World Journal of Advanced Research and Reviews
eISSN: 2581-9615 CODEN (USA): WJARAI
Cross Ref DOI: 10.30574/wjarr
Journal homepage: https://wjarr.com/

(REVIEW ARTICLE)

Check for updates

Security in the sixth generation cellular networks: A review

Collins Omondi Ogolla *

Jaramogi Oginga Odinga University of Science and Technology.

World Journal of Advanced Research and Reviews, 2025, 25(03), 2305-2334

Publication history: Received on 16 February 2025; revised on 29 March 2025; accepted on 31 March 2025

Article DOI: https://doi.org/10.30574/wjarr.2025.25.3.0634

Abstract

The advent of sixth-generation (6G) wireless networks promises unprecedented advancements in speed, latency, and connectivity, enabling futuristic applications such as holographic communication, intelligent edge computing, and ubiquitous AI-driven automation. However, these innovations introduce complex security challenges that must be addressed to ensure the resilience and reliability of 6G networks. This survey paper provides a comprehensive overview of emerging security threats in 6G, including quantum attacks, AI-driven cyber threats, privacy vulnerabilities, and challenges associated with terahertz (THz) communication and massive-scale device connectivity. This paper analyzes analyze existing security frameworks from 5G and discuss their limitations in the 6G era. Furthermore, it explores cutting-edge security solutions such as quantum cryptography, blockchain for decentralized trust, AI-powered threat detection, and secure-by-design architectures. By synthesizing current research trends and future directions, this paper aims to guide researchers, policymakers, and industry stakeholders in developing robust security mechanisms for next-generation wireless networks.

Keywords: 6G; Security; Privacy; Attacks; Threats; Authentication

1. Introduction

The rapid evolution of wireless communication technologies has led to the emergence of sixth-generation networks, expected to revolutionize connectivity with ultra-high data rates, near-zero latency, and intelligent, autonomous systems [1]-[5]. As shown in Figure 1, the 6G network aims to integrate advanced technologies such as artificial intelligence (AI), blockchain, quantum communication, and edge computing, enabling applications like holographic telepresence, smart cities, digital twins, and space-air-ground-sea integrated networks [6], [7]. While these advancements promise unprecedented societal and industrial transformations, they also introduce new and complex security challenges.

The transition from 5G to 6G brings about an expanded attack surface, driven by the massive deployment of Internet of Things (IoT) devices, the use of terahertz frequency bands, AI-powered network management, and decentralized architectures [8]-[10]. Traditional security mechanisms designed for 5G networks may be insufficient to address threats such as quantum attacks, AI-generated cyber threats, adversarial machine learning, and privacy breaches in ultra-dense connectivity environments [11]-[13]. Moreover, the integration of intelligent and autonomous decision-making systems in 6G networks raises concerns about security vulnerabilities in AI models, trust management in decentralized networks, and data integrity across interconnected systems. This survey paper provides a comprehensive analysis of the emerging security challenges in 6G networks, highlighting key vulnerabilities and potential attack vectors. It explores existing security mechanisms from previous generations and assess their applicability to the 6G era.

* Corresponding author: Collins Omondi Ogolla.

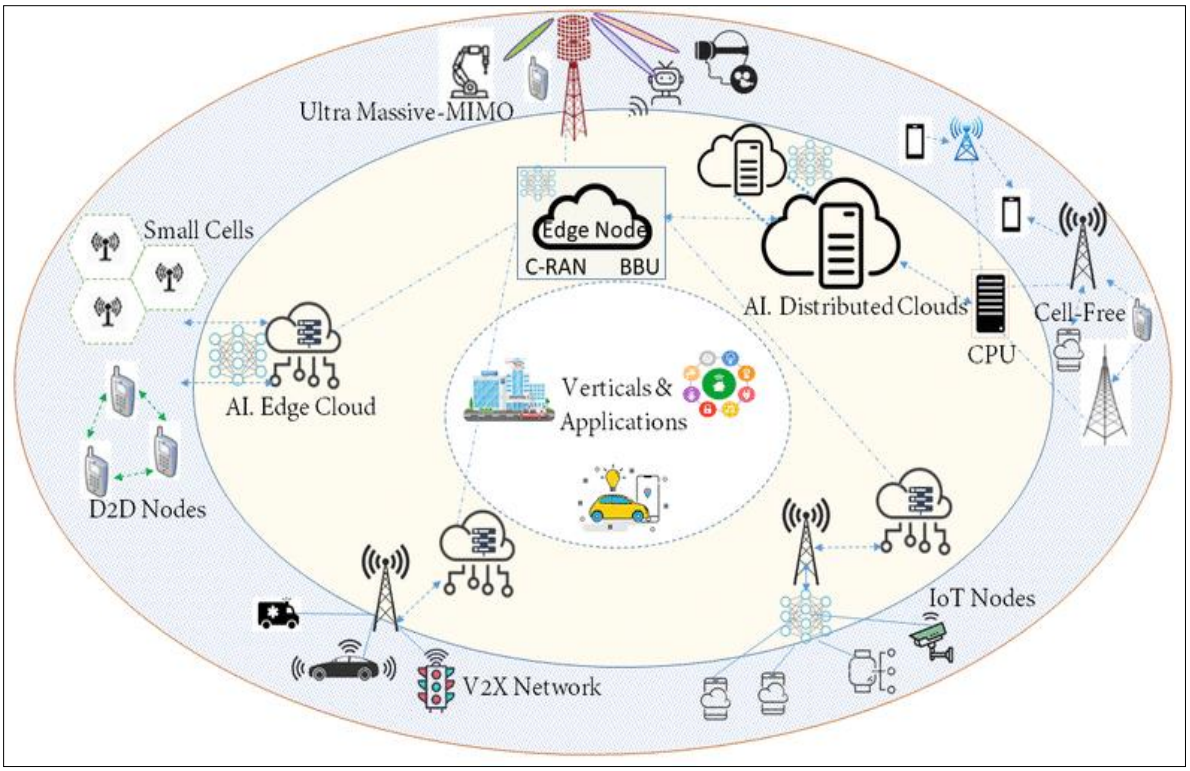

Figure 1 The 6G network environment

Furthermore, it discusses state-of-the-art security solutions, including quantum cryptography, AI-driven cybersecurity, blockchain-based trust frameworks, and privacy-enhancing technologies. By synthesizing current research trends and identifying future directions, this paper aims to provide valuable insights for researchers, industry stakeholders, and policymakers working toward the development of secure and resilient 6G communication systems.

2. 6G network architecture

The 6G network architecture represents a major shift from previous generations, incorporating advanced technologies to provide seamless, intelligent, and secure communication [14], [15]. It builds on a multi-layered infrastructure that extends beyond traditional terrestrial networks, integrating satellite, aerial, and underwater communication systems [16]-[17], as shown in Figure 2. This holistic approach ensures global connectivity, even in the most remote areas, and supports ultra-high data rates, near-instantaneous latency [20], and intelligent network automation.

One of the defining aspects of 6G is its reliance on artificial intelligence (AI) to manage and optimize network operations [21], [22]. Unlike previous generations, which required human intervention for most network adjustments, 6G will be largely autonomous. AI-driven self-optimizing networks will predict traffic patterns, allocate resources dynamically, and detect faults before they cause service disruptions [23]-[25]. These intelligent systems will also play a critical role in security, using deep learning algorithms to identify and neutralize cyber threats in real-time. AI-powered cognitive radio networks will further enhance spectral efficiency [26] by enabling dynamic spectrum allocation, allowing devices to communicate more efficiently without interference.

In terms of communication technologies, 6G will introduce terahertz (THz) communication, which operates in the 0.1–10 THz frequency range [27], [28]. This will enable data transmission at speeds in the terabits per second, allowing for ultra-fast wireless communication that supports bandwidth-intensive applications like holographic telepresence, extended reality (XR), and high-resolution 3D mapping. However, THz communication comes with challenges, such as limited propagation distance and vulnerability to atmospheric absorption [29]. To overcome these limitations, intelligent reflecting surfaces (IRS) will be deployed, using reconfigurable metamaterials to dynamically control wireless signals, enhance coverage, and improve energy efficiency.

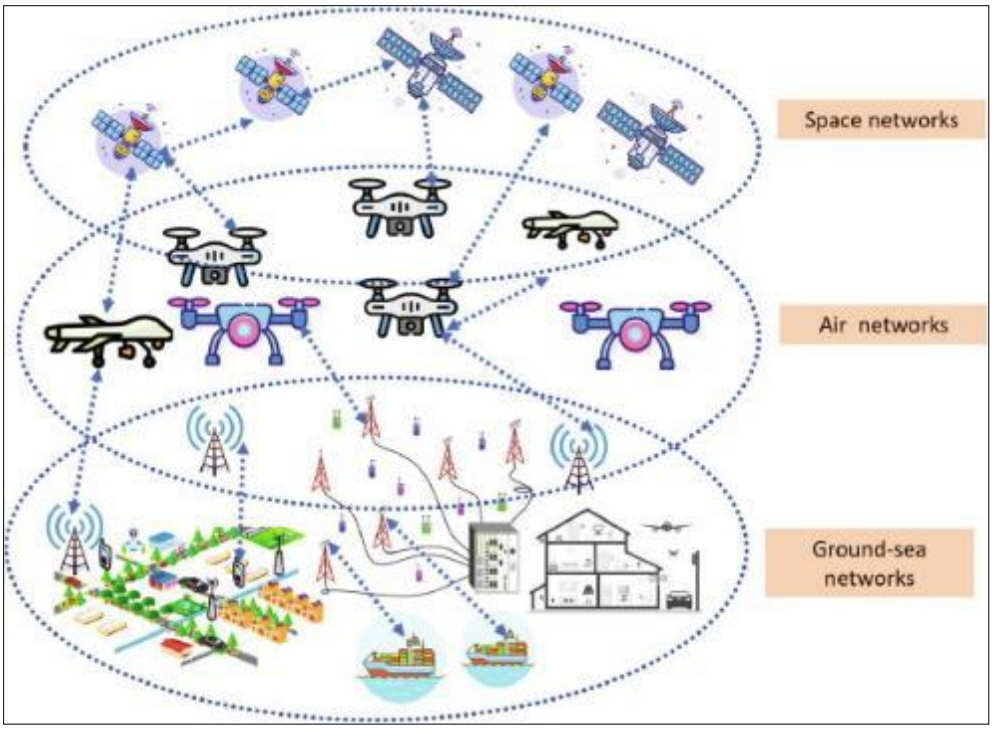

Figure 2 The 6G network technologies and applications

Another crucial component of 6G is integrated sensing and communication (ISAC) as illustrated in Figure 3. Unlike previous networks that primarily focused on data transmission, 6G will merge wireless communication with environmental sensing [30], enabling applications like gesture recognition, autonomous vehicle navigation, and smart infrastructure monitoring. This means that 6G networks will not only transmit data but also perceive and interpret their surroundings, opening new possibilities for human-machine interaction and real-time decision-making [31]-[34]. Optical wireless communication (OWC), including visible light communication (VLC) and free-space optical (FSO) communication, will complement radio frequency (RF) systems, offering high-speed data transmission in environments where traditional signals may be obstructed.

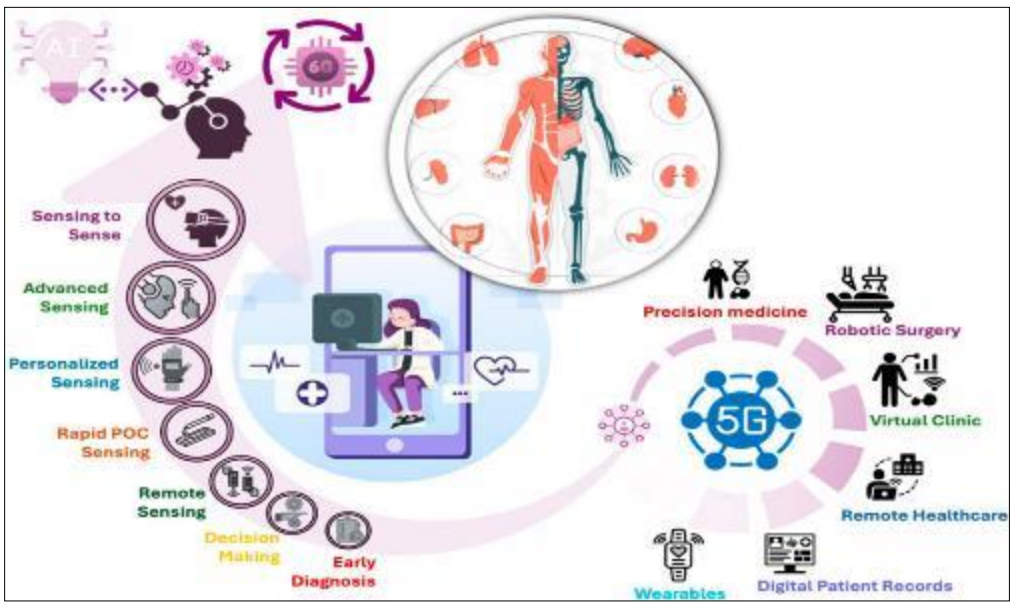

Figure 3 Integrated sensing and communication

Security in 6G networks will be fundamentally different from previous generations, incorporating decentralized and quantum-safe approaches. As shown in Figure 4, blockchain technology [35] will be widely used to enhance trust

management, ensuring secure identity verification and transaction processing without reliance on centralized authorities. Additionally, quantum communication and post-quantum cryptography will provide next-generation encryption techniques that are resistant to quantum computing attacks [36]-[40]. Traditional security mechanisms will no longer be sufficient, as quantum computers will have the ability to break existing encryption algorithms. Therefore, 6G networks will rely on quantum key distribution (QKD) to secure transmissions and prevent eavesdropping.

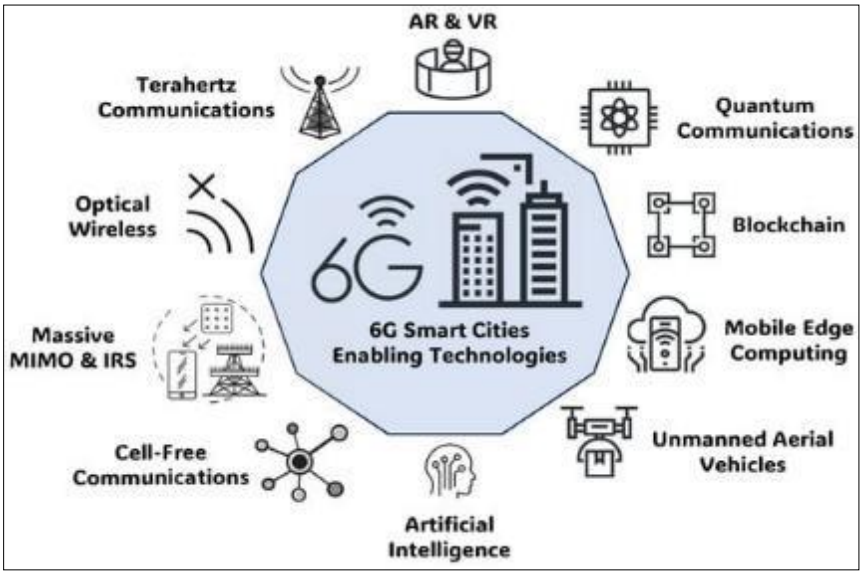

Figure 4 Enabling technologies in 6G

To support ultra-reliable and low-latency communication (URLLC), 6G will integrate edge and fog computing, processing data closer to the source rather than relying on distant cloud servers [41]-[44]. This will reduce latency and enhance security, making real-time applications such as remote surgery, autonomous vehicles [45], and industrial automation more efficient and reliable. The tactile internet will also emerge as a major innovation, enabling real-time haptic feedback for applications like remote-controlled robotics and virtual reality simulations.

The multi-layered infrastructure of 6G will extend beyond traditional terrestrial networks. As shown in Figure 2, satellites in Low Earth Orbit (LEO) and Geostationary Orbit (GEO) will provide global coverage, ensuring connectivity even in remote and underserved areas [46]-[49]. These satellite networks will communicate with aerial platforms such as high-altitude balloons and drones, which will serve as mobile base stations to extend coverage dynamically. The underwater communication layer will further expand connectivity to maritime and deep-sea applications [50], using optical and acoustic communication to support underwater IoT devices and ocean monitoring systems.

By integrating AI-driven automation, THz communication, blockchain-based security, quantum technologies, and multi-layered connectivity, the 6G network architecture will revolutionize the way we interact with the digital world [51]-[55]. It will not only enhance traditional mobile communication but also enable futuristic applications such as digital twins, holographic communication, and immersive extended reality experiences. These advancements will pave the way for a truly intelligent and interconnected society, where communication is instantaneous, secure, and seamlessly integrated into everyday life.

