JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

# Network Security and Data Privacy in 6G Environment: Impacts and Challenges

**Swathi Prathigadapa, Assistant Professor in CSE**
Geethanjali College of Engineering and Technology, Hyderabad-501301, Telangana, India
**Dr. Sree Rama Chandra Murthy Dasika**
Professor in CSE (Retd.), Hyderabad, India
**Dr. Vijayalakshmi Kakulapati**
Professor and Associate Dean (R & D), Department of Information Technology
Sreenidhi Institute of Science and Technology, Hyderabad – 501301, India

**Dr. Shailaja Saligrama**
University of the Cumberlands, Kentucky, USA

*Abstract*

**1G, the first generation of wireless cellular technology was born and by 1984. In Path to 5G, 1G facilitated the introduction of the mobile phone to consumers. 2G was created on a digital cellular network standard. 3G standards were required to provide peak data rates of at least 144 Kbps with a maximum of 14 Mbps. 4G offered faster web access and added cloud, gaming, High Definition (HD) videos, and 3D TV to the growing list of amenities devices that it could handle. The 5G technology standard for broadband cellular networks to provide connectivity for cell phones began deploying worldwide in 2019. 6G (Sixth Generation Wireless) the successor to 5G cellular technology, will be able to use higher frequencies than 5G networks and provide substantially higher capacity and much lower latency. One of the goals of the 6G internet is to support one microsecond latency communications. Examples of 6G include e-health for all, precision health care, smart agriculture, earth monitor, digital twins, cobots and robot navigation. 6G networks will operate by using signals at the higher end of the radio spectrum. Primarily, 6G will operate by Making use of free spectrum, Improving the efficiency of the free spectrum, taking advantage of mesh networking, Integrating with the "new IP. Network Security is the security designed to protect the integrity of the network from unauthorized access and threats. Network Security is one of the most important aspects to consider when working over the internet, no matter how small or big your business is. The network Security consists of Protection, Detection, and Reaction. Data Privacy generally means the ability of a person to determine for themselves when, how, and to what extent personal information about them is shared with or communicated to others. Impacts in 6G include Advancing Extended Reality, Artificial Intelligence, Machine Learning, Digital Twinning, and more, 6G Shows Potential to Optimize Communications, Interoperability, and Sustainability. The development of the 6 G network faces many challenges: the technological issues include terahertz waves, peak throughput, higher energy efficiency, connection flexibility, and self-aggregating communications fabric; the non-technical challenges include industry barriers, spectrum allocation and usage rules, and policies and regulations. Security Issues in 6G are Virtualization Security Solution, Automated Management System, Data security using AI, Users' Privacy-preserving, Post-Quantum Cryptography. Impacts and Challenges of Network Security and Data Privacy in 6G Environment include real-time intelligent edge, distributed AI, intelligent radio, and 3D intercoms. The main security and privacy concerns here**

relate to authentication, access control, data transmission and encryption.

*Keywords*: 1G-5G, 6G, Network Security, Data Privacy, Impacts, Challenges, Applications, Special Issues.

*Introduction*

*G*

"G" refers to "Generation" [1]. 1G was introduced in 1979 in Tokyo. This first generation of wireless cellular technology was born and by 1984, the entire country of Japan had 1G. 1G was approved in the United States in 1983 with Canada and the United Kingdom following a few years later.

*Path to 5G*

1G facilitated the introduction of the mobile phone to consumers. However, because of the exorbitant cost, it was mostly used by business executives and seen as a status symbol. It was time to make the product and service affordable for greater consumption and address cellular technology inefficiencies. With 1G analog mobile communications standards:

- Coverage was poor.
- Sound quality was subpar.
- There was no compatibility between systems or providers.
- Because an analog wave comes through exactly as it is created, calls between people could be overheard via radio scanners, making for a lack of privacy.
- Maximum speed was 2.4 Kbps.

2G was created on a digital cellular network standard. Because digital converts analog to numbers, 2G offered encrypted calling with better sound quality, text messaging, and picture or multimedia file messages. Enabling these alternative communication types was possible because 2G offered a theoretical maximum transfer speed of 40 Kbps. 2G saw larger-scale construction of cell towers and considerable buy-in from the public as phones and service plans became more affordable.

