Computers, Materials & Continua
DOI:10.32604/cmc.2021.014869
Article

Tech Science Press

Integrity Assessment of Medical Devices for Improving Hospital Services

Fahad A. Alzahrani[1], **Masood Ahmad**[2], **Mohd Nadeem**[2], **Rajeev Kumar**[2,3,*] **and Raees Ahmad Khan**[2]

[1]Department of Computer Engineering, Umm Al-Qura University, Mecca, 24381, Saudi Arabia
[2]Department of Information Technology, Babasaheb Bhimrao Ambedkar University, Lucknow, 226025, Uttar Pradesh, India
[3]Department of Computer Application, Shri Ramswaroop Memorial University, Barabanki, 225003, Uttar Pradesh, India
[*]Corresponding Author: Rajeev Kumar. Email: rs0414@gmail.com

Received: 23 October 2020; Accepted: 19 December 2020

Abstract: The present study examines the various techniques being used to maintain the integrity of the medical devices, and develops a quantitative framework to list these in the sequence of priority. To achieve the intended objective, the study employs the combined procedure of Fuzzy Analytic Network Process (ANP) and Fuzzy Technical for Order Preference by Similarities to Ideal Solution (TOPSIS). We selected fuzzy based decision making techniques for assessing the integrity of medical devices. The suggested methodology was then used for classifying the suitable techniques used to evaluate the integrity of medical devices. Different techniques or the procedures of integrity assessment were ranked according to their satisfaction weights. The rating of the options determined the order of priority for the procedures. As per the findings of the study, among all the options, A1 was assessed to be the most likely option. This means that the integrity of medical devices of A2 is the highest amongst all the chosen alternatives. This analysis will be a corroborative guideline for manufacturers and developers to quantitatively test the integrity of medical devices in order to engineer efficacious devices. The evaluations undertaken with the assistance of the planned procedure are accurate and conclusive. Hence instead of conducting a manual valuation, this experimental study is a better and reliable option for assessing the integrity of the medical devices.

Keywords: Integrity of the medical devices; fuzzy-ANP.TOPSIS; security assessment

1 Introduction

Medical devices are the virtual lifelines of the present day healthcare services and are utilized used extensively in the prevention, detection or the diagnosis of the diseases. However due to software and design related vulnerabilities, these devices have also become an easy prey of cyber intrusions. Ironically, the devices intended to safeguard the patients' health are now becoming a major health hazard because of cyber threats. The alarming instance of intruders gaining easy access to insulin pump is just one among several such violations [1]. In fact, the last few years have registered an exponential rise in the instances of attacks on the entire healthcare sector. Security experts opine that the reason for this spike could be the growing market for the healthcare data on the dark web. Various attacks are engineered on the medical devices, threatening not only the efficacy of the device but also corrupting the information saved in the device. For instance, custom attacks by the *Conficker worm* can easily target any running window system, and target nearly 100 MRI machines at a given time.

To address the rising episodes of breaches, the FDA drafted a report that analyzed the security of the medical devices in 2012 [2]. In 2013, FDA released a set of guidelines in the security of the medical devices for the vendors [3]. Researchers, developers and manufacturers need to work on more foolproof procedures to resolve the threats of medical devices [4].

Besides the protection of medical devices, the integrity of devices is another aspect that needs to be improved [5]. The safety element of the device varies from the integrity of the medical device's design. Healthcare network and medical devices network attacks threaten both the integrity of the device and data security [6]. Studies performed in the context of network breach of medical device have found many vulnerabilities and health hazards. Some of these are: *Implantable Medical devices (IMDs)* [7], *wearable devices* [8] *and surgical robots* [9], *network vulnerabilities present in the hospital's network* [10], *and third party networks service* (example, pharmacies, hospitals, etc.) [11–14].

All these events allow the attackers to enter the network and manipulate it. The attackers exploit the vulnerabilities in the network to get access to the medical devices and extract the users' names and passwords [15–20]. It is essential to reduce the vulnerabilities that are sometimes introduced into the devices due to design deficiencies so as to maximize the effectiveness of the medical devices. In order to make medical device more safe and effective, the credibility of the medical device is thus an essential research principle and assumes greater importance.

