An Investigation of Vulnerabilities in Internet of Health Things

Saifur Rahman[1(✉)], Tance Suleski[1], Mohiuddin Ahmed[1], and A. S. M. Kayes[2]

[1] School of Science, Edith Cowan University, Joondalup, WA 6027, Australia
{saifurb,tsuleski}@our.ecu.edu.au, mohiuddin.ahmed@ecu.edu.au

[2] Department of Computer Science and Information Technology, La Trobe University, Melbourne, VIC 3086, Australia
a.Kayes@latrobe.edu.au

Abstract. Medical devices are the machines or instruments that play a vital role in diagnosis or treatment for patients in a healthcare ecosystem. As technologies advances so are these medical devices, and with time they are getting smarter and interconnected to themselves and other devices. These smarter devices attract attracts hackers to launch cyber-attack against these machines targeting vulnerabilities that exist within them. In this paper, we provide a brief description of medical devices in relation to different regulatory bodies, through which we try to understand the need to make the medical device safe for the users. We explore the vulnerabilities of medical devices and how they may be exploited to infiltrate the full healthcare system and other devices in the network. The paper covers three recent incidents of medical device vulnerabilities and explores the concept of blockchain that may be used to limit the vulnerabilities and their limitation. To ensure patient safety and privacy, it is essential that all relevant bodies including manufacturers, regulators, healthcare providers, etc. understand the risk and take proper steps to limit the threats.

Keywords: IoHT · Healthcare · Cybersecurity · Medical device · Vulnerability

1 Introduction

The devices intended to be used for medical purposes, to benefit patients by providing support to health care personnel for treatment, diagnosis so that patients can overcome sickness and disease can be termed as a Medical device. They are defined and regulated differently from one country or region to another country or region. This is due to different regulatory bodies in different countries and regions oversee their distribution. Medical devices have a risk classification level [25] associated with them, which allows regulatory bodies to scrutinize different medical devices differently and establish different levels of control. Regulatory bodies assess the medical device based on their safety towards maintaining

H. Jin et al. (Eds.): CROWNCOM 2021/WiCON 2021, LNICST 427, pp. 296–306, 2022.
https://doi.org/10.1007/978-3-030-98002-3_22

patient and facilitator safe. They also consider cyber threats [2] (See Fig. 1) in consideration when providing approval and follow different standards based on country, region, risk levels such as ISO 14971, ISO 13485, IEC 62304, AAMI/UL 2800, etc. [5].

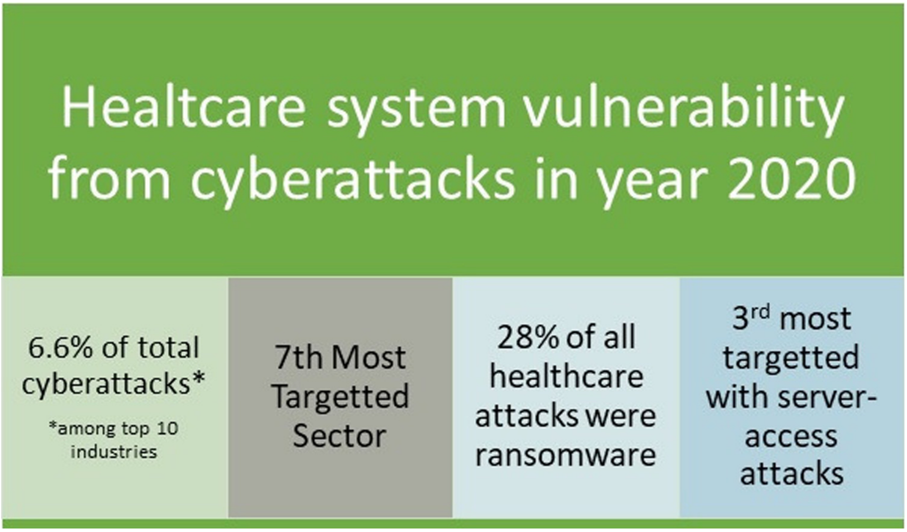

Fig. 1. Cyberattack on healthcare industry in year 2020.

