Smart Health in the 6G Era: Bringing Security to Future Smart Health Services

Edgar Batista, Pablo López-Aguilar, and Agusti Solanas, *Senior Member, IEEE*

***Abstract*—6G promises to revolutionise not only the way we understand wireless communications but all the interactions, services and daily activities that are built upon. The increase in device density and data rates combined with the reduction of energy needs and latency open the door to ground-breaking opportunities in multiple domains. In particular, smart health services could benefit from the adoption of 6G to become more efficient, resilient, sustainable, affordable and ubiquitous. With the adoption of 6G, the current sensing, communication and interaction capabilities of context-aware environments will be magnified resulting in unprecedented, supercharged smart health services. However, despite all the advantages of 6G, health services must deal with sensitive data and for 6G-based healthcare to be a reality, challenges related to security and privacy must be addressed from its inception. In this article, we present the opportunities and novel services that 6G technology enables for smart health. We provide a thorough discussion of the security aspects, by identifying specific security requirements, highlighting security challenges, and pointing out gaps that remain open and must be bridged by future research.**

***Index Terms*—6G, Smart health, Information security, Data privacy, Information systems.**

I. Introduction

SINCE the 1980s, wireless communications have experienced steady progress guided by a new mobile (cellular) technology every decade. While 5G systems are currently being deployed for the 2020s intelligent information society, some limitations hindering ground-breaking use cases have already been identified. To face these limitations, 6G communications envisage a truly connected, omnipresent information society built upon ubiquitous computing, artificial intelligence (AI)-based services, and unprecedented communication capabilities in terms of speed, reliability, density and latency [1].

6G technology will reshape the world as we know it, and by 2030, it will usher in game-changing paradigms in many verticals. In particular, it will transform the healthcare industry, which has been deeply affected by information and communication technologies since the early 2000s (see Fig. 1). Nowadays, many health services follow the smart health paradigm [2], which advocates for using the sensing infrastructure and communication networks of context-aware environments, such as smart homes, smart buildings and smart cities. As the sensing and communication capabilities of these context-aware environments will be magnified, future smart health services will encounter in 6G-enabling technologies a tremendous opportunity to face the needs of an increasingly demanding ageing population, and the growth of comorbidities and chronic diseases.

The standard specifications of 6G are yet to be fully defined, and relevant issues such as security and privacy for 6G networks are still in an embryonic stage [3]. Although these aspects are fundamental to safeguarding communications, they have even greater relevance within the healthcare domain, which deals with highly sensitive information. Hence, the practical adoption of 6G in healthcare will not be possible unless security and privacy concerns are addressed.

In this article, we provide a holistic investigation of the security aspects to be considered in realistic smart health scenarios enabled by 6G technology. To this end, we elaborate on the relationships between three main pillars: 6G, smart health, and security. Although some articles have addressed the issues of smart health [2] and security [4], this article considers them along with 6G globally. The key contributions of the article can be summarised as follows:

- Describe novel and exciting opportunities of next-generation smart health services with the consolidation of 6G networks along with their enabling technologies.
- Identify the most relevant security concerns of 6G networks and their enabling technologies.
- Contextualise the importance of security aspects in the smart health domain.
- Identify specific, fine-grained security requirements for 6G to enable smart health.
- Pinpoint the main challenges of 6G systems from multiple angles, and set the ground for future research directions.

II. 6G and Smart Health

Smart health services evolve along with the underlying technologies they use: the more capable technologies are, the more sophisticated those services become. 6G enhances (in one to two orders of magnitude) the data rate, latency, density and reliability of current 5G-based health services. This results in a better quality of service/experience. There are numerous 6G-enabling technologies that will benefit smart health. Table I provides a features taxonomy that groups the most promising technologies. Such technologies are expected to enable a myriad of enhanced smart health services that contribute to a better citizens' quality of life. Next, we describe several smart health use cases enabled by 6G (see Fig. 2 for a graphical representation).

- *Real-time health provisioning*: On-body sensors, nanodevices and implants can capture and transmit physiological

The authors are with Universitat Rovira i Virgili, Department of Computer Engineering and Mathematics, Tarragona, Spain. A. Solanas is also with Institut d'Investigació Sanitària Pere Virgili, Tarragona, Spain.
Corresponding author: agusti.solanas@urv.cat