The present study assesses the multiple integrity management systems and procedures that are currently being used to determine the integrity of the medical devices. To conduct a thorough empirical analysis, the analysis builds on the views of the professionals on the integrity of the medical devices as inputs for the implementation of the planned procedure. The objectives of the present study are: Enlisting the similar procedures; integrity management systems; and applying the proposed procedure to test the integrity of medical devices.

2 Related Approaches

Several research studies address the privacy and qualities of the medical devices. However, there are very few researches that carry on the integrity of the medical device which is the core objective of our study. The related studies are discussed here with particular reference to integrity:

Li et al. designed the architecture that can be used for managing the integrity. *Code pointer overwrites exploitation* is the most important run-time attack [2]. Prevention from runtime attacks is important for strengthening the integrity of the devices. Code pointer exploits memory vulnerability as buffer overflows. LO-FAT architecture calculates the hash value of the device which takes Lo-FAT works base on prover and verifier. Here, the prover works as a low-end device overseeing software, and verifier is a far computer which manages the software execution of the device. Each time when the challenge is sent to the prover, the execution flow varies and cumulative hash values are evaluated. Verifier uses this hash value for validating the execution flow of the programme taken for the execution. However, this method doesn't secure the patient's information and hackers can also take control of the program.

Almohri et al. [3] designed the architecture C-FLAT for checking the integrity of the devices. This method prevents the run-time attacks which can be the reason for exploiting the memory vulnerability. C-FAT architecture assesses the hash value of the path taken by the device path in execution. C-FAT works base on prover and verifier. However, this method also doesn't secure the patient's information. Moreover, the hackers can also take control of the program.

Bresch et al. [15] proposed HCFI application. It makes medical devices secure depending on the control flow [15]. The secure code is evaluated in this process based on its security and performance perspective. This approach effectively protects the system from attacks through code-reuse. The procedure authenticates each edge by making the software's flow graph. Each destination node labels are verified at the time of execution flow to the other. If the vertex labels are different, then it is easy to detect the control-flow attacks. However, the approach is vulnerable to data attacks.

Newaz et al. [17] proposed the HAFIX system for assisting hardware integrity flow [17]. This approach uses the backward edges of execution flow graph's to check code reuse attacks, but it is easy to adjust the forward edge. Therefore, this procedure is vulnerable to data attacks. Information about the security of medical devices is given by the procedure discussed above. We analysed various procedures for preserving the protection and integrity of the medical devices in the subsequent chapter. These procedures became the basis for organizing this study's methodological structure.

3 Medical Device Integrity Mechanisms

Medical devices are implanted and connected the with patients' body and capture the sensitive activity from the body. Device collects information and transmits it to the doctors and laboratories through the network. Low power sensor-based devices are most vulnerable to intrusions attached with the network. Most of the manufacturers want to provide low cost embedded devices that consume less power. Hence, additional security mechanisms that will make the device complex and also increase the manufacturing costs are not preferred [18]. For instance, keeping the device secure is often not the first priority of the developers while making low cost on-site devices like Ultrasound, MRI, and X-ray, etc.

Designers usually concentrate on the device's functional requirement and tend to overlook the efficacy of the security features associated with the device. Medical equipment, such as hardware and old version of software, create system centric vulnerabilities that are easy to hack. Reverse engineering procedures can hack the onsite devices easily and compromise their confidentiality and integrity. Both the software and hardware layers are part of security needs in the connected devices. The important features for developing the high secure medical devices are: *Integrity, availability, authentication, confidentiality, safety and privacy, unauthorized tampering*. Due to traditional security algorithms that cannot be utilized because of implantable and sensors devices, maintaining the security of the devices is a demanding task.

However in the recent years, professionals have built new algorithms for CIA prevention that resolve the integrity and security issues associated with the devices. These are not ideal for all types of cyber-attacks. On-site devices (ultrasound, X-ray and MRI) are also prone to cyber-attacks [19]. Various techniques have been developed for maintaining the integrity of the devices. These techniques have been elucidated in Fig. 1.

