International Journal of Advanced Technology in Engineering and Science
Vol. No. 09, Issue No. 11, November 2021
www.ijates.com
ijates
ISSN 2348 - 7550

Cyber Security Quantification of Healthcare Medical Devices through Soft computing technique

Masood Ahmad[1] , Mohd Nadeem[1] , Adil Hussain Seh[1], Raees Ahmad Khan[1]

[1]*Information Technology, Babasaheb Bhim Rao Ambedkar Univeristy, Lucknow, India*

Abstract

Medical device play vital role in healthcare services. Security of medical device is a most important need in healthcare services because most of the medical devices developed lack of security patch. So, healthcare device softly come under the attacker's target. Attackers can alter the patients information capturing by the medical devices this may cause the life threat. So medical devices and healthcare Big data security is a major concern in the healthcare services. In this research authors try to find the most relevant security factors which affect the security of medical devices. For assessment the security of the medical devices authors applied Fuzzy TOPSIS mythology. Fuzzy TOPSIS is a best ranking method; it's provided the ranks in quantitative way and removes the vagueness of the human error in the taken decision.

Keywords: Medical devices, Cyber Security, Fuzzy TOPSIS, Big Data.

1. Introduction

Computational capabilities of medical devices increase the focused of refresher and development in the healthcare sector [1]. Computational capabilities of medical devices are provide the better treatment and earlier stage diagnosis of diseases; in other side they invite the cyber threat due to computational capabilities [2]. World Health Organization (WHO) define the medical device as, medical device is a machines, apparatus, and embedded system which is used for the monitoring, treatment, and diagnosis the sickness of the patients[3,4].

By the Medical device patients gets better treatment by using the communication technologies. In this time mostly medical devices are network connected, network related threats invited by these devices. Failure of medical device can affect the working of hospital and affecting the people. Implantable devices shows essential role in treatment and monitoring of the patient's activity [5]. Innovation on the medical device technologies are two side of a coin. Where one side is beneficial for the healthcare treatment and other side is opened area for the security breaches which affect the lives. Software of medical device should be fulfilling system properties like that of safety, security, reliability, availability, and confidentiality etc., [6]. Software based medical devices for patient's treatment particularly ranges from the computerized treatments of disease through the mobile apps and computer systems. A small change in medical devices security can harm the patient [2]. During 2006 to 2011 there were a total 5294 recalls. 20 to 25% of these recalls were due to computer failure [7]. Medical devices consist of computing functions like a wireless communication or connectivity for software based control. This computing function causes cyber-

attacks. Cyber security protects the computing system from the vulnerability to security beaches. Most of the medical devices contain embedded systems [3].

Attackers attacks on the networked medical devices through the malware. Malware involves in healthcare data tempering. Malware can harmful for healthcare bigdata. We show a graphical representation in Fig. 1 of malware discovered year wise, this data is publically available by AV-TEST. Daily AV-TEST files the 3.5 lakhs new malware programs [8]. Extremely fast growing of the cyber threats, medical device manufacturers and vendors should quick revise with these threats.

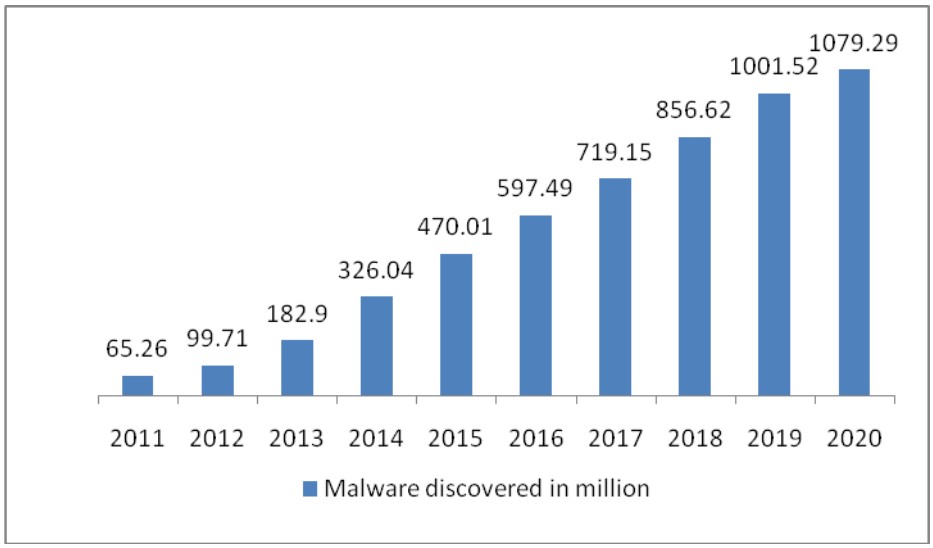

Figure. 1. Malware discovered year-wise from AV-TEST.

