IoT Health Data in Electronic Health Records (EHR): Security and Privacy Issues in Era of 6G

Ana Koren[1,*] and Ramjee Prasad[2]

[1]*University of Zagreb, Faculty of Electrical Engineering and Computing, Unska 3, 10000, Zagreb, Croatia*
[2]*CTIF GLOBAL CAPSULE, Department of Business Development and Technology, Aarhus University, Herning, Denmark*
E-mail: ana.koren@fer.hr; ramjee@btech.au.dk
[*]*Corresponding Author*

Received 21 September 2021; Accepted 07 November 2021;
Publication 11 February 2022

Abstract

Millions of wearable devices with embedded sensors (e.g., fitness trackers) are present in daily lives of its users, with the number growing continuously, especially with the approaching 6G communication technology. These devices are helping their users in monitoring daily activities and promoting positive health habits. Potential integration of such collected data into central medical system would lead to more personalized healthcare and an improved patient-physician experience. However, this process is met with several challenges, as medical data is of a highly sensitive nature. This paper focuses on the security and privacy issues for such a process. After providing a comprehensive list of security and privacy threats relevant to data collection and its handling within a Central Health Information system, the paper addresses the challenges of designing a secure system and offeres recommendations,

Journal of ICT Standardization, Vol. 10_1, 63–84.
doi: 10.13052/jicts2245-800X.1014

solutions and guidelines for identified pre-6G and 6G security and privacy issues.

Keywords: Wearable sensors, eHealth, healthcare, 6G, internet of things, internet of medical things, electronic health record, EHR.

1 Introduction

Fitness tracker is an electronic wearable device (usually a wristband) with embedded sensors that monitors various health-related metrics, such as heart rate, oxygen saturation, steps taken, or distance walked. The popularity of fitness trackers is continuously on the rise, especially in the era of Coronavirus disease 2019 (COVID-19) [1]. Fortune Business Insights reported the global market size for fitness trackers amounted to USD 30 billion in 2019 and is estimated to reach USD 92 billion by 2027 [2]. Utilizing health-related data collected via fitness trackers would prompt massive improvements to fields of medicine [3–5], telemedicine [6, 7], and personal well-being [7–9], as it would lead to an improved, personalized healthcare approach since it would enable the physicians continuous comprehensive insight into the patient's state of health. Thus, integrating the personal health data, collected by various sensors within a fitness tracker into the formal Electronic Health Record (EHR) shall provide tailored medical services in compliance with standards and regulations, and offer the patients a more personalized and consistent care while helping physicians to make better and more informed decisions. Smart healthcare:

- Creates well-connected healthcare system
- Allows use of smart biomedical devices
- Offers more personalized healthcare
- Provides better access to healthcare
- Allows improved patient monitoring
- Enables easier tracking of chronic illnesses, as well as early detection and prevention of some diseases
- Improves efficiency and is cost-effective because of preventive care it provides.

However, in order to achieve this, several requirements must be met. Challenges are:

- System needs to handle large volumes of sensor-collected data
- Data quality of the data generated by the sensors

Table 1 6G and 5G performance comparison

	5G	6G
Peak data rate	10 Gb/s	1 Tb/s
End-to-end (E2E) latency	10 ms	1 ms
Maximum spectral efficiency	30 (b/s)/Hz	100 (b/s)/Hz
Maximum frequency	90 GHz	10 THz
Mobility support	500 km/h	1000 km/h
Architecture	Massive MIMO	Intelligent surface
Satellite integration	No	Yes
AI	Limited	Yes
Autonomous vehicles	Limited	Yes
Haptic communication	Limited	Yes
THz communication	Limited	Yes

- Data interpretation
- Scalability
- Software complexity
- Compliance to standards and regulations
- Security and privacy

Main challenges identified are guaranteeing data quality, ensuring security, and maintaining privacy and compliance to the applicable standards and regulations. The way data is being used is changing, with once ordinary devices becoming more and more useful (e.g., smart watch or smart glasses). This will result in massive growth in the rate of information exchanged, and, in the future, might pose a problem to capacity of 5G system. Six-generation (6G) communications is expected to begin in the 2030s [10]. The 6G system has higher capacity and data rates, with lower latency, as shown in Table 1. It also offers superior security and improved quality of service (QoS) compared to the 5G system. Future 6G system is said to revolutionize Internet of Things (IoT) applications in multiple domains, such as:

- Internet of Medical Things (IoMT),
- Vehicular Internet of Things and Autonomous Driving,
- Unmanned Aerial Vehicles (UAV),
- Satellite Internet of Things,
- Industrial Internet of Things.

Thus, (IoT), including IoMT, is identified as one of the key candidate technologies and application scenarios [11]. Finally, [12] presents a comprehensive survey on enabling massive IoT via 6G.

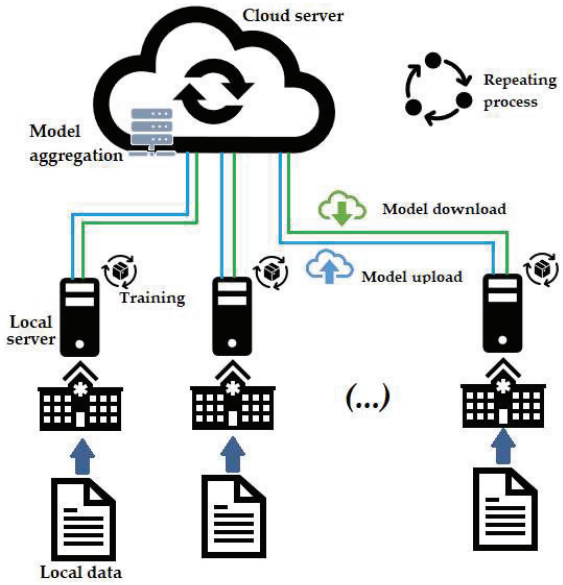


Figure 1 COVID-19 data analytics.

