Computers, Materials & Continua

Tech Science Press

Doi:10.32604/cmc.2025.064028

REVIEW

A Survey on Artificial Intelligence and Blockchain Clustering for Enhanced Security in 6G Wireless Networks

A. F. M. Shahen Shah[1,*], **Muhammet Ali Karabulut**[2], **Abu Kamruzzaman**[3], **Dalal Alharthi**[4] and **Phillip G. Bradford**[5]

[1]Department of Electronics and Communication Engineering, Yildiz Technical University, Istanbul, 34220, Türkiye
[2]Department of Electronics Engineering, Turkish Air Force Academy, National Defense University, Istanbul, 34129, Türkiye
[3]Department of Business and Economics, School of Business and Information Systems, York College, The City University of New York, New York, NY 11451, USA
[4]College of Applied Sci & Tech, The University of Arizona, Tuscon, AZ 85721, USA
[5]Department of Computer Science, University of Connecticut, Stamford, CT 06901, USA

*Corresponding Author: A. F. M. Shahen Shah. Email: shah@yildiz.edu.tr

Received: 02 February 2025; Accepted: 30 April 2025; Published: 03 July 2025

ABSTRACT: The advent of 6G wireless technology, which offers previously unattainable data rates, very low latency, and compatibility with a wide range of communication devices, promises to transform the networking environment completely. The 6G wireless proposals aim to expand wireless communication's capabilities well beyond current levels. This technology is expected to revolutionize how we communicate, connect, and use the power of the digital world. However, maintaining secure and efficient data management becomes crucial as 6G networks grow in size and complexity. This study investigates blockchain clustering and artificial intelligence (AI) approaches to ensure a reliable and trustworthy communication in 6G. First, the mechanisms and protocols of blockchain clustering that provide a trusted and effective communication infrastructure for 6G networks are presented. Then, AI techniques for network security in 6G are studied. The integration of AI and blockchain to ensure energy efficiency in 6G networks is addressed. Next, this paper presents how the 6G's speed and bandwidth enables AI and the easy management of virtualized systems. Using terahertz connections is sufficient to have virtualized systems move compute environments as well as data. For instance, a computing environment can follow potential security violations while leveraging AI. Such virtual machines can store their findings in blockchains. In 6G scenarios, case studies and real-world applications of AI-powered secure blockchain clustering are given. Moreover, challenges and promising future research opportunities are highlighted. These challenges and opportunities provide insights from the most recent developments and point to areas where AI and blockchain further ensure security and efficiency in 6G networks.

KEYWORDS: AI; blockchain; clustering; energy efficiency; security; challenges; future perspectives; 6G

1 Introduction

Wireless communication technology has advanced at an unprecedented rate. These wireless advances add value to numerous areas of our lives. Significant gains have been made with the implementation of 5G networks, including faster data speeds, lower latency, and better connectivity. However, an even more advanced wireless infrastructure is required to fulfill the needs of upcoming applications such as self-driving cars, the Internet of Things (IoT), and virtual reality. In this context, the 6G protocol proposals seek to transcend the constraints of 5G by introducing previously unimaginable capabilities [1,2].

The 6G proposals offer critical infrastructure for IoT systems. Particularly, 6G is expected to have features such as ultra-fast data transfer, low latency, and high reliability. However, despite these advantages offered by 6G, issues such as security, scalability, and energy efficiency have not yet been fully resolved. The security vulnerabilities that occur when connecting IoT devices to the 6G network will be a critical problem, especially in terms of decentralized identity management and data integrity. Existing studies independently address solutions such as blockchain or artificial intelligence in IoT security. Combining these technologies has not been sufficiently investigated. AI-based threat detection systems have great potential for IoT security, but there is still an open question about how existing AI security solutions should be optimized due to the decentralized and ultra-high-speed nature of 6G [3–6]. Blockchain and AI-based security solutions require more data processing power and low latency in 6G compared to traditional networks. However, how these two technologies can work together more effectively and be scalable is not yet understood.

6G enables IoT devices to operate faster and more reliably with ultra-low latency and high bandwidth. It also offers advanced security mechanisms and AI-supported automation processes for IoT devices. The rapid increase in the number of IoT devices leads to issues such as handling big data analytics, secure authentication, and energy efficiency. The next-generation network architecture offered by 6G should be optimized to meet these requirements. This study examines how IoT can be integrated with 6G securely and efficiently and discusses how AI and blockchain-based security solutions can contribute to this process [7–10]. Given the low latency and high bandwidth expected for 6G networks, these networks go beyond moving data efficiently to give the opportunity for moving virtual compute environments. Moving these virtual compute environments offers a lot, including optimization and security. As an example, this survey explores virtual Raspberry Pis as systems that can be migrated to follow incidents while leveraging blockchain technology and AI. Migrating virtual machines quickly is feasible due to the speed and bandwidth of 6G.

This article analyzes the use of AI and blockchain clustering to improve security in 6G wireless networks. Blockchain clustering divides the blockchain network into smaller clusters to improve scalability and efficiency. AI approaches can be used to improve cluster management and identify security issues. Table 1 demonstrates that our study differs from previous survey papers.

Table 1: Difference between our survey and other survey papers of a similar nature

Surveys	AI	Blockchain clustering	Enhanced security in 6G
Pathak et al. [11]	√	√	
Velliangiri et al. [12]		√	√
Zhang et al. [13]	√		√
Mao et al. [14]	√		√
Liu et al. [15]		√	√
Kamal et al. [16]	√	√	
Bargavi et al. [17]		√	√
Alanhdi and Toka [18]	√	√	
Rustemi et al. [19]	√	√	
Bhat et al. [20]		√	√
Our Survey	√	√	√

This study makes the following significant contributions to the literature on 6G security:

- A comprehensive perspective: A comprehensive overview of the security implications of AI and blockchain clustering in 6G networks is presented.
- AI and blockchain integration: How the synergistic integration of AI and blockchain enhances 6G security is investigated.
- Future directions: Future directions and open research issues for AI and blockchain research in 6G security are identified.

The rest of the paper is organized as follows: Section 2 discusses the concept of blockchain clustering and its benefits in 6G networks. Section 3 examines related AI techniques for 6G security. Section 4 presents the architecture and mechanisms of AI and blockchain integration. Section 5 discusses case studies and applications that demonstrate the effectiveness of the proposed approach. Section 6 highlights the challenges encountered and future research directions. Finally, Section 7 summarizes the conclusions of the paper.

2 Blockchain Clustering Security for 6G

Blockchain is a distributed ledger system that provides a decentralized, transparent, and immutable structure. Each block comprises a series of transactions that are cryptographically linked to the previous block, making it intractable to modify or erase data. These characteristics make blockchain an excellent solution for 6G security because blockchains provide dependable data sharing, authentication, and authorization processes. However, blockchain technology's scalability and performance constraints can present issues, particularly in networks that need high data rates and dense device connections, such as 6G. At this stage, blockchain clustering appears to be a potential method for overcoming these restrictions by leveraging 6G network requirements [21–25]. Fig. 1 shows a application scheme blockchain for 6G.

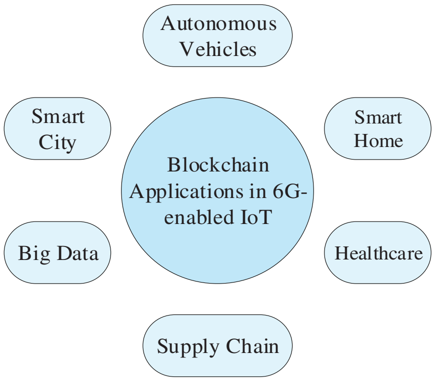

Figure 1: Blockchain applications for 6G

Blockchain clustering is the partitioning of blockchain nodes into smaller, logically grouped clusters based on shared security needs, geographic distribution, or transaction types. Unlike sharding, which distributes ledger storage and transactions across independent chains for scalability, clustering enhances security and efficiency by forming groups of nodes that work together dynamically. This enables data exchange and resource sharing between different blockchains while also providing the flexibility required to deal with the complexities of 6G networks. For example, a study by [26] found that blockchain clustering provides a secure and scalable communication infrastructure for IoT devices. In this study, devices within each cluster use their blockchain networks, so communication between clusters is safe. The blockchain clustering approaches described in Table 2 have the potential to significantly increase security and efficiency in 6G networks.

Table 2: The blockchain clustering methods

Clustering method	Description	Security impacts
Clustering by geographic location	Nodes are grouped into clusters based on their geographic location. This facilitates communication between nearby nodes and reduces network latency.	Isolation of attacks within a specific region Increased resistance to distributed denial-of-service (DDoS) attacks Implementation of local security policies
Clustering by connection strength	Nodes are grouped into clusters based on their network connectivity. This allows for more efficient use of resources and increased network performance.	Protection of critical nodes Optimization of security resources Creation of high-performance clusters
Clustering by confidence level	Nodes are grouped into clusters based on their trustworthiness. This prevents malicious nodes from harming the network and increases security.	Isolation of malicious nodes Increased resistance to Sybil attacks Creation of reliable clusters
Hybrid clustering	Combining different clustering methods creates a more flexible and efficient network structure. For example, geographic location and trustworthiness can be used together to create clustering that both reduces latency and increases security.	Flexible and adaptable network structure Meeting different security requirements Enhanced security and performance
AI-Assisted clustering	Artificial intelligence algorithms provide dynamic and automatic clustering by analyzing network conditions and security threats. This allows the network to adapt to changing conditions and proactively address vulnerabilities.	Dynamic and automatic cluster management Advanced security threat analysis Proactive remediation of vulnerabilities

2.1 Blockchain Clustering Methods

Blockchain clustering can be implemented using different architectures and protocols. Some of the commonly used methods are:

➢ A structure in which a pre-selected group of nodes manages the blockchain network. This can increase scalability and performance, but reduce decentralization. For example, Hyperledger Fabric [27] is a federation-based blockchain platform that can be used for applications such as identity management and access control in 6G networks.

➢ These are secondary blockchains linked to the main blockchain. Sidechains promote scalability by minimizing the strain on the main chain and are suitable for specialized applications. For example, Liquid Network [28] or the Stacks chain [29] are sidechains that connect to the Bitcoin blockchain and enables rapid and secure transactions. Sidechains in 6G networks can be leveraged for different services.

- ➢ It allows transactions to be processed in parallel by dividing the blockchain network into smaller pieces (shards). This significantly increases transaction speed and network capacity. Zilliqa [30] is a blockchain platform that uses sharding. So Zilliqa may be suitable for 6G applications that require high transaction throughput.
- ➢ Protocols that allow data sharing between blockchain networks. This allows different blockchains to collaborate and increases flexibility in the 6G ecosystem. Cosmos [31] is one example of a protocol that offers interoperability between different blockchains and can help integrate heterogeneous blockchain networks in 6G networks.

2.2 Benefits of Blockchain Clustering in 6G Security

Blockchain clustering offers several benefits to increase security in 6G networks:

- ➢ Blockchain clustering's distributed and immutable structure reduces single points of failure and improves cyber-attack resistance.
- ➢ Blockchain clustering increases the scalability and efficiency of 6G networks by distributing the processing load.
- ➢ Blockchain clustering can be integrated with techniques such as zero-knowledge proofs and homomorphic encryption to increase privacy protection. For example, a study by [32] provided secure and confidential data sharing in 6G networks using blockchain clustering and homomorphic encryption.
- ➢ Blockchain-based authentication systems provide reliable and secure identity management in 6G networks.

2.3 Challenges of Blockchain Clustering

The application of blockchain clustering to 6G security also presents some challenges:

- ➢ Standards are needed to ensure interoperability between different blockchain platforms.
- ➢ Blockchain clustering architectures can be complex and difficult to implement.
- ➢ Some blockchain clustering methods result in high energy consumption.

Despite these challenges, blockchain clustering has significant potential to improve security in 6G networks. Future research should focus on addressing these challenges and further improving the effectiveness of blockchain clustering in 6G security.

