Biomedical & Pharmacology Journal, September 2023. Vol. **16**(3), p. 1263-1270

A Review of the Impact of Cybersecurity in High-risk Medical Devices And In-vitro Medical Devices All Over The World

D. Nagasamy Venkatesh[1] and K. Muthupranesh[2]

[1]Department of Pharmaceutics, JSS College of Pharmacy (JSS Academy of Higher Education & Research, Mysuru), Ooty – 643 001. Tamil Nadu. India.
[2]Department of Pharmaceutical Regulatory Affairs, JSS College of Pharmacy (JSS Academy of Higher Education & Research, Mysuru), Ooty – 643 001. Tamil Nadu. India.
*Corresponding author E-mail: nagasamyvenkatesh@jssuni.edu.in

https://dx.doi.org/10.13005/bpj/2707

(Received: 17 February 2023; accepted: 12 May 2023)

In modern healthcare systems, medical devices are playing a major role which involves personalized medical devices which improve the patient's lifestyle as they can be remotely monitored and their data are transmissible. Due to these data transmissions, the number of connections to the existing computer networks is increased. Being interoperable and interconnected these personalized medical devices provide great benefits like improved sensing capabilities and actuating capabilities. But the problem with high connectivity computer networks is that it exposes medical device to high cybersecurity vulnerabilities. The main targets are the pacemakers and institutions like hospitals and clinics. Hackers can easily hack medical devices and change prescriptions. So a cybersecurity breach can leak a patient's sensitive and confidential data and risk the patient's life. To prevent these multifaceted problems from happening these problems must be viewed from a systematic perspective and requires governance, technical controls, regulation, and standards.

Keywords: Medical devices, Cybersecurity, Cyberattack, Informed consent, Remote monitoring, Confidentiality.

Latest advancements in technology have resulted in the transformation of the healthcare system which tends to improve patient care. One of the major parts of the healthcare system is the pharmaceutical sector and having medical devices is their critical aspect[1]. After implanted in the body or attached to the patient externally they serve a critical function by providing continued automated assistance to save lives. The medical devices attached to a single patient are commonly referred to as Personalized Medical Devices (PMDs)[2]. The devices implanted in the patient's body are called Implantable Medical Devices (IMPDs). PMDs are medical devices with small firmware and modern hardware. They are wireless, mobile, and user-friendly. And they're interconnected and interoperable as well. The interconnectivity and interoperability may provide a great benefit but they also expose the medical device to major risk concerns like cybersecurity breaches and cybersecurity vulnerabilities that can be exploited maliciously or triggered intentionally this can affect the device's performance and they can be harmful to the patient by producing illness, injury

or death[3]. So, all the stakeholders like Government, Hospitals, Healthcare organizations, and Medical Device Industries are responsible for maintaining the safety of the Patient as well as the Medical Device.

In the case of High-risk medical devices like cardiac pacemakers, insulin pumps, and implantable pulse generators they can be easily controlled and monitored using mobiles by using Bluetooth or an internet connection[4]. Some patients, such as prominent public figures are at greater risk of cybersecurity attacks. These attacks can do greater harm to the patients. And if this information is reported in the media it will greatly decrease the reputation of lifesaving medical implants. Usually, private information about high-risk medical devices is stored in Electronic Health Records (EHS) which has been reported that 90% of medical devices and Electronic Health Records have been the victims of cyber attacks[5].

Because of these risks, the software and hardware used in high-risk medical devices require prior marketing approval and Remote monitoring of the High-risk medical devices and IVDs after being marketed to prevent and reduce cyberattacks. And one of the common methods is to apply security standards and policies including cyberattack awareness programs. The trends of cybersecurity can be understood based on 2 aspects:

1. Weakness and Bug Detection in the system
2. Identifying the cyber hackers and their methods[6].

In this paper, we are going to discuss the methods that can be used to enhance safety, security, and privacy for medical devices that are controlled by the Internet while at the same time enabling higher mobility and Remote Monitoring.