Figure 1 illustrates a potential process of using 6G technologies to analyze COVID-19. Each hospital server has generative adversarial network (GAN), which consists of a generator and discriminator which uses convolutional neural network (CNN, or ConvNet) to learn COVID-19 data distribution from its own dataset. Afterwards, multiple GANs synchronize, and exchange learned information. Model parameters are aggregated in cloud server and form a global model. Global model is propagated to the servers by the cloud server for another round. This process is repeated several times, each time increasing the accuracy [13].

In Section 2, relevant related research is given, including summarized past work by the authors pertinent to the topic. Section 3 provides comprehensive overview of potential security risks and privacy concerns relevant to data collection and communication of information to and within e-Health system, while Section 4 offers threat analysis. Finally, conclusion offers security recommendations and proposition of future work.

2 Related Research

Systematic review [14] and summary of 67 studies [15] concluded wearable devices meet acceptable accuracy and offer high reliability. However, several

studies [16–19] point out the need to clean data collected via wireless sensors, as imprecise data can easily lead to erroneous data analytics and ill-informed decisions. Thus, our previous work [20] compared various data-driven models for cleaning health-related sensor data with the goal of providing accurate and relevant data that could be used in formal EHR. The paper identified multiple linear regression and neural network as the best models for data imputation which were further optimized and resulted in 10–17% improvement in accuracy, depending on the person monitored.

Compliance to standards and regulations was addressed in depth in previous work [21]. Semantic constraints for healthcare datatypes were defined and a process of semantic verification and Schematron-based validation was proposed. The process was then verified using datasets containing various health-related datatypes. The medical information was communicated to healthcare service providers through Health Level 7 Fast Healthcare Interoperability Resources (HL7 FHIR), a standard for health care data exchange, published by HL7, for exchanging healthcare information electronically.

Data collected via wearable sensors are vulnerable to data security breaches [22] offers security analysis of a various fitness trackers available on the market, focusing on the possibility of malicious injection of false data by the user into the tracker's cloud-based services [23] importance of secure pairing mechanisms to avoid eavesdropping attacks as the data is wirelessly transmitted from tracker to smartphone using Bluetooth LE (low energy). SecuWear [24], a multi-domain wearable testbed platform, expedites security research of wearables by conducting attacks in order to identify vulnerabilities of hardware and software. Unencrypted communication between the application and cloud-based server is identified as the biggest risk to data privacy in [25]. [26] proposes a filter system that would balance the security and sharing of health data and [27] presents SensCrypt, a secure protocol for managing Bluetooth fitness trackers. [28] uses the AES algorithm for data encryption and decryption as it prevents the data to be manipulated with. Privacy is another issue as [29] reports many health applications compatible with popular fitness trackers communicate with "unexpected" third parties, such as social networks or advertisement services.

Even though this information must be disclosed in the app's privacy policy, most users never read it [30] and are thus unaware their data is being shared. Finally, patients' adoption of new healthcare technologies is crucial for achieving improved, personalized, and more cost-effective healthcare. However, evidence suggests some patients resist it as they perceive it as a threat to their privacy. [31] examines the impact of privacy concerns have

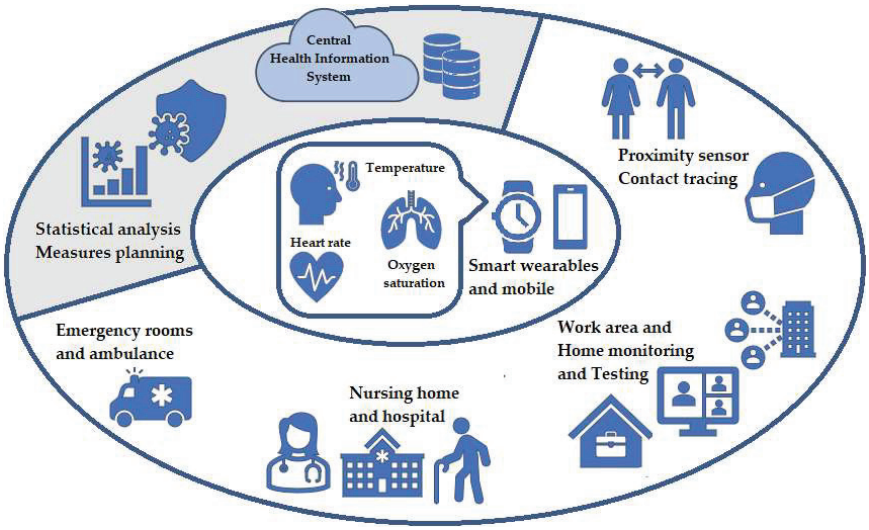


Figure 2 Use-case scenarios for sensing wearable devices and telemedicine.

on the decision whether to accept e-Health technologies. The results show the strongest predictor to the use of digital health technologies is the perception of benefits. Similarly, [32] shows high correlation between individuals' on-going health condition and their healthcare technology acceptance decisions.

