Computer Systems Science & Engineering
DOI:10.32604/csse.2021.015775
Article

Tech Science Press

Unified Computational Modelling for Healthcare Device Security Assessment

Shakeel Ahmed* **and Abdulaziz Alhumam**

Department of Computer Science, College of Computer Sciences and Information Technology King Faisal University, Al-Ahsa, 31982, Kingdom of Saudi Arabia
*Corresponding Author: Shakeel Ahmed. Email: shakeel@kfu.edu.sa
Received: 16 November 2020; Accepted: 20 December 2020

Abstract: This article evaluates the security techniques that are used to maintain the healthcare devices, and proposes a mathematical model to list these in the order of priority and preference. To accomplish the stated objective, the article uses the Fuzzy Analytic Network Process (ANP) integrated with Technical for Order Preference by Similarities to Ideal Solution (TOPSIS) to find the suitable alternatives of the security techniques for securing the healthcare devices from trespassing. The methodology is enlisted to rank the alternatives/ techniques based on their weights' satisfaction degree. Thereafter, the ranks of the alternatives determine the order of priority for the techniques used in healthcare security. The findings of our analysis cite that Machine Learning (ML) based healthcare devices obtained the highest priority among all the other security techniques. Hence the developers, manufacturers and researchers should focus on the ML techniques for securing the healthcare devices. The results drawn through the aid of the suggested mathematical model would be a corroborative reference for the developers and the manufacturers in assessing the security techniques of the healthcare devices.

Keywords: Medical devices; fuzzy-ANP.TOPSIS; security techniques; machine learning

1 Introduction

Healthcare devices play an essential role in digital treatment of the patients. Digital diagnosis enables the monitoring and diagnosis of the patients from any remote place. Internet of Healthcare Things (IoHT) and implantable devices are fully equipped by the sensors which take the data from the body and send the same to the healthcare organization for diagnosis and monitoring [1]. Healthcare wearable devices (*pulse reading, blood pressure, insulin pump* etc.) also sense the body's data [2]. All these data are highly sensitive, particularly from the patients' point of view because the data pertains to their personal health related information. If the data is leaked and altered, it could even be life threatening for the patients.

Healthcare devices are a soft target for the hackers because of the ineffective and inadequate security mechanisms that are applied on these devices [3]. The attackers take advantage of a lack of security mechanism and easily gain access to the healthcare devices [4]. In the last few years, the attacks on the

healthcare sector have risen exponentially. The reason for the increasing number of attacks on healthcare is the high demand and cost of the data on the dark web. Multiple attacks on the healthcare device not only affect the functionality of the device but also steal the data stored in the devices [5]. In 2012, Food and Drug Administration (FDA) formulated guidelines for analysing the security of the healthcare devices [6]. In the next year 2013, FDA issued guidelines for the developers and manufactures to design the devices and check the security at the time of developing the devices [7].

There is an imminent need for the researchers, developers and manufacturers to work on more fool proof mechanisms to contain the threats to medical devices. Attempts to integrate enhanced safety mechanisms right from the design and development phase of the medical devices would be a pre-emptive step in this direction. Healthcare device security is yet another facet that needs to be strengthened in the security of the devices. The design of healthcare device's security is different from the safety aspect of the healthcare device. While safety focuses on the hazardous situations that may happen accidentally and intensely, security of the device protects it against the alterations done in the device or the changes that might be made in the information stored in the device [8].

Networked devices are more vulnerable than the non-networked devices. Attacks on the networked devices threaten both the security of the device and safety of the information [9]. Several research studies have identified vulnerabilities and safety concerns that occur due to network compromise of the healthcare devices. Few are listed here: *Implantable Medical devices (IMDs), wearable devices and surgical robots* [10]. *Network vulnerabilities exist in the network configuration of the hospitals, third party service provider networks (like, laboratories, pharmacies etc.)*. These weaknesses permit the eavesdroppers to gain access over the network of the healthcare industry. The eavesdroppers make their way through the network to steal the credentials of the medical devices and exploit the vulnerabilities.

To optimise upon the efficacy of the healthcare devices, it is imperative to eliminate the vulnerabilities that are often inbuilt in the devices due to faults in design, software, hardware and network [11]. Hence, security of the healthcare device becomes an important research premise and assumes greater significance in the efforts to make the healthcare devices more secure and reliable. Against this backdrop, the present research pursuit intends to analyse the various security checking mechanisms and methodologies that are being used at present for assessing the security of the healthcare devices. Thereafter, the study draws upon the opinions of the experts regarding the security of the healthcare devices as inputs for applying the proposed methodology. We will outline the related approaches, security checking mechanisms and methodology for assessing the security of the healthcare devices.

2 Related Approaches

The authors referred to several useful studies that were done in the context of privacy and qualities of the healthcare devices. But, here we have discussed studies that essentially focus on maintaining the security of the healthcare device. Few of the relevant articles with specific reference to security are cited below:

Bresch et al. [12] designed an application for securing the medical devices which depend on the control flow of the program. In this approach, the secure code is assessed based on its functional and security point of view.

Newaz et al. [13] designed HEKA intrusion detection system (IDS) for tracing the traffic network of personal medical devices, HEKA used n-gram-based approach in traffic monitoring and different ML model was used for detection of the irregular traffic flow over the network. This IDS was validated on eights personal medical devices network and performance was calculated on four different attacks on it. The accuracy of the IDS of attacks detection was 98.4%.

Christoulakis et al. [14] – The authors proposed the HCFI architecture. This model defends the device from *code-reuse* attacks. This model verifies each edge by labelling in the execution flow graph of the

software. At the time of execution, flow transfer to each labels are verified. If the vertex labels are not matched, the event of the control-flow attacks can be detected easily. However, the model is vulnerable to data attacks.

Zhou et al. [15] - HAFIX architecture proposed the integrity flow of hardware assessment. In this model, authors used the graph's backward edges execution flow for identifying the code reuse attacks, however, the forward edge can be altered easily. Thus, this model is vulnerable to data attacks.

Gao et al. [16] proposed a ML based method and evaluated the feasibility of methods to detect the attacks easily. The authors also designed features sets for medical device to check even little changes in the working of the device.

Rayand et al. [17] proposed hardware signature security technique which detected the hardware Trojan (HT) at the time of run through verifying the hardware working functionality. In this architecture, the authors addressed the threats by splitting the design into a two chip method. Here, the signature generated at the beginning of data generating, and the signature is verified at the time of data encryption. This HT detection technique is able to detect HT attacks and also removes the attacks from the healthcare device.

Costan et al. [18] designed a Dynamic Time Warping (DTW) algorithm which is used in the authentication and identification of the authorized users whether they are accessing the device or not. The comparative results of this algorithm with other algorithms shows that this design algorithm is more efficient and light weight in comparison to the other algorithms.

