A Survey on 6G Requirements, Implementation Challenges and Potential Use Cases

Innovatus: A Journal on Computing Technology Innovations, Vol. 6, Issue No. 1

Rosemarie E. Reyes [1]
rosemarie.reyes@uap.asia
[1]*Department of Information Science and Technology, University of Asia and the Pacific, Pasig, Philippines*

ISSN (Print:) 2651-6993, ISSN (E) 2980-5031
Pre-print DOI No. 10.5281/zenodo.7889104

FOR PUBLISHERS ONLY:
Manuscript received: April 29, 2023; revised: May 2, 2023; accepted: May 3, 2023

ABSTRACT

The evolution of wireless technology has drastically transformed how we communicate and access information. As we approach the end of the 5G era, attention is already turning to the next generation of wireless technology: 6G. While 6G is still in its early stages of development, experts predict that it will offer even faster speeds, lower latency, and greater capacity than its predecessor. However, implementing 6G poses a number of significant challenges. This paper will explore the critical challenges in 6G implementation and discuss potential solutions, opportunities and use cases that this new generation of technology may provide.

KEYWORDS 5G, 6G, IoT, 6G Technologies, 6G Challenges, 6G Use Cases

1. INTRODUCTION

This section intends to cover the development and transition from fifth-generation mobile network (5G) towards the sixth generation mobile networks (6G).

5G Development and Challenges

The 5G mobile network is the latest, most advanced, and most sophisticated cellular technology. It provides seamless connectivity and mobility in wireless networks [1] and outperforms its predecessors in terms of data transmission speed, capacity, latency, and reliability. As a result, 5G technology has transformed industries such as healthcare, transportation, financial services, telecommunications, and entertainment.

One of the most significant benefits of 5G technology is its capacity to handle a large number of linked devices. This capability is critical for advancing the Internet of Things (IoT), with applications such as autonomous driving, industry 4.0, and metaverse that will generate massive volume of data at the network edge [2]. In addition, the Internet of Things involves the interconnection of multiple devices and systems to increase efficiency and productivity.

Another critical benefit of 5G technology is its lower latency, which enables near-instantaneous data transfer. This functionality is crucial for real-time communication applications such as remote surgery and autonomous vehicles.

However, implementing 5G technology poses a number of challenges. One of the most pressing challenges is the need for a massive infrastructure upgrade, including the installation of new base stations and fiber-optic connections, which can be costly and time-consuming. Additionally, there are concerns about the impact of 5G networks on human health, as some studies have suggested that exposure to high-frequency electromagnetic radiation may cause adverse effects. Lastly, concerns have also been raised about the security and privacy of data carried through 5G networks which can be a potential for increased cyber threats. With more devices connected to the internet, there is a greater risk of cyber-attacks, which could compromise sensitive data and disrupt critical systems.

In order to address these challenges, the next major step in the evolution of 5G towards the 6G mobile networks is called 5G-Advanced, a new term approved by 3GPP in April 2021 as a response to a new era of 5G. Built on the strong 5G foundation, 5GAdvanced will introduce numerous new capabilities to boost the performance and to enable or expand new use cases and verticals to use 5G technology. At the same time, several forward-looking topics as part of 5G-Advanced will also build the bridge towards 6G technology development [3].

Early Development of Technology

The 6th Generation (6G) cellular network standard is advancing, and several institutions have started researching 6th Generation wireless technology. 6G is expected to be implemented by 2030 [4]. There have been many 6G initiatives around the globe, driven by research interest, industry expectations, and strategic government plans [3]. Many countries have participated in the 6G Research. Finland was the first country to launch a 6G program called 6Genesis [5]. In 2018, the University of Oulu in Finland partnered with Aalto University, VTT Technical Research Centre of Finland, and the Joint Center for Future Connectivity (a venture of Oulu and Nokia Bell Labs).