As more and more devices are invented and developed, most of the devices are becoming smart medical devices generating and providing real-time data to health care professionals, for example, mySIgnals [7]. They are using state of the art software to improve the device performance and whose developments are regulated by regulating authority across the world. Smart devices are also generating in-depth diagnoses and report towards a better understanding of the cause of concern for patients. Patient's in interactions with smart medical devices are increasing day by day, similarly, the number of sensors, testing instruments, scanners, etc. evolving with the development of technological advances in miniaturization capacity of devices, computing power, and shifting towards wireless technology [6]. Due to the increasing usage of the Internet in the healthcare sector and state-of-the-art medical devices, cybercriminals are more than ever motivated to launch attacks on medical devices, and unfortunately in such a scenario, the result of the attack may even lead to loss of life. Compromised medical devices can change the way how the device operates, generate false readings from sensors and result in life-threatening situations for patients [11,12,14,16]. Manufacturers are guided to consider potential cyber threats and encouraged to limit the risk for the lifecycle of the medical device [3]. The risk and vulnerability of medical devices lie not only with connected devices but also with standalone devices. The weakness in technical and physical security controls of the device may be hardware or software-related. All these devices are at risk of being hacked (See Fig. 2) with unauthorized access and malware. Evolving nature of cyber threats should be addressed by the manufacturer of medical devices to address the security challenges of the present and potential future security threats [29,30] Systems, resources need to be managed in such a way that it provides efficient and effective medical devices to the end-users and constantly upgrading in such a way that it can combat threats with the help of device manufacturers, resulting in a quality and safe environment for patients and users of the medical devices. Organizations, especially health care providers at management level should have strategies to tackle the issue of medical device security issues.

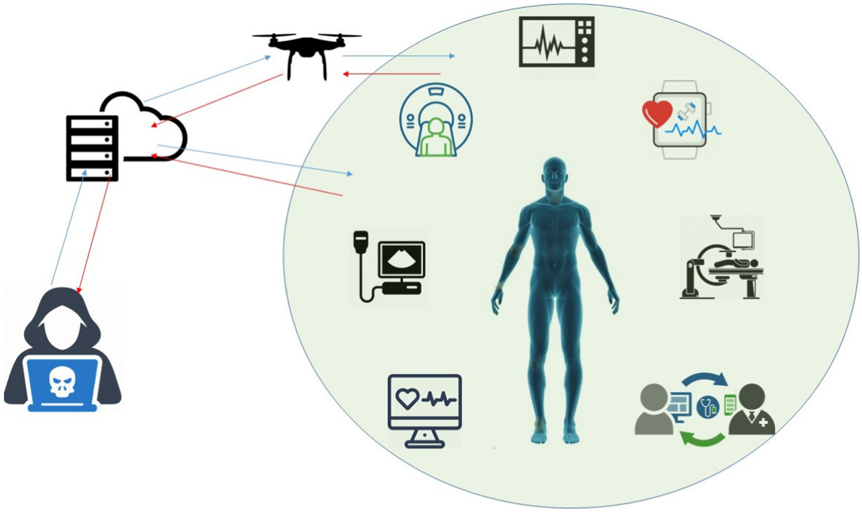

Fig. 2. Medical devices vulnerable to cyberattacks adapted from the Internet.

1.1 Paper Roadmap

The rest of the paper is organized as follows. Section 2 discusses the vulnerabilities found in digital healthcare and the critical analysis of medical device vulnerabilities. Section 3 highlights the recent incidents and motivations of cybercriminals. Section 4 discusses the solution trends for healthcare device cyber-attacks, notably the Blockchain. Section 5 concludes the paper followed by references.