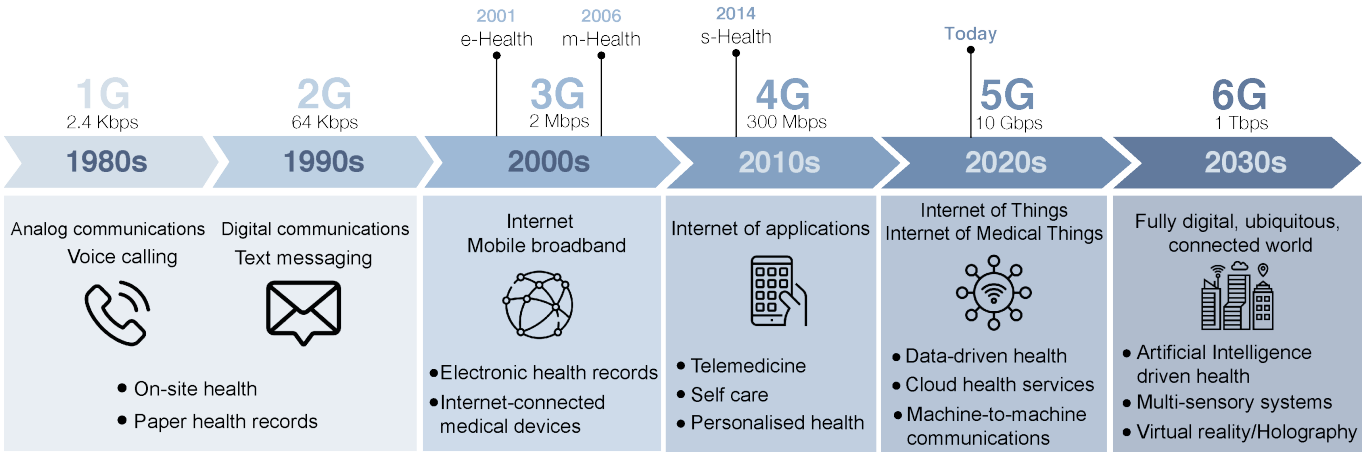

Fig. 1. Evolution of healthcare over mobile generations: from 1G to the emerging 6G. Each generation is associated with a decade. The conceptualisation of the main digital health paradigms is also highlighted: e(lectronic)-Health, m(obile)-Health, and s(mart)-Health.

and contextual data in real-time using extremely reliable links. Networks of intra-body devices communicating through molecular communications are possible. AI analytics allow for monitoring people's health, predicting health conditions, and providing immediate responses more effectively. Interaction with intra-body actuators, such as insulin pumps and implantable cardioverter defibrillators, could reduce the risk of fatal consequences.

- *Virtual consultations*: Holographic technology enables virtual remote consultations. Traditional medical appointments will be redefined, and physicians will assist patients without being physically present. Virtual consultations go far beyond video calls: physicians will be able to diagnose patients using haptic technology. Thus relaxing physical and temporal burdens, and enhancing consultation services in rural areas and developing countries.
- *Better diagnostics*: AI techniques could provide accurate and fast disease diagnoses by seeking hidden patterns in vast amounts of medical data. The accuracy of decision-support systems will increase. Also, augmented reality (AR), holographic and haptic technologies can help evaluate the internal organs of patients in high resolution without invasive, painful procedures.
- *Telesurgeries*: Remote interventions will be feasible over 6G networks. Doctors will perform surgeries remotely with an unprecedented sub-millisecond latency, *i.e.,* nearly real-time. Video streaming, augmented with virtual reality (VR) or holographic technologies, along with novel interaction capabilities through haptic technology will be a game changer.
- *Medical imaging*: Millimetre-precision terahertz (THz) imaging-based scanning can benefit many medical disciplines, such as oncology and dermatology. Moreover, thanks to the use of nanocameras and AI-based image enhancement, diagnoses will be more precise.
- *Interaction with disabled people*: Enhancing the quality of life of disabled people using technology able to translate emotions, perceptions and thoughts into physical commands will be ground-breaking. Haptic communications and brain-computer interfaces (BCI) boost exciting smart health opportunities to interact with disabled people by digitising all five senses.
- *Realistic training*: Fully immersive VR and holography will help physicians to practice complex, high-risk medical procedures in simulation environments without expensive medical equipment. The safety of life-threatening procedures will drastically improve.
- *Digital twins*: The massive sensorisation, THz communications and AI will enable replicating physical entities (*e.g.,* people, objects, places...) in a virtual world. Such digital replicas can be used to explore reality in a virtual and safe environment, enhance business processes, and evaluate the impact of medical or strategic decisions.
- *Pandemics management*: Tracking infectious diseases is hard. Wearables, the Internet of Nano-Things (IoNT), the Internet of Bio-Nano-Things (IoBNT) and AI can help detect outbreaks using real-time medical information of large populations. Also, physicians (a high-risk group) could take advantage of haptics to remotely interact with patients and contribute to stopping the disease's spread.
- *Emergency response*: Disasters, like wildfires and earthquakes, unfortunately happen, and people's lives might be at stake. 6G technology can improve traditional positioning systems, and provide people's location with extreme accuracy. Consequently, rescue teams could act faster and more effectively.
- *Hospital-to-Home services*: Ambulance services will incorporate AI and holographic technology to enhance life-saving procedures. In this context, hospitals and ambulances could be connected, and doctors (at the hospital) will make rapid patients assessments with the support of paramedics (in the ambulance).
- *Connected infrastructures*: Connecting multiple cyber-physical systems will lead to a truly connected society. Context-aware environments (*e.g.,* smart cities) will pave the way to cognitive environments, able to gather and analyse large amounts of data, apply learning procedures, and adapt their settings in accordance to past experiences.