Demand for better accessibility drove the creation of 3G in 2001. It brought global interoperability. Now, users could access data anywhere in the world via greater web connectivity. It's faster speed added new communications options like video conferencing, streaming, and voice over IP (VoIP). 3G standards were required to provide peak data rates of at least 144 Kbps with a maximum of 14 Mbps.

Now that human-to-human communication was settled, it was time to tackle the need to handle large quantities of data. Reduced latency, the amount of time that information takes to travel from its source to its destination, and then come back to its source, is a major benefit of 4G.

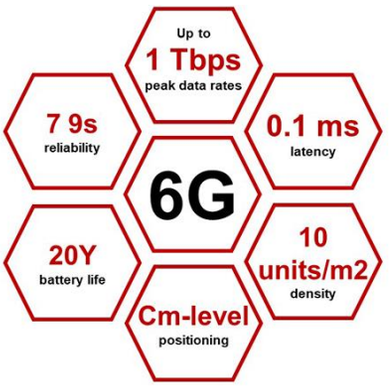
4G offered faster web access and added cloud, gaming, High Definition (HD) videos, and 3D TV to the growing list of amenities devices that it could handle. 4G standards set minimum requirements at 10 Mbps and peak speed at 100 Mbps. However, the quicker data exchange and new features made it necessary to purchase 4G-enabled devices.

Even 4G was not going to be fast enough to advance technology and accommodate the potential of the Internet of Things (IoT) to control thermostats, connected vehicles, smart cities, and more or enable healthcare possibilities with wearables, telehealth, image transfer, and more.

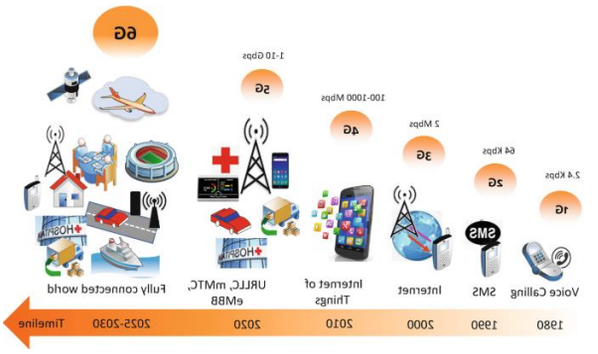
The 5G technology standard for broadband cellular networks to provide connectivity for cell phones began deploying worldwide in 2019. 5G technology increased bandwidth, the capacity on the radio spectrum, to connect more devices in an area and boasts eventual download speeds of 10 Gbps. 5G can operate in 3 frequencies, including

low-band (600-900 MHz with download speeds of 30-250 Mbps), mid-band (1.7-4.7 GHz with download speeds of 100-900 Mbps), or, the new addition, high-band millimetre wave (mmW) (24-47 GHz with download speeds of Gbps).

*6G (Sixth Generation Wireless)*




In telecommunications, 6G is the designation for a future technical standard of a sixth-generation technology for wireless communications [2]. It is the planned successor to 5G, and is in development by numerous companies like Airtel, Anritsu, Apple, Ericsson, Fly, Huawei, Jio, Keysight, LG, Nokia, NTT Docomo, Samsung, Vi, Xiaomi; research institutes like Technology Innovation Institute and the Interuniversity Microelectronics Centre and countries like United States, European Union, Russia, China, India, Japan, South Korea, Singapore and United Arab Emirates that have shown interest in 6G networks. 6G networks will likely be significantly faster than previous generations, and are expected to be more divers, and are likely to support applications beyond current mobile use scenarios, such as ubiquitous instant communications, pervasive intelligence and the Internet of Things (IoT). It is expected that mobile network operators will adopt flexible decentralized business models for 6G, with local spectrum licensing, spectrum sharing, infrastructure sharing, and intelligent automated management underpinned by mobile edge computing, Artificial Intelligence (AI), short-packet communication and blockchain technologies. 6G networks are expected to be developed and released by late 2020s.