3. Security issues in 6G

The evolution from 5G to 6G introduces a new era of hyper-connectivity, driven by artificial intelligence, quantum computing, blockchain, and terahertz communication [56], [57]. While these advancements promise revolutionary applications, they also bring unprecedented security challenges. Unlike previous generations, 6G will not only connect humans but also integrate autonomous machines, smart environments, and space-based communication, significantly expanding the attack surface [58]. Ensuring the security, privacy, and trustworthiness of 6G networks will be a crucial challenge.

3.1. Expanded attack surface and new threat vectors

With 6G networks supporting massive machine-type communication (mMTC), including billions of IoT and edge devices, the number of potential attack points increases exponentially [59], [60] as evidenced in Figure 5. The integration of space, air, ground, and underwater communication layers further complicates security management [61]. This expanded attack surface creates multiple entry points for cyber threats such as Distributed Denial of Service (DDoS) attacks, data breaches, and AI-driven cyber threats.

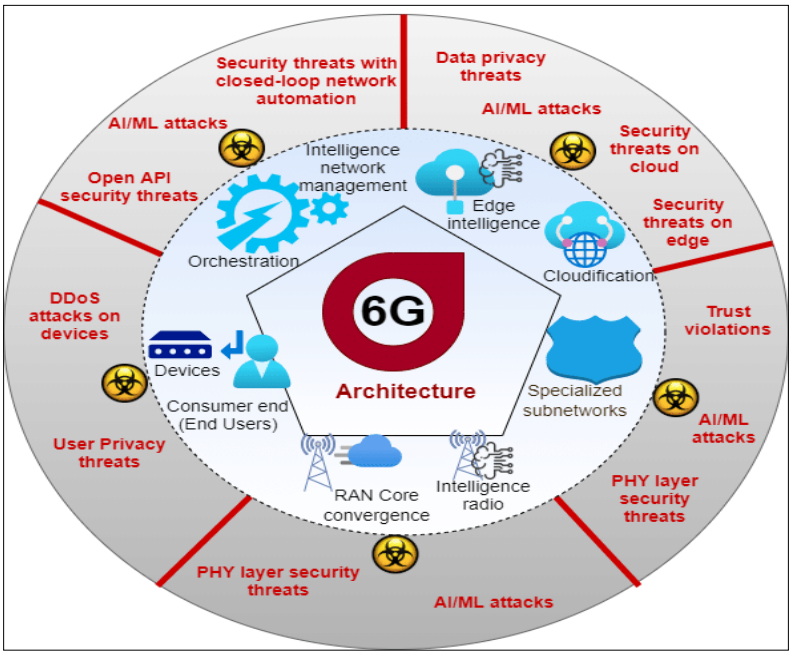

Figure 5 Threat landscape in 6G

6G will also rely heavily on AI for decision-making, which introduces vulnerabilities in AI models themselves [62]. Adversarial machine learning attacks, where attackers manipulate input data to deceive AI algorithms, can lead to incorrect network decisions, opening new security risks [63]-[65]. Attackers may target AI-driven network automation systems to cause disruptions, data poisoning, or biased decision-making.

3.2. Threats from quantum computing

One of the most significant challenges in 6G security is the rise of quantum computing, which threatens traditional cryptographic mechanisms [66]-[68]. Current encryption techniques, such as RSA and ECC (Elliptic Curve Cryptography), rely on the difficulty of mathematical problems like prime factorization, which quantum computers can solve exponentially faster using Shor's algorithm. This makes existing encryption techniques obsolete, leaving 6G networks vulnerable to decryption and data breaches.

To counteract quantum threats, 6G must adopt post-quantum cryptography (PQC) and quantum key distribution [69]. PQC involves cryptographic algorithms designed to withstand quantum attacks, while QKD leverages quantum mechanics principles to create theoretically unbreakable encryption keys [70]. However, the integration of these quantum-safe techniques will require significant infrastructural changes and computing resources.

3.3. Privacy and data security concerns

6G networks will facilitate ultra-high-speed data exchange across smart cities, healthcare, autonomous vehicles, and industrial automation, raising critical privacy concerns [71]-[74]. The pervasive nature of 6G means vast amounts of sensitive data will be continuously collected, processed, and transmitted, making privacy protection more complex. One major risk is data exposure through edge computing and fog computing. Since 6G will rely on edge nodes to process data closer to users, unauthorized access [75] to edge devices could lead to massive data breaches. Edge devices may lack the computational resources to run advanced security mechanisms, making them attractive targets for cybercriminals [76].

Homomorphic encryption (shown in Figure 6) and differential privacy will be essential in addressing these privacy risks. Homomorphic encryption allows computations on encrypted data without decryption, ensuring privacy preservation in cloud and edge computing environments [77]-[80].

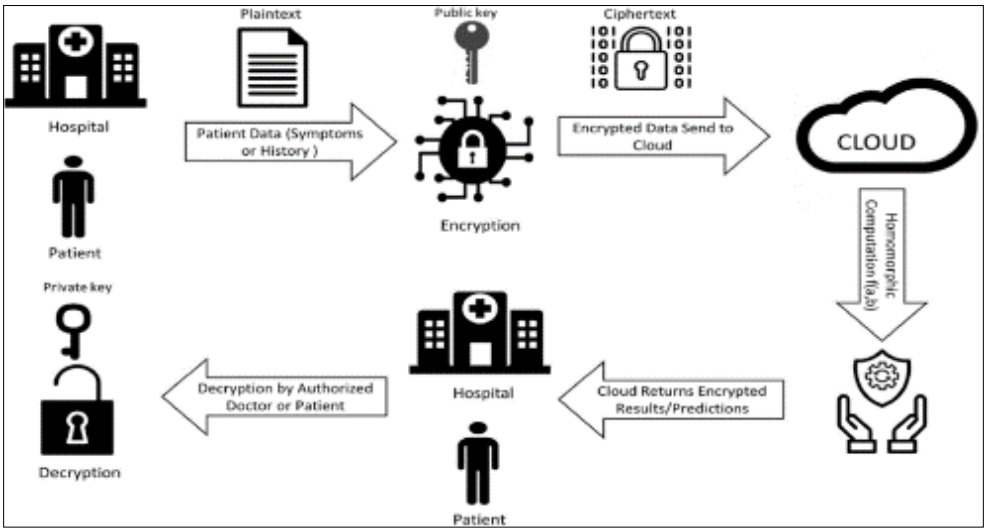

Figure 6 Homomorphic encryption

Differential privacy techniques help minimize the risk of identifying individuals from aggregated datasets, making it useful for applications like smart healthcare and personalized AI services.

3.4. AI-driven cyber threats

As shown in Figure 7, AI has become a core component of 6G security systems. However, it can also be exploited by cybercriminals. AI-powered attacks will enable sophisticated cyber threats such as automated phishing, deepfake-based social engineering, and AI-generated malware [81]-[84]. Attackers may also deploy Generative Adversarial Networks (GANs) to manipulate security models, bypass authentication mechanisms [85], and create deceptive attacks that traditional security systems cannot detect.

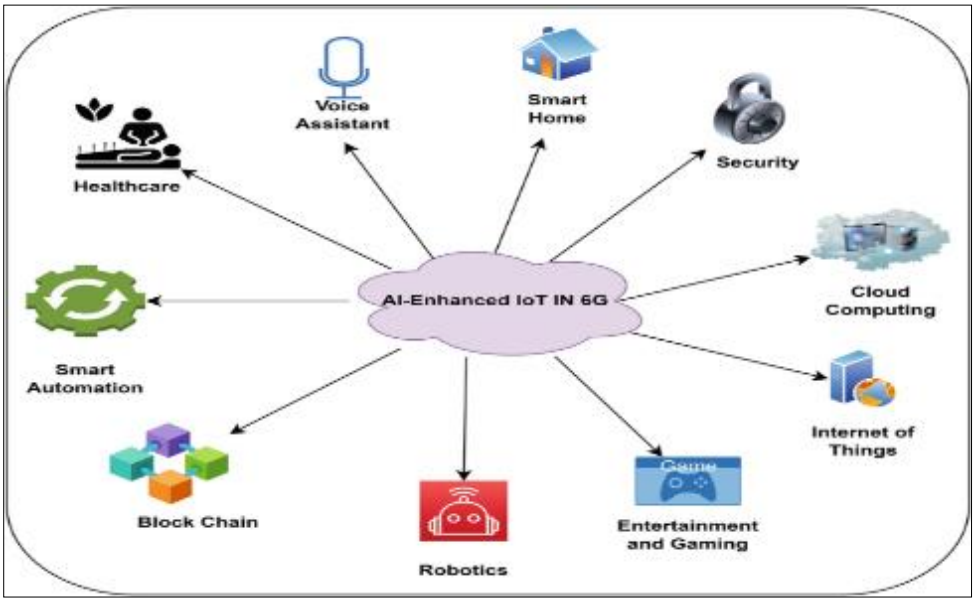

Figure 7 AI in 6G networks

Furthermore, AI models used in 6G security frameworks are susceptible to model inversion attacks, where attackers reconstruct original input data from AI model outputs [86]-[89]. This can lead to severe privacy violations, especially in

applications involving biometric authentication or personal health data. Ensuring AI robustness in 6G requires adversarial training, secure federated learning, and AI explainability mechanisms to detect and prevent manipulative attacks.

3.5. Blockchain security challenges

Blockchain technology is expected to play a key role in 6G security, particularly in trust management, identity authentication [90], and secure transactions. This is well illustrated in Figure 8. However, blockchain itself is not immune to security threats. The increasing computational demand for blockchain-based security solutions raises concerns about scalability and energy efficiency in 6G networks [91], [92]. Blockchain-based smart contracts, which automate transactions and agreements, can introduce vulnerabilities if not properly secured [93], [94]. Reentrancy attacks and logic flaws in smart contracts can be exploited to manipulate transactions or drain cryptocurrency wallets. Additionally, consensus algorithm attacks, such as 51% attacks, can compromise blockchain networks, leading to fraudulent data manipulation.

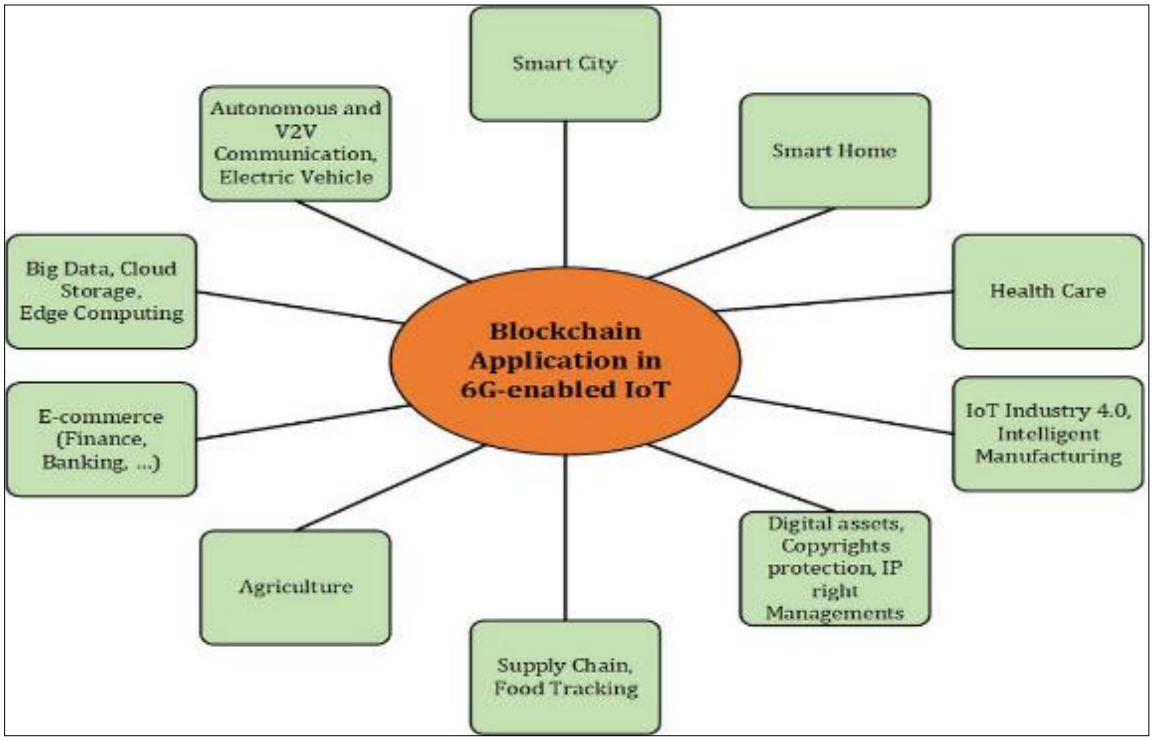

Figure 8 Blockchain use cases in 6G networks

To address these concerns, lightweight blockchain solutions and zero-knowledge proofs (ZKPs) can be employed to enhance security while minimizing computational overhead [95], [96]. ZKPs allow verification of transactions without revealing sensitive information, ensuring privacy and security in decentralized applications.

3.6. Secure device authentication and trust management

With billions of interconnected devices in 6G, ensuring secure authentication and trust management becomes a critical challenge [97]-[100]. Traditional centralized authentication systems may not scale efficiently, leading to increased vulnerability to identity spoofing, credential theft, and unauthorized access. One of the major security risks is device impersonation attacks, where malicious entities disguise themselves as legitimate devices to gain network access [101]. Such attacks can be particularly dangerous in applications like autonomous driving, where false sensor data could lead to catastrophic failures.

Decentralized identity management based on blockchain can mitigate these risks by eliminating single points of failure, as illustrated in Figure 9. Self-sovereign identity (SSI) models, where users control their own digital identities without relying on centralized authorities, can enhance security while maintaining privacy [102], [103].

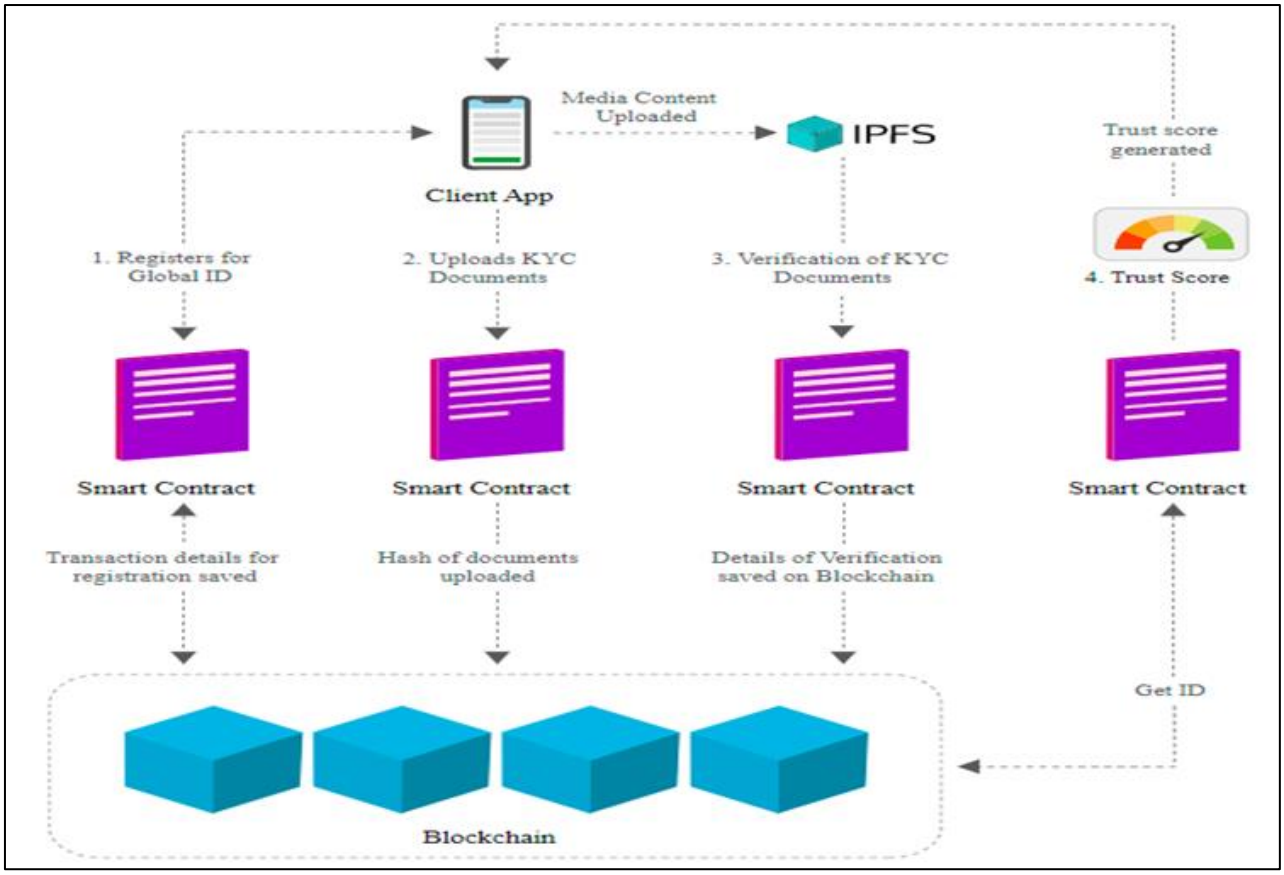

Figure 9 Blockchain-based identity management

Additionally, AI-driven behavioral authentication techniques can provide continuous user authentication based on behavioral patterns rather than static credentials.