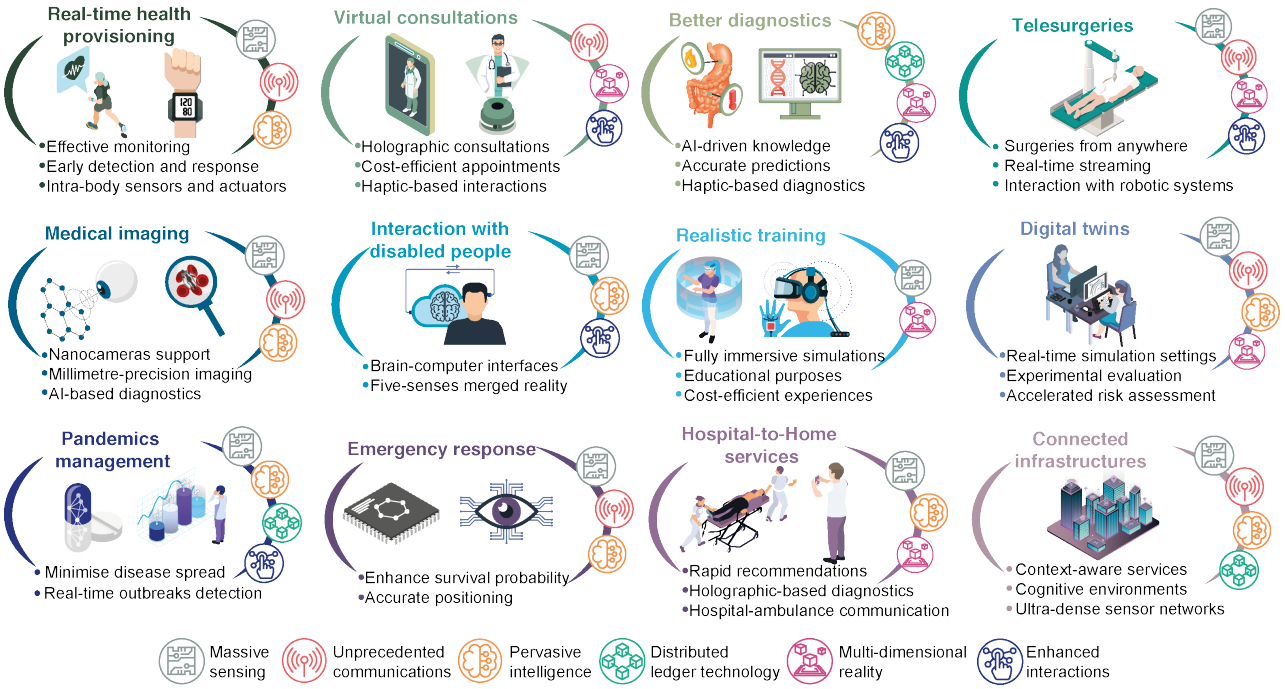

Fig. 2. Description of smart health use cases over 6G. The features playing major roles in each application are highlighted.

III. 6G AND SECURITY

Building secure, private and trustworthy systems is far from straightforward given the sheer number of potential vulnerabilities and threats. With the adoption of 6G, these systems will increase in complexity and, consequently, novel security considerations will arise.

Most 6G-related security analyses [3] classify security issues into three main groups: (i) security threats inherited from previous cellular networks (*e.g.,* legacy protocols, devices compatibility supporting access to both 6G and pre-6G networks, mutual authentication, end-to-end encryption,...), (ii) security threats from the 6G architecture (*e.g.,* physical layer, sub-networks, edge intelligence, intelligence network management,...), and (iii) security threats from the 6G-enabling technologies (*e.g.,* jamming or eavesdropping of novel communication signals, AI poisoning, quantum computing,...). These issues are generally evaluated according to the three security requirements from the CIA model, which considers confidentiality (*i.e.,* preserving authorised restrictions on information access and disclosure), integrity (*i.e.,* completeness and reliability of data), and availability (*i.e.,* protection against malevolent concealment of information).

Given that AI will augment 6G networks with unprecedented capabilities in terms of network management, monitoring, and automation, protecting AI from adversaries is of utmost importance. Also, AI is used to boost network security by detecting eavesdropping or jamming attacks, predicting attacks based on network traffic or node behaviour, and identifying network anomalies that require a potential security enhancement, among others. Notwithstanding, targeted attacks on AI-based systems can drastically decrease the efficiency of 6G infrastructures or even allow attackers to bypass the infrastructures' security [5]. Hence, the challenge is twofold: to secure AI from targeted attacks and to be resilient against AI-based attacks.