For the hacker's healthcare industries are most favourite target because in the healthcare large attacking areas are available for the hackers [9]. New study mentioned near about 10 to 15 networked medical devices can be presented in a single bed hospital [10]. Software security measure in the development of the software is a common issue. Software is vital polls in the medical device because all computing function is managed by the software. Software vulnerabilities if remains in the medical devices than attackers can be easily successful in the healthcare [11-12]. In the last decades, nearby 1,527,311 breaches were occurs by the software vulnerability of the medical devices [13]. New medical devices will be safe and secure if we are aware about the cyber security vulnerability in the design and development phase [14]. The major challenge for the security experts is to secure the medical device against the vulnerabilities by providing the software patches or updates but without changing the platforms. The Department of Homeland Security (DHS) has analyzed 11 vulnerabilities, named URGENT/11. This cyber security vulnerability may change the functions of medical device [7].

Contribution in this study as follows: related works are discussed in the 2nd part of this study. 3rd part of this study discuss about the security model of the medical device and results obtained by the fuzzy TOPSIS methodology. Discussion of the study elaborates in 4th part and 5th part of this study discusses the conclusion of the part.

2. Related work

Jagannathan & Adam Sorini [2015] - Designed a system which enables the self-authentication of medical device software. They used encryption for software purpose and only those parts of the software will be decrypted that are required for the operation of the device. Here, the decrypted parts are involved in the integrity checking and no modification can be done unless validated by authentication [10].

Ma et al. [2019] - Provides a quantitative technique for security of medical imaging devices. In this paper they have used pre and post market security guideline for security assessment. Mostly medical devices are at risk because devices are networked and they offer the attacker the loopholes through which they can threaten the privacy and safety of the patients. FAHP technique has been used for assessment of the security. This process is automated and less time consuming [9].

Abdullah et al.[2020] proposed a hybrid approach for security assessment of the medical device software that are used in healthcare services. In this framework authors assessment the security at the pre and post development of software for medical devices and provide the guidelines for developing the secure software. And also identify the infected software which is send by the third party vendors in the name of updating [2].

Abdulaziz et al.[2020] also designed a framework for device security assessment of IoT. In this research authors used TOPSIS ranking approach for assigning the ranking of devices based on their security [4].

Al-Zahrani et al.[2020] designed a frame work for integrity assessment of medical devices by using Fuzzy ANP. TOPSIS method, in this research authors try to find the most secure devices which maintain the integrity. Authors finds various integrity approaches for maintain the integrity of medical devices with the help of this framework authors opts the most likely approach for maintain the integrity of medical devices in healthcare [5].
In this study, Authors have used medical devices for security assessment Big Data security perspective. Authors used Fuzzy TOPSIS methods to assessment the security in medical device software provided by the medical device manufacturers and third party software providers.

3. Medical Device Security Model and Methodology

3.1 Security Model

Medical device security model discussed below in details.

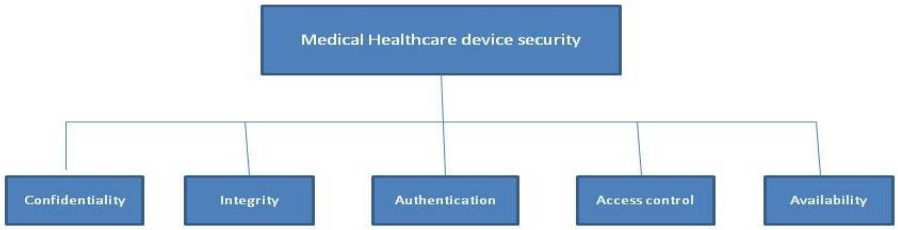

Figure 2. Medical device security model.

Confidentiality-

Confidentiality measures are designed to prevent unauthorized access attempts of sensitive information. It is common for data to be categorized according to the amount and type of damage that could be done if it fell into the wrong hands [1].

Integrity

Maintaining the consistency, accuracy and trustworthiness of data over its entire lifecycle. Data must not be changed in transit, and steps must be taken to ensure data cannot be altered by unauthorized people [2].