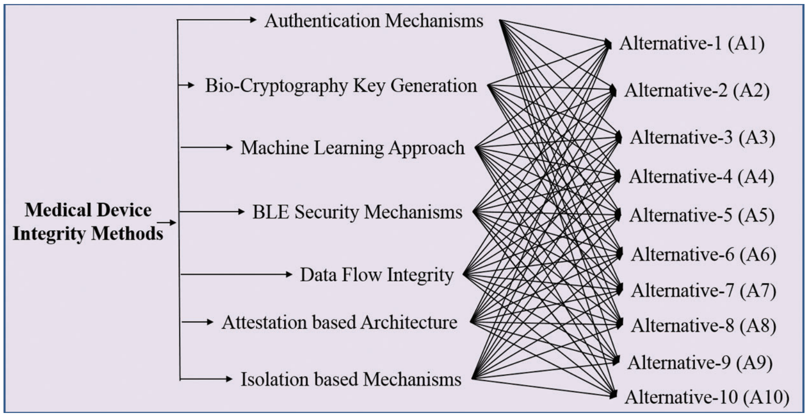

Figure 1: Integrity techniques in medical devices

3.1 Attestation-Based Architecture

This approach is used for preventing the *run-time attacks* on the devices which impact the integrity of the devices. By evaluating hashes and making vertexes to handle the program flow [13], this procedure overcomes the unauthorized access. The procedure also monitors the overflow and verifies whether or not the programme for the device is performing accurately [14]. However, this technique doesn't consider data integrity attacks and is not used fully by the software developers for the medical devices.

3.2 Isolation Based Mechanisms

This technique is used for controlling the flow of the integrity of the devices. This mechanism divides the system in two-zones: the *trusted zone* and *untrusted* zone. *Syscalls* manage the communication between the trusted and the untrusted zone. The resource security level is classified as trusted zone [20] and is used at hardware level. It uses special bits to point out the trust and the untrusted zone. On the other hand, *software syscalls* are used for pointing the trusted zone and the untrusted zone. Functions and resources allocated in the trusted zone cannot be accessed from the untrusted zone.

3.3 Data Flow Integrity

Data flow integrity mechanism is used in maintaining the integrity of the device. For maintaining the integrity of the devices, *developer's code pointer* at the time of development plays an important role. The pointer maintains the integrity of the pointer track [21]. At the compilation time, the pointer is marked at source code. The base and bound values of these pointers are stored outside the hardware range. Pointer validity is checked by the system when the pointer is accessed. If the pointer is reconfigured in an unlawful manner, then the pointer values of base and bound do not match with the memory of the storage values. This approach is used in hardware custom for ensuring the software integrity.

3.4 Bio-Cryptography Key Generation

This technique is used in secure communication and security for the medical device. Researchers used blood pressure, PPG and ECG capture by sensors for generating the key for secure Cryptography [22,23]. The physiological signals and the inter-pulse interval (IPI) and frequency domain are the two procedures used for generating a secret key. Both the procedures are adopted in the generation of cryptography key.

3.5 Authentication Mechanisms

Authentication mechanism prevents the unauthorized access of information. In this mechanism, [24,25] a lightweight mechanism AES 128 is used with current hash message verification code where nonce is utilized for confirming the personality of the customer's clinical gadget and door worker. Here nonce is utilized as an introduction vector (IV) for the encryption by utilizing the AES 128 key. This scheme is effective in preventing the unauthorized access.

3.6 Bluetooth Low Energy (BLE) Security Mechanisms

BLE is made by using any four secure matching methodologies. These methodologies contain low energy (LE) secure association blending, passkey and numeric examination [18]. BLE starts transmission when the peripheral device is turned on. Normal pairing approach performs the task without the interference of users. It is suitable for the wearable because it does not contain the screen and user interface.

3.7 External Mechanism

IMD devices contain the IMD shield, IMDGaurd, and Cloaker for the security issues. The IMD shield contains antenna and full-duplex radio device [3–5]. Receiving antenna breaks the chain of receiving signals by receives signal. For key generation, IMDGaurd uses ECG signals; it ignores the broadcasting of periodic message. Cloaker is an important external mechanism which provides security to the medical device. If Cloaker is activated, then the device denies all the communication requests that arrive on it. On the other side, if the IMD is open, all the requests are accepted. This scheme's reliability totally depends on the Cloaker's presence in the IMD.