The approaches discussed above provide knowledge about the security of medical devices. In the ensuing section, we have discussed different medical devices' security approaches that became the base for structuring the empirical framework of this study.

3 Healthcare Device Security Tactics

Healthcare devices are generally implanted and attached with the human body and collect the required data from the organs. Further, healthcare devices send the data over the network for the processing to the experts. Low power sensor-based healthcare devices associated with the network are more vulnerable to attacks. Healthcare demands low cost devices for best treatment. So the manufacturers try to provide low cost healthcare devices. But the security of the healthcare device is also important because of the sensitive information that is stored and processed in the devices [19]. Any additional security features increase the manufacturing costs and make the device complex. All devices have their own vulnerabilities like implantable devices have owns and on-sites devices have owns. Developers focus on the functionality of the device and most of them do not know about the safety and precautions of the device.

Medical device components like hardware and outdated software generate vulnerabilities in the device that become easy exploits for the hackers. On-site devices can be exploited by reverse engineering techniques and easily violate the integrity and availability of devices. Important features that make the healthcare devices more secure are: *availability, confidentiality and integrity (CIA)*. Maintaining the security of the devices is a tough task due to conventional security algorithms that cannot be used because of implantable and sensor devices [20]. But in the last few years, refreshers have developed new CIA prevention algorithms that do address the security issues of the healthcare devices. However, due to some bars, these are not suitable for all types of cyber-attacks. For instance, the on-site medical devices (MRI, X-ray and ultrasound) are still vulnerable to cyber-attacks. Various techniques have been developed for maintaining the security of the devices. Healthcare security approaches have been displayed in Fig. 1 and discussed below:

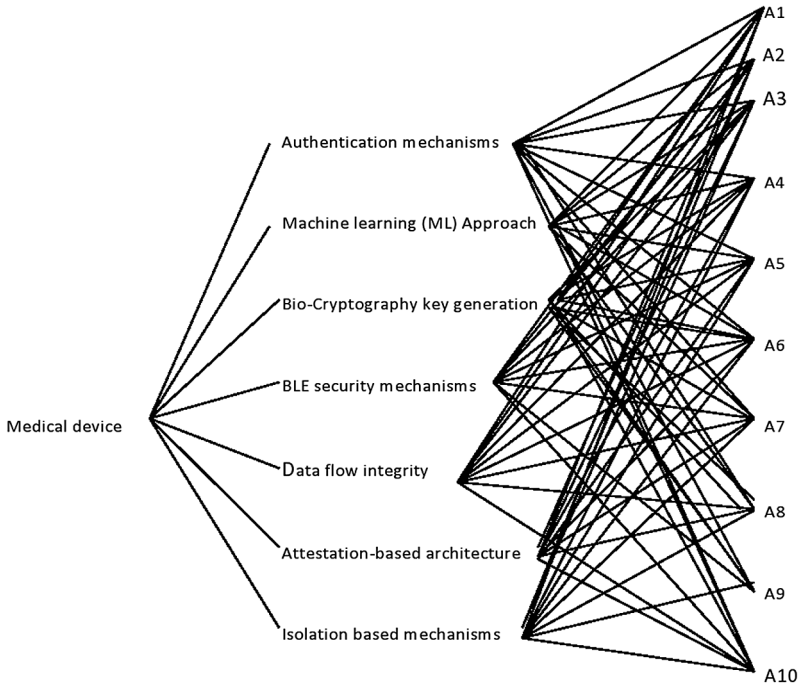

Figure 1: Security techniques in medical devices

3.1 Authentication Mechanisms

In this mechanism, the unauthorized access of data is prevented. AES 128 lightweight encryption is used with current hash message verification code where authentication mechanism is utilized for confirming the genuine user's access to the clinical gadget. Here *nonce* is utilized as an Introduction Vector (IV) for the encryption by utilizing the AES 128 key [21]. Unauthorized access is effectively prevented by this mechanism.

3.2 Machine Learning

Machine learning, is used as a computational method to learn from the information while relying on predetermined models. ML techniques are used in the present era for securing the healthcare data, network and healthcare devices from the attackers [16]. ML techniques make the healthcare data, network and devices more secure and help in fraud detection.

3.3 Data Flow

Data flow mechanism is used to maintain the security of the device. Code pointer plays an important role at the time of development for maintaining the security of the devices. The security of the pointer track is maintained by the pointer. The pointer is marked at source code at the compilation time. The base and bound values are stored in out of the range of hardware in these pointers. When the pointer is accessed, firstly, the pointer's validity is checked. If the pointer is altered in an unauthorized way, then the base and bound stored in memory do not match with the pointer's value [22]. This helps in finding the alteration in the system. Data flow is used in hardware custom to ensure software security.

3.4 Bio-Cryptography

Bio-cryptography is used in the security of the healthcare device and encryption the data for secure communication over the network. This technique uses blood pressure, PPG and ECG data through the sensors for producing the key for secure Cryptography on the healthcare data. Two approaches are used

for the generation of the secret key: first approach (physiological signals) is used for secret key generation, and the second is used for the inter-pulse interval (IPI) for frequency domain generation [23]. Both the approaches are important in cryptography key generation and for making the biological data secure.

3.5 Hardware Signature

Hardware security also needs attention because malicious hardware (Hardware Trojan) is inserted at the time of manufacturing medical devices. In this approach, the hardware signature is imposed at the time of data harvesting and then these signatures are verified at the time of data processing [17].

3.6 Attention Based

The *run-time attacks* on the devices are prevented by the attention based approach. In this approach, computing hashes and labelling vertices are used to manage the flow of the program. This approach resolves the remote code execution limitation. The technique also uses buffers overflow for verifying the medical device application in running accurately and performing well [13]. The limitation is that it does not consider data attacks and is not used fully by the software developers for the medical devices.

4 Methods and Results

In this section, we proposed the Fuzzy ANP.-TOPSIS based healthcare device security assessment. We have set the criteria and alternatives for the healthcare device for security assessment. Based on these criteria, we have evaluated the security of the healthcare device and found the best alternatives among them. The authors have integrated three different concepts in this paper and developed a new approach. The fuzzy set theory concepts, Analytic Network Process (ANP) and TOPSIS for selection of the best security algorithm are used for assessing the security of the healthcare devices [24]. This integrated approach is highly efficient and effective to elicit outcomes. The Fuzzy ANP.-TOPSIS has been explained and implemented here.

4.1 Fuzzy-ANP.TOPSIS

Assessment of the security of the healthcare device was done by using the multiple criteria decision-making technique (MCDM). Multiple criteria decision making method used here Analytic Network Process (ANP) technique. An essential type of Analytic Hierarchy Process concepts used in the Analytic network process (ANP) [24]. ANP is a network based systematic method which uses the fuzzy theory and network based process for the selection of the alternatives. Multiple conflicting opinions arise in other approaches. To resolve these varying and differing opinions in the process of choosing the most conversant alternatives, the MCDM approach proves to be the most effective procedure. And TOPSIS is a compensatory aggregation method which compares the alternatives with the obtained weights for each criteria, and finds the distance between the alternatives and ideal solution and assigns the ranks of each criteria [25,26].

