Health Care in the Cyberspace: Medical Cyber-Physical System and Digital Twin Challenges

Jaime Ibarra Jimenez, Hamid Jahankhani and Stefan Kendzierskyj

Abstract Cyber-Physical Systems and Digital Twins are commonly used today in the industrial sector, and the healthcare sector is keen to implement these technological solutions to enhance their capabilities and offer better services for patient care provision. In fact, the adoption of Wireless Body Area Networks (WBAN) based on IoT along with cloud computing systems has led to the development of new methodologies to monitor and treat patients. However, the adoption of the new technologies comes with several challenges in terms of performance and security. Considering that, WBAN can be wearable or implanted under the skin, and the overall concept leads to several cybersecurity challenges that would require deeper investigation. This chapter presents an analysis of the impact that WBAN has on health care. It also provides some definitions of Medical Cyber-Physical Systems (MCPSs) and Digital Twins along with technological enablers such as cloud and IoT.

Keywords Digital twin · Medical Cyber-Physical system · Internet of things · Wireless body area networks · Biohacking · Personal health information · MCPS · WBAN · VM · Hypervisor

1 Introduction

Adoption of Cyber-Physical Systems (CPS) is gaining pace among most of industrial organisations and this trend is also being observed in the healthcare sector. *Medical Cyber-Physical Systems* (MCPS) is defined as critical, networked, distributed and context-aware systems of devices used in medicine. Therefore, MCPSs connect the physical and digital environment through network connectivity along with embedded

J. I. Jimenez (✉) · H. Jahankhani · S. Kendzierskyj
Northumbria University, London, London, Greater London, UK
e-mail: jaime.jimenez@northumbria.ac.uk

H. Jahankhani
e-mail: hamid.jahankhani@northumbria.ac.uk

S. Kendzierskyj
e-mail: stefan.kend@gmail.com

M. Farsi et al. (eds.), *Digital Twin Technologies and Smart Cities*,
Internet of Things, https://doi.org/10.1007/978-3-030-18732-3_6

software. Likewise, Digital Twin represents the digitalisation of physical devices and artefacts. This technology has been used in industry, allowing it to simulate physical environments and specific machinery pieces in order to make decisions and assess risks in virtual environments prior to its implementation. This is the similar within the context of health care. Patients' body and physiognomy data are monitored on a real-time 24/7 basis with a view to provide more informed and real-time relevant healthcare responses.

Even though the Digital Twin is not implemented fully yet in medical setting, it is a topic that deserves further investigation, opening numerous challenges and research directions. It is an emerging engineering paradigm, which could allow healthcare data-driven practices such as delivering customised 3D printing prosthesis to be applied for surgical practices for instance. A Digital Twin in health care would take the concept of MCPS to a higher level. This can be viewed as a step closer to implementation of real smart city. The term 'Digital Twin' connects the physical and digital world, allowing users to visualise information of interest, on computers, mobile devices or even in holographic projections. The connectivity in Digital Twins, irrespective of the application context is enabled using sensory systems such as the ones used in embedded systems and Internet of Things (IoT). The concept of Digital Twin has been applied by NASA for the development and monitoring of aerospace vehicles.

This paper comprehensively and critically analyses the challenges that MCPSs and Digital Twins generate with a focused view on performance and security. Society is facing an era of an interconnected world, a 'Cyberspace', where devices, data, people, 'everything' are interconnected. Therefore, there is a need to conduct research on cutting-edge technologies prior to their design, configuration, implementation, monitoring and maintenance. The rest of the paper is organised as follows: Sect. 2 provides a brief discussion on MCPSs and Digital Twins. Section 3 analyses the impacts of Wireless Body Area Networks (WBAN) in health care. Section 4 discusses the challenges of MCPSs and Digital Twins in terms of performance, security and privacy. Finally, Sect. 5 concludes this chapter and suggests further research.

