Analysis of the Transformative Impact of 5G and 6G Technologies on Healthcare

Meenakshi Kashyap[1], Samir Savaliya[2], Dhruvil Talaviya[3], Rushabh Sutariya[4]
[1,2,3,4] *Department of Information Technology, P P Savani University, Damdod, Surat, India*

***Abstract*—In contemporary healthcare, traditional, hospital-centric approaches are being replaced with a decentralized, patient-first approach. One of the main forces behind this improvement is the development of wireless communication, which makes it possible to provide proactive and customized medical care outside of hospital settings. While 4G laid the groundwork for mobile health, it cannot supply the massive device connectivity and throughput required for the cutting-edge medical services currently being developed. Next-generation 5G and 6G networks represent a major turning point because of their high reliability and virtually low latency needed for life-critical applications like telesurgery, continuous biometric monitoring, and immersive virtual diagnostics. By connecting these networks to the Internet of Things (IoT), we can overcome long-standing challenges in system performance and network reach. This article examines how 5G and 6G designs facilitate this digital shift, describing the supporting technologies and their practical applications. We also address the pressing issues of data privacy and cybersecurity, and we conclude with a roadmap of the research issues that will influence future smart healthcare.**

***Index Terms*—5G/6G, Smart Healthcare, Data Security**

I. INTRODUCTION

The healthcare sector is undergoing a dramatic change right now. A more sophisticated system that emphasizes remote care, ongoing monitoring, and preventative health is increasingly replacing the traditional paradigm, which has mostly relied on in-person and reactive therapy. The availability of dependable communication networks is crucial to this more recent system. The value of connected medical equipment was shown by the first e-Health systems, which were based on 4G LTE and related wireless technologies. However, as healthcare applications have become more complex—such as vast amounts of sensor data and real-time high-quality video for telemedicine—4G networks have been unable to support these new demands effectively. The emergence of 5G and the eventual development of 6G are expected to give healthcare a more

robust and intelligent technological base [1]. These networks bring significant changes, such as quicker access, an extremely reliable communication without delay, and the possibility to support a very high number of connected devices—features that are all crucial for the healthcare of the present day.

II. THE EVOLUTION FROM 4G TO NEXT-GENERATION NETWORKS

Every new generation of wireless technology is characterized by order-of-magnitude upgrades in the crucial performance indicators (KPIs).
The transition from 4G to 5G and eventually 6G is crucial since many medical use cases require both rapid speeds and good reliability.

A. The Three Core Strengths of 5G

Three main service areas that address various healthcare demands are at the core of 5G technology:

- Enhanced Mobile Broadband (eMBB): eMBB may deliver extremely high data rates, up to 20 Gbps during peak usage and over 100 Mbps during regular use. Large medical files like CT and MRI pictures, excellent video for remote consultation, and extremely advanced technologies like AR/VR for surgery planning and instruction are all made possible by this.
- Ultra-Reliable Low-Latency Communication (URLLC): URLLC is providing communication that is extremely reliable with the delay going as low as 1 millisecond and the reliability being over 99.999%. This is crucial in real-time medical activities such as robotic telesurgery, where even a tiny delay can be significant. Besides that, it also enables smooth communication between emergency vehicles, traffic systems, and hospitals [2].
- Massive Machine-Type Communication (mMTC): mMTC is capable of accommodating up to one million connected devices in a single

square kilometer. This enables the use of a large network of wearables, smart implants, and hospital sensors that daily monitor the health of patients and the environment.

B. The 6G Vision: A Highly Connected Healthcare Future

While 5G is still expanding globally, 6G's early studies are already envisioning how communication will be revolutionized next. 6G will most probably make use of the terahertz (THz) frequency spectrum, provide ultra-low latency and deliver data rates of up to 1 terabit per second [3].

For healthcare, 6G delivers a vision of communication beyond mere speed:

- Integrated Sensing and Communication (ISAC): Future networks will be more than just data routers. They will also become sensing systems. By studying how signals are changed by the environment, the network may, for example, help in detecting movement, monitoring the patient's breathing without any physical contact, or even be capable of recognizing a senior's fall.
- Holographic Tele presence: With very high bandwidth and extremely low latency, 6G could enable 3D holographic communication, which will be just like face-to-face interaction. Doctors can virtually be in the operating rooms/hospitals with the patients, providing the necessary guidance during the procedure without their physical presence.

