Cybersecurity Challenges in Healthcare Medical Devices

Ana Longras[1(✉)], Teresa Pereira[2], and António Amaral[3]

[1] Instituto Politécnico de Viana do Castelo, Viana do Castelo, Portugal
ana.longras@ipvc.pt
[2] Centro ALGORITMI, Universidade do Minho, Guimarães, Portugal
tpereira@dsi.uminho.pt
[3] INESC TEC–Institute for Systems and Computer Engineering, Technology and Science, 4200-465 Porto, Portugal
antonio.m.amaral@inestec.pt

Abstract. Medical devices are rapidly evolving and becoming more interconnected with healthcare networks, overcoming resource constraints, and increasingly focused on patient well-being and needs.

This work intends to identify future research themes in the area of cybersecurity in health by surveying the articles being developed and identifying their current limitations and future work. The developed analysis was based on the publications with the highest number of citations, enabling us to find several challenges and restrictions such as integrating devices in systems.

Innovations and the emergence of new technologies with inherent security vulnerabilities, will continue to evolve, escalating the attackers interest in exploiting unknown cybersecurity risks within healthcare. It is mandatory to consider cybersecurity risks since the conception of the devices to reduce security flaws, ensure the patients with a better quality of life, and guarantee information security properties.

Keywords: Cybersecurity · Medical devices · Healthcare · Review · Vulnerability · Digital transformation

1 Introduction

Medical Device Regulation considers a medical device an instrument, apparatus, appliance, software, implant, reagent, material, or other article is used for any of the following procedures: diagnosis, prevention, monitoring, treatment or alleviation of disease, disability, or injury, but not used for disability or injury prevention [1].

The distinction between a medical device and a device used in the healthcare context is often confused. The rule is clear, any device that is "intended for use in diagnosing disease or other conditions, or in curing, mitigating, treating, or preventing disease" requires Food and Drug Administration (FDA) approval to be a medical device [1].

T. Pereira et al. (Eds.): IoECon 2022, LNICST 458, pp. 66–75, 2023.
https://doi.org/10.1007/978-3-031-25222-8_6

There are approximately 2 million medical devices on the market worldwide [2]. Some can be implanted in patients' bodies called Implantable Medical Devices (IMD) to continuously or automatically treat or deliver one or more medical conditions.

Technological advances provide transformations in the provision of healthcare and also in self-care devices. In practice, it is in healthcare that greater use of wearables is seen more often.

Generally, patient health wearables are considered low risk and not regulated by the FDA as its primary services for general wellness use.

Wearables are self-contained, non-invasive devices that perform a specific medical function, such as monitoring or support over a long time period, aiming to provide a personal medical assistant. Generally, they are equipped with wireless communication capabilities for system/software upgrades, device reconfiguration, data access, and transfer [3].

However, with the advancement of wearable technology, the FDA has regulated some new features. For example, the Apple Heart Study has received FDA approval for the pulse and electrocardiogram function, thus supporting the agency's decision [4].

Additionally, it is available on the market with a wide variety of devices with more and more functionalities, from sleep monitoring, electrocardiogram, oxygen meter, connection to emergency services, and temperature measurement, among others. The 5G network access will provide even more potential with more efficient batteries, use of the cloud, and use of artificial intelligence to support the user with advice or reports that can be shared with medical institutions or health professionals towards facilitating diagnosis and prevention of diseases at a broader distance and more in advance.

The isolation and restrictions resulted from COVID-19 pandemic context has brought positive transformations and opened up a multitude of opportunities for change, accelerating the adoption of digital solutions at a pace never seen before. It led people to monitor their health condition more and has demonstrated the value of eHealth services such as telemedicine and remote patient care. Remote care is here to stay, helping the entire healthcare sector to become increasingly digital and interconnected.

The interconnectedness between all systems and devices in the health sector brought significant contributions to all stakeholders, playing a crucial role in the provision of health care, consequently increasing the life expectancy and providing active aging of the population, with huge impacts on the sustainability of health care systems.

In the meantime, the massive use of devices is not only a positive point, but it has also opened a gap in commitment and guarantee of user safety.

The massive use of devices leads the healthcare sector to face the complexity of systems, the increasing number of connected devices, software and operating systems used on the devices, communication between devices, the transfer and storage of health information, and its regulation. All these elements have inherent security risk vulnerabilities, being exposed to attackers intended to compromise the confidentiality, integrity, and availability of services and data.

The FDA recognizes the safety of medical devices is a shared responsibility among stakeholders, including healthcare facilities, patients, suppliers, and medical device manufacturers.