2 Medical Cyber-Physical Systems and Digital Twins

2.1 Medical Cyber-Physical Systems

MCPSs can be defined as intelligent systems related to medical devices [1] regardless of where they are being used (within hospitals, clinics or via wearable devices (see Sect. 3 regarding WBAN)). MCPSs are interconnected in the cyberspace using different networking protocols, frameworks and standards and are being considered in some countries such as Australia and UK as part of their Critical National Infrastructure (CNI). In addition, they are processed and manipulated via embedded software applications and monitored by caregivers. CPSs, which have been implemented in

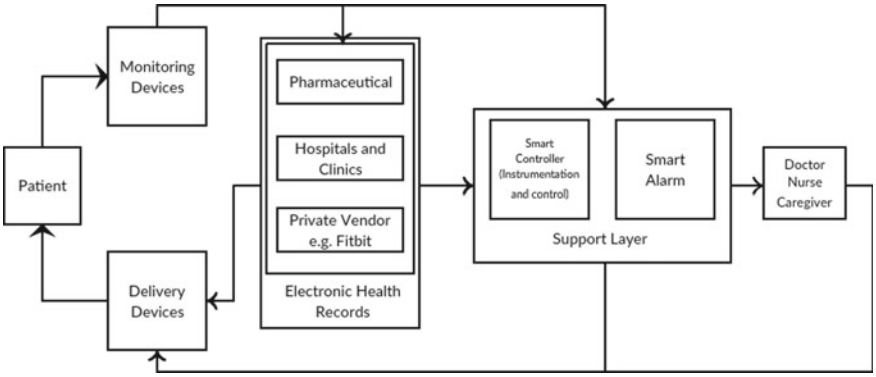

Fig. 1 Overview of a medical cyber-physical system, drawn from data provided in [1]

other sectors, utilised electronic sensors connected to Programmable Logic Controllers (PLCs) for sending physical information to customised applications, allowing operators to make decisions over their mechatronic infrastructures. The main difference in the medical CPS setting would be that sensors are allocated within medical devices connected to computer networks or used daily by patients through wearable devices (e.g., smartwatches and smartphones).

The values measured by sensors are triggered to transmit data in the following scenarios: (1) Within hospitals, communications can be triggered through Wireless Sensor Networks (WSN). (2) Using wearable devices, sensors send relevant information to applications installed in mobile devices through other wireless technologies (i.e., Bluetooth, ZigBee and radio frequency). Both cases offer a real-time monitoring while doctors can immediately evaluate any threats that can compromise a patient's health status [2]. The information can be available at Electronic Health Records (EHR) by accessing any administrative entity such as hospitals or clinics, pharmaceutical stores or private entities. These data are generally allocated in cloud computing systems and thanks to this technology, patients have faster access and better access rights to their health information compared to caregivers. One curious feature of MCPSs is the implementation of decision support devices formed by electronic and instrumented circuits which can trigger an alarm when an abnormal behaviour is observed with the patient health status. The support layer allows caregivers to make decisions in order to enhance the patient status [1]. In this architecture, the devices can be divided into two categories: monitoring devices used as sensors and delivery devices such as actuators which get modified according to the caregiver decisions (please see Fig. 1).

In addition, the research from Kocabas et al. [3] provides a general MCPS architecture divided into four layers, which are illustrated in Fig. 2.

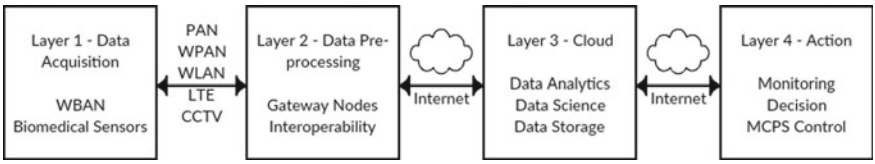

Fig. 2 Medical cyber-physical system architecture, drawn from data provided in [3]

2.1.1 Layer 1—Data Acquisition

Considered normally a Wireless Body Area Network (WBAN) using wireless protocols [4] in order to acquire interaction with the Internet using technologies such as ZigBee, WSNs, Bluetooth, Wireless Local Area Networks (WLAN), Wireless Personal Area Networks (WPAN), video surveillance systems and mobile networks [2, 4]. In the healthcare context, a WBAN uses biomedical sensors placed in different parts of the body and can be either wearable or implanted under the skin [5], allowing a real-time monitoring of the patient's health status such as blood pressure or body temperature, for instance.

2.1.2 Layer 2—Data Preprocessing

Currently, sensors have low computational power and are limited in hardware resources. Due to the high amounts of data gathered, it must be transmitted to a more sophisticated device prior to sending it throughout the Internet [2] in order to adapt the packet to traditional TCP/IP networks. Sensors require a gateway node (which acts as a concentrator) using a wireless communication. The concentrator allows these wearables or implanted devices to enhance their data concentration capabilities in order to transmit the information to cloud servers [6]. Likewise, the cloudlet has similar features compared to the concentrator; however, it is applied for more powerful devices, e.g., a smartphone. Typically, a cloudlet has a dedicated Internet connection and is configured from a dedicated computer as well [7, 8].

