Ensuring the Future: Addressing Security and Privacy Hurdles in 6G Networks

Megha Jain* and Ravi Verma

School of Computing Science and Engineering, VIT Bhopal University, Sehore, M.P, India
E-mail: meghajain37@gmail.com; ravi.verma@vitbhopal.ac.in
**Corresponding Author*

Received 12 April 2024; Accepted 14 July 2025

Abstract

This research paper provides a brief overview of the security and privacy challenges found in sixth-generation (6G) networks. With the rise of ultra-fast data speeds, extremely low latency, and holographic communication, 6G networks offer remarkable potential for progress. However, they also introduce fresh vulnerabilities, necessitating strong security measures. The article examines authentication, encryption, data protection, and AI-driven security mechanisms in the context of 6G. Additionally, it discusses emerging privacy issues such as location tracking and user profiling. Through an in-depth analysis of existing literature and current trends, this study aims to illuminate the evolving landscape of security and privacy in 6G networks. Additionally, we analyze existing studies, identify research gaps, and discuss ongoing standardization efforts. We further incorporate real-world case studies and propose a novel classification framework for 6G security threats, contributing to a deeper understanding of security and privacy in future networks. It stresses the importance of proactive steps to safeguard user data and preserve infrastructure integrity in future communication networks.

Keywords: 6G networks, security, privacy, holographic communication, ultra-low latency, AI-driven security, data protection.

Journal of Mobile Multimedia, Vol. 21_5, 811–830.
doi: 10.13052/jmm1550-4646.2151

1 Introduction

6G networks, which advance the innovations of preceding generations like 5G, signify the sixth phase of wireless communication technology. Figure 1 illustrates that these networks are anticipated to revolutionize connection by delivering unprecedented speeds, exceptionally low latency, and vast connectivity potential. Essentially, 6G aims to enable seamless and efficient device-to-device connectivity, hence unlocking numerous applications across various sectors and domains. Ultra-high throughput, facilitating data speeds quantified in terabits per second (Tbps), is a projected characteristic of 6G networks. This will facilitate exceptionally rapid download and data transfer rates. A vital element is exceptionally low latency, which must be reduced to microseconds, facilitating real-time communication and applications like autonomous vehicles and telemedicine. The expansion of IoT applications in domains such as smart cities, healthcare, and industry will be facilitated by 6G networks' capacity to enable extensive Internet of Things (IoT) connectivity, accommodating billions or even trillions of linked devices [1]. The predicted features collectively exemplify the potential of 6G networks to fundamentally revolutionize our interactions, connections, and communications in the digital era.

6G networks are anticipated to introduce other revolutionary features beyond ultra-high speed, minimal latency, and extensive IoT connection. These may encompass enhancements in spectral efficiency, facilitating a more efficient utilization of spectrum resources and accessible frequency bands. Enhanced spectral efficiency facilitates increased data capacity and improved network performance, especially in densely populated urban areas where spectrum congestion poses a significant challenge. Moreover, to address emerging dangers and safeguard private information transmitted across the network, 6G networks may integrate sophisticated security and privacy measures. 6G networks will incorporate advanced technologies such as artificial intelligence, machine learning, and quantum cryptography to implement robust security protocols that prevent cyberattacks and safeguard user privacy [2].

1.1 The Imperative of Addressing Security and Privacy Concerns in 6G Networks

For a number of reasons, it is imperative that security and privacy issues in 6G networks be addressed. First and foremost, maintaining the security and privacy of 6G networks is essential to safeguarding public safety, economic stability, and societal well-being since these networks are anticipated to

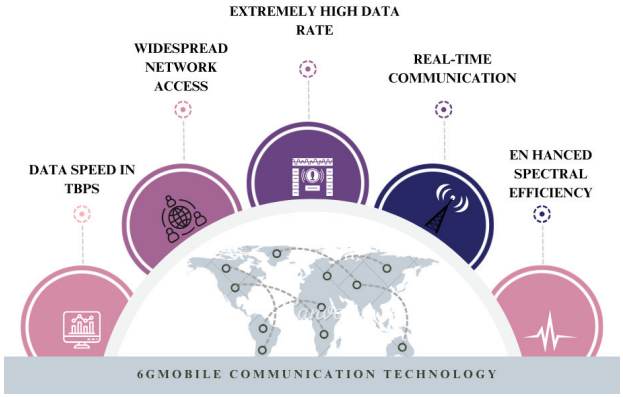

Figure 1 Significant characteristics of mobile communication technology in 6G.

serve as the foundation of vital infrastructure and enable a wide range of applications in industries like healthcare, transportation, and finance. Adversaries may take advantage of new attack vectors and vulnerabilities brought about by the interconnectedness of 6G networks, the extensive use of IoT devices [3], and the integration of data-intensive applications. 6G networks may be exposed to a range of cyberthreats, including data breaches, network intrusions, and service interruptions, in the absence of strong security measures. These threats could have serious repercussions.

