Computer Systems Science & Engineering
DOI:10.32604/csse.2022.020097
Article

Tech Science Press

Healthcare Device Security Assessment through Computational Methodology

Masood Ahmad[1], Jehad F. Al-Amri[2], Ahmad F. Subahi[3], Sabita Khatri[2], Adil Hussain Seh[1], Mohd Nadeem[1] and Alka Agrawal[1,*]

[1]Department of Information Technology, Babasaheb Bhimrao Ambedkar University, Lucknow, 226025, Uttar Pradesh, India
[2]Department of Information Technology, College of Computers and Information Technology, Taif University, Taif, 21944, Saudi Arabia
[3]Department of Computer Science, University College of Al Jamoum, Umm Al Qura University, Makkah, 21421, Saudi Arabia
*Corresponding Author: Alka Agrawal. Email: alka_csjmu@yahoo.co.in

Received: 08 May 2021; Accepted: 09 June 2021

Abstract: The current study discusses the different methods used to secure healthcare devices and proposes a quantitative framework to list them in order of significances. The study uses the Hesitant Fuzzy (HF), Analytic Hierarchy Process (AHP) integrated with Fuzzy Technical for Order Preference by Similarities to Ideal Solution (TOPSIS) to classify the best alternatives to security techniques for healthcare devices to securing the devices. The technique is enlisted to rate the alternatives based on the degree of satisfaction of their weights. The ranks of the alternatives consequently decide the order of priority for the techniques. A1 was the most probable alternative of all the alternatives, according to the ranks of the alternatives acquired. This means that the security of A2 healthcare devices is the greatest of all the alternatives picked. A corroborative guide for the developers and the makers in quantitatively determining the security of healthcare devices to engineer efficacious devices will be the findings drawn up with the assistance of the proposed framework. The assessments performed using the proposed framework are systematic, precise, and definitive. Therefore, the results of the present empirical analysis are a stronger and accurate choice than the manual assessment of the device's security.

Keywords: Healthcare devices; HF-AHP.TOPSIS; device security

1 Introduction

Healthcare devices are the virtual lifelines of today's healthcare systems and are commonly used to avoid, track, or diagnose diseases. However, these devices have also become an easy target for cyber intrusions due to software and design-related vulnerabilities. Ironically, due to cyber-attacks, devices meant to protect the health of patients' are now becoming a major health threat. Only one among such breaches is the troubling instance of intruders gaining easy access to insulin pumps [1–5]. An exponential increase in attacks on the entire healthcare sector has been reported in the last few years. Security experts suggest that the high demand and cost of healthcare data on the dark web may be the explanation for this increase [6–9]. Several attacks on healthcare devices are carried out, risking not only the effectiveness of the system but also corrupting the data. For example, any running window system can easily target custom worm and infect more than 100 MRI machines at a time.

The FDA drafted a study that examined the security of healthcare devices in 2012 [2] to increasing episodes of breaches. The FDA issued a set of guidelines on the security of healthcare devices' for manufactures in 2013 [3]. Researchers, developers, and manufacturers are imminently needed to work on more foolproof mechanisms to resolve the threats to healthcare devices. Attempts to incorporate improved security measures right from the healthcare device design and development process would be a pre-emptive step in this direction [10–15].

In addition to the security of healthcare devices, the credibility of the devices [16–21] is yet another fact that needs to be improved. The security element of the device varies from the safety of the healthcare device's design. Although safety focuses on the hazardous circumstances that may arise accidentally and intensely, the security of the device from modifications to the data contained in the device may be made. Attacks on the healthcare network and network of healthcare devices threaten both the security of devices and the safety of information [22–25]. Due to the network breach of healthcare devices, research studies performed in this area have found many vulnerabilities and safety issues. Implantable Medical Devices (IMDs) [26], wearable devices [27,28] and surgical robots [29] are some of these devices. There are network flaws in the hospital network configuration [30–33], a third party service provider networks (like, laboratories, pharmacies, etc.) [34,35].

All these events allow the attackers to enter the network and take control. To gain access to the healthcare devices and steal the credentials [36–39] and exploit the vulnerabilities the attackers use the network. It is important to remove the efficacy that is sometimes introduced into healthcare devices due to design or software development to maximize the effectiveness of the healthcare devices [40–43]. The healthcare device credibility is thus an essential research premise and assumes greater significance in the efforts to make the medical devices more secure and reliable [44,45].

Against this context, the current research aims to examine the different security checking mechanisms and methodologies that are currently being used to determine the security of healthcare devices. The analysis then draws on the experts' views on the security of healthcare devices as inputs for the implementation of the proposed methodology. We will outline the relevant method, security examination mechanisms, and methodology for determining the security of the healthcare devices. As an insight into the methodology, we apply the expert's opinion about the security of the medical devices. And the debate on the empirical analysis of the method and sensitivity analysis of the empirical discussed.

2 Medical Device Security Mechanisms

Healthcare devices are effectively implanted and connected to the body of the patients and collect the body's sensitive data [46]. The device gathers the patient's activity of the body and sends it to the experts and laboratories through the network for processing. Network associated, low-power sensor-based devices are more vulnerable to intrusions. Many manufacturers want to supply embedded devices that use less power at a low cost. Therefore, additional safety mechanisms are not favored, which would make the device complex and raise the costs of manufacturing [47–49]. For example, when making on-site medical devices such as X-ray, MRI, and Ultrasound, etc., keeping the device secure and protecting it from hackers is not the priority of the developers.

Developer's concentrate on the working of the device, as most of them, do not even know about the safety and precautions. In a healthcare device, parts such as hardware and outdated software also invite vulnerabilities in the device that are easy for hackers to exploit [50,51]. Reverse engineering techniques can manipulate on-site devices and easily breach the security and availability of devices. The software and hardware layers are also part of the security needs [52,53]. Integrity, availability, authentication, confidentiality, safety and privacy, unauthorized tampering, are the essential features for developing highly secure healthcare devices. Due to traditional security algorithms that cannot be used because of implantable and sensor devices, maintaining the security of the devices is a tough task challenge.

But in recent years, refreshers have built a new algorithm for the CIA that resolve integrity and security issues. These are not ideal for all forms of cyber-attacks because of certain bars. The on-site healthcare devices (MRI, X-ray, and ultrasound) are also vulnerable to cyber-attacks [26–29]. Various techniques for preserving the security of the devices have been developed. Such approaches have been elucidated in Fig. 1.

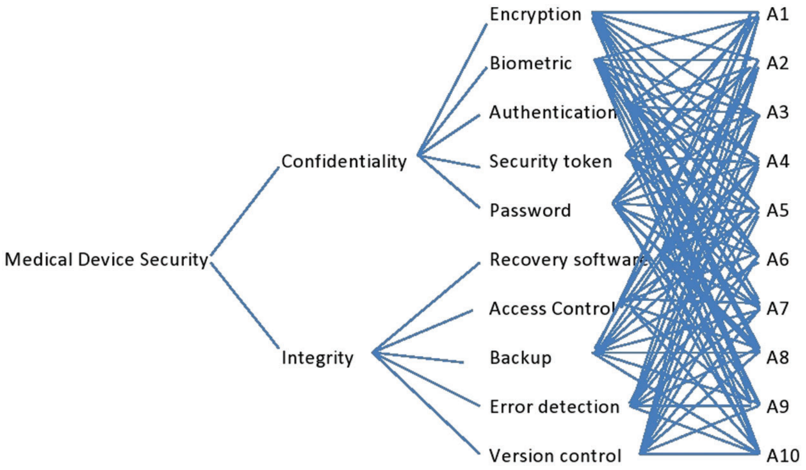

Figure 1: Medical devices security methods

2.1 Encryption

Converting the simple characters into some special type of code through a systematic algorithm is called the encryption process [20]. This process has a special position in security mechanics because it gives a special ability of secrecy to the sender's message or information.