Failure of cybersecurity protection can result in compromised device functionality, loss of availability or data integrity (medical or personal), or exposure of other connected devices or networks to security threats. This, in turn, can result in the patient's illness, injury, or even in a more dramatic situation into death [5].

This work is organized as follows: Sect. 1 introduces cybersecurity challenges. Section 2 identifies the current state of the art, presenting the different issues on the subject based on the most cited articles. Section 3 consists of identifying and characterizing challenges related to cybersecurity in medical health devices. Section 4 ends with some conclusions from the current challenges of medical devices in healthcare.

2 Literature Review

2.1 Methodology Approach

The research methodology developed was based on a literature review of medical devices used for monitorization and health support and their associated cybersecurity risks supported by a bibliometric analysis using the VOSviewer software [6].

The literature review consisted of analyzing the 20 most cited articles to understand the structure and knowledge research developed by peers, including all types of sources, e.g., conference journals, chapters, etc. The extracted documents were carried out in December 2021 from two knowledge bases, Scopus and Web of Science (WoS).

Search queries defined are followed presented:

- ALL (cybersecurity) OR ALL ("cyber security") AND TITLE-ABS-KEY ("medical device"))
- ALL = (cybersecurity) AND (TI = (medical devices) OR TS = (medical devices) OR AB = (medical devices) OR AK = (medical devices))

The search results were stored in files in "txt" format, including citation information, bibliographic information, abstract and keywords, and other information such as conference and reference information. The objective of confirming all the information was to validate the quality of the sources within the universe of the most cited articles.

Figure 1 shows that in most cited articles, the keyword 'security' was confirmed as expected with the highest number of occurrences. Followed by the keywords 'medical devices' and 'biomedical equipment' with the same number of occurrences. Simultaneously, the keywords 'computer security'; 'embedded systems'; 'implantable medical devices'; 'patient safety'; 'security and privacy', and 'network security' were abundantly mentioned.

There is a wide range of research topics based on the keywords that are present along with cybersecurity and medical devices.

2.2 Literature Review Overview

The literature studied mentions different medical devices from biosensors related to implant devices. Accordingly, to Camera et al. (2015), an implant consists of a sensor

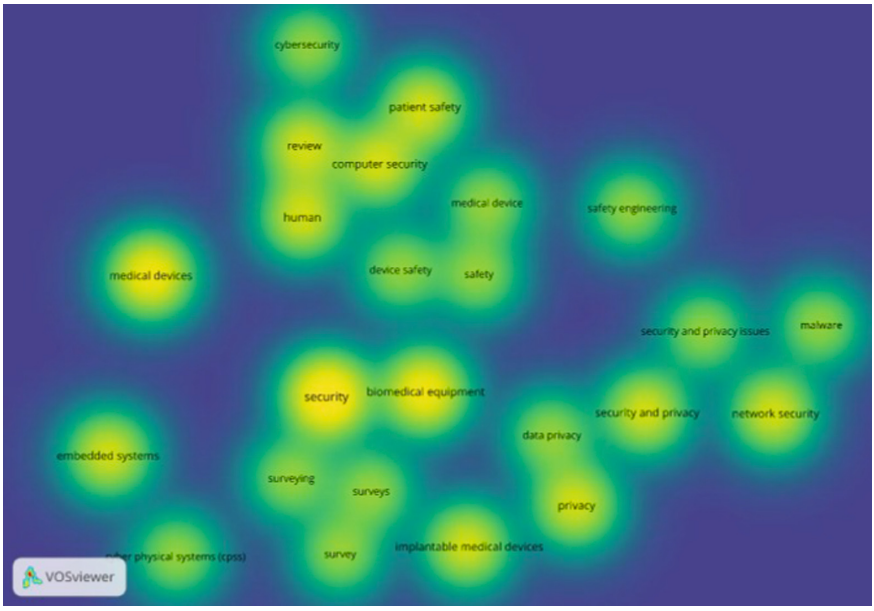

Fig. 1. Keywords of the most cited sources in the area of cybersecurity in health.

or a set of sensors placed inside the human body to monitor any part of it; neurostimulators are devices that transmit low-amplitude electrical signals through one or more electrodes placed in different locations in the brain; cardiac devices such as pacemakers and implantable cardioverter defibrillators (ICD) when equipped with telemetry have a radio transmitter that communicates with an external device and sends physiological data, which the healthcare professional can use to detect the patient's pathology [7].