3.7. Threats to terahertz (THz) communication

6G will utilize terahertz frequency bands to achieve ultra-high-speed wireless communication. However, THz signals are highly susceptible to eavesdropping, jamming, and signal interception due to their propagation characteristics [104],[105]. Unlike traditional radio waves, THz waves have limited penetration through obstacles, making them easy targets for localized interception attacks.

To enhance THz communication security, physical layer security (PLS) techniques such as beamforming, directional modulation, and cooperative jamming can be employed. These methods help protect THz signals from unauthorized interception [106] and ensure secure data transmission.

3.8. Supply chain and hardware security risks

The complexity of 6G networks introduces significant supply chain security risks. Many network components, including routers, base stations, and AI chips, are manufactured by multiple vendors, increasing the likelihood of hardware backdoors, firmware vulnerabilities, and counterfeit devices entering the supply chain [107]. Figure 10 gives an elaboration of typical supply chain attacks.

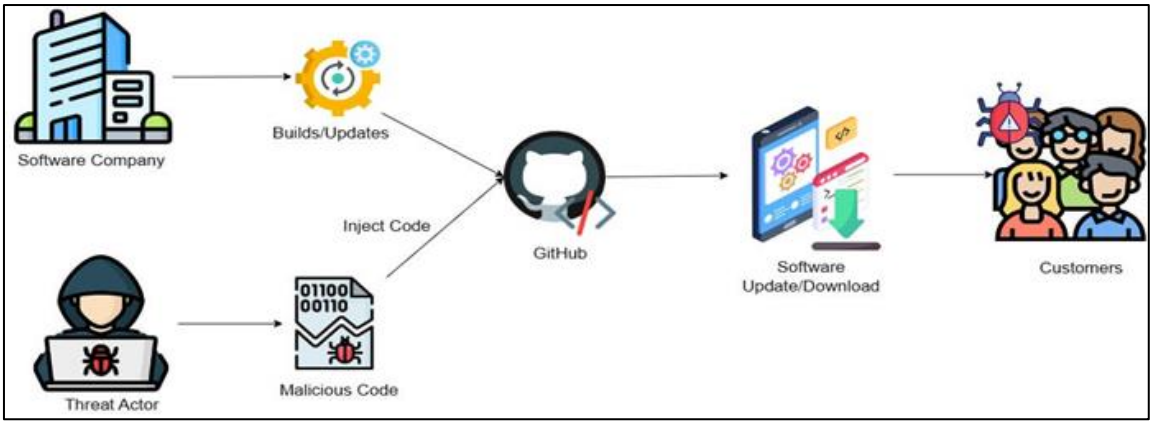

Figure 10 Supply chain risks

Hardware Trojans and malicious firmware injections pose serious threats to 6G security, as compromised components can be used for surveillance, data exfiltration, or network disruption [108], [109]. To mitigate these risks, 6G must adopt hardware attestation mechanisms, trusted execution environments (TEEs), and blockchain-based supply chain tracking to ensure the integrity of network infrastructure components.

It is evident that security in 6G networks will be more complex than in previous generations due to the integration of AI, quantum computing, blockchain, and THz communication. The vast attack surface, coupled with AI-driven cyber threats and quantum vulnerabilities, necessitates a multi-layered security approach. Quantum-safe cryptography, AI-based intrusion detection, decentralized trust management, and hardware attestation will play a crucial role in securing 6G networks [110], [111]. Addressing these challenges proactively is essential to ensure that 6G can deliver secure, reliable, and privacy-preserving communication in the hyper-connected future.

4. Security solutions in 6G

The transition to 6G networks introduces new technologies and applications that demand robust, adaptive, and future-proof security solutions. Traditional security approaches will not be sufficient due to the expanded attack surface, quantum computing threats, AI-driven cyberattacks, and the integration of space-air-ground-underwater networks [112]. 6G security solutions must incorporate advanced cryptographic techniques, AI-based security frameworks, blockchain trust mechanisms, and physical layer security to ensure end-to-end protection.

4.1. Quantum-safe cryptography and secure key management

One of the most pressing concerns in 6G security is the advent of quantum computing, which threatens traditional encryption methods [113], [114]. Classical encryption schemes such as RSA and ECC (Elliptic Curve Cryptography) rely on mathematical problems that quantum computers can solve efficiently using algorithms like Shor's Algorithm, making current security protocols obsolete. To counteract quantum threats, 6G will employ the following techniques.

4.1.1. Post-Quantum Cryptography (PQC)

PQC involves cryptographic algorithms that are resistant to quantum attacks. These algorithms are based on mathematical problems that remain difficult even for quantum computers [115]. PQC refers to cryptographic algorithms designed to withstand attacks from quantum computers, which can break traditional encryption schemes like RSA and ECC using algorithms such as Shor's algorithm [116], [117]. Unlike classical cryptography, PQC relies on mathematical problems that remain difficult even for quantum computers, such as lattice-based, hash-based, code-based, and multivariate polynomial-based cryptography illustrated in Figure 11. These algorithms ensure secure encryption, digital signatures, and key exchanges in a post-quantum era. Since quantum computers pose a serious threat to data confidentiality and integrity [118], PQC is essential for future-proofing security in 6G networks, IoT devices, and cloud computing environments. Prominent PQC techniques include:

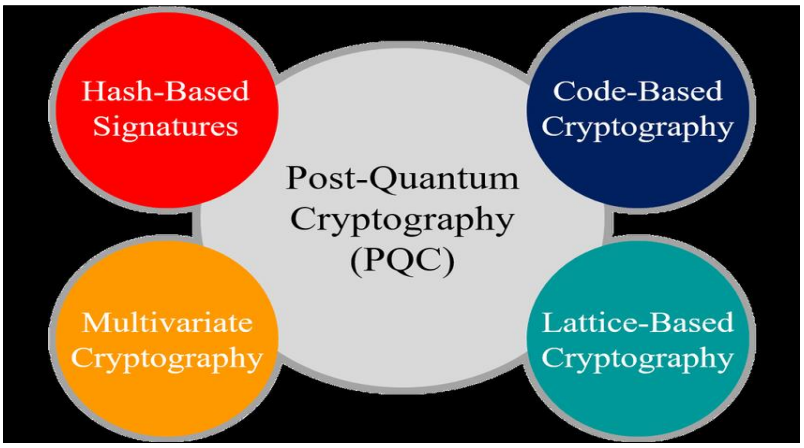

Figure 11 post-quantum cryptography

- **Lattice-based cryptography**: Uses high-dimensional lattices to create encryption keys that are resistant to quantum decryption [119].
- **Hash-based cryptography**: Relies on cryptographic hash functions for secure digital signatures [120].
- **Code-based cryptography**: Based on error-correcting codes to ensure secure key exchanges [121].
- **Multivariate polynomial cryptography**: Uses complex polynomial equations that quantum computers cannot efficiently solve [122].

4.1.2. Quantum Key Distribution (QKD)

QKD is a revolutionary cryptographic method that enables two parties to generate and exchange encryption keys [123] securely using quantum mechanics principles. As shown in Figure 12, QKD is a secure communication method that uses the principles of quantum mechanics to generate and exchange encryption keys between two parties, ensuring confidentiality even against quantum computer attacks [124]-[127]. Unlike classical cryptographic key exchange methods, QKD relies on quantum states—typically photons—encoded in different quantum bases.

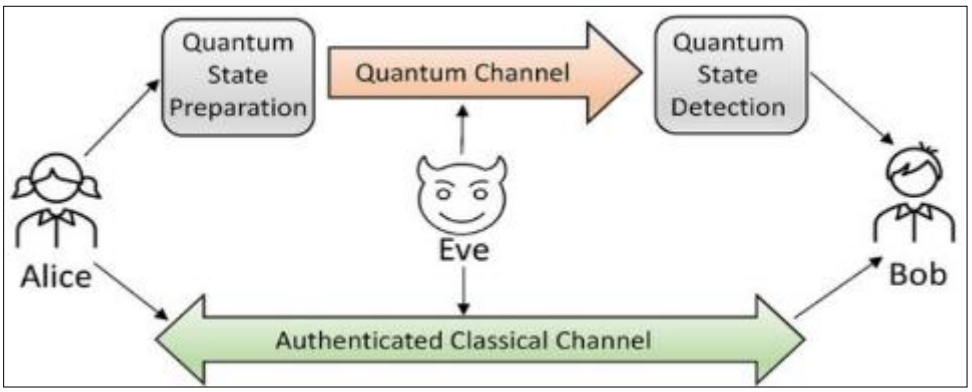

Figure 12 Quantum key distribution protocol

If an eavesdropper attempts to intercept the transmission [128], quantum mechanics laws (such as the Heisenberg Uncertainty Principle and quantum no-cloning theorem) ensure that any intrusion alters the quantum state, alerting the communicating parties to a security breach. Protocols like BB84 and E91 enable secure key distribution, making QKD a crucial technology for achieving quantum-safe encryption in 6G networks and beyond. If an eavesdropper attempts to intercept the key exchange, quantum mechanics laws will detect their presence, ensuring secure communication.

BB84 Protocol: One of the most widely used QKD protocols [129], where key bits are encoded in photon states.

E91 Protocol: Uses quantum entanglement for secure key generation [130].

4.1.3. Lightweight cryptography for IoT and edge devices

Since 6G will support a massive number of IoT and edge devices with limited computing power, lightweight cryptographic algorithms must be deployed [131], [132]. Lightweight cryptography is a specialized form of encryption designed for IoT and edge devices with limited processing power, memory, and energy resources [133]. Traditional cryptographic algorithms, such as AES and RSA, are computationally intensive and unsuitable for resource-constrained environments [134]-[138]. Lightweight cryptographic techniques, such as PRESENT, HIGHT, Simon & Speck, and lightweight ECC, provide strong security while minimizing computational overhead and power consumption. These algorithms ensure secure data transmission, authentication, and integrity for billions of IoT devices in 6G networks, protecting them from cyber threats like data breaches and unauthorized access while maintaining efficiency in real-time operations. These lightweight algorithms include:

PRESENT Cipher: A lightweight block cipher suitable for IoT encryption [139].

HIGHT Cipher: Designed for high-speed and low-power applications [140].

Elliptic Curve Cryptography (ECC) with optimized parameters for constrained devices.

4.2. AI-Driven security frameworks

As evidenced in Figure 13, artificial intelligence will play a pivotal role in 6G security by enabling real-time threat detection, adaptive security policies, and automated intrusion response [141]. AI-driven security frameworks leverage artificial intelligence and machine learning to detect, prevent, and respond to cyber threats in real time [142], [143]. These frameworks use deep learning, neural networks, and anomaly detection to analyze vast amounts of network traffic, identify suspicious patterns, and adapt security measures dynamically.

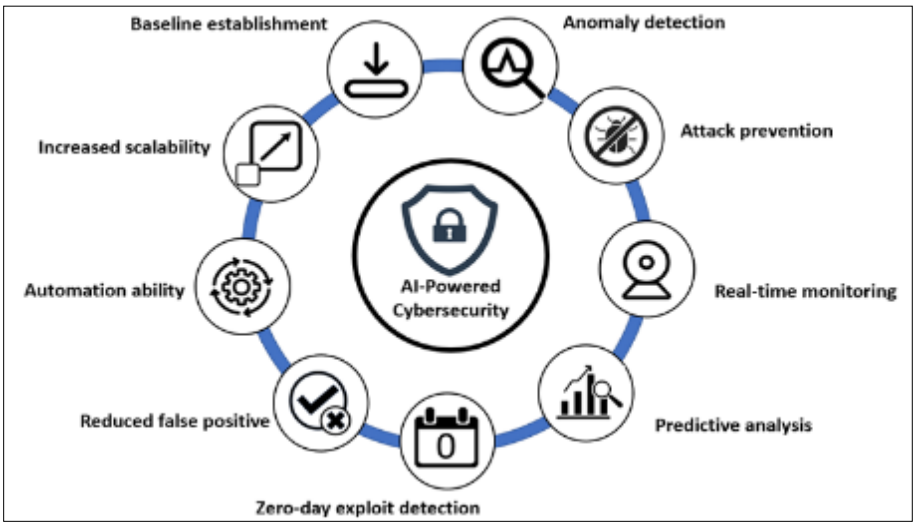

Figure 13 AI-driven security framework

AI enhances intrusion detection and prevention systems (IDPS), automates threat intelligence, and enables predictive analytics to mitigate cyberattacks before they occur. Additionally, techniques like federated learning ensure privacy-preserving AI training across decentralized 6G networks [144], [145]. While AI strengthens cybersecurity defenses, it also introduces risks such as adversarial attacks and data poisoning, necessitating robust AI security strategies to maintain trust and reliability in 6G networks. However, AI itself introduces new risks, such as adversarial attacks and model poisoning.

4.2.1. AI-Powered Intrusion Detection and Prevention Systems (IDPS)

IDPS enhance network security by using artificial intelligence and machine learning to detect, analyze, and mitigate cyber threats in real time [146]. Unlike traditional IDPS, which rely on static rule-based detection, AI-driven IDPS continuously learn from network traffic patterns (as illustrated in Figure 14), enabling them to identify zero-day attacks, advanced persistent threats (APTs), and sophisticated malware [147], [148].

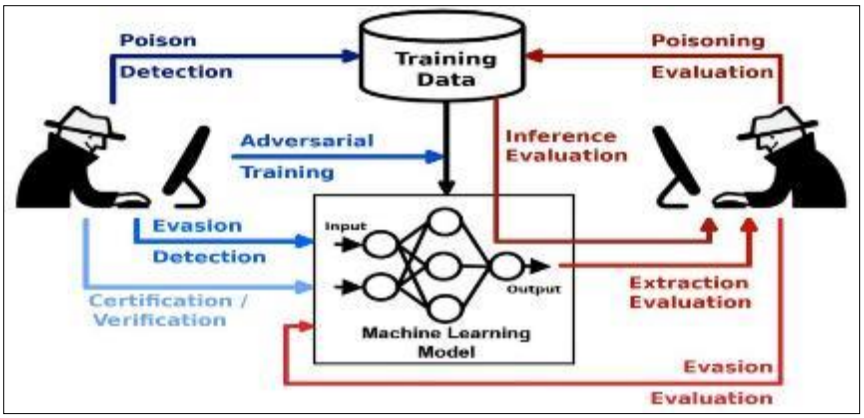

Figure 14 AI-based intrusion detection system

Deep learning models, such as convolutional neural networks (CNNs) and recurrent neural networks (RNNs), help detect anomalies, while reinforcement learning allows adaptive threat response. AI-powered IDPS can also automate threat mitigation by blocking malicious activities instantly, reducing the need for manual intervention [149]. In 6G networks, where vast and dynamic infrastructures increase attack surfaces, AI-driven IDPS are essential for real-time, scalable, and intelligent cybersecurity defenses.

4.2.2. Adversarial machine learning defense

This involves techniques to protect AI models from malicious attacks that manipulate input data to deceive or degrade model performance [150]. As shown in Figure 15, attackers can craft adversarial examples—subtly altered inputs that cause AI models to make incorrect predictions—posing a serious threat to AI-driven security in 6G networks [151]. Defense strategies include adversarial training, where models are trained on both normal and adversarial examples to improve resilience, and gradient masking, which obscures the model's decision-making process to make it harder for attackers to exploit vulnerabilities [152], [153].