In November 2019, China's Ministry of Science and Technology set up a working group called "China 6G Wireless Technology Task Force" responsible for the national 6G research and development and another working group consisting of government agencies – Ministry of Science and Technology and the International Mobile Telecommunications 2030 (IMT-2030) promotion group to promote the development of 6G technology [3] [5].

In the U.S., the Alliance for Telecommunications Industry Solutions (ATIS) launched Next G Alliance in October 2020 to advance North American leadership in 6G [3] [4] [5].

Japan established the Beyond 5G Promotion Consortium and Beyond 5G New Business Strategy Center in December 2020 to promote beyond 5G/6G development. The Japanese Ministry of Internal Affairs and Communications released its strategic plan [3] [5].

Europe has also launched various 6G initiatives, notably the Hexa-X project launched in January 2021, which aims to shape the European 6G vision and develop key 6G technologies to enable the vision [4] [5].

In June 2021, South Korea established a 6G implementation plan to lay the groundwork for 6G research and development, which aims to push to launch commercial 6G services by around 2028 [3].

In April 2021, Germany announced an investment in 6G research, including a 6G Research Hub and a 6G Platform. In Europe, the 6G Smart Networks and Services Industry Association (6G-IA) has been set up for next-generation networks and services [3] [5]. As an international organization for standardization, the International Telecommunications Union (ITU) released the initial schedule of 6G research in 2020. It is expected that the research on the 6G vision and corresponding technical propositions will likely be completed by 2023. The most recent initiative is the TERA6G project. It is a project funded by the European Union to develop a new generation and State-of-the-Art Terahertz (THz) transceivers employing massive MIMO for beyond5G networks enabling the Fiber-over-the-air Concept [5].

The table 1 shows the summary the 6G research projects initiated globally.

Table 1: 6G Global Research Projects

Reference	Year	Country	6G Project
[5]	2018	Finland	6Genesis.
[3],[5]	2019	China	China 6G Wireless Technology Task Force
[3],[4],[5]	2020	U.S.A.	Next G Alliance
[3],[5]	2020	Japan	Beyond 5G Promotion Consortium and Beyond 5G New Business Strategy Center. Released the 6G Strategic Plan
[4],[5]	2021	EU	Hexa-X
[5]	2021	South Korea	6G research and development to launch 6G services by 2028
[3],[5]	2023	EU	Tera6G

Objective of the Study
In order to aid in future research efforts towards 6G, this study discusses briefly the background on 6G technologies, the KPIs and requirements of 6G, the related study articles, the challenges particularly on the security and privacy issues as well as the potential solutions and the opportunities and use cases. Table 2 refers to the Acronyms used in this paper.

Table 2: Acronyms

Terms	
3GPP	3rd Generation Partnership Program
5G	Fifth Generation
6G	Sixth Generation
AID	Autonomous Intelligent Driving
AI/ML	Artificial Intelligence and Machine Learning
CPS	Cyber Physical System/Continuum
DetNet	Deterministic Networking
EU	European Union
eMBB	Enhanced Mobile Broadband
FL	Federated Learning
IoTs	Internet of Things
IoEV	Internet of Everything
IoBT	Internet of Battlefield Things
ITU	International Telecommunications Union
JCAS	Joint Communication and Sensing
MIMO	Multiple Input and Multiple Output
MBRLLC	Mobile Broadband Reliable Low Latency Communication
MITM	Man in the Middle (Attacks)
ML	Machine Learning
mURLLC	Massive Ultra Reliable and Low Latency Communication
OPC UA	Open Platform Communications Unified Architecture
QoS	Quality of Service
SAAS	Software as a Service
S&C	Sensing and Communication
SYN	Synchronize

THz	Terahertz
TSN	Time Sensitive Networking
UAV	Unmanned Aerial Vehicle
URLLC	Ultra Reliable and Low Latency Communication
XR	Extended Reality

This survey is organized as follows: Remainder of Section I will discuss the related articles, Section II discusses 6G technology development, Section III discusses the proposed technologies in 6G. Section IV highlights the 6G challenges, proposed solutions, and use cases. Lastly, the conclusion of this survey.