Cybersecurity on medical devices is closely related to cyber-physical systems (CPS), which are systems used to monitor and control the physical world, embedded systems in a network. In medical devices, cyber-physical systems are present in wearables and IMD.

Several authors investigated medical devices regarding the security and privacy of presented CPS. They highlighted the complexity of the CPS identification due to the components' heterogeneity, which introduces difficulties in cybersecurity and privacy protection [8, 9].

Vulnerabilities and Attacks. All assets (physical, digital and human resources) have inherent security vulnerabilities, usually underestimated and exploited by attackers to create critical impacts and gain financial advantage [10]. A recent technical report claims that nearly 10 to 15 networked medical devices are present within a single bed in a hospital [11]. Hence, the interest in the security of networked medical devices has increased, thus increasing the attack reach. The theme most explored by the authors of the most cited articles in the area, is focused on the failures and weaknesses/flaws of medical devices.

The weaknesses are mainly concentrated on the software, which goes from storing credentials, and weak or non-existent authentication to arbitrarily running code. The

hardware also has inherent vulnerabilities, which can be exploited, such as on the sensors, where the attacker may interfere with the signal [12]. Most medical devices have wireless communication and, consequently, interferences vulnerabilities, which can result in attacks, noise, eavesdropping, repetition, repetition attacks, and injection attacks, compromising the integrity and availability of the devices. Therefore, one of the recurrent causes is the lack of encryption [8]. Some authors suggest that given the cryptographic hash function and the decentralized nature, several devices need to be protected; as a solution, using blockchain to store data. However, one of the main difficulties of many medical devices is related to energy consumption in a blockchain network, where each transaction needs to be validated, requiring computational power, which some devices do not have [4].

Yaqoob et al. (2019) studied a hundred medical devices to understand cybersecurity problems; identifying hardware, firmware, and software vulnerabilities used in medical devices is of extreme importance since it is responsible for critical functions; vulnerabilities coming from a personal computer or smartphone application; connections from applications to the gateway via Wi-Fi; data stored in the cloud and data storage at the gateway where there may be a lack of authentication and weak encryption; lack of access control to data stored in the cloud; and finally, communication protocols like BLE/Zigbee/Wi-Fi/RF/Ethernet can also be an attack vector [13].

Critical vulnerabilities were recently exploited by a Denial of Service (DoS) attack on millions of connected devices used in hospital networks based on stacks of Nucleus TCP/IP. The attack consists of remote code execution, which allowed attackers to disrupt medical equipment and patient monitors, as well as IoT devices that control systems and equipment in all facilities, such as lighting and ventilation systems, exploits the vulnerability CVE-2021-31886 critical in File Transfer Protocol (FTP) servers does not correctly validate the length of user commands, leading to stack-based buffer overflows that can be used for denial of service and remote code execution [14].

False data injection attack (FDIA) consists of manipulating or altering data intended to inject the same data and losing data integrity [15]. A simple example is a change of a health record, such as the blood type or type of diabetes, which could seriously impact the patient.

Other types of attacks have been mentioned by the authors of the most cited documents in the area, such as the ransomware attack. In May 2021, Ireland's public health service was forced to shut down its information systems due to a ransomware attack. The attack forced several hospitals and clinics to cancel appointments and disrupted the system for tracking contacts and scheduling new vaccines for covid-19 [16].

The 2020 and 2021 years were marked by the COVID-19 pandemic, increasing the wide use and dependence on applications and technological gadgets and, consequently, increasing the number of phishing attacks. Sometimes, a phishing attack is just a mean to materialize a bigger and, more powerful attack. An example that enables us to demonstrate this statement is the cyber-attack that occurred at the University of Florida Health Leesburg Hospital and The Villages Regional Hospital on May 31, 2021, which compromised the electronic health record (EHR), turning them unavailable, and yet not recovered, since the patient care records are still handled by paper. The ultimate goal

was a ransomware attack, which exploited the employee's vulnerability through a simple phishing email [17].

Another example of a phishing attack occurred at Saint Agnes Health Care, Inc. of Maryland, by compromising an email account with privileged access. Nearly 25,000 medical records with patient names, dates of birth, medical record numbers, health insurance information, and clinical data were exposed [18].

Solutions. In the literature review, several solutions and proposals were presented to mitigate cybersecurity risks on medical devices.

Pycroft et al. (2018) state that the solutions to IMD's concerns go through 4 cybersecurity recommendations: First, there must be an audit, where there must be detailed records of device activities and access events; second, there must be post-sale surveillance to identify and correct faults quickly; then point out that there are access controls as an access requirement, and finally, make doctors aware of cybersecurity risks [19].