2.2 Biometrics

Biometric is human physical or behavioral characteristics that can be used to identify an individual digitally to grant access to systems, devices, or information [21]. Fingerprints, facial expressions, speech, or typing are examples of these biometric signatures.

2.3 Authentication

The method of verifying the identity of a person or system is known as authentication [22]. When a person wants to log in, a typical example is entering a username and password. Entering the correct login information helps that person is accessing the device.

2.4 Security Token

A peripheral system used to gain access to an electronically limited resource is a security token [23]. In addition to or in place of a password, the token is used.

2.5 Password

A password, also referred to as a passcode, is a memorized secret, normally a character string generally used to confirm the identity of a user [23].

2.6 Recovery Software

After accident deletion, formatting, partition mistake, device crash, etc., data recovery software can help restore data [24]. This is used in the integrity of the data.

2.7 Access Control

Access control is a way of ensuring that people are who they say they are and that they have the right access to personal information [25].

2.8 Backup

A backup is a copy of data taken and stored somewhere so that it can be used during a data loss event to recover the original [26]. Backup is the verb form referring to the method of doing so, while a backup is the noun and adjective form.

2.9 Error Detection

Error detection is the method of identifying errors in a communication device that is present in the data transmitted from the transmitter to the receiver [27]. To recognize these errors, we use some redundancy codes by adding them to the data while it is transmitted from the source (transmitter).

2.10 Version Control

The practice of monitoring and handling modifications to software code is version control, often referred to as source control [28]. Version control systems are automated mechanisms that assist software teams to handle source code revisions over time.

3 Methodology Followed

Some real-world issues demand unique or multi choice-based solutions that are crucial for real users to conduct without any solid base. To tackle this situation and give an ideal quantitative solution to these issues the adopted MCDM approaches are implemented by various researchers. Specifically adopted AHP approach combined with fuzzy linguistic term set theory is more effective and simple in the comparison of others it is evident from various previous research initiatives [5,9]. If there is more than one option available for evaluation in the technique during the computation process, then this situation influences the calculated results even more strongly. In the context of the proposed article authors adopt a hesitant fuzzy set-based MCDM approach that gives an extra efficiency in results for evaluation. Besides, the TOPSIS approach has been used to assess the security of healthcare devices results obtained. Besides, to get more productive and accurate results, this study adopts the hesitant fuzzy approach. Moreover, for testing the evaluated results adopted the methodology of TOPSIS is the most promised and effective approach available in MCDM approaches. The biggest beneficial advantage of this methodology is that it gives a positive and negative both impact evaluation in the same evaluation and considers it in the calculation.

The authors followed the hesitant fuzzy set approach [15] when decision-makers find the possibility or situation of choosing any other value for numbering besides previously used ones. This type of situation opens a possibility of hesitant value use in evaluation which is prepared and discussed firstly by a study [28] and then modified and more systematically explained by Algarni et al. [14].

In cloud-based security architecture, Torra et al. [28] presented a TOPSIS integrated methodology that yielded successful results. For this article, the methodology adopted can skip and handle ambiguities and other AHP-TOPSIS methodology issues. Besides, by evaluating stock selection on paper, the model often validates its results. Similarly, Torra et al. [28,29] in their study have used the same approach. The authors verified the reliability of this technique by objectively analyzing the security of healthcare devices. Besides, Xu et al. [30] and Kumar et al. [31] have also used the specified technique to generate convincing results for their study in the sense of the energy solution.

In our research, HF-AHP methods were enlisted to estimate the priority of the healthcare device security factors, and then we tested their approach HF-TOPSIS on alternatives for similar factors [32]. A phase by phase methodology, in brief, is discussed below:

Phase 1: The first step in the implemented approach is the hierarchy development of factors.

Phase 2: In Tab. 1, examiners use linguistic terminology to create accurate and beneficial assessment criteria for the decision-makers.

Phase 3: The next step in technique evaluation is the adoption of fuzzy wrappers [29] from Eq. (1).

$$OWA(a_1,\ a_2,\ \ldots a_n) = \sum_{j=1}^{n} W_j b_j \tag{1}$$

Table 1: Scale for HF-AHP technique

Rank	Linguistic term	Abbreviation	Values
10	Absolutely high importance	AHI	(7.0000, 9.0000, 9.0000)
9	Very high importance	VHI	(5.0000, 7.0000, 9.0000)
8	Essentially high importance	ESHI	(3.0000, 5.0000, 7.0000)
7	Weakly high importance	WHI	(1.0000, 3.0000, 5.0000)
6	Equally high importance	EHI	(1.0000, 1.0000, 3. 0000)
5	Exactly equal	EE	(1.0000, 1. 0000, 1.0000)
4	Equally low importance	ELI	(0.3300, 1.0000, 1.0000)
3	Weakly low important	WLI	(0.2000, 0.3300, 1.0000)
2	Essentially low importance	ESLI	(0.1400, 0.2000, 0.3300)
1	Very low importance	VLI	(0.1100, 0.1400, 0.2000)
0	Absolutely low importance	ALI	(0.1100, 0.1100, 0.1400)

Same as experts evaluate the trapezoidal numbers $\tilde{C} = (a,\ b,\ c,\ d)$ by the Eqs. (2)–(5) after Eq. (1).

$$a = min\{a_L^i,\ \ a_M^i,\ a_M^{i+1},\ \ \ldots\ldots a_M^j,\ a_R^j\} = a_L^i \tag{2}$$

$$d = max\{a_L^i,\ \ a_M^i,\ a_M^{i+1},\ \ \ldots\ldots a_M^j,\ a_R^j\} = a_R^j \tag{3}$$

$$b = \left\{ \begin{array}{c} a_M^i,\ if\ i+1=j \\ OWA_w\ 2\left(a_m^j,\ \ldots\ldots a_m\ \frac{i+j}{2} \right),\ if\ i{+}j\ is\ even \\ OWA_w\ 2\left(a_m^j,\ \ldots\ldots a_m\ \frac{i+j+1}{2} \right),\ if\ i{+}j\ is\ odd \end{array} \right\} \tag{4}$$

$$c = \left\{ \begin{array}{c} a_M^{i+1},\ if\ i+1=j \\ OWA_{w_2}\left(a_m^j a_m^{j-1},\ .....a_m \dfrac{(i+j)}{2} \right),\ if\ i{+}j\ is\ even \\ OWA_{w_2}\left(a_m^j, a_m^{j-1}\ .....a_m \dfrac{(i+j+1)}{2} \right),\ if\ i{+}j\ is\ odd \end{array} \right\} \tag{5}$$

After imposing the Eqs. (3)–(5), the experts decide the first and second form of weights η, i.e., the number between [0, 1] and Eqs. (6)–(7) applied by the experts to obtain these numbers.

1st type weights $(W1 = (w_1^1,\ w_2^1,\ \ldots\ldots.w_n^1))$:

$$w_1^1 = \eta_2,\ \ w_2^1 = \eta_2(1-\eta_2),\ \ \ldots\ldots.w_n^1\eta_2(1-\eta_2)^{n-2} \tag{6}$$

2nd type weights $\left(W2 = \left(w_1^2,\ w_2^2,\ \ldots\ldots.w_n^2\right)\right)$:

$$w_1^2 = \eta_1^{n-1},\ \ w_2^2 = (1-\eta_1)\eta_1^{n-1} \tag{7}$$

The numerical form for the highest rank in the formula $\eta_1 = \dfrac{g-(j-1)}{g-1}$ s, and $\eta_2 = \dfrac{g-(j-1)}{g-1}$ is g and lowest, highest rank factors are shown by i and j, respectively.