Cybersecurity incidents

The most impact on the cybersecurity in a medical device is faced by Insulin pumps and Pacemakers. Research from the Archimedes – Ann Arbor Research Center for Medical Device Security at the University of Michigan has demonstrated the potential compromise to implanted devices[30]. It is found that insulin pumps- web interfaces, hard code administration passwords, and internet-accessed devices are found to be highly vulnerable in the environment of hospitals. And the internet accessed devices without authentication and encryption are the most vulnerable[31, 36].

Data transmission in medical devices

Nowadays radio frequency is commonly used for data transfer[37]. The bandwidth of the radio-frequencies for implants and pacemakers is 402-405 MHz, this bandwidth is common for devices all over the world, so this makes the devices more vulnerable. So, the process of broadcasting or misusing radiofrequency is called "radio piracy"[11].

Electromagnetic interference is also one of the major concerns in which the non-cardiac external signals will interfere with the cardiac signals and manipulate them, for example, the airport scanners, smartwatches, and mobile phones[38]. Using filters like Bandpass filters we can filter the unwanted interference of the non-cardiac waves to interfere with medical devices[12, 35].

Radiofrequency identification is a part of radiofrequency but it differs from Radiofrequency identification can carry more data but the range is shorter comparatively. There are two types – active and passive[27]. Active requires a battery source and is more complex unlike the passive which can deliver fewer data but shorter bandwidth[33]. And the shorter the bandwidth less possibility for hackers to hack as it reduces the surface area of attack whereas longer bands are costly to produce[29]. But it does not mean that it is not possible to hack the devices that transfer data in shorter bands, as we already have a history of hackings like Banking cards which deliver only shorter bands[12].

Ways to Protect Our Devices From Cybersecurity Risks

Increasing the security of the weakest link

Hackers usually target the weakest link as it requires only a minimum amount of time. So, they will target loopholes and insecure areas instead of targeting security areas[22].

Multiple Defense mechanism

Instead of focusing on a single solution, focus on complex interconnected solutions as if one system fails other interconnected systems will protect the device[23].

Level of trust

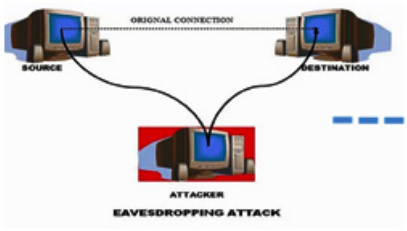
The level of trust between the application components is essential and proper controls should be maintained to ensure that a proper level of trust is established between the interactions[26].

Hiding credentials

Keeping the encryption keys and passwords hidden is a critical task. So, a depth

Security Threats To Internet-connected Devices Environment

2.1 Eavesdropping:



The confidentiality of transmitted private data, such as patient personal information, medical measurements, and user information, is jeopardized by eavesdropping attacks.

2.2 Man-in-the-Middle:

Without either party being aware until it's too late, a man-in-the-middle attack enables a spammer to intercept, send, and receive data intended for someone else or that wasn't intended to be sent at all[7].

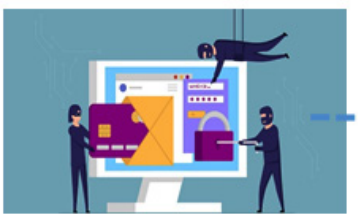
2.3 Denial of Service:

A denial of service attack (DOS) is any type of attack on a networking structure to disable a server from servicing its clients. Attacks range from sending millions of requests to a server to slow it down, flooding a server with large packets of invalid data, to sending requests with an invalid or spoofed IP address[8]

2.4 Side-Channel-Attack:

In this work, we discuss a class of physical attacks known as side-channel attacks, in which an adversary attempts to take advantage of physical information leaks including timing information, power usage or electromagnetic radiation. They represent a substantial risk to the security of majority of cryptographic hardware devices since they are passive, non-invasive, and typically possible with inexpensive tools[8].

2.5 Data Leak/ Data Breach:



Data Breach, an event where the personal confidential information got stolen without the authorization of a system owner. The information might contain financial data such as credit card details, bank details, trade secrets, personally identifiable data (PID) and corporate information. The baddies are the hackers targets the computing machines. In data breaches, there are types. Based on the type of attacks, naming is given. They are: Phishing, Password attacks, Denial of service, malware, and ransomware. Password attacks are one of the types in the data breaches where the cryptanalyst tries to run a program to crack the password. It often refers to brute force attack. Might be in one form or another form every company is becoming the victim to data breach[9].