2.1.3 Layer 3—Cloud System

The cloud allows users such as doctors, nurses or patients to access Personal Health Information (PHI). It can be used to perform data analytics to predict possible required changes based on a patient's condition with a view to prevent severe health illnesses, facilitating decision support for caregivers [9, 10]. Furthermore, one of the most important capabilities that cloud presents is data storage; however, the acquisition of accurate diagnosis requires long-term monitoring, and hence the requirement of stronger cloud storage security mechanism to secure the collected data for long periods of time [11, 12].

2.1.4 Layer 4—Action

The two main objectives of this layer are to provide either 'active' or 'passive' actions. In the *active action*, an actuator is used to elaborate changes within the MCPS. For instance, a doctor sends an order to elevate the dose of medicine in the serum or the usage of robotic arms for *surgery assistance* [13]. Meanwhile, the *passive action* provides the opportunity of a better visualisation of the current state of the patient, allowing caregivers decision support.

2.2 Digital Twins

Digital Twin refers to the virtualisation of physical assets to monitor assets. This is enabled through electronic sensors communicating with each other using customised application software and are capable of controlling the digitised assets [14].

Nowadays, modern engineering technologies have immensely contributed to the evolution of healthcare services. In fact, the usage of mathematical models for processing of higher volumes of 'biodata' enables effective medical interventions. Some early prototypes of digital twins were realised in the ESB Logistics Learning Factory, which using a cloud-based software application a multidimensional data along with an information model were built [15]. By reading patients sensory data, even at the molecular level a 'digital' representation of a patient—a 'virtual patient' can be created. Therefore, the Digital Twin can be a platform to exhibit cutting-edge engineering solutions within health care. Many universities are training and preparing students in clinical technology, whilst doctors are working along with engineers from a wide range of backgrounds to enhance the functionality of contemporary medical practice [16].

In the wider context, Digital Twins are used to monitor the performance of artefacts and pieces of machinery in order to perform preventative maintenance. In fact, digitalisation of individual artefacts seems a straightforward task since it is based on the instrumentation of electronic sensors placed across the artefact. Besides, such artefacts have a unique shape after its manufacturing, making such instrumentation easier. In health care, however, the human structure is more complex due to the constant molecular and physiological changes throughout the body, making it very complex to extract precise molecular data. Unfortunately, Digital Twin seems a complex challenge, even though digital models of individuals' genetic, biochemical, physiological and behavioural features have already been implemented [17].

3 Impact of WBAN in Health Care

WBANs provide an extensive range of monitoring applications for different contexts such as health care, military, sports and video gaming, among others [18]. The health-

care sector is keen to adopt such a technology to enhance medical capabilities and to consequently improve the lifestyle of the human being. WBANs provide continuous health monitoring of patients allowing caregivers an easier decision support in order to send the necessary medical prescription or treatment without the requirement of patients' physical presence at clinics and hospitals [5]. WBANs used in health care consists of multiple *biomedical sensors*, which can be either wearable (e.g., fitness watches) or implanted under the human skin like electronic chips created with nanotechnology. Implanting chips under skin is referred to as '*biohacking*', a term that would be in discussion for the coming years with a focused consideration of the relevant cybersecurity challenges (e.g., cyber espionage). Some applications of WBANs are discussed in the following subsections.

3.1 Cardiovascular Application

The research from [19] shows that more than 20 million people suffer from cardiovascular diseases. The usage of WBANs allows to monitor users' health state remotely and on a real-time basis. Therefore, healthcare service providers can immediately prepare a preventive patient treatment plan when any abnormal information is measured by the sensor nodes.

3.2 Body Temperature

Body temperature is one of the most common physiological features measured through human activity monitoring [20]. It allows caregivers to detect medical stress that may lead to diverse health conditions based on the variation of corporal temperature. Such conditions include stroke, heart attacks and shock. Measuring body temperature is valuable to deter the physiological condition of a patient as well as for other care such as activity pattern monitoring [21, 22] and corporal heat harvesting [23].

3.3 Blood Glucose Monitoring

One of the current serious chronic health diseases throughout the world is diabetes. This disease has been increasing because of higher levels of sedentary habits given by comfortable options to the human being without having appropriate exercise. If diabetes is not treated properly and on time, it can cause serious complications such as blindness, stroke, kidney disease, heart disease and high blood pressure [24]. WBANs allow the continuous monitoring of patients' blood glucose level to provide information on healthier habits for food consumption and frequency of body exercise.