Whatever the challenges, the potential and benefits of such a system are gaining more interest than ever, especially because of the current coronavirus (COVID-19). On Figure 2, possible use-case scenarios for wearable devices and telehealth systems during COVID-19 pandemic are illustrated. This includes measuring and tracking personal health data using smart wearables, proximity sensor and contact tracing, work area and home monitoring and testing, aiding staff in caring for patients in nursing homes, hospitals and emergency rooms as well as statistical analysis which allows for more informed measures planning. For example, [34] proposes a BloCoV6, a blockchain-assisted unmanned aerial vehicles (UAV) contact tracing scheme for identifying potential COVID-19 patients.

3 Security and Privacy Threats

Data security protects digital information from being accessed by unauthorized individuals, modified in a destructive manner (corruption), or

stolen. Three major threats to the security of medical data [29] are the following:

- integrity – data must not be tampered with,
- availability – data must be readily accessed when desired,
- confidentiality – data must not be disclosed to unauthorized parties.

Data security must be robust and properly implemented. It needs to protect the information from external malicious parties but also internal threats and human error.

On the other hand, privacy ensures data is handled in a correct manner, including asking for users' consent, giving necessary notice, and following regulatory obligations. Specifically, concerns in context of data privacy are:

- sharing data with third parties,
- how data is collected and stored,
- regulatory restrictions (e.g., GDPR or HIPAA).

General Data Protection Regulation (GDPR) is a single law that unifies data protection within the European Union. In the United States, medical data protection is legislated by Health Insurance Portability and Accountability Act (HIPAA). Comparison of GDPR and HIPAA is given in the Table 2 below. As there are some clear differences, in order for full EHR interoperability, ultimate solution needs to consider all relevant laws and regulations.

In this paper, we focus on European Union and, thus, GDPR. General principles of GDPR are:

- consent – patient must be unambiguously informed and agree to processing of data,
- purpose limitation – must have clearly meaningful purpose,
- data minimization – only required data,

Table 2 GDPR and HIPAA comparison

	GDPR	HIPAA
Data protected	Any information related to identifiable individual	Protected Health Information (PHI)
Accountability	Data controller	Covered entity (health provider)
Breach notification	Must report breach within 72 hours; must inform users affected by the breach	Covered entity required to notify the patient
Third parties	Written safeguards	User must be informed
Sanctions	Depends on the country	Criminal and money penalties

- transparent to the user,
- accuracy of collected data,
- privacy by design (default) – consideration of privacy in design and implementation process,
- data subject right – patient has the right to access data and request data be deleted,
- retention period – data should not be stored indefinitely,
- security measures – ensuring data integrity, availability, and confidentiality.

"Health data" is defined in GDPR by Article 4 paragraph 15, as "personal data related to the physical or mental health of a person, including the provision of health care services, which reveal information about his or her health status". However, some types of data, such as fitness tracker data aren't strictly defined as belonging to this category. Therefore, health data is further specified as:

- strictly medical data - data in a formal medical setting, such as EHR data,
- raw data – e.g., collected by fitness tracker's sensors – only when it's used to assess person's health. While data as heartbeat rate, oxygen saturation or blood pressure are straightforwardly labeled as health data, step count may or may not be, depending if it is being used in medical context or not.

Thus, when using raw data from a tracker, it is crucial to rigidly define types of data being collected, as different types of data may have divergent legal implications.

Privacy Impact Assessment (PIA) is a crucial step when handling confidential data. PIA's goal is to identify and assess privacy implications when collecting, storing, managing, and sharing data, and, thus, to mitigate information risks [35]. The assessment must be made before starting the development of any system which is planned to collect or manage personal data of individuals. Privacy issues found during this process must be documented so the risks can be further analyzed. Then, compulsory actions are set depending on determined impact and probability of occurrence.

4 Threat Analysis

Figure 3 gives an overview of identified security and privacy threats in eHealth system which uses patient-side collected personal health data, i.e.,

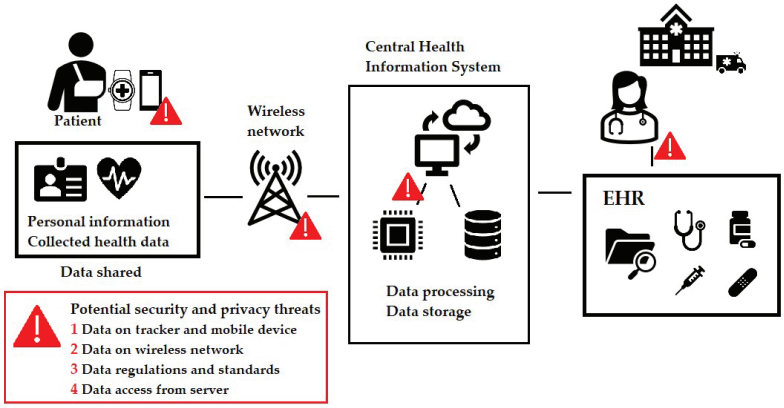


Figure 3 Overview of security and privacy issues in mHealth system.

data collected by a fitness tracker. As illustrated in Figure 3, security and privacy threats when handling personal health data may occur at the following stages:

- while collecting data (sensors) and communicating to mobile device,
- while transmitting data via wireless networks,
- while processing and storing information on healthcare servers, i.e., complying to standards and regulations,
- while accessing stored information (e.g., physician viewing patient's EHR).

4.1 Data on Tracker and Mobile Devices

Identified vulnerabilities of fitness trackers in the past years include:

- use of third-party analytics,
- lack of privacy policy,
- internal (device-side) or external (cloud-side) poor encryption,
- poor protection at transport layer, i.e., using HTTP instead of HTTPS protocol,
- poor security at application implementation, enabling client-side injection, e.g., SQL injection,
- lack of authentication and authorization (password-protected access),
- improper session handling.