Furthermore, safeguarding user privacy becomes crucial as 6G networks manage ever-increasing amounts of sensitive and personal data, such as location data, health records, and biometric information [4]. The potential societal benefits that 6G promises to bring could be undermined if privacy concerns in 6G networks are not sufficiently addressed. This would erode user trust and make people reluctant to adopt new technologies. The need for robust privacy-enhancing measures in 6G networks to ensure compliance with regulations and reduce legal liabilities is further highlighted by the increasingly strict regulatory requirements and legal frameworks governing data protection and privacy around the world.

1.2 Key Contribution

The primary objective of this article is to reveal notable discoveries concerning the security aspects of 6G technology. Key highlights include –

1. The study offers a comprehensive analysis of the prospects and difficulties in 6G security and privacy through an extensive evaluation of current trends and previous literature.

2. A comprehensive analysis investigates the evolution of mobile generations and the security challenges they face.
3. The article examines many security issues related to 6G networks, including data protection, encryption, authentication, and AI-driven security procedures.
4. The paper highlights emerging privacy concerns, like location tracking and user profiling, which require thorough examination and mitigation strategies, alongside security considerations.
5. Real-world case studies demonstrating practical security and privacy threats.
6. A novel classification framework for 6G security challenges.

1.3 Article Organization

The structure of the remaining article is outlined as follows: Section 2 conducts a thorough comparison of recent surveys and roadmaps. Section 3 explores the progression of wireless networks, including a comparative analysis of security and privacy concerns among various generations, alongside the distinctive considerations brought by 6G networks. Section 4 discusses the case studies with scrutiny of security and privacy challenges. Section 5 offers an overview of existing security and privacy mechanisms within 6G networks. Finally, Section 6 concludes the article.

2 Related Work

Numerous academic papers contribute to the discussion surrounding sixth-generation (6G) networks, covering topics such as security, privacy, technological progress, and associated challenges. Primault et al. [5] conducted a survey on assessment metrics for protection mechanisms, emphasizing privacy, utility, and performance, while also addressing computational location privacy issues. Giordani et al. [1] examined the technologies propelling the transition to 6G networks, viewing them as facilitators for various potential applications. Wang et al. [2] The examination delved into four essential components of 6G networks, covering instant intelligent edge computing, decentralized AI, sophisticated radio systems, and three-dimensional communication interfaces. It also addressed pertinent issues surrounding security and privacy. Porambage et al. [6] Gave an overview of 6G security, defining security metrics and outlining a preliminary threat landscape based on the proposed architecture. Siriwardhana et al. [7] focused on AI's role in securing

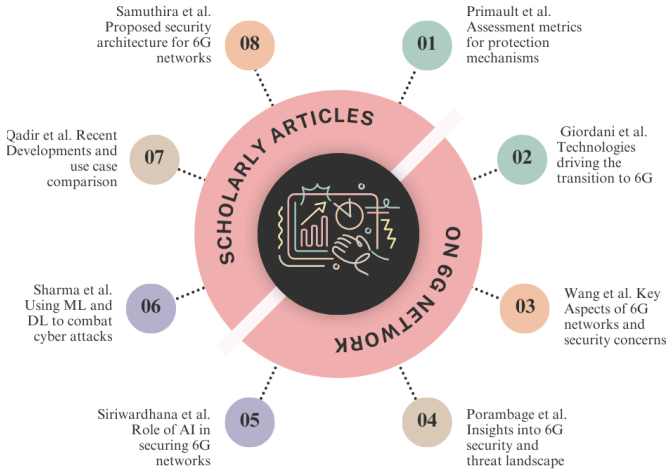

Figure 2 Summary of scholarly articles on 6G networks.

6G networks, presenting its potential applications alongside challenges and potential remedies. Sharma et al. [8] concentrated on combating malware and ransomware attacks, proposing ML and DL models as solutions and comparing their efficacy based on accuracy. Qadir et al. [9] Highlighted were recent advancements and emerging trends in 6G technology, network requirements, enabling technologies, and a comprehensive comparison of use cases between 5G and 6G networks. These pieces collectively provide valuable insights into the diverse landscape of 6G networks and their implications for security, privacy, and technological progress. Lastly, Samuthira et al. [10]Introduced a new security architecture for 6G wireless networks, utilizing secret key authentication and flexible position-based identification analysis, setting the groundwork for exploring identity management and adaptable authentication methods. Figure 2 provides the authors and main focuses of scholarly articles related to 6G networks.

3 Progression of Wireless Communication: From 1G to 6G

3.1 A Brief Look at How Wireless Networks Have Advanced from 1G to 6G

This Section discusses the progression of wireless communication technologies over the generations illustrated in Figure 3, highlighting the key features, advancements, and challenges encountered in each generation.