Phase 4: Eqs. (8)–(9) are used by the experts after evaluating the entire previous approach to satisfy the remaining comparison matrix attributes. Thereafter, experts use Eq. (10) to defuzzify the matrix to determine the comparison matrix.

$$\tilde{A} = \begin{bmatrix} 1 & \cdots & \tilde{c}_{1n} \\ \vdots & \ddots & \vdots \\ \tilde{c}_{n1} & \cdots & 1 \end{bmatrix} \tag{8}$$

$$\tilde{c}_{ji} = \left(\frac{1}{cij_u}, \frac{1}{cij_{m2}}, \frac{1}{cij_{m1}}, \frac{1}{cij_1} \right) \tag{9}$$

$$\mu_x = \frac{l + 2m_1 + 2m_2 + h}{6} \tag{10}$$

Phase 5: The phase of defuzzification provides correct values. The experts examine the Consistency Ratio (CR) by applying the Eqs. (11)–(12) to analyse the CR of these values.

$$CI = \frac{\gamma_{max} - n}{n-1} \tag{11}$$

$$CR = \frac{CI}{RI} \tag{12}$$

Phase 6: In this step, by Eq. (13), the experts assess the geometrical mean of the values.

$$\tilde{r}_i = \left(\tilde{c}_{i1} \bigotimes \tilde{c}_{i2} \ldots\ldots \bigotimes \tilde{c}_{in} \right)^{1/n} \tag{13}$$

Phase 7: The most significant criterion in the entire set is evaluated by experts by applying the Eq. (14).

$$\tilde{w}_i = \tilde{r}_1 \bigotimes \left(\tilde{r}_1 \bigoplus \tilde{r}_2 \ldots\ldots.\tilde{r}_n\right)^{-1} \tag{14}$$

Phase 8: Examiners analyze the defuzzified values by Eq. (15).

$$\mu_x = \frac{l + 2m_1 + 2m_2 + h}{6} \tag{15}$$

Phase 9: By applying the Eq. (16), experts transform the defuzzified values into normalized values or weights.

$$\frac{\tilde{w}_i}{\sum_i \sum_j \tilde{w}_j} \tag{16}$$

Now after identifying priority list for selected attributes the second adopted methodology of TOPSIS is used for testing the effectiveness of obtained results. TOPSIS is effective as a MADM technique in recommending the most preferred option for use. The definition of the TOPSIS approach was introduced by Lai et al. The synthesis of positive and negative ideas is the TOPSIS methodology; the most accurate and effective option is the most precise and reliable factor. The worst option, on the other hand, is an irrelevant factor. The authors utilized the hesitant fuzzy AHP TOPSIS approach to test and assess the security of healthcare devices [14]. The TOPSIS method associates the distance between two linguistic values such as H1s and H2s and performs its computations. Below, the procedure has been clarified (Eq. (17)):

$$d(H1s,\ H2s) = |q^* - q| + |p^* - p| \tag{17}$$

Phase 10: The following terms are described as the starting process:

The following written formulas are applied as $(C = \{C_1,\ C_2,\ \ldots.. C_E\})$ and n criteria $(C = \{C_1,\ C_2,\ \ldots.. C_n\})$ to define alternatives and criteria in TOPSIS.

Similarly, k is used to show the numeric count of experts in TOPSIS e_x Denotes the experts.

The equation $\tilde{X}^l = \left[H^l_{S_{ij}}\right]_{E\times n}$ is used in TOPSIS technique to represent HF matrix.

The standards are written for TOPSIS to determine the criteria and effect of outcomes:

The standard for TOPSIS evaluation lies in between very poor and very good scale,

r_1^1 = between medium and good (bt M&G)

r_2^1 = at most medium (am M)

r_1^2 = at least good (al G)

r_2^2 = between very bad and medium (bt VB&M)

For HF matrix, the following formulas are used [9]:

env_F(EGH (btM&G)) = T (0.3300, 0.5000, 0.6700, 0.8300)

env_F(EGH (amM)) = T (0.0000, 0.0000, 0.3500, 0.6700)

env_F(EGH (alG)) = T (0.5000, 0.8500, 1.0000, 1.0000)

env_F(EGH (btVB&M)) = T (0.0000, 0.3000, 0.3700, 0.6700)

Phase 11: By applying the Eq. (18) formula, the associated combined matrix is created:

$$T_{pij} = min\left\{min_{i=1}^{K}\left(maxH_{t_{ij}}^{x}\right),\ max_{i=1}^{K}\left(minH_{t_{ij}}^{x}\right)\right\}$$

$$T_{qij} = max\left\{min_{i=1}^{K}\left(maxH_{t_{ij}}^{x}\right),\ max_{i=1}^{K}\left(minH_{t_{ij}}^{x}\right)\right\} \tag{18}$$

Phase 12: The effective factor where most effective factor is indicated by Aj, is shown by alpha in the TOPSIS evaluation, and alpha shows the cost-related preferences. In addition, the latest efficient alternatives need high precision for cost related preferences. The following Eqs. (19)–(22) are used to define and compare cost as well as effective factors:

$$\tilde{V}_{pj}^{+} = max_{i=1}^{K}\left(max_i\left(minH_{S_{ij}}^{x}\right)\right)\ j \in \alpha_b \text{ and } \mathrm{min}_{\mathrm{i}=1}^{\mathrm{K}}\left(\mathrm{min}_{\mathrm{i}}\left(\mathrm{minH}_{\mathrm{S}_{\mathrm{ij}}}^{\mathrm{x}}\right)\right)\ \mathrm{j} \in \alpha_{\mathrm{c}}) \tag{19}$$

$$\tilde{V}_{qj}^{+} = max_{i=1}^{K}\left(max_i\left(minH_{S_{ij}}^{x}\right)\right)\ j \in \alpha_b \text{ and } \mathrm{min}_{\mathrm{i}=1}^{\mathrm{K}}\left(\mathrm{min}_{\mathrm{i}}\left(\mathrm{minH}_{\mathrm{S}_{\mathrm{ij}}}^{\mathrm{x}}\right)\right)\ \mathrm{j} \in \alpha_{\mathrm{c}}) \tag{20}$$

$$\tilde{V}_{pj}^{-} = max_{i=1}^{K}\left(max_i\left(minH_{S_{ij}}^{x}\right)\right)\ j \in \alpha_c \text{ and } \mathrm{min}_{\mathrm{i}=1}^{\mathrm{K}}\left(\mathrm{min}_{\mathrm{i}}\left(\mathrm{minH}_{\mathrm{S}_{\mathrm{ij}}}^{\mathrm{x}}\right)\right)\ \mathrm{j} \in \alpha_{\mathrm{b})} \tag{21}$$

$$\tilde{V}_{qj}^{-} = max_{i=1}^{K}\left(max_i\left(minH_{S_{ij}}^{x}\right)\right)\ j \in \alpha_c \text{ and } \mathrm{min}_{\mathrm{i}=1}^{\mathrm{K}}\left(\mathrm{min}_{\mathrm{i}}\left(\mathrm{minH}_{\mathrm{S}_{\mathrm{ij}}}^{\mathrm{x}}\right)\right)\ \mathrm{j} \in \alpha_{\mathrm{b})} \tag{22}$$

Phase 13: Experts evaluate TOPISIS +ve and −ve concepts components by applying following Eqs. (23)–(24).