These can be avoided but manufacturers need to ensure privacy and security when developing fitness tracker. Likewise, any mHealth mobile

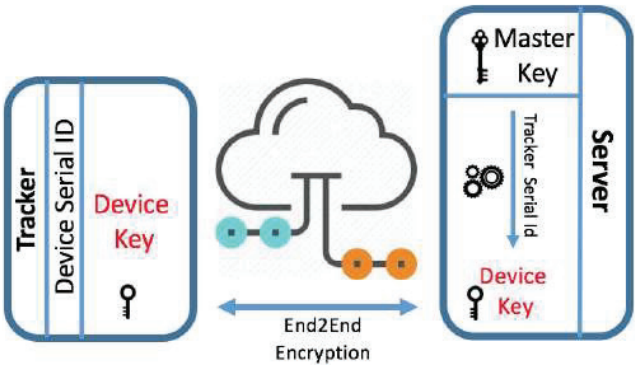


Figure 4 End-to-end encryption.

application must be insusceptible to tampering and capable of protecting itself by detecting threats at runtime.

4.2 Data on Wireless Network

During its transmission from mobile device to cloud server, data is susceptible to being manipulated, e.g., Man-in-the-middle attack, (MITM). In order to prevent this from happening, end-to-end encryption (E2EE), illustrated in Figure 4, with a device-specific key is necessary.

4.3 Data Regulations and Standards

Data must be stored in such a form that it is compliant with applicable standards and regulations, which includes following semantic constraints for healthcare datatypes. This can be achieved with aforementioned process of data verification and validation using Schematron-based validation process [21]. Furthermore, legislative regulations must be obeyed. In case of GDPR this entails privacy policy where patient is explicitly informed what data will be collected, how it will be used, and whether it will be shared to third parties. Patient must give their consent in order data to be used. Patient may revoke their consent at any point in time.

4.4 Data Access From Server

The Electronic Health Record proves to be an important tool in providing medical care as it is implemented in many Central Health Information systems around the world. In order to prevent unauthorized personnel accessing

it, security policy must be implemented within the hospital (or other access point). The policy must have role-based access control to ensure patient privacy and guarantee confidentiality of data within the EHR.

Finally, Table 3 shows possible both security and privacy risks and solutions for how to mitigate them. This should be viewed as general solution ideas and guidelines for future model designs and implementations of systems that handle IoMT health data (e.g., data collected via wearable sensors) within Central Health Information System, i.e., EHR.

Number of such devices is increasing exponentially, and with introduction of new technologies, such as 5G and, in the future, the approaching 6G which envisions Internet of Everything (IoE), new opportunities arise. However, along with higher capacity and data rates, lower latency, and better quality of service, new challenges arise as well. Following section covers security and privacy issues in such future systems.

5 6G: Security and Privacy

In terms of 6G, analysis of security and privacy threats is shown in Figure 5.

Billions of interconnected devices will form the Internet of Everything in era of 6G. Device security model of subscriber identification module (SIM) is not viable for such devices, considering their small form factor. This is especially true when talking about Internet of Medical Things (IoMT) and on-body and in-body sensors. [36] reports key distribution and management to be inefficient in a network of such scale. Furthermore, these devices are operating with limited resources and cannot support cryptography necessary to ensure high security level [37]. This leads to them being the primary target to malicious parties. Once compromised, the device can them be used to propagate attacks in the network. Finally, exploiting the same vulerabilities could lead to data theft which in turns compromises privacy.

6G systems will inherit some 5G technologies, and with it, related security, and privacy issues. Best examples of this are:

- attacks targeting Software-Defined Networking controller, interfaces, and deployment platform vulenrabilities [38],
- attacks on virtual machines, hypervisor, and Network Function Virtualization (NFV) related attacks [39],
- Multi-access Edge Computing (MEC) security and privacy threats, such as information theft using compromised slices [40] or man-in-the-middle (MitM) and Distributed denial os service (DDoS) attacks [41].

Table 3 List of possible risks and solutions

Risk	Solution	Result
The purpose of collecting the patient's data has not been precisely explained to the patient before data has been collected	The purpose of collecting data must be stated explicitly in the privacy policy or consent form, e.g., COVID-19 symptoms or chronic illness tracking	Mitigated
The nature of data collected, i.e., exact data types, is not made clear to the patient	The nature of the medical data being collected must be explicitly stated in the privacy policy/consent form, e.g., heartbeat rate, oxygen saturation, body temperature, etc.	Mitigated
Privacy policy or consent form does not explicitly specify to what extent and in which way the data will be used	Before medical data collection of any kind, patient must be explicitly informed via privacy policy/consent form, which he must consent to	Mitigated
Privacy policy or consent form does not address whether the data will be shared with third parties and for what purpose	If the data is to be shared with third parties (e.g., anonymized data for statistical purposes), this must be explicitly stated in the privacy policy/consent form	Mitigated
No option for withdrawing consent and deleting all the data collected is given to the patient	Patients can, at any given moment, withdraw their consent. If this is to happen, all their data must be deleted	Mitigated
Patients are not able to request revision or modification of potentially incorrect data	Patients must be able to inform of errors in data, or ask for a revision, via secure channel	Mitigated
Data is not anonymized	Data must be anonymized, i.e., data must be processed in such a way it is impossible to identify a specific patient	Mitigated
Data is being stored for a longer period of time than necessary for it to be processed	Data is retained only temporarily until it is has not finished being uploaded to the cloud	Mitigated
Data is being stored in an insecure manner (e.g., unencrypted or publicly accessible)	Medical data must be stored encrypted and cannot be accessible via external storage devices or other applications present on the same hardware or device	Mitigated