3 AI Techniques

AI refers to a set of techniques and procedures that allow computer systems to demonstrate human-like intelligence. Given the complexity and dynamic nature of 6G networks, AI is critical for identifying, preventing, and responding to security attacks [33–36]. In this section, we look at the primary AI techniques that can be utilized to improve 6G security. The AI approaches listed in Table 3 provide effective tools for increasing security in 6G networks. Fig. 2 shows AI-enabled applications for 6G networks.

Table 3: Various AI techniques

AI technique	Description	Security impacts
Machine Learning (ML)	ML is a type of AI that allows computers to learn from data without being explicitly programmed. In 6G networks, ML algorithms can be used to analyze network traffic, detect anomalies, and predict attacks.	Detection of network attacks and anomalies Development of intrusion prevention systems Detection of vulnerabilities
Deep Learning (DL)	DL is a subset of ML that uses multilayered artificial neural networks. DL algorithms are increasingly used in 6G network security due to their ability to learn complex patterns and analyze large data sets.	Detection of complex attacks and anomalies Detection of zero-day attacks Advanced security analytics
Natural Language Processing (NLP)	NLP is a field of AI that allows computers to understand and process human language. In 6G networks, NLP can be used to analyze text-based data (e.g., social media posts, forums) to identify security threats.	Detection of social engineering attacks Early warning system of security threats Analysis of security incidents
Computer Vision	Computer vision is a field of AI that allows computers to "see" and interpret images. In 6G networks, computer vision can be used to analyze images from security cameras and detect anomalies.	Detection of physical security breaches Prevention of unauthorized access Image-based security analytics
Reinforcement Learning (RL)	RL is a type of ML that allows an agent to learn by interacting with an environment and receiving rewards. In 6G networks, RL algorithms can be used to optimize security policies and allocate resources efficiently in dynamic environments.	Creation of dynamic security policies Optimization of network resources Automatic response to security threats

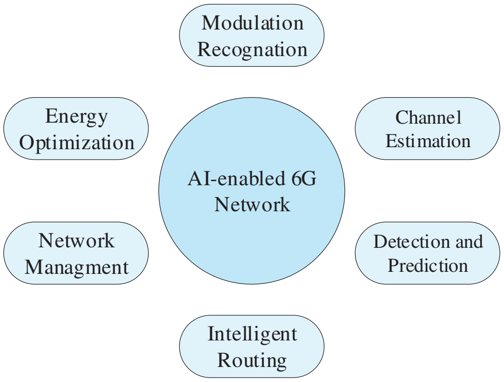

Figure 2: AI-enabled applications for 6G network

3.1 Machine Learning (ML)

Machine learning (ML) is an area of AI that allows systems to learn from data without being explicitly programmed. Analyzing network traffic allows ML systems to discover anomalies, categorize malware, and predict attacks in 6G security. For example, Ref. [37] presents a solution to detect DDoS attacks in 6G networks based on unsupervised learning algorithms. This technology detects irregularities in network traffic and blocks attacks in real time. Similarly, the authors of [38] created a machine learning model for detecting intrusions in 6G networks. Analyzing network data allows this model to detect odd behavior and avoid security breaches.

3.2 Deep Learning (DL)

Deep learning (DL) is a kind of machine learning that uses multilayer artificial neural networks to extract complicated patterns from data. DL is particularly useful for dealing with massive datasets and complicated security risks. In 6G security, deep learning can be utilized for tasks including image identification, natural language processing, and time series analysis. For example, the authors of [39] suggested a deep learning model for detecting malware in 6G networks. This technique can categorize malware samples accurately and improve network security. This technology can analyze network configurations to identify potential security concerns and provide preventive steps.

3.3 Reinforcement Learning (RL)

Reinforcement learning (RL) is an AI technique that enables an entity to learn by interacting with its surroundings and getting incentives. In 6G security, RL can be utilized to create self-learning systems capable of adapting to changing environments and optimizing security rules. For example, Adawadkar and Kulkarni [40] presented a reinforcement learning approach to improve resource allocation and prevent security assaults in 6G networks. This technique, which dynamically allocates network resources, can reduce the impact of attacks while improving network speed.

3.4 Other AI Techniques

In addition to the techniques mentioned above, other AI techniques can be used to enhance 6G security. These include fuzzy logic, genetic algorithms, and expert systems. Fuzzy logic can be used to address uncertainty and complexity, while genetic algorithms can be used to optimize security parameters. Expert systems can be used to make security decisions by imitating human expertise. The integration of AI techniques into 6G security offers a powerful toolkit to combat complex and ever-evolving cyber threats. These techniques increase the reliability and security of 6G networks by making security systems more proactive, adaptive, and effective [41,42].

3.5 AI Clustering

AI clustering is a machine learning method that recognizes certain patterns by analyzing large data sets and makes dynamic decisions using this information. AI clustering can be used for the following basic purposes in 6G networks:

- ➢ AI clustering can detect deviations from normal by analyzing network traffic and can identify cyberattacks at an early stage. For example, during a DDoS attack, abnormal traffic clusters can be automatically identified by AI algorithms, and preventive measures can be taken.
- ➢ AI-supported clustering algorithms can allocate resources such as bandwidth, processing power, the location of virtual compute environments, and energy consumption in the most efficient way in 6G

networks. For example, by analyzing the traffic density of mobile users in a certain area with AI clustering, the load distribution of base stations can be optimized.

➢ AI clustering can create dynamic authentication systems to prevent security breaches by analyzing user behavioral data. For example, when there is an unusual login attempt, the AI model can automatically activate additional security measures.

4 Integration of AI and Blockchain

6G wireless networks may be characterized by unprecedented scale of data generation and device connectivity. This leads to the inadequacy of traditional security mechanisms and makes the network vulnerable to many cyber threats. The integration of AI and blockchain technologies emerges as a promising solution to strengthen 6G security and overcome these challenges. While AI offers intelligent decision-making and automated response capabilities, blockchain provides a reliable and transparent platform. The synergistic combination of these two technologies offers new possibilities to address vulnerabilities and establish a reliable communication infrastructure in 6G networks [43–46]. The integration methods outlined in Table 4 illustrate how AI and blockchain technologies can be combined to improve security in 6G networks.

Table 4: Integration of artificial intelligence and blockchain technologies

Integration method	Description	Security impacts
AI-Enabled blockchain consensus mechanisms	AI algorithms can be used to develop more efficient and secure consensus mechanisms in blockchain networks. For example, machine learning models can be used to detect malicious nodes and prevent network attacks.	Faster and more efficient transaction verification Improved security and attack resistance Reduced energy consumption
Blockchain-Based AI models	AI models can be trained and deployed in a distributed manner using blockchain technology. This increases the security and transparency of models while reducing data manipulation and bias.	Increased model reliability and integrity Protecting data privacy and security Increased model transparency and accountability
Blockchain-Based security auditing	Blockchain technology can provide a reliable and transparent platform for security auditing in 6G networks. Network events and security breaches can be recorded on the blockchain in an immutable manner, allowing the incidents to be reviewed and analyzed later.	Detection and analysis of security incidents Determining the source of attacks Remediation of security vulnerabilities
Blockchain-Based identity management	Blockchain technology can provide a secure and decentralized identity management system in 6G networks. Users can securely store and manage their credentials on the blockchain, preventing identity theft and unauthorized access.	Secure authentication and authorization Protection of personal data Increased user privacy

(Continued)

Table 4 (continued)

Integration method	Description	Security impacts
AI-Enabled smart contracts	AI algorithms can be used to enhance the functionality and security of smart contracts. For example, machine learning models can be used to detect anomalies in smart contracts and prevent fraud.	Automation and optimization of smart contracts Reducing vulnerabilities and errors Increased reliability and transparency of smart contracts

6G networks pose critical security challenges with their ultra-low latency, large-scale connections, and broadband data transfer features. To solve these challenges, artificial intelligence can detect threats in real time using big data analysis and take adaptive security measures. However, the accuracy and integrity of the decision mechanisms of AI-based security systems are a major problem. At this point, blockchain increases the reliability of AI by providing transparency and data integrity to decision mechanisms. For example, security threats identified by AI-supported anomaly detection can be recorded on the blockchain, ensuring that all security nodes in the network have simultaneous information. Thus, decentralized security management becomes possible.

Training AI models usually requires large data sets, and it is important to store and share this data securely. Blockchain provides a decentralized and immutable data storage environment, providing secure and verifiable data usage during the training of AI models. For example, when AI models need to be trained with patient data in the medical and healthcare sector, blockchain can be used to protect data ownership, ensure data validity, and prevent unauthorized access.

AI-based biometric verification systems can be integrated into blockchain to ensure that user credentials are kept secure in a decentralized manner. By combining AI's dynamic threat detection and automatic response capabilities of blockchain-based smart contracts, autonomous security measures can be taken in 6G networks. Large data sets analyzed with AI can be encrypted and securely stored on the blockchain, preventing data manipulation and forgery.

Blockchain and AI integration is not just a theoretical combination, but an important requirement to ensure security, data integrity, and system transparency, especially in complex network environments such as 6G. Thanks to this integration, AI's decision-making mechanisms can be secured and the integrity of the data used by AI can be ensured. Therefore, the combined use of AI and blockchain creates a new paradigm shift in modern security systems.

6G enables real-time processing of large volumes of data by providing ultra-high data speeds (up to 1 Tbps). With latencies falling below milliseconds, the ability of AI-supported systems to make instant decisions is increased. Dynamic spectrum management, network optimization, and self-adaptive security mechanisms can be provided using AI. 6G increases the need for decentralized security approaches, and at this point, blockchain plays a critical role in issues such as secure data sharing and identity verification. In this context, the integration of AI and blockchain into the 6G ecosystem is not just an option, but a necessity to increase network security and efficiency.

4.1 Benefits of AI and Blockchain Integration in 6G Security

The integration of AI and blockchain can improve security in 6G networks in the following ways:

➢ AI algorithms can detect anomalies and prevent attacks in real time by analyzing large amounts of data stored on the blockchain. For example, Liu et al. [47] proposed an AI-based system to detect vulnerabilities in smart contracts on the blockchain. This system can identify potential security risks and prevent attacks by analyzing smart contract code.

➢ Blockchains provide a secure platform for identity management and access control by providing a decentralized and immutable structure. AI can be used to automate identity verification processes and prevent unauthorized access. For example, Al Hwaitat et al. [48] developed a system that combines blockchain and biometric authentication techniques for secure authentication in 6G networks. This system prevents unauthorized access by securely verifying user's identities.

➢ Blockchains enable secure and transparent sharing of data. AI can develop encryption and anonymization techniques to protect the confidentiality of sensitive data. For example, Gao et al. [49] proposed a system that combines blockchain and federated learning techniques for secure data sharing in 6G networks. This system facilitates data sharing and collaboration by preserving the confidentiality of data.

➢ Blockchains increase the resilience of 6G networks by eliminating a single point of failure thanks to their decentralized structure. AI can further strengthen this resilience by optimizing network resources and dynamically responding to attacks.

4.2 Challenges and Future Directions of AI and Blockchain Integration

Although AI and blockchain integration have great potential to enhance 6G security, it also presents some challenges. These include blockchain's scalability limitations, the need for large datasets for training AI models, and ensuring interoperability between different AI and blockchain platforms [50–52]. Future research should focus on addressing these challenges to further enhance the effectiveness of AI and blockchain integration in 6G security.

AI-powered network security solutions detect threats with 30% higher accuracy than traditional systems. It has been measured that blockchain-based data storage systems provide 99.9% data immutability compared to centralized databases. It has been observed that network latency is reduced by 25% as a result of optimizing blockchain consensus algorithms with AI-based prediction systems [53–55]. This data shows that AI and blockchain integration provide not only theoretical but also measurable, tangible advantages in 6G networks.