4 Methodology and Results

In this study, we have integrated three different approaches of the fuzzy set theory concepts, Analytic Network Process (ANP) and TOPSIS. The integrated approach of Fuzzy-ANP-TOPSIS is a novel and a highly effective methodology to elicit conclusive outcomes. The Fuzzy-ANP-TOPSIS has been discussed below in detail.

4.1 Fuzzy-ANP.TOPSIS

Assessing the integrity of the medical devices is a multiple criteria decision-making process. Analytic network process (ANP) is an essential type of AHP [12]. AHP is used to construct the multi-level hierarchy with goal, criteria and alternatives, and ANP is as a network and cycles connecting structure. ANP is a systematic approach that utilizes the fuzzy set theory concept and network analysis process for the selection of the alternatives. The MCDM approach can easily resolve the multiple and conflicting opinions that arise while selecting the most conversant alternatives. Fuzzy ANP-TOPSIS has been used for assessing the integrity techniques of the medical devices. The attributes selection plays an important role in Fuzzy-ANP.TOPSIS approach [19–21].

We opted for the fuzzy integrated method of ANP & TOPSIS [12] because fuzzy provides the condition where there is no limitation for judgments. In the same league, Fuzzy-ANP.TOPSIS approach provides a quantitative assessment of the varied and huge data obtained from the decision-makers. TFN is used to assess the decision-makers' preferences because of its simplicity in design and implementation. A step-by-step assessment procedure of the weights of the selected factors along with ranks of the factors obtained through Fuzzy-ANP.TOPSIS is discussed below:

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

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

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

Experts ranked the linguistic terms impacting the characteristics quantitatively in alignment with the TFNs depicted in Tab. 1.

Table 1: Linguistic terms and the corresponding TFNs

Saaty_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: By the Eqs. (2)–(5), linguistic values are converted into TFNs, and indicated as (*lij, mij, hij)* where, *lij* = *lower*, *mij* = *middle and hij* = higher values. Further, TFN [ηij] is determined by:

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

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

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

$$\mathrm{mi_{ij} = (J_{ij1}, J_{ij2}, J_{ij3})^{\frac{1}{x}}} \tag{4}$$

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

In the Eqs. (2)–(5), J_{ijk} 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 experts.

By the extension rule, consider two TFNs $M1 = (l_1, mi_1, h_1)$ and $M2 = (l_2, mi_2, h_2)$ 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: Pair-wise Comparison- After receiving the decision elements from the experts, we prepared the pair-wise decision-matrix. The Consistency Index (CI) is evaluated by Eq. (9).

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

Here, $N =$ Number of analyzed components.

We calculated the consistency ratio (CR) by Eq. (10).

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

Step** 5*: ***Defuzzification: After formulating the pair-wise comparison-matrix, Fuzzy values are converted into crisp values by the Eq. (11)–(13).

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

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

Such that,

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

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

For preferences of experts, α and β are utilized in these conditions; *α and β values* lie in the *range of 0 and 1*.

Step** 6*: ***Super-matrix: The entire paths and connections are described in the network and by using the *Markov* based approach, we determined the fuzzy priorities of the criteria.

Step 7: For evaluating the TOPSIS, the performance priority of all the alternative options over every normalized factor is calculated by Eq. (14).

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

Here, $i = 1, 2, \ldots, m$; and $j = 1, 2, \ldots, n$.

***Step 8: Normalized Weighted Matrix*:** In this step, the Normalized Weighted Decision Matrix is evaluated by the given Eq. (15).

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

where, $i = 1, 2, \ldots, m$ and $j = 1, 2, \ldots, n$.

Step 9: Positive and Negative Ideal Solution: Positive (R^+) & Negative ideal solution (R–) are calculated by Eq. (16).

$$R^+ = s_1^+, s_2^+, s_3^+, \ldots, s_n^+$$

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

where, $s_j^{+} = \text{Max} s_{ij}$, if j is a preferred position factor and Max s_{ij} if j is a cost factor; $s_j^{-} = \text{Min} s_{ij}$, if j is a bit of leeway factor s_{ij} if j is a cost factor.