Currently, the measurement of blood glucose level can be done by means of a test strip pricking a finger. However, biomedical sensors can be implanted in a body to monitor the glucose level throughout the day. Using WBAN sensors, caregivers inject the necessary amount of insulin in patients using the actuator nodes within MCPS when the glucose level reaches a threshold [25].

3.4 Stress Monitoring

Stress leads to numerous diseases. It can lead to negative psychological illnesses such as anxiety, decreased patient satisfaction and depression [26]. Accelerated lifestyles in industrialised countries such as United States and Great Britain have increased stress levels among the population leading to negative consequences such as alcoholism and addictive smoking [27]. WBANs provide real-time monitoring of stress levels in individuals supporting physicians for appropriate treatments [28]. Modern smartphones can provide this service and the same platform can authenticate the users' fingerprints for privacy and security purposes.

3.5 Rehabilitation and Therapy

The main goal of rehabilitation is to support patients in restoring their physical and functional capabilities back to normal conditions, when they get dismissed from a hospital [29, 30]. Rehabilitation is a dynamic process in which necessary techniques are used to enhance the physical behaviour of a patient to his/her ideal physiological state. Therefore, tracking and detecting human mobility becomes an essential factor for home-based therapy treatments. Wearing or having implanted biomedical sensors, data fusion and real-time feedback for patients along with virtual reality environments are examples of techniques that could be used for rehabilitation [30].

4 Challenges in Medical Cyber-Physical Systems and Digital Twins

Even though these technologies are still in development and under specific research, it is suggested to study the challenges mentioned below in order to take the necessary actions to assure the appropriate balance between security, privacy and performance. The next subsections discuss some challenges on the studied technologies including cloud systems and Internet of things.

4.1 High Assurance Software

Software deployment is playing an increasingly important role when developing new MCPSs. Actually, the functionality of modern devices are software based and comparing with some years ago, when some functions were traditionally implemented in hardware have been replaced by software solutions. Thus, the higher demand for developing software offers confidentiality, integrity, reliability and ease of use to deploy safe and effective MCPSs and digital twins in the future. It is required to balance effectiveness in software engineering along with secure coding to avoid disruptions in healthcare organisations due to time consumption given by software patching.

4.2 Certification and Regulatory Issues

MCPSs and digital twins in health care are safety-critical systems and they must be prone to regulatory observation through certification or approval processes. Traditional regulatory regimes used by the Food and Drugs Association (FDA) to approve medical devices and medicines are becoming inappropriate due to the complexity of these cutting-edge technologies [31]. The FDA currently requires study cases as elements of the documentation submitted for future approval assurance considering regulatory modifications, for instance, the infusion pump improvement initiative [32]. Therefore, it is expected that similar or even specific and complex requirements will be demanded for the approval of MCPSs and digital twins, in general.

In addition, other important part of this challenge is software certification and methods to make it part within the regulatory approval process for the deployed device. Most of the medical devices possess large amounts of embedded software performing various monitoring and care delivery tasks. Considering that medical devices are becoming more complex and interconnected, it should become more evident for the requirement of certification and regulation at early design stages. This can be done in two ways: (1) The ‘design for verification’ approach [33] can support on better verification techniques including scalability and easier verification evidence generation; (2) model-based generative techniques can be used to perform verification early in the design and then extend the guarantees provided by the performed verification prior to its implementation through code verification.

4.3 Security and Privacy

These technologies provide interoperability capabilities, allowing to connect and transfer information through multiple platforms, acquiring functionalities that previously were never possible to appreciate; however, they also open new concerns

in terms of security and privacy [34]. An attacker able to penetrate MCPSs or digital twin software has the potential and capability to harm or terminate the life of the patient by reprogramming devices [35]. There are four types of targets when attacking these systems [36].