Equally important is the security of the 6G physical layer to protect such ultra-dense, heterogeneous, low-resourced networks [6]. With regards to 6G-enabling communications, both THz and visible light communications (VLC) are characterised by highly directional signals at ultra-fast data transmission rates and limited coverage (*e.g.,* light cannot penetrate walls), thus making these technologies theoretically more secure. For example, eavesdropping attacks are much more complicated because adversaries need to be located close to the receiver to intercept the signals without blocking them (and without revealing their malicious intentions). Also, incorporating frequency hopping strategies in such communications decreases the effectiveness of jamming signals. However, such communications are not foolproof yet, and they could be susceptible to attacks under especial settings, *e.g.,* signals might be intercepted by placing an object in the line-of-sight transmission path to scatter radiation towards adversaries or take place close to reflective surfaces such as windows [7].

Nanotechnology is another pivotal technology to unleash the potential of 6G systems. Whereas wearable technology as well as the Internet of Things (IoT) and the Internet of Medical Things (IoMT) paradigms fostered the development of lightweight cryptography, it is still insufficient in the context of nanotechnology and its IoNT/IoBNT paradigms. Thus, novel ultra-lightweight cryptography solutions are needed. In addition, the 6G standard will have to deal with the potential security issues raised by quantum computing. Although quantum computing is still in its early stages, 6G shall be prepared for the post-quantum era with the so-called post-quantum cryptography [8], whose algorithms and protocols (*e.g.,* quantum key distribution) will be cornerstones for the provision of se-

TABLE I
FEATURES TAXONOMY WITH THE MOST RELEVANT 6G-ENABLING TECHNOLOGIES AND THEIR BENEFITS TO SMART HEALTH.

Features	Technologies	Concept	Benefits to smart health
Massive sensing	Internet of Nano-Things (IoNT)	Novel sensors and actuators boosted by nano-technology able to transmit data over the network	Accelerate precise medicine (nanocameras for diagnostics, ingestible sensors for drug delivery, surgical nanorobots…)
	Internet of Bio-Nano-Things (IoBNT)	Interplay between IoNT and biology to collect and transmit biological signals and biochemical processes	Connectivity over the human body (intra-body continuous monitoring and molecular-precision theranostics)
	Internet of Everything (IoE)	Network of connections between people, things, processes, and data to improve cognition across the environment	Unprecedented network of connections to enhance intelligence on the immediate environment
Unprecedented communications	Terahertz (THz) communications	Ultra-fast communications ($\geq$ 1 Tbps) characterised with ample bandwidth and large capacity at short ranges	Foster in-vivo health monitoring, precise medicine, and THz sensing and imaging of biological tissues
	Visible light communications (VLC)	Cost-efficient solution of THz systems (operating at 400–800 THz frequency range) for transmitting data with visible light	Revolutionise indoor communications (emergency rooms, hospitals or nursing homes) with low-cost deployments
	Molecular communications (MC)	Data transmission among nanodevices inside the human body at high rates and low-energy consumption using biochemical signals	Advances in in-body procedures, such as drug delivery, disease detection, imaging, tissue engineering or nanosurgery
	Quantum communications (QC)	Interconnect remote systems over quantum channels, which operate under quantum mechanics	Protect healthcare infrastructures and communications from the post-quantum era, including cryptographic key exchange
Pervasive intelligence	Artificial intelligence (AI)	6G's core component to enable systems with self-awareness, self-learning, and self-decision capabilities, to all 6G networks' layers	Rise of AI-driven healthcare services, by allowing more effective clinical diagnostics and decision-making processes
Distributed ledger technology	Blockchain	Distributed, immutable, tamper-proof database (ledger) containing all the transactions across a peer-to-peer network	Secure patients' electronic health records, exchange data among health facilities in a transparent and trustworthy way
Multi-dimensional reality	Augmented reality (AR)	Interactive experience overlaying visual, auditory or other sensory information onto the real world in real-time	Improve robotic-assisted surgery, access to real-time patients records, and patient engagement in physical rehabilitation
	Virtual reality (VR)	Computer-simulated, fully immersive 3D experience that enables users to explore and interact with their virtual surroundings	Enhance the efficiency of medical training with virtual surgeries, and speed up recovery in physical therapies
	Holography	Photographic technique able to produce a 3D image of an object in very high resolution using lasers	Enhance medical imaging, render advanced diagnostic capabilities and surgical planning, and improve training sessions
Enhanced interactions	Haptic technology	Create experiences of virtual touch (by using force, motion, and vibration) that can be transferred to users or robots	Ground-breaking remote services, including preciser diagnostics or telesurgeries without the physician's presence
	Brain-computer interfaces (BCI)	Direct communication link between the brain and a computer or other device by acquiring and analysing brain signals	Enhance quality of life of elderly or impaired people, such as controlling exoskeletons and improving communication skills

curity, reliability and trust in 6G communications. Combining post-quantum cryptography and nanotechnology will certainly be a major challenge.