Gollakota et al. (2011) proposed the use of an external device called a "shield" for all communications between IMD and the programmer to limit communications access.

Proximity-based access controls are another proposal, conditioning device communications located within a short distance [20].

The hardware tokens are solutions for the medical team's use as a key to access the devices.

There are still proposals for the use of biometric solutions through the reading of the iris with a near-infrared camera, validating the access identity.

Regarding the devices requiring energy charge, Fei et al. present a CPS-oriented solution to control the physical object to prevent an attacker from guessing the resonant frequency of the energy charge and manipulating the values [21].

Camara et al. (2015) prioritize mechanisms to detect anomalies specifically for implantable medical devices rather than solutions to mitigate threats. If an attack is detected, the patient is notified, or the device is no longer accessible, disconnecting all communications and keeping the medical functions running. Depending on the device, it is devised based on parameters like location, time, day, and the time interval of the same reader action. Based on the activity, the classifier will determine whether it is valid. Each time the reader tries to contact the medical device, it sends a message to the patient's cell phone with the access pattern. The phone runs the sorting algorithm and returns an output which is sent back to the IMD [7].

Some medical devices have highly sensitive information, most often communicated to health professionals. If the information suffers an attack that causes unavailability or compromises its authenticity, it can cause severe consequences for the patient. In this approach presented by Priya et al., it is used a neural network (deep neural network) as a critical solution to increase the efficiency of an Intrusion Detection System (IDS) in cyberattacks' detection [22].

Limitations. The diverse solutions still have limitations or open other points vulnerable to failure in the cybersecurity of medical devices.

The external device proposals assume that the device is not an entry point for exploring the primary device; they assume the external device is trustworthy.

Proposals based on proximity of the calculated distance is less than a fixed limit, communication continues; otherwise, it is interrupted. The main disadvantage of using tokens or biometric solutions is that other solutions have external devices and even at a distance. In an emergency where the healthcare professional needs to access and manipulate the device, it is essential to guarantee its availability and accessibility in person or remotely. Patient safety is always the priority, giving rise to a set of solutions called "Breaking the Glass" (BTG), which consists of allowing all cybersecurity controls to be turned off in a critical event health situation for the patient, thus ensuring the priority is the patient's life. In the meantime, the BTG solution creates an opportunity for the attacker.

The authors in [8] highlight that the devices have to be considered whole. Devices are integrated into a system right from the beginning of the design, and the cybersecurity vulnerabilities of the device must be foreseen in the interaction with other devices and with people. They emphasize the importance of working together between manufacturing, bioengineering, and cybersecurity specialists to ensure that in addition to the devices being functional, the patient is guaranteed the security of data and communications and the privacy of health information.

Although proposed and implemented defense solutions already exist, it is emphasized the need to have further investments in research for CPS cybersecurity flaws, to provide new solutions and respond to the threats and vulnerabilities recently identified and others yet to emerge. The technological advances and the organizations' interest to rapidly turn the products available in the market result, most of the time, in the underestimation of cybersecurity risks, which encourage attackers to exploit their inherent vulnerabilities [9].

One of the many medical device limitations identified by several authors is within the IMD, which has few processing resources, physical size limitations, and battery life. The emergency, where the patient's life is at stake, is highlighted by most cited authors as a clear additional challenge for cybersecurity. The devices cannot be accessible to unauthorized persons; however, in an emergency, they cannot prevent patient care.

The authors in [23] state that the first step to addressing cybersecurity challenges is for organizations to understand the vulnerabilities of networked medical devices, including the exposure of confidential and privacy-threatening information. Followed by the definition of cybersecurity requirements in the design and manufacturing processes and reviewed with the application of standards. Finally, the need to establish cybersecurity responsibility as a requirement in device design is mentioned.

The authors in [24] mention that cybersecurity should be part of the patient care culture. In this context, the patient must be informed and aware of the cybersecurity risks and threats that can compromise the integrity and availability of medical devices.

Although there is research in the field of cybersecurity in medical devices, many patients are unaware of the extent of cyberattacks and the cybersecurity risks that can affect information security properties, namely authentication, integrity, non-repudiation, confidentiality, availability, and authorization [25].

Medical devices are used outside of hospital settings. Depending on the device and procedures, they are used in leisure spaces, in the workplace, and at home, handled by health professionals to lay caregivers. A wide variety of environmental conditions add

difficulties to the cybersecurity of devices and patients; for example, there is no way to prevent the user from connecting devices to untrusted networks.