Related Study Articles

Various papers present a vision of the 6G mobile networks covering the enabling technologies, potential applications, requirements, challenges, and solutions. In this section, a brief overview of the current survey papers for the period 2021 to 2023 discussing all facets of the 6G networks is presented.

Fatima, et al. [6], analyzed the fundamental issues of network security and privacy in 5G and 6G. The authors created a framework comparing the achievements from 1G to 5G, setting the preparation for the 6G organization's development. They also created a security analysis of 5G and 6G protocols.

Luo, et al. [2], discussed Federated Learning or FL and highlighted that it is expected to be a key enabler for ubiquitous AI in 6G networks. They also discussed the system and statistical heterogeneity challenges in 6G networks. According to Google Research, Federated Learning enables mobile phones to collaboratively learn a shared prediction model while keeping all the training data on device, decoupling the ability to do machine learning from the need to store the data in the cloud. This goes beyond the use of local models that make predictions on mobile devices (like the Mobile Vision API and On-Device Smart Reply) by bringing model training to the device as well. Lastly, the authors also presented the open problems and directions for future research.

The study conducted by Sharma et al. [7] discussed innovative use cases such as adaptive/mobile industrial automation, extended reality (XR), and wearable robotics which are part of a convergence process that is ongoing towards a cyber physical continuum. They stressed the importance of a fully converged end-to-end deterministic communication infrastructure to support the upcoming cyber-physical continuum. They cited four main challenges to be addressed to realize such future systems: Predictability of stochastic communications, end-to-end technology integration of systems such as 5G URLLC, TSN, and Det Net along with Edge computing and OPC UA, end-to-end security provisioning over heterogeneous infrastructures, as well as defining new scalable, vertical interfaces for cyber-physical system (CPS).

Chen, et al. [3], discussed a comprehensive overview of the 3rd Generation Partnership Program (3GPP) 5G-Advanced development, the state-of-the-art technologies in 3GPP and the key evolution directions for future research and standardization. They also covered the main technical challenges in the following areas: transmission systems, access and resource management and mobility management.

Ounza [8] covered a brief review of 5G service types, 5G security threats and vulnerabilities, and the 6G technologies, services, applications, security threats and vulnerabilities, and proposed solutions. He also discussed various 6G applications such UAV Based Mobility, Holographic Telepresence, Extended Reality, Connected Autonomous Vehicles, Smart Grid 2.0, Industry 5.0, Intelligent Health Care, Digital Twin, Distributed Ledger Technology, Haptic communication, Multi-dimensional Reality, Tactile Internet, and Wireless Brain Computer.

Hakeem, et al., [4], provided insights on the critical problems related to the security, privacy, and trust issues of 6G networks. The author also discussed the 6G security architecture, and improvements over the 5G architecture as well as the issues and challenges of the 6G physical layer.

In the study [9], Sandeepa, et al, provided a comprehensive survey on privacy-related aspects of B5G/6G networks, discussing a taxonomy of different privacy perspectives, conceptualizing a set of challenges, providing solutions, and providing an overview of standardization initiatives for privacy preservation. It also provides a roadmap of future directions for new research towards privacy enhanced B5G/6G network.

The studies conducted by Wang, et al. [5], Banafaa, et al. [10], Nguyen, et al. [11], and Shahraki, et al. [12] provided a comprehensive portrayal of 6G vision, technical requirements, and application scenarios, critical appraisal of network architecture and key technologies, challenges, and potential solutions. Of the 4 papers mentioned, only [5] discussed in detail the existing testbed, the advanced 6G verification platforms, lessons learned and future research directions.

Mu, et al. [13], Wild, et al. [14], and Liu, et al. [15], discussed the background, range of key applications and state-of-the-art approaches of Integrated Sensing and Communications (ISAC). It discusses the interplay between sensing and communications (S&C) from a historical point of view, analyzes performance tradeoffs between S&C, discusses signal processing aspects of ISAC, and identifies potential integration between ISAC and other emerging communication technologies. Wild, et al. [14], also presented an analysis of the choice of the waveform that points towards choosing the one that is best suited for communication also for radar sensing. They also discussed several techniques for efficiently integrating the sensing capability into the JCAS or Joint Communication and Sensing.