TABLE I. Comparative Analysis of 4G, 5G and 6G Networks

Metric	4G (LTE-A)	5G	6G (Envisioned)
Peak Data Rate	~1 Gbps	~20 Gbps	>1 Tbps
Latency	~10-50 ms	~1 ms	<1 ms (sub-μs)
Connection Density	10^5 devices/km²	10^6 devices/km²	10^7 devices/km²
Reliability	~99.9%	>99.999%	>99.99999%
Frequency Bands	Sub-6 GHz	Sub-6 GHz, mmWave	Sub-6 GHz, mmWave, THz

III. 5G/6G HEALTHCARE NETWORKS' ARCHITECTURAL FOUNDATIONS

5G and 6G are not just a single technology. Instead, their advanced capabilities are the outcome of a synergistic combination of architectural innovations at the core network, radio access network, and device level.

A. Key Network Technologies

Network Function Virtualization (NFV) and Software-Defined Networking (SDN): Both these strategies change the way a network's control system interacts with the physical layer hardware. SDN offers a unified, central point from where the network can be administered, thus facilitating easier adjustments and control. NFV substitutes the expensive, dedicated hardware (like routers and firewalls) with software that can perform the same functions on a standard server [4]. By combining the two, a 'network slicing' concept is enabled, where a single physical network can be split into multiple independent virtual networks. Each virtual network is like a tailor-made network for one specific requirement. Say, for instance, a remote surgery procedure being conducted on a network slice, which has been completely separated from the usual hospital data and the guest Wi-Fi, of that hospital, for the purpose of security, priority, etc.

- Multi-Access Edge Computing (MEC): MEC relocates storage and processing from far-off data centers, to places closer to the user. This is one of the main ways to fulfill the need for ultra-low latency. For example, in a smart hospital, a MEC server located nearby can take care of the information coming from medical devices instantly thereby paving the way for quick emergency notifications/actions without the usual time lag data has when it travels over the long-range [5].

B. Innovations in Radio Access Networks (RAN)

- Massive MIMO: This technology gives the cellular base stations a large number of antennas. As a result, it supports beam forming, which is the targeting the signal at a particular user device instead of just spreading the signal everywhere. The benefits that come from this include better signal strength, less interference, and thus improved speed and efficiency.
- Terahertz (THz) and millimeter wave (mmWave) bands: These extremely high-frequency bands provide a large amount of the unused spectrum that is great for multi-gigabit speed. Even though mmWave/THz-band signals have a short range and can be blocked by the presence of obstacles, they are great for use in

controlled environments such as hospital rooms, operating theatres or patient homes.

- Non-Orthogonal Multiple Access (NOMA): NOMA makes it possible for several users to share the same time and frequency resources through the allocation of different power levels to them. The greatly increased spectrum usage efficiency is one of the main benefits. In addition, it helps to face the challenge of the tremendous growth of the number of small, low-power medical devices in the future healthcare environments [6].

IV. PRIVACY AND SECURITY IN HYPERCONNECTED HEALTHCARE

Healthcare is a major target for cyber-attacks mainly because of connected medical devices that are widely used and very sensitive Electronic Health Records (EHRs). A completely new security model must be adopted as the attack surface 5G and 6G offer is bigger and more complicated.

A. The Changing Environment of Threats

The security risks in modern healthcare networks can be grouped into a few main categories:

- Confidentiality: This is one of the violations where, for example, someone secretly listening to the communication between medical systems or intercepting the data being transferred. In other words, it refers to accessing patient's information without the patient or an authorized personnel knowing.
- Integrity: The meaning of this is that the medical information is changed without the permission or knowledge of the person who owns it or the doctor who gave the information. Even such minor changes as changing a patient's blood type or medicine dosage in the health record may bring disastrous results.
- Availability: The primary goal of such threats is to deny people access to services. It is said that a hospital network attack can be such an example, which can hamper a doctor's monitoring through remote, stop online consultation by doctor and patient, or even a telesurgery in progress can be brought to a standstill.
- Authentication: The main point here is that an intruder acts as a legitimate hospital staff when trying to gain access so he may get a hold of the hospital systems.
- Non-repudiation: This characteristic of the system guarantees that each action or message cannot be rejected later. It plays a crucial role in record keeping, accountability, and legal purposes [7].