$$D^{+} = \begin{bmatrix} d\left(x_{11},\ \tilde{V}_1^{+}\right)+ & d\left(x_{12},\ \tilde{V}_2^{+}\right)+ & \ldots +d\left(x_{1n},\ \tilde{V}_n^{+}\right) \\ d\left(x_{21},\ \tilde{V}_1^{+}\right)+ & d\left(x_{22},\ \tilde{V}_2^{+}\right)+ & \ldots +d\left(x_{21},\ \tilde{V}_n^{+}\right) \\ d\left(x_{m1},\ \tilde{V}_1^{+}\right)+ & d\left(x_{m2},\ \tilde{V}_1^{+}\right)+ & \ldots +d\left(x_{mn},\ \tilde{V}_n^{+}\right) \end{bmatrix} \tag{23}$$

$$D^{-} = \begin{bmatrix} d\left(x_{11},\ \tilde{V}_1^{-}\right)+ & d\left(x_{12},\ \tilde{V}_2^{-}\right)+ & \ldots +d\left(x_{1n},\ \tilde{V}_n^{-}\right) \\ d\left(x_{21},\ \tilde{V}_1^{-}\right)+ & d\left(x_{22},\ \tilde{V}_2^{-}\right)+ & \ldots +d\left(x_{21},\ \tilde{V}_n^{-}\right) \\ d\left(x_{m1},\ \tilde{V}_1^{-}\right)+ & d\left(x_{m2},\ \tilde{V}_1^{-}\right)+ & \ldots +d\left(x_{mn},\ \tilde{V}_n^{-}\right) \end{bmatrix} \tag{24}$$

Phase 14: Experts build and assess the closeness of positive and negative factors evaluated by Eqs. (25)–(26).

$$CS(A_i) = \frac{D_i^{+}}{D_i^{+} + D_i^{-}}\ , \qquad i = 1,\ 2,\ \ldots .m \tag{25}$$

where

$$D_i^{+} = \sum_{j=1}^{n} d\left(x_{ij},\ V_j^{+}\right) \text{ and } \mathrm{D}_{\mathrm{i}}^{-} = \sum_{\mathrm{j}=1}^{\mathrm{n}} \mathrm{d}\left(\mathrm{x}_{\mathrm{ij}},\ \mathrm{V}_{\mathrm{j}}^{-}\right) \tag{26}$$

Phase 15: The ranks are allocated to conclude the process, and the tabular forms of options are focused on their assessment of effectiveness.

In further parts of this study, a highly detailed and evaluated numerical assessment of healthcare device security has been conducted.

4 Data Analysis

In this section, authors discussed the analysis of results of the proposed method, and compare the proposed method with existing methods to verdict the proposed method advantages.

4.1 Security Assessment

Managing security and its characteristic in a system is crucial and challenging task for experts. Security measures for healthcare devices can be enhanced with the aid of quantitative evaluation. But because of growing security breaches and user dissatisfaction, practitioners are often confused during process of development. Therefore, to avoid this situation and manage the security perfectly adopted approach is used for evaluation in this proposed article. Further, it is decision-making challenge to ensure the security of healthcare devices. To quantitatively analyze and solve this kind of dilemma, there are so many decision-making processes.

Firstly, in order to conduct the adopted evaluation approach forty five different experts for academic and industry background are called on a virtual meeting environment for discussion. During this discussion they get briefly introduced by topic of research and then selected attributes in order to achieve the desired objective. O the basis of that introduction and their own experience in relevant field they provide values that work as key decision makers in the evaluation. Further, on the basis of their values authors prepare matrix for evaluation which are portray by them in following headings. At level 1 of the hierarchy, two characteristics are shown according to Fig. 1. In the gathering, both practitioners were given a joint decision. Fuzzy envelops (consistent) for features at level 1 are shown in Tab. 2.

Table 2: Fuzzy envelopers for characteristics of level 1

	F1	F2
F1	EE	B/W EHI and WHI
F2	–	EE

The accuracy of every evaluation was checked by phase 5 and Eqs. (1)–(12) after obtaining the score. The consistency was found to be lower than 0.1 for all groups characteristics of the hierarchy. The results of level 1 function from Tabs. 1 and 2 and Eqs. (1)–(12) were evaluated by the authors as follows:

"B/W EHI and WHI" were designated as the fuzzy envelope (F1). The linguistic values associated with the Triangular Fuzzy Numbers (TFN) are (1, 1, 3) and (1, 3, 5), respectively. The trapezoidal fuzzy numbers $\tilde{C} = (a, b, c, d)$, representing the linguistic value, are estimated from Eqs. (1)–(5). Tab. 3 describes the calculated results at level 1.

Table 3: Trapezoidal fuzzy pair-wise comparison matrix at level 1

	F1	F2
F1	1.00000, 1.00000, 1.00000, 1.00000	1.00000, 1.00000, 3.00000, 5.00000
F2	0.20000, 0.33000, 1.00000, 1.00000	1.00000, 1.00000, 1.00000, 1.00000

Calculating the fuzzy weights of characteristics, from Eqs. (13)–(14). After that by Eq. (14), the weight of corresponding characteristic can be evaluated. In addition, from Eq. (15), the defuzzified value of respective characteristic is calculated and the weights are finally normalized by Eq. (16).

The same method for evaluating fuzzy local weights as shown in Tab. 3 is used to describe attributes weightage present in next layer of first layer. Further, global weights and ranks of the attributes are shown in Tab. 4. Moreover, Tabs. 5 and 6 are available to present values based on the level and its importance towards usability of device security, with the help of Eqs. (17)–(22). Further, Tab. 7 and Fig. 2 show the satisfaction degree of alternatives and overall impacts obtained by Eqs. (23)–(26).

Table 4: Global weights through the hierarchy

Factors of L. 1	Local weights	Factors of L. 2	Local weights	Global weights	Defuzzified and normalized weights		Priority
C1	0.07225, 0.12226, 0.13524, 0.25226	C11	0.07625, 0.21245, 0.45525, 1.23156	0.00212, 0.01548, 0.04547, 0.15556	0.04562	4.562%	7
		C12	0.03525, 0.09724, 0.19826, 0.51326	0.00256, 0.00968, 0.01787, 0.07778	0.10156	10.156%	5
		C13	0.03556, 0.09747, 0.19826, 0.51356	0.00556, 0.02857, 0.06154, 0.24574	0.01181	1.181%	10
		C14	0.12256, 0.26564, 0.58441, 1.43256	0.00457, 0.01025, 0.02458, 0.13254	0.30155	30.155%	1
		C15	0.06225, 0.12584, 0.41547, 0.65264	0.00658, 0.03055, 0.07584, 0.26587	0.11164	11.164%	3
C2	0.11214, 0.28226, 0.33214, 0.51226	C21	0.03552, 0.09726, 0.19854, 0.51385	0.03565, 0.06547, 0.07654, 0.11254	0.22512	22.512%	2
		C22	0.03315, 0.12985, 0.21256, 0.78195	0.00236, 0.08574, 0.09025, 0.13654	0.10236	10.236%	4
		C23	0.03197, 0.07869, 0.12156, 0.39568	0.01254, 0.01958, 0.12547, 0.32547	0.01434	1.434%	9
		C24	0.03526, 0.09568, 0.19256, 0.51356	0.00658, 0.03055, 0.07584, 0.26587	0.03375	3.375%	8
		C25	0.02356, 0.07457, 0.11356, 0.50326	0.00556, 0.02857, 0.06154, 0.24574	0.05225	5.225 %	6