When cybersecurity risks are detected in software, hardware, or any other technology, which can result in a cybersecurity attack, the FDA shares the information with all entities, from manufacturers, healthcare providers, and government agencies, among others, to mitigate manufacturers products' vulnerabilities and find solutions [24].

In short, the most cited sources know the need to involve all areas of design and idealization of medical devices with cybersecurity professionals. They present different proposals with the limitations and implications of the devices and systems inserted. However, the patient's life will always be a priority. The starting point to be considered in investigations is that in case of life or death, cybersecurity rules cannot prevent the assistance of any health professional from assisting the patient.

3 Cybersecurity Challenges

The challenges in the literature focus on mitigating or extinguishing the limitations and attack vectors of the systems.

One of the great challenges of medical devices and the entire healthcare area, consider the interoperability of systems as the key to progress to improve healthcare. Reducing costs and improving clinical decision-making using different information insights. For systems to be interoperable, problems such as: not transmitting or not knowing how to transmit information accurately and securely must be resolved; the need to have or learn how to receive information securely; there is integration and learning how to process and correlate with data from various sources and optimize for the data for the intended purpose, working to maintain the three pillars (confidentiality, integrity, and availability) from the beginning to the end of the life cycle of medical devices.

In addition to the interoperability challenge, cybersecurity has to be seen not as a problem that can be solved but as a risk that everyone involved has an obligation to manage. We predict that cybersecurity attacks on medical devices will continue for the value of health information. We reinforce that there are already some standards such as Health Insurance Portability and Accountability Act (HIPAA), ISO 27000 series, NIST cybersecurity standards, with a lot of documentation, there is no need to invent, and the standards progress and are revised. Notwithstanding, the evolvement of digital literacy between citizens and health professionals will help to reduce the impacts of cybersecurity attacks, as well as to deepen the awareness level of the probable causes of the attacks which globally might reduce the frequency and its impacts.

4 Conclusions

Human life and patient health are priorities and are increasingly dependent on medical systems and devices. The healthcare industry will always be an interesting industry for attackers to exploit cybersecurity flaws.

Many proposals provide a reasonable level of security but require a lot of resources, which is unfeasible given the need to save resources on some of the devices. Alternatively,

all technological solutions are often vulnerable to attack as a result of weak or over-priced designs.

Devices must be used responsibly, and users must know various details about their functioning and potential threats to raise awareness to adopt cybersecurity devices' good practices. It is crucial for the users' awareness of cybersecurity policies and good practices because an incorrect behavior can compromise the most sophisticated technological security procedure.

The most cited publications in the cybersecurity health domain focus on communications between devices and third parties, methods of protecting data stored and in transit, access controls, maintenance and updates of device software, incident response, cybersecurity training from patients to healthcare providers, to guarantee the confidentiality, integrity, and availability of information and all medical systems. The future will involve working on better architecture/idealization of solutions implemented across the healthcare sector, working together with healthcare, manufacturing, and cybersecurity specialists.