B. Modern Protective Methods

Instead of depending on a single barrier, healthcare networks must be protected by multiple levels of security. This strategy is more adaptable and more appropriate for rapidly evolving digital contexts.

Blockchain Technology: A shared, unchangeable record of access to and modifications to medical data systems can be created via a blockchain. It provides a clear way for anyone to access and edit patient data. As a matter of fact, it can also help patients manage their entire record-viewer's list.

Advanced Network Monitoring Tools: Modern systems may quickly identify security risks by analyzing massive volumes of network data for any unusual activity. By automatically disconnecting a suspect device, for example, these tools can stop the problem from spreading [8].

Transparent Alert Systems: Administrators must be informed of the reasoning behind any security alerts generated by automated processes. In addition to reducing the amount of false alarms and boosting staff confidence in the system's decision-making, well-written and justified alerts aid with danger confirmation.

Next-Generation Cryptography: Standard encryption methods are about to become weak and outdated due to technological advancements like powerful computers. New encryption techniques are being developed to protect data from both anticipated and current threats. They will be the primary means of ensuring the confidentiality of long-term medical records.

V. UNRESOLVED RESEARCH ISSUES AND PROSPECTS

Although a fully integrated 5G/6G healthcare ecosystem has a lot of potential, there are still a lot of unanswered questions that require concerted investigation.

Technical Challenges:

- Energy Efficiency: According to research, billions of medical devices—the majority of which are small and run on batteries—need incredibly energy-efficient communication techniques in order to work for extended periods of time without the need for battery replacement or charging.

- Terahertz (THz) Channel Understanding: To begin with, it is uncertain how terahertz transmissions behave in intricate indoor environments like hospital buildings [9]. The creation of reliable networks at such frequencies requires more trials and precise modeling.
- Smooth Network Integration: Using a range of communication technologies, such as 5G, Wi-Fi 6, and LoRaWAN, is a defining feature of the contemporary healthcare system. Allowing devices to switch between various networks smoothly and continuously is still a major design challenge.

Challenges with Security and Privacy:

- Lightweight encryption: Medical devices with limited processing power will need security techniques that are both robust and easy to operate on little hardware.
- Privacy-protecting data methods: There are several techniques to analyze health data on a wide scale without identifying any patients. Although there are always opportunities for more extensive research, these techniques should ensure that sensitive data sets are solely investigated on local devices or hospital systems.
- Protection against data manipulation: The healthcare industry should be protected from attacks that infect its datasets with damaging or dishonest data, which could lead to inaccurate records or negatively impact medical choices [10].

Regulatory and Moral Difficulties:

- Data Control and Responsibility: To identify the owners, managers, and individuals accountable for the vast amounts of data produced by modern medical equipment, clear regulations must be put in place.
- Fairness and Equal Treatment: Digital technologies for healthcare should be created to avoid biased outcomes based on community identity, gender, or socioeconomic status.
- Standardization: To create a cohesive and reliable healthcare system, it is essential to have globally accepted standards for data formatting and medical device communication.

VI. CRITICAL ANALYSIS: CONNECTING THE FUTURE WITH THE PRESENT

Even though 5G and 6G have a lot of potential benefits for the healthcare industry, it's crucial to look past the technological benefits and take into account the practical difficulties of implementing these systems. In addition to technology, successful adoption requires addressing a number of structural and practical challenges that are frequently disregarded [11].

A. The Digital Divide and Economic Barriers

The high expense of constructing and modernizing the necessary infrastructure is one of the main obstacles. This entails setting up fiber networks, modernizing communication towers, and providing hospitals and clinics with technologies that operate. Due to these expenses, well-funded hospitals and big cities are more likely to have advanced connection first, whereas smaller facilities and rural locations can find it difficult to keep up. Instead of increasing access for everyone, this could inadvertently exacerbate the divide between communities and create an unequal healthcare system.