(*Continued*)

Table 3 Continued

Risk	Solution	Result
Password and/or encryption keys are kept in plain text	Secure hash algorithm (SHA) is used to store encryption keys	Mitigated
Points of data-input are not secure; validation of input data is needed in order to prevent client-side attacks or tampering with data (e.g., SQL injection)	Client-side attacks are prevented by input sanitization	Mitigated
Insecure data communications channel for transmission of data	Secure data transmission via Secure Sockets Layer (SSL) protocol	Mitigated
Poor logging practices, i.e., writing collected sensitive data into logs	No data classified as health data, i.e., confidential, is being written into log files	Mitigated
Lack of encryption process when backing up data	Data backup is stored after encryption process	Mitigated
Possibility of data being accessed by unauthorized parties (data breach)	Processes of authentication and authorization follow AuthO2 standard. Access control is role-based	Mitigated
Possibility of data modification by unauthorized parties (data tampering)	All data is encrypted, and keys are hidden securely	Mitigated
Possibility of exploits by malicious software, i.e., taking advantage of bugs or vulnerabilities to cause harm	Software, if possible, should be sandboxed (in an isolated virtual)	Partially mitigated

As Terahertz (THz) communications are seen as major part of future 6G technology [42], small cells (5G) will be replaced with tiny cells, leading to ultra-dense networks and mesh connectivity. However, this leads to threat increase as malicious attackers can now potentially target large amount of vulnerable multi-connected devices and compromise the network.

6G will make use of artificial intelligence and blockchain which provide network autonomy and decentralized resource management, respectively. However, this will cause potential security threats to arise. Machine learning systems can potentially be compromised using logic corruption, input inference (model inversion), data manipulation, or poisoning attacks [43]. Similarly, blockchain can potentially be destabilized by attacks using quantum computers.

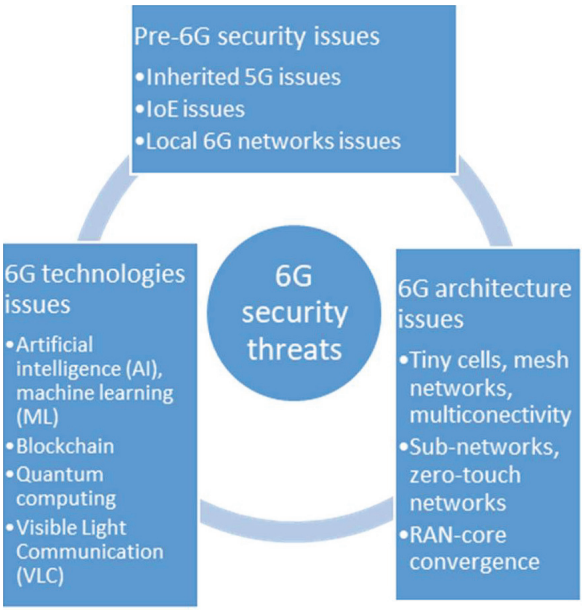


Figure 5 Security and privacy threats in the context of 6G.

In terms of EHR and sensitive IoMT data, possible security issues include:

- Attacks on weak cryptographic systems by the use of quantum computers,
- Compromised or rogue IoT devices,
- Data theft from IoT devices,
- Eavesdropping of communication channels,
- Signal jamming.

6 Discussion: Solutions, and Future Work

General security concerns regarding 6G era are an active research area. In an attempt to mitigate these risks, artificial intelligence is suggested as the main tool [33] to create resilient and robust systems. Table 4 shows how security risks can be mitigated by using AI and machine learning. New design challenge arises, which is to balance the defense improvements with performance degradation due to the increase of resources necessary for the implementation of additional defense mechanisms.

Table 4 Security risk mitigation using machine learning

Security Threat	ML Defense Mechanism
Poisoning attacks	Input validation
	Robust learning
Evasion attacks	Adversarial training
	Defensive distillation
API-based attacks	Differential privacy
	Homomorphic
	Encryption
Present cryptography solutions vulnerable against quantum computers	ML-based algorithms that detect malicious traffic, e.g. ML Multilayered intrusion detection and prevention [44]
Use of AI for attacking, making rule-based detection systems ineffective	Advanced defense techniques are necessary, e.g., using distributed intelligence, moving target [45] or use of quantum computers [46]

Furthermore, present authentication and authorization systems using key management will become inadquate when dealing with large scale mesh networks consisting of huge number of heterogeneous devices. Thus, new security mechanisms should be developed in the future. [33] suggests a hierarchical security mechanism that would distinguish sub-network level sub-network to wide area network security. Other open questions are preserving privacy in automated 6G networks and implementing automated machine ethics.