2 Medical Device Vulnerability Analysis

As digitization and connectivity of medical devices are on the rise, these are devices are also vulnerable to following cyberattacks and bringing harm to patients Following Attacks are the ones most deadly to the healthcare ecosystem [5].

- Denial of service or therapy to patients.
- Directly alter the function of device and causing the patient harm.
- Loss of data and privacy of health data.
- Server Access attacks on healthcare device networks.
- Ransomware on medical devices.

All medical devices should pass through proper risk assessment and regulatory control before being deployed in the market. Following figure (See Fig. 3) shows some of the known cybersecurity vulnerabilities of medical device.

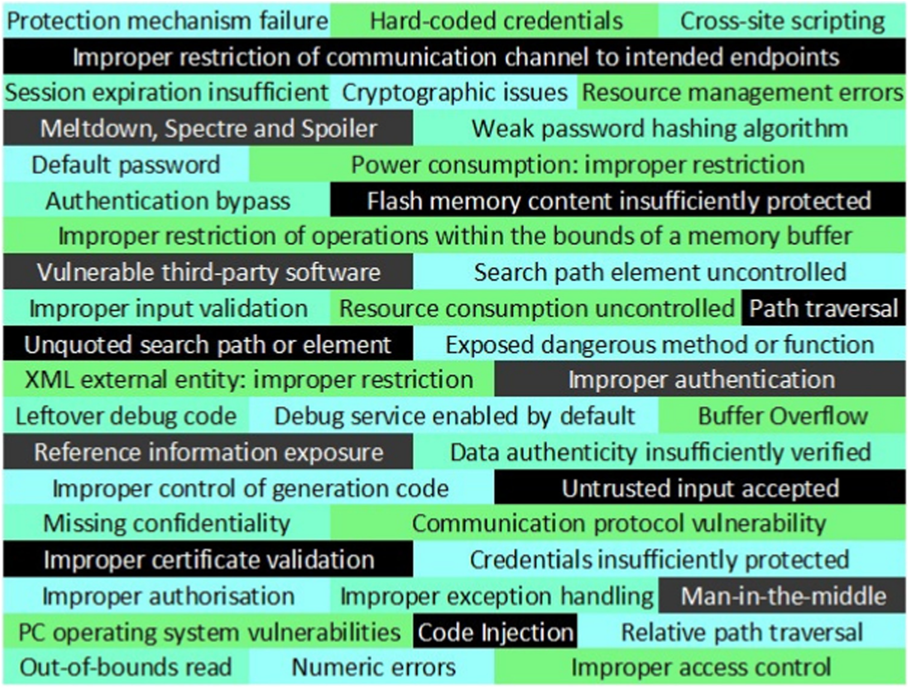

Fig. 3. Vulnerabilities of medical devices.

2.1 Vulnerability Exposure of Medical Devices

Medical devices falls victim to attacks due to vulnerabilities in them, which ranges from technical issues, management and human factors. These limitations contribute not only security threats to the medical devices itself but also on overall vulnerability of the health sector.

Information on Technical Specification: The technical information on working of the device through device manual, systems and their connectivity specification, and other vital data related to device is available not only from manufacturer also from certification body and patent databases. Which in turn provides opportunity for the attackers to reverse engineer [17] and find vulnerabilities of device for attack.

Legacy System and Software: When the device or the software becomes old, due to advancement in mode of cyberattack, it opens up security loop holes which were un-known before. This may also be due to unregulated system integration, misconfigured and incompatible system integration, mainly with third party software [18].

Patch and Software Updates: If the devices are not updated with latest patch [9] and software updates that are available, they provide opportunity for attackers to hack the system. Though it is recommended to upgrade as soon the software or patch is available, it becomes difficult from system administrator as the devices are linked with other devices and may affect their performance if not properly tested on compatibility with new updates.

Security Features: Some of the devices comes with very basic security features, such as continuous glucose level monitoring level machine [4], which can be easy attacked and compromised. Thus not only becomes vulnerable for themselves also other devices in the network.