B. Integrating New Systems With Older Equipment

Hospitals and clinics are complex ecosystems composed of legacy IT systems, medical equipment from several vendors, and established workflows. Easy integration of new 5G and 6G-capable devices is essential for a smooth IoMT network. In reality, ensuring interoperability between next-generation networks, proprietary software, and decades-old hardware is really challenging. Without widely recognized data standards and communication protocols, the hyperconnected hospital could become an uncontrollably fragmented collection of isolated technology [12].

C. Hyper-Connectivity: Risks and Emerging Dependencies

The shift to remote and automated healthcare places a heavy burden on network availability and integrity. High reliability is guaranteed by URLLC, but sophisticated cyberattacks, network outages, and software errors are still possible [13][14]. A successful DDoS assault or a centralized network failure might simultaneously stop thousands of remote patient monitoring devices or numerous remote surgeries, creating a single point of failure with potentially catastrophic consequences. The need for offline fail-safe procedures and backup plans is called into doubt by this over-reliance.

VII. CONCLUSION

The combination of 5G and 6G technology is predicted to be one of the biggest change-catalysts in the history of healthcare. These networks will provide the basic framework for a future in medicine that is more customized, predictive, preventative, and participative. From enabling complex remote procedures with haptic feedback to continually monitoring entire populations through a huge network of intelligent sensors, the potential to enhance patient outcomes and operational efficiency is considerable.

But reaching this objective necessitates a comprehensive and proactive approach. Due to the complexity of the architecture and the vital importance of data security and privacy, there are substantial challenges. Success will require a multi-stakeholder collaboration involving researchers, legislators, medical experts, and technology. 5G and 6G's full revolutionary potential can be unlocked to produce a smarter, more equitable, and more responsive global healthcare system.

REFERENCES

[1] R. C. Sofia, H. Shen, Y. Liu, S. Kacianka, and H. Pfeifer, "White paper: Towards human-centric and sustainable 6G services—The fortiss research perspective," arXiv:2507.14209, July 2025.

[2] B. Ananthula and N. Budde, "The deeper investigation of smart healthcare systems using 5G security," unpublished.

[3] X. Xie, Y. Tian, J. Huang, Q. Luo, and T. Chen, "Surgery without distance: Will 5G-based robot-assisted telesurgery redefine modern surgery?" Transl. Lung Cancer Res., vol. 14, no. 5, pp. 1821–1829, May 2025.

[4] A. M. Peralta-Ochoa et al., "Smart healthcare applications over 5G networks: A systematic review," Appl. Sci., vol. 13, no. 3, p. 1469, Jan. 2023.

[5] P. Pritika, B. Shanmugam, and S. Azam, "A review of risk assessment of heterogeneous IoMT devices," Technologies, vol. 11, no. 1, p. 31, Feb. 2023.

[6] I. Batool, "Real-time health monitoring using 5G networks: A deep learning-based architecture for remote patient care," arXiv:2501.01027, January 2025.

[7] D. Van Anh et al., "Innovative health: How 6G and wearable devices are shaping the future," J. Commun., vol. 20, no. 3, pp. 338–348, Mar. 2025.

[8] N. Kaur and L. Gupta, "Explainable AI for securing healthcare in IoT-integrated 6G wireless networks," unpublished.

[9] Y. Y. Ghadi et al., "Improving patient care through mobile edge computing and 5G: Difficulties and solutions for safe online health tools," J. Cloud Comput., vol. 13, no. 1, p. 93, May 2024.

[10] F. Meng et al., "Urology applications of 5G telesurgery," UroPrecision, vol. 1, no. 1, pp. 31–37, March 2023.

[11] I. Ahmad, I. Ahmad, and E. Harjula, "Adaptive security in 6G for sustainable healthcare," arXiv:2403.01100, March 2024.

[12] A. Ahad et al., "A thorough review on 5G-based smart healthcare network security: Taxonomy, issues, solutions, and future research directions," Array, vol. 18, p. 100290, July 2023.

[13] H. Pennanen et al., "6G: The intelligent network of everything," IEEE Access, vol. 13, pp. 1319–1421, 2025.

[14] Devi et al., "A review of 5G technology in healthcare and wearable devices," Sensors, vol. 23, no. 5, p. 2519, Feb. 2023.