- *Patient*: The attacker can target directly to the patient's health. It means attacking to the sensing, processing communication and treatment delivery aspects of the MCPS. For instance, reprogramming an infusion pump to provide a larger amount of medicine than the prescribed.
- *Data*: An attacker can access highly confidential and sensitive data belonging to the patient or the involved ones in the medical treatment. The loss of data privacy can lead to potential blackmailing, computer abuse and discrimination [37].
- *Device*: An attacker can perform a Denial of Service (DoS) attack on the MCPS, or also be part of it (e.g., wearable or implanted device), and deploy it to belong to a huge botnet in order to perform robust Distributed Denial of Service attacks (DDoS). Moreover, this can also result in privacy loss over systems that should be designed to fail open as suggested [38].
- *Institution*: The goal of a cyberattack is to compromise the interaction between the MCPS and the corporate network of the institution in order to obtain unauthorised access or at larger scale, patient data theft or network operational information infiltration.

Recent years have been a great issue for medical devices in terms of security addressed to several devices such as wearable, implantable [36, 38] or interoperable devices [37]. Nonetheless, in most of the cases, the focus is addressed to specific features of MCPS security like encrypted communication and effective access controls. In addition, the main challenge of deploying secure MCPS involves flexible and open solutions while mitigating the following issues: (1) heterogeneity of systems, (2) improving usability (even transparency) of security solutions developed and (3) considering safety implications of security solutions and decisions including the mitigation of human error and insider threats.

4.4 Challenges in Involved Systems

As studied in previous sections, thanks to the usage of WBAN, healthcare systems show dependency during the communication between patients and caregivers through cloud and IoT-based systems. The following subsections will discuss some challenges on the mentioned ones.

4.4.1 Cloud Computing

Cloud services are commonly available to users through the Internet (e.g., web browser) [39], using standard protocols and mechanisms for its communication [40].

External cloud communications are similar to any other communications over the Internet (i.e., traditional data centres). Therefore, the challenges faced by the cloud are the same as conventional IT solutions [41], including denial of service, Man-In-The-Middle (MITM), eavesdropping, IP-spoofing and masquerading attacks [42, 43]. Traditionally, these challenges are solved as the common ones such as implementation of Secure Socket Layer (SSL), IPSec, cryptographic algorithms, intrusion detection and prevention systems and digital certificates [42, 44].

Users and system administrators must be aware that cloud computing systems result in the sharing of computational, storage and network infrastructure resources [45], leading it to third-party risks. Shared network components allow attackers the possibility to perform horizontal privilege escalation techniques and the exploitation of other systems prior to the main target [46]. Commonly, users on cloud environments are granted with superuser privileges for the main purpose of managing their Virtual Machines (VMs) [47], and therefore attackers are motivated to acquire essential components from the system like IP and MAC addresses and perform malicious actions such as sniffing and spoofing over the real network.

The two main components of cloud are virtualisation and storage. Virtualisation allows the sharing of the same physical resources with multiple system environments. A separate VM is isolated for each user providing a virtual operating system, and the module in charge of managing the VMs along with the assigned resources is the VM Monitor (VMM) or hypervisor, allowing to run multiple operating systems at the same time [48]. Security challenges in terms of virtualization involve VM image sharing [46], VM isolation [40, 49], VM migration [46] and hypervisor issues where a compromised one can put all the VMs under the attacker's control [50]. Cloud system providers do not deliver to users full control over data, and users experience some control levels only on the VMs [51]. The fact that users do not have control over data belonging to the organisation results on significant third-party risks like data breaches. Moreover, the storage present in cloud environments shows challenges in terms of data privacy and integrity because data present in cloud is more prone to risks attempting against the confidentiality, integrity and availability compared to traditional data centre architectures [52]. In addition, data backup is an important element when having cloud systems and it demands to be secured against unauthorised access and illegal manipulation [40]. Generally, the access to cloud systems are done via web applications such as a Google Chrome for instance, and therefore, the requirement to protect these from vulnerabilities published by the OWASP [53].

4.4.2 Internet of Things

IoT is growing steadily and the medical sector is expected to experience an expanded adoption of it, creating cutting-edge eHealth IoT devices along with embedded applications. The challenges that IoT has for a secure healthcare networked environment include the computational limitations that devices present with their low-speed processors, memory and energy limitations. IoT networks present challenges in terms

of scalability because of its high acquisition, along with the required compatibility with known network protocols. Medical devices are connected through several wireless protocols such as Zigbee, WiFi, GSM, WiMax, 6LowPAN, 3G/4G and soon 5G networks. The requirement of having a cross-platform system allowing IoT devices communicate with IP networks and making it part of known systems is a challenge as well, and another important aspect is the capability of producing tamper-resistant packets [54]. In-transit and stored health information can be eavesdropped or manipulated by an attacker. Some attacks include DoS attacks causing interruption, data breaches affecting the patient's privacy, data tampering and modifying the behaviour of sensing and delivering devices [55, 56].