Thanks to the integration of AI-based sensor data analysis with blockchain-based verification mechanisms, fake data injection attacks are reduced by 40%. Storing medical data analyzed with AI in encrypted form on blockchain reduces patient data breaches by 35%. Energy efficiency has been improved by up to 20% thanks to the management of energy consumption predictions with blockchain-based smart contracts with AI [56–59].

Considering the existing studies on AI and blockchain, the original contributions of this article are clarified. While previous research has generally focused on either AI or blockchain, this study highlights the benefits of integration in the context of 6G. It also discusses in detail how these technologies can be optimized together, particularly in terms of scalability and energy efficiency.

4.2.1 Practical and Real-life Uses of AI and Blockchain in 6G

AI-supported threat detection systems can identify dynamic security threats in real time in 6G, and threat records can be stored immutably with blockchain-based distributed security infrastructures. Given the decentralized structure of 6G, blockchain-based identity verification systems can ensure the security of personal data. Also, fraud detection can be improved with AI-supported analysis. AI-supported driving assistants and communicating vehicles can create a reliable and manipulation-resistant communication infrastructure thanks to blockchain-based secure data sharing protocols. In 6G-supported smart city applications, AI can improve instant decision-making processes with big data analytics, while blockchain can increase data security.

AI-based sensor data analysis and blockchain-based trusted data sharing mechanisms can protect autonomous vehicles from spoofed signals. For example, one study reported that blockchain-supported data verification mechanisms provide 30% higher security in autonomous vehicle systems. Medical imaging data analyzed with AI can be stored immutably using blockchains and made accessible only to authorized persons. For example, it has been observed that the rate of misdiagnosis has decreased by 20% as a result of integrating AI-supported patient diagnosis systems with blockchains. When AI-supported threat detection systems are combined with blockchain-based attack recording mechanisms, the time to detect attacks has accelerated by 40%. These examples show how AI and blockchains can be effectively combined in real-world scenarios.

Blockchains allow transactions to be performed in parallel by fragmenting the blockchain network and increasing scalability. For example, the Ethereum 2.0 network aims to increase transaction capacity using sharding. The concept discussed in this study refers to the coming together of certain groups of nodes to perform certain tasks. For example, AI-supported blockchain clustering can direct security-sensitive transactions to certain trusted nodes. Unlike sharding, clustering focuses on data storage and security optimization. These differences will help clarify the concept of blockchain clustering and prevent readers from confusing this approach with sharding.

6G's low latency supports AI's real-time decision-making ability. 6G's large-scale connections make centralized security approaches inadequate. Blockchain-based security solutions offer a critical advantage at this point. Experiments have shown that AI-supported network management systems combined with blockchains increase 6G network performance by 25%.

5 Case Studies and Applications

5.1 Security for 6G

Billions of connected devices and sensors, where subnetworks may be operating in untrusted domains where there are expectations that the new types of security threats will be introduced to 6G. Even though there will be great benefits in speed, capacity and connectivity introduced in 6G networks, there will be some great security concerns with the integrations of Artificial Intelligence (AI), Internet of Things (IoT) devices, integrated systems into the network utilizing the power of 6G [60–63]. Some key security concerns and mitigations as highlighted in Table 5 can minimize the risk and increase the security for 6G. Table 6 compares the new mechanisms offered by 6G in terms of security with 5G.

Table 5: 6G basic security concerns & mitigations [63]

Security concerns	Mitigations
Data privacy and integrity	Encryption and anonymization
Network vulnerabilities	AI and machine learning for security

(Continued)

Table 5 (continued)

Security concerns	Mitigations
Advanced persistent threats (APTs)	Comprehensive security frameworks
Identity theft and fraud	User awareness and education

Table 6: Comparison of 6G and 5G security mechanisms

Security criteria	5G security mechanisms	6G security mechanisms	Development area
Identity management	Centralized authentication (PKI (public key infrastructure), subscriber identity module (SIM)-based)	Decentralized blockchain-based authentication	Reducing centralization, secure access
Encryption methods	AES-256, ECDH	Quantum secure encryption (Lattice-based cryptography)	Resistance to quantum attacks
Threat detection	Traditional rule-based IDS (Intrusion Detection System)/IPS (Intrusion Prevention System)	AI-powered threat detection and autonomous security systems	Real-time attack detection
Data integrity	Centralized data management	Blockchain-based data storage and integrity verification	Decentralized and reliable data sharing
Access control	RAN-based access control	AI-powered dynamic access control mechanisms	Secure access to sensitive data
Privacy protection	Differential Privacy, basic anonymization	Privacy-focused AI training with Federated Learning	Decentralized data processing
Attack prevention	DDoS filtering, firewalls	AI-powered anomaly detection and autonomous attack prevention	Faster and more effective attack prevention

5.1.1 6G Network Architecture Security Concerns

6G security requires integrating physical, connection, and application layers to enhance security functions. The security requirements of 6G applications are complex due to their high communication needs and performance expectations, necessitating a careful balance of security and performance. The emphasis on zero trust (ZT) principles and adaptive security measures are critical for effectively combating emerging threats.

Zero-trust architecture (ZTA) refers to the relationships between network entities, protocol processes, and access rules using the ZT concept. ZTA should be the foundation of 6G security architecture, focusing on adaptive collaboration among control domains to prevent malicious access behaviors such as DDoS attacks and malware propagation [64–66]. Although an official standard for 6G has not yet been established, organizations such as ITU-T (ITU Telecommunication Standardization Sector), European Union projects, and NGMN (Next Generation Mobile Networks) define the vision and basic requirements of 6G.

ITU-T 2030 Vision

ITU-T's 6G vision envisions this technology to have the following critical components:

- ➢ Faster connections will be provided with data rates of up to 1 Tbps.
- ➢ 6G will enable instant data transmission with latency of less than 1 ms.
- ➢ 6G will have an infrastructure that optimizes itself with AI-based decision mechanisms and can respond instantly to security threats.
- ➢ 6G will include next-generation protocols that reduce carbon footprint and optimize energy consumption.

HEXA-X Project and European Union 6G Studies

EXA-X is a project funded by the European Union that determines the basic building blocks of 6G technology. Some of the critical issues that HEXA-X focuses on are:

- ➢ Dynamic allocation of network resources with AI-supported communication protocols.
- ➢ Creation of 6G's distributed security infrastructure using blockchain and AI.
- ➢ Integration of technologies such as terahertz (THz) bands and reconfigurable intelligent surfaces (RIS) into 6G.

NGMN 6G Studies

NGMN Alliance serves as a platform that defines the basic requirements of 6G for mobile operators. Some of the basic requirements determined by NGMN are as follows:

- ➢ 6G must have a scalable and flexible structure suitable for different usage scenarios.
- ➢ 6G is intended to be used for critical tasks by supporting features such as ultra-reliable low-latency communication (URLLC).
- ➢ 6G will offer a wide range of connectivity options for both IoT devices and human-centric services.

3GPP (3rd Generation Partnership Project) TR 23.288—AI-Enabled Network Management

- ➢ TR 23.288 defines how AI-enabled network management can be optimized and used in automation processes. In the context of 6G, AI-based network management will be critical for dynamic spectrum allocation and real-time security analysis.
- ➢ When AI is used to provide autonomous management of 6G networks, it can predict network outages in advance and allocate network resources in the most efficient way, in accordance with the principles set out in TR 23.288.

3GPP TR 28.809—AI-Enabled Security and Network Optimization

- ➢ TR 28.809 describes the role of AI in identifying, analyzing and preventing security threats. In 6G networks, it is suggested that AI will be combined with blockchain to provide decentralized threat management.

➢ TR 28.809 addresses how AI-based systems should be protected against attacks and what mechanisms can be developed against adversarial attacks. In the context of 6G, it is emphasized that AI-enabled security solutions should be secured with blockchain-based verification mechanisms.

3GPP TS 28.104—AI-Enabled Network Automation

➢ 3GPP TS 28.104 includes recommendations for AI-based automatic network management and security protocols. This standard is a guide on how 6G networks can be made more secure and efficient with AI and blockchains.

➢ AI-supported network automation can detect threats with blockchain-based records by pre-determining malicious attacks. The role of AI in security for 6G is detailed based on this standard.

5.1.2 6G Security Goals & Metrics

The goals and metrics on 6G security cover architecture, applications, technologies, policies, and standardization. It's very important to have a clear vision and goal with practical solutions to detect and resolve network attacks such as Zero-day attacks. In order to anticipate, detect, mitigate, and prevent security assaults as well as to restrict the spread of such vulnerabilities in 6G networks, it will be more crucial than ever to implement intelligent and adaptable security systems. Key Performance Indicators (KPIs) described in Table 7 will assist in fully accounting for the aspects of impact that transcend the purview of deterministic performance metrics.

Table 7: 6G Security KPIs & impact [67]

KPI	Description	6G impact
Protection level	The guarantee of protection from particular dangers and assaults.	Higher requirements due to widespread 6G usage and elevated risk levels.
Response time (average, maximum, etc.)	The duration needed for security mechanisms to address malicious activities.	Significantly reduced as 6G's faster pace allows attacks to escalate more quickly.
Coverage	The extent to which security measures protect 6G elements and functionalities.	Becomes more complex due to the diverse and highly distributed nature of 6G systems.
Automaticity level	The ability of security systems to act autonomously.	Easier to implement with widespread AI, but potential AI-related vulnerabilities could introduce risks.
AI robustness	The network's AI algorithm's ability to survive security threats.	Harder to ensure consistent reliability across the system but increasingly vital due to AI's prominence in 6G.
Security AI model training time	The amount of time needed for AI-based security models to settle and adjust.	Better hardware and more sophisticated AI/ML models are helpful, but complexity and data availability continue to be major obstacles.
Security function chain latency	The amount of time required for connected security procedures to run and react.	6G's decentralized architecture poses challenges, though device- and edge-centric solutions offer some relief.

(Continued)

Table 7 (continued)

KPI	Description	6G impact
Deployment cost of security functions	The financial cost of implementing and maintaining security measures.	Significantly higher due to the complexity, making it difficult to achieve desired performance levels.

A summary of the 6G security threat landscape is given in Fig. 3. Both public and private blockchain systems may have security problems. They result in issues including decreased system availability, loss of accuracy, and monetary losses in cryptocurrency. Table 8 is a list of some of the most significant security holes in smart contracts and blockchain systems. Before deployment, appropriate validation is required to detect semantic problems, use security tools, and carry out formal verification to prevent such security flaws. Strong authentication and access control procedures are also necessary to stop malicious bots and Sybil attacks.

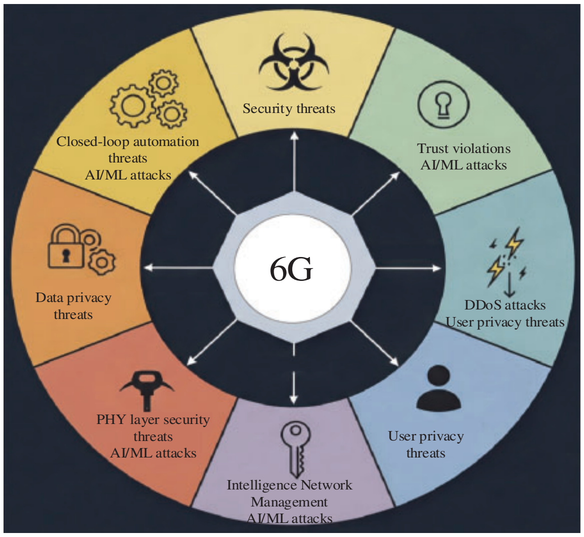

Figure 3: Diagram of 6G security threat landscape

Table 8: Blockchain 6G services security vulnerabilities [67]

No.	Vulnerability	Description
1	The majority attack/51% attack	Malicious actors gain control over the majority of nodes to dominate the blockchain.
2	Double-spending attack	Reusing the same token multiple times fraudulently.
3	Re-entrancy attack	Exploiting smart contracts by repeatedly invoking another contract in a harmful way.
4	Sybil attacks	Gaining network control by creating numerous fake identities.