7 Conclusions

Advanced monitoring which IoT device offer, i.e., continuously track patient's vital signs or activities of daily living can positively influence the quality of healthcare they receive. Continuous real-time monitoring of persons health and well-being includes tracking vital signs. For this, sensor-equipped wearable electronic devices are required. Considering the quantity of data and the necessary quality of service (QoS), 6G technology could prove itself to be the key solution for such a healthcare system as it promises greater connectivity, low latency, and high speeds. Security and privacy, however, are major impediments when designing and implementing smart healthcare system. Any applications providing or facilitating medical services must comply with local regulations and legislation concerning data protection, in this case, GDPR. Healthcare data must not be susceptible to unauthorized

access or tampering. Privacy can be ensured by guaranteeing confidentiality, integrity, and authentication. The work presents comprehensive security and privacy threat identification and analysis when integrating IoMT health data into EHR, both in pre-6G and future 6G era. Solutions associated with the identified threats are provided for pre-6G, while general solution ideas for 6G are discussed, with some open questions being highlighted.

References

[1] S. S. Kumar, "Emerging Technologies and Sensors That Can Be Used During the COVID-19 Pandemic," 2020 International Conference on UK-China Emerging Technologies (UCET), 2020, pp. 1–4, doi: 10.1109/UCET51115.2020.9205424.

[2] Fitness Tracker Market Size, Share & COVID-19 Impact Analysis (2020–2027), Fortune Business Insights, Oct 2020.

[3] P. Huang, C. Lin, Y. Wang and H. Hsieh, "Development of Health Care System Based on Wearable Devices," 2019 Prognostics and System Health Management Conference (PHM-Paris), 2019, pp. 249–252, doi: 10.1109/PHM-Paris.2019.00049.

[4] R. Qian, "Healthcare on Consumer-grade Wearable Devices," 2020 IEEE 3rd International Conference of Safe Production and Informatization (IICSPI), 2020, pp. 298–303, doi: 10.1109/IICSPI51290.2020.9332400.

[5] G. Assenza, C. Fioravanti, S. Guarino and V. Petrassi, "New Perspectives on Wearable Devices and Electronic Health Record Systems," 2020 IEEE International Workshop on Metrology for Industry 4.0 & IoT, 2020, pp. 740–745, doi: 10.1109/MetroInd4.0IoT48571.2020.9138170.

[6] X. Ding et al., "Wearable Sensing and Telehealth Technology with Potential Applications in the Coronavirus Pandemic," in IEEE Reviews in Biomedical Engineering, vol. 14, pp. 48–70, 2021, doi: 10.1109/RBME.2020.2992838.

[7] K. Ueafuea et al., "Potential Applications of Mobile and Wearable Devices for Psychological Support During the COVID-19 Pandemic: A Review," in IEEE Sensors Journal, vol. 21, no. 6, pp. 7162–7178, 15 March 15, 2021, doi: 10.1109/JSEN.2020.3046259.

[8] F. A. A. Naqiyuddin, W. Mansor, N. M. Sallehuddin, M. N. S. Mohd Johari, M. A. S. Shazlan and A. N. Bakar, "Wearable Social Distancing Detection System," 2020 IEEE International RF and Microwave

Conference (RFM), 2020, pp. 1–4, doi: 10.1109/RFM50841.2020.9344786.

[9] K. Grifantini, "Tracking Sleep to Optimize Health," in IEEE Pulse, vol. 11, no. 5, pp. 12–16, Sept.–Oct. 2020, doi: 10.1109/MPULS.2020.3022142.

[10] N. Khiadani, "Vision, Requirements and Challenges of Sixth Generation (6G) Networks," 2020 6th Iranian Conference on Signal Processing and Intelligent Systems (ICSPIS), 2020, pp. 1–4, doi: 10.1109/ICSPIS51611.2020.9349580.

[11] C. Yizhan, W. Zhong, H. Da and L. Ruosen, "6G Is Coming : Discussion on Key Candidate Technologies and Application Scenarios," 2020 International Conference on Computer Communication and Network Security (CCNS), 2020, pp. 59–62, doi: 10.1109/CCNS50731.2020.00022.

[12] F. Guo, F. R. Yu, H. Zhang, X. Li, H. Ji and V. C. M. Leung, "Enabling Massive IoT Toward 6G: A Comprehensive Survey," in IEEE Internet of Things Journal, vol. 8, no. 15, pp. 11891–11915, 1 Aug.1, 2021, doi: 10.1109/JIOT.2021.3063686.

[13] D. C. Nguyen et al., "6G Internet of Things: A Comprehensive Survey," in IEEE Internet of Things Journal, doi: 10.1109/JIOT.2021.3103320.

[14] Evenson KR, Goto MM, Furberg RD. Systematic review of the validity and reliability of consumer-wearable activity trackers. Int J Behav Nutr Phys Act. Dec 2015. doi: 10.1186/s12966-015-0314-1.

[15] Feehan LM, Geldman J, Sayre EC, Park C, Ezzat AM, Yoo JY, Hamilton CB, Li LC. "Accuracy of Fitbit Devices: Systematic Review and Narrative Syntheses of Quantitative Data. JMIR Mhealth Uhealth", Aug 2018. doi: 10.2196/10527.

[16] M. G. Rahman, M. Z. Islam, T. Bossomaier and Junbin Gao, "CAIRAD: A co-appearance-based analysis for Incorrect Records and Attribute-values Detection," The 2012 International Joint Conference on Neural Networks (IJCNN), Brisbane, QLD, 2012, pp. 1–10.

[17] M. G. Rahman, M. Z. Islam, "FIMUS: A decision tree-based missing value imputation technique for data pre-processing," Volume 56 Issue C, January 2014, pp. 311–327.

[18] O. Salem, A. Guerassimov, A. Mehaoua, A. Marcus and B. Furht, "Sensor fault and patient anomaly detection and clas-sification in medical wireless sensor networks," 2013 IEEE International Conference on Communications (ICC), Budapest, 2013, pp. 4373–4378.

