Intelligent Automation & Soft Computing
DOI:10.32604/iasc.2021.015092
Article

Tech Science Press

Device Security Assessment of Internet of Healthcare Things

Abdulaziz Attaallah[1], Masood Ahmad[2], Md Tarique Jamal Ansari[2], Abhishek Kumar Pandey[2], Rajeev Kumar[2,3,*] and Raees Ahmad Khan[2]

[1]Faculty of Computing and Information Technology, King Abdulaziz University, Jeddah-21589, Saudi Arabia
[2]Department of Information Technology, Babasaheb Bhimrao Ambedkar University, Lucknow-226025, Uttar Pradesh, India
[3]Department of Computer Application, Shri Ramswaroop Memorial University, Barabanki 225003, Uttar Pradesh, India
[*]Corresponding Author: Rajeev Kumar. Email: rs0414@gmail.com
Received: 06 November 2020; Accepted: 14 December 2020

Abstract: Security of the Internet of Healthcare Things (IoHT) devices plays a vital role in e-healthcare today and there has been a rapid increase in the use of networked devices of IoHT in the present healthcare services. However, these networked devices are also highly vulnerable to attackers who constantly target the security of devices and their components to gain access to the patients' data. Infringement of patients' data is not only a violation of privacy but can also jeopardize patients' health if the health records are tampered with. Once the device has been intruded upon, attackers can not only change the record of the patients but also block and switch off the device. Decidedly, the security of IoHT devices is at a huge risk and needs to be designed, manufactured and networked with more secure mechanisms. In this league, the present study employs a new methodology to assess the privacy and security of the IoHT devices. The study analyses the security defects of the medical devices by enlisting the opinions of the hacking experts. Based on the collated list of defects cited by the experts, the authors have designed a list of criteria and represented the defects in hierarchical format for assessing the security defects in the devices. Thereafter, the Technical for Order Preference by Similarity to Ideal Solution (TOPSIS) method has been used for ranking the security of IoHT devices, based on their security features. The findings of the study iterate that the proposed mechanism would be an efficacious approach for evaluating the security of the medical devices.

Keywords: Healthcare device; TOPSIS method; security and privacy; IoHT

1 Introduction

Healthcare industry started the use of computers in the last few decades, thus bringing in a phenomenal change. Imaging based security of IoHT devices have revolutionized the treatment procedures by providing novel capabilities like the early diagnosis of diseases that enables prompt and efficacious treatment. In this context, the computational capabilities of IoHT devices are being given greater focus and have emerged as the domain for new development in the healthcare industry [1,2]. However, the computational capabilities of IoHT devices are two sides of the same coin. While on one side, the computational capabilities of devices

provide better treatment and diagnosis of the diseases in the early stages itself, on the other side, they render the devices vulnerable to intrusions [3–6]. Medical industry is very different from the other industries and the development process of a medical device is also singularly different from any other device's life cycle in design, implementation and application [7–12]. The World Health Organization (WHO) defines a medical device as, "*a machine, apparatus, and embedded system which is used for the monitoring, treatment, and diagnosis of the sickness of the patients*" [13–16]. Security features of IoHT devices are differentiated according to their working and properties which are software based, hardware based and software-hardware based [17–21].

Networked devices provide a wide range of technologies that aid in monitoring, and diagnosing the ailments of patients. Since the IoHT devices are network connected, the devices become prone to network related threats. Security of IoHT devices is an essential part of the healthcare organizations. Failure of the medical devices can stop the operations of the hospitals, thereby affecting the patients as well as the healthcare service providers. Implantable devices play an important role in treating and monitoring the patients' health [22–25].

Attackers usually invade the security of IoHT devices through malware. Malware is used for data tempering and modification in healthcare data. Malware can be harmful for healthcare and medical devices. The graph in Fig. 1 illustrates the malware discovered by the publically available data of AV-TEST year-wise.

