Received: January 26, 2020. Revised: May 7, 2020. 

INASS

International Journal of
Intelligent Engineering & Systems

http://www.inass.org/

# A Hybrid Fuzzy Rule-Based Multi-Criteria Framework for Security Assessment of Medical Device Software

**Abdullah Algarni[1] Masood Ahmad[2] Abdulaziz Attaallah[1] Alka Agrawal[2] Rajeev Kumar[2] Raees Ahmad Khan[2]**

[1]*Faculty of Computing and Information Technology, King Abdulaziz University, Jeddah, Saudi Arabia*
[2]*Department of Information Technology, Babasaheb Bhimrao Ambedkar University, Lucknow, Uttar Pradesh, India*
* Corresponding author's Email: rs0414@gmail.com

**Abstract:** The third party software components for medical devices are a critical issue because the hackers can send the updates for medical device software which may contain malware that can affect the medical devices. To quote an instance in this regard is the report generated by Zoll, a supplier of medical devices, which states that several patients' data was exposed in 2019 due to an error which occurred at the time of software updating. In this paper we have attempted the assessment the security of medical devices software from different suppliers. We applied the Fuzzy Analytic Network Process (ANP) and Technique for Order Preference by Similarity to Ideal Solution (TOPSIS) methodology for the assessment of third party software component of medical imaging devices. We have listed the criteria and alternatives for the assessment of the software security. The tabulated results that have been presented in the study are evidently showing the satisfaction degree and the ranking of the software security in the obtained order of A6, A1, A2, A5, A4, and A3. Furthermore, the ranking of the software shows that Rank 1 obtained A6 alternatives, which implies that it is absolutely important. Likewise, Rank 2 implies strongly important, 3rd Rank shows fairly important, 4th shows weakly, 5th shows equally and the 6th Rank equates with bad. Use of our framework would be an apt guideline for the manufacturers and users in developing software that is efficacious while being secure for all the stakeholders associated with the use of medical devices. Should the developers adhere to the suggested framework in this study, they can be assured of developing secure medical device software at the initial level of development of the software.

**Keywords:** Software security, Medical device security, Fuzzy ANP-TOPSIS, Software updating.

## 1. Introduction

Software of medical device should be fulfilling system properties like that of safety, security, reliability, availability, and confidentiality etc., [1]. Software based medical devices for patient's treatment particularly ranges from the computerized treatments of disease through the mobile apps and computer systems. A takes prize of security risks in medical devices can harm the patient. During 2006 to 2011 there were a total 5294 recalls. 20 to 25% of these recalls were due to computer failure. Medical devices consist of computing functions like a wireless communication, software based control and network based transmission. This computing function causes cyber-attacks [2]. Cyber security protects the computing system from the vulnerability to security beaches. Most of the medical devices contain embedded systems [3].

The advancements of technology enable the communication with other devices for sending or receiving data, or affixing the software patches [4]. While this has multitude of benefits, it also renders the devices vulnerable to attackers [5]. A slight manipulation can lead to malfunctioning of the medical device resulting in patients' data being stolen or, worse, faulty treatment which could be life-threatening [6]. Vulnerabilities of software exploitation are publically available on the websites. However, FDA is not certain about these

vulnerabilities related events. The FDA provides the guidelines to the manufactures to examine cyber security all along the process of design phase and development phase to the medical devices and manufactures discuss the issue of cyber security management before the premarket submissions [7, 8]. New medical devices will be safe and secure if we are aware about the cyber security vulnerability in the design and development phase of the software [9]. Usually we talk about changing the hardware in medical device which is a very tough task [10, 11]. However, there is an easy way to mix the cyber security to govern the medical device software and give software patches or updates. Software based control device can be overcome by a stubborn traducer. And, most of the attackers attack on the devices through the software updates by sending the mails for updating to the users or the healthcare organizations. When the users open the link then the attackers easily exercise control of the device and infect the device. Infected medical devices will malfunction and be slow in processing [12].

The major challenge for the security experts is to secure the medical device against the vulnerabilities by providing the software patches or updates but without changing the platforms. The Department of Homeland Security (DHS) has analyzed 11 vulnerabilities, named URGENT/11[13] which affect the medical device through the software. Most of the vulnerabilities in medical device come through the third party software. To assess the malicious version of software sending by the third party, we have used the Fuzzy ANP-TOPSIS methods. The main purpose of employing the Fuzzy ANP-TOPSIS is to assess the software security and development of the guidelines for secure development of software. By the Fuzzy ANP TOPSIS, the authors of this study have provided the ranks of the software that is safe or unsafe for medical device. Such a technique has been used for the first time for the security assessment of medical device software. This technique has been enlisted for the classification and selection of methods, devices, risks and other things but in this paper the authors have used it for software security checking. After ranking the software, authors have also added validation for making the software secure. This methodology can also be used by the manufactures and vendors for security assessment of the software at the time of development time. This approach ensures safer medical device at the primary stage of installation of the device. This is totally automated framework in which only the vendors and manufacturers set the list of criteria required for the software security assessment.

## 2. Literature review

Daniel et al. [2012] Authors have done the evaluation of FDA post market device through surveillance methods for assessing the security and privacy qualities. Most of the medical devices have computational powers like wireless transmission, internet connectivity for software base controlling device and stored medical information, etc. These features invite security and privacy risks. In the analysis, it was found that recall of software increases the security risk due to unsafe updates of software. Device problems associated with privacy and security should be clinically identified to be developed into recordable form because these challenges are difficult to find. Authors suggest that best techniques should be used to evaluate the functions of the device.