The security of 6G systems is complex by nature, so revisiting the security aspects of its key technology enablers is necessary before the actual 6G deployment.

IV. SMART HEALTH AND SECURITY

Smart health has undeniably contributed to the provision of health services in terms of efficiency and sustainability. However, its ability to collect, transmit and analyse enormous amounts of information poses several risks. In particular, we highlight the importance of information security and privacy.

Security and privacy protection are crucial in almost every aspect of our lives, but they have even more relevance in healthcare. For instance, zero-day vulnerabilities or insecure protocols might not only disrupt health services, but they could also jeopardise people's privacy or even endanger people's lives. By considering the context-aware dimension of smart health, information related to people's habits, social status, sexual orientation or religion might be inferred. Such variables are very sensitive *per se*, but when combined with health information, the outcome is even more delicate.

The research community is still struggling to adequately secure current smart health infrastructures [4]. IoT/IoMT devices, such as fitness trackers, body-worn accessories and pacemakers, are the main attackers' entry points due to their limited security measures. Node capturing attacks, sleep deprivation attacks and firmware update attacks are commonplace after successfully exploiting vulnerabilities in the devices allowing attackers to disable or tamper with them. Although attacks against such devices (*e.g.,* pacemakers) might lead to fatal consequences, manufacturers tend to consider security issues an afterthought. Wireless communications, another central component of smart health, are also prone to attacks. Adversaries can exploit a broad number of attacks to intercept communications between two legitimate parties (*e.g.,* Man-in-the-Middle –MitM– attacks), manipulate or destroy data packets crossing the network (*e.g.,* data tampering attacks) or overload systems (*e.g.,* distributed denial-of-service –DDoS– attacks). Communications must, hence, deal with cryptography, secure routing algorithms, legitimate authentication protocols, and intrusion detection.

Besides security aspects, failing to properly protect smart health infrastructures can lead to serious privacy consequences. Medical data leakages have become commonplace, and the situation could worsen with the expected growth in the number of devices and actors involved in providing health services. Moreover, given nanotechnology's popularity, it will be particularly important to protect resource-constrained medical devices (*e.g.,* miniaturised sensors and nanoscopic actuators). To this end, lightweight privacy-preserving solutions will play a prominent role, although finding the balance between privacy enhancements and computational overhead is challenging. With the enforcement of more stringent privacy regulations, such as the European General Data Protection Regulation, smart health services must be developed following both security-by-design and privacy-by-design approaches.

V. ALL PIECES TOGETHER

All things considered, 6G-enabled services must be thoroughly designed with the highest security standards. Given the sensitive nature of the healthcare domain, security concerns are more acute, and security requirements must be strengthened accordingly. After examining the enabling technologies and their applicability in future smart health scenarios, we have identified six security requirements. These requirements, which complement the well-known CIA requirements, cover the needs of 6G-enabled smart health. The identified security requirements are (i) ultra-lightweight security, (ii) real-time security, (iii) proactive security, (iv) AI-driven security, (v) quantum-safe security, and (vi) zero-touch security.

Ultra-lightweight security (UL) is the ability to achieve a strong level of security in highly constrained systems because of their dimensions, computational capabilities, or power consumption. Securing nanoscopic scale targets, such as devices (especially in-body devices) and their communications with other devices from the IoNT/IoBNT network, is paramount due to the direct risks to human lives. By interconnecting intra-body nanoscale networks with bio-electronic devices, new threats such as bio-cyber terrorism arise. By exploiting vulnerabilities, adversaries could gain remote access to the human body, steal personal information, or launch life-threatening attacks, such as hijacking pacemakers, re-configuring smart pills dispensers or creating new types of diseases [9]. 6G nanotechnologies must face many attacks inherited from legacy IoT environments, namely eavesdropping (*e.g.,* capturing images from nanocameras), data injection (*e.g.,* altering data packets with the glucose dose of insulin pumps), spoofing attacks (*e.g.,* malicious nanodevices join the network), DDoS attacks (*e.g.,* draining a pacemaker battery), MitM attacks (*e.g.,* infiltrating between two nanorobots conducting micro-surgery), and malware attacks (*e.g.,* exploiting vulnerabilities of drug delivery systems and reprogram them). Those attacks might be fatal, and preventing them at a nanoscopic scale is not simple. Existing countermeasures in current wireless networks cannot be applied, and novel mechanisms are needed. We envisage four main challenges: (i) the management and distribution of cryptographic keys in a time- and energy-efficient manner, (ii) the development of access control and ultra-lightweight authentication schemes, (iii) the efficient scalability in large, dynamic nanoscopic networks, and (iv) the development of intrusion detection systems at the nanoscopic scale. Also, we foresee that biochemical cryptography [10] will play a prominent role in securing nanocommunications.