Step 10: Gap: The gap for each alternative is evaluated by the assistance of positive and negative ideal arrangement (Eqs. (17) and (18)).

Gap from Positive arrangement:

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

Gap from Negative arrangement:

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

$d_j^{+} =$ is the nearest from positive arrangement, and for i option, $d_i^{-} =$ distance from the negative arrangement.

Step 11: Alternative Preference: Calculation of the preference value for every alternative (p_i) is given by Eq. (19).

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

The previously mentioned steps are to be perused to evaluate the integrity of the medical device with the assistance of Fuzzy ANP TOPSIS strategy with various other options.

4.2 Data Analysis

Assessing the integrity of a medical device is a crucial task that demands meticulous care, time and money. The integrity of the confidential details of patients' are, however, compromised during the design of medical devices due to a growing demand for low cost IMDs. Hackers can easily manipulate even a minute mistake in the design or software of the medical device system; thereby threatening the patients' privacy and health. Though the FDA periodically updates the rules and regulations for securing the medical devices, there is a legitimate want to devise a systematic and highly reliable approach for determining the integrity of medical devices [25].

First step is to construct the network structure of the problem, data collection by the experts is done through the questionnaires; thereafter, the data is filtered to collate the relevant inputs. Fuzzy-ANP approach is applied on the inputs to determine the weights of the criteria. The weights are used as inputs for TOPSIS for quantitative analysis of the qualitative data. The last step is to identify the best integrity techniques for medical devices based on the satisfaction degree.

With the help of Eq. (1)–(19), we assessed the integrity of the medical devices by employing the Fuzzy.ANP.TOPSIS approach. From Eq. (1)–(10) and Tab. 1, we prepared the pair-wise comparison-matrix as displayed in Tab. 2.

Table 2: Pair-wise comparison matrix

	F1	F2	F3	F4	F5	F6	F7
F1	1.000000, 1.000000, 1.000000	1.615470, 2.347580, 3.154780	0.347780, 0.437750, 0.578570	1.404700, 1.824780, 2.457590	1.184500, 1.475600, 1.875270	0.795980, 0.968560, 1.148580	0.410400, 0.550700, 0.710470
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	1.000000, 1.000000, 1.000000	1.098580, 1.348590, 1.878980	1.615470, 2.347580, 3.154780
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	0.347780, 0.437750, 0.578570	1.404700, 1.824780, 2.457590	1.740100, 2.340200, 2.990300
F4	1.000000, 1.000000, 1.000000	1.615470, 2.347580, 3.154780	0.347780, 0.437750, 0.578570	1.404700, 1.824780, 2.457590	1.184500, 1.475600, 1.875270	0.795980, 0.968560, 1.148580	0.410400, 0.550700, 0.710470
F5	0.501400, 0.654500, 0.942540	1.000000, 1.000000, 1.000000	1.184500, 1.475600, 1.875270	0.795980, 0.968560, 1.148580	0.410400, 0.550700, 0.710470	1.198600, 1.548800, 2.035890	1.145810, 1.494470, 1.905480
F6	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	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

By using the Eq. (11)–(13), we defuzzified the pair-wise examination framework with the assistance of alpha cut and obtained the global weights of the medical devices. The results are displayed in Tabs. 3 and 4. In the defuzzified process, the decisions of the experts were converted into precise values for the ranking of the devices [12–15]. With the help of defuzzified values and the global weights' matrix, the super-matrix was constructed in step 6. Thereafter, we evaluated the TOPSIS approach by using the Eqs. (14)–(19). We have evaluated the subjective cognition matrix of the linguistic terms, normalized decision matrix, weighted normalized matrix & closeness coefficients of alternatives which have been displayed in Tabs. 5 to 7, respectively. We opted for different medical devices as alternatives for integrity assessment. The 10 alternatives for the analysis were denoted as $A1, A2, \ldots, A10$.