1. 1G (First Generation): The first generation (1G) of wireless networks marked the inception of mobile communication systems, primarily offering analog voice services. Introduced in the 1980s, 1G networks enabled basic voice calls through analog modulation techniques [11]. However, these networks had limited coverage, poor voice quality, and lacked support for advanced features like text messaging or data services. Despite these limitations, 1G networks laid the foundation for subsequent generations by demonstrating the feasibility of mobile communication on a wide scale, albeit in its early stages.
2. 2G (Second Generation): The transition from analogue to digital technology represented a significant progression in the second generation (2G) of wireless networks. Digital voice encoding (e.g., GSM) and text messaging (SMS) were implemented by 2G networks in the early 1990s, transforming communication capabilities [12]. 2G networks provide superior spectral efficiency, enhanced security measures, and improved voice quality compared to 1G networks. These advancements established the foundation for the mobile revolution by facilitating extensive mobile phone adoption and the introduction of fundamental data services.
3. 3G (Third Generation): The introduction of third generation (3G) wireless networks facilitated mobile internet access and high-speed data services, significantly enhancing mobile communication capabilities. Packet-switched technologies were implemented by 3G networks, which were launched in the early 2000s. This facilitated accelerated data transfer rates and accommodated multimedia applications [11]. 3G enabled users to access services such as video calling, mobile television, and internet surfing on their mobile devices. These advancements facilitated the advent of mobile broadband, transforming mobile phones into multifunctional multimedia devices [2].
4. 4G (Fourth Generation): The transition to fully IP-based networks in the fourth generation (4G) of wireless networks resulted in a paradigm change, delivering unprecedented network efficiency and data rates. The introduction of 4G LTE (Long-Term Evolution) technology in the late 2000s markedly enhanced spectral efficiency, reduced latency, and increased data speeds compared to earlier versions. Users saw accelerated upload and download speeds, seamless HD video streaming, and improved mobile gaming experiences with 4G [6]. Moreover, 4G networks facilitated the widespread adoption of app-based services, hence

propelling the growth of the digital ecosystem and mobile application economy.

5. 5G (Fifth Generation): The fifth iteration (5G) of wireless networks stands as the cutting-edge in mobile communication technology, providing exceptionally high speeds, extremely low latency, and extensive connectivity. Rolled out in the 2020s, 5G networks utilize sophisticated technologies like millimeter-wave spectrum, massive MIMO, and network slicing to deliver unparalleled performance and accommodate various applications [6]. With 5G, users can enjoy immersive AR/VR experiences, real-time gaming, and enhanced IoT connectivity. Additionally, 5G networks promise to revolutionize industries such as healthcare, transportation, and manufacturing with innovative use cases like remote surgery, autonomous vehicles, and smart factories.
6. 6G (Sixth Generation) The forthcoming sixth generation (6G) of wireless networks is poised to expand upon the progress made by 5G and introduce even more revolutionary capabilities. Expected to be rolled out in the 2030s, 6G networks are projected to offer exceptionally high throughput, extremely low latency, and backing for emerging technologies like holographic communication and tactile internet. With 6G, users can anticipate even faster data speeds, seamless real-time communication, and enhanced connectivity for IoT devices [6]. Moreover, 6G networks aim to address challenges such as sustainability, security, and privacy while unlocking new opportunities for innovation and socio-economic development. As research and development efforts continue to advance, 6G networks have the potential to revolutionize how we connect, communicate, and engage in the digital era [7].

3.2 Comparison of Security and Privacy Challenges Across Different Generations of Wireless Technology

The progression of wireless technology from 1G to the forthcoming 6G networks has brought about a changing terrain of security and privacy concerns. In the early stages of mobile communication, 1G and 2G networks faced security vulnerabilities such as limited authentication mechanisms and encryption flaws, leading to concerns like eavesdropping and identity spoofing [12]. As technology progressed to 3G and 4G, encryption key vulnerabilities and data privacy issues became prevalent, with increasing data collection raising concerns about user privacy [2, 6]. With the advent

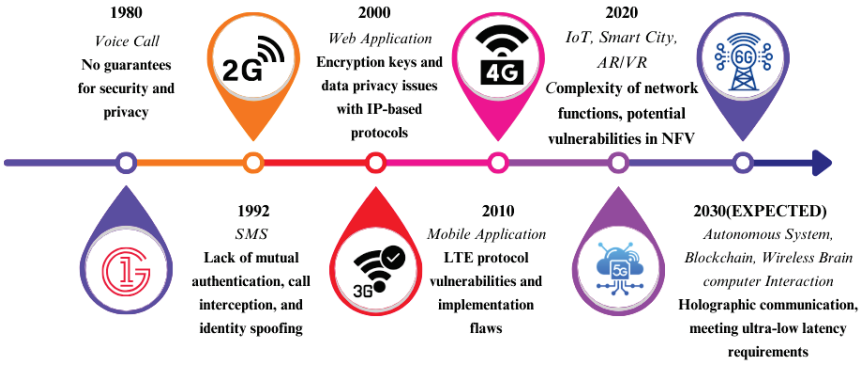

Figure 3 The progression of security and privacy issues in wireless systems.

of 5G, the complexity of network functions and extensive data collection for AI-driven services introduced new security and privacy challenges. Looking ahead to 6G, securing holographic communication, and addressing ultra-low latency requirements will be critical security considerations [13], while enhanced data collection for AI-driven services [14] and the need for privacy-preserving techniques in holographic communication will raise privacy concerns [6, 7]. Table 1 highlights the dynamic nature of security and privacy challenges across generations of wireless technology.