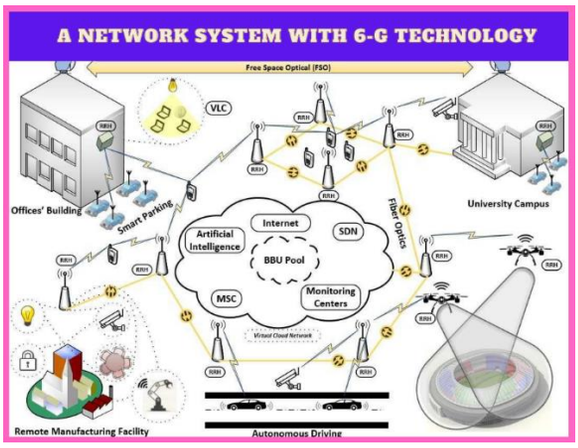

**Analog**

- **0G** Mobile Radio Telephone
- **1G**
- **1.5G** Digital Amps

**Digital**

- **2G**
- **2.5G** General Packet Radio Service
- **2.75G** Enhanced Data Rates for GSM Evolution
- **2.9G** CDMA2000 1X
- **3G**
- **3.5G** High Speed Packet Access
- **3.75G** Evolved High Speed Packet Access
- **3.9G/3.95G** LTE Telecommunication
- **4G** IMT Advanced
- **4.5G** LTE Advanced
- **4.9G** LTE Advanced Pro
- **5G**
- **5.25G** Ultra-wideband
- **5.5G** 5G Advanced
- **6G**

*6G*

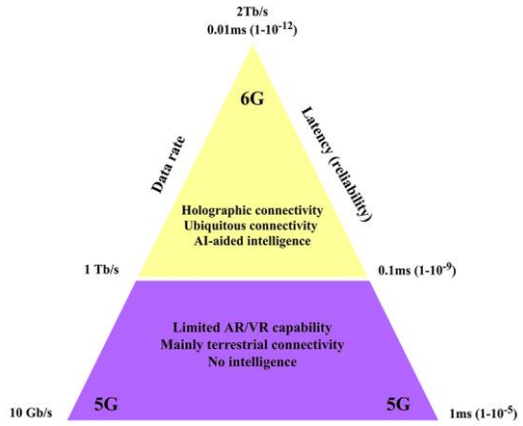



6G is the successor to 5G cellular technology [3]. 6G networks will be able to use higher frequencies than 5G networks and provide substantially higher capacity and much lower latency. One of the goals of the 6G internet is to support one microsecond latency communications. The 6G technology market is expected to facilitate large improvements in the areas of imaging, presence technology and location awareness. Working in conjunction with AI, the 6G computational infrastructure will be able to identify the best place for computing to occur; this includes decisions about data storage, processing and sharing. It is important to note that 6G is not yet a functioning technology. While some vendors are investing in the next-generation wireless standard, industry specifications for 6G-enabled network products remain years away.

*Examples of 6G*

Examples of 6G include e-health for all, precision health care, smart agriculture, earth monitor, digital twins, cobots and robot navigation.

*Advantages of 6G over 5G*




6G networks will operate by using signals at the higher end of the radio spectrum [4]. That estimate applies to data transmitted in short bursts across limited distances.

| Characteristic | 5G | 6G |
|---|---|---|
| Operating frequency | 3 - 300 GHz | upto 1 THz |
| Uplink data rate | 10 Gbps | 1 Tbps |
| Downlink data rate | 20 Gbps | 1 Tbps |
| Spectral efficiency | 10 bps/Hz/m2 | 1000 bps/Hz/m2 |
| Reliability | 10−5 | 10−9 |
| Maximum mobility | 500 km/h | 1000 km/hr |
| U-plane latency | 0.5 msec | 0.1 msec |
| C-plane latency | 10 msec | 1 msec |
| Processing delay | 100 ns | 10 ns |
| Traffic capacity | 10 Mbps/m2 | 1 - 10 Gbps/m2 |
| Localization precision | 10 cm on 2D | 1 cm on 3D |
| Uniform user experience | 50 Mbps 2D | 10 Gbps 3D |
| Time buffer | not real-time | real-time |
| Centre of gravity | user | service |
| Satellite integration | No | Fully |
| AI integration | Partially | Fully |
| XR integration | Partially | Fully |
| Haptic communication integration | Partially | Fully |
| Automation integration | Partially | Fully |

*Table1: Comparison Between 5G and 6G*

Table 1 compares the main specifications and technologies in both 5G and 6G. 6G will be able to connect everything, integrate different technologies and applications, support holographic, haptic, space and underwater communications and it will also support the Internet of everything, Internet of Nano-Things and Internet of Bodies.