[19] D. Yang et al., "A Novel Adaptive Spectrum Noise Cancellation Approach for Enhancing Heartbeat Rate Monitoring in a Wearable Device," in IEEE Access, vol. 6, pp. 8364–8375, 2018.

[20] Koren, A., Jurèević, M. & Prasad, R. "Comparison of Data-Driven Models for Cleaning eHealth Sensor Data: Use Case on ECG Signal". Wireless Personal Communications 114, 1501–1517 (2020). doi.org/10.1007/s11277-020-07435-7.

[21] A. Koren, M. Jurèević, R. Prasad, "Semantic Constraints Specification and Schematron-based Validation for Internet of Medical Things' Data"

[22] H. Fereidooni, T. Frassetto, M. Miettinen, A. Sadeghi and M. Conti, "Fitness Trackers: Fit for Health but Unfit for Security and Privacy," 2017 IEEE/ACM International Conference on Connected Health: Applications, Systems and Engineering Technologies (CHASE), 2017, pp. 19–24, doi: 10.1109/CHASE.2017.54.

[23] K. Lotfy and M. L. Hale, "Assessing Pairing and Data Exchange Mechanism Security in the Wearable Internet of Things," 2016 IEEE International Conference on Mobile Services (MS), 2016, pp. 25–32, doi: 10.1109/MobServ.2016.15.

[24] M. L. Hale, D. Ellis, R. Gamble, C. Waler and J. Lin, "Secu Wear: An Open Source, Multi-component Hardware/Software Platform for Exploring Wearable Security," 2015 IEEE International Conference on Mobile Services, 2015, pp. 97–104, doi: 10.1109/MobServ.2015.23.

[25] S. Anwar, D. Anwar and S. Abdulla, "Security Evaluation of Android Mobile Healthcare and Fitness Applications," 2020 International Conference on Electrical, Communication, and Computer Engineering (ICECCE), 2020, pp. 1–6, doi: 10.1109/ICECCE49384.2020.9179431.

[26] R. Saha, S. Sarkar and S. K. Datta, "Balancing security & sharing of fitness trackers' data," 2017 1st International Conference on Electronics, Materials Engineering and Nanotechnology (IEMENTech), 2017, pp. 1–6, doi: 10.1109/IEMENTECH.2017.8076942.

[27] M. Rahman, B. Carbunar and U. Topkara, "SensCrypt: A Secure Protocol for Managing Low Power Fitness Trackers," 2014 IEEE 22nd International Conference on Network Protocols, Raleigh, NC, 2014, pp. 191–196.

[28] A. R. Shekar, "Preventing Data Manipulation and Enhancing the Security of data in Fitness Mobile Application," 2019 International Conference on Smart Systems and Inventive Technology (ICSSIT), 2019, pp. 740–745, doi: 10.1109/ICSSIT46314.2019.8987892.

[29] A. Kazlouski, T. Marchioro, H. Manifavas and E. Markatos, "Do partner apps offer the same level of privacy protection? The case of wearable

applications," 2021 IEEE International Conference on Pervasive Computing and Communications Workshops and other Affiliated Events (PerCom Workshops), 2021, pp. 648–653, doi: 10.1109/PerComWorkshops51409.2021.9431018.

[30] D. B. Meinert, D. K. Peterson, J. R. Criswell, M. D. Crossland, Privacy policy statements and consumer willingness to provide personal information, Journal of Electronic Commerce in Organizations (JECO) 4(1) (2006) 1–17.

[31] E. Schomakers, C. Lidynia and M. Ziefle, "Listen to My Heart? How Privacy Concerns Shape Users' Acceptance of e-Health Technologies," 2019 International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), 2019, pp. 306–311, doi: 10.1109/WiMOB.2019.8923448.

[32] M. S. Rahman, "Does Privacy Matters When We are Sick? An Extended Privacy Calculus Model for Healthcare Technology Adoption Behavior," 2019 10th International Conference on Information and Communication Systems (ICICS), 2019, pp. 41–46, doi: 10.1109/IACS.2019.8809175.

[33] Y. Siriwardhana, P. Porambage, M. Liyanage and M. Ylianttila, "AI and 6G Security: Opportunities and Challenges," 2021 Joint European Conference on Networks and Communications & 6G Summit (EuCNC/6G Summit), 2021, pp. 616–621, doi: 10.1109/EuCNC/6GSummit51104.2021.9482503.

[34] M. Zuhair, F. Patel, D. Navapara, P. Bhattacharya and D. Saraswat, "BloCoV6: A blockchain-based 6G-assisted UAV contact tracing scheme for COVID-19 pandemic," 2021 2nd International Conference on Intelligent Engineering and Management (ICIEM), 2021, pp. 271–276, doi: 10.1109/ICIEM51511.2021.9445332.

[35] Rodrigues, J. J., De la Torre, I., Fernández, G., and López-Coronado M., (2013), "Analysis of the security and privacy requirements of cloud-based Electronic Health Records Systems," Journal of Medical Internet Research, vol. 15, no. 8, 2013.

[36] J. Mnjama, G. Foster and B. Irwin, "A privacy and security threat assessment framework for consumer health wearables," 2017 Information Security for South Africa (ISSA), 2017, pp. 66–73, doi: 10.1109/ISSA.2017.8251776.

[37] I. L. Pribadi and M. Suryanegara, "Regulatory recommendations for IoT smart-health care services by using privacy impact assessment (PIA)," 2017 15th International Conference on Quality in Research (QiR), International Symposium on Electrical and Computer Engineering, 2017, pp. 491–496, doi: 10.1109/QIR.2017.8168535.

