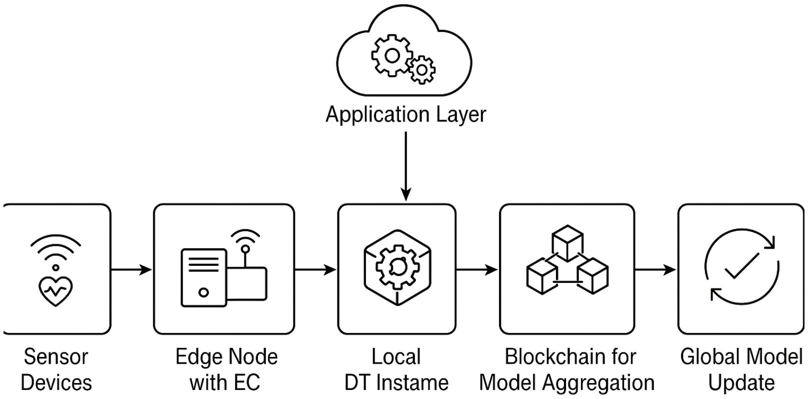

Figure 9: Workflow of DT, MEC, FL, and BC integrated framework

Table 12: Summary of the main functions of the key components of the framework

Component	Function	Security benefit
Sensor devices	Data sensing and streaming	Potential entry point for physical security hardening
EC	Data filtering, latency control	Preserves confidentiality and enables real-time defense
DT	Real-time mirroring, simulation, anomaly detection	Predicts and identifies abnormal behavior
FL	Decentralized model training	Prevents data exposure and supports privacy-preserving AI
BC	Immutable, consensus-based trust management	Ensures tamper-proof collaboration and auditability
Global model update	Fusion of knowledge and deployment	Delivers verified intelligence to all participants

5.3 Security Analysis of the Framework

The integrated DT-FL-BC-MEC model significantly enhances security by leveraging the unique strengths of each component.

1. Confidentiality and privacy
   As 6G networks become increasingly integrated into critical infrastructures such as healthcare, transportation, and smart government, the confidentiality of data and users' privacy take center stage. The highly distributed nature of these systems implies that vast amounts of sensitive information are generated and processed at the network edge. Traditional centralized security solutions are no longer sufficient, as they expose data to the risk of interception and misuse while being transmitted to central servers.
   FL in this context is a privacy-aware model that stores raw data locally, hence minimizing exposure. This is necessary in the case of privacy-concerned applications such as healthcare and personal mobility. EC also reduces privacy threats by offering localized data analysis and storage. In addition to this, BC technology also optimizes data access control by using smart contracts that apply fine-grained authorization and unalterable audit trails. Together, these technologies ensure a multi-layered defense mechanism that ensures confidentiality of the data but also maintains the usefulness of information in making intelligent decisions.
2. Integrity and authenticity
   Authenticity and integrity are necessary to ensure that data, control messages, and AI models in a 6G environment remain tamper-free and authentic. In applications such as autonomous vehicles or real-time diagnosis in healthcare, a slight change in the data or an unauthorized control message can prove catastrophic. Thus, end-to-end data integrity becomes mandatory, which cannot be waived.
   BC is one of the key elements of data integrity that maintains a tamper-proof record of all activity, including sensor logs, control messages, and AI model updates. Distributed verification protects against unauthorized updates and traceable entries allow auditing. In addition, attempted tampering is detectable with ease. DTs enable the monitoring of system behavior over time compared to forecast models and raise an alarm in real-time about divergence that may be a sign of data tampering or interference by an adversary. Thus, it can continuously authenticate physical system behavior, detecting

anomalies that could be indicators of spoofing or tampering. Furthermore, FL enables model updates to be traced back to source and permits malicious updates to be filtered through reputation mechanisms or Byzantine-resistant aggregation protocols.

3. Availability and resilience

   In future 6G systems, continuous availability of services and system fault or attack recoverability are critical to maintain user confidence and system reliability. For mission-critical use cases, e.g., industrial automation, and emergency response applications, service unavailability or reduced quality is unacceptable. Resilience, therefore, must be designed into all facets of the system.

   EC naturally enhances availability by distributing processing burdens across localized nodes, minimizing the likelihood of a central point failure. Even in the event of a loss of connectivity with the central cloud, edge nodes can continue to operate independently. Additionally, DTs offer predictive analytics by predicting potential system crashes or cyberattacks ahead of time in the physical world. The distributed nature of BC architecture further strengthens resilience through the guarantee that no single node holds essential data alone. This cooperative synergy ensures that services are robust, self-healing, and can function under stress or in partial system breakdown.

5.4 Trade-Offs in BC and FL for 5G/6G Security

While BC and FL each provide compelling advantages for securing 5G and 6G networks, both technologies introduce inherent trade-offs that can hinder large-scale deployment. Table 13 summarizes the major trade-offs, together with mitigation strategies offered by hybrid BC–FL approaches.

Table 13: Trade-offs in BC and FL with hybrid mitigation strategies

Technology	Advantages	Trade-offs/Limitations	Mitigation via Hybrid BC+FL
BC	Immutability and transparent record-keeping	High latency and energy consumption in consensus protocols; scalability bottlenecks with massive IoT devices	Lightweight consensus algorithms (e.g., PBFT, DPoS) combined with FL aggregation reduce redundant on-chain transactions
BC	Decentralized trust and tamper-evident storage	Increased storage/computation overhead at edge nodes	FL minimizes raw data exchanges, reducing BC transaction load
FL	Privacy-preserving collaborative model training	Reduced model accuracy under non-IID data and unbalanced client participation	BC ensures secure, auditable model aggregation and incentivizes honest participation
FL	Real-time threat detection at the edge	Susceptible to poisoning, backdoor, and free-rider attacks	BC provides verifiable update logs, reputation scoring, and consensus-based validation of local models
Hybrid BC + FL	Secure and privacy-preserving distributed intelligence	Higher communication and synchronization overhead	Adaptive model compression, hierarchical FL, and lightweight BC reduce costs while preserving robustness

Discussion: BC's immutability and decentralized design make it highly suitable for trust management and secure logging in wireless networks; however, its reliance on consensus protocols (e.g., Proof of Work, Proof of Stake) can result in *latency, scalability, and energy consumption bottlenecks*. On the other hand, FL enables *privacy-preserving data analytics* without raw data sharing, but is vulnerable to *model poisoning attacks and performance degradation* when client data is heterogeneous.

Hybrid frameworks that integrate BC and FL have recently emerged as promising solutions. For example, Sameera et al. [147] presents a comprehensive survey of FL-based intrusion detection approaches. It reviews the foundations of FL, highlights its advantages for privacy-preserving threat detection, and examines key challenges such as non-IID data, communication overhead, and security vulnerabilities. The study also discusses emerging solutions and outlines future research directions for deploying FL in real-world intrusion detection systems. Similarly, Ali et al. [148] present a survey on the integration of BC and FL for Internet of Things. They first used the notion of BC and its application in IoT systems. Then they described the privacy issues related to the implementation of BC in IoT and present privacy preservation techniques to cope with the privacy issues. Second, they introduced the FL application in IoT systems, devise a taxonomy, and present privacy threats in FL. Also, Ruckel et al. [149] present an FL system that incorporates BC technology, local differential privacy, and zero-knowledge proofs. Their implementation of a proof-of-concept with multiple linear regressions illustrates that these state-of-the-art technologies can be combined to a FL system that aligns economic incentives, trust, and confidentiality requirements in a scalable and transparent system.