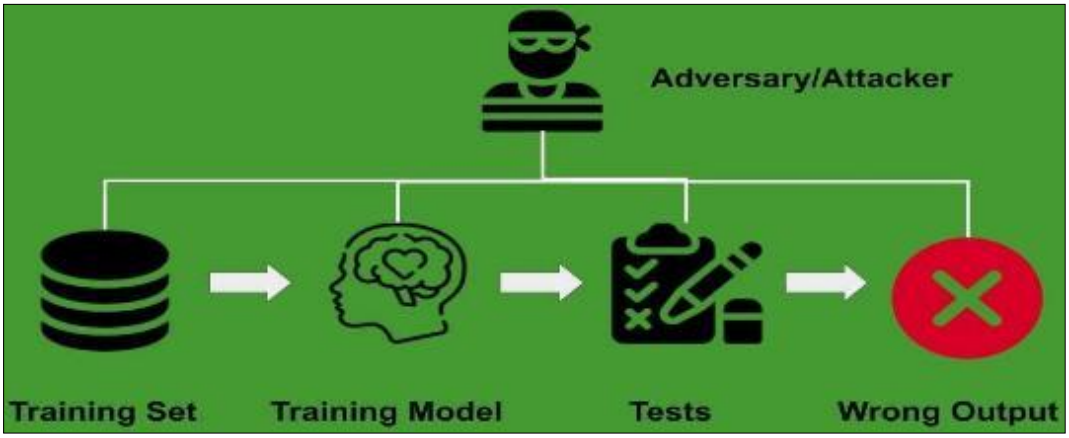

Figure 15 Adversarial machine learning

Other methods, such as defensive distillation (reducing model sensitivity to small input changes) and robust feature extraction using explainable AI (XAI), help mitigate adversarial risks. Ensuring AI security in 6G is critical, as AI-driven cybersecurity, network management, and autonomous decision-making will be foundational to next-generation communication systems.

4.3. Blockchain and decentralized security mechanisms

These mechanisms enhance trust, transparency, and security in 6G networks by eliminating reliance on centralized authorities, which are vulnerable to data breaches and single points of failure [154]. Blockchain ensures tamper-proof data integrity through its immutable ledger, while smart contracts automate secure transactions and access control without intermediaries [155], [156]. Decentralized Identity Management (DID) enables users to control their digital identities, reducing risks associated with centralized authentication systems. Additionally, Zero-Knowledge Proofs

(ZKP) allow authentication without exposing sensitive information [157]. By leveraging distributed consensus and cryptographic hashing, blockchain enhances secure data sharing, fraud prevention, and supply chain security, making it a critical component in securing 6G applications, from IoT devices to financial transactions [158]. 6G will rely on blockchain and decentralized identity management to enhance security and trustworthiness. Unlike centralized security models, blockchain offers immutable, tamper-resistant security for transactions, identity verification, and secure communication.

4.3.1. Blockchain-based authentication

Blockchain-based authentication enhances security by eliminating centralized identity verification systems, which are prone to data breaches and single points of failure [159], as shown in Figure 16. Instead of relying on traditional username-password mechanisms, blockchain leverages decentralized identity management, where user credentials are securely stored on a distributed ledger [160].

This ensures that authentication processes are tamper-resistant, transparent, and verifiable without exposing sensitive user data. Techniques such as Zero-Knowledge Proofs enable users to prove their identity without revealing private information, enhancing privacy [161], [162]. Additionally, smart contracts automate access control, ensuring that only authorized entities can access specific resources. In 6G networks, blockchain-based authentication is crucial for securing IoT devices, edge computing environments, and decentralized applications (dApps), providing a scalable and trustless security framework.

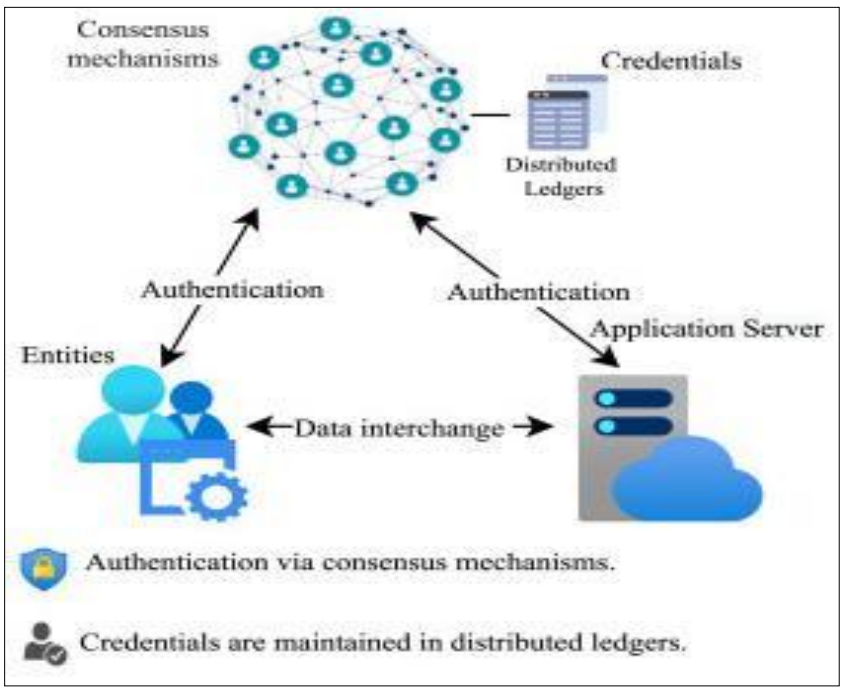

Figure 16 Blockchain-based authentication

4.3.2. Smart contract security

Smart contract security is crucial for ensuring the reliability and integrity of self-executing contracts deployed on blockchain networks [163]. Since smart contracts automatically enforce agreements without intermediaries, vulnerabilities such as reentrancy attacks, integer overflows, logic flaws, and unauthorized access can be exploited by attackers to manipulate transactions or drain funds [164]. To enhance security, formal verification techniques mathematically prove contract correctness before deployment, while secure coding practices, such as implementing checks-effects-interactions patterns, prevent vulnerabilities like reentrancy. Additionally, multi-signature authentication [165] ensures that critical contract actions require multiple approvals, reducing the risk of unauthorized changes. In 6G networks, where blockchain-powered applications play a key role in decentralized security, robust smart contract security is essential for protecting financial transactions, IoT operations, and automated service agreements.

4.3.3. Secure data sharing with blockchain

Secure data sharing with blockchain ensures privacy, integrity, and tamper-proof access control by leveraging decentralized, cryptographically secured ledgers [166]. Unlike traditional centralized databases, where data breaches and unauthorized modifications are common, blockchain enables immutable record-keeping and transparent access management through smart contracts [167]-[168]. Encryption techniques, such as homomorphic encryption and Zero-Knowledge Proofs, allow data to be shared without exposing sensitive information. Additionally, InterPlanetary File System (IPFS) + blockchain integration enables secure decentralized storage, ensuring scalability for large data sets in 6G applications [170]. By providing fine-grained access control and auditability, blockchain-based secure data sharing is vital for healthcare, finance, IoT ecosystems, and AI-driven analytics in next-generation networks.

4.4. Physical Layer Security (PLS) in 6G

Given the vulnerabilities of terahertz communication and free-space optical (FSO) networks, 6G must incorporate physical layer security techniques (illustrated in Figure 17) to prevent signal interception and jamming [171]. The PLS in 6G enhances data confidentiality and integrity by leveraging the physical characteristics of wireless communication channels to prevent eavesdropping and jamming attacks [172]-[174]. Unlike traditional cryptographic methods, PLS secures data at the signal level using techniques such as secure beamforming, where directional signal transmission minimizes interception, and artificial noise injection, which disrupts unauthorized receivers while maintaining communication for legitimate users.

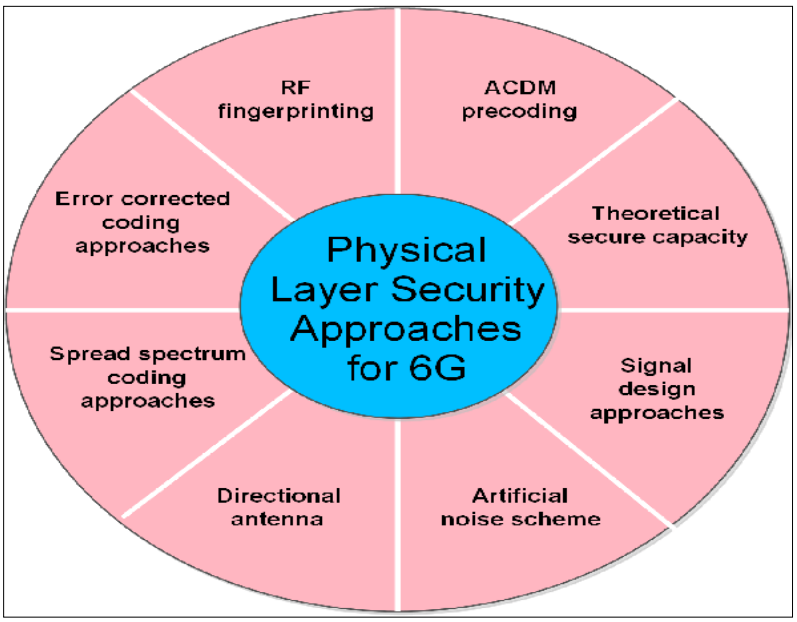

Figure 17 Physical layer security in 6G

Additionally, physical unclonable functions provide unique, hardware-based security for device authentication [175], preventing cloning attacks. Cooperative jamming further enhances PLS by introducing interference signals that obscure real transmissions from adversaries. Given 6G's reliance on terahertz (THz) and free-space optical (FSO) communication, PLS is essential for mitigating physical-layer threats and ensuring ultra-secure, high-speed wireless networks.

4.4.1. Secure beamforming and directional modulation

These are advanced physical layer security techniques in 6G that protect wireless communication from eavesdropping and signal interception. Secure beamforming focuses radio signals toward intended receivers while minimizing signal leakage in unintended directions, reducing the risk of unauthorized access [176], [177]. Directional modulation (DM) enhances security by embedding encryption directly into the signal's phase, amplitude, or frequency, ensuring that only users in a specific spatial direction can correctly decode the transmitted data [178]. These techniques are particularly vital for terahertz (THz) and millimeter-wave (mmWave) communications, where highly directional transmission is required. By dynamically adapting transmission patterns, secure beamforming and directional modulation prevent adversaries from intercepting or manipulating wireless signals, making them crucial for 6G network security..

4.4.2. Cooperative jamming

This is a physical layer security technique that enhances wireless communication security by deliberately introducing interference to prevent eavesdroppers from decoding transmitted signals [179]. Unlike traditional jamming, which disrupts all communications, cooperative jamming selectively injects artificial noise or interference in a way that degrades the signal quality [180] only for unauthorized receivers while ensuring legitimate users can still decode the intended message. This is achieved using relay nodes, friendly jammers, and intelligent reflecting surfaces to strategically direct jamming signals. In terahertz and millimeter-wave (mmWave) communications, where signals are more susceptible to interception [181], cooperative jamming plays a crucial role in securing confidential transmissions against passive and active eavesdropping attacks in 6G networks.

4.4.3. Secure device authentication with Physical Unclonable Functions (PUFs)

This leverages the inherent, unique physical variations in a device's hardware to generate unclonable cryptographic keys, ensuring robust security in 6G networks [182]. Unlike traditional authentication methods that rely on stored credentials, PUF-based authentication derives unique responses from the microscopic variations in circuit manufacturing, making each device inherently distinct and resistant to cloning or tampering [183, [184]. When a device undergoes authentication, it is challenged with an input signal, and its unique hardware characteristics produce a response that serves as a cryptographic key. Since PUFs are resistant to physical attacks and cannot be duplicated, they provide lightweight [185], tamper-proof authentication for IoT, edge devices, and autonomous systems in 6G, ensuring secure network access and preventing identity spoofing.

4.5. Secure edge and fog computing in 6G

These technologies ensure low-latency, decentralized data processing while maintaining strong security and privacy protections. Unlike traditional cloud computing, which centralizes data processing, edge and fog computing bring computation closer to the data source, reducing latency and bandwidth usage [186]. However, this distributed architecture introduces security challenges, including data breaches, unauthorized access, and cyberattacks on edge nodes [187]. To mitigate these risks, lightweight encryption, blockchain-based access control, and AI-driven threat detection are employed. Homomorphic encryption allows secure data processing without decryption, while trusted execution environments (TEEs) protect sensitive computations from tampering [188], [189]. By integrating zero-trust security models and secure multi-party computation (SMPC), 6G networks can ensure resilient, privacy-preserving edge and fog computing for IoT, autonomous systems, and real-time AI applications. Edge and fog computing will be integral to 6G, but they introduce security challenges due to decentralized data processing.

4.5.1. Secure Multi-Party Computation (SMPC)

This is a cryptographic technique that enables multiple parties to collaboratively compute a function over their private inputs without revealing those inputs to one another. This ensures data confidentiality while allowing secure data analysis and decision-making, making it essential for privacy-preserving applications [190] in 6G networks. SMPC relies on protocols like secret sharing, homomorphic encryption, and oblivious transfer, ensuring that even if some participants are compromised, the underlying data remains protected [191], [192]. It is particularly useful for secure federated learning, encrypted data analytics, and confidential transactions, where sensitive information, such as medical records or financial data, must be processed without exposing individual details. By enabling distributed trust and privacy-preserving computations, SMPC strengthens security in decentralized 6G applications, including IoT, AI, and cloud-edge environments.

4.5.2. Homomorphic encryption for secure computation

Homomorphic encryption (HE) is an advanced cryptographic technique that allows computations to be performed on encrypted data without needing decryption, ensuring privacy and security throughout the processing [193], [194]. This enables secure computations in cloud computing, edge computing, and AI-driven analytics within 6G networks, where sensitive data must be processed without exposing it to untrusted entities. HE supports operations like addition and multiplication on ciphertexts, producing an encrypted result that, when decrypted, matches the outcome of computations performed on plaintext data. Variants such as Partially, Somewhat, and Fully Homomorphic Encryption (FHE) provide different levels of computational flexibility, with FHE enabling unlimited operations on encrypted data. By preserving data confidentiality even during processing [195], homomorphic encryption is crucial for privacy-preserving AI, secure federated learning, and encrypted search in 6G applications.

4.5.3. Trusted Execution Environments (TEEs)

These are secure, isolated environments within a device's processor that enable confidential computing by protecting sensitive data and computations from unauthorized access, even if the system is compromised [196]. TEEs provide hardware-based security, ensuring that data remains encrypted and protected from malware, insider threats, and external attackers [197]. They support secure key management, encrypted processing, and remote attestation, allowing only trusted applications to access critical data [198]. In 6G networks, TEEs are essential for secure edge computing, IoT authentication, and privacy-preserving AI, where sensitive computations must be performed in untrusted environments. By enabling end-to-end security and integrity, TEEs enhance trust in decentralized and cloud-edge architectures, ensuring robust protection for next-generation applications.

4.6. AI-Driven threat intelligence and automated incident response

These activities enhance cybersecurity by using machine learning and big data analytics to detect, analyze, and mitigate cyber threats in real time. AI continuously monitors network traffic, identifying anomalies, zero-day attacks, and advanced persistent threats (APTs) through behavioral analysis and predictive modeling [199]. Threat intelligence platforms leverage natural language processing (NLP) and deep learning to analyze vast amounts of threat data from multiple sources, providing proactive defense measures [200]. Once a threat is detected, automated incident response systems initiate countermeasures, such as isolating compromised devices, blocking malicious traffic, and deploying security patches without human intervention. In 6G networks, where massive IoT and autonomous systems increase the attack surface [201], AI-driven threat intelligence ensures rapid detection, real-time mitigation, and adaptive security, reducing response time and minimizing damage.

In a nutshell, security in 6G networks must be adaptive, intelligent, and quantum-safe. Advanced cryptographic techniques, AI-driven security frameworks, blockchain-based trust mechanisms, and physical layer security will be crucial in safeguarding 6G networks. With the rise of quantum computing, AI-powered cyberattacks, and the proliferation of IoT and edge devices, these solutions will ensure end-to-end protection in the hyper-connected world of 6G.

5. Research gaps

The evolution of 6G networks introduces numerous technological advancements, including terahertz (THz) communications, AI-driven network management, quantum computing, and decentralized architectures. However, these innovations also present significant security challenges that require further research. Several key research gaps in 6G security remain unresolved, demanding innovative solutions for robust protection against emerging cyber threats.

5.1. Lack of standardized security frameworks

Despite the extensive research on 5G security, there is no universally accepted security framework for 6G. As the network integrates AI, blockchain, quantum cryptography, and edge computing, a unified security architecture is necessary to define authentication mechanisms, encryption standards, and threat mitigation strategies. According to [202], the lack of standardized security frameworks in 6G poses significant risks, as the next-generation network will introduce advanced technologies like AI-driven automation, terahertz communication, and decentralized architectures. Without a unified security framework, there will be inconsistencies in addressing vulnerabilities, making networks more susceptible to cyber threats, data breaches, and attacks on critical infrastructure [203], [204]. The absence of global standards could also lead to interoperability challenges, hindering secure communication across different regions and service providers. Establishing robust, standardized security measures early in 6G development is crucial to ensuring trust, privacy, and resilience in future networks [205]. Research is needed to develop adaptive, scalable, and interoperable security frameworks that align with the dynamic nature of 6G.