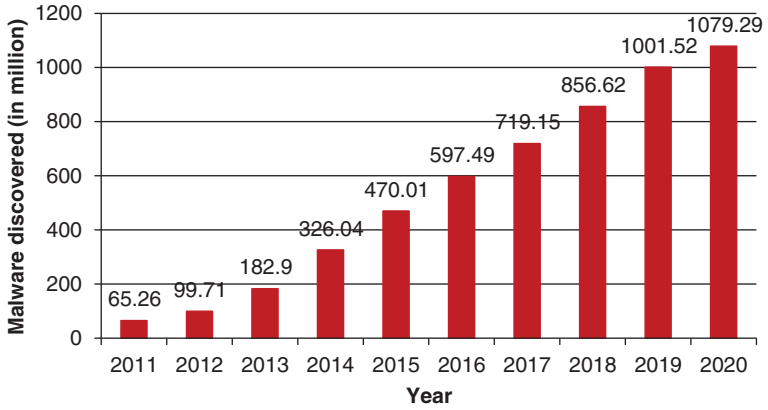

Figure 1: Malware discovered from AV-TEST year-wise

AV-TEST files 3.5 lakhs new malware programs daily [7]. Given the upsurge in the numbers and kinds of cyber threats that are evolving day-by-day, as cited by the figures mapped below, the manufacturers and vendors of IoHT devices must revise security mechanisms to engineer foolproof devices.

Healthcare industry is considered to be the *most prized target* of the hackers because of the availability of numerous vulnerabilities that are easy targets for the hackers. A recent study done in this context cites that nearly 10 to 15 networked IoHT devices can be present in a single bed hospital [8]. Software security measure is a common issue in the development of the software. Software is one of the most essential pillars in the medical device as the entire computing functioning of the device is controlled by the software.

If software vulnerabilities remain in the IoHT devices, then cyber attackers can easily invade the systems, thus hampering the devices' efficacy and use. Nearly 1,527,311 breaches occurred due to the software vulnerability of IoHT in the last decade [9].

Thus the present study undertakes a thorough perusal of the privacy and security features of the IoHT devices and, thereafter, proposes a methodology for evaluating the security of IoHT devices in an accurate and a conclusive manner. To achieve this intent, the study has been segregated in the following parts:

- Section 2 discusses the previous research initiatives in the context of the security of IoHT devices.
- In Section 3, the authors have designed the hierarchy system for evaluating the security of the medical devices with a set of chosen criteria and alternatives.
- In Section 4 & 5, we have discussed the methodology and the statistical findings, respectively.
- Conclusion of the article has been detailed in section 6.

2 Past Research Initiatives

Although an extensive reference was drawn for attempting the present research analysis, this section only discusses the security perspectives of IoHT devices, which were particularly useful for our study. The key pursuits are listed below:

McMahon et al. [10] proposed a model which used the Shodan database (collection of IP addresses) for checking the vulnerabilities of networked devices. This database passes with Nessus by python to check the vulnerability that exists in the network and finds that most of the devices are affected with drop bear SSH server problem, PHP Vulnerabilities and SSH weaknesses for bypassing the authentication.

Yaqoob et al. [25] did a review paper on the vulnerabilities in the security of IoHT devices and attacks. Jagannathan et al. [2] designed a security framework for assessing the cyber security risk and conducting preliminary Hazards analysis. The preliminary hazard analysis would help the vendors to customize the cybersecurity at the initial level.

Choudhri et al. [11] discussed the security issues for mobile medical imaging. In this study, the authors discussed the security and privacy guidelines for protecting the mobile medical imaging.

Pingchuan et al. [12] undertook a quantitative analysis of imaging medical device's security. In this study, the authors used Fuzzy Analytic Hierarchy Process (FAHP) for assessing the security of devices and provided the ranks of the devices according to their security. Fuzzy-AHP was used to assess the security of medical devices. Fuzzy-AHP has some limitations like complex computations, and rank reversal.

More specifically, to overcome these issues in our research pursuit, we have used the Fuzzy-TOPSIS methods. This methodology provides easy computation and addresses the rank reversal issues that might arise while ranking the alternatives.

3 Hierarchy System for Evaluating the Security of Medical Device

We have designed a multi-level hierarchy for the assessment of medical device's security in Fig. 2. We opted for the TOPSIS techniques for assigning the ranking. The attributes taken for the ranking were identified and collated by referring to the established standards, and after consulting with the industry experts and academicians. After developing the list of criteria, we checked the medical devices' security and assigned the ranks to the devices according to their security. The hierarchical model has been discussed below.

3.1 Confidentiality

Confidentiality of the medical device implies that only the genuine users can gain access to their data because the medical information contains personal data of the patients and mustn't be breached upon [13].