Table 5: Subjective cognition matrix

Characteristics/ alternatives	A1	A2	A3	A4	A5	A6	A7	A8	A9	A10
F11	1.18000, 2.82000, 4.82000, 6.45000	2.09000, 3.73000, 5.73000, 6.45000	2.82000, 4.64000, 6.64000, 8.72000	1.55000, 3.18000, 5.18000, 6.72000	1.18000, 2.82000, 4.82000, 6.45000	2.09000, 3.73000, 5.73000, 6.45000	2.09000, 3.73000, 5.73000, 6.45000	2.82000, 4.64000, 6.64000, 8.72000	1.18000, 2.82000, 4.82000, 6.45000	2.09000, 3.73000, 5.73000, 6.45000
F12	0.82000, 2.27000, 4.27000, 6.65000	2.91000, 4.64000, 6.00000, 6.45000	1.18000, 2.82000, 4.82000, 6.45000	2.09000, 3.73000, 5.73000, 6.45000	0.82000, 2.27000, 4.27000, 6.65000	2.91000, 4.64000, 6.00000, 6.45000	2.09000, 3.73000, 5.73000, 6.45000	1.18000, 2.82000, 4.82000, 6.45000	2.09000, 3.73000, 5.73000, 6.45000	2.82000, 4.64000, 6.64000, 8.72000
F13	1.18000, 2.82000, 4.82000, 6.45000	2.09000, 3.73000, 5.73000, 6.45000	2.82000, 4.64000, 6.64000, 8.72000	1.18000, 2.82000, 4.82000, 6.45000	2.09000, 3.73000, 5.73000, 6.45000	2.82000, 4.64000, 6.64000, 8.72000	1.18000, 2.82000, 4.82000, 6.45000	2.09000, 3.73000, 5.73000, 6.45000	2.82000, 4.64000, 6.64000, 8.72000	1.55000, 3.18000, 5.18000, 6.72000
F14	1.18000, 2.82000, 4.82000, 6.45000	2.09000, 3.73000, 5.73000, 6.45000	1.18000, 2.82000, 4.82000, 6.45000	2.09000, 3.73000, 5.73000, 6.45000	2.82000, 4.64000, 6.64000, 8.72000	1.55000, 3.18000, 5.18000, 6.72000	2.09000, 3.73000, 5.73000, 6.45000	2.82000, 4.64000, 6.64000, 8.72000	1.18000, 2.82000, 4.82000, 6.45000	2.09000, 3.73000, 5.73000, 6.45000
F15	0.82000, 2.27000, 4.27000, 6.65000	1.18000, 2.82000, 4.82000, 6.45000	2.09000, 3.73000, 5.73000, 6.45000	2.82000, 4.64000, 6.64000, 8.72000	1.55000, 3.18000, 5.18000, 6.72000	1.45000, 3.18000, 5.18000, 7.72000	2.09000, 3.73000, 5.73000, 6.45000	2.82000, 4.64000, 6.64000, 8.72000	1.18000, 2.82000, 4.82000, 6.45000	2.09000, 3.73000, 5.73000, 6.45000
F21	2.45000, 4.27000, 6.27000, 8.65000	0.82000, 2.27000, 4.27000, 6.65000	2.91000, 4.64000, 6.00000, 6.45000	1.45000, 3.00000, 4.91000, 5.45000	1.18000, 2.82000, 4.82000, 6.40500	2.09000, 3.73000, 5.73000, 6.45000	2.09000, 3.73000, 5.73000, 6.45000	1.18000, 2.82000, 4.82000, 6.45000	2.09000, 3.73000, 5.73000, 6.45000	2.82000, 4.64000, 6.64000, 8.72000
F22	5.36000, 6.36000, 7.12000, 8.51000	3.73000, 5.73000, 7.55000, 8.65000	1.18000, 2.82000, 4.82000, 6.45000	2.09000, 3.73000, 5.73000, 6.45000	2.82000, 4.64000, 6.64000, 8.72000	1.55000, 3.18000, 5.18000, 6.72000	1.18000, 2.82000, 4.82000, 6.45000	2.09000, 3.73000, 5.73000, 6.45000	2.82000, 4.64000, 6.64000, 8.72000	1.55000, 3.18000, 5.18000, 6.72000
F23	1.55000, 3.18000, 5.18000, 6.72000	1.18000, 2.82000, 4.82000, 6.45000	2.09000, 3.73000, 5.73000, 6.45000	2.09000, 3.73000, 5.73000, 6.45000	2.09000, 3.73000, 5.73000, 6.45000	2.82000, 4.64000, 6.64000, 8.72000	1.18000, 2.82000, 4.82000, 6.45000	2.09000, 3.73000, 5.73000, 6.45000	2.82000, 4.64000, 6.64000, 8.72000	2.82000, 4.64000, 6.64000, 8.72000
F24	1.18000, 2.82000, 4.82000, 6.45000	2.09000, 3.73000, 5.73000, 6.45000	2.82000, 4.64000, 6.64000, 8.72000	1.18000, 2.82000, 4.82000, 6.45000	2.09000, 3.73000, 5.73000, 6.45000	2.82000, 4.64000, 6.64000, 8.72000	1.18000, 2.82000, 4.82000, 6.45000	2.09000, 3.73000, 5.73000, 6.45000	2.82000, 4.64000, 6.64000, 8.72000	1.55000, 3.18000, 5.18000, 6.72000
F25	2.09000, 3.73000, 5.73000, 6.45000	2.82000, 4.64000, 6.64000, 8.72000	1.55000, 3.18000, 5.18000, 6.72000	2.09000, 3.73000, 5.73000, 6.45000	2.09000, 3.73000, 5.73000, 6.45000	1.18000, 2.82000, 4.82000, 6.45000	2.09000, 3.73000, 5.73000, 6.45000	2.82000, 4.64000, 6.64000, 8.72000	1.55000, 3.18000, 5.18000, 6.72000	1.45000, 3.18000, 5.18000, 7.70200