Fuzzy-ANP-TOPSIS has been used for assessing the security of healthcare devices. In the Fuzzy-ANP. TOPSIS approach, attribute selection plays an important role for calculating the weights and ranks of each alternative. Here, fuzzy sets provide the condition where there is no limitation for judgments, ANP helps in selection alternatives and TOPSIS provides the ranks to each alternative. Triangular fuzzy number is chosen for assessing the decision-makers' preferences because of its simplicity in design and implementation. Fuzzy ANP-TOPSIS quantitative assessment is used because of the numerous data provided by the decision makers [26]. The step-by-step process of Fuzzy-ANP.TOPSIS is discussed in detail below:

Step 1: A fuzzy number (f) is represented as $f = \{(x, \mu_a(x), x \in a\}$ *where x is a set and* $\mu_a(x)$ is a mapping from X to between the [0,1].

Step 2: Triangular fuzzy number (TFN) is denoted as *a = (l, m, h)*, where *l, m, and h (l ≤ m ≤ h)* are boundaries demonstrating *the lowest*, the *middle value*, and the *higher value* in the TFN (Fig. 2), separately. Its membership value $\mu_a\,(x) = Tn \rightarrow [0,\ 1]$ is denoted as Eq. (1).

$$\mu_a(x) = \begin{cases} \dfrac{x}{m-l} - \dfrac{l}{m-l} & x \in [l, m] \\ \dfrac{x}{m-h} - \dfrac{h}{m-h} & x \in [m, h] \\ 0 & Otherwise \end{cases} \tag{1}$$

Qualitative scale described by linguistics terms along with the ratings given by the experts in a quantitative way and aligned with the TFNs is displayed in Tab. 1.

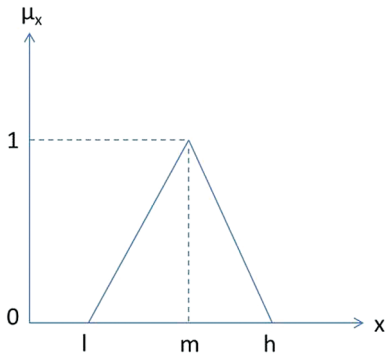

Figure 2: Triangular fuzzy number

Table 1: Scale of alternative ratings

Rating	Scale	TFNs
1	Equally important	(1, 1, 1)
3	Weakly important	(2, 3, 4)
5	Fairly important	(4, 5, 6)
7	Strongly important	(6, 7, 8)
9	Absolutely important	(9, 9, 9)
2	Intermittent values between two adjacent scales	(1, 2, 3)
4		(3, 4, 5)
6		(5, 6, 7)
8		(7, 8, 9)

Step 3: Qualitative Variables are converted into Quantitative Variables. With the help of Eqs. (2)–(5), qualitative variables are converted into quantitative form, and shown as (*lij, mij, hij*), where, *lij = lower, mij = middle and hij = higher values*. Further, TFN [ηij] are evaluated as:

$$\eta_{ij} = \left(l_{ij},\ m_{ij},\ h_{ij}\right) \tag{2}$$

where $l_{ij} \leq m_{ij} \leq h_{ij}$

$$l_{ij} = \min\left(J_{ijd}\right) \tag{3}$$

$$m_{ij} = \left(J_{ij1}, J_{ij2}, J_{ij3}\right)^{\frac{1}{x}} \tag{4}$$

$$\text{and } h_{ij} = \max\left(J_{ijd}\right) \tag{5}$$

In the Eqs. (2)–(5), J_{ijd} refers to the similar criticalness of the qualities between two rules given by the expert *d. i and j* refer to a few measures assessed by the experts.

By the extension rule, consider two TFNs M1 = (l_1, m_1, h_1) and M2 = (l_2, m_2, h_2) operations performed by Eqs. (6)–(8).

$$M1 + M2 = (l_1 + l_2,\ m_1 + m_2,\ h_2 + h_2) \tag{6}$$

$$M1 * M2 = (l_1 \times l_2,\ m_1 \times m_2,\ h_1 \times h_2) \tag{7}$$

$$(M)^{-1} = \left(\frac{1}{u_1}, \frac{1}{m_1}, \frac{1}{l_1}\right) \tag{8}$$

***Step 4: Consistency Index*:** After preparing the pair-wise decision-matrix, the Consistency Index (CI) is determined with the help of Eq. (9).

$$CI = (\gamma_{max} - N)/(N - 1) \tag{9}$$

Here, N = Number of analysed components.

***Step 5: Consistency Ratio*:** After calculating the consistency index, the Consistency Ratio (CR) is calculated by dividing the CI with Random Index (RI); RI is obtained from Saaty scale.

$$CR = CI/RI \tag{10}$$

***Step 6: Defuzzification*:** After the pair-wise comparison-matrix formulation, Fuzzy values are changed into crisp values with the help of Eqs. (11)–(13).

$$\mu_{\alpha,\beta}\left(\eta_{ij}\right) = \left[\beta.\eta\alpha\left(l_{ij}\right) + (1 - \beta).\ \eta\alpha\left(h_{ij}\right)\right] \tag{11}$$

Where, $0 \leq \alpha \leq 1$ and $0 \leq \beta \leq 1$

Such that,

$$\eta\alpha\left(l_{ij}\right) = \left(m_{ij} - l_{ij}\right).\alpha + l_{ij} \tag{12}$$

$$\eta\alpha\left(h_{ij}\right) = h_{ij} - \left(h_{ij} - m_{ij}\right).\alpha \tag{13}$$

For the option of experts, *α and β* are applied in these conditions; *α and β values* exist between the *range of 0 and 1*.

***Step 7: Super-matrix*:** All the connections are illustrated in the network, by using the *Markov* based approach; outline the fuzzy priorities of each criteria. The construction of the super matrix discusses the reaction of the matched evaluations among the goal, criteria, and alternatives.

***Step 8: TOPSIS*:** TOPSIS approach is used to obtain the ranks of the alternatives, the ratings of all the alternative options over every normalized factor is calculated by the Eq. (14).

$$E_{ij} = \frac{x_{ij}}{\sqrt{\sum_{i=1}^{m} x_{ij}^2}} \tag{14}$$

Here, i = 1,2, … m; and j = 1,2, . . . n.

***Step 9: Normalized Weighted Matrix*:** Normalized the Weighted Decision Matrix by the Eq. (15).

$$s_{ij} = w_i E_{ij} \tag{15}$$

Where, i = 1,2, … m and j = 1,2, … n.