(Continued)

Table 8 (continued)

No.	Vulnerability	Description
5	Authentication and access control flaws	Weaknesses in mechanisms for verifying identities and managing access rights.
6	Misconfigured security settings	Vulnerabilities are caused by outdated or improperly set security configurations.
7	Privacy breaches	Exposure of sensitive data, including user details and transaction information.
8	Miscellaneous vulnerabilities	Issues such as faulty contracts, random errors, and inefficient computations.

To stop privacy leaks in blockchain-based 6G services, privacy-preserving strategies like Trusted Execution Environments (TEE) and privacy by design should be incorporated. With varying security consequences, blockchain/DLT (Direct Linear Transformation) allows public, private, consortium, and hybrid systems. For example, 51% attacks pose a serious risk to public blockchains; hence, consortium or private blockchains may be better suited for some 6G applications, such as roaming or spectrum management, which require fewer miners. The appropriate selection of blockchain/DLT type can help mitigate the impact of specific attacks.

5.1.3 6G Blockchain Security Concerns

There are many potential opportunities for integrating blockchain technology into 6G applications. The following is a collection of security-related incidents that are offered in an analysis of the prospects and difficulties of blockchain implementation in 6G [68–70].

- ➢ Intelligent Resource Management
- ➢ Elevated Security Features
- ➢ Industrial Applications
- ➢ Smart Healthcare
- ➢ Edge Models ML training Model
- ➢ Decentralized 6G Communications
- ➢ Authentication, Availability, Integrity

Decentralization, transparency with anonymity, provenance, and non-repudiation of transactions, immutability and tamper-proof distributed ledgers, and the removal of single points of failure are some of the most obvious characteristics, if properly implemented.

5.1.4 6G AI Security Threats

Expectations that enhancements of AI into 6G will minimize security risks, but the new threats will emerge as hackers will find new venues to penetrate the security holes in 6G using AI limitations.

Fig. 4 shows a summary of an AI-based system that explains:

- ➢ Data Poisoning: Involves changing input objects or adding data with erroneous labels to datasets to trick ML systems.
- ➢ Algorithm Poisoning: Uploads modified weights to local learning models in an attempt to interfere with the distributed learning process.

➢ Model Poisoning: Substitutes a harmful model for the deployed one.

Among these, data poisoning poses the greatest challenge because input objects in outdoor environments are widely accessible, enabling attackers to perform advanced manipulations easily. Addressing these threats requires a multi-layered security approach, including blockchain-based verifiable training, differential privacy techniques, adversarial robustness testing, and federated learning validation mechanisms.

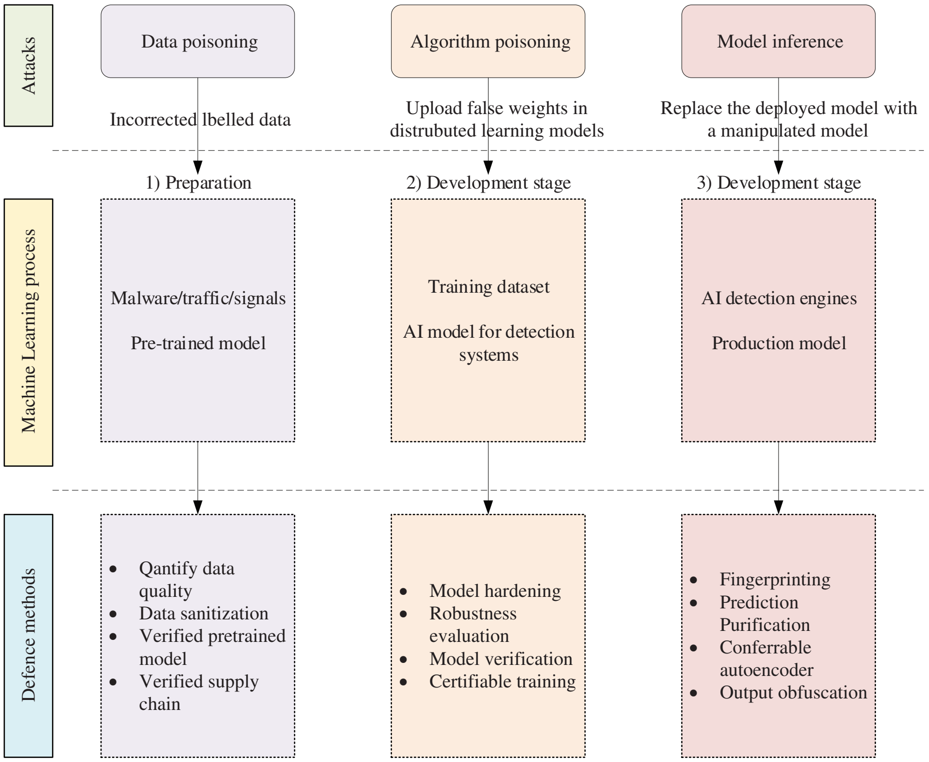

Figure 4: Diagram of 6G operated AI based security model with three attack methods and potential defense methods

Fig. 5 shows an example of an attack that involves using a drone to trick AI-driven control systems in self-driving cars by projecting a fake traffic light image onto a road banner. Similarly, attackers can interfere with AI-based resource allocation systems by using data poisoning techniques, such as inserting false data into transfer or federated learning models [71]. Additionally, it is possible to fool AI-based facial recognition software into thinking that an attacker (John) is someone else (Lucy). With the increasing reliance on AI for critical applications like autonomous driving in 6G networks, these threats pose significant risks [72].

There are several defense tactics that can be used to combat hostile threats to AI systems. By enhancing risk assessments and protecting the integrity of local data and AI models from attacks, technologies like blockchain and high-performance computing may be crucial in tackling AI security issues in the 6G future.

The vision for 6G includes significantly enhancing current AI protection methods through three main approaches:

➢ Improving Data Quality: This includes methods like as lowering noise, altering data characteristics in adversarial samples, or sanitizing tainted data during training. Using verified data sources, such as blockchain-enabled supply chains with mutual authentication, is also recommended.

- ➢ Model Protection: AI designers can implement measure like specialized detectors to block ongoing attacks or conduct multiple evaluations to verify the model's integrity.
- ➢ Restoring Output Integrity: Ensures that the final output remain reliable despite adversarial attempts.

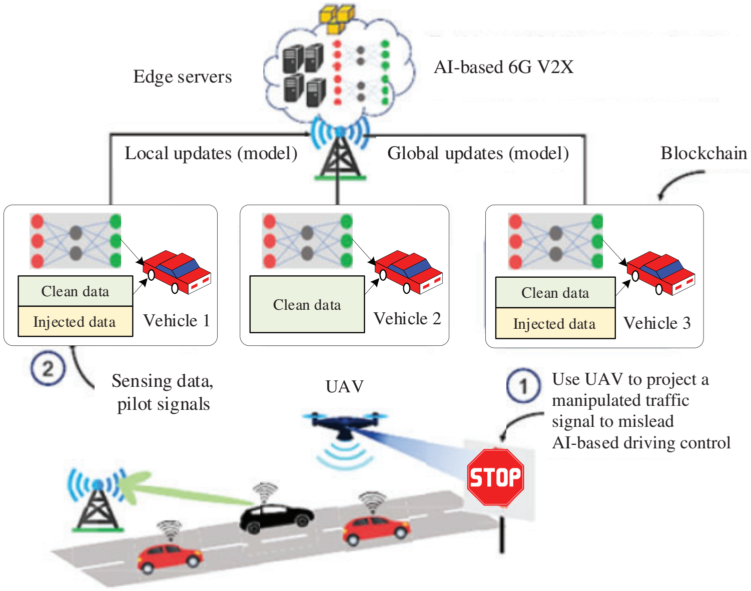

Figure 5: Diagram of physical poisoning and algorithmic attacks on an AI enhanced 6G UAV (unmanned aerial vehicle)

Overall, 6G technologies are expected to bolster AI defenses significantly.

Fig. 6 shows simplified defense against algorithm poisoning involves detecting adversarial models by comparing predictions made on original and compressed (squeezed) input data. Significant differences between the results suggest that adversarial samples may have tainted the original input. To ensure output integrity during deployment, techniques like output obfuscation and prediction purification can be employed.

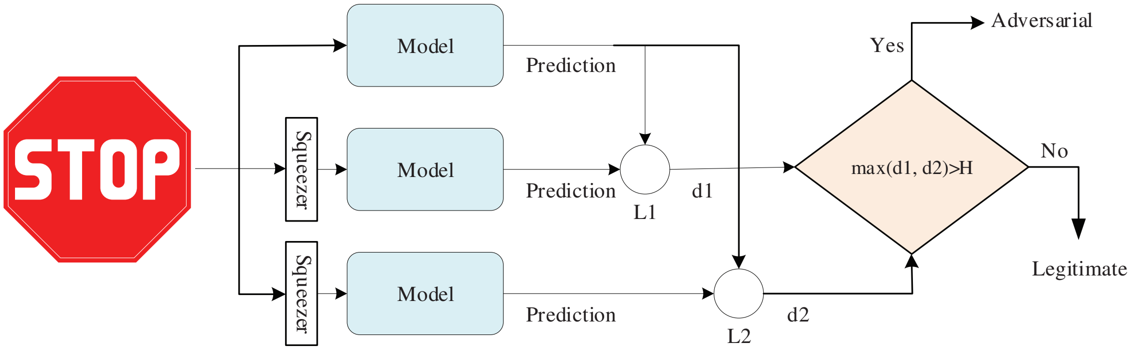

Figure 6: Diagram of defense for adversarial

In the 6G era, advanced methods for identifying vulnerabilities in AI-powered systems, such as model assessment and APIs for scanning weaknesses in AI services, are likely to be developed. The study of adversarial attacks and defenses in deep learning continues to be a significant focus for both academia and industry, emphasizing the need for ongoing research and innovation in AI security.

Since AI models are usually trained with large amounts of data, the security of this data is critical to the accuracy and reliability of AI. The following security risks and precautions that can be taken are detailed:

- ➢ Malicious actors can cause the AI model to make incorrect predictions by adding harmful or incorrect information to the training data. It is recommended that the data be stored in a secure and immutable blockchain-based environment against such attacks.
- ➢ The data used in AI training may contain personal or sensitive information. Techniques such as Federated Learning can increase privacy by enabling decentralized processing of data.
- ➢ AI-based fraud detection systems can prevent the injection of fake data by identifying anomalies. AI and blockchain integration can be used to increase the accuracy of such systems.

AI models can be manipulated or stolen, especially by attackers. In this context, the following security threats have been addressed:

- ➢ When the parameters of AI models are compromised, attackers can learn how the model works and use this information for malicious attacks. In order to reduce this risk, it is recommended that AI models be run in hardware-based secure environments.
- ➢ AI models can be made to make incorrect predictions by making small but deliberate changes. For example, adversarial noise can be added to computer vision systems to cause AI to incorrectly recognize objects. Defense mechanisms include adversarial training and model compression techniques.
- ➢ Malicious code can be added during the update of AI models, creating security vulnerabilities. To prevent such risks, AI model updates can be made to go through blockchain-based verification processes.

5.2 Intelligent 6G Security and Forensics: The Role of GenAI

The emergence of 6G networks, defined by their unprecedented speed and seamless integration of IoT devices, offers transformative potential in domains such as autonomous systems, smart cities, and biomedical informatics. However, the exponential growth of connected devices introduces novel challenges, particularly in ensuring security and conducting digital forensics. Traditional forensic methods struggle to adapt to the vast and heterogeneous environments enabled by 6G, necessitating advanced AI-driven approaches that combine intelligence and scalability to effectively manage modern cyber investigations [73–76].