Kevin Fu & James Blum [2013] performed a survey on cybersecurity Risks of Medical Devices software. The security and privacy risk detected at the time of development phase is easy to remove and effective, thus, keeping the device safe from cybersecurity threats.

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

Zery W et al. [2015] - Profiled an article on the security challenges on the medical devices: *Implantable devices, often dependent on software, they save lots of lives. But how?* Most of the medical devices have embedded software, this is called information system. Information system has operational goals like confidentiality, integrity, and availability. Medical device contains hardware, software and interoperable threats. They used formal methods for certifying the hardware and software of the medical device. Device behavior doesn't change at the time of verification through these formal methods.

Wang &Yaping Chai [2018] did a survey on how the medical devices are at risk: *Information Security on Diagnostic Imaging System*. They chose medical devices from different vendors and mapped checklist criteria to check the different parameters of diagnostic imaging system, like confidentiality, integrity, availability, auditing and supplementary requirements, etc. They found that many of the devices were at risk and they needed to improve security.

Riyaz et al. [2018] proposed a framework to assess cyber security challenges in smart cities. IoT devices are connected with the device. In some cases, the IoT devices are not connected directly to the device. They are connected with intermediate device. This makes the IoT connected device insecure. In this system, they used the Fuzzy AHP technique to provide the rank of affected areas by cyber security challenges in smart city.

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

To improve the medical imaging device fine grained security, Pingchuan Ma et al [12] planned a FAHP based quantitative model for the cyber security assessment. Proposed model was based on Medical imaging device for the assessment of security. In this study, the authors have used medical imaging devices and focused on the medical device software security checking provided by the third party vendors. In FDA, publishing a security outfit described 11 vulnerabilities, known as URGENT/11[13]. This vulnerability happens through the software and they may allow the hackers to remotely control the medical device and updated devices functions. The reason behind it is the denial of service attacks, information leaks and logical flaws in the device. We used Fuzzy ANP-TOPSIS methods for assessing the software security in medical device provided by the medical device manufacturers and third party software providers [14, 15].

A lot of the work has been done in the context of medical device security. However, the software security assessment has yet not been done in the domain of medical device software security. A quantitative assessment of software security of medical device is necessary because manually testing of software is not always effective. Manual testing of software may lead to questions on the testing or the tester biasness. Authors framework is fully automated which is free from biasness and human errors that can be made at the time of testing of software.

## 3. Security assessment of medical device software

Medical device contains embedded system (Hardware, software) for diagnosis and treatment of the patients. Software plays an important role in medical devices for communication with the other devices and in ensuring connectivity over the Internet. During the communication and connectivity, attackers avail of openings to intrude on the device. So, the software planners of medical devices should prioritize their focus on not just the functionality but also on the security. Medical device security is important from the patient's point of view. For this research, we have chosen Confidentiality, Integrity and availability (CIA) [16] attributes because these are the basic attributes for information system security for software security assessment. This study also explains the effect of these attributes on the medical device software. Identified security attributes are classified in the level 1 and level 2, level 1 attributes affect the level 2 attributes like confidentiality affects reliability, extensibility and effectiveness [17] and remaining two attributes also affect the same. This is shown in Fig. 1.

### 3.1 Confidentiality

In terms of software security, confidential means keeping the users' information secret from publication and unauthorized access. Only authorized people can access the confidential data. Most of the incident happens due to loss of confidentiality.

### 3.2 Availability-

The availability means that a system is to be available for authorized persons when the authorized persons want to update the software for security patches. Availability of data or system is checked by the access of the information without any interruption.

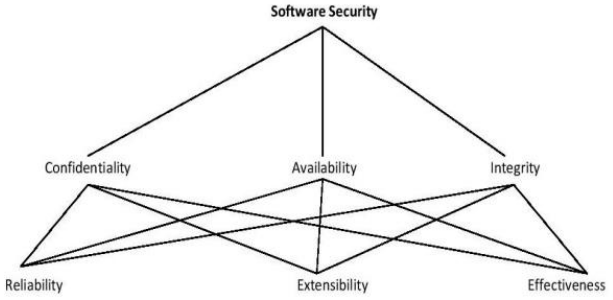


Figure. 1 Security assessment attributes

### 3.3 Integrity

Integrity means that the accuracy of the information in the terms of software security information should not be changed, and the origin of information should be from the actual origin. Integrity shows truthiness, accuracy and correctness of information overall. Software security factors in first level are shown as F1, F2 and F3 and security factors that are further classified in the second level are: Reliability, Extensibility and Effectiveness. All security factors are defined as:

**Reliability-** refers to the software's ability to work within the given situation for specified time duration. In terms of software security, reliability is to maintain the functionality of the system.

**Extensibility-** Extensibility is the principle of system design; Security will be improved if we change their requirements. If we want to make a system more secure then we will have to change the existing methodology.

**Effectiveness-** Effectiveness in software is the ability to generate a motive outcome. Effectiveness is also the reference to achieving the desired level of security. Design plays an important role in software development and a defect in the design could be fatal in the case of the security of medical devices [16]. Security has become a volatile property of software. Vulnerabilities are easily identified by hackers and once a particular weakness is traced by the hacker, the system is at the risk. Whenever the developers of a system find vulnerability, they must fix the problem. Updates should be sent to the system with those problems. The updates themselves may be used for an attack. Hence, security must be the top preference in medical device software development.