Step 10: Positive and Negative Ideal Solutions: Positive (R^+) and Negative (R^-) ideal solutions are determined by Eqs. (16)–(18).

$$R^+ = s_1^+, s_2^+, s_3^+ \ldots..s_n^+, \quad R^- = s_1^-, s_2^-, s_3^- \ldots..s_n^- \tag{16}$$

Where,s_j^+ = Max s_{ij},s_{j-} = Min s_{ij}

Step 11: Gap: The gap between each alternative is calculated by the assessment of positive and negative distance calculation:

Gap from Positive arrangement:

$$d_i^+ = \sqrt{\sum_{j=1}^{m} \left(s_i^+ - s_{ij}\right)^2}\,; i = 1, 2, 3 \ldots.m \tag{17}$$

Gap from Negative arrangement:

$$d_i^- = \sqrt{\sum_{j=1}^{m} \left(s_{ij} - s_i^-\right)^2}\,; i = 1, 2, 3 \ldots.m \tag{18}$$

d_j^+ = Nearest from the positive arrangement, and for i option, d_i^- = Distance from the negative arrangement.

Step 12: Alternative Preference: The weightage value for all the alternatives (p_i) is obtained by Eq. (19).

$$p_i = \frac{d_i^-}{d_i^- - d_i^+} \quad i = 1, 2, 3 \ldots.m \tag{19}$$

The steps discussed above are to be followed for obtaining the healthcare device's security with the support of Fuzzy ANP TOPSIS approach.

4.2 Quantitative Assessment

Assessing the best security techniques for healthcare devices is a critical task and requires meticulous investment of resources, time and efforts. However, in catering to the high demand for low cost IMDs, focus on the security and preserving the patients' personal information is undermined while designing the healthcare devices. Even a little flaw in the design or the software flaw of the healthcare device can be easily exploited by the attackers, thus jeopardising the patients' life. The FDA regularly modifies the guidelines for vendors and manufactures so as to monitor the security of the healthcare devices both before and after the launch of the device [27–29]. There is a compelling need to formulate a standardised and highly conclusive technique for assessing the security of the healthcare devices accurately. In this context, the authors designed a framework for assessing the best security techniques for the healthcare device by using the Fuzzy ANP.TOPSIS technique, as shown in Fig. 3.

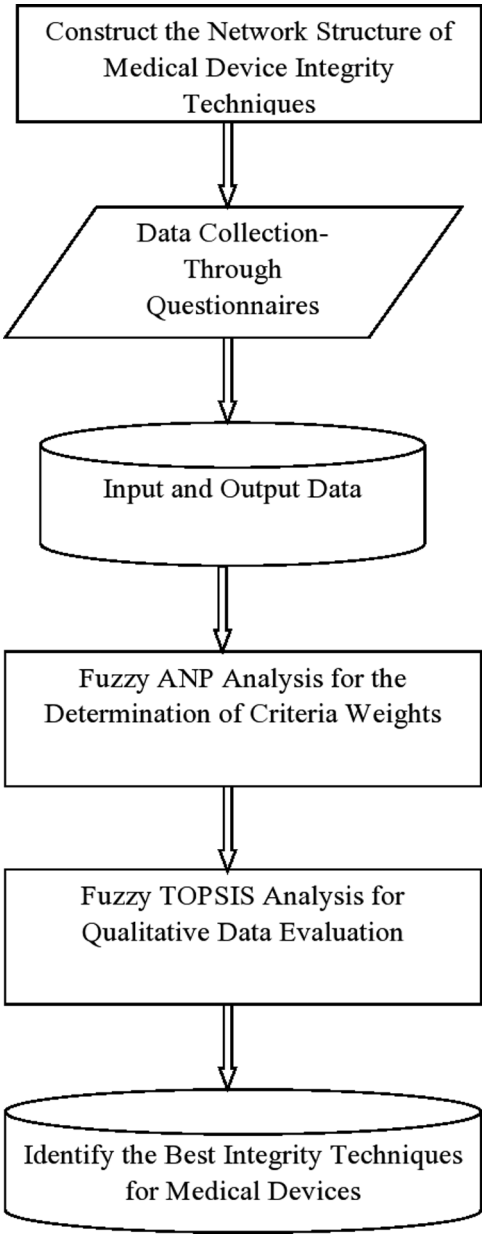

Figure 3: Fuzzy-ANP.TOPSIS analysis flowchart

According to Fig. 3, the initial step is to construct the network for the issue with the help of questionnaires. Thereafter, we collected the data given by the experts. Then, from the collected data, we extracted the relevant data (inputs). Fuzzy-ANP approach is applied onto the inputs for obtaining the weights of the criteria. The weights calculated by the fuzzy ANP work as an input for TOPSIS to quantitatively determine the qualitative data.

After that, we assigned the ratings to the security techniques and identified the best security technique for healthcare devices based on the satisfaction degree. For the assessment of selection for security technique of the healthcare device, the authors designed the problem in network form as goal, criteria and alternatives. All of these have been discussed in the above section and shown in Fig. 1. By using the Eqs. (1)–(19), we

assessed and selected the best security technique for use in the healthcare devices' security by using the Fuzzy ANP.TOPSIS technique. With the Eqs. (1)–(10) and Tab. 1, we constructed the pair-wise comparison-matrix, as displayed in Tab. 2, and with the Eqs. (11)–(13), defuzzified values were obtained. Global weights of the healthcare devices are shown in Tabs. 3 and 4, respectively. Further, Tab. 4 and Fig. 4 shows the ranks of the security techniques. As per the findings, we observed (Tab. 4) that *ML techniques* obtained the highest global weights amongst all the security techniques.

Table 2: Pair-wise comparison matrix

	F1	F2	F3	F4	F5	F6	F7
F1	1.000000, 1.000000, 1.000000	0.561100, 0.661200, 0.751300	1.741400, 2.341300, 2.914400	0.617400, 0.935740, 1.064570	0.494750, 0.654570, 0.844720	1.045250, 1.004700, 1.007470	0.445000, 0.514500, 0.664500
F2	0.501400, 0.654500, 0.942540	1.000000, 1.000000, 1.000000	1.184500, 1.475600, 1.875270	0.795980, 0.968560, 1.148580	1.461450, 1.864500, 2.224500	1.337880, 1.527850, 1.807870	1.554500, 2.204500, 2.850450
F3	1.161400, 1.671200, 1.961300	0.530450, 0.684500, 0.854700	1.000000, 1.000000, 1.000000	1.098580, 1.348590, 1.878980	1.615470, 2.347580, 3.154780	0.347780, 0.437750, 0.578570	1.404700, 1.824780, 2.457590
F4	0.341700, 0.431500, 0.586500	0.884570, 1.044570, 1.264700	0.534700, 0.744500, 0.534560	1.000000, 1.000000, 1.000000	1.545780, 1.935890, 2.355890	0.958590, 1.088650, 1.645890	1.254570, 1.644570, 2.034580
F5	0.322500, 0.412500, 0.592300	0.454560, 0.544500, 0.694500	1.145800, 1.564590, 1.815890	0.420890, 0.520790, 0.670770	1.000000, 1.000000, 1.000000	1.198600, 1.548800, 2.035890	1.145810, 1.494470, 1.905480
F6	0.382200, 0.482300, 0.632400	0.567500, 0.664700, 0.754700	1.740100, 2.340200, 2.990300	0.610780, 0.930750, 1.060750	0.494590, 0.655890, 0.845680	1.000000, 1.000000, 1.000000	0.404570, 0.514570, 0.664410
F7	1.102400, 1.564700, 1.814570	0.357450, 0.454570, 0.647580	0.410400, 0.550700, 0.710470	0.490470, 0.610450, 0.800450	0.535890, 0.675890, 0.845860	1.515680, 1.965890, 2.515680	1.000000, 1.000000, 1.000000