2.6 Password Guessing:

Users must retain information created for authentication in order to use knowledge-based authentication. Despite the rise of alternate graphical and textual systems, text passwords and personal identification numbers (PINs) continue to be widely used. Text-based passwords are difficult to remember and are frequently forgotten, among other issues. In order to cope, some users create brief, simple passwords. These flimsy passwords are susceptible to targeted guessing, dictionary, and brute-force assaults[9].

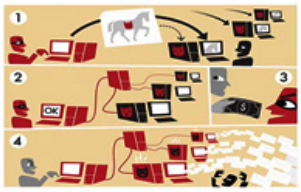
2.7 Remote Hijacking/ Session Hijacking:

The attacker uses bugs that are particularly notorious, as they can often be exploited by a remote attacker to execute arbitrary code on the victim host, effectively compromising that machine[8].

2.8 Impersonation:

A sort of social engineering known as an impersonation attack occurs when a perpetrator pretends to be someone else or poses as a legitimate user (or group of users) in order to obtain information, they are not authorized to have. In this type of attack, the attacker will often use social engineering techniques to gain information about the system[9].

2.9 Cloning Attack:



Cybercriminals use cloning, also known as phishing, as a form of social engineering assault to trick its victims into believing a malicious email looks just like a valid one. Due to their resemblance to authentic emails, clone phishing assaults are often far more difficult to detect for the unwary.

2.10 Physical Attack:

A physical attack occurs when an attacker physically accesses a physical object within the infrastructure system with the intent to harm, disable, steal from, or otherwise make use of it[10].

approach should be established to keep the credentials private and safe[25].

Least privilege principle

Each function of a security system should be maintained with the least privilege. As maintaining the least privilege prevents/ reduces any damages occurring from the loopholes of the system[19].

Default security

While designing the systems access decisions should be provided rather than denying it. So, the user will get the option to accept or deny the program which is much easier to design and safer[21].

Security Zoning

Encapsulation methods are used to create security zones/ trust zones, to handle the damage created by the trust or access breach[20].

Simple Designs

These designs are systematically easy-to-use and verify systems and which is because simpler designs are much preferred[18].

Privacy Promotion

Maintain privacy about the instructions and processes about the system works which provides hackers with the system information[24].

Incorrect assumptions

Incorrect assumptions are always a major concern and major loopholes are due to these incorrect assumptions. So, they should be avoided[13,14].

Cybersecurity and remote monitoring

The development of implantable medical devices leads to a reduction in their size and they have to typically rely on the software alone for their functioning they are highly internet accessible compared to the old devices[17]. The implantable medical devices contain radio interfaces that are programmed with wireless communication with the help of external device programmers[34]. The benefits are more but this broadens the surface area of the attack leaving the device vulnerable[28]. And wireless attacks are much easier to launch and whereas analog attacks are comparatively harder because of the narrow surface area for attack[35]. So, the remote monitoring of medical devices has become essential and medical devices should be monitored periodically[15,16].

CONCLUSION

The risk of cybersecurity has becoming a major concern and, in this paper, we have learnt about the different types of cybersecurity attacks, and major cybersecurity incidents and the ways to prevent the cybersecurity attacks. Each type of cybersecurity attack requires specific methods of prevention. The need to protect businesses' digital assets and medical equipment from cyberattacks has grown as a result of the development of the digital landscape. One of the difficulties in project management is balancing investments in security measures with rising development costs. Software testing experts and IT infrastructure staff need to incorporate security testing into their testing processes and regularly learn about security testing technologies and the most recent software and hardware security flaws. Given the multitude of rules, standards, frameworks, guidance documents, technical studies, and best practices on this subject, it has become more and more challenging to gain a clear understanding of regulatory requirements that address the security of connected medical devices and related software. While some standards lack explicit requirements on cybersecurity, they do offer some advice on how security controls should be implemented. In the software life cycle procedures, cybersecurity has grown to be of the utmost importance. The value of the company's goods and services can increase by putting in place a proactive security strategy against risks.