Table 3: Defuzzified matrix

	F1	F2	F3	F4	F5	F6	F7	Weights
F1	1.000000	1.771450	2.564780	2.177440	0.777450	1.894250	1.767450	0.265123
F2	0.562450	1.000000	1.725410	0.984570	0.544570	1.000000	1.436450	0.141123
F3	1.124570	0.571000	1.000000	0.984570	2.604540	0.694570	2.121240	0.115123
F4	1.000000	1.771450	0.891450	2.564780	2.177440	0.777450	1.894250	0.101154
F5	0.562450	1.000000	1.725410	1.211450	1.000000	1.824570	1.767450	0.227125
F6	1.124570	0.571000	1.000000	0.984570	0.544570	1.000000	1.436450	0.128911
F7	0.394540	0.824570	1.014750	1.000000	0.566520	0.694580	1.000000	0.021441
CR = 0.072000								

In Tab. 7, positive and negative ideal solution of the integrity of medical devices has been assessed. Furthermore, the alternatives are ranked on the basis of their satisfaction degree values which are obtained through the calculations done by the Fuzzy-ANP.TOPSIS approach. According to Fig. 2, *alternative (A2)* obtained the highest degree. Fuzzy_AHP.TOPSIS gives the flexibility to the decision-makers to choose the most likely alternative from a host of availabilities. Final ranks of the alternatives are in the order of: *A2>A1>A9>A6> A8>A4>A5>A7>A10>A3*. According to obtained ranks of the alternatives, A1 was the *most likely* alternative amongst all the alternatives. This means that the integrity of medical devices of *A2* is the highest.

Table 4: Global weights

Attributes	Global weights	Percentage	Global priorities
F1	0.265123	26.5123%	1
F2	0.141123	14.1123%	3
F3	0.115123	11.5123%	5
F4	0.101154	10.1154%	6
F5	0.227125	22.7125%	2
F6	0.128911	12.8911%	4
F7	0.021441	2.1441%	7

Table 5: Subjective cognition matrix

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

Table 6: 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	0.04400, 0.07100, 0.09600	0.04400, 0.07500, 0.10600	0.03800, 0.06500, 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	0.03800, 0.06500, 0.09000
F2	0.04000, 0.06100, 0.07900	0.02400, 0.04600, 0.07000	0.04400, 0.06600, 0.08400	0.01100, 0.03500, 0.06700	0.04400, 0.07500, 0.10600	0.04000, 0.06100, 0.07900	0.02400, 0.04600, 0.07000	0.04400, 0.06600, 0.08400	0.01100, 0.03500, 0.06700	0.04400, 0.07500, 0.10600
F3	0.04400, 0.07500, 0.10600	0.03800, 0.06500, 0.09000	0.03800, 0.06500, 0.09000	0.04400, 0.07100, 0.09600	0.01300, 0.04500, 0.08200	0.04400, 0.07500, 0.10600	0.03800, 0.06500, 0.09000	0.03800, 0.06500, 0.09000	0.04400, 0.07100, 0.09600	0.01300, 0.04500, 0.08200
F4	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	0.03800, 0.06500, 0.09000	0.04400, 0.07500, 0.10600	0.03800, 0.06500, 0.09000	0.03800, 0.06500, 0.09000	0.04400, 0.07100, 0.09600
F5	0.00500, 0.02800, 0.06100	0.04000, 0.06100, 0.07900	0.02400, 0.04600, 0.07000	0.04400, 0.06600, 0.08400	0.01100, 0.03500, 0.06700	0.04400, 0.07500, 0.10600	0.01100, 0.03500, 0.06700	0.04400, 0.07500, 0.10600	0.04400, 0.07500, 0.10600	0.04400, 0.06600, 0.08400
F6	0.04400, 0.06600, 0.08400	0.01100, 0.03500, 0.06700	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	0.04400, 0.06600, 0.08400	0.02400, 0.04600, 0.07000	0.01300, 0.04500, 0.08200
F7	0.04400, 0.06600, 0.08400	0.01100, 0.03500, 0.06700	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	0.04400, 0.06600, 0.08400	0.04400, 0.06600, 0.08400	0.01100, 0.03500, 0.06700