Generative AI (GenAI) has emerged as a pivotal tool for securing 6G networks. Its ability to process vast amounts of real-time data facilitates the identification of anomalies and potential intrusions with unparalleled speed. By leveraging machine learning models, GenAI enables predictive analytics that anticipate vulnerabilities and mitigate threats before they can materialize [75]. Additionally, GenAI's capacity to correlate fragmented data streams plays a crucial role in reconstructing cyber incidents, making it indispensable for comprehensive forensic analysis in the distributed and dynamic 6G ecosystem [76,77]. Its integration with edge computing ensures localized, low-latency analysis for detecting threats at the source, which further enhances its forensic capabilities. These capabilities underscore GenAI's transformative potential in fortifying 6G networks against emerging threats.

However, the integration of GenAI into 6G security frameworks introduces its own set of vulnerabilities. Prompt injection attacks, where adversarial inputs manipulate AI-generated responses, pose significant risks to 6G applications. Similarly, threats such as data poisoning and model theft jeopardize the integrity of GenAI systems by compromising training datasets and enabling unauthorized access to sensitive architectures. Additionally, inference attacks, which deduce sensitive data from GenAI outputs, and supply chain threats affecting LLM plugins, present further challenges in securing 6G systems. These challenges necessitate robust frameworks like LLMSecOps, which emphasize secure development practices, adversarial training, and the application of differential privacy to safeguard GenAI deployments [77]. Moreover, the inclusion of blockchain technology within these frameworks offers immutable evidence storage, which further strengthens forensic reliability in 6G networks.

Despite its challenges, GenAI holds immense promise for enhancing 6G security and forensics. Its role extends beyond security, encompassing proactive mitigation strategies such as integrating GenAI with decentralized identity verification systems, which enables self-healing networks and automating responses to detecting anomalies. Its application in real-time threat detection, predictive analytics, and forensic investigations highlights its potential to address the limitations of traditional methods. To fully realize this potential, future research must focus on developing resilient GenAI models tailored to 6G environments, mitigating vulnerabilities outlined in the OWASP taxonomy, and integrating GenAI with blockchain for tamper-proof forensic evidence. By addressing these avenues, GenAI can establish itself as a cornerstone of intelligent 6G security and forensic frameworks, which ensures a secure and resilient digital future [77].

5.3 Mobile Virtual Compute Environments and 6G

Easy access, high security, smart connectivity, integrated sensing, industrial IoT, deep learning network augmentation, AR/VR, and ultra-high wireless data transfer rates are all goals for the 6G wireless protocol [78–80]. It is projected that ultra-high wireless data transfer rates will be in the terahertz (THz or 10^{12} cycles per second) range. Distributed edge computing with high-speed and broad connections will be a critical part of realizing many of these goals. In turn, this gives opportunities for small headless virtual machines to play an important role in 6G. This allows mobile virtual compute environments to be easily migrated to enhance optimality or for other reasons. As central examples, virtual Raspberry Pis are very small virtualized headless computers. Here, virtual Raspberry Pis are proxies for any small virtual and headless devices made with off-the-shelf components. Such machines may play a significant role in 6G. The headless virtual machines of focus have small operating system images. These modest image sizes may be run on emulators seated on powerful and extensive physical systems serving the 6G network.

Headless computers have no persistent screen or keyboard attached to them. Headless computers are common in the cloud, where they are focused on delivering value. Juxtaposed to headless computers are personal mobile devices such as mobile phones and tablets. These devices have screens and keyboards or other human-geared data entry methods. Furthermore, AR/VR, holographic, and haptic systems may enhance immersive experiences. In addition to physically moving systems such as drones and vehicles.

Virtual machines (VMs) are software instantiations of physical machines. There are several types of virtualizations. Emulation is the imitation of all aspects of a system. All virtual emulation is done by VMMs (Virtual Machine Manager). VMMs run on hosts. The guest machine is the VM. VMMs perform several different types of emulation or virtualization. Full virtualization is complete software emulation of a physical machine. Hardware-assisted virtualization requires updates to the guest operating system so it can be emulated. Paravirtualization is the emulation of a physical machine by having a guest machine call subroutines on the host for emulation. In OS-level virtualization or containerization, the guest operating system shares major subsystems, i.e., the kernel, of the host operating system. Process-language virtualization is the virtualization of an abstract language-based machine. For example, the JVM, .NET framework, or Python3.

Virtual Raspberry Pi guests typically run on full virtualization, hardware assisted virtualization, or paravirtualization. In turn, these virtual machines can run a host of software tools. They can dynamically install new software when needed. They can participate in significant distributed computation. They can also have high speed and broad connectivity on the edge. For example, physical Raspberry Pis can transmit data through their RJ45 connectors at 1 GB/s, given a suitably fast connector. Where 6G wireless may be able to use THz wireless transmissions, which are anticipated to go as fast as 100 GB/s. Assuming a 1 THz wireless communication network for 6G, consider a virtualized Raspberry Pi. Since these virtual machines are not limited by RJ45s or, more significantly, their connecting cable's capacity, these virtual machines can run as fast as their VMMs and their software and hardware.

Non-Turing complete edge-systems or embedded systems are generally easier to virtualize than complete computers. Emulating these edge systems may help edge computing for 6G. In addition, there are software defined networks and network function virtualization [81]. Personal mobile devices are important endpoints on 6G wireless systems. Today, personal mobile devices leverage cloud systems. Though for many 6G applications, these mobile devices require high-speed and high bandwidth networking, so the cloud may not be ideal for communication or computational support. Along with reliable, high-speed, and high-capacity networking, a lot of computation can be done on the edge to enhance 6G applications. Indeed, the cloud will play a significant role in 6G, though it will be augmented by significant edge computing and edge networking. Particularly, to make 6G most effective, a great deal of edge computing will be necessary.

Initially, early applications of physical Raspberry Pis focused on education. Often, technologies focused on education find their way into significant application areas. Small virtual headless machines will likely follow the same path. Virtual Raspberry Pis and similar headless computers have significant potential for computing on the edge. Interestingly, on one hand, physical components may fail in short time spans. For instance, inexpensive SD cards or other components may fail within a year of use for physical Raspberry Pis. On the other hand, when the hardware is virtualized, there are no SD cards or other hardware issues to worry about. Of course, the systems emulating these machines have taken the responsibility of forestalling physical system failure. This means putting VMMs in several places on the edge. These VMMs emulate virtual machines. In this way, VMMs can be deployed for edge computing. VMMs on the edge have several advantages over physical devices: (1) a VM may be emulated by several differently located VMMs, (2) VMs may be dynamically migrated to several other edge locations or the cloud, (3) VMs may be horizontally scaled by cloning for scaling or failure resistance.

There are also potential issues for these VMMs. For example, VMMs are complex and sophisticated software systems requiring care and maintenance. VMMs run on a specific architecture and may require a lot of resources. VMMs often focus their emulation on specific ISAs (instruction set architectures) and systems. For example, VirtualBox emulates x86 machines, VMware emulates x86-64, Intel VT-x, and AMD-V (AMD Virtualization). QEMU emulates a host of systems, including various ARMs (Advanced RISC Machine) and x86 ISAs. QEMU machines can also take device-tree-blobs for describing systems. In many cloud data centers, OS-level VMs run on fully virtualized machines. These nested virtual machines add a level of abstraction and enhance flexibility. However, this can also cause a great deal of slowdown. For example, suppose an edge VMM runs an x86-64 emulator to run a fully virtualized machine M. Then, if M must run QEMU to emulate an ARM processor A, this may lead to software emulation of A while M may use hardware assisted virtualization, perhaps using VT-x or AMD-V, or paravirtualization. So, M may be efficiently emulated, but A not so much.

Also, bootability needs to be secured. Although physical access to computers or embedded systems can compromise security in any case. The UEFI (Unified Extensible Firmware Interface) unifies and offers a standard booting system for both computers and embedded systems [82]. UEFI is vulnerable when an attacker has physical access to a device. If a copy of a VM is obtained by an attacker, they may have full access to the UEFI instance. Hence, they may be able to circumvent a software version of UEFI.

There are security advantages for virtual Raspberry Pi computers [83]. The attributes that make small virtual machines useful include agility, clonability, migration, and ease of provisioning. They point out that

VMs may also follow situations or individuals by migration. They can use blockchain/DTL (Data Control Language) [84]. These VMs can follow situations along the edge to invalidate deepfakes. For example, systems or mobile devices may benefit from mobile VMs following people or situations in several ways. Data describes situations or people, for example, via face recognition. Repeatedly validating face recognition with locations as a person of interest travels can have added value. Validating factors may be embedded into blockchains for permanence and verifiability.

VM migration can be done by checkpoint and restart [85,86]. Generally, this may lead to stopping the VM. Live VM migration is challenging [85]. Live VM migration moves live VMs from one VMM to another. In any case, it seems best for VMMs to be proactively available in destination locations. Process migration is more challenging due to residual dependencies [86]. These residual dependences include libraries, file handles, expected structures, etc. Standard process-language virtualization has language-based virtual machines. In this case, the developers and system admins must manage the process-language virtualization and its needs to ensure it transfers occur without residual dependencies. For instance, these process-language virtualization systems generally have serialization built into their languages. Serialization allows the conversion of objects or data structures for transportation or persistence. This alleviates some residual dependencies. Process-language virtualization may also be combined with container virtualization to include other dependencies.

At the same time, the terahertz wireless connections that are projected for 6G may allow fast live VM migration in the edge. Particularly, terahertz connections can move a terabit per second. So, moving 1 TB (TeraByte) will take up to a handful of seconds. Connections to major clouds can run at similar speeds.

Though the Cloud is susceptible to unanticipated congestion. Though the Cloud is very useful for very large-scale data sharing. Virtual Raspberry Pi's can be used to enhance security [83]. Small devices can be easily cloned or migrated. Residual dependencies are not an issue with VM migration. For instance, small Raspberry Pi operating system images currently range from 1/2 gigabyte for lite versions to under three gigabytes for full versions. Many ARM operating system images also have accompanying device-tree blobs for describing the hardware of an emulated system. These device-tree-blob files are quite small. Larger operating systems such as Ubuntu routinely have images of five or more gigabytes. Of course, some container-based operating system images, such as Alpine, require as little as five megabytes. No matter the size of the images, these operating systems may be run on large and high-resource hardware platforms.

Moving such virtual machines to, from, or around the edge can soak up a lot of resources. However, 6G networks allow these VMs to be moved easily. Images of these VMs can also be verified on blockchains using message-digest hash functions. Clonability allows horizontal and vertical scaling. Generally, cloning of based on fixed images and may require time to complete installations and booting. Horizontal scaling is done by cloning more virtual systems to enhance security when needed. Blockchains/DLT can be leveraged to record security incidents while the virtual Raspberry Pis are following the likely causes of incidents. Vertical scaling is resizing the system to help with anticipated or actual issues. Small devices can also be provisioned in many useful ways. Significantly, Anwar et al. [79] discuss applications of small virtual devices for investigations.

Virtual machines can migrate for many reasons, as well. For example, small virtual machines may follow mobile devices on the edge. This allows computation to continue on the edge even when connectivity may not be consistent. Specifically, as the demands on 6G subnets evolve, virtual machines can migrate to more optimal locations.

Particularly Ref. [84] shows how to build (insecure) blockchain-like systems on virtual Raspberry Pis. These systems illustrate that small, constrained devices can participate in the security aspects of a secure blockchain. Perhaps building a side chain that is in an isolated, secure location on the edge.

6 Challenges and Future Perspectives

Although AI and blockchain clustering have great potential to improve the security of 6G networks, the implementation and integration of these technologies pose several challenges. In this section, we address these challenges and shed light on future research directions. The challenges and future perspectives, as outlined in Table 9, highlight key issues that need to be addressed for the successful implementation of AI and blockchain clustering technologies to enhance security in 6G networks.