In various studies by Liu, et al. [16], Akbar, et al. [17], Mitra, et al. [18] and Xue, et al. [19], Machine Learning and Artificial Intelligence solutions are promising for future 6G networks to fulfill diverse Quality of Service (QoS) requirements for various URLLC (Ultra-Reliable and Low-Latency Communications) applications.

Lastly, Porambage, et al. [20], and Nguyen, et al. [21], discussed the threat landscape in future 6G wireless systems, focusing on the security and privacy challenges and prospective technologies for 6G in physical, connection, and service layers, as well as through lessons learned from the failures of existing security architectures and state-of-the-art defenses.

Table 3 illustrates all the discussed papers in this section.

Table 3: A Comparison of 6G Literature

Reference	Year	6G Vision/Key Features	6G Application Scenarios	6G Network Architecture	6G Key Technologies	Test Beds	6G Challenges	6G Potential Security Solutions
Fatima, et al. [6]	2023	✓	✓	✓	✓		✓	✓
Luo, et al. [2]	2023	✓					✓	
Sharma, et al. [7]	2023				✓			
Chen, et al. [3]	2023						✓	
Ounza [8]	2023		✓		✓		✓	✓
Wang, et al. [5]	2023	✓	✓	✓	✓	✓	✓	✓
Hakeem, et al. [4]	2022	✓	✓	✓	✓		✓	✓
Sandeepa, et al. [9]	2022	✓	✓	✓	✓		✓	✓
Liu, et al. [15]	2022	✓						
Banafaa, et al. [10]	2022	✓	✓	✓	✓		✓	✓
Akbar, et al. [17]	2022	✓	✓	✓	✓		✓	✓
Mitra, et al. [18]	2022	✓	✓	✓	✓		✓	✓
Xue, et al. [19]	2022	✓	✓	✓	✓		✓	✓
Porambage, et al. [20]	2021	✓	✓	✓	✓		✓	✓
Nguyen, et al. [11]	2021	✓	✓	✓	✓		✓	✓
Shahraki, et al. [12]	2021	✓	✓	✓	✓		✓	✓
Wild, et al. [14]	2021		✓		✓			
Liu, et al. [16]	2021		✓		✓			

2. 6G KPIS AND REQUIREMENTS

The adoption of 6G technologies around 2030s is expected to be 100 to 1000 times faster than 5G with up to terabit-per-second speeds. The 6G networks are expected to offer enhanced connectivity along with substantially higher data delivery rates for regular tasks. These tasks may include quicker downloads, uploads, and higher resolution streaming. The following key points can be shown as the estimated possible key requirements for 6G networks [10]. Table 4 summarizes the KPIs for 6G.

1. **Peak Data Rate.** One of the use cases for next generation wireless communication is eMBB, which simply implies high data rates. Hence, we can download HD videos in a few seconds. The data rate requirements of users are increasing since the birth of wireless communications. The final target for 6G max in terms of peak data rate is 1 Terabyte per second. Comparing it with the 5G max throughput of 10 Gigabyte per second, it is approximately 50 times of 5G throughput [5] [22].

2. **User Experienced Data Rate.** It is the data rate that can be achieved even in harsh environment. In 6G, it is expected to achieve 1 Gigabyte per second data rate in harsh conditions which is around 100 times higher than 5G [5] [22].

3. **Latency.** Currently, it would be a little bit tricky to achieve 1ms Latency in 5G, but at least it is doable. In 6G, it is targeted to achieve the latency target of 0.1 millisecond (100 us) which is 10 times shorter than 5G. [5] [22].