Table 6: The weighted normalized matrix

Characteristics/ Alternatives	A1	A2	A3	A4	A5	A6	A7	A8	A9	A10
F11	0.03200, 0.05300, 0.07200, 0.09800	0.00800, 0.01200, 0.01600, 0.02100	0.11500, 0.16700, 0.18300, 0.19900	0.14200, 0.17900, 0.19800, 0.21900	0.03200, 0.05300, 0.07200, 0.09800	0.05550, 0.08700, 0.10400, 0.12200	0.03200, 0.05300, 0.07200, 0.09800	0.00800, 0.01200, 0.01600, 0.02100	0.11500, 0.16700, 0.18300, 0.19900	0.14200, 0.17900, 0.19800, 0.21900
F12	0.03200, 0.05300, 0.07200, 0.09800	0.05550, 0.08700, 0.10400, 0.12200	0.04280, 0.05900, 0.06400, 0.06800	0.03440, 0.05700, 0.08200, 0.11000	0.04700, 0.07400, 0.09200, 0.11200	0.03200, 0.05300, 0.07200, 0.09800	0.03200, 0.05300, 0.07200, 0.09800	0.05550, 0.08700, 0.10400, 0.12200	0.04280, 0.05900, 0.06400, 0.06800	0.03440, 0.05700, 0.08200, 0.11000
F13	0.08540, 0.09300, 0.09300, 0.09860	0.03200, 0.05300, 0.07200, 0.09800	0.00800, 0.01200, 0.01600, 0.02100	0.11500, 0.16700, 0.18300, 0.19900	0.14200, 0.17900, 0.19800, 0.21900	0.14200, 0.17900, 0.19800, 0.21900	0.08540, 0.09300, 0.09300, 0.09860	0.03200, 0.05300, 0.07200, 0.09800	0.00800, 0.01200, 0.01600, 0.02100	0.11500, 0.16700, 0.18300, 0.19900
F14	0.05550, 0.08700, 0.10400, 0.12200	0.04280, 0.05900, 0.06400, 0.06800	0.03440, 0.05700, 0.08200, 0.11000	0.05550, 0.08700, 0.10400, 0.12200	0.04280, 0.05900, 0.06400, 0.06800	0.03440, 0.05700, 0.08200, 0.11000	0.05550, 0.08700, 0.10400, 0.12200	0.04280, 0.05900, 0.06400, 0.06800	0.03440, 0.05700, 0.08200, 0.11000	0.05550, 0.08700, 0.10400, 0.12200
F15	0.05550, 0.08700, 0.10400, 0.12200	0.04280, 0.05900, 0.06400, 0.06800	0.03440, 0.05700, 0.08200, 0.11000	0.04700, 0.07400, 0.09200, 0.11200	0.00800, 0.01200, 0.01600, 0.02100	0.05550, 0.08700, 0.10400, 0.12200	0.04280, 0.05900, 0.06400, 0.06800	0.03440, 0.05700, 0.08200, 0.11000	0.04700, 0.07400, 0.09200, 0.11200	0.14200, 0.17900, 0.19800, 0.21900
F21	0.03200, 0.05300, 0.07200, 0.09800	0.00800, 0.01200, 0.01600, 0.02100	0.11500, 0.16700, 0.18300, 0.19900	0.14200, 0.17900, 0.19800, 0.21900	0.03200, 0.05300, 0.07200, 0.09800	0.00800, 0.01200, 0.01600, 0.02100	0.11500, 0.16700, 0.18300, 0.19900	0.14200, 0.17900, 0.19800, 0.21900	0.03200, 0.05300, 0.07200, 0.09800	0.05550, 0.08700, 0.10400, 0.12200
F22	0.03200, 0.05300, 0.07200, 0.09800	0.05550, 0.08700, 0.10400, 0.12200	0.04280, 0.05900, 0.06400, 0.06800	0.03440, 0.05700, 0.08200, 0.11000	0.03200, 0.05300, 0.07200, 0.09800	0.05550, 0.08700, 0.10400, 0.12200	0.04208, 0.05900, 0.06400, 0.06800	0.03440, 0.05700, 0.08200, 0.11000	0.04700, 0.07400, 0.09200, 0.11200	0.03200, 0.05300, 0.07200, 0.09800
F23	0.03200, 0.05300, 0.07200, 0.09800	0.00800, 0.01200, 0.01600, 0.02100	0.11500, 0.16700, 0.18300, 0.19900	0.14200, 0.17900, 0.19800, 0.21900	0.03200, 0.05300, 0.07200, 0.09800	0.03200, 0.05300, 0.07200, 0.09800	0.00800, 0.01200, 0.01600, 0.02100	0.11500, 0.16700, 0.18300, 0.19900	0.14200, 0.17900, 0.19800, 0.21900	0.03200, 0.05300, 0.07200, 0.09800
F24	0.03200, 0.05300, 0.07200, 0.09800	0.05550, 0.08700, 0.10400, 0.12200	0.04280, 0.05900, 0.06400, 0.06800	0.03440, 0.05700, 0.08200, 0.11000	0.04700, 0.07400, 0.09200, 0.11200	0.03200, 0.05300, 0.07200, 0.09800	0.05550, 0.08700, 0.10400, 0.12200	0.04280, 0.05900, 0.06400, 0.06800	0.03440, 0.05700, 0.08200, 0.11000	0.04700, 0.07400, 0.09200, 0.11200
F25	0.08540, 0.09300, 0.09300, 0.09860	0.03200, 0.05300, 0.07200, 0.09800	0.00800, 0.01200, 0.01600, 0.02100	0.11500, 0.16700, 0.18300, 0.19900	0.14200, 0.17900, 0.19800, 0.21900	0.08540, 0.09300, 0.09300, 0.09860	0.03200, 0.05300, 0.07200, 0.09800	0.00800, 0.01200, 0.01600, 0.02100	0.11500, 0.16700, 0.18300, 0.19900	0.14200, 0.17900, 0.19800, 0.21900

Table 7: Closeness coefficients of alternatives

Alternatives	d + i	d − i	Satisfaction Degree p_i	Ranks
Alternative 1	0.16264	0.07965	0.31367	2
Alternative 2	0.24574	0.12132	0.32564	1
Alternative 3	0.24225	0.07524	0.21265	9
Alternative 4	0.45658	0.16854	0.27658	4
Alternative 5	0.48447	0.18123	0.27457	6
Alternative 6	0.15154	0.06564	0.28958	3
Alternative 7	0.24695	0.07784	0.21265	10
Alternative 8	0.45485	0.16567	0.27657	5
Alternative 9	0.48894	0.18365	0.27267	7
Alternative 10	0.48888	0.18333	0.27111	8

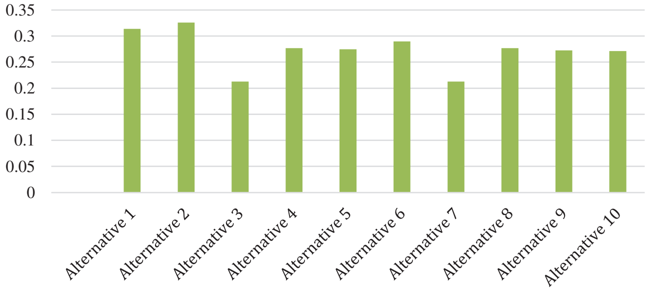

Figure 2: Graphical representation of satisfaction degrees

Tab. 7 and Fig. 2 represent the closeness coefficients of alternatives, in this table distance calculated from a positive and negative ideal solution and satisfaction degree is calculated. According to the satisfaction, degree assigns the ranks and we observed that alternative 2 obtain the highest ranks and best alternative after that A1 obtain the highest priority. After review, we checked the findings of our analysis by adjusting the variable.

4.2 Sensitivity Analysis and Comparison

Authors performed sensitivity analysis of the presented method in order to verified the accuracy and validity of results and compare with Ahmed's method [33], Algarni method [14] and classical method of both method with presented method in this paper has some advantages with rest method: presented method increase the acceptability/accuracy of the decision making results, easily determined the uncertainty in decision making, presented method can better reflect decision compared to other decision making method. Authors have done sensitivity analysis within 10 experiments because authors have chosen 10 alternatives in the last level of hierarchy of Fig. 1. In order to evaluate, the sensitivity weights of each factors are changed at various times, while the other factors weights and satisfaction levels are remain constant. Sensitivity analysis depicted on Tab. 8.

Table 8: Sensitivity analysis

Weights/ alternatives	A1	A2	A3	A4	A5	A6	A7	A8	A9	A10
Original weights	0.313670	0.325640	0.212650	0.276580	0.274570	0.289580	0.212650	0.276570	0.272670	0.271110
F11	0.357350	0.398069	0.346740	0.307708	0.312260	0.314507	0.314705	0.307708	0.312260	0.314507
F12	0.258507	0.287047	0.243604	0.202402	0.212560	0.217409	0.216302	0.202402	0.212560	0.217409
F13	0.258507	0.287047	0.243604	0.202402	0.212560	0.217409	0.216302	0.202402	0.212560	0.217409
F14	0.316095	0.345065	0.301904	0.248203	0.283250	0.292607	0.286504	0.248203	0.283250	0.292607
F15	0.318506	0.348087	0.302704	0.271250	0.272560	0.272607	0.272607	0.271250	0.272560	0.272607
F21	0.328509	0.355062	0.365470	0.269405	0.285740	0.294570	0.286509	0.269405	0.285740	0.294570
F22	0.258507	0.287047	0.243604	0.202402	0.212560	0.217409	0.216302	0.202402	0.212560	0.217409
F23	0.258507	0.287047	0.243604	0.202402	0.212560	0.217409	0.216302	0.202402	0.212560	0.217409
F24	0.316095	0.345065	0.301904	0.248203	0.283250	0.292607	0.286504	0.248203	0.283250	0.292607
F25	0.318506	0.348087	0.302704	0.271250	0.272560	0.272607	0.272607	0.271250	0.272560	0.272607

Authors performed comparison with other existent method; in the comparison same data applied by authors for evaluation the other methods available in the study. Comparison results with other methods is depicted in Tab. 9 and proof is available in results that HF-AHP-TOPSIS (proposed) method gives improved results in compare to other methods available in study.