ACKNOWLEDGEMENT

The authors would like to thank the Department of Science and Technology – Fund for Improvement of Science and Technology Infrastructure in Universities and Higher Educational Institutions (DST-FIST), New Delhi for their infrastructure support to our department.

REFERENCES

1. Hegde V. Cybersecurity for medical devices. *Annual Reliability and Maintainability Symposium* (RAMS) (2018) Jan 22 (pp. 1-6) IEEE (2018).

2. Beavers J, Pournouri S. Recent cyber-attacks and vulnerabilities in medical devices and healthcare institutions. *Blockchain and Clinical Trial*: Securing Patient Data:, 2019; 249-67.
3. Schwartz S, Ross A, Carmody S, Chase P, Coley SC, Connolly J, Petrozzino C, Zuk M. The evolving state of medical device cybersecurity. *Biomedical instrumentation & technology*, 2018; **52**(2):103-11.
4. Lechner NH. An overview of cybersecurity regulations and standards for medical device software. In Central European Conference on Information and Intelligent Systems (pp. 237-249). *Faculty of Organization and Informatics*, 2017; Varazdin.
5. Yuan S, Fernando A, Klonoff DC. Standards for medical device cybersecurity in. *Journal of diabetes science and technology*., 2018; 12(4):743-6.
6. Baranchuk A, Refaat MM, Patton KK, Chung MK, Krishnan K, Kutyifa V, Upadhyay G, Fisher JD, Lakkireddy DR, American College of Cardiology's Electrophysiology Section Leadership. Cybersecurity for cardiac implantable electronic devices: what should you know? *Journal of the American College of Cardiology*, 2018;71(11):1284-8.
7. Biasin E, Kamenjasevic E. Cybersecurity of medical devices: regulatory challenges in the EU (2022).
8. Ransford B, Kramer DB, Foo Kune D, Auto de Medeiros J, Yan C, Xu W, Crawford T, Fu K. Cybersecurity and medical devices: a practical guide for cardiac electrophysiologists. *Pacing and Clinical Electrophysiology,* 2017; ;40(8):913-7.
9. Gaukstern E, Krishnan S. Cybersecurity threats targeting networked critical medical devices; 2018.
10. Williams PA, Woodward AJ. Cybersecurity vulnerabilities in medical devices: a complex environment and multifaceted problem. Medical Devices: *Evidence and Research.,* 2015; 305-16.
11. Stern AD, Gordon WJ, Landman AB, Kramer DB. Cybersecurity features of digital medical devices: an analysis of FDA product summaries. *BMJ open*., 2019; 9(6):e025374.
12. Karmakar KK, Varadharajan V, Tupakula U, Nepal S, Thapa C. Towards a security-enhanced virtualized network infrastructure for *the Internet of Medical Things (IoMT)*. In(2020) 6th IEEE conference on network softwarization (NetSoft) Jun 29 (pp. 257-261). *IEEE* (2020).
13. Pycroft L, Aziz TZ. Security of implantable medical devices with wireless connections: The dangers of cyber-attacks. *Expert Review of Medical Devices*., 2018; 15(6):403-6.
14. Tabasum A, Safi Z, AlKhater W, Shikfa A. Cybersecurity issues in implanted medical devices. In(2018*) International Conference on Computer and Applications* (ICCA) Aug 25 (pp. 1-9). *IEEE*, 2018.
15. Sadhu PK, Yanambaka VP, Abdelgawad A, Yelamarthi K. Prospect of internet of medical things: A review on security requirements and solutions. *Sensors*., 2022; ;22(15):5517.
16. Tran-Dang, H. Krommenacker, N.; Charpentier, P.; Kim, D.S. Toward the Internet of Things for Physical Internet: Perspectives and Challenges. *IEEE Internet Things* J., 2020; **7**: 4711–4736.
17. Wazid, M. Singh, J. Das, A.K.; Shetty, S. Khan, M.K.; Rodrigues, J.J.P.C. ASCP-IoMT: AI-Enabled Lightweight Secure Communication Protocol for Internet of Medical Things. *IEEE Access*, 2022; **10**, 57990–58004.
18. Amin, F. Majeed, A. Mateen, A. Abbasi, R.; Hwang, S.O. A Systematic Survey on the Recent Advancements in the Social Internet of Things. *IEEE Access*, 2022; **10**: 63867–63884.
19. Noguchi, H.; Mori, T.; Sato, T. Framework for Search Application based on Time Segment of Sensor Data in Home Environment. In Proceedings of the Seventh International Conference on Networked Sensing Systems (INSS), Kassel, Germany, 2020; 15–18 June; pp. 261–264.
20. Shamsoshoara, A. Korenda, A. Afghah, F. Zeadally, S. A Survey on Physical Unclonable Function (PUF)-based Security Solutions for Internet of Things. *Comput. Netw.,* 2020; **183**: 107593.
21. Masud, M. Gaba, G.S.; Alqahtani, S. Muhammad, G.; Gupta, B.B. Kumar, P. Ghoneim, A. A Lightweight and Robust Secure Key Establishment Protocol for Internet of Medical Things in COVID-19 Patients Care. *IEEE Internet Things J*., 2021; **8**: 15694–15703.
22. Ullah, S.S. Hussain, S. Gumaei, A. Alhilal, M.S.; Alkhamees, B.F.; Uddin, M.; Al-Rakhami, M. A Cost-Effective Approach for NDN-Based Internet of Medical Things Deployment. *Comput. Mater. Contin.,* 2022; **70**: 233–249.
23. Egala, B.S.; Pradhan, A.K. Badarla, V.R.; Mohanty, S.P. Fortified-chain: A blockchain-based framework for security and privacy-assured internet of medical things with effective access control. *IEEE Internet Things J*., 2021; **8**: 11717–11731.
24. Lin, P. Song, Q. Yu, F.R.; Wang, D. Guo, L.