Real-time security (RT) is characterised by the ability to respond to events within very specific time constraints. Although this property spreads over all layers of 6G architectures, the physical layer is paramount to secure the entire architecture. To render most attacks useless, real-time data packet inspectors in 6G communication channels could be considered. However, identifying and filtering malicious/suspicious packets within huge data flows in real-time is not easy. Thus, research on advanced threat detection and intrusion prevention systems will be a cornerstone of 6G networks. Regarding 6G-enabling devices, real-time security engines should be deployed in mobile and edge devices to the extent possible since real-time security in nanotechnology may not be feasible.

Proactive security (PR) refers to the approach that anticipates security breaches by periodically identifying and eliminating vulnerabilities. In contrast to reactive security, this approach focuses on prevention rather than detection and response. This requirement applies to sensitive domains that need to prevent potentially harmful situations, such as the disruption of health services. 6G network monitoring (using statistical, behavioural and heuristic analyses) and penetration testing of 6G-enabled devices and systems are good practices to be adopted.

Being AI a key enabler of 6G, it could help creating *AI-driven security* to equip systems with more sophisticated protection mechanisms. Smart health services using 6G would, hence, run in a more secure, autonomous, accurate, and AI-protected infrastructure. Unfortunately, AI is a double-edged sword that could also be exploited by attackers to alter the functioning of AI components of the 6G network. Using poisoning attacks or evasion attacks, adversaries could mislead the outcome of the AI models and bypass security measures. To keep 6G networks safe, future research on AI-enabled cybersecurity is encouraged, allowing to automate threat detection and incidence response, learn from experiences and establish causal relationships among events, and respond more effectively than conventional policy-driven strategies. To this end, advancing in explainable AI will be a must [11].

In the post-quantum era, where 6G health systems will operate, *quantum-safe security* (QS) systems are unavoidable. In this context, the research community is bullish on the potential of quantum algorithms to enhance the security of 6G networks. Main concerns arise from the high cost, computational overhead and energy consumption required to implement fully quantum-resistant solutions. Since resource-constrained devices are likely to prioritise performance over security, this requirement may apply to specific systems of the smart health infrastructure. Health IT leaders should start implementing proof-of-concept quantum-safe services and developing a roadmap for transitioning to quantum-safe systems. However, situations in this arena might be very variable in the years to come, *e.g.,* CRYSTALS-Kyber, a post-quantum encryption algorithm, recently recommended by the National Institute of Standards and Technology, has been broken using AI combined with side channel attacks [12].

Zero-touch security (ZT) refers to the process in which systems can be automatically set up and provisioned by an authorised user by minimising human interaction and reducing potential errors. 6G will leverage this approach to automatically orchestrate and launch 6G networks on-demand in a secure manner. Virtual experiences, such as remote services and immersive training practices, are candidates to adopt this emerging security model. Automating the security of these networks will minimise threats to VR and holographic experiences, such as forged experiences and immersive attacks, which could physically or mentally harm users if disrupting critical VR experiences (*e.g.,* telesurgeries) [13]. Although still under development, securing holography and haptics from eavesdropping and false data injection attacks will be crucial.

TABLE II
TECHNOLOGIES, SECURITY REQUIREMENTS, THREATS AND COUNTERMEASURES OF THE 6G-ENABLED SMART HEALTH USE CASES. THE NEED FOR FULFILLING A REQUIREMENT CAN BE HIGH (✓), MEDIUM (∼), OR LOW (×).