4. **Spectrum Efficient Network.** The future intelligent wireless network will comprise of intelligent/smart factories, intelligent/smart hospitals, schools, universities, and autonomous robots. This will require a highly spectral efficient network having high computing power. A high-density and high-rate network will require high bandwidth. The scarcity of the bandwidth will increase with the increase of data in the network. For reliable communication, an ultra spectral efficient network would therefore be needed while at the same time satisfying the criteria for QoS of all users in next-generation wireless networks, which will be smart enough to move to a new state with changing environmental conditions. With the increasing number of mobile devices and communication types, the scarcity of the radio wireless spectrum has increased. Therefore, some communication protocols are needed to be designed for spectral efficient communication. So that the bandwidth resource is effectively utilized. The spectral efficiency of 6G networks is supposed to be >3 times that of 5G [5] [22].

5. **Network Energy Efficiency.** The next-generation wireless communication system will consist of massive self-organizing and self-healing robots. All these intelligent robots/devices will require high computation power. Therefore, the need for energy will be increasing with the increase in intelligent robots. Currently, traditional GPUs are not meeting the energy efficiency requirements of next-generation wireless networks communication networks. In such a scenario, an energy-efficient and scalable intelligent network design will be required. The industry has moved towards IoTs, IoEV and IoBTs. We have sensors deployed everywhere. There is a sensor in our door, in our air conditioner, in our car, on the TV, in the refrigerator, in

offices. All these sensors need energy-efficient communication [5] [22].

6. **Mobility.** More mobility robustness is also required in next-generation communication systems. High data rates should be maintained in highly mobile devices. For instance, if we are moving in the airplanes or high-speed bullet trains, the communication should not be disturbed, and data rates should be maintained. The mobility requirements for 6G, as defined by ITU, is >1000Km/hr. [5] [22].

Table 4: The KPIs and requirements of 6G [5], [22]

KPI	Definition	6G Req.	Enhancement (Compared to 5G)
Peak Data Rate	Max achievable data rate under ideal conditions per user/device	1Tbps	100x.
User Experienced Data Rate	The data rate that is available ubiquitously across the coverage area to a mobile user/device	1Gbps	100x
Latency	The time from when the source sends a packet to when the destination receives it.	0.1ms	10x
Delay Jitter	The latency variations in the system.	$1\mu s$	1000x
Spectrum Efficiency	Average data throughput per unit of spectrum resources and per cell	100 bps/Hz	>3x
Network Energy Efficiency	The quantity of information bits transmitted to/received from users, per unit of energy consumption	10^9 bit/J	>10x relative to 5G
Mobility	Maximum speed at which a defined quality of service (QoS) and seamless	1000 km/h	2x

	transfer between radio nodes can be achieved.

3. 6G Services

The table below shows the new 6G service classes for the 6G network which are expected to refine the current 5G core service classes such as URLLC, eMBB, and mMTC [12]. Refer to Table 5 for the summary of the 6G services.

1. **Massive URLLC.** Massive URLLC refers to communications with high reliability, low latency, and high availability for mission-critical scenarios, such as IoT and remote surgery. URLLC for many devices will be an essential scenario for future communication systems and networks with applications such as Autonomous Intelligent Driving where several important considerations such as considerations must be considered simultaneously, such as motion planning, automated driving, automatic vehicle monitoring, obstacle detection, emergency rescue operations, and so on [12].

2. **MBRLLC.** Mobile broadband reliable and low latency communication (MBRLLC), for scenarios with high data rate, large bandwidth, low latency, and high reliability. Examples include wireless data centers and wireless brain machine interfaces [5].

3. **Human-Centric Services.** Since the inception of 5G, the terrestrial mobile communication system has achieved higher coverage, larger bandwidth, faster speed, lower delay, and denser network. However, when an area suffers from largescale natural disasters, such as earthquakes, floods, mudslides, or other severe accidents caused by humans, the terrestrial communication network in the area may be completely paralyzed. People who need help cannot send out distress signals in time, and the external rescue task will also be hindered. Besides, there is not enough communication network coverage in several scenarios, such as oceans and deserts. In the event of accidents and emergencies, the golden 72 hours will be the key to saving people’s lives. With the further realization of 3D full space coverage in 6G, UAV unmanned aerial vehicles and satellite communication networks will respond quickly and be deployed on demand, providing emergency communications to help quick search and rescue. Taking the golden rescue time into account, it is required to quickly provide a large-bandwidth network deployment with sufficient coverage area [5].