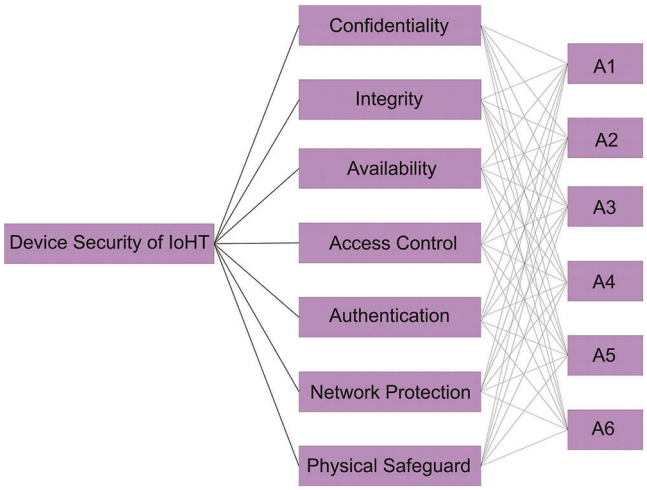

Figure 2: Multi-level hierarchy for the assessment of the security of a medical device

3.2 Integrity

Integrity of the medical data should be maintained and there should be no change in the functioning of the device in case of any attack on the machine [14]. In the context of healthcare data integrity, the data of the patients and diagnosis report should not vary.

3.3 Availability

Availability of the medical device means that it should be available in any circumstances, and at any given time, for the processing of the patients' images and data [15]. In the context of healthcare, the data should be available when required, or at the time when the device goes off.

3.4 Access Control

Access control also is an authentication process of the authentic users [16]. The Authentication processes are used for the access control of the security of IoHT device.

3.5 Authentication

The authentication process is done to protect the device from the unauthorized access [17]. In the authentication process, the users' details are verified so as to permit the users to access the device.

3.6 Network Protection

Networked devices always suffer from the *man-in-the-middle* attacks. For the safety of the medical device [18], the first thing to do is to make the network secure.

3.7 Physical Safeguard

All the vendors of the medical devices should develop the physical safeguards for the IoHT devices' security [19] because these devices mostly suffer from the *brute-force- attacks*.

Confidentiality of the devices cannot be checked at the time of purchase. Hence, identity authentication is required at every level. But identity authentication cannot be applied on the doctors when the surgical devices are in use. All these factors also determine the security of IoHT devices.

4 Fuzzy TOPSIS Methodology

TOPSIS is the most widely used methodology for solving the real time problems. This method is a multi-criteria decision making process and is simple and easy to calculate. In this methodology, the selected alternatives are compared with each criterion for obtaining the weights. Thereafter, the weights are normalized and the geometric length among the alternatives is evaluated to determine the best rank among the criteria. Exact values are used for representing the experts' opinions in the traditional TOPSIS format [20]. Usually, the decision making models do not accept precise values, as is seen in many practical cases. Hence, the decision makers opt for approximate values instead of exact values.

TOPSIS technique cannot resolve the ambiguities and uncertainties that arise due to variations in experts' choices of attributes because they are not in specific values. Hence, the fuzzy set theory is applied in place of exact values to permit the experts for options like: *partial ignorance, the non-obtainable information, incomplete information* in the decision making process. Fuzzy-TOPSIS approach is constructed for finding solutions to the challenges like rating and evidence [21,22]. In this form, the selected alternative that has the farthest geometric distance from the fuzzy negative ideal solution (FNIS), and is also the closest to the fuzzy positive ideal solution (FPIS) is ranked as the best alternative. TOPSIS assigns fuzzy numbers to the real-time fuzzy setting to reflect the relative importance of the criterion. The technique of Fuzzy-TOPSIS is as follows:

Step 1- In this step, membership values, in linguistic terms, are assigned to the chosen factors. Thereafter the weights for the factors are determined. Then, the ranks of the alternatives are established as per their weights.

Step 2- Draw the fuzzy decision matrix.