By combining BC's transparency and auditability with FL's privacy-preserving model training, these hybrid schemes offer scalable, verifiable, and resilient security mechanisms for next-generation networks.

5.5 Trust Management

Establishing trust in highly distributed, multi-actor systems, such as those envisioned in 6G, is challenging. Devices, users, organizations, and services will not have prior relationships but must communicate securely and efficiently. Conventional identity and access control mechanisms are often inadequate for such dynamic and heterogeneous systems. Integrating BC enables establishing a decentralized trust model in which every transaction, update, or interaction is verifiable and recorded irrevocably.

Smart contracts allow the automatic enforcement of trust policies without human intervention. DTs enable contextual awareness and behavioral baselines for all physical and virtual things, enabling intelligent, semantic trust modeling. FL contributes to the scenario by enabling trusted AI collaboration without private data sharing. Together, all of these components form a zero-trust environment in which trust is continuously observed and enforced through transparent and verifiable means. Fig. 10 presents the secure communication flow over the proposed framework. Furthermore, Table 14 summarizes the key contributions of the security enhancements of the proposed technology-integrated framework.

5.6 Storage Optimization in Edge-Integrated BC

BC ledgers are inherently immutable, which poses challenges for edge nodes with limited storage capacity in 5G/6G networks. Without proper optimization, continuously growing ledgers can overwhelm resource-constrained devices, impacting performance and scalability.

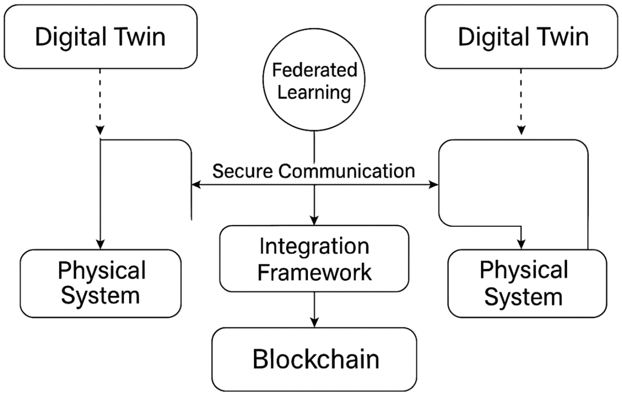

Figure 10: Security over the DT, MEC, FL, and BC integrated framework

Table 14: Security analysis of DT, MEC, FL, and BC framework

Security attribute	Contribution of DT	Contribution of FL	Contribution of BC	Contribution of MEC
Confidentiality	Behavior monitoring	Local data retention	Smart contract enforcement	Local data processing
Integrity	Real-time validation	Authentic model updates	Immutable ledger	System redundancy
Availability	Fault prediction	Distributed training	Decentralized storage	Edge redundancy
Trust management	Behavioral expectations	Participant authentication	Consensus-based trust	Localized decision making

5.6.1 Pruning Techniques

Pruning selectively removes historical transaction data that is no longer necessary for current operations while preserving cryptographic proofs required for auditability. Common approaches include:

- **State Pruning:** Only the latest state (e.g., account balances or aggregated model updates in FL) is retained, while older transactions are discarded. Merkle proofs ensure that removed transactions remain verifiable.
- **Checkpointing:** Periodically record a checkpoint summarizing ledger state, enabling nodes to discard older blocks while maintaining trust in the chain.

5.6.2 Compression and STARKs

Advanced cryptographic proofs such as STARKs (Scalable Transparent Arguments of Knowledge) allow:

- Verification of large computation histories using succinct proofs.
- Significant reduction in the amount of data stored on edge nodes, while retaining full auditability and tamper-resistance.
- Post-quantum security properties, ensuring long-term robustness in 6G networks.

5.6.3 Discussion

By combining pruning and STARK-based compression, as shown in Fig. 11:

- Edge nodes maintain a lightweight ledger without losing the ability to verify past transactions.
- Integration with FL ensures that only the necessary model updates or aggregated data are stored locally, reducing communication and storage overhead.
- Such techniques make BC feasible for resource-constrained environments, supporting real-time 5G/6G applications like IoT, vehicular networks, and edge AI.

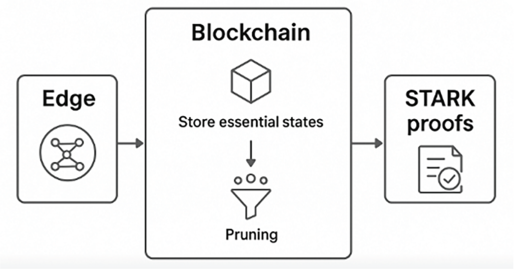

Figure 11: Edge-integrated BC with pruning and STARK-based compression: only essential states are stored locally, while proofs ensure full auditability

5.7 Potential Security Solutions for 5G/6G Networks

The security challenges in 5G/6G wireless networks are significant due to their ultra-dense connectivity, heterogeneous devices, and high data rates. To address these challenges, integrating FL with BC has emerged as a promising solution. FL enables distributed model training while keeping raw data local, thus mitigating privacy risks and reducing exposure to centralized attacks. BC provides decentralized trust, ensures data integrity, prevents single-point failures, and introduces incentive mechanisms for cooperative participants. The combination of BC and FL further strengthens network security by ensuring privacy-preserving, tamper-proof, and reliable operations. Additionally, cryptographic techniques such as homomorphic encryption, differential privacy, and quantum-safe protocols can be applied to enhance confidentiality and robustness in critical applications, including the Internet of Things (IoT) and Internet of Vehicles (IoV).

6 Lessons Learned and Future Research Trends

This section provides the key lessons learned from previous studies and highlights emerging research trends that can guide future investigations in BC, Fl and 5G/6G.

6.1 Lessons Learned

The following highlights the main takeaways from the survey:

1. Need for adaptive security frameworks: 5G and 6G networks are dynamic environments that are difficult for traditional, static security techniques to handle. BC and FL integration calls for flexible frameworks that can change to accommodate new threats, network architectures, and upcoming technologies. For example, integrating BC for real-time mitigation with AI-driven threat detection might greatly improve security.
2. Interdisciplinary innovation: BC and FL for 5G/6G security require interdisciplinary cooperation to be deployed successfully. Innovations that combine the concepts of EC, distributed systems, artificial

intelligence, and cryptography have shown greater success rates in thwarting threats like data tampering and DDoS attacks. This implies that future research should involve greater cross-domain collaborations.