*Key Features for Future 6G*

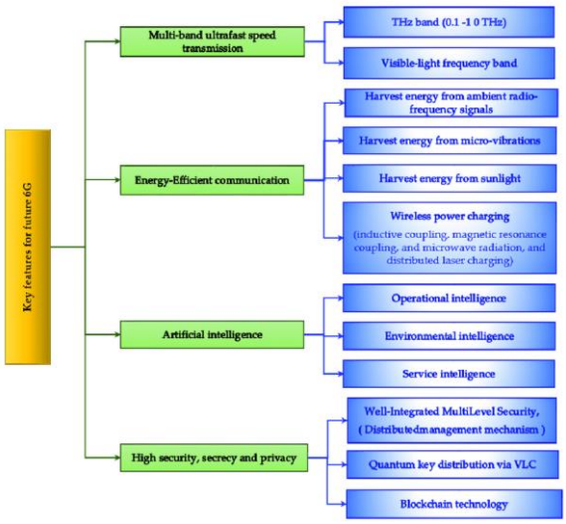



**Fig 1. Key features for future 6G**

**Fig. 1 summarizes the key features for future 6G [5]. the THz wireless communications system, AI, and programmable intelligent surfaces are the outstanding concepts among all the blocks listed in Fig. 1. These innovations welcome a radical departure from the traditional design principles and implementation norms practiced in mobile wireless telecommunication industries.**

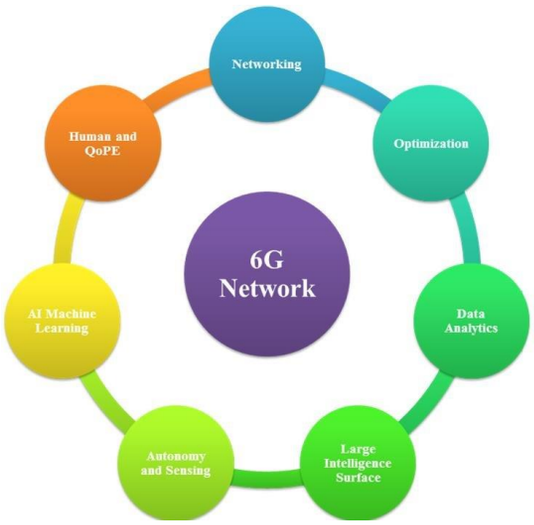
***6G Network***

**6G network is defined as a cellular network that operates in untapped radio frequencies and uses cognitive technologies like AI to enable high-speed, low-latency communication at a pace multiple times faster than fifth-generation networks [6]. 6G is the sixth-generation mobile system standard currently being developed for wireless communications over cellular data networks in telecommunications. It is the successor, or the next bend in the road, after 5G and will likely be much faster. The International Telecommunication Union (ITU) standardizes wireless generations every decade. Typically, they are denoted by a gap in the "air interface," which signifies a shift in transmissions or coding. This is implemented so that older devices cannot be updated to the newer generation since doing so would generate a limitless quantity of "noise" and "spectrum pollution". 6G network enables high-speed, low-latency communication at a pace multiple times faster than fifth-generation networks. Primarily, 6G will operate by:**

- **Making use of free spectrum: A significant portion of 6G research focuses on transmitting data at ultra-high frequencies. Theoretically, 5G can support frequencies up to 100GHz, even though no frequency over 39GHz is currently utilized. For 6G, engineers are attempting to transfer data across waves in the hundreds of Giga Hertz (GHz) or Tera Hertz (THz) ranges. These waves are minuscule and fragile, yet there remains a massive quantity of unused spectrum that could allow for astonishing data transfer speeds.**
- **Improving the efficiency of the free spectrum: Current wireless technologies permit transmission or reception on a specific frequency at the same time. For two-way communication, users may divide their streams as per Frequency Division Duplex (FDD) or by defining Time Division Duplex (TDD). 6G might boost the efficiency of current spectrum delivery using sophisticated mathematics to transmit and receive on the same frequency simultaneously.**
- **Taking advantage of mesh networking: Mesh networking has been a popular subject for decades, but 5G networks are still primarily based on a hub-and-spoke architecture. Therefore, end-user devices (phones) link to anchor nodes (cell towers), which connect to a backbone. 6G might use machines as amplifiers for one another's data, allowing each device to expand coverage in addition to using it.**
- **Integrating with the "new IP:" A research paper from the Finnish 6G Flagship initiative at the University of Oulu suggests that 6G may use a new variant of the Internet Protocol (IP). It**