Task Offloading for Wireless VR-Enabled Medical Treatment With Blockchain Security Using Collective Reinforcement Learning. *IEEE Internet Things J*., 2021; **8**: 15749–15761.

25. Abdellatif, A.A. Samara, L. Mohamed, A. Erbad, A. Chiasserini, C.F. Guizani, M.; O'Connor, M.D. Laughton, J. Medge-chain: Leveraging edge computing and blockchain for efficient medical data exchange. *IEEE Internet Things J*. 2021; **8**: 15762–15775
26. Ding, Y. Wu, G. Chen, D. Zhang, N. Gong, L. Cao, M. Qin, Z. DeepEDN: A Deep-Learning-Based Image Encryption and Decryption Network for Internet of Medical Things. *IEEE Internet Things J*., 2020; **8**: 1504–1518.
27. Liu, X. Yang, X. Luo, Y. Zhang, Q. Verifiable Multi-Keyword Search Encryption Scheme with Anonymous Key Generation for Medical Internet of Things. *IEEE Internet Things J.*
28. Li, X. Peng, J. Obaidat, M.S.; Wu, F. Khan, M.K. Chen, C. A Secure Three-factor User Authentication Protocol with Forward Secrecy for Wireless Medical Sensor Network Systems. *IEEE Syst. J*., 2019; **14**; 39–50.
29. Kumar, P. Lee, S.G.; Lee, H.J. E-SAP: Efficient-strong Authentication Protocol for Healthcare Applications using Wireless Medical Sensor Networks. Sensors, 2012; **12**; 1625–1647.
30. Liu, H. Yao, X. Yang, T. Ning, H. Cooperative Privacy Preservation for Wearable Devices in Hybrid Computing-based Smart Health. IEEE Internet Things J., 2018; **6**: 1352–1362.
31. Dharminder, D.; Gupta, P. Security Analysis and Application of Chebyshev Chaotic Map in the Authentication Protocols. *Int. J. Comput. Appl*., 2019; **43**; 1095–1103.
32. Kumar, M. Chand, S. A Secure and Efficient Cloud-Centric Internet-of-Medical-Things-Enabled Smart Healthcare System with Public Verifiability. *IEEE Internet Things J*., 2020; **7**: 10650–10659.
33. Deebak, B.D. Al-Turjman, F. Smart Mutual Authentication Protocol for Cloud-Based Medical Healthcare Systems using Internet of Medical Things. *IEEE J. Sel. Areas Commun.,* 2020; **39**: 346–360.
34. Sadhu, P.K. Yanambaka, V.P. Abdelgawad, A. Yelamarthi, K. Performance Analysis of Ring Oscillator PUF for Robust Security in Smart Transportation. In Proceedings of the Proceedings of *IEEE 7th World Forum on Internet of Things* (WF-IoT), New Orleans, LA, USA, 14 June–31 July; 2021; 301–302.
35. Aman, M.N.; Javaid, U.; Sikdar, B. A Privacy-preserving and Scalable Authentication Protocol for the Internet of Vehicles. *IEEE Internet Things J*., 2020; **8**: 1123–1139.
36. Ivanovska, E. Ribarska, J.T. Lazova, J. Popstefanova, N. Jovanoska, M.D. Jolevska, S.T. Providing Clinical Evidence under the MDR (2017)/745–New Challenges for Manufacturers in Medical Device Industry. *Arh. Farm*., 2019; **69**: 39–49.
37. Sampath, T. Thamizharasan, S. Vijay Kumar Shetty, K. Timiri Shanmugam, P.S. ISO 14971 and ISO 24971: Medical Device Risk Management. In *Medical Device Guidelines and Regulations Handbook; Springer*: Berlin, Germany, 2022; 31–56.