3. Importance of lightweight and sustainable solutions: Lightweight solutions that reduce computational overhead and energy consumption are necessary due to the growing deployment of edge devices in 5G and 6G. Green computing techniques, including BC systems that use sharding or FL models tailored for low-power edge devices, should be incorporated into future security designs.
4. Ecosystem-wide standardization: A significant barrier has been identified as the lack of consistency in the application of FL and BC across 5G/6G infrastructures. To guarantee smooth implementation in various contexts, industry and academia must collaborate to create internationally accepted protocols and compatible frameworks.
5. Enhancing trust through federated systems: In decentralized networks, trust is vital. Consortium-based BC models or federated BC systems have the potential to balance stakeholder trust while resolving performance issues. For instance, combining reputation-based BC technology with hierarchical FL can produce safe trust models for extensive Internet of Things applications.
6. In addition, as discussed in Table 13, both BC and FL introduce inherent trade-offs that must be carefully balanced in real-world deployments. Hybrid BC-FL frameworks represent a promising research direction, as they combine the privacy-preserving intelligence of FL with the transparency and auditability of BC. Future work should explore lightweight consensus mechanisms, hierarchical FL architectures, and adaptive model compression to further mitigate communication overhead and latency, thereby enhancing the scalability of such systems in practical 5G/6G environments.
7. Challenges with Consensus Mechanisms in MEC:
   Scalability: Traditional blockchain consensus mechanisms like PoW and PoS may struggle to scale effectively in MEC environments due to the large number of edge devices and the dynamic nature of mobile networks.

- **Resource Constraints:** Edge devices often have limited computational power, memory, and battery life, making high-computation consensus mechanisms unsuitable.
- **Latency:** Consensus mechanisms need to meet the low-latency requirements of MEC applications, such as real-time data processing and IoT device coordination.
- **Security and Trust:** Ensuring security and trustworthiness in a decentralized manner without overloading edge nodes is a significant challenge.

6.2 Future Research Trends

Despite notable progress, some of the key challenges remain unresolved; this subsection outlines future research trends that can address these gaps and drive innovation.

1. **Integration of BC with cross-silo FL in 6G**
   Explore how BC can facilitate privacy-preserving collaboration among multiple service providers, industries, or governments through cross-silo FL models in 6G environments.
2. **Lightweight BC frameworks for edge-based FL in 5G/6G**
   Develop lightweight, resource-efficient BC architectures tailored for edge devices participating in FL within low-latency 6G networks.
3. **AI-driven consensus mechanisms for FL**
   Design intelligent consensus algorithms that dynamically adjust based on network traffic, trust scores, and FL performance to optimize BC performance in real-time communication systems.

4. **Quantum-resilient BC protocols for 6G security**
   As quantum computing emerges, secure BC protocols that are resistant to quantum attacks will be vital for long-term FL-6G ecosystems.
5. **Energy-efficient FL and BC synergy**
   Investigate optimization strategies for reducing the energy consumption of BC operations and FL model training on resource-constrained 5G/6G edge devices.
6. **Scalable incentive mechanisms for participation in FL over BC**
   Create reputation-based or tokenized incentive schemes using BC smart contracts to encourage long-term, honest participation in FL tasks.
7. **Standardization of BC-FL frameworks for multi-domain 6G applications**
   Develop interoperable frameworks and standards to support adoption across heterogeneous domains, such as autonomous vehicles, smart grids, healthcare, and finance.
8. **Adaptive privacy-preserving mechanisms for dynamic 6G environments**
   Propose flexible privacy-preserving models that adapt to changing network conditions, mobility patterns, and user contexts in 5G/6G networks.
9. **Real-time FL model auditing and traceability via BC**
   Enable real-time model auditability, provenance tracking, and rollback mechanisms using transparent BC logs in federated training pipelines.
10. **Secure multi-hop communication in federated edge networks using BC**
    Design BC-enhanced secure routing protocols to support FL across multi-hop, decentralized 5G/6G edge infrastructures.
11. Consensus mechanisms are a critical component of blockchain-enabled MEC systems, ensuring secure, decentralized, and reliable operations. However, selecting and optimizing these mechanisms to suit the unique demands of MEC remains an ongoing area of research. Future developments in this area will likely focus on scalability, resource efficiency, and maintaining security in diverse and dynamic EC environments.
12. To optimize blockchain-enabled MEC systems, researchers may explore some hybrid consensus mechanisms that combine the strengths of various protocols. For example, combining PoS for economic efficiency with PBFT for security can provide a balance between performance and security. Other approaches include developing lightweight consensus algorithms specifically designed for EC, which can minimize computational overhead and reduce latency while maintaining robust security features.

7 Conclusion

This paper has comprehensively reviewed the integration of BC and FL as transformative technologies for addressing the pressing security challenges in 5G/6G wireless networks. These next-generation networks bring unprecedented connectivity, speed, and scalability, and expose vulnerabilities that demand innovative solutions. BC's decentralized and immutable architecture provides robust mechanisms to mitigate threats such as DDoS attacks, data tampering, and impersonation. At the same time, FL ensures privacy-preserving model training and real-time anomaly detection. BC and FL's convergence offers not only strong security solutions but also a path to achieving the full potential of 5G/6G networks in creating secure, intelligent, and scalable communication environments. This survey highlights the synergistic potential of these technologies in securing wireless communication infrastructures, highlighting real-world implementations and their scalability across diverse applications, from IoT ecosystems to autonomous vehicles and smart cities. However, issues like computational overhead, energy efficiency, and the development of lightweight consensus mechanisms remain critical barriers to widespread adoption. Future research must focus on addressing these issues, exploring hybrid frameworks, and incorporating quantum-safe encryption and AI-driven threat mitigation.

Acknowledgement: The authors would like to thank Prince Sultan University for their support.

Funding Statement: This paper is derived from a research grant "Cybersecurity Research and Innovation Pioneers Grants Initiative" funded by The National Program for RDI in Cybersecurity (National Cybersecurity Authority)-Kingdom of Saudi Arabia-with grant number (CRPG-25-3168). This work was supported by EIAS Data Science and Blockchain Lab, CCIS, Prince Sultan University. Also, the authors would like to thank Prince Sultan University for paying the article processing fees for this paper.

Author Contributions: The authors confirm contribution to the paper as follows: The authors confirm contribution to the paper as follows: Conceptualization, Muhammad Asim; methodology, Muhammad Asim and Abdelhamied A. Ateya; investigation, Abdelhamied A. Ateya and Mudasir Ahmad Wani; writing—original draft preparation, Muhammad Asim, Abdelhamied A. Ateya; writing—review and editing, Muhammad Asim, Abdelhamied A. Ateya, Mohammed ELAffendi, Gauhar Ali, Mudasir Ahmad Wani, Ahmed A. Abd El-Latif and Reshma Siyal; visualization, Abdelhamied A. Ateya, Mudasir Ahmad Wani, Gauhar Ali, Reshma Siyal and Ahmed A. Abd El-Latif; supervision, Mohammed ELAffendi and Ahmed A. Abd El-Latif; project administration, Muhammad Asim, Abdelhamied A. Ateya and Mohammed ELAffendi; funding acquisition, Mohammed ELAffendi. All authors reviewed the results and approved the final version of the manuscript.

Availability of Data and Materials: Not applicable.

Ethics Approval: Not applicable.

Conflicts of Interest: The authors declare no conflicts of interest to report regarding the present study.