Table 9: Different method results

Alternatives	(Proposed method)	(Algarni's method)	(Ahmed's method)	Classical Algarni's method	(Classical Ahmed's method)
1	0.313670	0.310020	0.307120	0.296720	0.312350
2	0.325640	0.320030	0.332230	0.309440	0.315340
3	0.212650	0.210020	0.202480	0.197140	0.213620
4	0.276580	0.270040	0.248120	0.260570	0.282440
5	0.274570	0.270060	0.270230	0.312140	0.274570
6	0.289580	0.280010	0.269580	0.281250	0.285550
7	0.212650	0.212610	0.212885	0.212223	0.212854
8	0.276570	0.276552	0.276447	0.276113	0.277769
9	0.272670	0.2726477	0.274545	0.272852	0.274425
10	0.271110	0.271111	0.271125	0.271132	0.274112

5 Discussion

The security of healthcare devices is compromised at the execution time by the method of data transfer, data storage, and migration process. By updating the software patch, using the hardware security guards and network encryption techniques all these problems can be addressed. Healthcare devices hold confidential information relating to the health and personal data of patients. We have established an approach for quantitative assessment of the security of healthcare devices from the proposed article through HF-AHP. TOPSIS approach in our framework, which is the best decision making and ranting approach. The decision-makers allocated the rating of the healthcare devices based on their security using this approach. The study has enlisted the help of 45 experts in different fields of security. Based on their experiences, they ranked the healthcare devices accordingly. Finally, on the provided data for performance assessment of the healthcare devices, HF.AHP.TOPSIS was applied. The findings of this research work as shows:

- Most researchers work on the security of healthcare devices, but do not have sufficient guidelines for the development and design of the software and security of the device.
- Our approach is systematic and provides the developers with effective guidelines to build the software by adhering to the security rules.
- Security evaluation of healthcare devices will not only ensure the operation of healthcare devices and the personal details of patients but will also improve the device's technological characteristics.
- Manufacturers and government agencies may use our framework to quantitatively and reliably verify the security of healthcare devices.

6 Conclusions

In the current situation, dependability on healthcare devices has improved enormously, more so in the aftermath of a health emergency such as the COVID-19 pandemic when home quarantine instead of attending hospitals was recommended to patients. For health care monitoring and treatment, doctors and patients alike depend on medical devices. Healthcare devices submit data from patients to physicians who prescribe the course of care after the data has been checked. However, the confidentiality of the data and system is under consideration. Even a small difference in the data of the patient can lead to an incorrect diagnosis, thus endangering the health and well-being of the patient. Quantitative and automated evaluation of the security of medical devices is an efficient solution for ensuring the security of the healthcare device. In the above observation, the A2 alternative obtains the highest ranks among the best alternatives. In the current analysis, this was done with the help of the HF-AHP.TOPSIS approach. Among the different alternatives, this method is best for decision making and provides corroborative results. This framework is well validated and tested; manufactures may use a tested approach to security checking to protect the healthcare devices.

Acknowledgement: This research was supported by Taif University Researchers Supporting Project number (TURSP-2020/211), Taif University, Taif, Saudi Arabia.

Funding Statement: This Project was funded by the Taif University Researchers Supporting Projects at Taif University, Kingdom of Saudi Arabia, under Grant Number: TURSP-2020/211.

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

References

[1] D. Halperin, T. S. H. Benjamin, B. Ransford, S. S. Clark, B. Defend *et al.,* "Pacemakers and implantable cardiac defibrillators: Software radio attacks and zero-power defenses," in *Proc. of the IEEE Symp. on Security and Privacy*, Oakland, CA, USA, pp. 129–142, 2008.

[2] C. Li, A. Raghunathan and N. Jha, "Hijacking an insulin pump: Security attacks and defenses for a diabetes therapy system," in *Proc. of the 2011 IEEE 13th Int. Conf. on e-Health Networking, Applications and Services*, Columbia, MO, USA, pp. 150–156, 2011.

[3] H. Almohri, L. Cheng, D. Yao and M. Alemzadeh, "On threat modeling and mitigation of medical cyber-physical systems," in *Proc. of the IEEE/ACM Int. Conf. on Connected Health: Applications*, System, Philadelphia, PA, USA, pp. 114–119, 2017.

[4] MassDevice, "Confickered! medical devices and digital medical records are getting hacked," 2009. [Online]. Available: https://www.massdevice.com/confickered-medical-devices-and-digital-medical-records-are-getting-hacked/.

[5] Business Wire, "Nomoreclipboard notice to individuals of a data security compromise," 2015. [Online]. Available: https://www.businesswire.com/news/home/20150610005964/en/NoMoreClipboard-Notice-to-Individuals-of-a-Data-Security-Compromise.

[6] GAO: U. S. Government Accountability Office, "Medical devices: FDA should expand its consideration of information security for certain types of devices," 2012. [Online]. Available: https://www.gao.gov/products/GAO-12-816.

[7] U. S. Food & Drug Administration, "FDA's role in regulating medical devices," 2018. [Online]. Available: https://www.fda.gov/medical-devices/home-use-devices/fdas-role-regulating-medical-devices.

[8] Y. Xu, D. Tran, Y. Tian and H. Alemzadeh, "Poster abstract: Analysis of cyber-security vulnerabilities of interconnected medical devices," in *Proc. of the 2019 IEEE/ACM Int. Conf. on Connected Health: Applications, Systems and Engineering Technologies*, Arlington, VA, USA, pp. 23–24, 2019.

[9] Wired Magazine, "Hospital networks are leaking data, leaving critical devices vulnerable," 2014. [Online]. Available: https://www.wired.com/2014/06/hospital-networks-leaking-data/.

[10] T. Bonaci, J. Yan, J. Herron, T. Kohno and H. J. Chizeck, "Experimental analysis of denial-of-service attacks on tele operated robotic systems," in *Proc. of the ACM/IEEE Sixth Int. Conf. on Cyber-Physical Systems*, New York, NY, USA, pp. 11–20, 2015.

[11] 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.

[12] G. McGraw, "Software security," *IEEE Security and Privacy*, vol. 2, no. 2, pp. 80–83, 2004.

[13] A. Algarni, M. Ahmad, A. Attaallah, 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. 13, no. 5, pp. 51–62, 2020.

[14] A. Algarni, 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.

[15] C. Bresch, S. Chollet and D. Hely, "Towards an inherently secure run-time environment for medical devices," in *Proc. of the IEEE Int. Congress on Internet of Things*, San Francisco, USA, pp. 140–147, 2018.

[16] N. Christoulakis, G. Christou, E. Athanasopoulos and S. Ioannidis, "HCFI: Hardware-enforced control-flow integrity," in *Proc. of the Sixth ACM Conf. on Data and Application Security and Privacy*, New York, NY, USA, pp. 38–49, 2016.

[17] A. I. Newaz, A. K. Sikder, L. Babun and A. S. Uluagac, "HEKA: A novel intrusion detection system for attacks to personal medical devices," in *Proc. of the 2020 IEEE Conf. on Communications and Network Security*, Avignon, France, pp. 1–9, 2020.

[18] L. Zhou and Y. Makris, "HAFIX: Hardware-assisted flow integrity extension," in *Proc. of the 52nd Annual Design Automation Conf.*, San Francisco, CA, USA, pp. 1550–1555, 2015.

[19] S. Gao and G. Thamilarasu, "Machine-learning classifiers for security in connected medical devices," in *Proc. of the 2017 26th Int. Conf. on Computer Communication and Networks*, Vancouver, BC, Canada, pp. 1–5, 2017.

[20] A. Ray and C. Rance, "An analysis method for medical device security," in *Proc. of the Symp. and Bootcamp on the Science of Security*, New York, NY, USA, pp. 1–2, 2014.

[21] V. Costan, I. Lebedev and S. Devadas, "Sanctum: Minimal hardware extensions for strong software isolation," in *Proc. of the 25th USENIX Security Symp., USENIX Security 16*, Austin, TX, USA, pp. 857–874, 2016.