## 4. Methodology

Decision making is a multiple criteria process in the terms of security attributes [18]. Therefore, the assessment of medical device software security would also relate to Multi Criteria Decision Making (MCDM). Multiple approaches are available for solving the decision making problem. If multiple contentions occur at the time of calculation, then we can use MCDM approaches which support the experts' decision [18, 19, 20]. For medical device software security assessment, we have used the Fuzzy ANP- TOPSIS approach. ANP refers to the goal, criteria, and alternatives in the form of network [21, 22]. The analysis of outcomes in distinct applications with the help of TOPSIS approach shows the quality assessment indicators which affect the calculating of

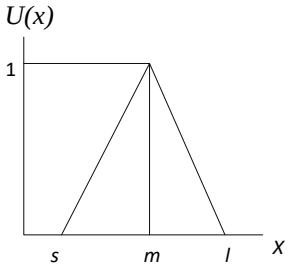


Figure. 2 Triangular fuzzy number

Table 1. Linguistic terms and the corresponding TFNs values

| Saaty Scale Definition | Fuzzy Triangle Scale | |
|---|---|---|
| 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<br>4<br>6<br>8 | Intermittent values between two adjacent scales | (1 ,2, 3)<br>(3 ,4, 5)<br>(5 ,6, 7)<br>(7 ,8, 9) |

results. Attributes selection is very important. Fuzzy ANP- TOPSIS hybrid approaches are used here [23, 24, 25]. A systematic way of calculating the weights and ranking of the satisfaction degree has been shown below in systematic way:

***Stage 1:*** TFN express as s- small, m- middle, and l- large. We have used in this paper TFN membership function and its values lies between 0 and 1 interval. Also, Fuzzy number Fn on Tn is called TFN. TFN membership function is calculated with statement (1 and 2).

$$\mu_a(x) = Tn \rightarrow [0,1] \tag{1}$$

$$\mu_a(x) = \begin{cases} \frac{x}{m-s} - \frac{s}{m-s} & x \in [s, m] \\ \frac{x}{m-l} - \frac{l}{m-l} & x \in [m, l] \\ 0 & \text{Otherwise} \end{cases} \tag{2}$$

Decision makers allot numbers to the facts which affects the values in a numeric from, scale presented in Table 1. Statement (3 to 6) used for changing the numeric values into TFN and TFN shows as s- small, m- middle, and l- large. TFN [ŋij] is assessment as:

$$\eta_{ij} = (s_{ij}, mi_{ij}, l_{ij}) \; ; Where \; l_{ij} \leq mi_{ij} \leq u_{ij} \tag{3}$$

$$S_{ij} = min(J_{ija}) \tag{4}$$

$$m_{ij} = (J_{ij1}, J_{ij2}, J_{ij3})^{\frac{1}{x}} \quad (5)$$

$$and \quad l_{ij} = max(J_{ijd}) \quad (6)$$

Experts give the comparative importance ($J_{ijk}$) values between the criteria. In $J_{ijk,}$ i and j shows Pair of criteria decided by experts $\eta_{ij}$ values is assessed on the behalf of geometric mean of experts' views for a exact kin. We find the total TFN values by the statement number (7 to 9). Assume TFNs Tf1and Tf2 Where Tf1= ($s_1$, $m_1$, $l_1$) and Tf2= ($s_2$, $m_2$, $l_2$). Operations are performed on two triangular fuzzy numbers which are shown as:

$$(s_1, m_1, l_1) + (s_2, m_2, l_2) = (s_1 + s_2, m_1 + m_2, l_1 + l_1) \quad (7)$$

$$(s_1, m_1, l_1) + (s_2, m_2, l_2) = (s_1 + s_2, m_1 + m_2, l_1 + l_2) \quad (8)$$

$$(s_1, m_1 l_1)^{-1} = (\frac{1}{s_1}, \frac{1}{m_1}, \frac{1}{l_1}) \quad (9)$$

***Stage 2:*** According to the reply from the experts, we designed the pair-wise decision matrix and tested the consistency of the experts' perspectives. We prepared the Consistency Index (CI) which is assessed by statement (10).

$$CI = (\gamma_{max}\text{-}N)/(N\text{-}1) \quad (10)$$

Here CI = Consistency Index, N = number of compared elements.

In addition, the authors divide the Consistency Index by Random Index [(*RI)*] generated through *Saaty* to calculate the Consistency Ratio (CR) given by the different experts. Consistency ratio is used here for trying out the consistency of pair-wise comparison matrix in table. This is shown in statement (11):

$$CR = CI/RI \quad (11)$$

***Stage 3****:* After the pair-wise comparison matrix has been constructed, we do defuzzification for again getting the crisp value situated on the assessment of TFN values. Defuzzification is commonly helped as an alpha cut method. Defuzzification process can be derived from statement (12) and is shown in statement (12 to 14).

$$\mu_{\alpha,\beta}(\eta_{ij}) = [\beta.\eta\alpha(s_{ij}) + (1\text{-}\beta).\eta\alpha(l_{ij})] \quad (12)$$

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

$$\eta\alpha(s_{ij}) = (m_{ij} - s_{ij}).\alpha + s_{ij} \quad (13)$$

$$\eta\alpha(l_{ij}) = l_{ij} - (l_{ij} - m_{ij}).\alpha \quad (14)$$

In the above statements, α and β are used for preferences of experts. Both values lie in 0 and 1 interval.

***Stage 4****:* the super matrix construct with the priority vector of pair-wise comparisons of different groups which contain goal, criteria, sub criteria, and alternatives.