4 The Security and Privacy Obstacles Encountered within 6G Networks

4.1 Security Challenges

Securing 6G networks presents multiple problems that require creative strategies to ensure communication integrity, secrecy, and availability. Among these obstacles is the unparalleled magnitude and complexity of 6G networks, which integrate several technologies, including holographic communications, extensive deployment of the IoT, and AI. This complexity broadens the possible attack surface, complicating the identification and remediation of vulnerabilities. Moreover, the integration of AI into 6G presents new security challenges, including adversarial attacks and the necessity for transparency in AI-facilitated decision-making [14, 15]. Another critical issue is the growing reliance on edge computing and distributed architectures, which introduce potential weak points and susceptibility to attacks [2, 16, 17]. Table 2 Summarizing prospective security problems in 6G communication networks.

Table 1 Services and functions, security & privacy challenges across generations

Generation	Services & Functions	Security & Privacy Challenges
1G	Analog-based telephony	Limited authentication mechanisms, susceptibility to eavesdropping, lack of encryption, vulnerability to unauthorized access.
2G	Digital telephony and text messaging	GSM encryption vulnerabilities, call interception, identity spoofing, lack of mutual authentication, privacy risks in SMS transmission.
3G	Cellular internet and video conferencing	Brute-force attacks on encryption keys, potential for DoS attacks, data privacy concerns with IP-based protocols, unauthorized access to mobile data.
4G	Accelerated data services and broadband mobility	LTE protocol vulnerabilities, implementation flaws, data collection and monetization by service providers, advertisers.
5G	Real-time responsiveness with extensive IoT deployment	Complexity of network functions, potential NFV vulnerabilities, increased data collection for AI-driven services, user consent issues.
6G	3D holographic transmissions, AI-powered applications, and sub-millisecond delay	Challenges in securing holographic communication, ultra-low latency requirements, enhanced data collection for AI-driven services, privacy-preserving holographic communication.

Figure 4 Illustration depicting the security challenges faced within the domain of 6G networks. A solution involves the creation of sophisticated encryption methods and secure key management systems to protect data carried across 6G networks. Establishing comprehensive identity and access management systems can facilitate the authentication and authorization of legitimate people and devices, hence mitigating the risk of unauthorized access. Additionally, utilizing machine learning and artificial intelligence to detect irregularities. Behaviour analysis, as referenced in [25], can augment the ability to swiftly detect and mitigate new hazards. Cooperative initiatives among industry participants, standardization organizations, and regulatory agencies are essential for creating a cohesive and resilient security framework for 6G networks. Regular security audits, constant monitoring, and the exchange of threat intelligence can enhance a proactive security posture, thereby fortifying the resilience of future communication technologies against changing cyber threats [26].

Table 2 Security challenges in 6G networks

Security Challenge	Description
Extensive Device Connectivity and IoT Security [3]	Addressing the challenge of protecting a growing number of IoT devices and maintaining data integrity across interconnected systems.
AI-Based Vulnerabilities [14], [15]	Mitigating threats such as adversarial manipulation that target AI and machine learning components embedded in 6G infrastructure.
Risks in Distributed Edge Environments [18]	Handling security challenges arising from decentralized edge computing frameworks prevalent in 6G deployments.
User Privacy in Data-Driven Networks [16, 17, 19]	Protecting personal information and sensitive user data within networks characterized by pervasive data collection and exchange.
Isolation in Network Slicing [20, 21]	Ensuring the isolation of network slices to prevent inter-slice vulnerabilities and maintain service-specific security.
Post-Quantum Cryptography Readiness [22]	Developing encryption techniques robust against the potential threats posed by quantum computing in future 6G systems.
Trust in AI Decision Processes [23]	Promoting transparent and dependable AI-driven decisions to enhance trust among stakeholders and end-users.
Security in Adaptive Spectrum Allocation [24]	Safeguarding dynamically allocated spectrum from unauthorized access, eavesdropping, and malicious interference.

