Integrating 6G and Tactile Internet in Participatory Healthcare: A Pathway to Enhanced Security and Resilience

MATTEO GROSSE-KAMPMANN, Rhine-Waal University of Applied Sciences, AWARE7 GmbH, Germany
TOBIAS URBAN, Insitute for Internet Security, Westphalian University of Applied Sciences, Germany

This paper discusses the transformative potential of 6G technology and the tactile Internet in reshaping participatory healthcare models while architecturing these digital healthcare systems with security and resiliency by design. As healthcare continues to advance towards more inclusive and patient-centered approaches, the role of emerging technologies like mobile health, 6G, and the Internet will become increasingly significant in facilitating these interactions while ensuring the security and privacy of patient data. Furthermore, the organizations providing healthcare to patients must ensure compliance with different regulations, which are also focusing more and more on cybersecurity issues.

Initially, we explore the evolution of participatory healthcare, emphasizing its efficacy in improving patient engagement and outcomes. With 6G technology being currently developed, we start a new era in mobile digital healthcare that promises ultra-reliable, low-latency communication (URLLC). This technology is essential in realizing a tactile internet, where the immediacy and physicality of human experiences can be digitally replicated. This technology can revolutionize tele- and mobile medicine in healthcare, enabling remote surgeries and patient care with real-time precision and sensory feedback. Therefore, the involvement and contentment of the patient will be increased. Nevertheless, this will raise concerns among patients and the general public that must be considered promptly.

We examine the current state of participatory healthcare, highlighting its benefits in enhancing patient engagement, satisfaction, and health outcomes. However, this model's reliance on digital platforms introduces complex security and privacy challenges, for example, in the context of mobile healthcare (mHealth). The technological advancements bring forth sophisticated security challenges. The paper examines these challenges, especially in the context of an increased or altered attack surface presented by 6G and modern communication networks. We outline potential vulnerabilities and the impact of cyber threats on patient trust and safety in highly interconnected digital healthcare environments.

Addressing the resilience of these advanced systems, we assess how 6G and tactile Internet can enhance the capability to withstand and recover from cyber threats. We propose innovative security frameworks tailored for 6G-enabled healthcare systems, drawing on lessons from other sectors and emerging cybersecurity technologies. We evaluate existing security frameworks and their applicability to healthcare systems, identifying gaps and proposing enhancements.

Moreover, we discuss the role of ethics, governance, and policy in shaping the security landscape of digital healthcare when implementing 6G and tactile Internet. Drawing from cross-sector insights, we analyze how lessons from other domains like finance and public services can inform healthcare-specific digital security strategies. Furthermore, ethics should balance the need for robust security measures with the ethical imperative to maintain patient privacy, autonomy, and, first and foremost, patient care.

Finally, we envision the future of secure, participatory, and tactile healthcare enabled by 6G technology. Future healthcare systems must deal with real-time, immersive medical interactions in ubiquitous, connected environments. Therefore, these systems must strengthen security and resilience against emerging threats. We conclude with policy

Authors' addresses: Matteo Große-Kampmann, matteo.grosse-kampmann@hochschule-rhein-waal.de, Rhine-Waal University of Applied Sciences, AWARE7 GmbH, Germany; Tobias Urban, urban@internet-sicherheit.de, Insitute for Internet Security, Westphalian University of Applied Sciences, Germany.

recommendations and strategic directions for stakeholders, aiming to fortify the security and resilience of a patient-centric healthcare ecosystem in an increasingly digital world.

ACKNOWLEDGEMENT

The authors gratefully acknowledge funding from the *Federal Ministry of Education and Research* (16KISR001K & 16KISR002 “HealthNet”), and the *Federal Office for Information Security of Germany* (grants 01MO23033B “5Guide” and 01MO23025B “Pentest-5GSec”).