***Stage 5***: Involves resolving the TOPSIS, we use performance ranking of each and every alternative in place of normalized factor [18]. Statement (15) is shown as:

$$TOP_{ij} = \frac{x_{ij}}{\sqrt{\sum_{i=1}^{m} x_{ij}^2}}; (i = 1,2, \ldots m; \text{ and } j = 1,2, \ldots n.) \quad (15)$$

Normalized weighted decision matrix $s_{ij}$ is calculated by multiplying the wights ($w_i$) of criteria with normalized outcome. After that, Normalized Weighted Decision Matrix is calculated by statement (16):

$$s_{ij} = w_i TOP_{ij}; (i = 1,2, \ldots m \text{ and } j = 1,2, \ldots n.) \quad (16)$$

***Stage 6*:** We assessed the ($R^+$) positive ideal solution matrix and ($R^-$) negative ideal solution matrix by the statement (17). In this stage we ascertain the difference from ideal solution in positive and negative solution.

$$R^+ = v_1^+, v_2^+, v_3^+ \ldots\ldots v_n^+$$
$$R^- = v_1^-, v_2^-, v_3^- \ldots\ldots v_n^- \quad (17)$$

Here $v_j^+$, $v_j^-$ (j= 1,2,3...*n*)

***Stage 7*:** In the last stage, we identified the gap among each values of criterion and found the positive and negative ideal solution matrix, by the statement (18 & 19):

For Positive ideal solution:

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

here $d_i^+$ represent distance to the positive ideal solution for i option.
For Negative ideal solution:

$$d_i^- = \sqrt{\sum_{j=1}^{m}(s_{ij} - v_i^-)^2} \; ; i = 1,2,3 \ldots . m \quad (19)$$

Where $d_i^-$ is the distance to the negative ideal solution for i option.

Preference or satisfaction degree ($p_i$) is used to calculate the ranking of each alternative assessment by statement (20).

Satisfaction table shows that the alternatives are close to the positive solutions ($d_i^+$) and far from the negative solutions ($d_i^-$) shown in the equation below.

$$p_i = \frac{d_i^-}{d_i^- - d_i^+}; \quad \text{Where i= 1, 2, 3….m.} \quad (20)$$

Ranking of each alternative is calculated based on calculation of satisfaction degree. Thus, the security assessment of the *Third-Party Software Component Used in Medical Devices* is effectively done by using Fuzzy ANP- TOPSIS method and assigning the rank of the software alternatives. The next section further elaborates this with the detail discussion on the empirical assessment of software security.

## 5. Data analysis

Quantitative measuring of the medical device software security is a typical process. Third party software is a big issue in medical imaging device security. Through the software, the attackers can access the medical imaging device and information of patients. FDA also provides guidelines for security of medical imaging device [7]. In this paper, the authors have postulated a framework for security of the third party software of medical imaging devices by using Fuzzy ANP-TOPSIS methodology. Security assessment of third party software component goal is divided into criteria, sub-criteria, and alternatives [15, 19]. All of these have been explained in section-III in this paper and in Fig. 1.

Through the statement from (1 to 20), we calculated the security of third party software of medical imaging device by using Fuzzy ANP-TOPSIS methodology. This has been depicted step-by-step below. From the Table 1 and statement number (1 to 10), we have designed a pair-wise comparison matrix for level 1 as shown in Tables 2, 3, 4, and 5.

In the next stage, from the statements (11 to 14), we assessed the unweighted super matrix. Results are shown in table 6. In the next stage, with statement 15, we assessed the weighted super matrix, limit super matrix and Weight normalized by statement 16 and results have been shown in Table 7, 8, and 9.

Table 2. Fuzzy pair-wise comparison matrix for level 1

| | F1 | F2 | F3 | Normalized Weights |
|---|---|---|---|---|
| **F1** | 1.00, 1.00,1.00 | 1.70, 1.40,1.10 | 1.30, 1.80, 2.30 | 0.30, 0.40, 0.60 |
| **F2** | 0.90, 0.70,0.60 | 1.00, 1.00,1.00 | 1.70, 1.40, 1.80 | 0.20, 0.30, 0.40 |
| **F3** | 0.80, 0.60,0.40 | 0.98, 0.73,0.59 | 1.00, 1.00, 1.00 | 0.18, 0.25, 0.34 |

Table 3. Fuzzy pair-wise comparison matrix for level 2

| | F11 | F12 | F13 | Normalized Weights |
|---|---|---|---|---|
| **F11** | 1.00, 1.00, 1.00 | 1.40, 1.80, 2.30 | 2.50, 3.10,3.80 | 0.12, 0.19,0.31 |
| **F12** | 0.40, 0.60, 0.70 | 1.00, 1.00, 1.00 | 1.70, 1.90,2.10 | 0.10, 0.16,0.25 |
| **F13** | 0.30, 0.30, 0.40 | 0.50, 0.50, 0.60 | 1.00, 1.00,1.00 | 0.08, 0.13,0.21 |

Table 4: Fuzzy Pair-Wise Comparison Matrix for level 2

| | F21 | F22 | F23 | Normalized Weights |
|---|---|---|---|---|
| **F21** | 1.00, 1.00,1.00 | 0.50, 0.70,0.90 | 1.40, 1.80,2.20 | 0.10, 0.20, 0.30 |
| **F22** | 1.20, 1.50,1.90 | 1.00, 1.00,1.00 | 1.60, 1.90,2.20 | 0.04, 0.07, 0.11 |
| **F23** | 0.50, 0.60,0.70 | 0.50, 0.50,0.60 | 1.00, 1.00,1.00 | 0.06, 0.09, 0.14 |

Table 5: Fuzzy Pair-Wise Comparison Matrix for level 2

| | F31 | F32 | F33 | Normalized Weights |
|---|---|---|---|---|
| **F31** | 1.00, 1.00,1.00 | 0.60, 0.8, 0.90 | 0.90, 1.10,1.50 | 0.23, 0.23,0.33 |
| **F32** | 1.10, 1.30,1.70 | 1.00, 1.00,1.00 | 0.72, 0.90,1.10 | 0.14, 0.17,0.21 |
| **F33** | 0.80, 0.90,1.20 | 0.90, 1.50,1.90 | 1.00, 1.00,1.00 | 0.16, 0.20,0.25 |