References

1. Chowdhury MZ, Shahjalal M, Ahmed S, Jang YM. 6G Wireless Communication Systems: applications, requirements, technologies, challenges, and research directions. IEEE Open J Commun Soc. 2020;1:957–75. doi:10.1109/ojcoms.2020.3010270.
2. Latif R, Ahmed MU, Tahir S, Latif S, Iqbal W, Ahmad A. A novel trust management model for edge computing. Complex Intell Syst. 2022;8:3747–63. doi:10.1007/s40747-021-00518-3.
3. Asim M, Wang Y, Wang K, Huang PQ. A review on computational intelligence techniques in cloud and edge computing. IEEE Trans Emerg Top Comput Intell. 2020;4(6):742–63. doi:10.1109/tetci.2020.3007905.
4. Ejaz M, Gui J, Asim M, El-Affendi MA, Fung C, Abd El-Latif AA. RL-Planner: reinforcement learning-enabled efficient path planning in multi-UAV MEC systems. IEEE Trans Netw Serv Manag. 2024;21(3):3317–29. doi:10.1109/tnsm.2024.3378677.
5. Shi W, Cao J, Zhang Q, Li Y, Xu L. Edge computing: vision and challenges. IEEE Internet Things J. 2016;3(5):637–46. doi:10.1109/jiot.2016.2579198.
6. Dustdar S, Avasalcai C, Murturi I. Invited paper: edge and fog computing: vision and research challenges. In: 2019 IEEE International Conference on Service-Oriented System Engineering (SOSE); 2019 Apr 4–9; San Francisco, CA, USA. Piscataway, NJ, USA: IEEE; 2019. p. 96–9609.
7. Rehman A, Haseeb K, Jeon G, Bahaj SA. Secure edge-based energy management protocol in smart grid environments with correlation analysis. Sensors. 2022;22:9236. doi:10.3390/s22239236.
8. Roman R, Lopez J, Mambo M. Mobile edge computing, Fog et al.: a survey and analysis of security threats and challenges. Future Gener Comput Syst. 2018;78:680–98. doi:10.1016/j.future.2016.11.009.
9. Asim M, Abd El-Latif AA, ELAffendi M, Mashwani WK. Energy consumption and sustainable services in intelligent reflecting surface and unmanned aerial vehicles-assisted MEC system for large-scale internet of things devices. IEEE Trans Green Commun Netw. 2022;6(3):1396–407. doi:10.1109/tgcn.2022.3188752.

10. Kaleem S, Sohail A, Tariq MU, Asim M. An improved big data analytics architecture using federated learning for IoT-enabled urban intelligent transportation systems. Sustainability. 2023;15(21):15333. doi:10.3390/su152115333.
11. Awan SA, Khattak MAK, Sathio AA, Farman H, Memon S, Nasralla MM, et al. Dynamic strategy for adaptive block size optimization in blockchain technology. Discov Sustain. 2025;6:849. doi:10.1007/s43621-025-01749-x.
12. Pan C, Ren H, Wang K, Kolb JF, Elkashlan M, Chen M, et al. Reconfigurable intelligent surfaces for 6G systems: principles, applications, and research directions. IEEE Commun Mag. 2021;59(6):14–20. doi:10.1109/mcom.001.2001076.
13. Asim M, ELAffendi M, El-Latif AAA. Multi-IRS and Multi-UAV-assisted MEC system for 5G/6G networks: efficient joint trajectory optimization and passive beamforming framework. IEEE Trans Intell Transp Syst. 2023;24(4):4553–64. doi:10.1109/tits.2022.3178896.
14. Ejaz M, Gui J, Asim M, Abd El-Latif AA, ElAffendi M, Fung C, et al. Joint optimization of AAV deployment and task scheduling in multi-AAV-enabled mobile edge computing systems. IEEE Internet Things J. 2025;12(18):37077–93. doi:10.1109/jiot.2025.3583204.
15. Asim M, Mashwani WK, Shah H, Belhaouari SB. An evolutionary trajectory planning algorithm for multi-UAV-assisted MEC system. Soft Comput. 2022;26(16):7479–92. doi:10.1007/s00500-021-06465-y.
16. Popovski P, Trillingsgaard KF, Simeone O, Durisi G. 5G wireless network slicing for eMBB, URLLC, and mMTC: a communication-theoretic view. IEEE Access. 2018;6:55765–79. doi:10.1109/access.2018.2872781.
17. Yang M, Qu Y, Ranbaduge T, Thapa C, Sultan N, Ding M, et al. From 5G to 6G: a survey on security, privacy, and standardization pathways. arXiv:2410.21986. 2024.
18. Nguyen VL, Lin PC, Cheng BC, Hwang RH, Lin YD. Security and privacy for 6G: a survey on prospective technologies and challenges. IEEE Commun Surv Tutor. 2021;23(4):2384–428.
19. Ahmad I, Shahabuddin S, Kumar T, Okwuibe J, Gurtov A, Ylianttila M. Security for 5G and beyond. IEEE Commun Surv Tutor. 2019;21(4):3682–722.
20. Ramezanpour K, Jagannath J. Intelligent zero trust architecture for 5G/6G networks: principles, challenges, and the role of machine learning in the context of O-RAN. Comput Netw. 2022;217:109358. doi:10.1016/j.comnet.2022.109358.
21. Chen X, Feng W, Ge N, Zhang Y. Zero trust architecture for 6G security. IEEE Netw. 2024;38(4):224–32. doi:10.1109/mnet.2023.3326356.
22. Alnaim AK. Securing 5G virtual networks: a critical analysis of SDN, NFV, and network slicing security. Int J Inf Secur. 2024;23(6):3569–89. doi:10.1007/s10207-024-00900-5.
23. Shehab MJ, Kassem I, Kutty AA, Kucukvar M, Onat N, Khattab T. 5G networks towards smart and sustainable cities: a review of recent developments, applications and future perspectives. IEEE Access. 2022;10:2987–3006. doi:10.1109/access.2021.3139436.
24. Mathur S, Kalla A, Gür G, Bohra MK, Liyanage M. A survey on role of blockchain for IoT: applications and technical aspects. Comput Netw. 2023;227:109726. doi:10.1016/j.comnet.2023.109726.
25. Sharma PK, Kumar N, Park JH. Blockchain technology toward green IoT: opportunities and challenges. IEEE Netw. 2020;34(4):263–9. doi:10.1109/mnet.001.1900526.
26. Conti M, Dehghantanha A, Franke K, Watson S. Internet of Things security and forensics: challenges and opportunities. Future Gener Comput Syst. 2018;78:544–6. doi:10.1016/j.future.2017.07.060.
27. Tang Y, Zhang Y, Niu T, Li Z, Zhang Z, Chen H, et al. A survey on blockchain-based federated learning: categorization, application and analysis. Comput Model Eng Sci. 2024;139:2451–77.
28. Jain AK, Gupta N, Gupta BB. A survey on scalable consensus algorithms for blockchain technology. Cyber Secur Appl. 2025;3:100065. doi:10.1016/j.csa.2024.100065.
29. Luo X, Yang P, Wang W, Gao Y, Yuan M. S-PoDL: a two-stage computational-efficient consensus mechanism for blockchain-enabled multi-access edge computing. Phys Commun. 2021;46:101338. doi:10.1016/j.phycom.2021.101338.
30. Mershad K. COSIER: a comprehensive lightweight blockchain system for IoT networks. Comput Commun. 2024;224:125–44. doi:10.1016/j.comcom.2024.06.007.