The authors constructed the decision matrix which was based on the linguistic terms and the criteria (Eq. (1)-(3)). The matrix *mxn* was constructed wherein, *m* = *alternatives* and *n* = *criteria*.

$$\widetilde{FM} = \begin{array}{c} \\ A_1 \\ \dots \\ A_m \end{array} \begin{array}{c} \begin{array}{ccc} C_1 & \dots\dots & C_n \end{array} \\ \begin{bmatrix} \tilde{x}_{11} & \cdots & \tilde{x}_{1n} \\ \dots & \ddots & \dots \\ \tilde{x}_{m1} & \cdots & \tilde{x}_{mn} \end{bmatrix} \end{array} \tag{1}$$

where

$$\tilde{x}_{ij} = \frac{1}{D}\left(\tilde{x}_{ij}^{1} \cdots \oplus \tilde{x}_{ij}^{d} \oplus \cdots \tilde{x}_{ij}^{D}\right) \tag{2}$$

$$\tilde{x}_{ij}^{d} = (l_{ij}^{d}, mi_{ij}^{d}, u_{ij}^{d}) \tag{3}$$

In this matrix *A1,....Am* represent the alternatives, and *C1,C2...Cn* represent the criteria of the medical devices, and $\tilde{x}_{ij}^{d}$ is the ranking of alternatives (Eq. (4)).

$$\mathrm{w} = \mathrm{w}_1, \mathrm{w}_2, \dots..\mathrm{w}_n \tag{4}$$

Thereafter, the weights of the criteria, w = weight with criteria values are calculated.

Step 3- This step is used for normalizing the fuzzy decision matrix, this is done by the Eqs. (5) and (6).

$$\tilde{p}_{ij} = \left(\frac{l_{ij}}{u_j^+}, \frac{mi_{ij}}{u_j^+}, \frac{u_{ij}}{u_j^+}\right), \quad u_j^+ = max\{u_{ij},\ i = 1, 2, 3..n\} \tag{5}$$

$$\tilde{p}_{ij} = \left(\frac{l_j^-}{l_{ij}}, \frac{l_j^-}{mi_{ij}}, \frac{l_j^-}{u_{ij}}\right), \quad l_j^+ = min\{l_{ij},\ i = 1, 2, 3..n\} \tag{6}$$

For evaluating the security of the medical devices, we used the criteria max value by using the Eq. (5). Otherwise, the min value is determined by using Eq. (6).

Step 4- Weighted fuzzy decision matrix is calculated in this section. We obtained the weighted normalized fuzzy decision matrix $\widetilde{Q}$ by multiplying the fuzzy decision matrix $\tilde{p}_{ij}$ with the weights $\widetilde{w}_i$. Fuzzy weighted matrix can be normalized with the Eqs. (7) and (8).

$$\tilde{Q} = \left[\tilde{q}_{ij}\right]_{m\times n} i = 1, 2, ..m;\ j = 1, 2, 3 \ldots n \tag{7}$$

Here

$$\tilde{q}_{ij} = \tilde{p}_{ij} \otimes \tilde{w}_i \tag{8}$$

Step 5- The Fuzzy Positive-Ideal Solution (FPIS) and Fuzzy Negative-Ideal Solution (FNIS) are evaluated in this step, ranging from *0 to 1*. TFN of FPIS, and FNIS is represented as *(1,1,1) or (0,0,0)*. Eqs. (9) and (10) are used for calculating the values.

$$A^+ = \left(\tilde{q}^*_{1,\cdots\ldots}\tilde{q}^*_{j,\cdots\ldots}\tilde{q}^*_{n,}\right) \tag{9}$$

$$A^- = \left(\tilde{q}^*_{1,\cdots\ldots}\tilde{q}^*_{j,\cdots\ldots}\tilde{q}^*_{n,}\right) \tag{10}$$

Step 6- Calculate the distance of each alternative from FPIS and FNIS. The distance ($\tilde{d}_i^+ and\ \tilde{d}_i^-$) of each alternative from A^+ and A^- can be evaluated by Eqs. (11) and (12).

$$\tilde{d}_i^+ = \sum_{j=1}^{n} d\left(\tilde{q}_{ij}, \tilde{q}^*_{ij}\right) i = 1, 2, ..m;\ j = 1, 2, 3 \ldots n \tag{11}$$

$$\tilde{d}_i^- = \sum_{j=1}^{n} d\left(\tilde{q}_{ij}, \tilde{q}^*_{ij}\right) i = 1, 2, ..m;\ j = 1, 2, 3 \ldots n \tag{12}$$

Step 7- Closeness coefficients are determined. Closeness Coefficients (CC_i) is used to find the ranks of all the alternatives. Further, CC_i shows that alternative is closest to $\widetilde{d}_i^+$ and farthest from $\widetilde{d}_i^-$.