5 Conclusion and Further Research

In this paper, the MCPSs and digital twins were studied and analysed as new incoming technologies that enhance steadily the capabilities of healthcare services. Medicine is integrating the usage of information technology (i.e., EHRs) and is keen to involve operational technology as well to raise the possibilities for a better lifestyle to patients. Even though the digital twin is not yet implemented in medicine, it is a topic that is worth to undertake research addressed to this field. WBAN is allowing to develop sophisticated MCPSs and would be of great support to deploy digital twin solutions as well; however, it also requires a deeper research in terms of the mentioned security and privacy challenges considering the integration of WBAN with IoT networks and cloud environments. Healthcare organisations and providers are keen to enhance their security maturity, hence the need for researchers to focus on the different systems and architectures in order to develop appropriate measures for this cutting-edge technology. In fact, it is recommended to critically analyse the challenges of big data platforms as well, and the possibility to deploy customised systems addressed to the vulnerability assessment of MCPSs in order to deploy the necessary security updates and bug fixes. Health care must be part of the CNI for all countries due to the level of extortion that a cyberattack can cause, leading to life or death decisions that caregivers could make during a system disruption. Therefore, the requirement to develop the next generation of security researchers to enhance the posture and the assurance of system and patient data.

References

1. Lee, I., Sokolsky, O., Chen, S., Hatcliff, J., Jee, E., Kim, B., King, A., Mullen-Fortino, M., Park, S., Roederer, A., Venkatasubramanian, K.K.: Challenges and research directions in medical cyber–physical systems. Proc. IEEE **100**(1), 75–90 (2012)
2. Movassaghi, S., Abolhasan, M., Lipman, J., Smith, D., Jamalipour, A.: Wireless body area networks: a survey. IEEE Commun. Surv. Tutor. **16**(3), 1658–1686 (2014)

3. Kocabas, O., Soyata, T., Aktas, M.K.: Emerging security mechanisms for medical cyber physical systems. IEEE/ACM Trans. Comput. Biol. Bioinform. **13**(3), 401–416 (2016)
4. Cavallari, R., Martelli, F., Rosini, R., Buratti, C., Verdone, R.: A survey on wireless body area networks: technologies and design challenges. IEEE Commun. Surv. Tutor. **16**(3), 1635–1657 (2014)
5. Anwar, M., Abdullah, A.H., Qureshi, K.N., Majid, A.H.: Wireless body area networks for healthcare applications: an overview. Telkomnika **15**(3), 1088–1095 (2017)
6. Babu, S., Chandini, M., Lavanya, P., Ganapathy, K., Vaidehi, V.: Cloud-enabled remote health monitoring system. In: 2013 International Conference on Recent Trends in Information Technology (ICRTIT), pp. 702–707. IEEE (2013)
7. Soyata, T., Muraleedharan, R., Funai, C., Kwon, M., Heinzelman, W.: Cloud-vision: real-time face recognition using a mobile-cloudlet-cloud acceleration architecture. In: 2012 IEEE Symposium on Computers and Communications (ISCC), pp. 000059–000066. IEEE (2012)
8. Powers, N., Alling, A., Osolinsky, K., Soyata, T., Zhu, M., Wang, H., Ba, H., Heinzelman, W., Shi, J., Kwon, M.: The cloudlet accelerator: bringing mobile-cloud face recognition into real-time. In: 2015 IEEE Globecom Workshops (GC Wkshps), pp. 1–7. IEEE (2015)
9. Mao, Y., Chen, Y., Hackmann, G., Chen, M., Lu, C., Kollef, M., Bailey, T.C.: Medical data mining for early deterioration warning in general hospital wards. In: 2011 IEEE 11th International Conference on Data Mining Workshops (ICDMW), pp. 1042–1049. IEEE (2011)
10. Kocabaş, Ö., Soyata, T.: Medical data analytics in the cloud using homomorphic encryption. In: Handbook of Research on Cloud Infrastructures for Big Data Analytics, pp. 471–488. IGI Global (2014)
11. Nalinipriya, G., Kumar, R.A.: Extensive medical data storage with prominent symmetric algorithms on cloud-a protected framework. In: 2013 IEEE International Conference on Smart Structures and Systems (ICSSS), pp. 171–177. IEEE (2013)
12. Hani, A.F.M., Paputungan, I.V., Hassan, M.F., Asirvadam, V.S., Daharus, M.: Development of private cloud storage for medical image research data. In: 2014 International Conference on Computer and Information Sciences (ICCOINS), pp. 1–6. IEEE (2014)
13. Barbash, G.I., Glied, S.A.: New technology and health care costs—the case of robot-assisted surgery. N. Engl. J. Med. **363**(8), 701–704 (2010)
14. Brenner, B., Hummel, V.: Digital twin as enabler for an innovative digital shopfloor management system in the ESB logistics learning factory at Reutlingen-university. Procedia Manuf. **9**, 198–205 (2017)
15. Bruynseels, K., Santoni de Sio, F., van den Hoven, J.: Digital twins in health care: ethical implications of an emerging engineering paradigm. Front. Genet. **9**, 31 (2018)
16. Uhlemann, T.H.J., Schock, C., Lehmann, C., Freiberger, S., Steinhilper, R.: The digital twin: demonstrating the potential of real time data acquisition in production systems. Procedia Manuf. **9**, 113–120 (2017)
17. Uhlemann, T.H.J., Lehmann, C., Steinhilper, R.: The digital twin: realizing the cyber-physical production system for industry 4.0. Procedia CIRP **61**, 335–340 (2017)
18. Qureshi, K.N., Abdullah, A.H., Anwar, R.W.: The evolution in health care with information and communication technologies. In: Proceeding of 2nd International Conference of Applied Information and Communications Technology-2014. Elsevier, Oman (2014)
19. Ullah, S., Khan, P., Ullah, N., Saleem, S., Higgins, H., Kwak, K.S.: A review of wireless body area networks for medical applications (2010). arXiv:1001.0831
20. Mukhopadhyay, S.C.: Wearable sensors for human activity monitoring: a review. IEEE Sens. J. **15**(3), 1321–1330 (2015)
21. Parkka, J., Ermes, M., Korpipaa, P., Mantyjarvi, J., Peltola, J., Korhonen, I.: Activity classification using realistic data from wearable sensors. IEEE Trans. Inf Technol. Biomed. **10**(1), 119–128 (2006)
22. Winkley, J., Jiang, P., Jiang, W.: Verity: an ambient assisted living platform. IEEE Trans. Consum. Electron. **58**(2) (2012)
23. Leonov, V.: Thermoelectric energy harvesting of human body heat for wearable sensors. IEEE Sens. J. **13**(6), 1–8 (2013)