Smart health use cases	**Main technologies**	**Generic security requirements**			**Specific security requirements**						**Main threats**	**Possible countermeasures**
		C	**I**	**A**	**UL**	**RT**	**PR**	**AI**	**QS**	**ZT**		
Real-time health provisioning	Sensors, actuators, nanotechnology, IoT, AI, THz, MC	✓	✓	✓	✓	✓	✓	∼	∼	✓	Device hijacking Modification attacks DDoS attacks	End-to-end encryption Strong authentication Tamper-proofing Redundancy
Virtual consultations	VR, holography, THz, haptics	✓	✓	∼	✓	∼	∼	×	×	✓	Modification attacks Eavesdropping Spoofing attacks Forged experiences	End-to-end encryption Access control Anomaly detection Malware detection
Better diagnostics	AI, AR, VR, holography, haptics	✓	✓	✓	∼	×	∼	∼	×	∼	Adversarial attacks Modification attacks Malware	Distributed AI Tamper-proofing Blockchain
Telesurgeries	Nanotechnology, VR, holography, haptics, THz	✓	✓	✓	✓	✓	∼	∼	✓	✓	Modification attacks Device hijacking DDoS attacks Forged experiences	End-to-end encryption Strong authentication Access control Anomaly detection
Medical imaging	Nanotechnology, IoNT, THz, AI	✓	✓	✓	×	∼	×	×	×	∼	Eavesdropping Jamming Malware	Physical layer security End-to-end encryption Tamper-proofing
Interaction with disabled people	Sensors, actuators, nanotechnology, AI, haptics, BCI	✓	✓	∼	✓	×	∼	∼	∼	✓	Eavesdropping Identity theft Modification attacks Adversarial attacks	Strong authentication Malware detection End-to-end encryption
Realistic training	Sensors, VR, AR holography	∼	✓	∼	∼	×	×	∼	×	✓	Eavesdropping Spoofing attacks Forged experiences Modification attacks	Access control Strong authentication Anomaly detection
Digital twins	Sensors, AR, THz, AI	∼	✓	∼	∼	∼	×	✓	∼	∼	Adversarial attacks Modification attacks Malware	End-to-end encryption Strong authentication Access control
Pandemics management	Sensors, IoBNT, blockchain, AI, haptics	✓	✓	∼	∼	∼	×	∼	×	✓	Devices hijacking Adversarial attacks Spoofing attacks	End-to-end encryption Distributed AI Anomaly detection Strong authentication
Emergency response	Sensors, THz, AI	✓	✓	✓	∼	✓	✓	∼	∼	∼	Devices hijacking DDoS attacks Modification attacks	Physical layer security Strong authentication Access control
Hospital-to-Home services	Wearables, AI, VR, holography	✓	✓	✓	✓	✓	∼	∼	×	✓	Eavesdropping Modification attacks DDoS attacks	Strong authentication Access control End-to-end encryption
Connected infrastructures	Sensors, IoT, THz, AI, blockchain	✓	✓	✓	∼	∼	✓	✓	✓	✓	Devices hijacking Modification attacks DDoS attacks Malware	End-to-end encryption Strong authentication Redundancy Anomaly detection

Meeting these security requirements is preferable, but not always possible. Failing to achieve a given requirement might have different implications: the more severe the consequences, the more needed a requirement is. Following this criterion, we consider that the need for fulfilling a certain requirement is high if the effects of its absence are severe (*e.g.,* the disruption of the health service or even the loss of human lives). If the effects of the absence of a requirement result in a running, but degraded-quality service, the need for fulfilling the requirement is considered medium. If the effects of the absence of a requirement are testimonial because the service could still be provided without major consequences, the need for that requirement is considered low. Table II summarises, for each smart health use case, the identified need for fulfilling each requirement according to the previous criteria, the main 6G-enabling technologies, security threats, and potential countermeasures.

VI. DISCUSSION

6G technology promises a fully connected ecosystem allowing novel, enhanced health services. The diversity of 6G-enabled devices and networks along with the number of novel applications will create higher dependencies between the physical and digital worlds. Thus, the deployment of trustworthy and reliable 6G architectures for smart health must be approached, not only from the technical side, but also from ethical, legal, and socio-economical perspectives.

In this line, trustworthiness (*i.e.,* security, privacy, availability, resilience, and compliance with ethical frameworks) should be considered a key requirement for developing future 6G-based architectures. Although this technology will bring tremendous opportunities in the healthcare industry to enable more efficient and sustainable services, it will raise new ethical dilemmas too. Technologies are not ethically neutral: for example, how can we ensure that a given AI is not biased and it does not undermine certain users or network traffic? These concerns in the healthcare domain become even more severe [14]. Responsible innovation is everybody's job, and technoethics (*i.e.,* ethics in technology) is expected to contribute to it by developing technologies under an ethics-by-design approach. Encouraging the use of ethical-compliant technologies requires multidisciplinary cooperation between the healthcare industry, technicians, and legal/ethics experts. As a first step, the European Commission is setting the rules to promote a safe and trustworthy ecosystem with the emergence of numerous AI-related fields [15].

Similarly, standardisation bodies are called upon to address the challenges associated with the interoperability of networks and device connectivity. For instance, the lack of consistency and homogeneity of regulatory frameworks among countries needs to be redressed. The full deployment of 6G in healthcare will therefore require close collaboration among supranational institutions, national institutions, and healthcare supervisory authorities.

For 6G-enabled smart health services to succeed, a social transformation is required. Citizenship will have to accept these disruptive healthcare provision models. However, the massive sensorisation deployment (especially on-body and in-body sensors) and continuous data analysis processes can be negatively seen as over-surveillance, and a swathe of the population may be reluctant to accept it.

VII. Conclusion

6G technology will maximise worldwide connectivity and will come along with many opportunities, in particular, for the healthcare industry. However, it might also foster economic and social dependence on technology and networks and will open the door to new security threats that must be carefully considered. In this article, we have discussed the security aspects of 6G technology from the perspective of its use in the healthcare domain. Our discussion has been illustrated with relevant use cases and technologies that will impact the future 6G-enabled smart health services. Overall, from our perspective, it is clear that the benefits outweigh the risks, and if the proper security countermeasures are put in place, 6G technologies will shape the provision of healthcare in the future and will contribute to the improvement of the quality of life and well-being of humankind.