The CC_i can be calculated by Eq. (13).

$$CC_i = \frac{\tilde{k}_i^+}{\tilde{k}_i^+ + k_i^-},\ i = 1, 2, \ldots, m \tag{13}$$

Step 8- Rank of the alternatives.

After the overall calculations, the ranks of the alternatives are obtained; the highest rank denotes the best alternative.

5 Numerical Assessment

Fuzzy TOPSIS technique has been proposed for the evaluation of the security of the medical devices in this section [23,24]. Linguistic terms and their respective membership functions are shown in Tab. 1 [16,17]. The framework can be explained as follows:

Table 1: Linguistic scales for the rating

Linguistic terms	Corresponding membership function
Very poor (VP)	(0, 1, 3)
Poor (P)	(1, 3, 5)
Average (AV)	(3, 5, 7)
Good (G)	(5, 7, 9)
Very good (VG)	(7, 9, 10)

- ***Design the Fuzzy Decision Matrix***

Linguistic terms are changed into the TFNs by using the Tab. 1 and Eqs. (1)–(4). TFNs help in farming of the fuzzy decision matrices, as shown in Tab. 2.

Table 2: Fuzzy decision matrix of TFN

Criteria/Alternative		A1	A2	A3	A4	A5	A6
Criteria 1	C1	2.450000, 4.270000, 6.270000	3.910000, 5.910000, 7.820000	2.450000, 4.450000, 6.400050	1.640000, 3.550000, 5.550000	3.910000, 5.910000, 7.910000	3.550000, 5.550000, 7.450000
Criteria 2	C2	1.910000, 3.730000, 5.730000	2.550000, 4.450000, 6.450000	2.180000, 4.090000, 6.140000	2.450000, 4.270000, 6.270000	3.910000, 5.910000, 7.820000	2.450000, 4.450000, 6.450000
Criteria 3	C3	1.640000, 3.550000, 5.550000	3.910000, 5.910000, 7.910000	3.550000, 5.550000, 7.450000	1.910000, 3.730000, 5.730000	2.550000, 4.450000, 6.450000	2.180000, 4.090000, 6.140000
Criteria 4	C4	2.450000, 4.270000, 6.270000	3.910000, 5.910000, 7.820000	2.450000, 4.450000, 6.450000	1.640000, 3.550000, 5.550000	3.910000, 5.910000, 7.910000	3.550000, 5.550000, 7.450000
Criteria 5	C5	1.910000, 3.730000, 5.730000	2.550000, 4.450000, 6.450000	2.180000, 4.090000, 6.140000	2.450000, 4.270000, 6.270000	3.910000, 5.910000, 7.820000	2.450000, 4.450000, 6.450000
Criteria 6	C6	1.640000, 3.550000, 5.550000	3.910000, 5.910000, 7.910000	3.550000, 5.550000, 7.450000	1.910000, 3.730000, 5.730000	2.550000, 4.450000, 6.450000	2.180000, 4.090000, 6.140000
Criteria 7	C7	2.550000, 4.450000, 6.450000	3.100080, 5.180000, 7.090000	2.900000, 4.800000, 6.700000	1.640000, 3.550000, 5.550000	3.910000, 5.910000, 7.910000	3.550000, 5.550000, 7.450000

- ***Normalize the Aggregate Fuzzy Decision Matrix***

After designing the decision matrix, we calculated the normalized matrix by the Eqs. (5) and (6); the results are shown in Tab. 3.