31. Xue H, Huang B, Qin M, Zhou H, Yang H. Edge computing for Internet of Things: a survey. In: 2020 International Conferences on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData) and IEEE Congress on Cybermatics (Cybermatics); 2020 Nov 2–6; Rhodes Island, Greece. Piscataway, NJ, USA: IEEE; 2020. p. 755–60.
32. Adam M, Hammoudeh M, Alrawashdeh R, Alsulaimy B. A survey on security, privacy, trust, and architectural challenges in IoT systems. IEEE Access. 2024;12:57128–49. doi:10.1109/access.2024.3382709.
33. Moghaddasi K, Rajabi S. Blockchain-enhanced offloading in mobile edge computing: a systematic review and survey of current trends and future directions. arXiv:2403.05961. 2024.
34. Xue H, Chen D, Zhang N, Dai HN, Yu K. Integration of blockchain and edge computing in Internet of Things: a survey. arXiv:2205.13160. 2022.
35. Luo Q, Hu S, Li C, Li G, Shi W. Resource scheduling in edge computing: a survey. arXiv:2108.08059. 2021.
36. Mach P, Becvar Z. Mobile edge computing: a survey on architecture and computation offloading. IEEE Commun Surv Tutor. 2017;19(3):1628–56.
37. Mikavica B, Kostić-Ljubisavljević A. Blockchain-based solutions for security, privacy, and trust management in vehicular networks: a survey. J Supercomput. 2021;77(9):9520–75. doi:10.1007/s11227-021-03659-x.
38. Luo Y, Gong B, Zhu H, Guo C. A trusted federated incentive mechanism based on blockchain for 6G network data security. Appl Sci. 2023;13(19):10586. doi:10.3390/app131910586.
39. Haddad Z. Enhancing privacy and security in 5G networks with an anonymous handover protocol based on Blockchain and Zero Knowledge Proof. Comput Netw. 2024;250:110544. doi:10.1016/j.comnet.2024.110544.
40. Maroufi M, Abdolee R, Tazekand BM, Mortezavi SA. Lightweight blockchain-based architecture for 5G enabled IoT. IEEE Access. 2023;11:60223–39. doi:10.1109/access.2023.3284471.
41. Yang M, Wang X, Qian H, Zhu Y, Zhu H, Guizani M, et al. An improved federated learning algorithm for privacy preserving in cybertwin-driven 6G system. IEEE Trans Ind Inform. 2022;18(10):6733–42. doi:10.1109/tii.2022.3149516.
42. Wan Y, Qu Y, Gao L, Xiang Y. Privacy-preserving blockchain-enabled federated learning for B5G-Driven edge computing. Comput Netw. 2022;204:108671. doi:10.1016/j.comnet.2021.108671.
43. Lu Y, Huang X, Zhang K, Maharjan S, Zhang Y. Blockchain and federated learning for 5G beyond. IEEE Netw. 2021;35(1):219–25. doi:10.1109/mnet.011.1900598.
44. Asad M, Shaukat S, Javanmardi E, Nakazato J, Bao N, Tsukada M. Secure and efficient blockchain-based federated learning approach for VANETs. IEEE Internet Things J. 2024;11(5):9047–55. doi:10.1109/jiot.2023.3322221.
45. Kalapaaking AP, Khalil I, Rahman MS, Atiquzzaman M, Yi X, Almashor M. Blockchain-based federated learning with secure aggregation in trusted execution environment for Internet-of-Things. IEEE Trans Ind Inform. 2023;19(2):1703–14. doi:10.1109/tii.2022.3170348.
46. Akoramurthy B, Surendiran B, Dhivya K, Chowdhury S, Govindaraj R, Mehbodniya A, et al. Chapter 8—Blockchain-based federated learning in internet of health things. In: Imoize AL, Obaidat MS, Song HH, editors. Federated learning for digital healthcare systems. Intelligent data-centric systems. San Diego, CA, USA: Academic Press; 2024. p. 175–201.
47. Azzaoui AE, Singh SK, Pan Y, Park JH. Block5GIntell: blockchain for AI-enabled 5G networks. IEEE Access. 2020;8:145918–35. doi:10.1109/access.2020.3014356.
48. Liu Y, Peng J, Kang J, Iliyasu AM, Niyato D, El-Latif AAA. A secure federated learning framework for 5G networks. IEEE Wirel Commun. 2020;27(4):24–31. doi:10.1109/mwc.01.1900525.
49. Du Q, Li B, Shao Z, Wu Y, Yang C. Chapter 4-Federated learning for distributed intrusion detection in IoT networks. In: Hoang DT, Hieu NQ, Nguyen DN, Hossain E, editors. Advanced machine learning for cyber-attack detection in IoT networks. San Diego, CA, USA: Academic Press; 2025. p. 85–110. doi:10.1016/b978-0-44-329032-9.00009-9.
50. Chelghoum M, Bendiab G, Labiod MA, Benmohammed M, Shiaeles S, Mellouk A. Blockchain and AI for collaborative intrusion detection in 6G-enabled IoT networks. In: 2024 IEEE 25th International Conference on High Performance Switching and Routing (HPSR); 2024 Jul 22–24; Pisa, Italy. Piscataway, NJ, USA: IEEE; 2024. p. 179–84.