38. Alsubaei, F. Abuhussein, A.; Shandilya, V. Shiva, S. IoMT-SAF: *Internet of Medical Things Security Assessment Framework. Internet Things*, 2019; **8**: 100123.
39. Baranchuk A, Refaat MM, Patton KK, Chung MK, Krishnan K, Kutyifa V, Upadhyay G, Fisher JD, Lakkireddy DR, American College of Cardiology's Electrophysiology Section Leadership. Cybersecurity for cardiac implantable electronic devices: what should you know? *Journal of the American College of Cardiology*. 2018;**71**(11):1284-8.
40. Li C, Raghunathan A, Jha NK. Hijacking an insulin pump: Security attacks and defenses for a diabetes therapy system. In2011 IEEE 13th international conference on e-health networking, applications and services, Jun 13 (pp. 150-156). *IEEE*, 2011.
41. Sivakorn S, Polakis I, Keromytis AD. The cracked cookie jar: HTTP cookie hijacking and the exposure of private information. In IEEE Symposium on Security and Privacy (SP) May 22 (pp. 724-742). *IEEE* (2016).
42. Alabdulkreem E, Alduailij M, Alduailij M, Mansour RF. Optimal weighted fusion-based insider data leakage detection and classification model for Ubiquitous computing systems. *Sustainable Energy Technologies and Assessments*. 2022; **54**:102815.
43. Zuo C, Lin Z, Zhang Y. Why does your data leak? uncovering the data leakage in cloud from mobile apps. In IEEE Symposium on Security and Privacy (SP) May 19 (pp. 1296-1310). *IEEE* (2019).
44. Jin X, Chen PY, Hsu CY, Yu CM, Chen T. CAFE: Catastrophic data leakage in vertical federated learning. *Advances in Neural Information Processing Systems*. 2021;**34**:994-1006.
45. Fu X, Gao Y, Luo B, Du X, Guizani M. Securi

ty threats to Hadoop: data leakage attacks and investigation. *IEEE Network*. 2017;**31**(2):67-71.
46. Fu X, Gao Y, Luo B, Du X, Guizani M. Security threats to Hadoop: data leakage attacks and investigation. IEEE Network. 2017;**31**(2):67-71.
47. Bosu A, Liu F, Yao D, Wang G. Collusive data leak and more: Large-scale threat analysis of inter-app communications. In Proceedings of the ACM on Asia Conference on Computer and Communications Security, 2017; 71-85.
48. Alabdulkreem E, Alduailij M, Alduailij M, Mansour RF. Optimal weighted fusion based insider data leakage detection and classification model for Ubiquitous computing systems. *Sustainable Energy Technologies and Assessments*, 2022; **54**:102815.
49. Palit T, Monrose F, Polychronakis M. Mitigating data leakage by protecting memory-resident sensitive data. In Proceedings of the 35th Annual Computer Security Applications Conference, 2019: 598-611).
50. Flynn T, Grispos G, Glisson W, Mahoney W. Knock! knock! who is there? investigating data leakage from a medical internet of things hijacking attack.