Table 3: Normalized aggregate fuzzy-decision matrix

Criteria/Alternative		A1	A2	A3	A4	A5	A6
Criteria 1	C1	0.290000, 0.540000, 0.820000	0.420000, 0.690000, 1.000000	0.290000, 0.570000, 0.880000	0.320000, 0.560000, 0.810000	0.290000, 0.570000, 0.880000	0.490000, 0.740000, 0.980000
Criteria 2	C2	0.470000, 0.740000, 1.000000	0.270000, 0.560000, 0.860000	0.250000, 0.550000, 0.860000	0.490000, 0.740000, 1.000000	0.250000, 0.550000, 0.860000	0.320000, 0.560000, 0.810000
Criteria 3	C3	0.470000, 0.740000, 1.000000	0.270000, 0.560000, 0.860000	0.250000, 0.550000, 0.860000	0.490000, 0.740000, 1.000000	0.250000, 0.550000, 0.860000	0.490000, 0.740000, 1.000000
Criteria 4	C4	0.380000, 0.640000, 0.890000	0.420000, 0.690000, 1.000000	0.390000, 0.700000, 1.000000	0.400000, 0.650000, 0.890000	0.390000, 0.700000, 1.000000	0.400000, 0.650000, 0.890000
Criteria 5	C5	0.290000, 0.540000, 0.820000	0.420000, 0.690000, 1.000000	0.290000, 0.570000, 0.880000	0.320000, 0.560000, 0.810000	0.290000, 0.570000, 0.880000	0.320000, 0.560000, 0.810000
Criteria 6	C6	0.470000, 0.740000, 1.000000	0.270000, 0.560000, 0.860000	0.250000, 0.550000, 0.860000	0.490000, 0.740000, 1.000000	0.250000, 0.550000, 0.860000	0.490000, 0.740000, 1.000000
Criteria 7	C7	0.380000, 0.640000, 0.890000	0.420000, 0.690000, 1.000000	0.390000, 0.700000, 1.000000	0.400000, 0.650000, 0.890000	0.390000, 0.700000, 1.000000	0.400000, 0.650000, 0.890000

- ***Design the Weighted Normalized Decision Matrix***

In this step, we evaluated the weighted fuzzy decision matrix after normalizing the decision matrix with the help of Eqs. (7) and (8). The weighted matrix is shown in Tab. 4.

Table 4: Weighted normalized aggregate fuzzy-decision matrix

		A1	A2	A3	A4	A5	A6
Criteria 1	C1	0.041000, 0.095000, 0.242000	0.059000, 0.121000, 0.296000	0.041000, 0.100000, 0.260000	0.059000, 0.121000, 0.296000	0.040001, 0.100000, 0.260000	0.045000, 0.098000, 0.239000
Criteria 2	C2	0.061000, 0.121000, 0.233000	0.034000, 0.091000, 0.200000	0.032000, 0.089000, 0.200000	0.034000, 0.091000, 0.200000	0.032000, 0.089000, 0.200000	0.063000, 0.120000, 0.233000
Criteria 3	C3	0.059000, 0.121000, 0.296000	0.041000, 0.100000, 0.260000	0.045000, 0.098000, 0.239000	0.041000, 0.100000, 0.260000	0.045000, 0.098000, 0.239000	0.063000, 0.120000, 0.233000
Criteria 4	C4	0.034000, 0.091000, 0.200000	0.032000, 0.089000, 0.200000	0.063000, 0.120000, 0.233000	0.032000, 0.089000, 0.200000	0.063000, 0.120000, 0.233000	0.112000, 0.146000, 0.306000

Table 4 (continued).

		A1	A2	A3	A4	A5	A6
Criteria 5	C5	0.041000, 0.095000, 0.242000	0.059000, 0.121000, 0.296000	0.041000, 0.100000, 0.260000	0.059000, 0.121000, 0.296000	0.041000, 0.100000, 0.260000	0.045000, 0.098000, 0.239000
Criteria 6	C6	0.060001, 0.121000, 0.233000	0.034000, 0.091000, 0.200000	0.032000, 0.089000, 0.200000	0.034000, 0.091000, 0.200000	0.032000, 0.089000, 0.200000	0.063000, 0.120000, 0.233000
Criteria 7	C7	0.034000, 0.091000, 0.200000	0.032000, 0.089000, 0.200000	0.114000, 0.144000, 0.306000	0.125000, 0.155000, 0.344000	0.116000, 0.157000, 0.344000	0.112000, 0.146000, 0.306000

- ***Evaluate the FPIS and FNIS***

The ideal solution is the distance calculated by FPIS and FNIS with the help of Eqs. (9)–(13); the results are shown in Tab. 5 and Fig. 3.