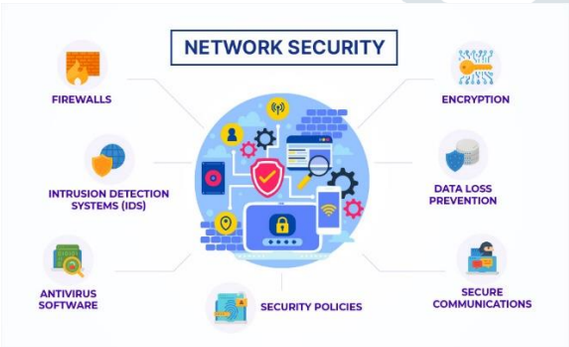
**compares a current IP packet in IPv4 or IPv6 to regular snail mail, complete with a labelled envelope and text pages. The "new IP" packet would be comparable to a fast-tracked courier package with navigation and priority information conveyed by a courier service.**

*Applications of 6G Network*




- **6G is expected to fuel innovative applications such as Holographic-Type Communications (HTC), Tactile Internet, Connected Autonomous Vehicles (CAVs), Unmanned Aerial Vehicles (UAVs), Autonomous Healthcare Solutions and Manufacturing Systems, Virtual Reality (VR) / Augmented Reality (AR)/ Extended Reality (XR), and more.**

*Network Security*




**Network Security [6] is the security designed to protect the integrity of the network from unauthorized access and threats. The network administrators are responsible for adopting various defensive measures to guard their networks from possible security risks. Computer networks are linked in daily transactions and communication within the government, private, or corporates that needs security. The most common and straightforward strategy of protecting network support is allocating it with a unique name and a corresponding password. Network security is one of the most important aspects to consider when working over the internet, Local Area Networks (LAN) or other method, no matter how small or big your business is. While there is no network that is immune to attacks, a stable and efficient network security system is essential to protecting client data. A good network security system helps business reduce the risk of falling victim of data theft and sabotage. Network security helps protect your workstations from harmful spyware. It also ensures that shared data is kept secure. Network security infrastructure provides several levels of protection to prevent Main-in-the-Middle (MiM) attacks by breaking down information into numerous parts, encrypting these parts and transmitting them through independent paths, thus preventing cases like eavesdropping. Getting connected to the internet means that you could receive lots of traffic. Huge traffic can cause stability problems and may lead to vulnerabilities in the system. Network security promotes reliability of your network by preventing lagging and downtimes through continuous monitoring of any suspicious transaction that can sabotage the system. The network security consists of:**

1. **Protection: The user should be able to configure their devices and networks accurately.**
2. **Detection: The user must detect whether the configuration has changed or get a notification if there is any problem in the network traffic.**

3. **Reaction: After detecting the problems, the user must respond to them and must return to a protected position as quickly as possible.**

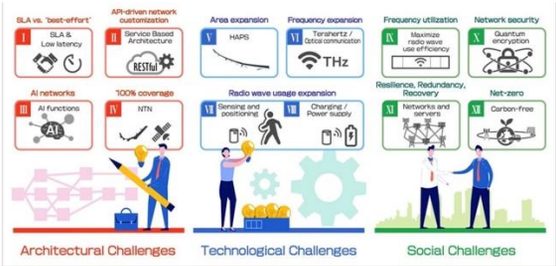
***Data Privacy***


**Data Privacy [7] generally means the ability of a person to determine for themselves when, how, and to what extent personal information about them is shared with or communicated to others. This personal information can be one's name, location, contact information, or online or real-world behavior. Just as someone may wish to exclude people from a private conversation, many online users want to control or prevent certain types of personal data collection. As Internet usage has increased over the years, so has the importance of data privacy. Websites, applications, and social media platforms often need to collect and store personal data about users in order to provide services. However, some applications and platforms may exceed users' expectations for data collection and usage, leaving users with less privacy than they realized. Other apps and platforms may not place adequate safeguards around the data they collect, which can result in a data breach that compromises user privacy.**