Web Service Interface: For interfacing with an existing system web service [24] are popular choice, most of the time they are not secured and without proper authentication, leaving open doors for attackers.

Compromised Device: One compromised device may be used to attack other devices in the same network within the organization. Through malware and phishing schemes malicious scripts planted on devices to gain access to a particular device in a healthcare network. Which opens the backdoor for attacker to gain access other devices in the network [13].

Balance of safety and security: It is very difficult to balance safety of patients with the maximum cyber security protocols. In time of patient's emergency it may be difficult to follow all the practice and protocols for access control and encryption process in place, where time plays a vital role. This lapse opens up window of opportunity for attackers [19].

Limited Energy use: Many of the medical devices use very low or limited power and runs on battery [31]. Increased security protocols with many encryptions may actually reduce the battery life of the device [23], prompting the manufacturers not to use state of the art security features. As more communication, data transfer, system monitoring with use of micro controller is required more energy is consumed from batteries in the device. Limiting such activities may increase battery life but increases chance of security threats [19].

3 Motivation of Attacks and Recent Incidents

3.1 Attacker's Motivation

The motivation to exploit the medical devices and carry out an attack by attacker influenced by financial gain, state or national interest, sparking cyber terrorism, extract performance data of a device for corporate espionage, etc. [28]. Out of all the motivation factor money is the biggest motivator. The devices on hospitals and other medical facilities has lot of information, including sensitive personal information which attracts lot of attacker to extract the data and sell to potential buyers.

3.2 Recent Incidents

Sweyn Tooth Vulnerability [22] is a collection of 12 vulnerabilities and possible of more to be identified and released. It affects 7 different Bluetooth Low Energy (BLE) SoC manufacturers utilizing different models of software development kit (sdk). Medical devices from following BLE SoC manufacturer is said to be affected (See Fig. 4). The stated vulnerability allows an attacker to trigger deadlocks, buffer overflows, crashes or completely bypass the security from radio range, thus compromising the medical device.

GE Healthcare Clinical Information Central Stations and Telemetry Server [1] are exposed to vulnerabilities from using specific software version. These medical devices are used to monitor physiological parameters of patients (e.g. blood pressure, temperature, etc.). The vulnerability allows the attacker to take control of medical devices and silence the alarm, generate false alarm and interfere with patients monitors connected to these devices.

Urgent/11 is a collection of 11 identified vulnerabilities [8], in IPnet, a thirdparty software components, that supports network communication between computers. There are many medical devices may be affected by the use of software includes infusion pump, imaging system, anesthesia machines and more to be identified. The vulnerability allows attacker to take control of medical devices, change function, causes denial of service which may lead to information leaks or logical flaws and prevent device function.

4 Solution Trends for Healthcare Device Cyber Attacks Considering Blockchain and Constraints

Researchers are engaging in blockchain strategies to make healthcare ecosystem more secure. Medical devices are becoming more independent and dependent on more wireless connectivity, thus giving rise to decentralized healthcare institutions [21]. In blockchain transaction is done via public and private keys, where