24. W H Organization. Global report on diabetes (2016)
25. Schwiebert, L., Gupta, S.K., Weinmann, J.: Research challenges in wireless networks of biomedical sensors. In: Proceedings of the 7th Annual International Conference on Mobile Computing and Networking, pp. 151–165. ACM (2001)
26. Regehr, C., Glancy, D., Pitts, A., LeBlanc, V.R.: Interventions to reduce the consequences of stress in physicians: a review and meta-analysis. J. Nerv. Ment. Dis. **202**(5), 353–359 (2014)
27. Cassel, J.: Physical illness in response to stress. In: Social Stress, pp. 189–209. Routledge (2017)
28. Milenković, A., Otto, C., Jovanov, E.: Wireless sensor networks for personal health monitoring: issues and an implementation. Comput. Commun. **29**(13–14), 2521–2533 (2006)
29. Hadjidj, A., Souil, M., Bouabdallah, A., Challal, Y., Owen, H.: Wireless sensor networks for rehabilitation applications: challenges and opportunities. J. Netw. Comput. Appl. **36**(1), 1–15 (2013)
30. Zhou, H., Hu, H.: Human motion tracking for rehabilitation—A survey. Biomed. Signal Process. Control **3**(1), 1–18 (2008)
31. High Confidence Software and Systems Coordinating Group, B High-confidence medical devices: Cyber-physical systems for 21st century health care. A research and development needs report, NCO/NITRD (2009)
32. Goodman, C.: Food and Drug Administration Center for Devices and Radiological Health (1988)
33. Alexander, K., Clarkson, P.J.: Good design practice for medical devices and equipment, Part II: design for validation. J. Med. Eng. Technol. **24**(2), 53–62 (2000)
34. Ackerman, M.J., Filart, R., Burgess, L.P., Lee, I., Poropatich, R.K.: Developing next-generation telehealth tools and technologies: patients, systems, and data perspectives. Telemed. e-Health **16**(1), 93–95 (2010)
35. Halperin, D., Heydt-Benjamin, T.S., Fu, K., Kohno, T., Maisel, W.H.: Security and privacy for implantable medical devices. IEEE Pervasive Comput. **1**, 30–39 (2008)
36. Arney, D., Venkatasubramanian, K.K., Sokolsky, O., Lee, I.: Biomedical devices and systems security. In: 2011 Annual International Conference of the Engineering in Medicine and Biology Society, EMBC, pp. 2376–2379. IEEE (2011)
37. Venkatasubramanian, K.K., Gupta, S.K.S., Jetley, R.P., Jones, P.L.: Interoperable medical devices. IEEE Pulse **1**(2), 16–27 (2010)
38. Denning, T., Fu, K., Kohno, T.: Absence makes the heart grow fonder: new directions for implantable medical device security. In: HotSec (2008)
39. Kifayat, K., Merabti, M., Younis, Y.A.: Secure Cloud Computing for Critical Infrastructure: A Survey (2012)
40. Subashini, S., Kavitha, V.: A survey on security issues in service delivery models of cloud computing. J. Netw. Comput. Appl. **34**(1), 1–11 (2011)
41. Ficco, M., Rak, M.: Stealthy denial of service strategy in cloud computing. IEEE Trans. Cloud Comput. **3**(1), 80–94 (2015)
42. Sankar, K., Kannan, S., Jennifer, P.: On-demand security architecture for cloud computing. Middle-East J. Sci. Res. **20**(2), 241–246 (2014)
43. Liu, B., Bi, J., Vasilakos, A.V.: Toward incentivizing anti-spoofing deployment. IEEE Trans. Inf. Forensics Secur. **9**(3), 436–450 (2014)
44. Ali, M., Khan, S.U., Vasilakos, A.V.: Security in cloud computing: opportunities and challenges. Inf. Sci. **305**, 357–383 (2015)
45. Fernandes, D.A., Soares, L.F., Gomes, J.V., Freire, M.M., Inácio, P.R.: Security issues in cloud environments: a survey. Int. J. Inf. Secur. **13**(2), 113–170 (2014)
46. Hashizume, K., Rosado, D.G., Fernndez-Medina, E., Fernandez, E.B.: An analysis of security issues for cloud computing. J. Internet Serv. Appl. **4**(1), 1–13 (2013)
47. Bilal, K., Malik, S.U.R., Khan, S.U., Zomaya, A.Y.: Trends and challenges in cloud data centers. IEEE Cloud Comput. Mag. **1**(1), 10–20 (2014)
48. Neng-Hai, Y., Hao, Z., Xu, J., Zhang, W., Zhang, C.: Review of cloud computing security. Acta Electron. Sinica **41**(2), 371–381 (2013)