Table 3: Defuzzified matrix

	F1	F2	F3	F4	F5	F6	F7	Weights
F1	1.000000	1.771450	0.891450	2.564780	2.664580	2.344740	0.936520	0.288000
F2	0.562450	1.000000	1.725410	1.211450	1.854520	1.794750	2.411450	0.189000
F3	1.124570	0.571000	1.000000	0.984570	2.604540	0.694570	2.121240	0.165000
F4	0.394540	0.824570	1.014750	1.000000	2.177440	0.777450	1.894250	0.133000
F5	0.374570	0.547410	0.385850	0.455890	1.000000	1.824570	1.767450	0.257400
F6	0.427410	0.554570	1.447450	1.297650	0.544570	1.000000	1.436450	0.118900
F7	1.071560	0.412450	0.473570	0.526520	0.566520	0.694580	1.000000	0.090460
								CR = 0.072000

Table 4: Global weights

Attributes	Global weights	Percentage	Global priorities
Authentication Mechanism (F1)	0.1891240	18.9124 %	2
Machine Learning (F2)	0.2074570	20.7457 %	1
Bio-Cryptography Key Generation (F3)	0.1851450	18.5145 %	3
BLE Security (F4)	0.1654710	16.5471 %	4
Data Flow Integrity (F5)	0.1124550	11.2455 %	5
Attestation Based Architecture (F6)	0.0724560	7.2456 %	6
Isolation Based (F7)	0.0678920	6.7892 %	7

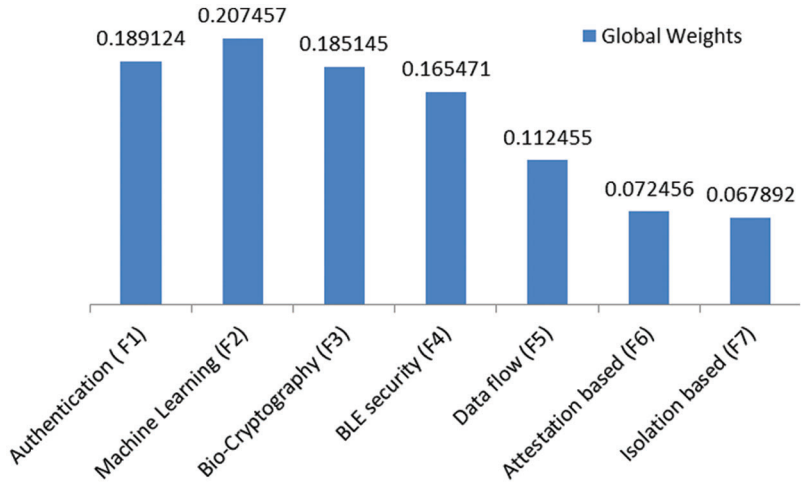

Figure 4: Global weights of each security techniques

After that, by using the global matrix, the super-matrix was designed in the step 6. In step 7, we executed the TOPSIS technique with the help of Eqs. (14)–(19). We have selected various healthcare devices as alternatives to conduct the security assessment of the devices. We have taken ten alternatives in this study including A1, A2, A3, A4, A5, A6, A7, A8, A9 and A10. Additionally, we have converted the qualitative values into the quantitative values, and calculated decision matrix, weighted decision matrix, and closeness coefficients of the alternatives as depicted in the Tabs. 5 to 8, respectively. Closeness coefficient and satisfaction degree analysis of the security techniques of various healthcare devices is shown in Tab. 8. Distance from the positive and negative ideal solution of the security techniques of healthcare devices has been displayed in Tab. 8. Based on the satisfaction degree values, we have assigned the ranks to the alternatives as shown in Fig. 5.

Based on Fig. 5, *alternative (A2)* gained the highest degree of satisfaction and obtained the 1st rank. Our framework provides flexibility to the decision-makers in the selection of most likely alternatives among multiple availabilities. Final ranks gained by the alternatives are in the order of: *A2>A1>A9>A6>A8>A4>A5>A7>A10>A3*. According to the obtained ranks of the alternatives, A1 was the *most likely* alternative amongst all the available ones. This means that the security techniques used in healthcare devices of *A1 are* most secure.

Table 5: Subjective cognition matrix

Attributes/ Alternatives	A1	A2	A3	A4	A5	A6	A7	A8	A9	A10
F1	4.45000, 6.45000, 8.00000	1.18000, 3.00000, 5.00000	3.00000, 4.82000, 6.55000	1.18000, 3.00000, 5.00000	0.64000, 2.27000, 4.27000	1.18000, 3.00000, 5.00000	4.45000, 6.45000, 8.00000	1.18000, 3.00000, 5.00000	3.00000, 4.82000, 6.55000	1.18000, 3.00000, 5.00000
F2	3.00000, 4.82000, 6.55000	0.73000, 2.45000, 4.45000	3.00000, 4.82000, 6.55000	0.73000, 2.45000, 4.45000	0.36000, 1.73000, 3.73000	0.73000, 2.45000, 4.45000	3.00000, 4.82000, 6.55000	0.73000, 2.45000, 4.45000	3.00000, 4.82000, 6.55000	0.73000, 2.45000, 4.45000
F3	3.00000, 4.82000, 6.55000	0.64000, 2.27000, 4.27000	3.55000, 5.36000, 7.00000	0.64000, 2.27000, 4.27000	1.18000, 3.00000, 5.00000	0.64000, 2.27000, 4.27000	3.00000, 4.82000, 6.55000	0.64000, 2.27000, 4.27000	3.55000, 5.36000, 7.00000	0.64000, 2.27000, 4.27000
F4	3.55000, 5.36000, 7.00000	0.36000, 1.73000, 3.73000	4.45000, 6.45000, 8.00000	0.36000, 1.73000, 3.73000	1.18000, 3.00000, 5.00000	0.36000, 1.73000, 3.73000	3.55000, 5.36000, 7.00000	0.36000, 1.73000, 3.73000	4.45000, 6.45000, 8.00000	0.36000, 1.73000, 3.73000
F5	3.00000, 4.82000, 6.55000	0.64000, 2.27000, 4.27000	3.55000, 5.36000, 7.00000	0.64000, 2.27000, 4.27000	1.18000, 3.00000, 5.00000	0.64000, 2.27000, 4.27000	3.00000, 4.82000, 6.55000	0.64000, 2.27000, 4.27000	3.55000, 5.36000, 7.00000	0.64000, 2.27000, 4.27000
F6	3.55000, 5.36000, 7.00000	0.36000, 1.73000, 3.73000	4.45000, 6.45000, 8.00000	0.36000, 1.73000, 3.73000	1.18000, 3.00000, 5.00000	0.36000, 1.73000, 3.73000	3.55000, 5.36000, 7.00000	0.36000, 1.73000, 3.73000	4.45000, 6.45000, 8.00000	0.36000, 1.73000, 3.73000
F7	4.45000, 6.45000, 8.00000	1.18000, 3.00000, 5.00000	3.00000, 4.82000, 6.55000	1.18000, 3.00000, 5.00000	0.64000, 2.27000, 4.27000	1.18000, 3.00000, 5.00000	4.45000, 6.45000, 8.00000	1.18000, 3.00000, 5.00000	3.00000, 4.82000, 6.55000	1.18000, 3.00000, 5.00000