[22] A. Ali and F. A. Khan, "Key agreement schemes in wireless body area networks: Taxonomy and state-of-the-art," *Journal of Medical Systems*, vol. 39, no. 10, pp. 1–14, 2015.

[23] D. Karaolan, A. Levi and V. Tuzcu, "Deriving cryptographic keys from physiological signals," *Pervasive and Mobile Computing*, vol. 39, no. 4, pp. 65–79, 2017.

[24] K. Sahu, F. A. Alzahrani, R. K. Srivastava and R. Kumar, "Hesitant fuzzy sets based symmetrical model of decision-making for estimating the durability of web application," *Symmetry*, vol. 12, no. 6, pp. 1770–1792, 2020.

[25] A. Attaallah, M. Ahmad, M. Tarique, A. K. Pandey, R. Kumar *et al.*, "Device security assessment of internet of healthcare things," *Intelligent Automation & Soft Computing*, vol. 27, no. 2, pp. 593–603, 2021.

[26] S. A. Khan, M. Alenezi, A. Agrawal, R. Kumar and R. A. Khan, "Evaluating performance of software durability through an integrated fuzzy-based symmetrical method of ANP and TOPSIS," *Symmetry*, vol. 12, no. 4, pp. 1–15, 2020.

[27] F. A. Alzahrani, M. Ahmad, M. Nadeem, R. Kumar and R. A. Khan, "Integrity assessment of medical devices for improving hospital services," *Computers, Materials & Continua*, vol. 67, no. 3, pp. 3619–3633, 2021.

[28] V. Torra and Y. Narukawa, "The index and the number of citations: Two fuzzy integrals," *IEEE Transactions on Fuzzy Systems*, vol. 16, no. 6, pp. 795–797, 2008.

[29] W. Alosaimi, R. Kumar, A. Alharbi, H. Alyami, A. Agrawal *et al.*, "Computational technique for effectiveness of treatments used in curing sars-cov-2," *Intelligent Automation & Soft Computing*, vol. 28, no. 3, pp. 617–628, 2021.

[30] X. Xu, Z. Shi and B. Pan, "A new unsupervised hyperspectral band selection method based on multi objective optimization," *IEEE Geoscience and Remote Sensing Letters*, vol. 14, no. 11, pp. 2112–2116, 2017.

[31] R. Kumar, M. Zarour, M. Alenezi, A. Agrawal and R. A. Khan, "Measuring security durability of software through fuzzy-based decision-making process," *International Journal of Computational Intelligence Systems*, vol. 12, no. 2, pp. 627–642, 2019.

[32] K. Sahu, F. A. Alzahrani, R. K. Srivastava and R. Kumar, "Evaluating the impact of prediction techniques: Software reliability perspective," *Computers, Materials & Continua*, vol. 67, no. 2, pp. 1471–1488, 2021.

[33] S. Ahmed and A. Alhumam, "Unified computational modeling for healthcare device security assessment," *Computer Systems Science and Engineering*, vol. 37, no. 1, pp. 1–18, 2021.

[34] R. Kumar, A. I. Khan, Y. B. Abushark, M. M. Alam, A. Agrawal *et al.*, "An integrated approach of fuzzy logic, AHP and TOPSIS for estimating usable-security of web applications," *IEEE Access*, vol. 8, no. 8, pp. 50944–50957, 2020.

[35] R. Kumar, S. A. Khan and R. A. Khan, "Fuzzy analytic hierarchy process for software durability: Security risks perspective," *Advances in Intelligent Systems and Computing*, vol. 508, pp. 469–478, 2017.

[36] R. Kumar, S. A. Khan and R. A. Khan, "Secure serviceability of software: Durability perspective," *Communications in Computer and Information Science*, vol. 628, pp. 104–110, 2016.

[37] R. Kumar, S. A. Khan and R. A. Khan, "Durability challenges in software engineering," *CrossTalk*, vol. 42, no. 4, pp. 29–31, 2016.

[38] R. Kumar, M. T. J. Ansari, A. Baz, H. Alhakami, A. Agrawal *et al.*, "A multi-perspective benchmarking framework for estimating usable-security of hospital management system software based on fuzzy logic, ANP and TOPSIS methods," *KSII Transactions on Internet and Information Systems*, vol. 15, no. 1, pp. 240–263, 2021.

[39] K. Sahu and R. K. Srivastava, "Soft computing approach for prediction of software reliability," *ICIC Express Letters*, vol. 12, no. 12, pp. 1213–1222, 2018.

[40] R. Kumar, M. Zarour, M. Alenezi, A. Agrawal and R. A. Khan, "Measuring security durability of software through fuzzy-based decision-making process," *International Journal of Computational Intelligence Systems*, vol. 12, no. 2, pp. 627–642, 2019.

[41] K. Sahu and R. K. Srivastava, "Needs and importance of reliability prediction: An industrial perspective," *Information Sciences Letters*, vol. 9, no. 1, pp. 33–37, 2020.

[42] R. Kumar, S. A. Khan and R. A. Khan, "Revisiting software security: Durability perspective," *International Journal of Hybrid Information Technology*, vol. 8, no. 2, pp. 311–322, 2015.

[43] W. Alosaimi, A. Alharbi, H. Alyami, M. Ahmad, A. K. Pandey *et al.*, "Impact of tools and techniques for securing consultancy services," *Computer Systems Science and Engineering*, vol. 37, no. 3, pp. 347–360, 2021.

[44] R. Kumar, S. A. Khan and R. A. Khan, "Durable security in software development: Needs and importance," *CSI Communications*, vol. 10, no. 10, pp. 34–36, 2015.

[45] R. Kumar, S. A. Khan and R. A. Khan, “Revisiting software security risks,” *Journal of Advances in Mathematics and Computer Science*, vol. 11, no. 6, pp. 1–10, 2015.

[46] K. Sahu and R. K. Srivastava, “Revisiting software reliability,” *Advances in Intelligent Systems and Computing*, vol. 802, pp. 221–235, 2019.

[47] R. Kumar, S. A. Khan and R. A. Khan, “Analytical network process for software security: A design perspective,” *CSI Transactions on ICT*, vol. 4, no. 2, pp. 255–258, 2016.

[48] R. Kumar, S. A. Khan, A. Agrawal and R. A. Khan, “Measuring the security attributes through fuzzy analytic hierarchy process: Durability perspective,” *ICIC Express Letters*, vol. 12, no. 6, pp. 615–620, 2018.

[49] K. Sahu and R. K. Srivastava, “‘Predicting software bugs of newly and large datasets through a unified neuro-fuzzy approach: Reliability perspective,” *Advances in Mathematics: Scientific Journal*, vol. 10, no. 1, pp. 543–555, 2021.

[50] R. Kumar, S. A. Khan and R. A. Khan, “Software security testing: A pertinent framework,” *Journal of Global Research in Computer Science*, vol. 5, no. 3, pp. 23–27, 2014.

[51] R. Kumar, A. I. Khan, Y. B. Abushark, M. M. Alam, A. Agrawal *et al.*, “A knowledge-based integrated system of hesitant fuzzy set, AHP and TOPSIS for evaluating security-durability of web applications,” *IEEE Access*, vol. 8, no. 8, pp. 48870–48885, 2020.

[52] M. T. J. Ansari, A. Baz, H. Alhakami, W. Alhakami, R. Kumar *et al.*, “P-STORE: Extension of store methodology to elicit privacy requirements,” *Arabian Journal for Science and Engineering*, pp. 1–24, Article in press, 2021.

[53] R. Kumar, A. Baz, H. Alhakami, W. Alhakami, A. Agrawal *et al.*, “A hybrid fuzzy rule-based multi-criteria framework for sustainable-security assessment of web application,” *Ain Shams Engineering Journal*, pp. 1–21, Article in press, 2021.