Availability

Information should be consistently and readily accessible for authorized parties. This involves properly maintaining hardware and technical infrastructure and systems that hold and display the information [4].

Access Control

Once authenticated, the users can enter an information system but their access will still be governed by an access control policy which is typically based on the privilege and right of each practitioner authorized by patient or a trusted third party. It is then, a powerful and flexible mechanism to grant permissions for users. It provide sophisticated authorization controls to ensure that users can perform only the activities for which they have permissions, such as data access, job submission, cluster administration, etc. A number of solutions have been proposed to address the security and access [5].

Authentication

Authentication is the act of establishing or confirming claims made by or about the subject are true and authentic. It serves a vital function within any organization: securing access to corporate networks, protecting the identities of users, and ensuring that a user is who he claims to be [5].

3.2 Methodology

3.2.1 Fuzzy TOPSIS

The Fuzzy-TOPSIS technique is the best technique in decision making or assigning the ranks of the techniques. The traditional way of selecting techniques for the issues is very awful. In many cases, human decisions become fail where the little bit of deference occurs in technique and human opts inaccurate solution technique and get the results inaccurate. To remove this inaccuracy in technique selection authors applied the Fuzzy-TOPSIS technique. Propose technique estimate the appropriate alternative which is near to the ideal solution. Alternatives distance could be positive and negative. Fuzzy TOPSIS evaluates the Fuzzy positive and negative ideal solution, where positive denotes the benefit of technique and negative denotes the cost of the technique [4-5, 16]. This technique opts for the alternatives which have the smallest distance from the positive solution and far from the negative solution.
The overall methodology is discussed as follows.

1) For all criteria determine the linguistic terms. A set of membership functions are assigned for each linguistic term.
2) Design the fuzzy decision matrix depends on the alternatives. If the number of alternatives is n and the number of tasks is m, then m*n size decision matrix will be constructed.
3) Normalized fuzzy decision matrix with the help of decision matrix
4) Estimated the weighted fuzzy decision matrix
5) Evaluate positive and negative ideal solution and calculate the distance of each alternatives from positive and negative ideal solution
6) Satisfaction degree is used to find the ranking of alternatives.

Table 1. Rank of the security factors.

Alternatives	D. +i	D. -i	CC,+i (Gap Degree)	CC, -i (Satisfaction Degree)	Ranking
Co-1	0.0653	0.0356	0.5051	0.6456	1
In -2	0.0557	0.0386	0.3697	0.6366	2
Av -3	0.0470	0.0586	0.6059	0.3967	5
Au -4	0.0432	0.0386	0.2446	0.5637	3
Ac -5	0.4522	0.0545	0.5326	0.4786	4

Following the computations of the weighted fuzzy matrix, positive and negative ideal solution operations are performed. If the closeness coefficient is calculated then the classification of all alternatives can be easily fined. Fuzzy TOPSIS makes the easy tasks for the decision-makers to find the most appropriate alternative based on the Satisfaction degree of all alternatives. Final result and classification of algorithms depicted in Tab. 6. With the help

of the satisfaction degree, the ranking of the algorithms will be Co-1> In-2> Av-4> Au-5 > Ac-3.

4 Discussion

In this study, authors have extracted the security issues in medical devices, by discussing pre existing techniques for gaining security in which healthcare organization are likely to be highly beneficial. In this section, authors citing some frameworks and methodologies pre existed in different researches with emphasis on their focus and limitations. For instance, the methodology applied in 2, which introduced a hybrid framework for measuring the software security of medical devices and addresses the security issues in medical devices. Another research 1 discusses insight and implication in healthcare device. In 4 research authors address the security issues and apply the TOPSIS method for assessing the security and provide the guidelines for vendors and healthcare organization also. 5 proposed a Fuzzy ANP TOPSIS based framework which is used for checking and selecting the most appropriate integrity approach for medical device security. These entire frameworks help us in this article and clear the road map for this research. In this research, authors applied Fuzzy TOPSIS technique for measuring the medical device security. And we observed that confidentiality obtained highest priority among other factors and second highest likely factor is integrity of device. It means that confidentiality of medical is more important for maintaining the security of device.