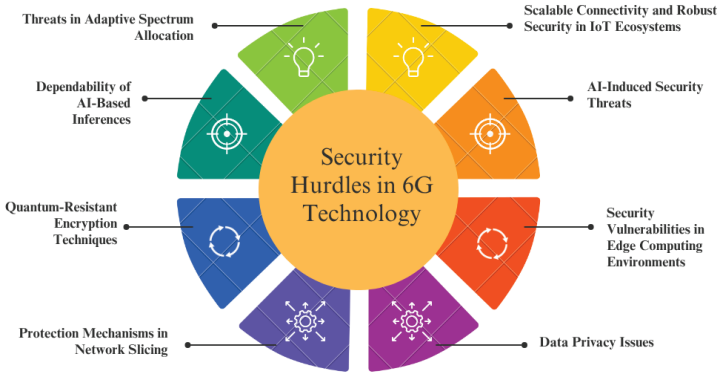

Figure 4 Security hurdles in the realm of 6G communication networks.

4.2 Privacy Challenges

Privacy challenges in 6G networks encompass safeguarding user data amidst extensive IoT proliferation and ensuring compliance with evolving regulations, necessitating robust privacy-preserving measures. Figure 5 represents privacy Challenges in 6G Networks.

1. Data Privacy – Protecting personal information, whether it be physically or electronically, and making sure it isn't accessed, used, or disclosed without the right authorization is known as data privacy. This involves safeguarding private information such as financial records, medical histories, and private correspondence. As worries about identity theft and data breaches grow, strong data privacy measures are crucial [4].
2. Location Privacy – Location privacy safeguards individuals' private location information against exploitation or unlawful access. It involves safeguarding information regarding an individual's previous trips, which may reveal sensitive facts such as political affiliations, financial status, and behavioural tendencies. As Internet of Things (IoT) and Location-Based Services (LBS) technologies grow, safeguarding location privacy becomes increasingly crucial [5].
3. User Profiling and Behaviour Tracking – User profiling and behaviour tracking entail the collection and analysis of data to construct detailed user profiles and monitor their activities within the network. This involves acquiring information about geographical location, communication behaviours, application utilization, and internet browsing tendencies. These methods engender privacy and surveillance apprehensions

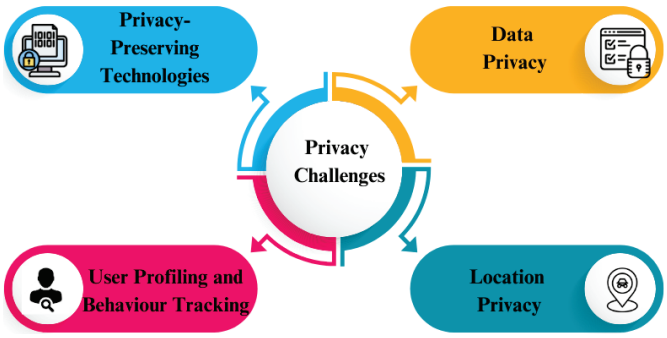

Figure 5 Privacy challenges in 6G networks.

notwithstanding their efficacy in optimising network efficiency and personalizing offerings. Robust privacy safeguards and transparency protocols are essential to ensure the ethical and secure management of user data.

4. Privacy-Preserving Technologies – Privacy-protecting technologies encompass tools and methodologies designed to safeguard individuals' private information while facilitating data collection, analysis, and sharing. Methods that diminish the probability of illegal access or exposure of personal data include encryption, anonymisation, and differential privacy [16]. These technologies are essential for safeguarding privacy across several settings, including communication channels, analytics, and data exchange.

4.3 Case Studies: Real-World 6G Security Challenges

To ground theoretical discussions in practical applications, we analyze real-world security threats:

1. AI-Powered Cyberattacks: Cyberattacks are increasingly sophisticated, as hackers employ AI methodologies to avoid detection. Researchers have inadequately examined AI-driven cyberattacks, resulting in a deficiency in comprehension regarding their complexity. Guembe et al. examines the burgeoning threat of AI-driven cyberattacks and offers insights on the nefarious application of AI in such attacks. Findings indicate that current cyber defence systems will be insufficient to counter AI-driven assaults, prompting organisations to allocate resources towards AI cybersecurity frameworks to mitigate these evolving threats [15]. Oleg et al. examines the creation of a novel entropy-focused methodology termed security- or cybersecurity-informed safety (SIS) for assessing the safety and reliability of autonomous transport systems. This methodology expands and synthesizes the established FMECA and IMECA procedures alongside the novel SISMECA technique [27].
2. Quantum Computing Threats: Quantum computing provides a significant exponential advantage for some situations, particularly in cybersecurity. This research consolidates fundamental works on quantum cybersecurity, outlining proposed methodologies and emphasizing the potential for both threats and solutions. Findings suggest quantum computing can improve cybersecurity threats while posing unexpected threats [28]. Another article examines the potential of quantum computing to augment blockchain technology. It emphasizes risks including accelerated

nonce generation, expedited hash collision searches, and the undermining of classical encryption. Incorporating quantum features can enhance the robustness and efficiency of blockchain technology [29].