***Impacts in 6G***

**By Advancing Extended Reality, Artificial Intelligence, Machine Learning, Digital Twinning, and more, 6G Shows Potential to Optimize Communications, Interoperability, and Sustainability.**

***Challenges in 6G***




**The development of the 6 G network faces many challenges: the technological issues include terahertz waves, peak throughput, higher energy efficiency, connection flexibility, and self-aggregating communications fabric; the non-technical challenges include industry barriers, spectrum allocation and usage rules, and policies and regulations. [8]**

***Security Issues in 6G [9]***

- **Virtualization Security Solution: Virtualization security concerns need the use of a system with a secure virtualization layer, which includes a security technology that identifies concealed harmful software, such as rootkits. In addition, the hypervisor must enable total separation of computing, storage, and the network of different network services using secure protocols such as Transport Layer Security (TLS), Secure Shell (SSH), Virtual Private Network (VPN), and so forth. Virtual Machine Introspection (VMI) is a feature of the hypervisor that examines and identifies security risks by analysing the vCPU register information, file IO, and communication packets of each Virtual Machine (VM) to prevent infiltration. When using containerization, the operating system should appropriately set the different containers' privileges and prevent the mounting of essential system directories and direct access to the host device file container.**
- **Automated Management System: To manage vulnerabilities caused by the use, update, and**

disposal of open sources is the most important thing to do when addressing open-source security issues. That is why fast detection of threats necessitates an automated management system that can discover vulnerabilities and apply patches. An additional step is needed to ensure that the patched software is applied quickly and securely using the secure Over-The-Air (OTA) technique. Furthermore, a security governance framework must be established to handle (1) open-source vulnerabilities from a long-term view, (2) changes in the developer's perception, and (3) the deployment of security solutions.

- Data security using AI: To guarantee that AI systems are safe from Automated Machine Learning (AML), they must be transparent about how they safeguard their users and the mobile communication system from AML. Creating AI models in a dependable system is the first step in the process. Additionally, a method such as digital signatures must be used to verify if the AI models running in User Equipment (UE), Radio Access Networks (RAN), and the core have been maliciously updated or altered by a hostile assault. When a harmful AI model is found, a system must conduct self-healing or recovery operations. The system should also restrict the data gathering for AI training to trustworthy network parts.
- Users' Privacy-preserving: Users' personal information should be stored and used in accordance with agreed-upon protocols between the service provider, the Mobile Network Operator (MNO), the subscriber, and the MNO in order to ensure their safety. Personal information is kept secure in a Trusted Execution Environment (TEE) and dependable SW by the 6G system, which also reduces or anonymizes the amount of information that is made publicly available when it is used. Authenticity and authorization must be verified before MNO releases personal information. Another option is to utilize Homomorphic Encryption (HE) when dealing with user information so that the data may be accessed in an encrypted form. AI-based solutions, such as a learning-based privacy-aware offloading scheme, may also be used to preserve the privacy of the user's location and use patterns.
- Post-Quantum Cryptography: The 6G system has to get rid of existing asymmetric key encryption techniques since quantum computers will make them insecure. Post-Quantum Cryptography (PQC) solutions, such as lattice-based cryptography, code-based cryptography, multivariate polynomial cryptography, and hash-based signature, have been the focus of many researchers. As part of its PQC study, the US National Institute of Standards and Technology (NIST) is scheduled to pick the best PQC algorithms between 2022 and 2024. In comparison to Rivest–Shamir–Adleman (RSA), the key length presently under consideration for PQC is projected to be many times larger. PQCs are likely to have a larger computational cost than the current RSA method. As a result, it is essential that PQC be appropriately integrated into the 6G network's HW / SW performance and service needs.