49. Gonzalez, N., Miers, C., Redigolo, F., Simplicio, M., Carvalho, T., Näslund, M., Pourzandi, M.: A quantitative analysis of current security concerns and solutions for cloud computing. J. Cloud Comput. Adv. Syst. Appl. **1**(1), 11 (2012)
50. Szefer, J., Keller, E., Lee, R.B., Rexford, J.: Eliminating the hypervisor attack surface for a more secure cloud. In: Proceedings of the 18th ACM Conference on Computer and Communications Security, pp. 401–412. ACM (2011)
51. Wei, L., Zhu, H., Cao, Z., Dong, X., Jia, W., Chen, Y., Vasilakos, A.V.: Security and privacy for storage and computation in cloud computing. Inf. Sci. **258**, 371–386 (2014)
52. Wang, C., Wang, Q., Ren, K., Cao, N., Lou, W.: Toward secure and dependable storage services in cloud computing. IEEE Trans. Serv. Comput. **5**(2), 220–232 (2012)
53. Owasp.org. https://www.owasp.org/images/7/72/OWASP_Top_10-2017_%28en%29.pdf (2018). Accessed 31 Dec 2018
54. Islam, S.R., Kwak, D., Kabir, M.H., Hossain, M., Kwak, K.S.: The internet of things for health care: a comprehensive survey. IEEE Access **3**, 678–708 (2015)
55. Zia, T., Zomaya, A.: Security issues in wireless sensor networks. In: Proceedings of the IEEE International Conference on Systems and Networks Communications, October 2006, p. 40 (2006)
56. Wang, Y., Attebury, G., Ramamurthy, B.: A survey of security issues in wireless sensor networks (2006)