Table 9: The challenges and future perspectives in 6G networks

Challenge	Description	Future perspectives
Scalability	The scalability of blockchain technology is a major concern, especially in large-scale 6G networks. As the size of the blockchain network increases, transaction verification and block addition times also increase, which can negatively affect network performance.	Development of more efficient consensus mechanisms (e.g., Proof-of-Stake) Use of Layer-2 scaling solutions (e.g., Lightning Network) Partitioning the blockchain network into smaller pieces using techniques such as sharding
Privacy	Blockchain technology can bring privacy concerns due to the transparent recording of all transactions. It is important to develop privacy mechanisms to protect sensitive data in 6G networks.	Use of advanced cryptographic techniques such as zero-knowledge proofs and homomorphic encryption Development of privacy-preserving machine learning techniques Use of data anonymization and obfuscation techniques
Computational complexity	Artificial intelligence algorithms, especially deep learning models, can require high computational power. This can make it difficult for resource-constrained devices to join 6G networks.	Development of more efficient AI algorithms Use of technologies such as edge computing and cloud computing Use of hardware acceleration techniques C28 (e.g., Graphics Processing Units (GPUs))
Energy consumption	The energy consumption of blockchain and AI technologies can be a significant problem, especially for mobile devices. New solutions should be developed to improve energy efficiency in 6G networks.	Development of energy-efficient blockchain consensus mechanisms Design of less energy-consuming AI algorithms Use of technologies such as energy harvesting and wireless power transfer

(Continued)

Table 9 (continued)

Challenge	Description	Future perspectives
Standardization	The lack of standards for the use of AI and blockchain technologies in 6G networks can lead to compatibility issues between different systems.	Creation of standards by standards development organizations (e.g., 3GPP, IEEE(Institute of Electrical and Electronics Engineers)) Development of open-source software and hardware platforms Encouragement of industrial collaboration and knowledge sharing
Security vulnerabilities	AI and blockchain technologies can have their own vulnerabilities. For example, AI models can be vulnerable to adversarial attacks, while blockchain networks can be exposed to 51% attacks.	To improve the security of AI models Developing new consensus mechanisms and cryptographic techniques to increase the security of blockchain networks Using continuous monitoring and auditing mechanisms to detect and fix security vulnerabilities
Data quality	The performance of AI algorithms depends on the quality of the data they are trained on. It is important to develop high-quality data collection and labeling mechanisms in 6G networks.	Using data cleaning and preprocessing techniques to improve data quality Using distributed data storage and management systems Developing incentive mechanisms to encourage data sharing and collaboration
Legal and ethical issues	The use of AI and blockchain technologies may raise a number of legal and ethical questions, such as biased decisions made by AI algorithms or the use of blockchain technology for illegal activities.	Developing legal frameworks and regulations to ensure ethical use of AI and blockchain technologies Creating mechanisms to promote transparency and accountability Carrying out education and information activities to raise awareness in society and encourage ethical discussions

6.1 Challenges

- ➢ The scalability of blockchain technology is a significant challenge, especially considering the large data volumes and high transaction speeds in 6G networks. Blockchain clustering can help alleviate this problem, but new methods need to be developed to ensure efficient and secure communication between different blockchains [87,88].
- ➢ AI algorithms often require large amounts of data, which can raise privacy concerns. To exploit the potential of AI while preserving privacy in 6G networks, the use of privacy-preserving AI techniques such as federated learning (FL) is gaining importance [89,90].

- ➢ AI models can be particularly vulnerable to adversarial attacks. When using AI for 6G security, it is critical to develop models that are resilient to attacks such as adversarial examples and data poisoning [91,92].
- ➢ Blockchain and AI techniques can cause high energy consumption, which can be especially important for resource-constrained devices. To increase energy efficiency in 6G networks, it is necessary to develop new algorithms and hardware designs that optimize energy consumption [93,94].
- ➢ Standards are needed to ensure interoperability between different AI and blockchain platforms. Collaboration between standards development organizations and industry partners is important to facilitate harmonization and integration in the 6G ecosystem [95,96].
- ➢ The use of AI and blockchain technologies raises legal and ethical issues such as data privacy, liability, and bias. It is necessary to develop legal frameworks and ethical rules to ensure the responsible and ethical use of these technologies in 6G networks [97,98].

6.2 Future Perspectives

- ➢ Hybrid solutions that combine different AI techniques (e.g., deep learning, reinforcement learning) and blockchain clustering methods can further improve 6G security. Such solutions can provide more comprehensive and effective protection against different security threats [99,100].
- ➢ The rise of quantum computing threatens existing cryptographic algorithms. To ensure the long-term security of 6G networks, it is necessary to develop new blockchain technologies that are resistant to quantum computers [101,102].
- ➢ AI can be used to optimize blockchain performance and scalability. For example, AI algorithms can improve blockchain efficiency by optimizing block size, mining difficulty, and transaction fees [103,104].
- ➢ Open-source platforms can accelerate the development and adoption of AI and blockchain technologies for 6G security. These platforms can support innovation by encouraging collaboration between researchers and developers [105,106]. AI and blockchain clustering offer a powerful synergy for securing 6G wireless networks. Continued research and development efforts are needed to fully realize the potential of these technologies and overcome the challenges we face.

6.3 6G Security Challenges—Research Focus

6G still faces major security challenges as highlighted in Table 10 [72].

Table 10: Major security challenges [72]

Challenges	Highlights
Automated software creation	Vulnerable software is a major contributor to security problems in modern networks and IT systems. Software complexity and variety will increase significantly, expanding the attack surface and creating multiple security challenges. Integrating AI/ML into the software development process adds numerous common defects since current AI/ML approaches are still in their infancy and fragmented. It's still difficult to fully utilize AI/ML for safe, highly automated software development.

(Continued)

Table 10 (continued)

Challenges	Highlights
Automated security operations	Automation based AI/ML has a lot of potential to solve today's problems and move toward more sophisticated, self-adjusting, and all-encompassing orchestration and management systems. AI/ML can improve network security, but it poses new threats as well. The two main challenges are: ■ Preparing for possible AI/ML-driven assaults. ■ Protecting AI/ML systems from targeted attacks while maintaining their explainability and reliability. The scope and impact of AI/ML-based attacks are still unpredictable. To properly respond and safeguard 6G networks, it is imperative to continuously monitor advances in Automated Security Operations.
Privacy preserving technologies	Large datasets, frequently gathered from diverse sources across multiple domains, are necessary for AI/ML techniques to create accurate models. Large volumes of sensitive data are produced in 6G networks with high-precision location and network sensing. It's difficult to protect data's privacy and confidentiality from outside threats and to minimize the amount of private information shared between parties in order to provide 6G services. 6G's enormous and ongoing data creation, a strong framework for data processing, and protecting privacy is crucial. The goals of the framework should be to regulate and keep an eye on data access and flows. New approaches that make use of edge processing, federated learning, and distributed 6G Het-cloud (heterogeneous-cloud) are required for overseeing and implementing adaptable data security and privacy regulations. Resolving performance issues improves data privacy.
Hardware & cloud embedded anchors of trust	Hardware-based trust anchors and embedded security are essential components of a dependable 6G system. 6G challenges of adapting per-server attestation to virtualization and container technologies, and making it work with the very flexible and dynamic network deployment of the het-cloud, even though it is effective in today's networks.
Quantum safe security	Research has already advanced significantly in the field of quantum-safe cryptography methods, producing several intriguing algorithm options that still need to be developed to their full potential. The amount of work needed to modify current security protocols to accommodate these novel algorithms and come to an agreement on them through an open standardization process should not be underestimated.

(Continued)

Table 10 (continued)

Challenges	Highlights
Jamming protection and physical layer security	To provide a secure 6G radio interface without compromising key performance indicators (KPIs), including latency, throughput, and energy efficiency, physical layer security (PLS) approaches should be researched. PLS can offer verified security, in contrast to cryptographic methods that depend on presumptions about the intricacy of particular procedures. It is nevertheless difficult to maintain the theoretical security characteristics in real-world implementations that satisfy the exacting specifications of 6G use cases and protect against highly skilled attackers. There is a trade-off between providing resilience to jamming and optimizing spectral efficiency, defending against jamming presents another key challenge. The scientific community has not yet created a complete solution for malicious jamming, despite the identification of certain promising strategies. Further investigation is required to guarantee a crucial high degree of availability required by critical 6G services.
Distributed Ledger Technologies (DLT)	The limitations of distributed ledger technologie's scalability, energy efficiency, and latency would be a significant barrier to real-world deployments, despite the fact that they provide a helpful framework for expediting the establishment of trust across various operator domains, enhancing use cases for the 6G era, and encouraging cumulative trust building based on verified device behavior. Future work is expected to concentrate on improving the scalability and quantum safety of DLT consensus algorithms while preserving reasonable latency and energy costs.

7 Conclusion

This article examines the potential of integrating AI and blockchain clustering to enhance security in 6G wireless networks. The promise of unprecedented speed, capacity, and connectivity of 6G also brings with it increased security risks and challenges. Traditional security mechanisms are inadequate for coping with the distributed and dynamic nature of 6G networks. Therefore, new and innovative solutions such as AI, blockchains, and mobile virtual devices are required to address vulnerabilities and ensure reliable and secure communication in 6G networks.

While AI offers the ability to detect anomalies, predict attacks, and dynamically adapt security measures, blockchains increase trust and transparency by providing a decentralized and immutable architecture. The synergistic integration of these two technologies can significantly improve security in 6G networks. In our study, we discussed in detail blockchain clustering methods (federations, sidechains, sharding) and various AI techniques (machine learning, deep learning, reinforcement learning) that can be applied to 6G security. We have shown that the integration of these technologies can provide significant benefits such as improved threat detection, secure identity management, reliable data sharing, and distributed, resilient infrastructure. We also addressed the challenges facing AI and blockchain integration. Scalability, privacy, reliability, energy consumption, standardization, and legal/ethical issues are obstacles to the widespread adoption of these technologies in 6G networks. We identified future research directions to overcome these challenges: hybrid

AI and blockchain solutions, quantum-resistant blockchain, AI-based blockchain optimization, mobile virtual compute environments, and open-source platforms.

In conclusion, AI and blockchain clustering offer a promising future for 6G security. The synergistic use of these technologies will play a key role in ensuring security and privacy in future wireless networks. However, to fully realize this potential, continuous collaboration and innovation between researchers, industry, and standards development organizations are required. We hope that this paper will be a valuable resource for researchers, engineers, and policymakers working in the field of 6G security.

Acknowledgement: Not applicable.

Funding Statement: The authors received no specific funding for this study.

Author Contributions: The authors confirm their contribution to the paper as follows: study conception and design: A. F. M. Shahen Shah; data collection: A. F. M. Shahen Shah and Muhammet Ali Karabulut; analysis and interpretation of results: A. F. M. Shahen Shah, Muhammet Ali Karabulut, Abu Kamruzzaman, Dalal Alharthi, and Phillip G. Bradford; draft manuscript preparation: A. F. M. Shahen Shah, Muhammet Ali Karabulut, Abu Kamruzzaman, Dalal Alharthi, and Phillip G. Bradford. All authors reviewed the results and approved the final version of the manuscript.

Availability of Data and Materials: Not applicable.

Ethics Approval: Not applicable.