51. Fu X, Peng R, Yuan W, Ding T, Zhang Z, Yu P, et al. Federated learning-based resource management with blockchain trust assurance in smart IoT. Electronics. 2023;12(4):1034. doi:10.3390/electronics12041034.
52. Liu Y, Jia Z, Jiang Z, Lin X, Liu J, Wu Q, et al. BFL-SA: blockchain-based federated learning via enhanced secure aggregation. J Syst Arch. 2024;152:103163. doi:10.1016/j.sysarc.2024.103163.
53. Zafar A. Reconciling blockchain technology and data protection laws: regulatory challenges, technical solutions, and practical pathways. J Cybersecur. 2025;11(1):tyaf002. doi:10.1093/cybsec/tyaf002.
54. Godyn M, Kedziora M, Ren Y, Liu Y, Song HH. Analysis of solutions for a blockchain compliance with GDPR. Sci Rep. 2022;12(1):15021. doi:10.21203/rs.3.rs-1712414/v1.
55. Haque AB, Islam AN, Hyrynsalmi S, Naqvi B, Smolander K. GDPR compliant blockchains—a systematic literature review. arXiv:2104.00648. 2021.
56. Shruti, Rani S, Sah DK, Gianini G. Attribute-based encryption schemes for next generation wireless IoT networks: a comprehensive survey. Sensors. 2023;23(13):5921. doi:10.3390/s23135921.
57. Behrad S, Bertin E, Crespi N. A survey on authentication and access control for mobile networks: from 4G to 5G. Ann Telecommun. 2019;74(9):593–603. doi:10.1007/s12243-019-00721-x.
58. Koutsouris N, Papanikitas K, Theologou M. Impact of data integrity verification on wireless agent-based applications. In: Proceedings of the 12th European Wireless Conference 2006—Enabling Technologies for Wireless Multimedia Communications; 2006 Apr 2–5; Athens, Greece. p. 1–7.
59. Islam MNU, Fahmin A, Hossain MS, Atiquzzaman M. Denial-of-service attacks on wireless sensor network and defense techniques. Wirel Pers Commun. 2021;116(3):1993–2021. doi:10.1007/s11277-020-07776-3.
60. Anmulwar S, Srivastava S, Mahajan SP, Gupta AK, Kumar V. Rogue access point detection methods: a review. In: Proceedings of the International Conference on Information Communication and Embedded Systems (ICICES2014); 2014 Feb 27–28; Chennai, India. p. 1–6.
61. Jimale MA, Z'aba MR, Kiah MLBM, Idris MYI, Jamil N, Mohamad MS, et al. Authenticated encryption schemes: a systematic review. IEEE Access. 2022;10:14739–66. doi:10.1109/access.2022.3147201.
62. Waqas M, Tu S, Halim Z, Rehman SU, Abbas G, Abbas ZH. The role of artificial intelligence and machine learning in wireless networks security: principle, practice and challenges. Artif Intell Rev. 2022;55(7):5215–61. doi:10.1007/s10462-022-10143-2.
63. Rathod T, Jadav NK, Alshehri MD, Tanwar S, Sharma R, Felseghi RA, et al. Blockchain for future wireless networks: a decade survey. Sensors. 2022;22(11):4182. doi:10.3390/s22114182.
64. Othman WM, Ateya AA, Nasr ME, Muthanna A, ElAffendi M, Koucheryavy A, et al. Key enabling technologies for 6G: the role of UAVs, terahertz communication, and intelligent reconfigurable surfaces in shaping the future of wireless networks. J Sens Actuator Netw. 2025;14(2):30. doi:10.3390/jsan14020030.
65. Mao B, Liu J, Wu Y, Kato N. Security and privacy on 6G network edge: a survey. IEEE Commun Surv Tutor. 2023;25(2):1095–127.
66. Nawaz SJ, Sharma SK, Wyne S, Patwary MN, Asaduzzaman M. Quantum machine learning for 6G communication networks: state-of-the-art and vision for the future. IEEE Access. 2019;7:46317–50. doi:10.1109/access.2019.2909490.
67. Dogra A, Jha RK, Jain S. A survey on beyond 5G network with the advent of 6G: architecture and emerging technologies. IEEE Access. 2021;9:67512–47. doi:10.1109/access.2020.3031234.
68. Ziegler V, Schneider P, Viswanathan H, Montag M, Kanugovi S, Rezaki A. Security and trust in the 6G era. IEEE Access. 2021;9:142314–27. doi:10.1109/access.2021.3120143.
69. Rajesh K, Vetrivelan P. Comprehensive analysis on 5G and 6G wireless network security and privacy. Telecommun Syst. 2025;88(2):52. doi:10.1007/s11235-025-01282-2.
70. Rashid A, Khan AR, Ashraf J. AI-driven security mechanisms for WLANs networks: streamlining, performance and reliability. Dialogue Soc Sci Rev (DSSR). 2025;3(6):243–63.
71. Humayun M, Jhanjhi N, Alruwaili M, Amalathas SS, Balasubramanian V, Selvaraj B. Privacy protection and energy optimization for 5G-aided industrial Internet of Things. IEEE Access. 2020;8:183665–77. doi:10.1109/access.2020.3028764.
72. Huang J, Qian Y, Hu RQ. Secure and efficient privacy-preserving authentication scheme for 5G software defined vehicular networks. IEEE Trans Veh Technol. 2020;69(8):8542–54. doi:10.1109/tvt.2020.2996574.

73. Al Ridhawi I, Otoum S, Aloqaily M, Jararweh Y, Baker T. Providing secure and reliable communication for next generation networks in smart cities. Sustain Cities Soc. 2020;56:102080. doi:10.1016/j.scs.2020.102080.
74. Hoque S, Aydeger A, Zeydan E, Liyanage M. A survey on distributed denial-of-service attack mitigation for 5G and beyond. IEEE Open J Commun Soc. 2025;6:5840–79. doi:10.1109/ojcoms.2025.3586199.
75. Kuadey NAE, Maale GT, Kwantwi T, Sun G, Liu G. DeepSecure: detection of distributed denial of service attacks on 5G network slicing—deep learning approach. IEEE Wirel Commun Lett. 2022;11(3):488–92. doi:10.1109/lwc.2021.3133479.
76. Patel N. AI-powered intrusion detection and prevention systems in 5G networks. In: Proceedings of the 2024 9th International Conference on Communication and Electronics Systems (ICCES); 2024 Dec 16–18; Coimbatore, India. p. 834–41.
77. Pirayesh H, Zeng H. Jamming attacks and anti-jamming strategies in wireless networks: a comprehensive survey. IEEE Commun Surv Tutor. 2022;24(2):767–809. doi:10.1109/comst.2022.3159185.
78. Mpitziopoulos A, Gavalas D, Konstantopoulos C, Pantziou G. A survey on jamming attacks and countermeasures in WSNs. IEEE Commun Surv Tutor. 2009;11(4):42–56.
79. Chen X, Ng DWK, Gerstacker WH, Chen HH. A survey on multiple-antenna techniques for physical layer security. IEEE Commun Surv Tutor. 2017;19(2):1027–53.
80. Arul Stephen C, Vijayalakshmi A, Broody J, Sathishkumar JS, Abishek BE, Sathish Kumar P. Detection of man in the middle attack in 5G IOT using machine learning. In: Proceedings of the 2023 International Conference on Recent Advances in Science and Engineering Technology (ICRASET); 2023 Nov 23–24; Nagara, India. p. 1–5.
81. Bhushan B, Sahoo G, Rai AK. Man-in-the-middle attack in wireless and computer networking—a review. In: Proceedings of the 2017 3rd International Conference on Advances in Computing, Communication & Automation (ICACCA) (Fall); 2017 Sep 15–16; Dehradun, India. p. 1–6.
82. Conti M, Dragoni N, Lesyk V. A survey of man in the middle attacks. IEEE Commun Surv Tutor. 2016;18(3):2027–51.
83. Babu PR, Bhaskari DL, Satyanarayana C. A comprehensive analysis of spoofing. Int J Adv Comput Sci Appl. 2010;1(6):157–62.
84. Dasgupta S, Rahman M, Islam M, Chowdhury M. A sensor fusion-based GNSS spoofing attack detection framework for autonomous vehicles. IEEE Trans Intell Transp Syst. 2022;23(12):23559–72. doi:10.1109/tits.2022.3197817.
85. Hoang VT, Ergu YA, Nguyen VL, Chang RG. Security risks and countermeasures of adversarial attacks on AI-driven applications in 6G networks: a survey. J Netw Comput Appl. 2024;232:104031. doi:10.1016/j.jnca.2024.104031.
86. Zhang H, Li J, Wang X. 6G technology risks: security threats, cybersecurity challenges, and countermeasures. Int J Commun Syst. 2024;37(5):e5234.
87. 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(3):281–91. doi:10.1016/j.dcan.2020.07.003.
88. Narsani HK, Ranjha A, Dev K, Memon FH, Qureshi NMF. Leveraging UAV-assisted communications to improve secrecy for URLLC in 6G networks. Digit Commun Netw. 2023;9(6):1458–64. doi:10.1016/j.dcan.2022.08.006.
89. Liu Y, Zhang T, Wang H. Supply chain attacks: examples and countermeasures. J Cybersecur Priv. 2022;2(1):1–10.
90. Li C, Liu C, Liu P, Li X, Qiu W, Lei L, et al. Blockchain-based privacy-preserving and accountable mobile edge outsourcing computing framework for the metaverse. IEEE Trans Green Commun Netw. 2025;9(2):711–24. doi:10.1109/tgcn.2024.3451513.
91. Zhang H, Leng S, Wu F, Chai H. A DAG blockchain-enhanced user-autonomy spectrum sharing framework for 6G-enabled IoT. IEEE Internet Things J. 2022;9(11):8012–23. doi:10.1109/jiot.2021.3109959.
92. Haddad Z, Fouda MM, Mahmoud M, Abdallah M. Blockchain-based authentication for 5G networks. In: Proceedings of the 2020 IEEE International Conference on Informatics, IoT, and Enabling Technologies (ICIoT); 2020 Feb 2–5; Doha, Qatar. p. 189–94.
93. Wijethilaka S, Kumar Yadav A, Braeken A, Liyanage M. Blockchain-based secure authentication and authorization framework for robust 5G network slicing. IEEE Trans Netw Serv Manag. 2024;21(4):3988–4005. doi:10.1109/tnsm.2024.3416418.