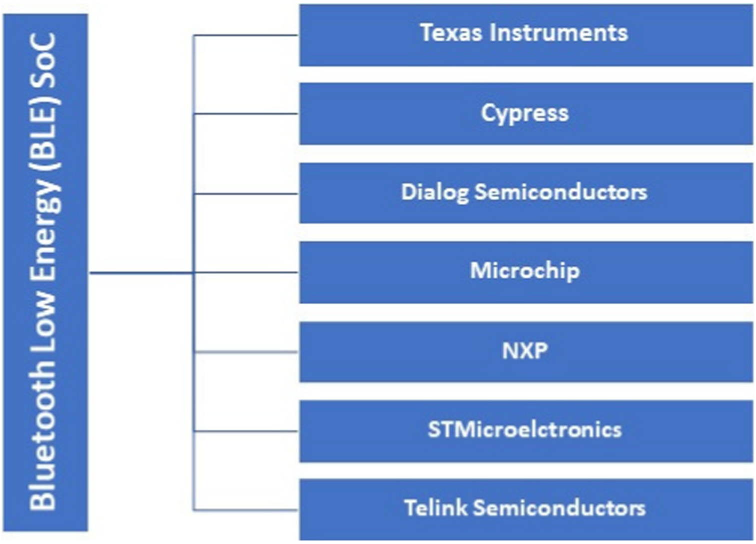

Fig. 4. Affected BLE SoC from manufacturer

private keys acts as security barrier for user authentication. Since the processing takes places at separate blocks it is independent of central server or database. Each node or decentralized block can perform the required task on its own [10].

4.1 Usage of Blockchains in Internet of Health Things (IoHT)

- Ethereum-Based Contributions: It proposes to implement smart contract for devices/user requests based on credentials on the domain. The authors [10] proposes proof medical stack (PoMS) to higher security against malicious attacks.
- Modified Consensus Protocol: The proposed system is consortium based blockchain architecture, where a patient agent (PA) software defines the blockchain functionalities [27]. The computing is done on Edge Computing network and data is stored in cloud based server in secure storage.
- Modified Cryptographic Technique: The proposal uses two software system integrated to original blockchain algorithm. For data encryption ARX algorithm and Diffie-Hellmman key exchange technique for transferring public keys [20]. The nodes must be certified before joining a blockchain and stores interconnected block with high data in cloud server with higher security. Cluster head is used to verify and store hash blocks in cloud servers and manages interactions between the clusters.
- Hyperledger-Based Contributions: The authors divides the blockchain in two segments, 1) Medical device blockchain to store data that were generated by medical device during treatment, 2) Consultation blockchain that store

patients records and data is maintained by health care provider [15]. Transactions are verified by smart contracts and execution is endorsed by Practical Byzantine Fault Tolerance algorithm.
- General Blockchain Concept Without Technical Specifications: The data is stored in shared between tamper-proof blocks between IoMT devices and healthcare providers. MedChain [26] proposes grouping the data generated by sensors in two groups 1) Blockchain network that store immutable data and 2) P2P network stores mutable data mainly focused on data query. MedChain uses BFT-SMaRt protocol.

4.2 Constraints to Use Blockchain on IoHT

Blockchain provides more security but it comes with constraints which makes it difficult to use in medical devices [21]. These are lsited below:

- Processing: The internal process of a block chain requires lots of resources for computation, thus also requires high energy. Which already a problem for medical device especially in context of energy use, more relevantly for wearable devices.
- Storage: The medical devices produces large amount of data with but not store them in different blocks and interacting through different nodes requires even larger space. This large space usually cannot be accommodated in IoHT devices.
- Real Time: In health care industry is very valuable to make decision, since blockchain involves connectivity between different blocks and nodes the computation time is increased, resulting loss of time for patient in care.
- Traffic Overhead: The inter-connectivity of the blockchains creates lots of traffic for data flow. This feature cannot be easily adopted by IoHT devices with limited bandwidth.

5 Conclusions

Medical devices are the keys to the well-being of human life. They must be protected from a cyber threat so that patients can take required health support from healthcare providers. The medical device regulatory bodies should come together with device manufacturers to formulate standards that are universally adopted and address the ever-changing technological environment. Concern bodies should work together and formulate the best solution via providing required funding so that researchers can develop an environment where human life will be safe from cyber threats. There exist limitations on technology and medical device computability which make them more vulnerable to security attacks, but the new process, innovations, algorithms are also being developed to address the issue. This paper briefly outlined vulnerabilities by keeping the focus on medical devices only, but there other areas of the healthcare system that is not discussed the paper also need attention. A further research scope on blockchain combined with edge computing may provide more secure and fast reliable solution to IoHT devices that is sought after.