5.2. Vulnerabilities in AI-driven security mechanisms

6G networks heavily rely on artificial intelligence and machine learning for autonomous network management, security threat detection, and optimization [206]. AI-driven security mechanisms in 6G, while enhancing threat detection and response, also introduce new vulnerabilities. Adversarial attacks, such as data poisoning and evasion techniques, can manipulate AI models [207], leading to misclassification of threats or system failures. Additionally, AI-based security systems require vast amounts of data, raising concerns about data privacy, unauthorized access, and potential bias in decision-making [208], [209]. The complexity of AI algorithms makes it challenging to interpret and audit security decisions, increasing the risk of undetected vulnerabilities. Without robust safeguards, AI-driven security in 6G could become a double-edged sword, potentially exploited by sophisticated cyber threats. According to [210], AI itself introduces security risks, such as adversarial attacks, model poisoning, and bias in threat detection models. Research is

required to develop robust AI-driven security solutions, including adversarial defense mechanisms, explainable AI (XAI) for security, and federated learning with enhanced privacy protections.

5.3. Post-quantum cryptography implementation challenges

Implementing post-quantum cryptography (such as the one in Figure 18) presents several challenges, primarily due to the computational complexity and resource-intensive nature of quantum-resistant algorithms [211]. These algorithms often require significantly larger key sizes and higher processing power, which can strain existing hardware, particularly in resource-constrained devices like IoT sensors and mobile devices [212], [213]. Additionally, transitioning from classical cryptographic standards to PQC demands extensive updates to protocols, infrastructure, and security policies, creating compatibility and interoperability issues. Ensuring a smooth migration while maintaining performance, scalability, and security across diverse 6G networks remains a critical challenge, requiring global coordination and investment in new cryptographic standards. According to [214], quantum computing threatens traditional cryptographic algorithms like RSA, ECC, and AES by enabling rapid decryption through Shor's and Grover's algorithms. While post-quantum cryptography solutions, such as lattice-based, hash-based, and code-based cryptography, are being developed, their practical implementation in real-world 6G networks remains uncertain [215]. Research must focus on optimizing PQC for low-latency, high-speed encryption suitable for edge computing, IoT, and ultra-reliable low-latency communications (URLLC).

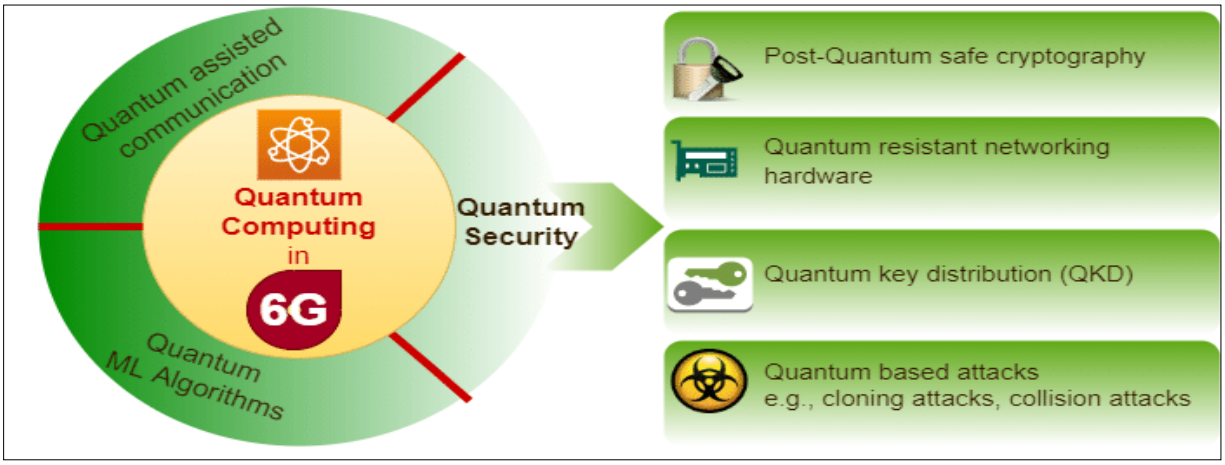

Figure 18 post-quantum cryptography

5.4. Security of Terahertz (THz) and optical wireless communications

6G networks will utilize THz and visible light communication (VLC) to achieve ultra-high data rates. However, these technologies introduce new security challenges, including eavesdropping risks due to line-of-sight (LoS) transmissions, beam misalignment attacks, and jamming threats [216]. As explain in [217], the security of Terahertz (THz) and optical wireless communications in 6G presents unique challenges due to their high-frequency, short-wavelength nature. While these technologies offer ultra-high data rates and low latency, they are highly susceptible to signal blockage, atmospheric absorption, and interception risks. The directional nature of THz and optical signals improves security against eavesdropping but also introduces vulnerabilities such as jamming, beam misalignment, and side-channel attacks [218]. Additionally, secure key distribution and encryption mechanisms must be adapted to these high-speed, high-frequency channels to prevent unauthorized access [219]. Addressing these challenges requires specialized security protocols and adaptive defense mechanisms to ensure reliable and secure communication. More research is needed on secure beamforming, directional modulation, and cooperative jamming techniques to enhance physical layer security.

5.5. Privacy and data protection in massive IoT and edge computing

Privacy and data protection in massive IoT and edge computing within 6G networks present critical challenges due to the vast number of distributed devices processing sensitive data outside centralized cloud systems [220], [221]. The decentralized nature of edge computing increases exposure to cyber threats such as unauthorized access, data interception, and tampering. Many IoT devices have limited computational resources, making it difficult to implement robust encryption, authentication, and intrusion detection mechanisms [222]-[224]. Additionally, ensuring compliance with diverse global data protection regulations adds complexity. To safeguard privacy, 6G must integrate secure data transmission protocols, AI-driven anomaly detection, and decentralized identity management while balancing security

with performance efficiency. As explained in [225], the massive-scale deployment of IoT devices in 6G introduces challenges related to data privacy, secure device authentication, and lightweight cryptography. Traditional encryption techniques are often too resource-intensive for low-power IoT devices, necessitating research into lightweight cryptographic algorithms, hardware-based security using physical unclonable functions, and privacy-preserving data sharing. Additionally, securing edge and fog computing infrastructures requires novel approaches, such as zero-trust security models and homomorphic encryption.

5.6. Blockchain scalability and security for decentralized 6G networks

Blockchain scalability and security are critical challenges for decentralized 6G networks, as traditional blockchain systems struggle with high transaction latency and energy-intensive consensus mechanisms [226]. In a 6G environment with massive IoT and edge computing, blockchain must efficiently handle a vast number of transactions while maintaining low latency and high throughput [227]. Scalability solutions like sharding, sidechains, and layer-2 protocols are needed to enhance performance without compromising security. However, decentralization also introduces risks such as 51% attacks, smart contract vulnerabilities, and privacy concerns [228]. To ensure secure and scalable blockchain integration in 6G, advanced cryptographic techniques, lightweight consensus mechanisms, and AI-driven security enhancements must be developed. While blockchain-based solutions enhance decentralized security, identity management, and secure data sharing [229], they face challenges related to scalability, energy efficiency, and attack vulnerabilities (e.g., Sybil attacks, 51% attacks, and smart contract exploits). Research is needed to develop lightweight, high-performance blockchain architectures tailored for 6G applications, such as IoT authentication, secure multi-party computation (SMPC), and AI-driven security automation.

5.7. Resilience against advanced cyber threats and zero-day attacks

Resilience against advanced cyber threats and zero-day attacks in 6G networks requires a proactive and adaptive security approach [230]. With AI-driven automation, massive IoT, and decentralized architectures, 6G expands the attack surface, making it more vulnerable to sophisticated threats like AI-generated malware, quantum-enabled cyberattacks, and zero-day exploits [231]-[233]. Traditional signature-based defenses are insufficient, necessitating AI-powered threat detection, real-time anomaly monitoring, and self-healing network capabilities. Additionally, integrating blockchain for secure identity management [234], post-quantum cryptography for encryption, and zero-trust architectures can strengthen resilience. A collaborative approach involving threat intelligence sharing and automated security updates is essential to mitigating emerging cyber risks in 6G. With the increased use of AI-driven cyberattacks, malware, and advanced persistent threats (APTs), traditional security measures are insufficient [235]-[240]. 6G networks require proactive security solutions that leverage predictive analytics, AI-powered Intrusion Detection and Prevention Systems (IDPS), and autonomous incident response mechanisms. Research must focus on self-healing networks, AI-enhanced anomaly detection, and real-time attack mitigation.

Evidently, 6G security presents unprecedented challenges that require interdisciplinary research in AI security, quantum cryptography, blockchain scalability, IoT privacy, and regulatory frameworks. Addressing these research gaps is crucial to building a secure, resilient, and privacy-preserving 6G network for the future.

6. Conclusion

Security in 6G cellular networks presents a complex and evolving challenge due to the integration of advanced technologies such as AI-driven automation, terahertz (THz) and optical wireless communications, massive IoT, and decentralized architectures. While these innovations promise unprecedented speed, efficiency, and connectivity, they also introduce new vulnerabilities, including AI security risks, quantum threats, and privacy concerns in edge computing. Addressing these challenges requires a multi-layered approach, incorporating post-quantum cryptography, blockchain scalability solutions, AI-powered threat detection, and zero-trust security frameworks. Standardized security protocols, global regulatory collaboration, and real-time adaptive defense mechanisms will be crucial for building a resilient 6G ecosystem. Future research should focus on developing scalable, energy-efficient security solutions that balance performance with robust protection against emerging cyber threats. By prioritizing security at the foundation of 6G design, we can ensure a trustworthy and sustainable next-generation network.

Compliance with ethical standards

Disclosure of conflict of interest

That author declares that he holds no conflict to declare.

References

[1] Hossain E, Vera-Rivera A. Next-Generation Wireless: Tracking the Evolutionary Path of 6G Mobile Communication. arXiv preprint arXiv:2501.14552. 2025 Jan 24.

[2] Hasan KM, Sajid M, Lapina MA, Shahid M, Kotecha K. Blockchain technology meets 6 G wireless networks: A systematic survey. Alexandria Engineering Journal. 2024 Apr 1;92:199-220.

[3] Ullah S, Li J, Chen J, Ali I, Khan S, Ahad A, Ullah F, Leung VC. A Survey on Emerging Trends and Applications of 5G and 6G to Healthcare Environments. ACM Computing Surveys. 2024 Dec 10;57(4):1-36.

[4] Ahmed M, Waqas F, Fatima M, Khan AM, Naz MA, Ahmed M. Enabling 6G Networks for Advances Challenges and Traffic Engineering for Future Connectivity. VFAST Transactions on Software Engineering. 2024 Dec 31;12(4):326-37.

[5] Alzaidi ZS, Yassin AA, Abduljabbar ZA, Nyangaresi VO. Development Anonymous Authentication Maria et al.'s Scheme of VANETs Using Blockchain and Fog Computing with QR Code Technique. In2024 10th International Conference on Control, Decision and Information Technologies (CoDIT) 2024 Jul 1 (pp. 2247-2252). IEEE.

[6] Murroni M, Anedda M, Fadda M, Ruiu P, Popescu V, Zaharia C, Giusto D. 6G—Enabling the new smart city: A survey. Sensors. 2023 Aug 30;23(17):7528.

[7] Imoize AL, Adedeji O, Tandiya N, Shetty S. 6G enabled smart infrastructure for sustainable society: Opportunities, challenges, and research roadmap. Sensors. 2021 Mar 2;21(5):1709.

[8] Bhide P, Shetty D, Mikkili S. Review on 6G communication and its architecture, technologies included, challenges, security challenges and requirements, applications, with respect to AI domain. IET Quantum Communication. 2024 Dec.

[9] Tera SP, Chinthaginjala R, Pau G, Kim TH. Towards 6G: An Overview of the Next Generation of Intelligent Network Connectivity. IEEE Access. 2024 Dec 26.

[10] Nyangaresi VO, Alsolami E, Ahmad M. Trust-enabled Energy Efficient Protocol for Secure Remote Sensing in Supply Chain Management. IEEE Access. 2024 Aug 12.

[11] Won D, Woraphonbenjakul G, Wondmagegn AB, Tran AT, Lee D, Lakew DS, Cho S. Resource management, security, and privacy issues in semantic communications: A survey. IEEE Communications Surveys & Tutorials. 2024 Oct 3.

[12] Golda A, Mekonen K, Pandey A, Singh A, Hassija V, Chamola V, Sikdar B. Privacy and security concerns in generative AI: a comprehensive survey. IEEE Access. 2024 Mar 25.

[13] Vu TH, Jagatheesaperumal SK, Nguyen MD, Van Huynh N, Kim S, Pham QV. Applications of generative AI (GAI) for mobile and wireless networking: A survey. IEEE Internet of Things Journal. 2024 Oct 29.

[14] Dogra A, Jha RK, Jain S. A survey on beyond 5G network with the advent of 6G: Architecture and emerging technologies. IEEE access. 2020 Oct 15;9:67512-47.

[15] Kadhim TA, Abduljabbar ZA, AL-Asadi HA, Nyangaresi VO, Ali ZA, Abduljaleel IQ. Lightweight Scheme for Secure Signaling and Data Exchanges in Intelligent Precision Agriculture. Cryptography. 2025 Jan 17;9(1):7.

[16] Quy VK, Chehri A, Quy NM, Han ND, Ban NT. Innovative trends in the 6G era: A comprehensive survey of architecture, applications, technologies, and challenges. IEEE Access. 2023 Apr 21;11:39824-44.

[17] Huang T, Yang W, Wu J, Ma J, Zhang X, Zhang D. A survey on green 6G network: Architecture and technologies. IEEE access. 2019 Dec 4;7:175758-68.

[18] Akhtar MW, Hassan SA, Ghaffar R, Jung H, Garg S, Hossain MS. The shift to 6G communications: vision and requirements. Human-centric Computing and Information Sciences. 2020 Dec;10:1-27.

[19] Banafaa M, Shayea I, Din J, Azmi MH, Alashbi A, Daradkeh YI, Alhammadi A. 6G mobile communication technology: Requirements, targets, applications, challenges, advantages, and opportunities. Alexandria Engineering Journal. 2023 Feb 1;64:245-74.

[20] Qiu Z, Ma J, Zhang H, Al Sibahee MA, Abduljabbar ZA, Nyangaresi VO. Concurrent pipeline rendering scheme based on GPU multi-queue and partitioning images. InInternational Conference on Optics and Machine Vision (ICOMV 2023) 2023 Apr 14 (Vol. 12634, pp. 143-149). SPIE.

[21] Yang H, Alphones A, Xiong Z, Niyato D, Zhao J, Wu K. Artificial-intelligence-enabled intelligent 6G networks. IEEE network. 2020 Oct 23;34(6):272-80.

[22] Zhang S, Zhu D. Towards artificial intelligence enabled 6G: State of the art, challenges, and opportunities. Computer Networks. 2020 Dec 24;183:107556.

[23] Yang Z, Yang Q, Yang M. Quality of Service-Oriented Data Optimization in Networks using Artificial Intelligence Techniques. International Journal of Advanced Computer Science & Applications. 2024 Jun 1;15(6).

[24] Kadiyala C, Chilukoori S, Gangarapu S. AI-Powered Network Automation: The Next Frontier in Network Management. Journal of Advanced Research Engineering and Technology. 2024;3:223-33.

[25] Al-Maliki H, AL-Asadi HA, Abduljabbar ZA, Nyangaresi VO. Reliable Vehicular Ad Hoc Networks for Intelligent Transportation Systems based on the Snake Optimization Algorithm. Engineering, Technology & Applied Science Research. 2024 Dec 2;14(6):18631-9.

[26] Joshi N, Arora N, Yadav H, Sharma SC. AI-Driven Cognitive Radio Networks for Transforming Industries and Sectors Towards a Smart World. InRecent Trends in Artificial Intelligence Towards a Smart World: Applications in Industries and Sectors 2024 Sep 10 (pp. 1-35). Singapore: Springer Nature Singapore.

[27] Alsharif MH, Albreem MA, Solyman AA, Kim S. Toward 6G communication networks: Terahertz frequency challenges and open research issues. Computers, Materials & Continua. 2021.

[28] Jiang W, Zhou Q, He J, Habibi MA, Melnyk S, El-Absi M, Han B, Di Renzo M, Schotten HD, Luo FL, El-Bawab TS. Terahertz communications and sensing for 6G and beyond: A comprehensive review. IEEE Communications Surveys & Tutorials. 2024 Apr 8.