Table 5: 6G Services [12]

Service Type	Performance Indicator.
Massive URLLC	• Ultra-high reliability • Massive connectivity • Massive reliability • Scalable URLLC

MBRLLC - Mobile Broadband Reliable Low Latency Communication	• Stringent ratereliability-latency requirements • Energy efficiency • Rate-reliabilitylatency in mobile environment
Human-Centric Services	• Capturing wireless metrics as well as human and physical factors

4. 6G SECURITY THREATS, VULNERABILITIES AND SOLUTIONS

Given the foregoing technological, architectural, and application-specific features of future 6G networks, they may face a wide range of security issues as threat landscapes. Advancements in technologies may also lead to more powerful attackers [20].

1. **Parameter attacks.** Parameter Tampering attack is based on the manipulation of parameters exchanged between client and server in order to modify application data, such as user credentials and permissions, price and quantity of products, etc. Usually, this information is stored in cookies, hidden form fields, or URL Query Strings, and is used to increase application functionality and control. It involves manipulation of network topology data to insert fake links and malicious codes. This can result to data injection, data manipulation and logic corruption. Continuous injection of false parameters may lead DoS attack to make the data services unresponsive. [20]

Solutions to Parameter attacks [20]:

- Input validation and user authentication
- Access control and rate limiting
- Clearly define the data type
- Control parameter passing
- Control parameters with incorrect format.
- Rigorous application testing

2. **Identity attacks.** this happens when a valid user's credentials have been compromised and an adversary is masquerading as that user, it is often very difficult to differentiate between the user's typical behavior and that of the hacker using traditional security measures and tools. Hackers may exploit the flaws in authentication and authorization. Sometimes, they may extract API keys and use them as credentials [20].

Solutions to Identity attacks [20]:

- Authentication using signed JSON Web Tokens, Open ID Connect
- Authorization (Role based access control, Attribute based access control, Access control lists)

3. **Man in the middle attack.** A man in the middle (MITM) attack is a general term for when a perpetrator positions himself in a conversation between a user and an application—either to eavesdrop or to impersonate one of the parties, making it appear as if a normal exchange of information is underway. Information obtained during an attack could be used for many purposes, including identity theft, unapproved fund transfers or an illicit password change. The goal of an attack is to steal personal information, such as login credentials, account details and credit card numbers. Targets are typically the users of financial applications, SaaS businesses, e-commerce sites and other websites where logging in is required. Attackers may obtain information from an unencrypted transmission of API messages between the API consumer and the provider. Once the API messages are intercepted, messages and confidential information may be revealed. [20]

Solutions to Man in the Middle attacks [20]:

- Use secure encrypted communication
- Use of Virtual Private Networks (VPNs)

4. **Denial of Service (DoS) / Distributed Denial of Service attacks (DDoS) attacks.** This is an attack meant to shut down a machine or network, making it inaccessible to its intended users. DoS attacks accomplish this by flooding the target with traffic or sending it information that triggers a crash. In both instances, the DoS attack deprives legitimate users (i.e., employees, members, or account holders) of the service or resource they expected [20].

There are two general methods of DoS attacks: flooding services or crashing services. Flood attacks occur when the system receives too much traffic for the server to buffer, causing them to slow down and eventually stop. Popular flood attacks include [20]:

- **Buffer overflow attacks. the most common DoS attack.** The concept is to send more traffic to a network address than the programmers have built the system to handle. It includes the attacks listed below, in addition to others that are designed to exploit bugs specific to certain applications or networks [20].
- **ICMP (Internet Control Message Protocol) flood.** leverages misconfigured network devices by sending spoofed packets that ping every computer on the targeted network, instead of just one specific machine. The network is then triggered to amplify the traffic. This attack is also known as the smurf attack or ping of death [20].
- **SYN (Synchronize) flood.** sends a request to connect to a server, but never completes the handshake. Continues until all open ports are saturated with requests and none are available for legitimate users to connect to [20].