3. Privacy Violations in Holographic Communication: Holographic telepresence is a 6G application that renders lifelike 3D renderings of remote individuals and objects, necessitating substantial bandwidth. As the quantity of gadgets escalates, security procedures must not encumber already strained bandwidths. Considerations must include diminished operational expenses and device heterogeneity. The fundamental challenge is the safeguarding of privacy, particularly when holographic pictures are transmitted to distant sites [6].

5 Overview of Existing Security and Privacy Mechanisms in 6G Networks

6G networks are still in the conceptual stage, and several existing security and privacy mechanisms are likely to be incorporated into their design, along with novel approaches to address emerging threats. Table 3 provides an overview of some existing mechanisms and potential improvements for Security and privacy aspects in 6G networks.

5.1 Standardization Efforts in 6G Security

Numerous Standards Developing Organizations (SDOs) pertinent to 6G security are discussed below.

1. ETSI has formed numerous Industry Specification Groups (ISG) to investigate 5G component technologies, such as NFV, AI, and network automation. NFV-SEC generates specifications centered on security, whilst ETSI ISG ENI delineates a Cognitive Network Management framework employing AI methodologies and context-sensitive rules. ETSI ISG SAI formulates technological standards to alleviate hazards linked to AI implementation and assaults on AI systems. These organizations seek to delineate AI dangers, demonstrate uses, identify mitigation strategies, and advocate for data exchange protocols [6].
2. The ITU-T has established the ITU-T Focus Group on Machine Learning for Future Networks to develop technical specifications for machine learning in future networks, including interfaces, network architectures, protocols, algorithms, and data formats, which will impact the security aspects of 6G networks.

Table 3 Security approaches, effectiveness, and limitations in 6g networks

Approach	Effectiveness	Limitation
Encryption and Authentication [4]	Encryption protocols like AES and TLS provide strong protection against eavesdropping and data tampering, while authentication mechanisms ensure that only authorized users and devices access network resources.	Vulnerabilities in key exchange protocols can be exploited by determined attackers, while improperly implemented authentication mechanisms may be susceptible to credential theft or brute-force attacks.
Network Slicing Security [20], [21]	Network slicing enhances security by logically isolating different services and applications, enabling customized security policies and resource allocation for each slice.	Potential misconfigurations or vulnerabilities in slice orchestration platforms and infrastructure.
AI-Powered Threat Detection [14]	AI-driven threat detection systems offer proactive and adaptive security measures by analyzing vast amounts of network data to identify patterns indicative of malicious activity.	AI-driven threat detection systems face challenges such as false positives/negatives, resulting in unnecessary alerts or missed detections, and susceptibility to adversarial attacks.
Technologies for Maintaining Privacy [16]	Privacy-enhancing technologies such as differential privacy and homomorphic encryption facilitate data sharing and analysis while safeguarding sensitive information.	Balancing privacy protection and data utility, potentially leading to trade-offs between privacy and accuracy in data analysis.
Quantum-Safe Cryptography [22]	Quantum-safe cryptography aims to future-proof security by developing algorithms resistant to quantum computing-based attacks.	Due to practical implementation hurdles and the need for careful planning to ensure compatibility with existing systems.

3. 3GPP has included AI/ML into its 5G Core Service Based Architecture, creating the Network Data Analytics Function for user behaviour and network status notifications [6].
4. NIST's Post-Quantum Cryptography Program standardizes quantum-resistant algorithms for digital signatures, public-key encryption, and cryptographic key establishment.

5. The IETF Security Automation and Continuous Monitoring Architecture RFC outlines a cooperative SACM ecosystem with components that share information. An orchestrator automates tasks like as configuration, coordination, and management, while also including repositories for policy, vulnerability definition data, and security information.
6. The 5G PPP has formed a Security Work Group to address security threats and issues related to 5G, focussing on architecture, access control, privacy, trust, security monitoring, and standardization. The group's findings have implications for networks exceeding 5G.
7. The NGMN5G End-to-End Architecture Framework v4.3 (2020) specifies the requirements for network entities and functions related to end-to-end security inside a potential 5G service framework.
8. The IEEE P1915.1 and P1917.1 standards delineate frameworks for the development and functioning of secure Software-Defined Networking and Network Functions Virtualization environments, prioritizing security, reliability, and quantum communications. The Security Standard aims to protect end users, network operators, and service providers, whereas the Reliability Standard focusses on service delivery infrastructure. The SDQC protocol enables the flexible creation of quantum endpoints in communication networks, allowing for adjustable protocol design [6].

5.2 Proposed Classification Framework for 6G Security Threats

To tackle rising security concerns in 6G networks, we offer an innovative classification approach that categorizes potential attacks into five principal areas:

1. Risks of Identity Management and Authentication: Insufficient authentication methods make people susceptible to identity theft and impersonation brought on by deepfakes.
2. Data Privacy and Anonymization: Risks associated with profiling, re-identification attacks, and extensive data collection are discussed in Data Privacy and Anonymisation.
3. Threats from Adversarial Learning and AI: Adversarial perturbations and model manipulation can cause vulnerabilities in AI-driven security models.
4. Network Slicing and Virtualization Risks: Risks associated with network slicing and virtualization include security issues with dynamically

assigned network slices that could result in data breaches and illegal access.