Table 5: Closeness coefficients of the different alternatives

Alternatives		d+i	d-i	Gap degree of CC+i	Satisfaction degree of CC-i	Ranks
Alternatives 1	A1	1.2114525	1.3485759	0.5124578	0.4844658	4
Alternatives 2	A2	0.6945785	0.8425657	0.5425458	0.4545879	5
Alternatives 3	A3	0.7789875	1.4854567	0.6526358	0.3477589	6
Alternatives 4	A4	2.1675648	1.4842578	0.4145782	0.5945782	1
Alternatives 5	A5	2.0457854	1.5452786	0.4457895	0.5678547	2
Alternatives 6	A6	0.4485478	0.3452578	0.4789856	0.5365385	3

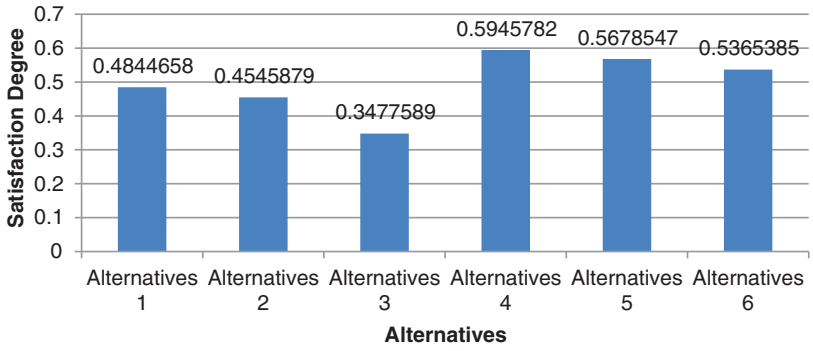

Figure 3: Graphical representation of closeness coefficients

We obtained the ranks of the alternatives after evaluating the closeness coefficients. TOPSIS technique permits the experts to choose the most suitable alternative from a host of options/choices. This has been calculated by Eq. (13). Final output and the ranks of the alternatives have been shown in Tab. 5 and

Fig. 3. According to the results, devices are ranked in the order of: A4, > A5, > A6, > A1, > A2, > A3. According to the ranking order, the alternative A4 is nearest to the FISP, and farthest from FNIS.

6 Conclusion

Security of the IoHT devices is not only a critical, but also an elemental concern in e-healthcare. Medical devices take the data inputs, store, process, and transmit the data. In all these processes, the important thing is to ensure the security of the data. However, a systematic and quantitative assessment of the security of the IoHT devices is still a matter of extensive research. We opted for the TOPSIS method for conducting a quantitative assessment of the security of the medical devices. The first step in this league was to formulate a list of criteria and alternatives. Thereafter, we conducted the evaluations as discussed in the section on the framework of evaluation. In the ensuing step, the ranking of the devices was done to identify the most secure device. The lowest ranked device was the one with *very poor security.* Such a method affords a highly feasible and efficacious way to assess the security levels of IoHT devices. The proposed mechanism can be used by the government, manufacturers and vendors to strengthen the security of the networked medical devices.

Funding Statement: The authors have not received no specific funding for this study. This pursuit is a part of their scholarly endeavours.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] M. Pingchuan, Z. Wang, X. Zou, J. Zhang, Q. Liu *et al.,* "Medical imaging device security: An exploratory study," arXiv preprint arXiv:1904.00224, 2019.

[2] S. Jagannathan and A. Sorini, "A cybersecurity risk analysis methodology for device security of IoHT," *IEEE Sym. on Product Compliance Engineering*, vol. 5, no. 6, pp. 1–6, 2015.

[3] M. T. J. Ansari, F. A. Al-Zahrani, D. Pandey and A. Agrawal, "A fuzzy TOPSIS based analysis toward selection of effective security requirements engineering approach for trustworthy healthcare software development," *BMC Medical Informatics and Decision Making*, vol. 20, no. 1, pp. 91, 2020.

[4] G. Syringe, OVERVIEW: FDA regulation of device security of IoHT, *Qrasupport.com*, 2013. [Online]. Available: http://www.qrasupport.com/FDA-MED-DEVICE.html. Last Visit Nov 21, 2020.

[5] G. Tanev, P. Tzolov and R. Apiafi, "A value blueprint approach to cybersecurity in networked device security of IoHT," *Technology Innovation Management Review*, vol. 5, no. 6, pp. 17–25, 2015.

[6] How U.S. life expectancy ranks in the world, HuffPost.com 2017. [Online]. Available: https://www.huffingtonpost.com/2013/11/21/uslife-expectancy-oecd n 4317367.html. Last Visit Nov 21, 2020.

[7] New Malicious programs [Online]. Available at: https://www.av-test.org/en/statistics/malware/. Last Visit Nov 21, 2020.

[8] D. Klonoff, MEDSec 2017 Security and Privacy for the internet of Medical Things, California, United States, 2017. [Online]. Available at: http://www.qrasupport.com/FDA-MED-DEVICE.html. Last Visit Nov 21, 2020.