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

References

1. Shah AFMS, Qasim AN, Karabulut MA, Ilhan H, Islam MB. Survey and performance evaluation of multiple access schemes for next-generation wireless communication systems. IEEE Access. 2021;9:113428–42. doi:10.1109/access.2021.3104509.
2. Shah AFMS. A survey from 1G to 5G including the advent of 6G: architectures, multiple access techniques, and emerging technologies. In: Proceedings of the IEEE 12th Annual Computing and Communication Workshop and Conference; 2022 Jan 26–29; Las Vegas, NV, USA.
3. Nguyen V, Lin P, Cheng B, Hwang R, Lin Y. Security and privacy for 6G: a survey on prospective technologies and challenges. IEEE Commun Surv Tutor. 2021;23(4):2384–428. doi:10.1109/comst.2021.3108618.
4. Zhang Z, Xiao Y, Ma Z, Xiao M, Ding Z, Lei X, et al. 6G wireless networks: vision, requirements, architecture, and key technologies. IEEE Veh Technol Mag. 2019;14(3):28–41. doi:10.1109/mvt.2019.2921208.
5. Wang M, Zhu T, Zhang T, Zhang J, Yu S, Zhou W. Security and privacy in 6G networks: new areas and new challenges. Digit Commun Netw. 2020;6(3):281–91. doi:10.1016/j.dcan.2020.07.003.
6. Giordani M, Polese M, Mezzavilla M, Rangan S, Zorzi M. Toward 6G networks: use cases and technologies. IEEE Commun Mag. 2020;58(3):55–61. doi:10.1109/mcom.001.1900411.
7. Dhar Dwivedi A, Singh R, Kaushik K, Rao Mukkamala R, Alnumay WS. Blockchain and artificial intelligence for 5G-enabled Internet of Things: challenges, opportunities, and solutions. Trans Emerg Tel Tech. 2024;35(4):e4329. doi:10.1002/ett.4329.
8. Ziyi Z, Oluwakayode O, Hao X, Lei Z, Muhammad I. AI and blockchain enabled future wireless networks: a survey and outlook. Distrib Ledger Technol. 2024;3(3):30. doi:10.1145/3644369.
9. Zuo Y, Guo J, Gao N, Zhu Y, Jin S, Li X. A survey of blockchain and artificial intelligence for 6G wireless communications. IEEE Commun Surv Tutor. 2023;25(4):2494–528. doi:10.1109/comst.2023.3315374.
10. Ji B, Wang Y, Song K, Li C, Wen H, Menon VG, et al. A survey of computational intelligence for 6G: key technologies, applications and trends. IEEE Trans Ind Inform. 2021;17(10):7145–54. doi:10.1109/tii.2021.3052531.
11. Pathak V, Pandya RJ, Bhatia V, Lopez OA. Qualitative survey on artificial intelligence integrated blockchain approach for 6G and beyond. IEEE Access. 2023;11:105935–81. doi:10.1109/access.2023.3319083.

12. Velliangiri S, Manoharan R, Ramachandran S, Rajasekar V. Blockchain based privacy preserving framework for emerging 6G wireless communications. IEEE Trans Ind Inf. 2022;18(7):4868–74. doi:10.1109/tii.2021.3107556.
13. Zhang P, Li L, Niu K, Li Y, Lu G, Wang Z. An intelligent wireless transmission toward 6G. Intell Converg Netw. 2021;2(3):244–57. doi:10.23919/icn.2021.0017.
14. Mao B, Tang F, Kawamoto Y, Kato N. AI models for green communications towards 6G. IEEE Commun Surv Tutor. 2022;24(1):210–47. doi:10.1109/comst.2021.3130901.
15. Liu Y, Peng S, Zhang M, Shi S, Fu J. Towards secure and efficient integration of blockchain and 6G networks. PLoS One. 2024;19(4):e0302052. doi:10.1371/journal.pone.0302052.
16. Kamal K, Kumar V, Seema, Sharma MK, Khan AA, Idrisi MJ. A systematic review of blockchain technology assisted with artificial intelligence technology for networks and communication systems. J Comput Netw Commun. 2024;2024(1):979371. doi:10.1155/2024/9979371.
17. Bargavi M, Dadhich A, Sharma A. Exploring the integration of blockchain in 6G networks for improved security and efficiency. In: Proceedings of the 2024 International Conference on Optimization Computing and Wireless Communication (ICOCWC); 2024 Jan 29–30; Debre Tabor, Ethiopia.
18. Alanhdi A, Toka L. A survey on integrating edge computing with AI and blockchain in maritime domain, aerial systems, IoT, and Industry 4.0. IEEE Access. 2024;12:28684–709. doi:10.1109/access.2024.3465274.
19. Rustemi A, Dalipi F, Atanasovski V, Risteski A. Enhancing academic credentials: the synergy of blockchain and artificial intelligence. In: Proceedings of the 2024 7th International Balkan Conference on Communications and Networking (BalkanCom); 2024 Jun 3–6; Ljubljana, Slovenia.
20. Bhat SA, Sofi IB, Chi C. Edge computing and its convergence with blockchain in 5G and beyond: security, challenges, and opportunities. IEEE Access. 2020;8:205340–73. doi:10.1109/access.2020.3037108.
21. Zhang Y, Zhang P, Guizani M, Zhang J, Wang J. Blockchain-based secure communication of internet of things in space-air–ground integrated network. Future Gener Comput Syst. 2024;158:391–9. doi:10.1016/j.future.2024.04.024.
22. Ning W, Zhu Y, Song C, Li H, Zhu L, Xie J, et al. Blockchain-based federated learning: a survey and new perspectives. Appl Sci. 2024;14(20):9459. doi:10.3390/app14209459.
23. Li Y, Li S. A novel 6G scalable blockchain clustering-based computer vision character detection for mobile images. Comput Mater Contin. 2024;78(3):3041–70. doi:10.32604/cmc.2023.045741.
24. Pajooh HH, Demidenko S, Aslam S, Harris M. Blockchain and 6G-enabled IoT. Inventions. 2022;7(4):109. doi:10.3390/inventions7040109.
25. Pal S, Dorri A, Jurdak R. Blockchain for IoT access control: recent trends and future research directions. J Netw Comput Appl. 2022;203:103371. doi:10.1016/j.jnca.2022.103371.
26. Dorri A, Mishra S, Jurdak R. Vericom: a verification and communication architecture for IoT-based blockchain. Ad Hoc Netw. 2022;133:102882. doi:10.1016/j.adhoc.2022.102882.
27. Elli A, Barger A, Bortnikov V, Cachin C, Christidis K, De Caro A, et al. Hyperledger fabric: a distributed operating system for permissioned blockchains. In: Proceedings of the Thirteenth EuroSys Conference; 2018 Apr 23–26; Porto, Portugal.
28. Liquid Network [Online]. [cited 2025 Jan 25]. Available from: https://blockstream.com/liquid/.
29. Stacks foundation. Level 2 Stacks chain on the Bitcoin Blockchain [Online]. [cited 2025 Mar 18]. Available from: https://stacks.org/.
30. Secure A. The zilliqa project: a secure, scalable blockchain platform [Online]. [cited 2025 Jan 25]. Available from: https://docs.zilliqa.com/positionpaper.pdf.
31. Kwon J, Buchman E. Cosmos whitepaper, a network of distributed ledgers [Online]. [cited 2025 Jan 25]. Available from: https://wikibitimg.fx994.com/attach/2020/12/16623142020/WBE16623142020_55300.pdf.
32. Shamsan SAM. Blockchain for secure and decentralized artificial intelligence in cybersecurity: a comprehensive review. Blockchain Res Appl. 2024;5(3):100193. doi:10.1016/j.bcra.2024.100193.
33. Nguyen T, Nguyen H, Gia TN. Exploring the integration of edge computing and blockchain IoT: principles, architectures, security, and applications. J Netw Comput Appl. 2024;226:103884. doi:10.1016/j.jnca.2024.103884.

34. Alhammadi A, Shayea I, El-Saleh AA, Azmi MH, Ismail ZH, Kouhalvandi L, et al. Artificial intelligence in 6G wireless networks: opportunities, applications, and challenges. Int J Intell Syst. 2024;2024:1–27. doi:10.1155/2024/8845070.

35. Patil A, Iyer S, Pandya RJ. A survey of machine learning algorithms for 6G wireless networks. arXiv:2203.08429v1. 2022.

36. Chinnasamy P, Babu GC, Ayyasamy RK, Amutha S, Sinha K, Balaram A. Blockchain 6G-based wireless network security management with optimization using machine learning techniques. Sensors. 2024;24(18):6143. doi:10.3390/s24186143.

37. Sakr HA, Fouda MM, Ashour AF, Abdelhafeez A, El-Afifi MI, Abdellah MR. Machine learning-based detection of DDoS attacks on IoT devices in multi-energy systems. Egypt Inform J. 2024;28:100540. doi:10.1016/j.eij.2024.100540.

38. Alwahedi F, Aldhaheri A, Ferrag MA, Battah A, Tihanyi N. Machine learning techniques for IoT security: current research and future vision with generative AI and large language models. Internet Things Cyber-Phys Syst. 2024;4:167–85. doi:10.1016/j.iotcps.2023.12.003.

39. Uysal DT, Yoo PD, Taha K. Data-driven malware detection for 6G networks: a survey from the perspective of continuous learning and explainability via visualisation. IEEE Open J Veh Technol. 2023;4:61–71. doi:10.1109/ojvt.2022.3219898.

40. Adawadkar AMK, Kulkarni N. Cyber-security and reinforcement learning—a brief survey. Eng Appl Artif Intell. 2022;114:105116. doi:10.1016/j.engappai.2022.105116.

41. Puspitasari AA, An TT, Alsharif MH, Lee BM. Emerging technologies for 6G communication networks: machine learning approaches. Sensors. 2023;23(18):7709. doi:10.3390/s23187709.

42. Abdel Hakeem SA, Hussein HH, Kim H. Security requirements and challenges of 6G technologies and applications. Sensors. 2022;22(5):1969. doi:10.3390/s22051969.

43. Aruna S, Priya SM, Reshmeetha K, Sudhayini ES, Narayanan AA. Blockchain integration with artificial intelligence and Internet of Things technologies. In: Proceedings of the 7th International Conference on Intelligent Computing and Control Systems (ICICCS); 2023 May 17–19; Madurai, India.

44. Chaudjary S, Kakkar R, Gupta R, Tanwar S, Agrawal S, Sharma R. Blockchain and federated learning-based security solutions for telesurgery system: a comprehensive review. Turk J Electr Eng Comput Sci. 2022;30(7):2446–88. doi:10.55730/1300-0632.3950.

45. Ahmed HA, Jasim HM, Gatea AN, Al-Asadi AAA, Al-Asadi HAA. A secure and efficient blockchain enabled federated Q-learning model for vehicular Ad-hoc networks. Sci Rep. 2024;14(1):31235. doi:10.1038/s41598-024-82585-3.

46. Karabulut MA, Shah AS. A study and future challenges in 6G networks: aeronautical network, AI and blockchain. JAST. 2024;17(2):122–38.

47. Liu Z, Jiang M, Zhang S, Zhang J, Liu Y. A smart contract vulnerability detection mechanism based on deep learning and expert rules. IEEE Access. 2023;11:77990–9. doi:10.1109/access.2023.3298048.

48. Al Hwaitat AK, Almaiah MA, Ali A, Al-Otaibi S, Shishakly R, Lutfi A, et al. A new blockchain-based authentication framework for secure IoT networks. Electronics. 2023;12(17):3618. doi:10.3390/electronics12173618.

49. Gao S, Li G, Feng L, Chen Y, Chen Y. A secure data sharing system for 6G networks. IEEE Access. 2023;11:133281–93.

50. Bathula A, Gupta SK, Merugu S, Saba L, Khanna NN, Laird JR, et al. Blockchain, artificial intelligence, and healthcare: the tripod of future—a narrative review. Artif Intell Rev. 2024;57(9):238. doi:10.1007/s10462-024-10873-5.

51. Letaief KB, Shi Y, Lu J, Lu J. Edge artificial intelligence for 6G: vision, enabling technologies, and applications. IEEE J Sel Areas Commun. 2022;40(1):5–36. doi:10.1109/jsac.2021.3126076.

52. Ismail L, Buyya R. Artificial intelligence applications and self-learning 6G networks for smart cities digital ecosystems: taxonomy, challenges, and future directions. Sensors. 2022;22(15):5750. doi:10.3390/s22155750.

53. Kuznetsov O, Sernani P, Romeo L, Frontoni E, Mancini A. On the integration of artificial intelligence and blockchain technology: a perspective about security. IEEE Access. 2024;12:3881–97. doi:10.1109/access.2023.3349019.