[38] N. Wang, P. Wang, A. Alipour-Fanid, L. Jiao, and K. Zeng, "PhysicalLayer Security of 5G Wireless Networks for IoT: Challenges and Opportunities," IEEE Internet of Things Journal, vol. 6, no. 5, pp. 8169–8181, 2019.

[39] Y. Yang, L. Wu, G. Yin, L. Li, and H. Zhao, "A Survey on Security and Privacy Issues in Internet-of-Things," IEEE Internet of Things Journal, vol. 4, no. 5, pp. 1250–1258, 2017.

[40] I. Ahmad, T. Kumar, M. Liyanage, J. Okwuibe, M. Ylianttila, and A. Gurtov, "Overview of 5G Security Challenges and Solutions," IEEE Communications Standards Magazine, vol. 2, no. 1, pp. 36–43, 2018.

[41] R. Khan, P. Kumar, D. N. K. Jayakody, and M. Liyanage, "A survey on security and privacy of 5g technologies: Potential solutions, recent advancements, and future directions," IEEE Communications Surveys & Tutorials, vol. 22, no. 1, pp. 196–248, 2019.

[42] P. Ranaweera, A. D. Jurcut, and M. Liyanage, "Survey on Multi-Access Edge Computing Security and Privacy," IEEE Communications Surveys Tutorials, pp. 1–1, 2021.

[43] S. Wijethilaka and M. Liyanage, "Survey on network slicing for internet of things realization in 5g networks," IEEE Communications Surveys & Tutorials, 2021.

[44] K. M. S. Huq, J. Rodriguez and I. E. Otung, "3D Network Modeling for THz-Enabled Ultra-Fast Dense Networks: A 6G Perspective," in IEEE Communications Standards Magazine, vol. 5, no. 2, pp. 84–90, June 2021, doi: 10.1109/MCOMSTD.001.2000048.

[45] C. Benzaid and T. Taleb, "AI for Beyond 5G Networks: A CyberSecurity Defense or Offense Enabler?" IEEE Network, vol. 34, no. 6, pp. 140–147, 2020.

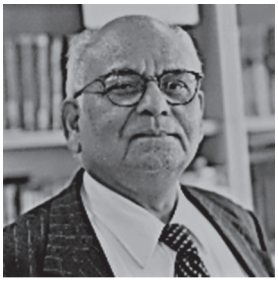
[46] I. H. Abdulqadder, S. Zhou, D. Zou, I. T. Aziz, and S. M. A. Akber, "Multi-layered Intrusion Detection and Prevention in the SDN/NFV enabled Cloud of 5G Networks using AI-based Defense Mechanisms," Computer Networks, vol. 179, p. 107364, 2020.

[47] J.-H. Cho, D. P. Sharma, H. Alavizadeh, S. Yoon, N. Ben-Asher, T. J. Moore, D. S. Kim, H. Lim, and F. F. Nelson, "Toward Proactive, Adaptive Defense: A Survey on Moving Target Defense," IEEE Communications Surveys & Tutorials, vol. 22, no. 1, pp. 709–745, 2020.

[48] J. Biamonte, P. Wittek, N. Pancotti, P. Rebentrost, N. Wiebe, and S. Lloyd, "Quantum Machine Learning," Nature, vol. 549, no. 7671, pp. 195–202, 2017.

Biographies

Ana Koren completed undergraduate studies in 2012, and graduate studies in 2014 at the Faculty of Electrical Engineering and Computing, University of Zagreb and is currently enrolled in a PhD programme at University of Zagreb. She has been a visiting researcher at TU Graz (Austria), Universidad de Zaragoza (Spain) and Universidad Nacional de Colombia (in Bogotá, Colombia). Main areas of interest include e-Health and wireless personal communications. She worked on implementing Croatia's Central Health Information System.



Ramjee Prasad, Fellow IEEE, IET, IETE, and WWRF, is a Professor of Future Technologies for Business Ecosystem Innovation (FT4BI) in the Department of Business Development and Technology, Aarhus University, Herning, Denmark. He is the Founder President of the CTIF Global Capsule (CGC). He is also the Founder Chairman of the Global ICT Standardization Forum for India, established in 2009. He has been honored by the University of Rome "Tor Vergata", Italy as a Distinguished Professor of the Department of Clinical Sciences and Translational Medicine on March 15,

2016. He is an Honorary Professor of the University of Cape Town, South Africa, and the University of KwaZulu-Natal, South Africa. Dr. Prasad has received Ridderkorset of Dannebrogordenen (Knight of the Dannebrog) in 2010 from the Danish Queen for the internationalization of top-class telecommunication research and education. He has received several international awards such as IEEE Communications Society Wireless Communications Technical Committee Recognition Award in 2003 for making contribution in the field of "Personal, Wireless and Mobile Systems and Networks", Telenor's Research Award in 2005 for impressive merits, both academic and organizational within the field of wireless and personal communication, 2014 IEEE AESS Outstanding Organizational Leadership Award for: "Organizational Leadership in developing and globalizing the CTIF (Center for TeleInFrastruktur) Research Network", and so on. He has been the Project Coordinator of several EC projects namely, MAGNET, MAGNET Beyond, eWALL. He has published more than 50 books, 1000 plus journal and conference publications, more than 15 patents, over 140 Ph.D. Graduates and a larger number of Masters (over 250). Several of his students are today worldwide telecommunication leaders themselves.