94. Li W, Su Z, Li R, Zhang K, Wang Y. Blockchain-based data security for artificial intelligence applications in 6G networks. IEEE Netw. 2020;34(6):31–7. doi:10.1109/mnet.021.1900629.

95. Rishiwal V, Agarwal U, Alotaibi A, Tanwar S, Yadav P, Yadav M. Exploring secure V2X communication networks for human-centric security and privacy in smart cities. IEEE Access. 2024;12:138763–88. doi:10.1109/access.2024.3467002.

96. Valitabar M, Fathi M, Navaie K. Efficient resource allocation for blockchain-enabled mobile edge computing: a joint optimization approach. IEEE Access. 2025;13:129011–23. doi:10.1109/access.2025.3590431.

97. Padmavathy TV, Goyal S. Blockchain based secure cross layer design for wireless sensor networks. In: Proceedings of the 2023 Second International Conference on Smart Technologies for Smart Nation (SmartTechCon); 2023 Aug 18–19; Singapore. p. 297–303.

98. Alzubi JA, Alzubi OA, Singh A, Mahmod Alzubi T. A blockchain-enabled security management framework for mobile edge computing. Int J Netw Manag. 2023;33(5):e2240. doi:10.1002/nem.2240.

99. McMahan B, Moore E, Ramage D, Hampson S, Arcas BA. Communication-efficient learning of deep networks from decentralized data. In: Artificial intelligence and statistics. London, UK: PMLR; 2017. p. 1273–82.

100. Kairouz P, McMahan HB, Avent B, Bellet A, Bennis M, Bhagoji AN, et al. Advances and open problems in federated learning. Found Trends® Mach Learn. 2021;14(1–2):1–210. doi:10.1561/2200000083.

101. Niknam S, Dhillon HS, Reed JH. Federated learning for wireless communications: motivation, opportunities, and challenges. IEEE Commun Mag. 2020;58(6):46–51. doi:10.1109/mcom.001.1900461.

102. Bonawitz K, Ivanov V, Kreuter B, Marcedone A, McMahan HB, Patel S, et al. Practical secure aggregation for privacy-preserving machine learning. In: Proceedings of the CCS '17: Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security; 2017 Oct 30–Nov 3; Dallas, TX, USA. p. 1175–91. doi:10.1145/3133956.3133982.

103. Amiri MM, Gündüz D. Federated learning over wirel fading channels. IEEE Trans Wirel Commun. 2020;19(5):3546–57. doi:10.1109/twc.2020.2974748.

104. Bonawitz K, Eichner H, Grieskamp W, Huba D, Ingerman A, Ivanov V, et al. Towards federated learning at scale: system design. Proc Mach Learn Syst. 2019;1:374–88.

105. Yu S, Cui L. Secure multi-party computation in federated learning. In: Security and privacy in federated learning. Cham, Switzerland: Springer; 2022. p. 89–98. doi:10.1007/978-981-19-8692-5_6.

106. Abadi M, Chu A, Goodfellow I, McMahan HB, Mironov I, Talwar K, et al. Deep learning with differential privacy. In: Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security; 2016 Oct 24–28; Vienna, Austria. New York, NY, USA: ACM; 2016. p. 308–18.

107. Fereidooni H, Marchal S, Miettinen M, Mirhoseini A, Möllering H, Nguyen TD, et al. SAFELearn: secure aggregation for private FEderated learning. In: 2021 IEEE Security and Privacy Workshops (SPW); 2021 May 27; San Francisco, CA, USA. p. 56–62. doi:10.1109/spw53761.2021.00017.

108. Fan S, Zhang H, Zeng Y, Cai W. Hybrid blockchain-based resource trading system for federated learning in edge computing. IEEE Internet Things J. 2021;8(4):2252–64. doi:10.1109/jiot.2020.3028101.

109. Huang X, Luo Y, Liu L, Zhao W, Fu S. Randomization is all you need: a privacy-preserving federated learning framework for news recommendation. Inf Sci. 2023;637:118943. doi:10.1016/j.ins.2023.118943.

110. Hernandez R, Bautista OG, Manshaei MH, Sahin A, Akkaya K. Outsourcing privacy-preserving federated learning on malicious networks through MPC. In: Proceedings of the 2023 IEEE 48th Conference on Local Computer Networks (LCN); 2023 Oct 2–5; Daytona Beach, FL, USA. p. 1–4.

111. Liu Y, Kang Y, Xing C, Chen T, Yang Q. A secure federated transfer learning framework. IEEE Intell Syst. 2020;35(4):70–82. doi:10.1109/mis.2020.2988525.

112. Abbas SR, Abbas Z, Zahir A, Lee SW. Federated learning in smart healthcare: a comprehensive review on privacy, security, and predictive analytics with IoT integration. Healthcare. 2024;12(24):2587. doi:10.3390/healthcare12242587.

113. Ramesh S, Prasanth A, Jain R, Meenakshi B, Kumari S, John Basha M. Enhancing IoT healthcare with federated learning and edge computing. In: Proceedings of the 2025 Third International Conference on Augmented Intelligence and Sustainable Systems (ICAISS); 2025 May 21–23; Trichy, India. p. 1065–71.

114. Lanka S, Moodhitaporn T. IoT security enhancements in smart healthcare using federated learning. In: Proceedings of the 2025 4th International Conference on Sentiment Analysis and Deep Learning (ICSADL); 2025 Feb 18–20; Bhimdatta, Nepal. p. 263–7.

115. Das S, Dutta S, Hazra S, Nandi S, Bandyopadhyay A, Disha M. Personalized healthcare empowered: federated learning integration with wearable device data for enhanced patient insights. In: Proceedings of the 2024 IEEE Region 10 Symposium (TENSYMP); 2024 Sep 27–29; New Delhi, India. p. 1–6.

116. Iqbal S, Choudhry IA, Ullah I, Kaur K, Choi BJ, Hassan MM. Domain adaptive FL for edge-enabled privacy-preserving MRI analysis. Alex Eng J. 2025;128:324–39. doi:10.1016/j.aej.2025.05.007.

117. Hakak S, Ray S, Khan WZ, Scheme E. A framework for edge-assisted healthcare data analytics using federated learning. In: Proceedings of the 2020 IEEE International Conference on Big Data (Big Data); 2020 Dec 10–13; Atlanta, GA, USA. p. 3423–7.

118. Ganesh D, Ramanaiah OBV. Edge federated learning for smart healthcare systems: applications and challenges. In: Proceedings of the 2024 4th International Conference on Sustainable Expert Systems (ICSES); 2024 Oct 15–17; Kaski, Nepal. p. 1727–35.