[9] T. Wizemann, "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), vol. 5, no. 6, pp. 12–18, 2011.

[10] E. McMahon, R. Williams, M. El, S. Samtani, M. Patton *et al.,* "Assessing medical device vulnerabilities on the Internet of Things," in *IEEE International Conference on Intelligence and Security Informatics (ISI)*, Beijing, pp. 176–178, 2017.

[11] A. F. Choudhri , A. R. Chatterjee, R. Javan, M. G. Radvany and G. Shih, "Security issues for mobile medical imaging: A primer," *Radiographic: A review publication of the Radiological Society of North America*, vol. 35, no. 6, pp. 1814–1824, 2015.

[12] M. Pingchuan, W. Zhiqiang, H. Xiali, Z. Xiaoxiang, Z. Jianyi *et al.,* "A quantitative approach for medical imaging device security assessment," *49th Annual IEEE/IFIP Int. Conf. on Dependable System and Networks-Supplemental*, vol. (DSN-S), Portland, OR, USA, USA: IEEE, pp. 5–6, 2019.

[13] M. T. J. Ansari and D. Pandey, "Risks, security, and privacy for HIV/AIDS data: Big data perspective," *Big Data Analytics in HIV/AIDS Research*, vol. 6, no. 7, pp. 117–139, 2018.

[14] M. T. J. Ansari, D. Pandey and M. Alenezi, "STORE: Security threat oriented requirements engineering methodology," *Journal of King Saud University-Computer and Information Sciences*, vol. 5, no. 6, pp. 1–13, 2018.

[15] A. Wirth and S. L. Grimes, "Medical device cybersecurity- at the convergence of CE and IT," Clinical engineering hankbook, 2nd ed., pp. 253–258, 2020.

[16] L. Wu, X. Du, M. Guizani and A. Mohamed, "Access control schemes for implantable medical devices: A survey," *IEEE Internet of Things Journal*, vol. 4, no. 5, pp. 1272–1283, 2017.

[17] H. Zhao, R. Xu, M. Shu and J. Hu, "Physiological-signal-based key negotiation protocols for body sensor networks: A survey," *Simulation Modelling Practice and Theory*, vol. 65, no. 6, pp. 32–44, 2016.

[18] K. Zetter, "Hospital Networks Are Leaking Data, Leaving Critical Devices Vulnerable," *Wired Magazine*, 2014. [Online]. Available at: http://www.wired.com/2014/06/ hospital-networks-leaking-data/. Last Visit Nov 21, 2020.

[19] H. Almohri, L. Cheng, D. Yao and H. Alemzadeh, "On threat modeling and mitigation of medical cyber-physical systems," *IEEE/ACM Int. Conf. on Connected Health: Applications, System and Engineering Technology*, vol. 5, no. 6, pp. 114–119, 2017.

[20] M. Moayeri, A. Shahvarani, M. H. Behzadi and F. L. Hosseinzadeh, "Comparison of fuzzy AHP and fuzzy TOPSIS methods for math teachers selection," *Indian Journal of Science and Technology*, vol. 8, no. 13, pp. 1–10, 2015.

[21] A. Abdullah, A. Attaallah, M. Ahmad, A. Agrawal, R. Kumar *et al.,* "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*, vol. 11, no. 1, pp. 481–489, 2020.

[22] A. Abdullah, A. Attaallah, M. Ahmad, A. Agrawal, R. Kumar *et al.,* "A hybrid fuzzy rule-based multi-criteria framework for security assessment of medical device software," *International Journal of Intelligent Engineering and Systems*, vol. 31, no. 5, pp. 51–62, 2020.

[23] A. K. Pandey, A. I. Khan, B. A. Yoosef, M. S. Alam, A. Agrawal *et al.,* "Key issues in healthcare data integrity: analysis and recommendations," *IEEE Access*, vol. 8, pp. 40612–40628, 2020.

[24] K. Shahroudi and H. Rouydel, "Using a multicriteria decision making approach (ANP-TOPSIS) to evaluate suppliers in Iran's auto industry," *International Journal of Applied Operational Research*, vol. 2, no. 2, pp. 37–48, 2012.

[25] T. Yaqoob, H. Abbas and M. Atiquzzaman, "Security vulnerabilities, attacks, countermeasures, and regulations of networked medical devices—A Review," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 4, pp. 3723–3768, 2019.