Table 6. Unweighted super matrix

| | Goal | F1 | F2 | F3 | F11 | F12 | F13 | F21 | F22 | F23 | F31 | F32 | F33 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Goal** | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 |
| **F1** | 0.20 | 0.50 | 0.40 | 0.30 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 |
| **F2** | 0.40 | 0.50 | 0.30 | 0.40 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 |
| **F3** | 0.40 | 0.10 | 0.30 | 0.30 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 |
| **F11** | 0.00 | 0.20 | 0.00 | 0.00 | 0.16 | 0.16 | 0.16 | 0.18 | 0.21 | 0.21 | 0.18 | 0.19 | 0.18 |
| **F12** | 0.00 | 0.20 | 0.00 | 0.00 | 0.16 | 0.13 | 0.19 | 0.18 | 0.16 | 0.18 | 0.19 | 0.19 | 0.18 |
| **F13** | 0.00 | 0.10 | 0.00 | 0.00 | 0.20 | 0.18 | 0.20 | 0.18 | 0.19 | 0.17 | 0.19 | 0.20 | 0.18 |
| **F21** | 0.00 | 0.00 | 0.20 | 0.00 | 0.14 | 0.12 | 0.15 | 0.14 | 0.16 | 0.16 | 0.14 | 0.16 | 0.14 |
| **F22** | 0.00 | 0.00 | 0.30 | 0.00 | 0.19 | 0.15 | 0.17 | 0.15 | 0.21 | 0.16 | 0.16 | 0.17 | 0.15 |
| **F23** | 0.00 | 0.00 | 0.20 | 0.00 | 0.15 | 0.13 | 0.20 | 0.19 | 0.19 | 0.21 | 0.17 | 0.14 | 0.20 |
| **F31** | 0.00 | 0.00 | 0.00 | 0.10 | 0.15 | 0.14 | 0.16 | 0.19 | 0.19 | 0.21 | 0.15 | 0.16 | 0.19 |
| **F32** | 0.00 | 0.00 | 0.00 | 0.14 | 0.18 | 0.18 | 0.20 | 0.20 | 0.19 | 0.23 | 0.20 | 0.18 | 0.20 |
| **F33** | 0.00 | 0.00 | 0.00 | 0.11 | 0.19 | 0.14 | 0.17 | 0.19 | 0.20 | 0.19 | 0.15 | 0.15 | 0.19 |

Table 7. Weighted super matrix

| | Goal | F1 | F2 | F3 | F11 | F12 | F13 | F21 | F22 | F23 | F31 | F32 | F33 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Goal** | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 |
| **F1** | 0.20 | 0.49 | 0.36 | 0.32 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 |
| **F2** | 0.40 | 0.44 | 0.32 | 0.35 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 |
| **F3** | 0.40 | 0.05 | 0.32 | 0.32 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 |
| **F11** | 0.00 | 0.19 | 0.00 | 0.00 | 0.03 | 0.03 | 0.03 | 0.03 | 0.03 | 0.03 | 0.03 | 0.04 | 0.03 |
| **F12** | 0.00 | 0.16 | 0.00 | 0.00 | 0.05 | 0.05 | 0.05 | 0.06 | 0.05 | 0.05 | 0.05 | 0.06 | 0.06 |
| **F13** | 0.00 | 0.13 | 0.00 | 0.00 | 0.05 | 0.05 | 0.05 | 0.06 | 0.05 | 0.06 | 0.06 | 0.06 | 0.05 |
| **F21** | 0.00 | 0.00 | 0.22 | 0.00 | 0.05 | 0.05 | 0.04 | 0.05 | 0.04 | 0.04 | 0.04 | 0.04 | 0.04 |
| **F22** | 0.00 | 0.00 | 0.29 | 0.00 | 0.05 | 0.04 | 0.04 | 0.04 | 0.04 | 0.04 | 0.04 | 0.04 | 0.04 |
| **F23** | 0.00 | 0.00 | 0.19 | 0.00 | 0.05 | 0.05 | 0.04 | 0.04 | 0.05 | 0.04 | 0.04 | 0.04 | 0.04 |
| **F31** | 0.00 | 0.00 | 0.00 | 0.13 | 0.03 | 0.03 | 0.04 | 0.04 | 0.05 | 0.04 | 0.04 | 0.04 | 0.05 |
| **F32** | 0.00 | 0.00 | 0.00 | 0.10 | 0.04 | 0.04 | 0.05 | 0.04 | 0.04 | 0.06 | 0.05 | 0.04 | 0.05 |
| **F33** | 0.00 | 0.00 | 0.00 | 0.10 | 0.05 | 0.05 | 0.04 | 0.04 | 0.04 | 0.04 | 0.04 | 0.04 | 0.04 |