54. Martinez D, Magdalena L, Savitri AN. AI and blockchain integration: enhancing security and transparency in financial transactions. Int Trans Artif Intell. 2024;3(1):11–20. doi:10.33050/italic.v3i1.651.
55. Bhumichai D, Smiliotopoulos C, Benton R, Kambourakis G, Damopoulos D. The convergence of artificial intelligence and blockchain: the state of play and the road ahead. Information. 2024;15(5):268. doi:10.3390/info15050268.
56. Chavali BT, Khatri SK, Hossain SA. AI and blockchain integration. In: Proceedings of the 8th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO); 2020 Jun 4–5; Noida, India.
57. Abdelhamid M, Sliman L, Ben Djemaa R, Perboli G. A review on blockchain technology, current challenges, and AI-driven solutions. ACM Comput Surv. 2025;57(3):1–39. doi:10.1145/3700641.
58. Charles V, Emrouznejad A, Gherman T. A critical analysis of the integration of blockchain and artificial intelligence for supply chain. Ann Oper Res. 2023;327(1):7–47. doi:10.1007/s10479-023-05169-w.
59. Zuo Y. Exploring the synergy: AI enhancing blockchain, blockchain empowering AI, and their convergence across IoT applications and beyond. IEEE Internet Things J. 2025;12(6):6171–95. doi:10.1109/jiot.2024.3507746.
60. 6G technologies—security, trust and privacy—Nokia Bell Labs [Internet]. [cited 2025 Jan 25]. Available from: https://www.bell-labs.com/research-innovation/what-is-6g/6g-technologies/security-and-trust.
61. Siriwardhana Y, Porambage P, Liyanage M, Ylianttila M. AI and 6G security: opportunities and challenges. In: Proceedings of the IEEE Joint European Conference on Networks and Communications & 6G Summit (EuCNC/6G Summit); 2021 Jun 8–11; Porto, Portugal.
62. Ara I, Kelley B. Physical layer security for 6G: toward achieving intelligent native security at layer-1. IEEE Access. 2024;12:82800–24. doi:10.1109/access.2024.3413047.
63. Porambage P, Gür G, Moya Osorio DP, Livanage M, Ylianttila M. 6G security challenges and potential solutions. In: 2021 Joint European Conference on Networks and Communications & 6G Summit (EuCNC/6G Summit); 2021; Porto, Portugal. p. 622–7. doi:10.1109/EuCNC/6GSummit51104.2021.9482609.
64. Blika A, Palmos S, Doukas G, Lamprou V, Pelekis S, Kontoulis M, et al. Federated learning for enhanced cybersecurity and trustworthiness in 5G and 6G networks: a comprehensive survey. IEEE Open J Commun Soc. 2024;6:3094–130. doi:10.1109/ojcoms.2024.3449563.
65. Nahar N, Andersson K, Schelén O, Saguna S. A survey on zero trust architecture: applications and challenges of 6G networks. IEEE Access. 2024;12:94753–64. doi:10.1109/access.2024.3425350.
66. Li W, Su Z, Li R, Zhang K, Wang Y. Blockchain-based data security for artificial intelligence applications in 6G networks. IEEE Netw. 2020;34(6):31–7. doi:10.1109/mnet.021.1900629.
67. Porambage P, Gür G, Osorio DPM, Liyanage M, Gurtov A, Ylianttila M. The roadmap to 6G security and privacy. IEEE Open J Commun Soc. 2021;2:1094–122. doi:10.1109/ojcoms.2021.3078081.
68. Wang X, Lyu J, Peter JD, Kim BG. Privacy-preserving AI framework for 6G-enabled consumer electronics. IEEE Trans Consum Electron. 2024;70(1):3940–50. doi:10.1109/tce.2024.3371928.
69. Moya Osorio DP, Ahmad I, Sanchez JDV, Gurtov A, Scholliers J, Kutila M, et al. Towards 6G-enabled Internet of vehicles: security and privacy. IEEE Open J Commun Soc. 2022;3:82–105. doi:10.1109/ojcoms.2022.3143098.
70. 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;16(3):67. doi:10.3390/fi16030067.
71. Saad W, Bennis M, Chen M. A vision of 6G wireless systems: applications trends technologies and open research problems. IEEE Netw. 2020;34(3):134–42. doi:10.1109/mnet.001.1900287.
72. Ziegler V, Schneider P, Viswanathan H, Montag M, Kanugovi S, Rezaki A. Security and trust in the 6G era. IEEE Access. 2021;9:142314–27. doi:10.1109/access.2021.3120143.
73. Shirwaikar RD, Faisal AM, Singh A, Shanbhag DD. A review on privacy and security in 6G networks. In: Proceedings of the International Conference on Forensics, Analytics, Big Data, Security (FABS); 2021 Dec 21–22; Bengaluru, India.

74. Siddiqui ST, Kamal MS, Qidwai KA, Alam MI, Khan H, Alam MZ, et al. Uncovering network vulnerabilities and conducting digital forensics analysis for IoT device security in 6G. In: Proceedings of the IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS); 2023 Dec 17–20; Jaipur, India. doi:10.1109/ANTS59832.2023.10469094.
75. Alqabbani A, Saleem K, Almazyad AS. Digital communication forensics in 6G and beyond networks. Appl Sci. 2023;13(19):10861. doi:10.3390/app131910861.
76. Akinbi AO. Digital forensics challenges and readiness for 6G Internet of Things (IoT) networks. WIREs Forensic Sci. 2023;5(6):e1496. doi:10.1002/wfs2.1496.
77. Nguyen T, Nguyen H, Ijaz A, Sheikhi S, Vasilakos AV, Kostakos P. Large language models in 6G security: challenges and opportunities. arXiv:2403.12239v1. 2024.
78. Jiao L, Shao Y, Sun L, Liu F, Yang S, Ma W, et al. Advanced deep learning models for 6G: overview, opportunities, and challenges. IEEE Access. 2024;12:133245–314.
79. Anwar N, Widodo AM, Sekti BA, Ulum MB, Rahaman M, Ariessanti HD. Comparative analysis of NIJ and NIST methods for microsd investigations: a technopreneur approach. APTISI Trans Technopreneurship. 2024;6(2):169–81. doi:10.34306/att.v6i2.407.
80. Shen LH, Feng KT, Hanzo L. Five facets of 6G: research challenges and opportunities. ACM Comput Surv. 2023;55(11):2023.
81. Alam I, Sharif K, Li F, Latif Z, Karim MM, Biswas S, et al. A survey of network virtualization techniques for Internet of Things using SDN and NFV. ACM Comput Surv. 2021;53(2):2021. doi:10.1145/3379444.
82. Zimmer V, Rothman M, Marisetty S. Beyond BIOS: developing with the unified extensible firmware interface. Berlin/Heidelberg, Germany: Walter de Gruyter GmbH & Co. KG; 2017. 322 p.
83. Tanque M, Bradford PG. Virtual Raspberry Pi-s with blockchain and cybersecurity applications. Adv Comput. 2023;131:201–32. doi:10.1016/bs.adcom.2023.04.005.
84. Bradford PG. Chains that bind us; 2023 Dec 28. 240 p. [cited 2025 Mar 15]. Available from: https://www.amazon.com/Chains-that-bind-Phillip-Bradford/dp/1917007884.
85. Le T. A survey of live virtual machine migration techniques. Comput Sci Rev. 2018;38:100304.
86. Milojičić DS, Douglis F, Paindaveine Y, Wheeler R, Zhou S. Process migration. ACM Comput Surv. 2000;23(3):241–99. doi:10.1145/367701.367728.
87. Andrew J, Isravel DP, Sagayam KM, Bhushan B, Sei Y, Eunice J. Blockchain for healthcare systems: architecture, security challenges, trends and future directions. J Netw Comput Appl. 2023;215:103633. doi:10.1016/j.jnca.2023.103633.
88. Javaid M, Haleem A, Singh RP, Suman R, Khan S. A review of blockchain technology applications for financial services. BenchCouncil Trans Benchmarks Stand Eval. 2022;2(3):100073. doi:10.1016/j.tbench.2022.100073.
89. Feretzakis G, Papaspyridis K, Gkoulalas-Divanis A, Verykios VS. Privacy-preserving techniques in generative AI and large language models: a narrative review. Information. 2024;15(11):697. doi:10.3390/info15110697.
90. Pati S, Kumar S, Varma A, Edwards B, Lu C, Qu L, et al. Privacy preservation for federated learning in health care. Patterns. 2024;5(7):100974. doi:10.1016/j.patter.2024.100974.
91. Catak FO, Kuzlu M, Catak E, Cali U, Unal D. Security concerns on machine learning solutions for 6G networks in mmWave beam prediction. Phys Commun. 2022;52:101626. doi:10.1016/j.phycom.2022.101626.
92. Giannaros A, Karras A, Theodorakopoulos L, Karras C, Kranias P, Schizas N, et al. Autonomous vehicles: sophisticated attacks, safety issues, challenges, open topics, blockchain, and future directions. J Cybersecur Priv. 2023;3(3):493–543. doi:10.3390/jcp3030025.
93. Alhussien N, Aaron Gulliver T. Toward AI-enabled green 6G networks: a resource management perspective. IEEE Access. 2024;12:132972–95. doi:10.1109/access.2024.3460656.
94. Gao P, Adnan M. Overview of emerging electronics technologies for artificial intelligence: a review. Mater Today Electron. 2025;11:100136. doi:10.1016/j.mtelec.2025.100136.
95. Chafiq T, Azmi R, Fadil A, Mohammed O. Investigating the potential of blockchain technology for geospatial data sharing: opportunities, challenges, and solutions. Geomatica. 2024;76(2):100026. doi:10.1016/j.geomat.2024.100026.

96. Farah MB, Ahmed Y, Mahmoud H, Shah SA, Al-Kadri MO, Taramonli S, et al. A survey on blockchain technology in the maritime industry: challenges and future perspectives. Future Gener Comput Syst. 2024;157:618–37. doi:10.1016/j.future.2024.03.046.

97. Huang C, Zhang Z, Mao B, Yao X. An overview of artificial intelligence ethics. IEEE Trans Artif Intell. 2023;4(4):799–819. doi:10.1109/tai.2022.3194503.

98. Abdallah M, Salah M. Artificial intelligence and intellectual properties: legal and ethical considerations. Int J Intell Syst Appl Eng. 2023;12(1):368–76.

99. Venkatesan K, Rahayu SB. Blockchain security enhancement: an approach towards hybrid consensus algorithms and machine learning techniques. Sci Rep. 2024;14(1):1149. doi:10.1038/s41598-024-51578-7.

100. Mishra S. Blockchain and machine learning-based hybrid IDS to protect smart networks and preserve privacy. Electronics. 2023;12(16):3524. doi:10.3390/electronics12163524.

101. Manjula SG, Mulay C, Durai K, Murali G, Ibrahim Syed Masood JA, Vijayarajan V, et al. Quantum blockchain: trends, technologies, and future directions. IET Quantum Commun. 2024;5(4):516–42. doi:10.1049/qtc2.12119.

102. Parida NK, Jatoth C, Reddy VD, Hussain MM, Faizi J. Post-quantum distributed ledger technology: a systematic survey. Sci Rep. 2023;13(1):20729. doi:10.1038/s41598-023-47331-1.

103. Hua W, Chen Y, Qadrdan M, Jiang J, Sun H, Wu J. Applications of blockchain and artificial intelligence technologies for enabling prosumers in smart grids: a review. Renew Sustain Energy Rev. 2022;161:112308. doi:10.1016/j.rser.2022.112308.

104. Zhang Z, Song X, Liu L, Yin J, Wang Y, Lan D. Recent advances in blockchain and artificial intelligence integration: feasibility analysis, research issues, applications, challenges, and future work. Secur Commun Netw. 2021;2021:1–15.

105. Ahammed TB, Patgiri R, Nayak S. A vision on the artificial intelligence for 6G communication. ICT Express. 2023;9(2):197–210. doi:10.1016/j.icte.2022.05.005.

106. Kharche A, Badholia S, Upadhyay RK. Implementation of blockchain technology in integrated IoT networks for constructing scalable ITS systems in India. Blockchain Res Appl. 2024;5(2):100188. doi:10.1016/j.bcra.2024.100188.