Table 7: Closeness coefficients of alternatives

Alternatives		$d+i$	$d-i$	Satisfaction Degree $\mathbf{p_i}$	Ranks
Alternatives1	A1	0.161145	0.075441	0.312145	2
Alternatives2	A2	0.241414	0.118124	0.324237	1
Alternatives3	A3	0.234412	0.075441	0.212347	10
Alternatives4	A4	0.454417	0.166114	0.278489	6
Alternatives5	A5	0.477112	0.175441	0.278467	7
Alternatives6	A6	0.175147	0.067114	0.284489	4
Alternatives7	A7	0.345115	0.095414	0.256465	8
Alternatives8	A8	0.254441	0.112414	0.284486	5
Alternatives9	A9	0.256514	0.132114	0.302465	3
Alternatives10	A10	0.365145	0.124114	0.235785	9

4.3 Sensitivity Analysis

Sensitivity investigation is one of the most powerful means to authenticate the results achieved. After obtaining the results through the suggested methodology, we evaluated the findings of our study by altering the parameters. We have performed 10 experiments [12,13] in our study because we gave 10 selected alternatives in the Fig. 1. By changing the parameters with regard to the obtained results, it was noticed that the A2 stays unchanged and continues to be in the top level. The tabulations of the sensitivity evaluation have been depicted in Tab. 8.

Fig. 3 shows the experiment results of the experiment in comparison to the original weights. We found that in all the 10 experiments, Exp-2 (A2) reached the best satisfaction degree with respect to original weight as shown in Tab. 8. As evident by the results, the alternatives are sensitive to the weights.

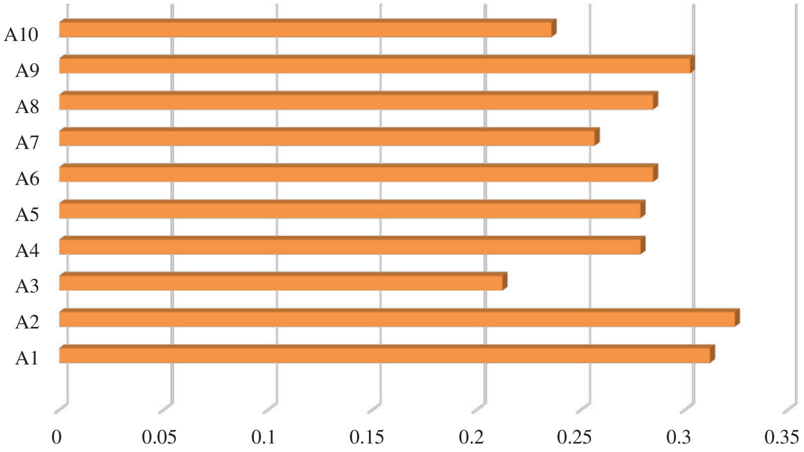

Figure 2: Alternatives obtained satisfaction degree

Table 8: Sensitivity analysis

Experiments		Obtained Weights	F1	F2	F3	F4	F5	F6	F7
Exp-1	A1	0.312145	0.202400	0.213600	0.218200	0.315300	0.308000	0.332000	0.315300
Exp-2	A2	0.324237	0.312300	0.313400	0.307000	0.213600	0.218200	0.202400	0.213600
Exp-3	A3	0.212347	0.315300	0.308000	0.332000	0.332000	0.315300	0.308000	0.332000
Exp-4	A4	0.278489	0.213600	0.218200	0.202400	0.315300	0.308000	0.332000	0.315300
Exp-5	A5	0.278467	0.332000	0.315300	0.308000	0.213600	0.218200	0.202400	0.213600
Exp- 6	A6	0.284489	0.315300	0.308000	0.332000	0.315300	0.308000	0.332000	0.316100
Exp-7	A7	0.256465	0.213600	0.218200	0.202400	0.213600	0.218200	0.202400	0.214600
Exp- 8	A8	0.284486	0.332000	0.315300	0.308000	0.332000	0.315300	0.308000	0.308000
Exp- 9	A9	0.302465	0.202400	0.213600	0.218200	0.202400	0.213600	0.218200	0.218200
Exp-10	A10	0.235785	0.312300	0.313400	0.307000	0.312300	0.313400	0.307000	0.314500