[29] Serghiou D, Khalily M, Brown TW, Tafazolli R. Terahertz channel propagation phenomena, measurement techniques and modeling for 6G wireless communication applications: A survey, open challenges and future research directions. IEEE Communications Surveys & Tutorials. 2022 Sep 9;24(4):1957-96.

[30] Nyangaresi VO, Al-Joboury IM, Al-sharhanee KA, Najim AH, Abbas AH, Hariz HM. A Biometric and Physically Unclonable Function-Based Authentication Protocol for Payload Exchanges in Internet of Drones. e-Prime-Advances in Electrical Engineering, Electronics and Energy. 2024 Feb 23:100471.

[31] Wang S, Qureshi MA, Miralles-Pechuán L, Huynh-The T, Gadekallu TR, Liyanage M. Explainable AI for 6G use cases: Technical aspects and research challenges. IEEE Open Journal of the Communications Society. 2024 Apr 16.

[32] Hu Z, Zhang P, Zhang C, Zhuang B, Zhang J, Lin S, Sun T. Intelligent decision making framework for 6G network. China Communications. 2022 Mar 30;19(3):16-35.

[33] Popovski P, Chiariotti F, Huang K, Kalør AE, Kountouris M, Pappas N, Soret B. A perspective on time toward wireless 6G. Proceedings of the IEEE. 2022 Jul 21;110(8):1116-46.

[34] Chataut R, Nankya M, Akl R. 6G networks and the AI revolution—Exploring technologies, applications, and emerging challenges. Sensors. 2024 Mar 15;24(6):1888.

[35] Alshuraify NA, Yassin AA, Abduljabbar ZA, Nyangaresi VO, Aldarwish AJ. Blockchain-Based CCTV Surveillance Cameras for Oil and Gas Industry Pipelines. InComputer Science On-line Conference 2024 Apr 25 (pp. 730-744). Cham: Springer Nature Switzerland.

[36] Aydeger A, Zeydan E, Yadav AK, Hemachandra KT, Liyanage M. Towards a quantum-resilient future: Strategies for transitioning to post-quantum cryptography. In2024 15th International Conference on Network of the Future (NoF) 2024 Oct 2 (pp. 195-203). IEEE.

[37] Chawla D, Mehra PS. A roadmap from classical cryptography to post-quantum resistant cryptography for 5G-enabled IoT: Challenges, opportunities and solutions. Internet of Things. 2023 Dec 1;24:100950.

[38] Li S, Chen Y, Chen L, Liao J, Kuang C, Li K, Liang W, Xiong N. Post-quantum security: Opportunities and challenges. Sensors. 2023 Oct 26;23(21):8744.

[39] Fernandez-Carames TM, Fraga-Lamas P. Towards post-quantum blockchain: A review on blockchain cryptography resistant to quantum computing attacks. IEEE access. 2020 Jan 23;8:21091-116.

[40] Nyangaresi VO. Extended Chebyshev Chaotic Map Based Message Verification Protocol for Wireless Surveillance Systems. InComputer Vision and Robotics: Proceedings of CVR 2022 2023 Apr 28 (pp. 503-516). Singapore: Springer Nature Singapore.

[41] Salh A, Audah L, Shah NS, Alhammadi A, Abdullah Q, Kim YH, Al-Gailani SA, Hamzah SA, Esmail BA, Almohammedi AA. A survey on deep learning for ultra-reliable and low-latency communications challenges on 6G wireless systems. IEEe Access. 2021 Mar 30;9:55098-131.

[42] Adhikari M, Hazra A. 6G-enabled ultra-reliable low-latency communication in edge networks. IEEE Communications Standards Magazine. 2022 Mar;6(1):67-74.

[43] Sefati SS, Halunga S. Ultra-reliability and low-latency communications on the internet of things based on 5G network: literature review, classification, and future research view. Transactions on emerging telecommunications technologies. 2023 Jun;34(6):e4770.

[44] Haque ME, Tariq F, Khandaker MR, Wong KK, Zhang Y. A survey of scheduling in 5G URLLC and outlook for emerging 6G systems. IEEE access. 2023 Apr 5;11:34372-96.

[45] Nyangaresi VO, Ghaib AA, Jasim HM, Abduljabbar ZA, Ma J, Al Sibahee MA, Aldarwish AJ, Ali AH, Neamah HA. Message Verification Protocol Based on Bilinear Pairings and Elliptic Curves for Enhanced Security in Vehicular Ad Hoc Networks. Computers, Materials and Continua. 2024 Oct 1;81(1):1029-57.

[46] Pritchard-Kelly R, Costa J. Low earth orbit satellite systems: comparisons with geostationary and other satellite systems, and their significant advantages. Journal of Telecommunications and the Digital Economy. 2022 Mar 1;10(1):1-22.

[47] Gur BA, Kulesza J. Equitable access to satellite broadband services: Challenges and opportunities for developing countries. Telecommunications Policy. 2024 Mar 11:102731.

[48] Al-Hraishawi H, Chougrani H, Kisseleff S, Lagunas E, Chatzinotas S. A survey on nongeostationary satellite systems: The communication perspective. IEEE Communications Surveys & Tutorials. 2022 Aug 9;25(1):101-32.

[49] Yue P, An J, Zhang J, Ye J, Pan G, Wang S, Xiao P, Hanzo L. Low earth orbit satellite security and reliability: Issues, solutions, and the road ahead. IEEE Communications Surveys & Tutorials. 2023 Aug 4;25(3):1604-52.

[50] Kumar S, Chinthaginjala R, Anbazhagan R, Nyangaresi VO, Pau G, Varma PS. Submarine Acoustic Target Strength Modelling at High-Frequency Asymptotic Scattering. IEEE Access. 2024 Jan 1.

[51] Arastouei N, Khan MA. 6G Technology in Intelligent Healthcare: Smart Health and Its Security and Privacy Perspectives. IEEE Wireless Communications. 2025 Feb 4;32(1):116-21.

[52] Sharma S, Popli R, Singh S, Chhabra G, Saini GS, Singh M, Sandhu A, Sharma A, Kumar R. The role of 6G technologies in advancing smart city applications: Opportunities and challenges. Sustainability. 2024 Aug 16;16(16):7039.

[53] Sinha P, Kandasamy M, Shanmugam R, Nageswari P. 6G communication challenges. 6G Communication Network: Architecture, Security and Applications. 2024 Nov 18.

[54] Dixit I, Varma MK, Singh A, Charith B, Aancy HM, Thakar CM. Security Roadmap for Industry 5.0: Managing Risks in the 6G Landscape. In6G Security Education and Multidisciplinary Implementation 2024 (pp. 212-231). IGI Global.

[55] Jawad M, Yassin AA, AL-Asadi HA, Abduljabbar ZA, Nyangaresi VO. Towards Building Multi-factor Authentication Scheme for Users in the Healthcare Sector Based on Blockchain Technology. InComputer Science On-line Conference 2024 Apr 25 (pp. 694-713). Cham: Springer Nature Switzerland.

[56] Sheraz M, Chuah TC, Lee YL, Alam MM, Han Z. A comprehensive survey on revolutionizing connectivity through artificial intelligence-enabled digital twin network in 6G. IEEE Access. 2024 Apr 3.

[57] Alraih S, Shayea I, Behjati M, Nordin R, Abdullah NF, Abu-Samah A, Nandi D. Revolution or evolution? Technical requirements and considerations towards 6G mobile communications. Sensors. 2022 Jan 20;22(3):762.

[58] Xiao Y, Ye Z, Wu M, Li H, Xiao M, Alouini MS, Al-Hourani A, Cioni S. Space-air-ground integrated wireless networks for 6G: Basics, key technologies and future trends. IEEE Journal on Selected Areas in Communications. 2024 Nov 6.

[59] Guo H, Li J, Liu J, Tian N, Kato N. A survey on space-air-ground-sea integrated network security in 6G. IEEE Communications Surveys & Tutorials. 2021 Nov 30;24(1):53-87.

[60] Nyangaresi VO. Anonymity preserving security protocol for wireless body area networks: towards the secure remote patient healthcare monitoring. InSensor Networks for Smart Hospitals 2025 Jan 1 (pp. 293-312). Elsevier.

[61] Khan LU, Guizani M, Yaqoob I, Niyato D, Al-Fuqaha A, Hong CS. A survey on metaverse-empowered 6G wireless systems: a security perspective. Internet of Things. 2024 Aug 14:101325.

[62] Kaur N, Gupta L. Securing the 6G–IoT Environment: A Framework for Enhancing Transparency in Artificial Intelligence Decision-Making Through Explainable Artificial Intelligence. Sensors. 2025 Jan 30;25(3):854.

[63] 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. Artificial Intelligence Review. 2022 Oct;55(7):5215-61.

[64] Rosenberg I, Shabtai A, Elovici Y, Rokach L. Adversarial machine learning attacks and defense methods in the cyber security domain. ACM Computing Surveys (CSUR). 2021 May 23;54(5):1-36.

[65] Radhi BM, Hussain MA, Abduljabbar ZA, Nyangaresi VO. Secure and Fast Remote Application–Based Authentication Dragonfly Using an LED Algorithm in Smart Buildings. In2024 International Conference on Artificial Intelligence in Information and Communication (ICAIIC) 2024 Feb 19 (pp. 509-517). IEEE.

[66] Nguyen VL, Lin PC, Cheng BC, Hwang RH, Lin YD. Security and privacy for 6G: A survey on prospective technologies and challenges. IEEE Communications Surveys & Tutorials. 2021 Aug 30;23(4):2384-428.

[67] Akbar MA, Khan AA, Hyrynsalmi S. Role of quantum computing in shaping the future of 6 G technology. Information and Software Technology. 2024 Jun 1;170:107454.

[68] Javeed D, Saeed MS, Ahmad I, Adil M, Kumar P, Islam AN. Quantum-empowered federated learning and 6G wireless networks for IoT security: Concept, challenges and future directions. Future Generation Computer Systems. 2024 Jun 13.

[69] Scalise P, Garcia R, Boeding M, Hempel M, Sharif H. An Applied Analysis of Securing 5G/6G Core Networks with Post-Quantum Key Encapsulation Methods. Electronics. 2024 Oct 30;13(21):4258.

[70] Nyangaresi VO. Efficient and provably secure framework for authenticating internet of medical things in smart hospitals. InBlockchain and Digital Twin for Smart Hospitals 2025 Jan 1 (pp. 207-236). Elsevier.

[71] Serôdio C, Cunha J, Candela G, Rodriguez S, Sousa XR, Branco F. The 6G ecosystem as support for IoE and private networks: Vision, requirements, and challenges. Future Internet. 2023 Oct 25;15(11):348.

[72] Mohapatra H. The Role of 6G in Empowering Smart Cities Enabling Ubiquitous Connectivity and Intelligent Infrastructure. InBuilding Tomorrow's Smart Cities With 6G Infrastructure Technology 2025 (pp. 237-264). IGI Global Scientific Publishing.

[73] Yadav M, Agarwal U, Rishiwal V, Tanwar S, Kumar S, Alqahtani F, Tolba A. Exploring synergy of blockchain and 6G network for industrial automation. IEEE Access. 2023 Dec 1;11:137163-87.

[74] Vashishth TK, Sharma V, Sharma MK, Sharma R. Healthcare and Smart Cities Applications of Secure 6G Infrastructure. InBuilding Tomorrow's Smart Cities With 6G Infrastructure Technology 2025 (pp. 399-432). IGI Global Scientific Publishing.

[75] Radhi BM, Hussain MA, Abduljabbar ZA, Nyangaresi VO, Aldarwish AJ. A Review on IoTs Applications and Security Threats via Data Transfer over Networks. InComputer Science On-line Conference 2024 Apr 25 (pp. 562-579). Cham: Springer Nature Switzerland.

[76] Molokomme DN, Onumanyi AJ, Abu-Mahfouz AM. Edge intelligence in Smart Grids: A survey on architectures, offloading models, cyber security measures, and challenges. Journal of Sensor and Actuator Networks. 2022 Aug 21;11(3):47.

[77] Kumari KA, Sharma A, Chakraborty C, Ananyaa M. Preserving health care data security and privacy using Carmichael's theorem-based homomorphic encryption and modified enhanced homomorphic encryption schemes in edge computing systems. Big Data. 2022 Feb 1;10(1):1-7.

[78] Zhang J, Chen B, Zhao Y, Cheng X, Hu F. Data security and privacy-preserving in edge computing paradigm: Survey and open issues. IEEE access. 2018 Mar 28;6:18209-37.

[79] Zhu B, Niu L. A privacy-preserving federated learning scheme with homomorphic encryption and edge computing. Alexandria Engineering Journal. 2025 Apr 1;118:11-20.

[80] Nyangaresi VO, AlRababah AA, Yenurkar GK, Chinthaginjala R, Yasir M. Anonymous Authentication Scheme Based on Physically Unclonable Function and Biometrics for Smart Cities. Engineering Reports. 2024:e13079.

[81] Maharana N, Kuppili SK, Ganesh BU, Das GP, Chaudhury SK. From Defense to Deception: An Analysis of the Financial Fraud in India in the Age of AI. InGenerative AI for Business Analytics and Strategic Decision Making in Service Industry 2025 (pp. 317-340). IGI Global Scientific Publishing.

[82] Raman R, Sahu AK, Nair VK, Nedungadi P. Opposing agents evolve the research: a decade of digital forensics. Multimedia Tools and Applications. 2024 Jun 11:1-29.

[83] Eichner AW. Artificial Intelligence and Weaponized Illusions: Methodologies for Federal Fraud Prosecutions Involving Deepfakes. Am. UL Rev.. 2023;73:1319.

[84] Shaaban OA, Yildirim R, Alguttar AA. Audio deepfake approaches. IEEE Access. 2023 Nov 16;11:132652-82.

[85] Abdali HK, Hussain MA, Abduljabbar ZA, Nyangaresi VO. Implementing Blockchain for Enhancing Security and Authentication in Iraqi E-Government Services. Engineering, Technology & Applied Science Research. 2024 Dec 2;14(6):18222-33.

[86] Hoang VT, Ergu YA, Nguyen VL, Chang RG. Security risks and countermeasures of adversarial attacks on AI-driven applications in 6G networks: A survey. Journal of Network and Computer Applications. 2024 Sep 18:104031.

[87] Khowaja SA, Khuwaja P, Dev K, Singh K, Li X, Bartzoudis N, Comsa CR. Block Encryption LAyer (BELA): Zero-Trust Defense Against Model Inversion Attacks for Federated Learning in 5G/6G Systems. IEEE Open Journal of the Communications Society. 2025 Jan 6.

[88] Ferrag MA, Friha O, Kantarci B, Tihanyi N, Cordeiro L, Debbah M, Hamouda D, Al-Hawawreh M, Choo KK. Edge learning for 6G-enabled internet of things: A comprehensive survey of vulnerabilities, datasets, and defenses. IEEE Communications Surveys & Tutorials. 2023 Sep 19;25(4):2654-713.

[89] Kocherla R, Dwivedi YD, Reena BA, Komala CR, Jennifer D, Dhanraj JA. Adversarial Challenges in Distributed AI: ML Safeguarding 6G Networks. InSecurity Issues and Solutions in 6G Communications and Beyond 2024 (pp. 61-79). IGI Global.

[90] Nyangaresi VO. Provably secure authentication protocol for traffic exchanges in unmanned aerial vehicles. High-Confidence Computing. 2023 Sep 15:100154.

[91] Jahid A, Alsharif MH, Hall TJ. The convergence of blockchain, IoT and 6G: Potential, opportunities, challenges and research roadmap. Journal of Network and Computer Applications. 2023 Aug 1;217:103677.

[92] Shahzad K, Aseeri AO, Shah MA. A blockchain-based authentication solution for 6G communication security in tactile networks. Electronics. 2022 Apr 25;11(9):1374.

[93] Singh A, Parizi RM, Zhang Q, Choo KK, Dehghantanha A. Blockchain smart contracts formalization: Approaches and challenges to address vulnerabilities. Computers & Security. 2020 Jan 1;88:101654.

[94] Hewa TM, Hu Y, Liyanage M, Kanhare SS, Ylianttila M. Survey on blockchain-based smart contracts: Technical aspects and future research. IEEE Access. 2021 Mar 23;9:87643-62.

[95] Zhou L, Diro A, Saini A, Kaisar S, Hiep PC. Leveraging zero knowledge proofs for blockchain-based identity sharing: A survey of advancements, challenges and opportunities. Journal of Information Security and Applications. 2024 Feb 1;80:103678.

[96] Ali ZA, Abduljabbar ZA, AL-Asadi HA, Nyangaresi VO, Aldarwish AJ, Neamah HA. Smart Grid and Renewable Energy Security Challenges: A Review. InComputer Science On-line Conference 2024 Apr 25 (pp. 805-825). Cham: Springer Nature Switzerland.