References

1. Cybersecurity vulnerabilities in certain GE healthcare clinical information central stations and telemetry servers: Safety communication. https://www.fda.gov/medical-devices/safety-communications/cybersecurity-vulnerabilities-certain-ge-healthcare-clinical-information-central-stations-and. Accessed on 04 Oct 2021
2. Healthcare cyberattacks doubled in 2020, with 28% tied to ransomware. https://healthitsecurity.com/news/healthcare-cyberattacks-doubled-in-2020-with-28-tied-to-ransomware. Accessed on 04 Oct 2021
3. How fda medical device cybersecurity guidance affects providers. https://healthitsecurity.com/features/how-fda-medical-device-cybersecurity-guidance-affects-providers. Accessed on 04 Oct 2021
4. Making the case for medical device cybersecurity. https://www.darkreading.com/edge-articles/making-the-case-for-medical-device-cybersecurity. Accessed on 04 Oct 2021
5. Medical device cyber security guidance for industry. https://www.tga.gov.au/publication/medical-device-cyber-security-guidance-industry. Accessed on 04 Oct 2021
6. Medtech and the internet of medical things. https://www2.deloitte.com/global/en/pages/life-sciences-and-healthcare/articles/medtech-internet-of-medical-things.html. Accessed on 04 Oct 2021
7. Mysignals. http://www.my-signals.com/. Accessed on 04 Oct 2021
8. Urgent/11 cybersecurity vulnerabilities safety communciation. https://www.fda.gov/medical-devices/safety-communications/urgent11-cybersecurity-vulnerabilities-widely-used-third-party-software-component-may-introduce. Accessed on 04 Oct 2021
9. Va, ul collaboration advances case for medical device security standards. https://www.healthcareitnews.com/news/va-ul-collaboration-advances-case-medical-device-security-standards. Accessed on 04 Oct 2021
10. Agbo, C.C., Mahmoud, Q.H., Eklund, J.M.: Blockchain technology in healthcare: a systematic review. Healthcare **7**(2) (2019)
11. Ahmed, M.: False image injection prevention using iChain. Appl. Sci. **9**(20) (2019). https://doi.org/10.3390/app9204328
12. Ahmed, M., Barkat Ullah, A.S.S.M.: False data injection attacks in healthcare. In: Boo, Y.L., Stirling, D., Chi, L., Liu, L., Ong, K.L., Williams, G. (eds.) Data Mining, pp. 192–202. Springer, Singapore (2018). https://doi.org/10.1007/978-981-13-0292-3_12
13. Ahmed, M., Byreddy, S., Nutakki, A., Sikos, L.F., Haskell-Dowland, P.: ECU-IoHT: a dataset for analyzing cyberattacks in internet of health things. Ad Hoc Netw. **122**, 102621 (2021)
14. Ahmed, M., Pathan, A.S.K.: False data injection attack (FDIA): an overview and new metrics for fair evaluation of its countermeasure. Compl. Adap. Syst. Model. **8**, 1–14 (2020)
15. Attia, O., Khoufi, I., Laouiti, A., Adjih, C.: An IoT-blockchain architecture based on hyperledger framework for healthcare monitoring application. In: 2019 10th IFIP International Conference on New Technologies, Mobility and Security (NTMS), pp. 1–5 (2019)