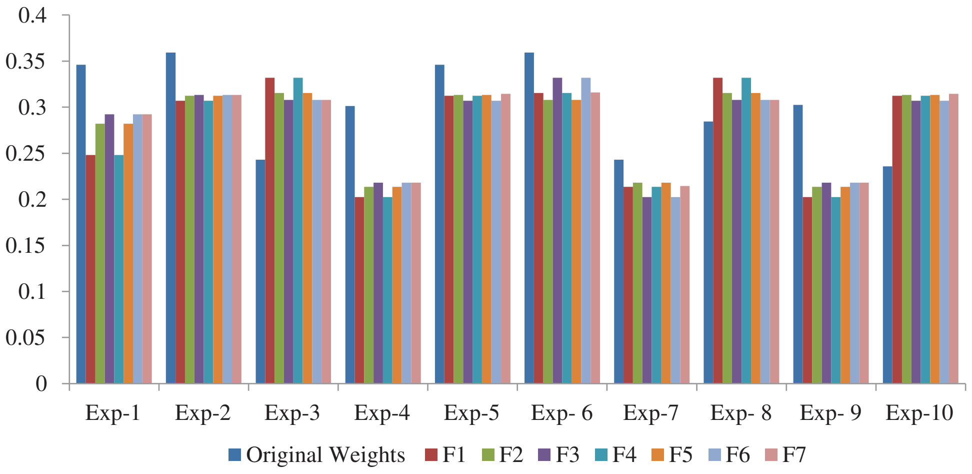

Figure 3: Experiment results compare with original weights

5 Conclusions

The integrity of medical devices is affected at the execution period by the method of data storage, data transfer and migration. However, these problems can be resolved by upgrading the software patch, the hardware security guards and network encryption procedures. Medical devices carry highly confidential details related to the patients' health and personal data. In this report, we have developed a framework which does a quantitative evaluation of the integrity of medical devices. We used the integrated Fuzzy-ANP.TOPSIS approach in our system, which is one of the best decision-making procedures and ranking approach.

By using these approaches, the decision-makers assigned the ranks of the medical devices as per their levels of integrity. The report engaged the support of 10 professionals working in various security fields. They assessed the devices' integrity based on their experiences and ranked them accordingly. Finally, F.ANP.TOPSIS was applied on the given data for evaluating the performance of the medical devices. Findings of this research work as follows:

- Most researchers work on the security of the medical devices, but do not have sufficient guidance for the design and development of the software of device.
- Our system is comprehensive and provides the developers with effective guidelines for software design by complying with the security laws.
- Integrity estimation of the medical devices will not only ensure secure operation of medical devices' and protect the personal details of patients, but will also improve the devices' technical characteristics.
- Manufactures and the government bodies could use the proposed system to check the integrity of the medical devices quantitatively and accurately.

Acknowledgement: This work has been funded by the grant number 12-INF2970-10 from the National Science, Technology and Innovation Plan (MAARIFAH), the King Abdul-Aziz City for Science and Technology (KACST), Kingdom of Saudi Arabia. We thank the Science and Technology Unit at Umm Al-Qura University for their continued logistics support.

Funding Statement: Funding for this study was granted by the King Abdul-Aziz City for Science and Technology (KACST), Kingdom of Saudi Arabia under the Grant Number: 12-INF2970-10.

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 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. 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 M. Alemzadeh, "On threat modeling and mitigation of medical cyber-physical systems," in *Proc. IEEE/ACM International Conference on Connected Health: Applications Syste*, 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] 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. 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] 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.

[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. IEEE Int. Congress on Internet of Things*, San Francisco, USA, pp. 140–147, 2018, https://hal.archives-ouvertes.fr/hal-01898660.

[16] 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.

[17] A. I. Newaz, A. K. Sikder, L. Babunand 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.

[18] 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.

[19] 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.

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

[21] 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. [Online]. Available: https://www.usenix.org/conference/usenixsecurity16/technical-sessions/presentation/costan.

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

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