[97] Ziegler V, Schneider P, Viswanathan H, Montag M, Kanugovi S, Rezaki A. Security and trust in the 6G era. Ieee Access. 2021 Oct 14;9:142314-27.

[98] Abdel Hakeem SA, Hussein HH, Kim H. Security requirements and challenges of 6G technologies and applications. Sensors. 2022 Mar 2;22(5):1969.

[99] Kazmi SH, Hassan R, Qamar F, Nisar K, Ibrahim AA. Security concepts in emerging 6G communication: Threats, countermeasures, authentication techniques and research directions. Symmetry. 2023 May 25;15(6):1147.

[100] Scalise P, Boeding M, Hempel M, Sharif H, Delloiacovo J, Reed J. A systematic survey on 5G and 6G security considerations, challenges, trends, and research areas. Future Internet. 2024 Feb 20;16(3):67.

[101] Nyangaresi VO, Moundounga AR. Secure data exchange scheme for smart grids. In2021 IEEE 6th International Forum on Research and Technology for Society and Industry (RTSI) 2021 Sep 6 (pp. 312-316). IEEE.

[102] Ahmed MR, Islam AM, Shatabda S, Islam S. Blockchain-based identity management system and self-sovereign identity ecosystem: A comprehensive survey. Ieee Access. 2022 Oct 25;10:113436-81.

[103] Soltani R, Nguyen UT, An A. A Survey of Self-Sovereign Identity Ecosystem. Security and Communication Networks. 2021;2021(1):8873429.

[104] Ma J, Shrestha R, Adelberg J, Yeh CY, Hossain Z, Knightly E, Jornet JM, Mittleman DM. Security and eavesdropping in terahertz wireless links. Nature. 2018 Nov 1;563(7729):89-93.

[105] Singh R, Sicker D. Thz communications-a boon and/or bane for security, privacy, and national security. InTPRC48: The 48th Research Conference on Communication, Information and Internet Policy 2020 Dec 16.

[106] Alshuraify NA, Yassin AA, Abduljabbar ZA, Nyangaresi VO. Monitoring and surveillance systems based IoTs with Blockchain: Literature Review. Basrah Researches Sciences. 2024 Dec 31;50(2):42-63.

[107] Hammi B, Zeadally S, Nebhen J. Security threats, countermeasures, and challenges of digital supply chains. ACM Computing Surveys. 2023 Jul 17;55(14s):1-40.

[108] Diro A. Space Systems and Malware: Potential Threats. InRansomware Evolution 2025 (pp. 208-232). CRC Press.

[109] Aslam MM, Tufail A, Apong RA, De Silva LC, Raza MT. Scrutinizing security in industrial control systems: An architectural vulnerabilities and communication network perspective. IEEE Access. 2024 Apr 29.

[110] Porambage P, Christopoulou M, Han B, Habibi MA, Bogucka H, Kryszkiewicz P. Security, Privacy, and Trust for Open Radio Access Networks in 6G. IEEE Open Journal of the Communications Society. 2024 Dec 18.

[111] Nyangaresi VO. Hardware assisted protocol for attacks prevention in ad hoc networks. InEmerging Technologies in Computing: 4th EAI/IAER International Conference, iCETiC 2021, Virtual Event, August 18–19, 2021, Proceedings 4 2021 (pp. 3-20). Springer International Publishing.

[112] Anvigh AA, Khavan Y, Pourghebleh B. Transforming vehicular networks: How 6G can revolutionize intelligent transportation?. Science, Engineering and Technology. 2024 Apr 2;4(1):80-93.

[113] Lilhore UK, Arya L, Sharma YK, Rastogi R. Privacy and security for 6G's IoT-connected future in the age of quantum computing. Industrial Quantum Computing: Algorithms, Blockchains, Industry 4.0. 2024 Dec 30:67.

[114] Duong TQ, Ansere JA, Narottama B, Sharma V, Dobre OA, Shin H. Quantum-inspired machine learning for 6G: fundamentals, security, resource allocations, challenges, and future research directions. IEEE open journal of vehicular technology. 2022 Aug 30;3:375-87.

[115] Joseph D, Misoczki R, Manzano M, Tricot J, Pinuaga FD, Lacombe O, Leichenauer S, Hidary J, Venables P, Hansen R. Transitioning organizations to post-quantum cryptography. Nature. 2022 May 12;605(7909):237-43.

[116] Jawad M, Yassin AA, Al-Asadi HA, Abduljabbar ZA, Nyangaresi VO. IoHT System Authentication Through the Blockchain Technology: A Review. In2024 10th International Conference on Control, Decision and Information Technologies (CoDIT) 2024 Jul 1 (pp. 2253-2258). IEEE.

[117] Tambe-Jagtap SN. A Survey of Cryptographic Algorithms in Cybersecurity: From Classical Methods to Quantum-Resistant Solutions. SHIFRA. 2023 Jun 1;2023:43-52.

[118] Tom JJ, Anebo NP, Onyekwelu BA, Wilfred A, Eyo RE. Quantum computers and algorithms: a threat to classical cryptographic systems. Int. J. Eng. Adv. Technol. 2023 Jun;12(5):25-38.

[119] Wang X, Xu G, Yu Y. Lattice-based cryptography: A survey. Chinese Annals of Mathematics, Series B. 2023 Nov;44(6):945-60.

[120] Fathalla E, Azab M. Beyond Classical Cryptography: A Systematic Review of Post-Quantum Hash-Based Signature Schemes, Security, and Optimizations. IEEE Access. 2024 Oct 23.

[121] Balamurugan C, Singh K, Ganesan G, Rajarajan M. Post-quantum and code-based cryptography—some prospective research directions. Cryptography. 2021 Dec 20;5(4):38.

[122] Dey J, Dutta R. Progress in multivariate cryptography: Systematic review, challenges, and research directions. ACM Computing Surveys. 2023 Mar 3;55(12):1-34.

[123] Nyangaresi VO. Masked Symmetric Key Encrypted Verification Codes for Secure Authentication in Smart Grid Networks. In2022 4th Global Power, Energy and Communication Conference (GPECOM) 2022 Jun 14 (pp. 427-432). IEEE.

[124] Alléaume R, Branciard C, Bouda J, Debuisschert T, Dianati M, Gisin N, Godfrey M, Grangier P, Länger T, Lütkenhaus N, Monyk C. Using quantum key distribution for cryptographic purposes: A survey. Theoretical Computer Science. 2014 Dec 4;560:62-81.

[125] Portmann C, Renner R. Security in quantum cryptography. Reviews of Modern Physics. 2022 Apr 1;94(2):025008.

[126] Pawar HR, Harkut DG. Classical and quantum cryptography for image encryption & decryption. In2018 International conference on research in intelligent and computing in engineering (RICE) 2018 Aug 22 (pp. 1-4). IEEE.

[127] Vasani V, Prateek K, Amin R, Maity S, Dwivedi AD. Embracing the quantum frontier: Investigating quantum communication, cryptography, applications and future directions. Journal of Industrial Information Integration. 2024 Mar 21:100594.

[128] Abdali HK, Hussain MA, Abduljabbar ZA, Nyangaresi VO, Aldarwish AJ. Comprehensive Challenges to E-government in Iraq. InComputer Science On-line Conference 2024 Apr 25 (pp. 639-657). Cham: Springer Nature Switzerland.

[129] Saeed MH, Sattar H, Durad MH, Haider Z. Implementation of qkd bb84 protocol in qiskit. In2022 19th International Bhurban Conference on Applied Sciences and Technology (IBCAST) 2022 Aug 16 (pp. 689-695). IEEE.

[130] Begimbayeva Y, Zhaxalykov T, Ussatova O. Investigation of Strength of E91 Quantum Key Distribution Protocol. In2023 19th International Asian School-Seminar on Optimization Problems of Complex Systems (OPCS) 2023 Aug 14 (pp. 10-13). IEEE.

[131] Guo F, Yu FR, Zhang H, Li X, Ji H, Leung VC. Enabling massive IoT toward 6G: A comprehensive survey. IEEE Internet of Things Journal. 2021 Mar 4;8(15):11891-915.

[132] Mao B, Liu J, Wu Y, Kato N. Security and privacy on 6G network edge: A survey. IEEE communications surveys & tutorials. 2023 Feb 14;25(2):1095-127.

[133] Nyangaresi VO, Morsy MA. Towards privacy preservation in internet of drones. In2021 IEEE 6th International Forum on Research and Technology for Society and Industry (RTSI) 2021 Sep 6 (pp. 306-311). IEEE.

[134] Ramakrishna D, Shaik MA. A Comprehensive analysis of Cryptographic Algorithms: Evaluating Security, Efficiency, and Future Challenges. IEEE Access. 2024 Dec 16.

[135] Khan MN, Rao A, Camtepe S. Lightweight cryptographic protocols for IoT-constrained devices: A survey. IEEE Internet of Things Journal. 2020 Sep 24;8(6):4132-56.

[136] Singh S, Sharma PK, Moon SY, Park JH. Advanced lightweight encryption algorithms for IoT devices: survey, challenges and solutions. Journal of Ambient Intelligence and Humanized Computing. 2024 Feb 1:1-8.

[137] Kumar S, Kumar D, Dangi R, Choudhary G, Dragoni N, You I. A review of Lightweight Security and privacy for resource-constrained IoT devices. Computers, Materials and Continua. 2024;78(1):31-63.

[138] Alshuraify A, Yassin AA, Abduljabbar ZA, Nyangaresi VO. Blockchain-based Authentication Scheme in Oil and Gas Industry Data with Thermal CCTV Cameras Applications to Mitigate Sybil and 51% Cyber Attacks. International Journal of Intelligent Engineering & Systems. 2024 Nov 1;17(6).

[139] Chatterjee R, Chakraborty R. A modified lightweight PRESENT cipher for IoT security. In2020 International conference on computer science, engineering and applications (ICCSEA) 2020 Mar 13 (pp. 1-6). IEEE.

[140] Kim B, Cho J, Choi B, Park J, Seo H. Compact implementations of HIGHT block cipher on IoT platforms. Security and Communication Networks. 2019;2019(1):5323578.

[141] RS P. An intelligent dynamic cyber physical system threat detection system for ensuring secured communication in 6G autonomous vehicle networks. Scientific Reports. 2024 Sep 5;14(1):20795.

[142] Rangaraju S. Secure by intelligence: enhancing products with AI-driven security measures. EPH-International Journal of Science And Engineering. 2023 Dec 1;9(3):36-41.

[143] Nyangaresi VO. Target Tracking Area Selection and Handover Security in Cellular Networks: A Machine Learning Approach. InProceedings of Third International Conference on Sustainable Expert Systems: ICSES 2022 2023 Feb 23 (pp. 797-816). Singapore: Springer Nature Singapore.

[144] Sirohi D, Kumar N, Rana PS, Tanwar S, Iqbal R, Hijjii M. Federated learning for 6G-enabled secure communication systems: a comprehensive survey. Artificial Intelligence Review. 2023 Oct;56(10):11297-389.

[145] Sun Y, Liu J, Wang J, Cao Y, Kato N. When machine learning meets privacy in 6G: A survey. IEEE Communications Surveys & Tutorials. 2020 Jul 23;22(4):2694-724.

[146] Al-Rubaye RH, Türkben AK. Using artificial intelligence to evaluating detection of cybersecurity threats in ad hoc networks. Babylonian Journal of Networking. 2024 Apr 30;2024:45-56.

[147] Mohandas R, Vaigandla KK, Sivapriya N, Kirubasankar K. Detection and Evaluation of Cybersecurity Threats in MANET Based on AI. In2024 4th International Conference on Ubiquitous Computing and Intelligent Information Systems (ICUIS) 2024 Dec 12 (pp. 1486-1492). IEEE.

[148] Mohammed MA, Hussain MA, Oraibi ZA, Abduljabbar ZA, Nyangaresi VO. Secure Content Based Image Retrieval System Using Deep Learning. J. Basrah Res.(Sci.). 2023 Dec 30;49(2):94-111.

[149] Rajendran RK, Priya TM, Blessing NW. AI Solutions for Complex Communication Network Challenges. InAI for Large Scale Communication Networks 2025 (pp. 45-58). IGI Global.

[150] Bountakas P, Zarras A, Lekidis A, Xenakis C. Defense strategies for adversarial machine learning: A survey. Computer Science Review. 2023 Aug 1;49:100573.

[151] Rupanetti D, Boukabou I, Kaabouch N. Examining Anticipated Massive MIMO 5G Network Attacks Through Adversarial Examples. In2023 3rd Intelligent Cybersecurity Conference (ICSC) 2023 Oct 23 (pp. 141-146). IEEE.

[152] He K, Kim DD, Asghar MR. Adversarial machine learning for network intrusion detection systems: A comprehensive survey. IEEE Communications Surveys & Tutorials. 2023 Jan 3;25(1):538-66.

[153] Malik J, Muthalagu R, Pawar PM. A systematic review of adversarial machine learning attacks, defensive controls and technologies. IEEE Access. 2024 Jul 4.

[154] Nyangaresi VO. Privacy Preserving Three-factor Authentication Protocol for Secure Message Forwarding in Wireless Body Area Networks. Ad Hoc Networks. 2023 Apr 1;142:103117.

[155] Afrin N, Pathak A. Blockchain-Powered Security and Transparency in Supply Chain: Exploring Traceability and Authenticity through Smart Contracts. International Journal of Computer Applications. 2023;85:5-15.

[156] Mishra R, Kshetri N, Jha SK. Leveraging Blockchain Technology for Making Secure IoT Networks. InBlockchain Technology for Cyber Defense, Cybersecurity, and Countermeasures 2025 Jan 30 (pp. 17-33). CRC Press.

[157] Thiyagarajan G. Enhancing Captive Portal Authentication With Zero-Knowledge Proofs (ZKP). International Journal of Computer Applications. 2024 Nov 26;186(48):43-51.

[158] Alghamedy FH, El-Haggar N, Alsumayt A, Alfawaer Z, Alshammari M, Amouri L, Aljameel SS, Albassam S. Unlocking a Promising Future: integrating Blockchain Technology and FL-IoT in the journey to 6G. IEEE Access. 2024 Jul 30.

[159] Al Sibahee MA, Abduljabbar ZA, Ngueilbaye A, Luo C, Li J, Huang Y, Zhang J, Khan N, Nyangaresi VO, Ali AH. Blockchain-Based Authentication Schemes in Smart Environments: A Systematic Literature Review. IEEE Internet of Things Journal. 2024 Jul 3.

[160] Liu Y. A Framework for Decentralized Identity and Credential Management Leveraging Blockchain Technology. Advances in Economics, Management and Political Sciences. 2024 Oct 25;103:108-19.

[161] Dwivedi AD, Singh R, Ghosh U, Mukkamala RR, Tolba A, Said O. Privacy preserving authentication system based on non-interactive zero knowledge proof suitable for Internet of Things. Journal of Ambient Intelligence and Humanized Computing. 2022 Oct 1:1-1.

[162] Yang X, Li W. A zero-knowledge-proof-based digital identity management scheme in blockchain. Computers & Security. 2020 Dec 1;99:102050.

[163] Siddiqui S, Hameed S, Shah SA, Arshad J, Ahmed Y, Draheim D. A smart-contract-based adaptive security governance architecture for smart city service interoperations. Sustainable Cities and Society. 2024 Oct 15;113:105717.

[164] Soofiyan S, Karami A. Ethereum Smart Contracts: A Hierarchical Analysis of Vulnerability Challenges and Mitigation Strategies. Cluster Computing. 2025 Feb 7:In-press.

[165] Nyangaresi VO. Provably Secure Pseudonyms based Authentication Protocol for Wearable Ubiquitous Computing Environment. In2022 International Conference on Inventive Computation Technologies (ICICT) 2022 Jul 20 (pp. 1-6). IEEE.

[166] Das S, Priyadarshini R, Mishra M, Barik RK. Leveraging Towards Access Control, Identity Management, and Data Integrity Verification Mechanisms in Blockchain-Assisted Cloud Environments: A Comparative Study. Journal of Cybersecurity and Privacy. 2024 Dec 2;4(4):1018-43.

[167] Ramasamy LK, Khan F. Secure and transparent educational data record-keeping with blockchain. InBlockchain for Global Education 2024 Feb 14 (pp. 147-164). Cham: Springer Nature Switzerland.

[168] Ghazali R, Ali FH, Bakar HA, Ahmad MN, Haron NS, Omar AH, Ahmadian A. Blockchain for record-keeping and data verifying: proof of concept. Multimedia Tools and Applications. 2022 Oct;81(25):36587-605.