Table 8. Limit super matrix

| | Goal | F1 | F2 | F3 | F11 | F12 | F13 | F21 | F22 | F23 | F31 | F32 | F33 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Goal** | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 |
| **F1** | 0.25 | 0.25 | 0.25 | 0.25 | 0.25 | 0.25 | 0.25 | 0.25 | 0.25 | 0.25 | 0.25 | 0.25 | 0.25 |
| **F2** | 0.38 | 0.38 | 0.38 | 0.38 | 0.38 | 0.38 | 0.38 | 0.38 | 0.38 | 0.38 | 0.38 | 0.38 | 0.38 |
| **F3** | 0.37 | 0.37 | 0.37 | 0.37 | 0.37 | 0.37 | 0.37 | 0.37 | 0.37 | 0.37 | 0.37 | 0.37 | 0.37 |
| **F11** | 0.60 | 0.60 | 0.60 | 0.60 | 0.60 | 0.60 | 0.60 | 0.60 | 0.60 | 0.60 | 0.60 | 0.60 | 0.60 |
| **F12** | 0.20 | 0.20 | 0.20 | 0.20 | 0.20 | 0.20 | 0.20 | 0.20 | 0.20 | 0.20 | 0.20 | 0.20 | 0.20 |
| **F13** | 0.20 | 0.20 | 0.20 | 0.20 | 0.20 | 0.20 | 0.20 | 0.20 | 0.20 | 0.20 | 0.20 | 0.20 | 0.20 |
| **F21** | 0.55 | 0.55 | 0.55 | 0.55 | 0.55 | 0.55 | 0.55 | 0.55 | 0.55 | 0.55 | 0.55 | 0.55 | 0.55 |
| **F22** | 0.35 | 0.35 | 0.35 | 0.35 | 0.35 | 0.35 | 0.35 | 0.35 | 0.35 | 0.35 | 0.35 | 0.35 | 0.35 |
| **F23** | 0.10 | 0.10 | 0.10 | 0.10 | 0.10 | 0.10 | 0.10 | 0.10 | 0.10 | 0.10 | 0.10 | 0.10 | 0.10 |
| **F31** | 0.39 | 0.39 | 0.39 | 0.39 | 0.39 | 0.39 | 0.39 | 0.39 | 0.39 | 0.39 | 0.39 | 0.39 | 0.39 |
| **F32** | 0.41 | 0.41 | 0.41 | 0.41 | 0.41 | 0.41 | 0.41 | 0.41 | 0.41 | 0.41 | 0.41 | 0.41 | 0.41 |
| **F33** | 0.20 | 0.20 | 0.20 | 0.20 | 0.20 | 0.20 | 0.20 | 0.20 | 0.20 | 0.20 | 0.20 | 0.20 | 0.20 |

Then we calculated the global weights through the network in second level by the repeating the process and showing the global weight in percentage in table 9. At the last stage, through the statement (17-20), we have assessed the subjective cognition, weight normalization and closeness coefficient shown in table10, table11, & table 12. We have chosen different alternatives in the form of A1, A2, and A3. A4, A5 & A6, and gaps in positive ideal solution and negative ideal solution way and the satisfaction degree and ranking of all alternatives of the satisfaction. This is shown in table 12. Fuzzy ANP-TOPSIS allows the decision makers to select the likely alternatives. Based on the collated data, the

satisfaction degree of each alternative is also calculated. The Final result and ranking of the software has been shown in table 12. With respect to the satisfaction degree, the ranking of all alternatives is A6> A1> A2> A5> A4> and> A3. Medical device software's security in different alternatives is good according to the findings and ranking of the software has been shown in the order.

Table 9. Global weights through the network

| Second Level Attributes | Global Weights | Global Weights in % |
|---|---|---|
| **F11** | 0.16 | 16% |
| **F12** | 0.17 | 17% |
| **F13** | 0.11 | 11% |
| **F21** | 0.13 | 13% |
| **F22** | 0.07 | 7% |
| **F23** | 0.09 | 9% |
| **F31** | 0.11 | 11% |
| **F32** | 0.09 | 9% |
| **F33** | 0.07 | 7% |

Table 10. Subjective cognition results of evaluators in linguistic terms

| | $A_1$ | $A_2$ | $A_3$ | $A_4$ | $A_5$ | $A_6$ |
|---|---|---|---|---|---|---|
| **F11** | 3.20, 4.60, 6.00 | 3.70, 5.30, 6.80 | 1.80, 2.80, 4.30 | 5.40, 6.70,7.70 | 2.90, 4.50,6.10 | 3.60, 5.40, 7.10 |
| **F12** | 4.00, 5.60, 7.10 | 2.20, 3.60, 5.30 | 3.20, 4.80, 6.30 | 3.70, 5.20,6.70 | 4.90, 6.50,7.80 | 2.60, 3.90, 5.40 |
| **F13** | 7.40, 8.90, 9.60 | 4.10, 5.40, 6.60 | 2.50, 3.90, 5.50 | 3.90, 5.70,7.40 | 5.00, 6.60,7.80 | 3.50, 5.00, 6.60 |
| **F21** | 2.90, 4.40, 5.90 | 3.40, 4.80, 6.30 | 4.90, 6.10, 7.10 | 2.50, 4.00,5.70 | 4.80, 6.20,7.40 | 2.40, 4.10, 5.90 |
| **F22** | 4.20, 5.70, 7.20 | 3.20, 4.50, 6.00 | 3.50, 4.60, 5.80 | 4.30, 6.10,7.70 | 2.70, 4.20,5.90 | 3.00, 4.40, 6.00 |
| **F23** | 3.20, 4.60, 6.00 | 3.70, 5.30, 6.80 | 1.80, 2.80, 4.30 | 5.40, 6.70,7.70 | 2.90, 4.50,6.10 | 3.60, 5.40, 7.10 |
| **F31** | 2.80, 3.90, 5.10 | 4.10, 5.60, 7.00 | 5.20, 6.70, 7.90 | 2.80, 3.70,4.90 | 4.10, 5.60, 7.00 | 5.10, 6.10, 6.90 |
| **F32** | 3.90, 5.50, 6.90 | 2.80, 4.10, 5.60 | 2.90, 4.40, 6.00 | 1.90, 2.90,4.30 | 3.50, 5.10,6.60 | 5.30, 6.80, 8.00 |
| **F33** | 2.90, 4.40, 5.90 | 3.40, 4.80, 6.30 | 4.90, 6.10, 7.10 | 2.50, 4.00,5.70 | 4.80, 6.20,7.40 | 2.40, 4.10, 5.90 |