119. Jia Z, Zhou T, Yan Z, Hu J, Shi Y. Personalized meta-federated learning for IoT-enabled health monitoring. IEEE Trans Comput-Aided Des Integr Circuits Syst. 2024;43(10):3157–70. doi:10.1109/tcad.2024.3388908.

120. Ewejobi P, Okokpujie K, Adetiba E, Alao B. Homomorphic encryption for genomics data storage on a federated cloud: a mini review. In: Proceedings of the 2024 International Conference on Science, Engineering and Business for Driving Sustainable Development Goals (SEB4SDG); 2024 Apr 2–4; Omu-Aran, Nigeria. Piscataway, NJ, USA: IEEE; 2024. p. 1–13.

121. Yuan B, Ge S, Xing W. A federated learning framework for healthcare IoT devices. arXiv:2005.05083. 2020.

122. Alasbali N, Ahmad J, Siddique AA, Saidani O, Mazroa AA, Raza A, et al. Privacy-enhanced skin disease classification: integrating federated learning in an IoT-enabled edge computing. Front Comput Sci. 2025;7:1550677. doi:10.3389/fcomp.2025.1550677.

123. Zhang L, Xu J, Vijayakumar P, Sharma PK, Ghosh U. Homomorphic encryption-based privacy-preserving federated learning in IoT-enabled healthcare system. IEEE Trans Netw Sci Eng. 2022;10(5):2864–80. doi:10.1109/tnse.2022.3185327.

124. Pandya S, Srivastava G, Jhaveri R, Babu MR, Bhattacharya S, Maddikunta PKR, et al. Federated learning for smart cities: a comprehensive survey. Sustain Energy Technol Assess. 2023;55:102987. doi:10.1016/j.seta.2022.102987.

125. Yang Q, Liu Y, Chen T, Tong Y. Federated learning: concept and applications. ACM Trans Intell Syst Technol. 2019;10(2):1–19.

126. Mirmahaleh SYH, Rahmani AM. Federated learning in smart cities. In: Proceedings of the Model optimization methods for efficient and edge AI: federated learning architectures, frameworks and applications. Piscataway, NJ, USA: IEEE; 2025. p. 351–89. doi:10.1002/9781394219230.ch18.

127. Li T, Sahu AK, Talwalkar A, Smith V. Federated learning: challenges, methods, and future directions. IEEE Signal Process Mag. 2021;37(3):50–60. doi:10.1109/msp.2020.2975749.

128. Jarour A. Empowering smart cities through federated learning an overview. In: Proceedings of the 2024 28th International Conference on System Theory, Control and Computing (ICSTCC); 2024 Oct 10–12; Sinaia, Romania. p. 551–7.

129. Zhang W, Liu X, Zhu C, Varjonen S, Wang F, Tarkoma S. Federated learning meets urban opportunistic crowdsensing in 6G networks: opportunities, challenges, and optimization potentials. IEEE Netw. 2025;39(2):36–43. doi:10.1109/mnet.2024.3520552.

130. Myakala PK, Jonnalagadda AK, Bura C. Federated learning and data privacy: a review of challenges and opportunities. Int J Res Publ Rev. 2024;5(12):10–55248.

131. Gandhi M, Singh SK, Ravikumar R, Vaghela K. Federated learning in secure smart city sensing: challenges and opportunities. In: Proceedings of the Edge of intelligence: exploring the frontiers of AI at the edge. Hoboken, NJ, USA: John Wiley & Sons, Inc.; 2025. p. 215–51.

132. Pang Y, Ni Z, Zhong X. Federated learning for crowd counting in smart surveillance systems. IEEE Internet Things J. 2023;11(3):5200–9. doi:10.1109/jiot.2023.3305933.

133. Ahmadi-Assalemi G, Al-Khateeb H, Epiphaniou G, Maple C. Cyber resilience and incident response in smart cities: a systematic literature review. Smart Cities. 2020;3(3):894–927. doi:10.3390/smartcities3030046.
134. Nakamoto S. Bitcoin: a peer-to-peer electronic cash system [Internet]. [cited 2025 Nov 12]. Available from: https://metzdowdcom.
135. Castro M, Liskov B. Practical Byzantine fault tolerance. In: 3rd Symposium on Operating Systems Design and Implementation (OSDI 99); 1999 Feb 22–25; New Orleans, LA, USA. Berkeley, CA, USA: USENIX Association; 1999. p. 173–86.
136. McMahan HB, Moore E, Ramage D, Arcas BA. Federated learning of deep networks using model averaging. arXiv: 1602.05629. 2016.
137. NIST. AI risk management framework. Gaithersburg, MD, USA: NIST; 2023.
138. European Parliament, Council of the EU, European Commission. Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) [Internet]. Brussels, Belgium: European Commission; 2024 [cited 2025 Nov 12]. Available from: https://www.europeansources.info/record/proposal-for-a-regulation-laying-down-harmonised-rules-on-artificial-intelligence-artificial-intelligence-act-and-amending-certain-union-legislative-acts/.
139. Villegas-Ch W, Gutierrez R, Maldonado Navarro A, Mera-Navarrete A. Lightweight blockchain for authentication and authorization in resource-constrained IoT networks. IEEE Access. 2025;13:48047–67. doi:10.1109/access.2025.3551261.
140. Soltani P, Ashtiani F. Analytical modeling and throughput computation of blockchain sharding. arXiv:2210.04599. 2022.
141. Wang Q, Yu J, Chen S, Xiang Y. SoK: diving into DAG-based blockchain systems. arXiv:2012.06128. 2020.
142. Wu XB, Zou Z, Song D. Learn Ethereum: a practical guide to help developers set up and run decentralized applications with Ethereum 2.0. Birmingham, UK: Packt Publishing Ltd.; 2023.
143. Thang DV, Volkov A, Muthanna A, Koucheryavy A, Ateya AA, Jayakody DNK. Future of telepresence services in the evolving fog computing environment: a survey on research and use cases. Sensors. 2025;25(11):3488. doi:10.3390/s25113488.
144. Khan LU, Saad W, Niyato D, Han Z, Hong CS. Digital-twin-enabled 6G: vision, architectural trends, and future directions. IEEE Commun Mag. 2022;60(1):74–80. doi:10.1109/mcom.001.21143.
145. Masaracchia A, Sharma V, Canberk B, Dobre OA, Duong TQ. Digital twin for 6G: taxonomy, research challenges, and the road ahead. IEEE Open J Commun Soc. 2022;3:2137–50. doi:10.1109/ojcoms.2022.3219015.
146. Lin X, Kundu L, Dick C, Obiodu E, Mostak T, Flaxman M. 6G digital twin networks: from theory to practice. IEEE Commun Mag. 2023;61(11):72–8. doi:10.1109/mcom.001.2200830.
147. Sameera KM, Nicolazzo S, Arazzi M, Nocera A, Rafidha Rehiman KA, Vinod P, et al. Privacy-preserving in blockchain-based federated learning systems. Comput Commun. 2024;222:38–67. doi:10.1016/j.comcom.2024.04.024.
148. Ali M, Karimipour H, Tariq M. Integration of blockchain and federated learning for Internet of Things: recent advances and future challenges. Comput Secur. 2021;108:102355.
149. Rückel T, Sedlmeir J, Hofmann P. Fairness, integrity, and privacy in a scalable blockchain-based federated learning system. Comput Netw. 2022;202:108621. doi:10.1016/j.comnet.2021.108621.