The Distributed Denial of Service (DDoS) attack is an additional type of DoS attack. A DDoS attack occurs when multiple systems orchestrate a synchronized DoS attack on a single target. The essential difference is that instead of being attacked from one location, the target is attacked from many locations at once [20].

Solutions to DoS and DDoS attacks [20]:

- Throttling/rate limiting the usage of APIs
- Deployment of API gateways and micro gateways
- AI-based API security for proactive monitoring

4. CONCLUSION

This paper discussed the summary of 6G technologies, the KPIs and requirements of 6G, the security threats, vulnerabilities, and the potential solutions. Furthermore, the latest research activities on the 6G technology have been presented. With the complexity and massive size of the 6G ecosystem, more research should be directed into its specific areas, particularly on addressing security threats, and vulnerabilities, to identify potential solutions. Because 6G network specifications have yet to be defined, the limited literature supports insightful discussions. In the future, I intend to perform a more thorough investigation of the security and privacy implications of 6G and comparable technologies.

REFERENCES

[1] Lundberg. John "Evolution of Wireless Communication Technologies", 2020 May, page 1.

[2] Luo, et al. "Optimization Design for Federated Learning in Heterogeneous 6G Networks", 2023

[3] Chen, et al. "5G-Advanced Towards 6G: Past, Present and Future", 2023 March 13, page 1.

[4] Hakeem, et al. "Security Requirements and Challenges of 6G Technologies and Applications. Sensors Basel, 2022 March 2, page 1.

[5] Wang, et.al. “On the Road to 6G: Visions, Requirements, Key Technologies and Test Beds. IEEE Communications, Surveys and Tutorials, 2023, page 4.

[6] Fatima, et al. “Network Privacy and Security Issues in 5G and 6G, 2023, page 2.

[7] Sharma, et.al. “Towards Deterministic Communications in 6G Networks: State of the Art, Open Challenges and Way Forward” 2023

[8] Ounza, “A taxonomical survey of 5G and 6G security and privacy issues” 2023

[9] Sandeepa, et al. “A Survey on Privacy for B5G/6G: New Privacy Challenges, and Research Directions”, 2022, page 7.

[10] Banafaa, et al, “6G Mobile Communication Technology: Requirements, Targets, Applications, Challenges, Advantages and Opportunities”, 2022

[11] Nguyen, et al., “Security and Privacy for 6G: A Survey on Prospective Technologies and Challenges”, 2021

[12] Shahraki, et al. “A Comprehensive Survey on 6G Networks: Applications, Core Services, Enabling Technologies, and Future Challenges”, 2021

[13] Mu, et al. “NOMA for Integrating Sensing and Communications towards 6G: A Multiple Access Perspective” 2022

[14] Wild, et al., “Joint Design of Communication and Sensing for Beyond 5G and 6G Systems” 2021

[15] Liu, et al., “Integrated Sensing and Communications: Towards Dual-functional Wireless Networks for 6G and Beyond”, 2021

[16] Liu, et al., “Machine Learning for 6G Enhanced UltraReliable and Low-Latency Services” 2022

[17] Akbar, et al., “6G Survey on Challenges, Requirements, Applications, Key Enabling Technologies, Use Cases, AI integration issues and Security aspects”, 2022

[18] Mitra, et al., “Towards 6G Communications: Architecture, Challenges, and Future Directions”, 2022

[19] Xue, et al., “Exploration and Application of AI in 6G Field”, 2022

[20] Porambage, et al. “6G Security Challenges and Potential Solution”, 2021

[21] Nguyen, et al. “Security and Privacy for 6G: A Survey on Prospective Technologies and Challenges”, 2021

[22] Akhtar, et al. “The Shift to Communications: Vision and Requirements”, 2020