Table 11.The weighted normalized fuzzy-decision matrix.

| | $A_1$ | $A_2$ | $A_3$ | $A_4$ | $A_5$ | $A_6$ |
|---|---|---|---|---|---|---|
| **F11** | 0.03,0.04,0.05 | 0.03,0.05, 0.06 | 0.01, 0.02,0.03 | 0.02, 0.02,0.03 | 0.01, 0.02,0.02 | 0.04,0.05, 0.07 |
| **F12** | 0.03,0.04,0.06 | 0.02,0.03,0.05 | 0.02, 0.03,0.04 | 0.01, 0.02,0.30 | 0.01, 0.02,0.03 | 0.03,0.03,0.05 |
| **F13** | 0.06,0.07,0.07 | 0.04,0.05,0.06 | 0.01, 0.02,0.03 | 0.01, 0.01,0.02 | 0.01, 0.02,0.02 | 0.03,0.04,0.06 |
| **F21** | 0.02,0.03,0.05 | 0.03, 0.04,0.07 | 0.03, 0.03,0.04 | 0.00, 0.01,0.02 | 0.01, 0.02,0.02 | 0.02,0.04, 0.05 |
| **F22** | 0.03,0.04,0.06 | 0.03, 0.04,0.05 | 0.02, 0.03,0.03 | 0.01, 0.02,0.03 | 0.01, 0.02,0.02 | 0.03,0.04,0.05 |
| **F23** | 0.03,0.04,0.06 | 0.02,0.03,0.05 | 0.02, 0.03,0.04 | 0.01, 0.02,0.03 | 0.01, 0.02,0.02 | 0.02,0.03,0.05 |
| **F31** | 0.03,0.04,0.05 | 0.03,0.04,0.05 | 0.01, 0.02,0.03 | 0.01, 0.01,0.02 | 0.01, 0.01,0.02 | 0.05,0.06,0.07 |
| **F32** | 0.02,0.03,0.05 | 0.03, 0.04,0.06 | 0.03, 0.03,0.04 | 0.01, 0.01,0.02 | 0.01, 0.02,0.02 | 0.02,0.04, 0.05 |
| **F33** | 0.03,0.04,0.06 | 0.03, 0.04,0.05 | 0.02, 0.03,0.03 | 0.01, 0.02,0.03 | 0.01, 0.01,0.02 | 0.03,0.04,0.05 |

Table 12. Closeness coefficients to the aspired level among the different alternatives

| Alternatives | | $d^{+i}$ | $d^{-i}$ | Satisfaction Degree of $p_i$ | Rank |
|---|---|---|---|---|---|
| **Alternative 1** | **A1** | 0.25 | 0.13 | 0.542540 | 2 |
| **Alternative 2** | **A2** | 0.24 | 0.15 | 0.495870 | 3 |
| **Alternative 3** | **A3** | 0.23 | 0.14 | 0.388540 | 6 |
| **Alternative 4** | **A4** | 0.22 | 0.15 | 0.425860 | 5 |
| **Alternative 5** | **A5** | 0.21 | 0.17 | 0.452540 | 4 |
| **Alternative 6** | **A6** | 0.22 | 0.20 | 0.545640 | 1 |

## 6. Comparison with the classical ANP-TOPSIS method

Similar set of inputs produce different results in different methods. For checking the consistency of results with applied methods, researchers use different techniques. In this paper, we used classical ANP-TOPSIS technique [20] for comparison to assess the accuracy of the results with FUZZY-ANP-TOPSIS. Classical ANP-TOPSIS and Fuzzy ANP-TOPSIS have the same way of data acquiring and data appraisal. The only difference is that no fuzzification is needed in the classical ANP-TOPSIS. In classical ANP-TOPSIS, data is shared in numeric form. Variances in the outcomes of fuzzy and classical ANP-TOPSIS are displayed in table 13 and variance display in graph has been shown in Fig. 2. The results obtained with both method classical

Table 13. Comparison results of Classical ANP and Fuzzy ANP-TOPSIS methods

| Methods/Alternatives | A1 | A2 | A3 | A4 | A5 | A6 |
|---|---|---|---|---|---|---|
| Fuzzy-ANP-TOPSIS | 0.542540 | 0.495870 | 0.388540 | 0.425860 | 0.452540 | 0.545640 |
| Classical-ANP-TOPSIS | 0.546697 | 0.494999 | 0.390997 | 0.425498 | 0.454999 | 0.540504 |

Table 14. Sensitivity Analysis

| Experiments | Weights/Alternatives | | A1 | A2 | A3 | A4 | A5 | A6 |
|---|---|---|---|---|---|---|---|---|
| Experiment-0 | Original Weights | Satisfaction Degree ($p_i$) | 0.54254 | 0.49587 | 0.38854 | 0.42586 | 0.45254 | 0.54564 |
| Experiment -1 | F1 | | 0.549237 | 0.500869 | 0.399537 | 0.431358 | 0.457539 | 0.546144 |
| Experiment-2 | F2 | | 0.52694 | 0.49087 | 0.38654 | 0.41986 | 0.44804 | 0.54564 |
| Experiment-3 | F3 | | 0.53054 | 0.48537 | 0.39354 | 0.41386 | 0.44354 | 0.54414 |