[169] Yadav S, Sharma N, Mangla M, Mahajan A. Blockchain and ipfs based framework for secure student document record keeping. Journal of Educational Multimedia and Hypermedia. 2021 Apr;30(2):165-81.

[170] Umran SM, Lu S, Abduljabbar ZA, Nyangaresi VO. Multi-chain blockchain based secure data-sharing framework for industrial IoTs smart devices in petroleum industry. Internet of Things. 2023 Dec 1;24:100969.

[171] Sanenga A, Mapunda GA, Jacob TM, Marata L, Basutli B, Chuma JM. An overview of key technologies in physical layer security. Entropy. 2020 Nov 6;22(11):1261.

[172] Zhang S, Huang W, Liu Y. A systematic survey on physical layer security oriented to reconfigurable intelligent surface empowered 6G. Computers & Security. 2024 Sep 4:104100.

[173] Mahmoud H, Ismail T, Baiyekusi T, Idrissi M. Advanced Security Framework for 6G Networks: Integrating Deep Learning and Physical Layer Security. Network. 2024 Oct 23;4(4):453-67.

[174] Ji Y, Yu J, Yao Y, Yu K, Chen H, Zheng S. Securing wireless communications from the perspective of physical layer: A survey. Internet of Things. 2022 Aug 1;19:100524.

[175] Nyangaresi VO, Mohammad Z. Session Key Agreement Protocol for Secure D2D Communication. InThe Fifth International Conference on Safety and Security with IoT: SaSeIoT 2021 2022 Jun 12 (pp. 81-99). Cham: Springer International Publishing.

[176] Sai M. Securing the secrets of 5G: Mitigating eavesdropping threats and enhancing network integrity. Emerging Trends in Computer Science and Its Application. 2025 Apr 8:143-9.

[177] Furqan HM, Solaija MS, Türkmen H, Arslan H. Wireless communication, sensing, and REM: A security perspective. IEEE Open Journal of the Communications Society. 2021 Jan 26;2:287-321.

[178] Hamamreh JM, Furqan HM, Arslan H. Classifications and applications of physical layer security techniques for confidentiality: A comprehensive survey. IEEE Communications Surveys & Tutorials. 2018 Oct 25;21(2):1773-828.

[179] Jameel F, Wyne S, Kaddoum G, Duong TQ. A comprehensive survey on cooperative relaying and jamming strategies for physical layer security. IEEE Communications Surveys & Tutorials. 2018 Aug 15;21(3):2734-71.

[180] Zaki Rashed AN, Ahammad SH, Daher MG, Sorathiya V, Siddique A, Asaduzzaman S, Rehana H, Dutta N, Patel SK, Nyangaresi VO, Jibon RH. Signal propagation parameters estimation through designed multi layer fibre with higher dominant modes using OptiFibre simulation. Journal of Optical Communications. 2022 Jun 23(0).

[181] Khoshafa MH, Maraqa O, Moualeu JM, Aboagye S, Ngatched TM, Ahmed MH, Gadallah Y, Di Renzo M. RIS-assisted physical layer security in emerging RF and optical wireless communication systems: A comprehensive survey. IEEE Communications Surveys & Tutorials. 2024 Oct 28.

[182] Gebali F, Elhadad MK. PUFGuard: Vehicle-to-Everything Authentication Protocol for Secure Multihop Mobile Communication. Computers. 2023 Nov 14;12(11):233.

[183] Shamsoshoara A, Korenda A, Afghah F, Zeadally S. A survey on physical unclonable function (PUF)-based security solutions for Internet of Things. Computer Networks. 2020 Dec 24;183:107593.

[184] Al-Ghuraybi HA, AlZain MA, Soh B. Exploring the integration of blockchain technology, physical unclonable function, and machine learning for authentication in cyber-physical systems. Multimedia Tools and Applications. 2024 Apr;83(12):35629-72.

[185] Nyangaresi VO. Lightweight anonymous authentication protocol for resource-constrained smart home devices based on elliptic curve cryptography. Journal of Systems Architecture. 2022 Dec 1;133:102763.

[186] Singh SP, Nayyar A, Kumar R, Sharma A. Fog computing: from architecture to edge computing and big data processing. The Journal of Supercomputing. 2019 Apr 1;75:2070-105.

[187] Ometov A, Molua OL, Komarov M, Nurmi J. A survey of security in cloud, edge, and fog computing. Sensors. 2022 Jan 25;22(3):927.

[188] Drucker N, Gueron S. Achieving trustworthy Homomorphic Encryption by combining it with a Trusted Execution Environment. J. Wirel. Mob. Networks Ubiquitous Comput. Dependable Appl.. 2018 Mar;9(1):86-99.

[189] Wang Z, Zhuang Y. Malicious code detection for trusted execution environment based on paillier homomorphic encryption. IEICE Transactions on Communications. 2020 Mar 1;103(3):155-66.

[190] Ahmad AY, Verma N, Sarhan N, Awwad EM, Arora A, Nyangaresi VO. An IoT and Blockchain-Based Secure and Transparent Supply Chain Management Framework in Smart Cities Using Optimal Queue Model. IEEE Access. 2024 Mar 18.

[191] Gowda SD. Secure Multiparty Computation: Protocols, Collaborative Data Processing, and Real-World Applications in Industry. InCloud Security 2024 Aug 28 (pp. 160-182). Chapman and Hall/CRC.

[192] Zhou I, Tofigh F, Piccardi M, Abolhasan M, Franklin D, Lipman J. Secure multi-party computation for machine learning: A survey. IEEE Access. 2024 Apr 15.

[193] Alloghani M, Alani MM, Al-Jumeily D, Baker T, Mustafina J, Hussain A, Aljaaf AJ. A systematic review on the status and progress of homomorphic encryption technologies. Journal of Information Security and Applications. 2019 Oct 1;48:102362.

[194] Acar A, Aksu H, Uluagac AS, Conti M. A survey on homomorphic encryption schemes: Theory and implementation. ACM Computing Surveys (Csur). 2018 Jul 25;51(4):1-35.

[195] Nyangaresi VO, Alsamhi SH. Towards secure traffic signaling in smart grids. In2021 3rd Global Power, Energy and Communication Conference (GPECOM) 2021 Oct 5 (pp. 196-201). IEEE.

[196] Feng D, Qin Y, Feng W, Li W, Shang K, Ma H. Survey of research on confidential computing. IET Communications. 2024 Jun;18(9):535-56.

[197] Muñoz A, Ríos R, Román R, López J. A survey on the (in) security of trusted execution environments. Computers & Security. 2023 Jun 1;129:103180.

[198] Coppolino L, D'Antonio S, Mazzeo G, Romano L. A comprehensive survey of hardware-assisted security: From the edge to the cloud. Internet of Things. 2019 Jun 1;6:100055.

[199] Mazher N, Basharat A, Nishat A. AI-Driven Threat Detection: Revolutionizing Cyber Defense Mechanisms. Eastern-European Journal of Engineering and Technology. 2024 Dec 3;3(1):70-82.

[200] Ekundayo F, Atoyebi I, Soyele A, Ogunwobi E. Predictive Analytics for Cyber Threat Intelligence in Fintech Using Big Data and Machine Learning. Int J Res Publ Rev. 2024;5(11):1-5.

[201] Ali ZA, Abduljabbar ZA, AL-Asadi HA, Nyangaresi VO, Abduljaleel IQ, Aldarwish AJ. A Provably Secure Anonymous Authentication Protocol for Consumer and Service Provider Information Transmissions in Smart Grids. Cryptography. 2024 May 9;8(2):20.

[202] Porambage P, Gür G, Osorio DP, Liyanage M, Gurtov A, Ylianttila M. The roadmap to 6G security and privacy. IEEE Open Journal of the Communications Society. 2021 May 10;2:1094-122.

[203] Aslan Ö, Aktuğ SS, Ozkan-Okay M, Yilmaz AA, Akin E. A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions. Electronics. 2023 Mar 11;12(6):1333.

[204] Djenna A, Harous S, Saidouni DE. Internet of things meet internet of threats: New concern cyber security issues of critical cyber infrastructure. Applied Sciences. 2021 May 17;11(10):4580.

[205] Wang Y, Kang X, Li T, Wang H, Chu CK, Lei Z. SIX-Trust for 6G: Toward a secure and trustworthy future network. IEEE Access. 2023 Oct 2;11:107657-68.

[206] Alhammadi A, Shayea I, El-Saleh AA, Azmi MH, Ismail ZH, Kouhalvandi L, Saad SA. Artificial intelligence in 6G wireless networks: Opportunities, applications, and challenges. International Journal of Intelligent Systems. 2024;2024(1):8845070.

[207] Nyangaresi VO, El-Omari NK, Nyakina JN. Efficient Feature Selection and ML Algorithm for Accurate Diagnostics. Journal of Computer Science Research. 2022 Jan 25;4(1):10-9.

[208] Chitimoju S. Ethical Challenges of AI in Cybersecurity: Bias, Privacy, and Autonomous Decision-Making. Journal of Computational Innovation. 2023 Nov 14;3(1).

[209] Kaushik K, Khan A, Kumari A, Sharma I, Dubey R. Ethical considerations in AI-based cybersecurity. InNext-generation cybersecurity: AI, ML, and Blockchain 2024 May 19 (pp. 437-470). Singapore: Springer Nature Singapore.

[210] Hu Y, Kuang W, Qin Z, Li K, Zhang J, Gao Y, Li W, Li K. Artificial intelligence security: Threats and countermeasures. ACM Computing Surveys (CSUR). 2021 Nov 23;55(1):1-36.

[211] Khan MA, Javaid S, Mohsan SA, Tanveer M, Ullah I. Future-proofing security for UAVs with post-quantum cryptography: A review. IEEE Open Journal of the Communications Society. 2024 Oct 28.

[212] Parida NK, Jatoth C, Reddy VD, Hussain MM, Faizi J. Post-quantum distributed ledger technology: a systematic survey. Scientific Reports. 2023 Nov 25;13(1):20729.

[213] Abduljabbar ZA, Nyangaresi VO, Jasim HM, Ma J, Hussain MA, Hussien ZA, Aldarwish AJ. Elliptic Curve Cryptography-Based Scheme for Secure Signaling and Data Exchanges in Precision Agriculture. Sustainability. 2023 Jun 28;15(13):10264.

[214] Sahoo A, AK IK, Rajagopal SM. Comparative Study of Cryptographic Algorithms in Post Quantum Computing Landscape. In2024 5th International Conference on Data Intelligence and Cognitive Informatics (ICDICI) 2024 Nov 18 (pp. 36-40). IEEE.

[215] Bhatt S, Bhushan B, Srivastava T, Anoop VS. Post-quantum cryptographic schemes for security enhancement in 5G and B5G (beyond 5G) cellular networks. In5G and Beyond 2023 Aug 30 (pp. 247-281). Singapore: Springer Nature Singapore.

[216] Sliti M, Mrabet M, Ben Ammar L. A survey of jamming vulnerabilities in free space optical communication systems and mitigation techniques. Optical and Quantum Electronics. 2024 Feb 18;56(4):706.

[217] Tripathi S, Sabu NV, Gupta AK, Dhillon HS. Millimeter-wave and terahertz spectrum for 6G wireless. In6G Mobile Wireless Networks 2021 Mar 22 (pp. 83-121). Cham: Springer International Publishing.

[218] Zaman S, Tariq F, Khandaker M, Khan RT. A Comprehensive overview of security and privacy in the 6G era. 6G Wireless. 2023 Jun 30:203-58.

[219] Nyangaresi VO, Petrovic N. Efficient PUF based authentication protocol for internet of drones. In2021 International Telecommunications Conference (ITC-Egypt) 2021 Jul 13 (pp. 1-4). IEEE.

[220] Alwarafy A, Al-Thelaya KA, Abdallah M, Schneider J, Hamdi M. A survey on security and privacy issues in edge-computing-assisted internet of things. IEEE Internet of Things Journal. 2020 Aug 10;8(6):4004-22.

[221] Veeramachaneni V. Edge Computing: Architecture, Applications, and Future Challenges in a Decentralized Era. Recent Trends in Computer Graphics and Multimedia Technology. 2025;7(1):8-23.

[222] Mishra N, Pandya S. Internet of things applications, security challenges, attacks, intrusion detection, and future visions: A systematic review. IEEE Access. 2021 Apr 15;9:59353-77.

[223] Chaabouni N, Mosbah M, Zemmari A, Sauvignac C, Faruki P. Network intrusion detection for IoT security based on learning techniques. IEEE Communications Surveys & Tutorials. 2019 Jan 30;21(3):2671-701.

[224] Al Sibahee MA, Nyangaresi VO, Ma J, Abduljabbar ZA. Stochastic Security Ephemeral Generation Protocol for 5G Enabled Internet of Things. InIoT as a Service: 7th EAI International Conference, IoTaaS 2021, Sydney, Australia, December 13–14, 2021, Proceedings 2022 Jul 8 (pp. 3-18). Cham: Springer International Publishing.

[225] Ahakonye LA, Nwakanma CI, Kim DS. Tides of blockchain in IoT cybersecurity. Sensors. 2024 May 14;24(10):3111.

[226] Zuo Y. Exploring the Synergy: AI Enhancing Blockchain, Blockchain Empowering AI, and their Convergence across IoT Applications and Beyond. IEEE Internet of Things Journal. 2024 Nov 27.

[227] Ni Q, Linfeng Z, Zhu X, Ali I. A novel design method of high throughput blockchain for 6G networks: Performance analysis and optimization model. IEEE Internet of Things Journal. 2022 Jul 29;9(24):25643-59.

[228] Khan SN, Loukil F, Ghedira-Guegan C, Benkhelifa E, Bani-Hani A. Blockchain smart contracts: Applications, challenges, and future trends. Peer-to-peer Networking and Applications. 2021 Sep;14:2901-25.

[229] Nyangaresi VO. Lightweight key agreement and authentication protocol for smart homes. In2021 IEEE AFRICON 2021 Sep 13 (pp. 1-6). IEEE.

[230] Liyanage M, Porambage P, Zeydan E, Senavirathne T, Siriwardhana Y, Yadav AK, Siniarski B. Advancing security for 6G smart networks and services. In2024 Joint European Conference on Networks and Communications & 6G Summit (EuCNC/6G Summit) 2024 Jun 3 (pp. 1169-1174). IEEE.

[231] Blika A, Palmos S, Doukas G, Lamprou V, Pelekis S, Kontoulis M, Ntanos C, Askounis D. Federated Learning For Enhanced Cybersecurity And Trustworthiness In 5G and 6G Networks: A Comprehensive Survey. IEEE Open Journal of the Communications Society. 2024 Aug 26.

[232] Suomalainen J, Ahmad I, Shajan A, Savunen T. Cybersecurity for tactical 6G networks: Threats, architecture, and intelligence. Future Generation Computer Systems. 2025 Jan 1;162:107500.

[233] Varadam D, Shankar SP, Nidhi NP, Dubey V, Jadwani A, Taj SF, Uthappa SC, Bharadwaj A. AI in 6G Network Security and Management. InReshaping CyberSecurity With Generative AI Techniques 2025 (pp. 173-200). IGI Global.

[234] Abduljabbar ZA, Omollo Nyangaresi V, Al Sibahee MA, Ghrabat MJ, Ma J, Qays Abduljaleel I, Aldarwish AJ. Session-Dependent Token-Based Payload Enciphering Scheme for Integrity Enhancements in Wireless Networks. Journal of Sensor and Actuator Networks. 2022 Sep 19;11(3):55.

[235] Tanikonda A, Pandey BK, Peddinti SR, Katragadda SR. Advanced AI-Driven Cybersecurity Solutions for Proactive Threat Detection and Response in Complex Ecosystems. Journal of Science & Technology. 2022 Jan;3(1).

[236] Zhang J, Tenney D. The Evolution of Integrated Advance Persistent Threat and Its Defense Solutions: A Literature Review. Open Journal of Business and Management. 2023 Dec 6;12(1):293-338.

[237] Kaloudi N, Li J. The ai-based cyber threat landscape: A survey. ACM Computing Surveys (CSUR). 2020 Feb 5;53(1):1-34.

[238] Malik V, Khanna A, Sharma N. Advanced Persistent Threats (APTs): Detection Techniques and Mitigation Strategies. International Journal of Global Innovations and Solutions (IJGIS). 2024 Aug 2.

[239] Salem AH, Azzam SM, Emam OE, Abohany AA. Advancing cybersecurity: a comprehensive review of AI-driven detection techniques. Journal of Big Data. 2024 Aug 4;11(1):105.

[240] Alessandro R, Giulia B. AI-Enhanced Cybersecurity Proactive Measures against Ransomware and Emerging Threats. Innovative: International Multi-disciplinary Journal of Applied Technology. 2024;2(11):77-92.