References

1. MDR - Article 2 - Definitions - Medical Device Regulation (2022). https://www.medical-device-regulation.eu/2019/07/10/mdr-article-2-definitions. Accessed 22 Jan 2022
2. Medical devices. https://www.who.int/health-topics/medical-devices#tab=tab_1. Accessed 05 Jan 2022
3. Feng, L., et al.: Research and application progress of intelligent wearable devices. Chinese J. Anal. Chem. **49**(2), 159–171 (2021). https://doi.org/10.1016/S1872-2040(20)60076-7
4. Sneha, S., Panjwani, A., Lade, B., Randolph, J., Vickery, M.: Alleviating challenges related to FDA-approved medical wearables using blockchain technology. IT Prof. **23**(4), 21–27 (2021). https://doi.org/10.1109/MITP.2021.3072535
5. FDA.gov (2022). https://www.fda.gov/files/Content-of-Premarket-Submissions-for-Management-of-Cybersecurity-in-Medical-Devices---Guidance-for-Industry-and-Food-and-Drug-Administration-Staff.pdf. Accessed 05 Jan 2022
6. VOSviewer - visualizing scientific landscapes. https://www.vosviewer.com/. Accessed 28 Feb 2022
7. Camara, C., Peris-Lopez, P., Tapiador, J.E.: Security and privacy issues in implantable medical devices: a comprehensive survey. J. Biomed. Inform. **55**, 272–289 (2015). https://doi.org/10.1016/j.jbi.2015.04.007
8. Humayed, A., Lin, J., Li, F., Luo, B.: Cyber-physical systems security—a survey. IEEE Internet Things J. **4**(6), 1802–1831 (2017). https://doi.org/10.1109/JIOT.2017.2703172
9. Hossain, M., Islam, S.M.R., Ali, F., Kwak, K.S., Hasan, R.: An Internet of Things-based health prescription assistant and its security system design. Future Gener. Comput. Syst. **82**, 422–439 (2018). https://doi.org/10.1016/J.FUTURE.2017.11.020
10. Pereira, T., Barreto, L., Amaral, A.: Network and information security challenges within Industry 4.0 paradigm. Procedia Manuf. **13**, 1253–1260 (2017). https://doi.org/10.1016/J.PROMFG.2017.09.047
11. Fierce Healthcare: 82% of healthcare organizations have experienced an IoT-focused cyberattack, survey finds. https://www.fiercehealthcare.com/tech/82-healthcare-organizations-have-experienced-iot-focused-cyber-attack-survey-finds. Accessed 22 Feb 2022
12. Rushanan, M., Rubin, A.D., Kune, D.F., Swanson, C.M.: SoK: security and privacy in implantable medical devices and body area networks. In: 35th IEEE Symposium on Security and Privacy (SP 2014), pp. 524–539 (2014). https://doi.org/10.1109/SP.2014.40

13. 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
14. NVD - CVE-2021-31886 (2021). https://nvd.nist.gov/vuln/detail/CVE-2021-31886. Accessed 14 Feb 2022
15. Ahmed, M., Pathan, A.S.K.: False data injection attack (FDIA): an overview and new metrics for fair evaluation of its countermeasure. Complex Adapt. Syst. Model. **8**(1), 1–14 (2020). https://doi.org/10.1186/S40294-020-00070-W/FIGURES/7
16. ABC News: Ireland's health service hit by "significant" ransomware attack. https://abcnews.go.com/International/irelands-health-service-hit-significant-ransomware-attack/story?id=77685241. Accessed 22 Jan 2022
17. Cyberattack Drives 2 UF Health Hospitals to EHR Downtime. https://healthitsecurity.com/news/cyberattack-drives-2-uf-health-hospitals-to-ehr-downtime. Accessed 22 Jan 2022
18. Saint Agnes Health Care Hack Exposes 25,000 HIPAA Records. https://www.hipaajournal.com/saint-agnes-healthcare-hack-exposes-25000-hipaa-records-5663/. Accessed 22 Jan 2022
19. Pycroft, L., Aziz, T.Z.: Security of implantable medical devices with wireless connections: the dangers of cyber-attacks. Expert Rev. Med. Devices **15**(6), 403–406 (2018). https://doi.org/10.1080/17434440.2018.1483235
20. Gollakota, S., Hassanieh, H., Ransford, B., Katabi, D., Fu, K.: They can hear your heartbeats: non-invasive security for implantable medical devices. SIGCOMM Comput. Commun. Rev. **41**(4), 2–13 (2011). https://doi.org/10.1145/2043164.2018438
21. Hu, F., et al.: Robust cyber-physical systems: concept, models, and implementation. Future Gener. Comput. Syst. **56**, 449–475 (2016). https://doi.org/10.1016/j.future.2015.06.006
22. Swarna Priya, R.M., et al.: An effective feature engineering for DNN using hybrid PCA-GWO for intrusion detection in IoMT architecture. Comput. Commun. **160**, 139–149 (2020). https://doi.org/10.1016/j.comcom.2020.05.048
23. Williams, P.A., Woodward, A.J.: Cybersecurity vulnerabilities in medical devices: a complex environment and multifaceted problem. Med. Devices (Auckland, N.Z.) **8**, 305–316 (2015). https://doi.org/10.2147/MDER.S50048
24. Coventry, L., Branley, D.: Cybersecurity in healthcare: a narrative review of trends, threats and ways forward. Maturitas **113**, 48–52 (2018). https://doi.org/10.1016/j.maturitas.2018.04.008
25. Patients Unaware of the Extent of Healthcare Cyberattacks and Data Theft. https://www.hipaajournal.com/patients-unaware-of-the-extent-of-healthcare-cyberattacks-and-data-theft/. Accessed 25 Feb 2022
26. Cybersecurity|FDA: https://www.fda.gov/medical-devices/digital-health-center-excellence/cybersecurity#safety. Accessed 25 Feb 2022