5. Challenges in Post-Quantum Cryptography: the need to create encryption techniques that are resistant to quantum errors in order to protect communications in the future.

This framework ensures strong and flexible security solutions by offering an organised method for detecting and reducing security threats in 6G networks.

6 Conclusion

In summary, this research article offers a brief exploration of the security and privacy challenges arising from the progression of sixth-generation (6G) networks. While 6G networks promise remarkable advancements in data rates, latency, and communication capabilities, they also introduce novel vulnerabilities that demand robust security solutions. Through an exploration of authentication, encryption, data protection, and AI-driven security mechanisms tailored to the 6G context, this article highlights the critical need for proactive security measures. Furthermore, it delves into emerging privacy concerns such as location tracking and user profiling, emphasizing the importance of safeguarding user data and infrastructure integrity in the evolving landscape of communication networks. By synthesizing existing literature and current trends, this research aims to provide valuable insights into the complexities of 6G security and privacy, advocating for a vigilant approach to address these challenges effectively.

References

[1] Marco Giordani, Michele Polese, Marco Mezzavilla, Sundeep Rangan, and Michele Zorzi. Toward 6g networks: Use cases and technologies. *IEEE Communications Magazine*, 58(3):55–61, 2020.

[2] Minghao Wang, Tianqing Zhu, Tao Zhang, Jun Zhang, Shui Yu, and Wanlei Zhou. Security and privacy in 6g networks: New areas and new challenges. *Digital Communications and Networks*, 6(3):281–291, 2020.

[3] Waqas Khalid, M Atif Ur Rehman, Trinh Van Chien, Zeeshan Kaleem, Howon Lee, and Heejung Yu. Reconfigurable intelligent surface for physical layer security in 6g-iot: Designs, issues, and advances. *IEEE Internet of Things Journal*, 2023.

[4] Chamara Sandeepa, Bartlomiej Siniarski, Nicolas Kourtellis, Shen Wang, and Madhusanka Liyanage. A survey on privacy for b5g/6g: New privacy challenges, and research directions. *Journal of Industrial Information Integration*, 30:100405, 2022.

[5] Vincent Primault, Antoine Boutet, Sonia Ben Mokhtar, and Lionel Brunie. The long road to computational location privacy: A survey. *IEEE Communications Surveys & Tutorials*, 21(3):2772–2793, 2018.

[6] Pawani Porambage, Gürkan Gür, Diana Pamela Moya Osorio, Madhusanka Liyanage, Andrei Gurtov, and Mika Ylianttila. The roadmap to 6g security and privacy. *IEEE Open Journal of the Communications Society*, 2:1094–1122, 2021.

[7] Yushan Siriwardhana, Pawani Porambage, Madhusanka Liyanage, and Mika Ylianttila. Ai and 6g security: Opportunities and challenges. In *2021 Joint European Conference on Networks and Communications & 6G Summit (EuCNC/6G Summit)*, pages 616–621. IEEE, 2021.

[8] Ankita Ankita and Shalli Rani. Machine learning and deep learning for malware and ransomware attacks in 6g network. In *2021 fourth international conference on computational intelligence and communication technologies (CCICT)*, pages 39–44. IEEE, 2021.

[9] Zakria Qadir, Khoa N Le, Nasir Saeed, and Hafiz Suliman Munawar. Towards 6g internet of things: Recent advances, use cases, and open challenges. *ICT express*, 9(3):296–312, 2023.

[10] Samuthira Pandi, Anitha Juliette Albert, K Naresh Kumar Thapa, and R Krishnaprasanna. A novel enhanced security architecture for sixth generation (6g) cellular networks using authentication and acknowledgement (aa) approach. *Results in Engineering*, 21:101669, 2024.

[11] Opeoluwa Tosin Eluwole, Nsima Udoh, Mike Ojo, Chibuzo Okoro, and Akintayo Johnson Akinyoade. From 1g to 5g, what next? *IAENG International Journal of Computer Science*, 45(3), 2018.

[12] Bhagyavati, Wayne C Summers, and Anthony DeJoie. Wireless security techniques: an overview. In *Proceedings of the 1st annual conference on Information security curriculum development*, pages 82–87, 2004.

[13] Van-Linh Nguyen, Po-Ching Lin, Bo-Chao Cheng, Ren-Hung Hwang, and Ying-Dar Lin. Security and privacy for 6g: A survey on prospective technologies and challenges. *IEEE Communications Surveys & Tutorials*, 23(4):2384–2428, 2021.

[14] Nektaria Kaloudi and Jingyue Li. The ai-based cyber threat landscape: A survey. *ACM Computing Surveys (CSUR)*, 53(1):1–34, 2020.