Table 6: The normalized matrix

	A1	A2	A3	A4	A5	A6	A7	A8	A9	A10
F1	0.06000, 0.31000, 0.67000	0.44000, 0.67000, 0.87000	0.12000, 0.39000, 0.74000	0.12000, 0.39000, 0.74000	0.13000, 0.44000, 0.80000	0.06000, 0.31000, 0.67000	0.44000, 0.67000, 0.87000	0.12000, 0.39000, 0.74000	0.12000, 0.39000, 0.74000	0.06000, 0.31000, 0.67000
F2	0.37000, 0.60000, 0.81000	0.17000, 0.46000, 0.80000	0.11000, 0.40000, 0.76000	0.37000, 0.60000, 0.81000	0.11000, 0.40000, 0.76000	0.37000, 0.60000, 0.81000	0.17000, 0.46000, 0.80000	0.11000, 0.40000, 0.76000	0.37000, 0.60000, 0.81000	0.17000, 0.46000, 0.80000
F3	0.44000, 0.67000, 0.87000	0.12000, 0.39000, 0.74000	0.06000, 0.31000, 0.67000	0.44000, 0.67000, 0.87000	0.06000, 0.31000, 0.67000	0.44000, 0.67000, 0.87000	0.12000, 0.39000, 0.74000	0.06000, 0.31000, 0.67000	0.44000, 0.67000, 0.87000	0.12000, 0.39000, 0.74000
F4	0.11000, 0.40000, 0.76000	0.37000, 0.60000, 0.81000	0.17000, 0.46000, 0.80000	0.17000, 0.46000, 0.80000	0.21000, 0.54000, 0.90000	0.11000, 0.40000, 0.76000	0.37000, 0.60000, 0.81000	0.17000, 0.46000, 0.80000	0.17000, 0.46000, 0.80000	0.11000, 0.40000, 0.76000
F5	0.06000, 0.31000, 0.67000	0.44000, 0.67000, 0.87000	0.12000, 0.39000, 0.74000	0.12000, 0.39000, 0.74000	0.13000, 0.44000, 0.80000	0.06000, 0.31000, 0.67000	0.44000, 0.67000, 0.87000	0.12000, 0.39000, 0.74000	0.12000, 0.39000, 0.74000	0.06000, 0.31000, 0.67000
F6	0.37000, 0.60000, 0.81000	0.17000, 0.46000, 0.80000	0.11000, 0.40000, 0.76000	0.37000, 0.60000, 0.81000	0.11000, 0.40000, 0.76000	0.37000, 0.60000, 0.81000	0.17000, 0.46000, 0.80000	0.11000, 0.40000, 0.76000	0.37000, 0.60000, 0.81000	0.17000, 0.46000, 0.80000
F7	0.44000, 0.67000, 0.87000	0.12000, 0.39000, 0.74000	0.06000, 0.31000, 0.67000	0.44000, 0.67000, 0.87000	0.06000, 0.31000, 0.67000	0.44000, 0.67000, 0.87000	0.12000, 0.39000, 0.74000	0.06000, 0.31000, 0.67000	0.44000, 0.67000, 0.87000	0.12000, 0.39000, 0.74000

Table 7: The weighted normalized matrix

	A1	A2	A3	A4	A5	A6	A7	A8	A9	A10
F1	0.04400, 0.07100, 0.09600	0.04400, 0.07500, 0.10600	0.03800, 0.06500, 0.09000	0.03800, 0.06500, 0.09000	0.04400, 0.07100, 0.09600	0.04400, 0.07500, 0.10600	0.03800, 0.06500, 0.09000	0.01300, 0.04500, 0.08200	0.03800, 0.06200, 0.08300	0.03800, 0.06500, 0.09000
F2	0.04400, 0.06600, 0.08400	0.01100, 0.03500, 0.06700	0.04400, 0.07500, 0.10600	0.04400, 0.07500, 0.10600	0.04400, 0.06600, 0.08400	0.01100, 0.03500, 0.06700	0.04400, 0.07500, 0.10600	0.01300, 0.04700, 0.09000	0.04400, 0.07100, 0.09600	0.04400, 0.07500, 0.10600
F3	0.01300, 0.04500, 0.08200	0.03800, 0.06200, 0.08300	0.01100, 0.03500, 0.06700	0.02400, 0.04600, 0.07000	0.01300, 0.04500, 0.08200	0.03800, 0.06200, 0.08300	0.01100, 0.03500, 0.06700	0.00500, 0.02800, 0.06100	0.04000, 0.06100, 0.07900	0.02400, 0.04600, 0.07000
F4	0.01300, 0.04700, 0.09000	0.04400, 0.07100, 0.09600	0.04400, 0.07500, 0.10600	0.01300, 0.04700, 0.09000	0.01300, 0.04700, 0.09000	0.04400, 0.07100, 0.09600	0.04400, 0.07500, 0.10600	0.04400, 0.07100, 0.09600	0.04400, 0.07500, 0.10600	0.01300, 0.04700, 0.09000
F5	0.02400, 0.04600, 0.07000	0.04400, 0.06600, 0.08400	0.02400, 0.04600, 0.07000	0.00500, 0.02800, 0.06100	0.02400, 0.04600, 0.07000	0.04400, 0.06600, 0.08400	0.02400, 0.04600, 0.07000	0.04400, 0.06600, 0.08400	0.01100, 0.03500, 0.06700	0.00500, 0.02800, 0.06100
F6	0.01300, 0.04700, 0.09000	0.04400, 0.07100, 0.09600	0.02000, 0.05500, 0.09500	0.04400, 0.07500, 0.10600	0.01300, 0.04700, 0.09000	0.04400, 0.07100, 0.09600	0.02000, 0.05500, 0.09500	0.01300, 0.04700, 0.09000	0.04400, 0.07100, 0.09600	0.04400, 0.07500, 0.10600
F7	0.00500, 0.02800, 0.06100	0.04000, 0.06100, 0.07900	0.05100, 0.07000, 0.08300	0.01100, 0.03500, 0.06700	0.00500, 0.02800, 0.06100	0.04000, 0.06100, 0.07900	0.05100, 0.07000, 0.08300	0.02400, 0.04600, 0.07000	0.04400, 0.06600, 0.08400	0.01100, 0.03500, 0.06700