Acknowledgments

This research is supported by Agència de Gestió d'Ajuts Universitaris i de Recerca (AGAUR) with grant 2020PANDE00103 (project ACTUA). This work was also supported by Ministerio de Ciencia, Innovación y Universidades, Gobierno de España (Agencia Estatal de Investigación, Fondo Europeo de Desarrollo Regional -FEDER-, European Union) under the research grant PID2021-127409OB-C33 CONDOR. Also, this project has been partially founded by AGAUR research group 2021SGR-00111: "ASCLEPIUS: Smart Technology for Smart Healthcare". This article is based upon work from COST Action CA 19121 (GoodBrother), supported by COST (European Cooperation in Science and Technology).

References

[1] I. F. Akyildiz *et al.*, "6G and Beyond: The Future of Wireless Communications Systems," *IEEE Access*, vol. 8, pp. 133 995–134 030, 2020.
[2] A. Solanas *et al.*, "Smart health: A context-aware health paradigm within smart cities," *IEEE Commun. Mag.*, vol. 52, no. 8, pp. 74–81, 2014.
[3] P. Porambage *et al.*, "The Roadmap to 6G Security and Privacy," *IEEE Open J. Commun. Soc.*, vol. 2, pp. 1094–1122, 2021.
[4] E. Batista *et al.*, "Sensors for Context-Aware Smart Healthcare: A Security Perspective," *Sensors*, vol. 21, no. 20, p. 6886, 2021.
[5] Y. Siriwardhana *et al.*, "AI and 6G Security: Opportunities and Challenges," in *Proc. Jt. EU Conf. Netw. Commun. & 6G Summit*. Porto, Portugal: IEEE, 2021, pp. 616–621.
[6] L. Mucchi *et al.*, "Physical-Layer Security in 6G Networks," *IEEE Open J. Commun. Soc.*, vol. 2, pp. 1901–1914, 2021.
[7] G. Blinowski, "Security of Visible Light Communication systems – A survey," *Phys. Commun.*, vol. 34, pp. 246–260, 2019.
[8] D. J. Bernstein *et al.*, "Post-quantum cryptography," *Nature*, vol. 549, no. 7671, pp. 188–194, 2017.
[9] S. Zafar *et al.*, "A Systematic Review of Bio-Cyber Interface Technologies and Security Issues for Internet of Bio-Nano Things," *IEEE Access*, vol. 9, pp. 93 529–93 566, 2021.
[10] F. Dressler *et al.*, "Towards Security in Nano-communication: Challenges and Opportunities," *Nano Commun. Netw.*, vol. 3, no. 3, pp. 151–160, 2012.
[11] Z. Zhang *et al.*, "Explainable Artificial Intelligence Applications in Cyber Security: State-of-the-Art in Research," *IEEE Access*, vol. 10, pp. 93 104–93 139, 2022.
[12] E. Dubrova *et al.*, "Breaking a Fifth-Order Masked Implementation of CRYSTALS-Kyber by Copy-Paste," Cryp. ePrint Arch., Paper 2022/1713, pp. 1–22, 2022, Accessed on 18 May 2023. [Online]. Available: https://eprint.iacr.org/2022/1713
[13] P. Casey *et al.*, "Immersive Virtual Reality Attacks and the Human Joystick," *IEEE Trans. Dep. Sec. Comput.*, vol. 18, no. 2, pp. 550–562, 2019.
[14] M. J. Rigby, "Ethical Dimensions of Using Artificial Intelligence in Health Care," *AMA J. Ethics*, vol. 21, no. 2, pp. 121–124, 2019.
[15] European Commission, "Proposal for a Regulation of the European Parliament and of the Council: Laying Down Harmonized Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts," Regulation COM/2021/206 final, 2021, Accessed on 14 May 2023. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52021PC0206

Edgar Batista is a postdoctoral researcher in the Department of Computer Engineering and Mathematics at Universitat Rovira i Virgili (URV) in Tarragona, Catalonia, Spain. He received his Ph.D. in Computer Engineering from URV in 2022 with honours (*A cum laude*).

Pablo López-Aguilar is a predoctoral researcher in the Department of Computer Engineering and Mathematics at Universitat Rovira i Virgili in Tarragona, Catalonia, Spain. He received a M.Sc. degree in Cybersecurity Management from Universitat Politècnica de Catalunya in 2018.

Agusti Solanas is the head of the Smart Technologies Research Group and Professor in the Department of Computer Engineering and Mathematics at Universitat Rovira i Virgili in Tarragona. Catalonia. Spain. He received a Ph.D. in Telematics Engineering from Universitat Politècnica de Catalunya in 2007 with honours (*A cum laude*).