5 Conclusion

In this paper, authors have discussed security issues in each and every components of medical device development are also presented with the existing methodologies in the context of healthcare bigdata. As medical devices collect, store and process health bigdata, the importance of keeping them secure cannot be over-emphasized. While government and industry have begun working to improve the security management of medical devices, a systematic and quantitative approach for security assessment still remains to be achieved. In addition of preexisting methods used to ensure patient's privacy in healthcare and effective diagnosis of the patient's diseases. In this context, as our future direction, perspectives will focus more on achieving effective solutions to the confidentiality of the medical devices and healthcare bigdata security generated by the device. We have presented a list of criteria to propose a fine-grained security assessment model. In analysis confidentiality of devices highest priority and integrity of the device obtained second highest. By using this approach, developers and government agencies can easily evaluate the medical devices security and mitigate the vagueness in manual methods.

References

1. Alhakami, W., Baz, A., Alhakami, H., Ahmad, M., & Ahmad Khan, R. Healthcare Device Security: Insights and Implications. Intelligent Automation and Soft Computing, 27, 2021, 409-424.

2. Algarni, A., Ahmad, M., Attaallah, A., Agrawal, A., Kumar, R., & Khan, R.A. A Hybrid Fuzzy Rule-Based Multi-Criteria Framework for Security Assessment of Medical Device Software. International Journal of Intelligent Engineering and Systems, 13, 2021, 51-62.
3. U.S. FDA. Content of premarket submissions for management of cybersecurity in medical devices— Draft guidance for industry and Food and Drug Administration staff. http://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm356186.htm (Oct 14, 2021).
4. Attaallah, A., Ahmad, M., Tarique Jamal Ansari, M., Kumar Pandey, A., Kumar, R., & Ahmad Khan, R. Device Security Assessment of Internet of Healthcare Things. Intelligent Automation and Soft Computing, 27, 2021, 593-603.
5. A. Alzahrani, F., Ahmad, M., Nadeem, M., Kumar, R., & Ahmad Khan, R. Integrity Assessment of Medical Devices for Improving Hospital Services. CMC-computers Materials & Continua, 67, 2021, 3619-3633.
6. Algarni, A., Ahmad, M., Attaallah, A., Agrawal, A., Kumar, R., & Ahmad, R. A Fuzzy Multi-Objective Covering-based Security Quantification Model for Mitigating Risk of Web based Medical Image Processing System. International Journal of Advanced Computer Science and Applications, 2020.
7. Ahmad, M., Jehad F. Al-Amri, Ahmad F. Subahi, Sabita Khatri, Adil Hussain Seh, Mohd Nadeem and Alka Agrawal. "Healthcare Device Security Assessment through Computational Methodology." Computer Systems Science and Engineering, 41(2), 2021, 811-828.
8. Urgent 11 Cybersecurity vulnerabilities in a widely-used Third party software component may introduce risks dusring use of certain medical devices: FDA safety communication. https://www.fda.gov/medical-devices/safety-communications/urgent11-cybersecurity-vulnerabilities-widely-used-third-party-software-component-may-introduce (14-Oct-2021).
9. New Malicious programs. https://www.av-test.org/en/statistics/malware/. (14-Oct-2021).
10. Pingchuan Ma, Zhiqiang Wang, Xiaoxiang Zou, Jianyi Zhang, Qixu Liu, Xin Lyu, and Wentao Wang. Medical imaging device security: An exploratory study. arXiv preprint arXiv:1904.00224, 2019.
11. S. Jagannathan and A. Sorini. A cybersecurity risk analysis methodology for medical devices. In 2015 IEEE Symposium on Product Compliance Engineering (ISPCE), 2015, 1–6.
12. T. Yaqoob, et al. "Security Vulnerabilities, Attacks, Countermeasures, and Regulations of Networked Medical Devices—A Review." IEEE Communications Surveys & Tutorials, 21,2019, 3723-3768.
13. K. Fu, "Public Health Effectiveness of the FDA 510(k) Clearance Process: Measuring Postmarket Performance and Other Select Topics: Workshop Report", Washington DC: National Academies Press (US), 2013.
14. Ma, Pingchuan& Wang, Zhiqiang&Hei, Xiali&Zou, Xiaoxiang& Zhang, Jianyi& Liu, Qixu&Lyu, Xin&Zhuo, Zihan. A Quantitative Approach for Medical Imaging Device Security Assessment. 49th Annual IEEE/IFIP Int. Conf. on Dependable System and Networks- Supplemental, Vol (DSN-S), 2019, 1-4.
15. H. William, H Maisel. Improving the security and privacy of implantable medical devices. The New England journal of medicine, 362(13), 2010.