*Impacts and Challenges of Network Security and Data Privacy in 6G Environment*

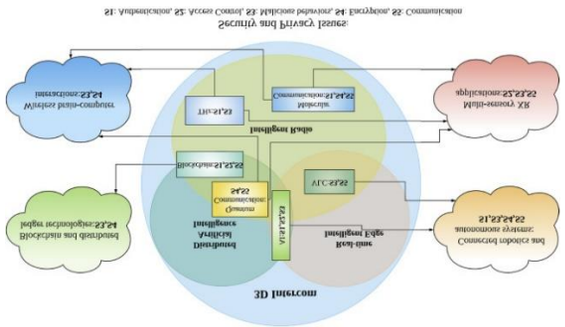



**Fig. 2. Security and privacy issues in the 6G network**

**The circles in Fig. 2 indicate the four key components of a 6G network, which include real-time intelligent edge, distributed AI, intelligent radio, and 3D intercoms [10]. We chose these four areas as our focus because they cover the most powerful part of the 6G study that is being conducted so far. They are also subject to the most security and privacy concerns. The technologies involved in the present research include the AI-based software, the molecular communications, the quantum communications, the blockchain, the Tera Hertz (THz) technology, and the Visible Light Communication (VLC) technology. As denoted in squares in Fig. 2, all these technologies hold great promise for use in various 6G network applications, such as multi-sensory X Reality (multi-sensory XR) applications, connected robotics and autonomous systems, wireless brain-computer interactions, and blockchain and distributed ledger technologies. These are shown as clouds in Fig. 2. The first three areas, namely, the distributed AI area, the real-time intelligent edge area and the intelligent radio area, contain intersecting technologies. Moreover, AI exists at the intersection of all three areas because we assume that 6G networks will be AI-empowered. The five main security and privacy issues are listed below the diagram. Most components of this diagram are vulnerable to authentication, access control, and malicious behavior. However, some technologies are particularly sensitive to certain issues. For example, the VLC, together with both real-time intelligent edge and intelligent radio, is particularly weak against malicious behavior and data transmission process. The molecular communication and the THz technology both support intelligent radio. The molecular communication technology is associated with security and privacy issues concerning authentication, encryption and communication, while the THz technology especially suffers from authentication security and malicious behavior. The blockchain technology and the quantum communication overlap with distributed artificial intelligence and intelligent radio. The main security and privacy concerns here relate to authentication, access control, data transmission and encryption.**

***References***


1. **https://standards.ieee.org/beyond-standards/how-6g-can-transform-the-world-and-technology**
2. **https://en.wikipedia.org/wiki/6G**
3. **https://www.techtarget.com/searchnetworking/definition/6G**
4. **Samar Elmeadawy and Raed M. Shubair, "6G Wireless Communications: Future Technologies and Research Challenges", IEEE International Conference on Electrical and Computing Technologies and Applications (ICECTA 2019), DOI: 10.1109/ICECTA48151.2019.8959607, Nov 2019.**
5. **Mohammed H. Alsharif, Anabi Hilary Kelechi, Mahmoud A. Albreem, Shehzad Ashraf Chaudhry, M. Sultan Zia and Sunghwan Kim, "Sixth Generation (6G) Wireless Networks: Vision, Research Activities, Challenges and Potential Solutions", Symmetry 2020, 12, 676,**

doi:10.3390/sym12040676, www.mdpi.com/journal/symmetry, Apr 2020.

6. https://www.spiceworks.com/tech/networking/articles/what-is-6g
7. https://www.cloudflare.com/learning/privacy/what-is-data-privacy
8. Yang Lu, Xianrong Zheng, "6G: A survey on technologies, scenarios, challenges, and the related issues", Journal of Industrial Information Integration (JIII), Vol. 19, Sep. 2020, 100158.
9. Shimaa A. Abdel Hakeem, Hanan H. Hussein, and HyungWon Kim, "Security Requirements and Challenges of 6G Technologies and Applications", doi: 10.3390/s22051969, Mar 2022.
10. Minghao Wang, Tianqing Zhu, Tao Zhang, Jun Zhang, Shui Yu, Wanlei Zhou, "Security and privacy in 6G networks: New areas and new challenges, Digital Communications and Networks", Vol. 6, Issue 3, Aug 2020, pp. 281–291, https://doi.org/10.1016/j.dcan.2020.07.003.