[15] Blessing Guembe, Ambrose Azeta, Sanjay Misra, Victor Chukwudi Osamor, Luis Fernandez-Sanz, and Vera Pospelova. The emerging threat of ai-driven cyber attacks: A review. *Applied Artificial Intelligence*, 36(1):2037254, 2022.

[16] Faisal Naeem, Mansoor Ali, Georges Kaddoum, Chongwen Huang, and Chau Yuen. Security and privacy for reconfigurable intelligent surface in 6g: A review of prospective applications and challenges. *IEEE Open Journal of the Communications Society*, 2023.

[17] Diana Pamela Moya Osorio, Ijaz Ahmad, José David Vega Sánchez, Andrei Gurtov, Johan Scholliers, Matti Kutila, and Pawani Porambage. Towards 6g-enabled internet of vehicles: Security and privacy. *IEEE Open Journal of the Communications Society*, 3:82–105, 2022.

[18] Yilong Hui, Nan Cheng, Yuanhao Huang, Rui Chen, Xiao Xiao, Changle Li, and Guoqiang Mao. Personalized vehicular edge computing in 6g. *IEEE Network*, 35(6):278–284, 2021.

[19] Ana Koren and Ramjee Prasad. Iot health data in electronic health records (ehr): Security and privacy issues in era of 6g. *Journal of ICT Standardization*, 10(1):63–84, 2022.

[20] Joberto SB Martins, Tereza C Carvalho, Rodrigo Moreira, Cristiano Both, Adnei Donatti, João H Corrêa, José A Suruagy, Sand L Corrêa, Antonio JG Abelem, Moisés RN Ribeiro, et al. Enhancing network slicing architectures with machine learning, security, sustainability and experimental networks integration. *IEEE Access*, 2023.

[21] Mohammad Asif Habibi, Bin Han, Amina Fellan, Wei Jiang, Adrián Gallego Sánchez, Ignacio Labrador Pavón, Amina Boubendir, and Hans D Schotten. Towards an open, intelligent, and end-to-end architectural framework for network slicing in 6g communication systems. *IEEE Open Journal of the Communications Society*, 2023.

[22] Georgi Gary Rozenman, Neel Kanth Kundu, Ruiqi Liu, Leyi Zhang, Alona Maslennikov, Yuval Reches, and Heung Youl Youm. The quantum internet: A synergy of quantum information technologies and 6g networks. *IET Quantum Communication*, 4(4):147–166, 2023.

[23] Nasir Khan, Sinem Coleri, Asmaa Abdallah, Abdulkadir Celik, and Ahmed M Eltawil. Explainable and robust artificial intelligence for trustworthy resource management in 6g networks. *IEEE Communications Magazine*, 2023.

[24] Gürkan Gür. Expansive networks: Exploiting spectrum sharing for capacity boost and 6g vision. *Journal of Communications and Networks*, 22(6):444–454, 2020.

[25] Mamoon M Saeed, Rashid A Saeed, Maha Abdelhaq, Raed Alsaqour, Mohammad Kamrul Hasan, and Rania A Mokhtar. Anomaly detection in 6g networks using machine learning methods. *Electronics*, 12(15):3300, 2023.

[26] Ferhat Ozgur Catak, Murat Kuzlu, Evren Catak, Umit Cali, and Devrim Unal. Security concerns on machine learning solutions for 6g networks in mmwave beam prediction. *Physical Communication*, 52:101626, 2022.

[27] Oleg Illiashenko, Vyacheslav Kharchenko, Ievgen Babeshko, Herman Fesenko, and Felicita Di Giandomenico. Security-informed safety analysis of autonomous transport systems considering ai-powered cyberattacks and protection. *Entropy*, 25(8):1123, 2023.

[28] Md Jobair Hossain Faruk, Sharaban Tahora, Masrura Tasnim, Hossain Shahriar, and Nazmus Sakib. A review of quantum cybersecurity: threats, risks and opportunities. In *2022 1st International Conference on AI in Cybersecurity (ICAIC)*, pages 1–8. IEEE, 2022.

[29] Wei Cui, Tong Dou, and Shilu Yan. Threats and opportunities: Blockchain meets quantum computation. In *2020 39th Chinese control conference (CCC)*, pages 5822–5824. IEEE, 2020.

Biographies

Megha Jain B.E. in Computer Science and Engineering from TRUBA Group of Institutes (2010), and M.Tech. in Computer Science and Engineering from SATI Vidisha (2012), currently pursuing Ph.D. at VIT Bhopal. With a 10 years of teaching experience, authored over 10 scientific papers on image processing, machine learning, and emerging technologies like 6G and network slicing.

Ravi Verma is a Senior Assistant Professor in the School of Computing Science and Engineering. He earned his Ph.D. in 2016 from Singhania University, Rajasthan. With over 14 years of experience in academia and industry, he has published 35 articles in esteemed international journals on IoT, Big Data, Cyber Security, and Blockchain.