Table 8: Closeness coefficients of alternatives

Alternatives		d+i	d-i	Satisfaction degree p_i	Ranks
Alternatives1	A1	0.161420	0.075520	0.312150	2
Alternatives2	A2	0.241240	0.118950	0.324250	1
Alternatives3	A3	0.234580	0.075450	0.212450	10
Alternatives4	A4	0.454570	0.166580	0.278590	6
Alternatives5	A5	0.477580	0.175690	0.278540	7
Alternatives6	A6	0.175960	0.067850	0.284570	4
Alternatives7	A7	0.345780	0.095780	0.256580	8
Alternatives8	A8	0.254870	0.112450	0.284570	5
Alternatives9	A9	0.256540	0.132540	0.302540	3
Alternatives10	A10	0.365480	0.124570	0.235870	9

4.3 Sensitivity Analysis

We conducted the sensitivity analysis to validate the obtained results. We have validated our results by changing the variables. In this article we performed 10 experiments because we have selected 10 alternatives, as shown in Fig. 1. We have changed the variables with respect to the results obtained, and observed that the A2 remains constant and also gets the highest rank. Tab. 9 depicts the sensitivity analysis obtained through

the experiments. Fig. 6 depicts the comparison of the experiments' results, displayed in Tab. 9, with the original weights. In 10 experiments we have observed that Exp. 2 (A2) obtained the highest experimental values with respect to the original weight. The alternatives are sensitive to the weights as is evident from the results in Fig. 6.

Table 9: Sensitivity analysis

Experiments		Obtained weights	F1	F2	F3	F4	F5	F6	F7
Exp-1	A1	0.346000	0.248100	0.282000	0.292300	0.248100	0.282000	0.292300	0.292300
Exp-2	A2	0.359400	0.307000	0.312300	0.313400	0.307000	0.312300	0.313400	0.313400
Exp-3	A3	0.243000	0.332000	0.315300	0.308000	0.332000	0.315300	0.308000	0.308000
Exp-4	A4	0.301400	0.202400	0.213600	0.218200	0.202400	0.213600	0.218200	0.218200
Exp-5	A5	0.346000	0.312300	0.313400	0.307000	0.312300	0.313400	0.307000	0.314500
Exp-6	A6	0.359400	0.315300	0.308000	0.332000	0.315300	0.308000	0.332000	0.316100
Exp-7	A7	0.243000	0.213600	0.218200	0.202400	0.213600	0.218200	0.202400	0.214600
Exp-8	A8	0.284570	0.332000	0.315300	0.308000	0.332000	0.315300	0.308000	0.308000
Exp-9	A9	0.302540	0.202400	0.213600	0.218200	0.202400	0.213600	0.218200	0.218200
Exp-10	A10	0.235870	0.312300	0.313400	0.307000	0.312300	0.313400	0.307000	0.314500

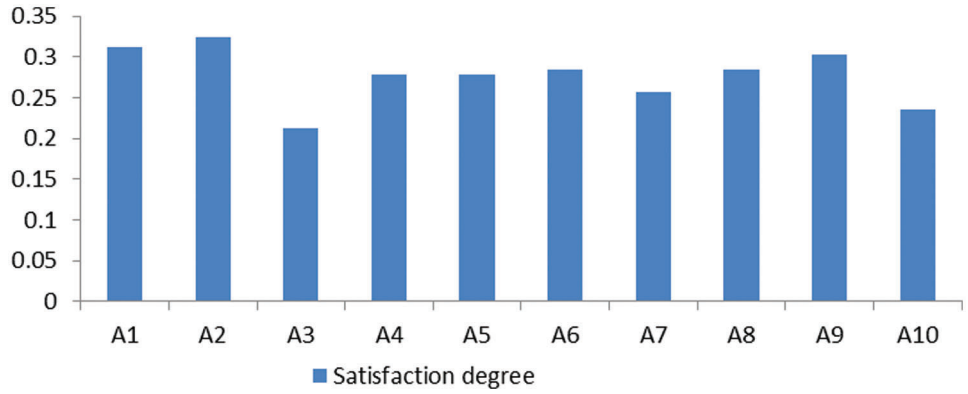

Figure 5: Alternatives obtained satisfaction degree

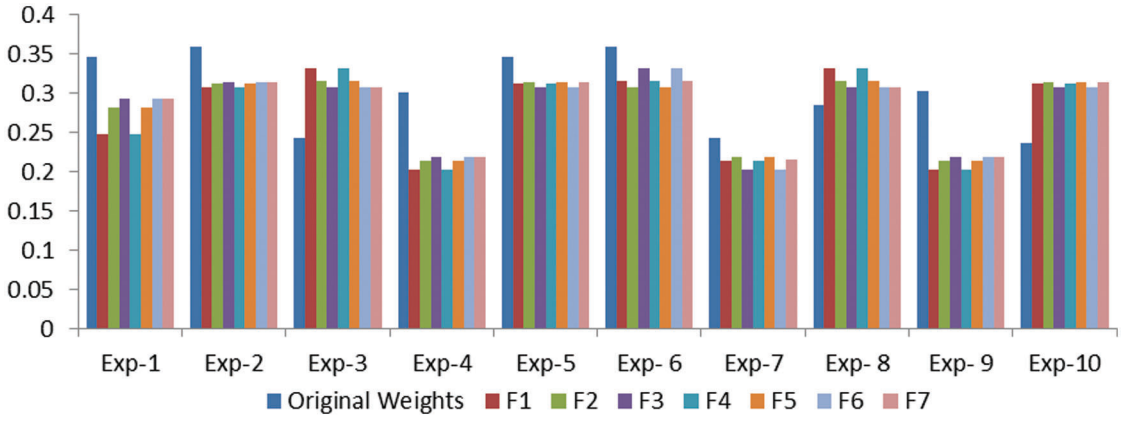

Figure 6: Comparison of the experiment's results with the original weights

5 Discussion

The security of healthcare devices is checked at the time of data transfer, data storage and process migration in the execution of the data. All these issues can be handled in the healthcare devices by updating the patch of the software and by using the hardware security guards and network security techniques.