16. Bostami, B., Ahmed, M., Choudhury, S.: False Data Injection Attacks in Internet of Things, pp. 47–58. Springer International Publishing, Cham (2019). https://doi.org/10.48550/arXiv.1910.01716
17. Burleson, W., Clark, S.S., Ransford, B., Fu, K.: Design challenges for secure implantable medical devices. In: DAC Design Automation Conference 2012, pp. 12–17 (2012). https://doi.org/10.1145/2228360.2228364
18. Chase, P., et al.: The evolving state of medical device cybersecurity. Biomed. Inst. Technol. **52** (2018). https://doi.org/10.2345/0899-8205-52.2.103
19. Clark, S.S., Fu, K.: Recent results in computer security for medical devices. In: Nikita, K.S., Lin, J.C., Fotiadis, D.I., Arredondo Waldmeyer, M.T. (eds.) Wireless Mobile Communication and Healthcare, pp. 111–118. Springer, Berlin, Heidelberg (2012). https://doi.org/10.1007/978-3-642-29734-2_16
20. Dwivedi, A.D., Srivastava, G., Dhar, S., Singh, R.: A decentralized privacy-preserving healthcare blockchain for IoT. Sensors **19**(2) (2019)
21. Ellouze, F., Fersi, G., Jmaiel, M.: Blockchain for internet of medical things: a technical review. In: Jmaiel, M., Mokhtari, M., Abdulrazak, B., Aloulou, H., Kallel, S. (eds.) The Impact of Digital Technologies on Public Health in Developed and Developing Countries, pp. 259–267. Springer International Publishing, Cham (2020). https://doi.org/10.1007/978-3-030-51517-1_22
22. Garbelini, M.E., Wang, C., Chattopadhyay, S., Sumei, S., Kurniawan, E.: Sweyntooth: unleashing mayhem over bluetooth low energy. In: 2020 USENIX Annual Technical Conference (USENIX ATC 2020), pp. 911–925. USENIX Association (2020). https://www.usenix.org/conference/atc20/presentation/garbelini
23. Kumar, S., Hu, Y., Andersen, M.P., Popa, R.A., Culler, D.E.: JEDI: Many-to-many end-to-end encryption and key delegation for IoT. In: 28th USENIX Security Symposium (USENIX Security 2019), pp. 1519–1536. USENIX Association, Santa Clara, CA (2019). https://www.usenix.org/conference/usenixsecurity19/presentation/kumar-sam
24. McCauley, V., Williams, P.: Trusted interoperability and the patient safety issues of parasitic health care software. In: 9th Australian Information Security Management Conference, AISM; Conference date: 05–12-2011 Through 07–12-2011, pp. 189–195 (2011)
25. Sametinger., J., Rozenblit., J.: Security scores for medical devices. In: Proceedings of the 9th International Joint Conference on Biomedical Engineering Systems and Technologies - SmartMedDev, (BIOSTEC 2016), pp. 533–541. INSTICC, SciTePress (2016). https://doi.org/10.5220/0005838805330541
26. Uddin, M.A., Stranieri, A., Gondal, I., Balasubramanian, V.: A patient agent to manage blockchains for remote patient monitoring. Stud. Health Technol. Inform. **254**, 105–115 (2018)
27. Uddin, M.A., Stranieri, A., Gondal, I., Balasubramanian, V.: Blockchain leveraged decentralized IoT ehealth framework. Internet of Things **9**, 100159 (2020)
28. Williams, P.A.H., Woodward, A.: Cybersecurity vulnerabilities in medical devices: a complex environment and multifaceted problem. Med. Dev. (Auckland, N.Z.) **8**, 305–316 (2015)
29. Xu, Y., Tran, D., Tian, Y., Alemzadeh, H.: Poster abstract: Analysis of cybersecurity vulnerabilities of interconnected medical devices. In: 2019 IEEE/ACM International Conference on Connected Health: Applications, Systems and Engineering Technologies (CHASE), pp. 23–24 (2019). https://doi.org/10.1109/CHASE48038.2019.00017

30. Yaqoob, T., Abbas, H., Atiquzzaman, M.: Security vulnerabilities, attacks, countermeasures, and regulations of networked medical devices-a review. IEEE Commun. Surv. Tutor. **21**(4), 3723–3768 (2019). https://doi.org/10.1109/COMST.2019.2914094
31. Yip, M.: Ultra-low-power circuits and systems for wearable and implantable medical devices. Ph.D. thesis, Massachusetts Institute of Technology, Cambridge, MA, USA (2013). http://hdl.handle.net/1721.1/84902