Healthcare devices process sensitive information of the patients' health and also carry the personal details. In the present study, we designed a Multi-criteria decision making framework which does a quantitative analysis of the security techniques for healthcare devices. In this framework, we used the Fuzzy ANP.TOPSIS integrated technique which is the best methodology for decision making and ratings technique. With the help of these techniques, the decision-makers assigned the ratings of the healthcare devices security techniques. In this study we have taken help of 10 experts from different security fields. Their opinions were taken in the process of selecting the best security techniques for healthcare devices based on their experiences. Finally, we imposed the F.ANP.TOPSIS on the given data for assessing the performance of the security techniques. As per the findings of our analysis, ML based healthcare devices obtained the highest priority among the security techniques and A2 alternative also obtained the highest rank. Based on our framework's evaluation, we concluded that researchers and vendors should focus on the ML techniques for securing the healthcare devices.

Recommendations as:

- Most of the researchers work on the security of the medical devices but do not provide proper guidelines for the development and design of the device's software and security.
- Our framework is systematic and provides effective guidelines for the developers to design the software by adhering to the security rules.
- Security assessment of the medical devices will not only secure the medical devices' functioning and patients' personal information but also strengthen the technical features of the device.
- The proposed framework can be used by the manufactures and government agencies for checking the medical devices security in a quantitative and accurate way.
- The proposed model can also help in the selection of the best security techniques.

6 Conclusion

The dependability on the healthcare devices has increased tremendously in the present scenario, more so in the wake of health emergencies like COVID-19 pandemic when the patients have been suggested home quarantine instead of visiting hospitals. Healthcare devices process the patients' data and send it to the doctors and store the data. But making healthcare devices secure and also protecting the data from attacks is a big issue. Even a minute alteration in the patient's data can change the whole result of the diagnosis. An effective solution in this league is to find a quantitative and systematic mechanism for the selection of the most conversant security techniques for the healthcare devices. All these features were obtained in the present study with the aid of Fuzzy ANP.TOPSIS technique. In this study, we have evaluated and rated that ML based healthcare device obtained the highest priority among the other security techniques that are being used at present for securing healthcare devices. Our framework can be used by the manufacturers and vendors to verify the healthcare device security. This is a fully automatic technique in decision making among the various alternatives and gives corroborative results. Our framework is well validated and a tested approach that can be used for the selection of the most efficacious security techniques.

Acknowledgement: The authors acknowledges the Deanship of Scientific Research at King Faisal University for the financial support under Nasher Track (Grant no. 206063).

Funding Statement: Funding for this study was granted by the Deanship of Scientific Research at King Faisal University, Kingdom of Saudi Arabia under grant no. 206063.

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. IEEE Sym. 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. 2011IEEE 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 Alemzadeh, "On threat modeling and mitigation of medical cyber-physical systems," in *Proc. IEEE/ACM Int. Conf. on Connected Health: Applications*, System, Philadelphia, PA, USA, pp. 114–119, 2017.

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

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

[6] Medical Devices: FDA Should Expand Its Consideration of Information Security for Certain Types of Devices "GAO: U. S. Government Accountability Office," 2012. [Online]. Available: https://www.gao.gov/products/GAO-12-816.

[7] FDA's Role in Regulating Medical Devices "U. S. Food & Drug Administration," 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. 2019 IEEE/ACM Int. Conf. on Connected Health: Applications, Systems and Engineering Technologies*, Arlington, VA, USA, pp. 23–24, 2019.

[9] Hospital Networks Are Leaking Data, Leaving Critical Devices Vulnerable "Wired Magazine," 2014. [Online]. Available: https://www.wired.com/2014/06/hospital-networks-leaking-data/.

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

[11] T. Yaqoob, H. Abbasand 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] C. Bresch, S. Chollet and D. Hely, "Towards an inherently secure run-time environment for medical devices," in *Proc. IEEE International Congress on Internet of Things*, San Francisco, USA, pp. 140–147, 2018. [Online]. Available: https://hal.archives-ouvertes.fr/hal-01898660.

[13] 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. 2020 IEEE Conf. on Communications and Network Security*, Avignon, France, pp. 1–9, 2020.

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

[15] L. Zhou and Y. Makris, "HAFIX: hardware-assisted flow integrity extension," in *Proc. 52nd Annual Design Automation Conf.*, San Francisco, CA, USA, pp. 1550–1555, 2015. [Online]. Available: https://dl.acm.org/doi/10.5555/3130379.3130740.

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

[17] A. Ray and C. Rance, "An analysis method for medical device security," in *Proc. Sym. and Bootcamp on the Science of Security*, New York, NY, USA, Article 16, pp. 1–2, 2014.

[18] V. Costan, I. Lebedev and S. Devadas, "Sanctum: Minimal hardware extensions for strong software isolation," in *Proc. 25th USENIX Security Symposium, USENIX Security 16*, Austin, TX, USA, pp. 857–874, 2016. [Online]. Available: https://www.usenix.org/conference/usenixsecurity16/technical-sessions/presentation/costan.

[19] 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. 337, 2015.

[20] 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.

[21] 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. 8, pp. 32–44, 2016.

[22] 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.

[23] 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.

[24] K. Shahroudi and H. Rouydel, "Using a multi criteria 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] Content of Premarket Submissions for Management of Cybersecurity in Medical Devices- Draft Guidance for Industry and Food and Drug Administration Staff "U. S. Food & Drug Administration," 2018. [Online]. Available: https://www.fda.gov/regulatory-information/search-fda-guidance-documents/content-premarket-submissions-management-cybersecurity-medical-devices.

[26] 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. 11, pp. 1770–1792, 2020.

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

[28] 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.

[29] R. Kumar, S. A. Khan and R. A. Khan, "Durability challenges in software engineering," *Crosstalk*, vol. 29, no. 5, pp. 29–31, 2016.

Appendix A

Symbols	Meaning
μ_a	Membership Function
A	Fuzzy Set
Tn	Triangular Number
X	Universe Of Discourse
l, m, h	Lower, Medium, High
TFN(ηij)	Triangular Fuzzy Number
CI	Consistency Index
N	Number Of Compared Elements
RI	Random Index
CR	Consistency Ratio
α and β	Preferences Of Experts (Values Vary Between 0 And 1)
E_{ij}	Topsis Function
s_{ij}	Normalized Weighted Matrix
(R^+), (R^-)	Positive And Negative Ideal Solution
s_j^+ and s_j^-	s_j^+ Is Max Of S_{Ij} If J Is A Advantage Factor, s_j^- Is Min Of S_{Ij} If J Is A Advantage Factor
d_i^+, d_i^-	Distance To The Positive And Negative Ideal Solution
(p_i)	Satisfaction Degree