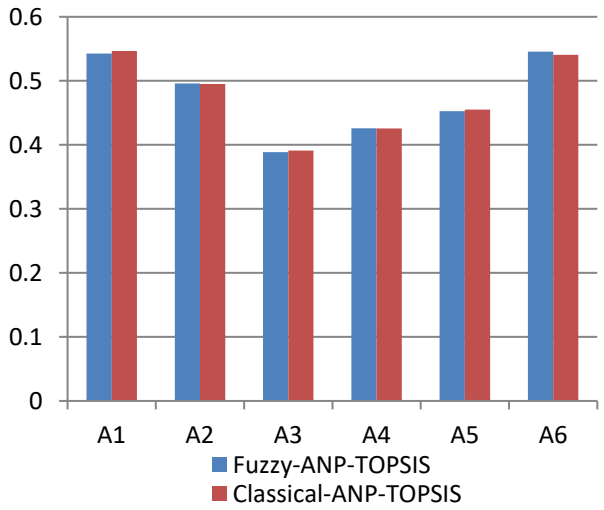


Figure. 3 Variances between results

ANP-TOPSIS method and Fuzzy ANP-TOPSIS method corresponds highly and the Pearson correlation coefficient is found to be 0.999176. Thus, it is conclusively proven that Fuzzy ANP-TOPSIS result accuracy is improved version of the classical ANP - TOPSIS.

## 7. Sensitivity analysis

For checking the validity of outcomes, we changed the set of inputs and did sensitivity analysis on it [18]. The weights are used as a variable in this work and sensitivity analysis is done on the weights result. In this paper, hierarchy has three factors and sensitivities are validated by weight performance. The weights of all the factors were modified and other factors weights remained unchanged and satisfaction degree ($p_i$) were measured by Fuzzy ANP-TOPSIS. Table 14 and graph in Fig. 4 depict the achieved outcomes of the sensitivity search. Variations are shown in Fig. 3 by the graph and saw that the Fuzzy-ANP-TOPSIS is give results better than the Classical- ANP-TOPSIS method.

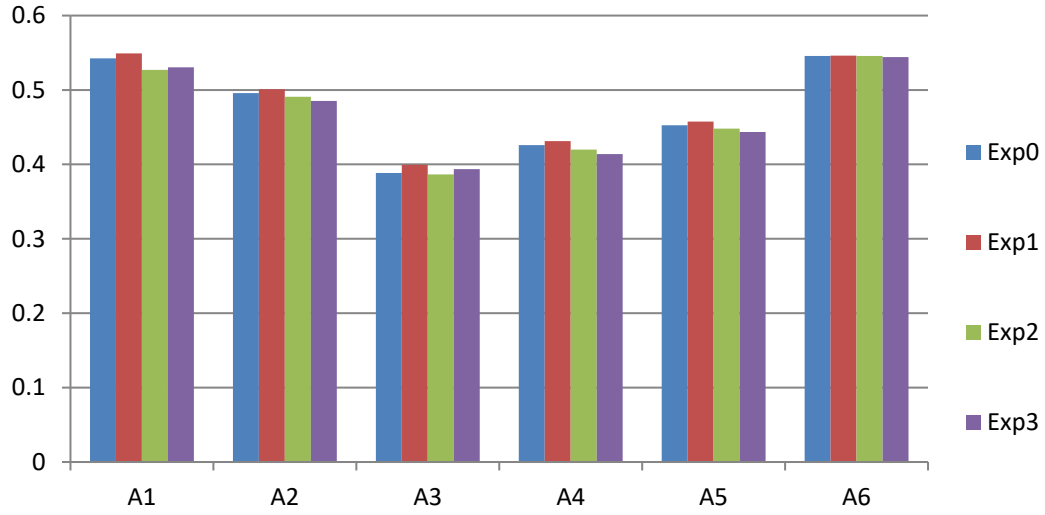


Figure. 4 Results of sensitivity analysis

In Table 14, the graph 4, first row shows the original weights of this work. According to original issues, alternative-6 (A6) has high satisfaction degree ($p_i$). From F1 to F3, three weights are executed. Accessed outcome shows that alternative-6 (A6) remains at the highest satisfaction degree ($p_i$) in 3 weights and the least weight of alternative-3 is in each weight. A deviation in the results with each other shows that the ratings of alternatives depend on the weights of the alternatives.

## 8. Discussion

As per the survey published by *Zoll* on January 24, 2019, 277319 patients' data and personal information was leaked after an error occurred at the time of server migration. Currently Zoll is also researching on methods for managing the third party dealers. Likewise, the dealers and suppliers of medical devices can also take preventive actions to avoid data breaches. Common reasons that affect the medical devices are the infected USB, Internet and software updating. The most common malicious software changed the medical devices to the nodes of "botnet" for criminal network. Through the malicious device node attackers keep eyes on the device and network. This is not just an issue pertaining to the health only but is also a theft of identity. Hence, the solution posited in this research study for employing Fuzzy ANP-TOPSIS for the assessment of security of medical software would be a nodal step towards the stated problem. Our security assessment is based on medical device software security because in the present era 23 to 25% attacks are done through the software. Hackers modus operandi is often to send mails for updating the software of the medical device. When the vendors and users update the software with malicious patch, then the hackers get control of the device and prey on the data. For our empirical analysis, we have chosen 10 different medical devices for assessment of security. Their names, however, cannot be part of the research paper as the privacy of the Brands has to be respected. We called 6 experts who had a lot of experience in their filed. They evaluated the security and gave the score for the device. After that, we took the data from experts and assessed the performance through the Fuzzy ANP-TOPSIS approach. Further, Findings of the paper are as follows:

- Security assessment of third party software in medical devices will not only secure the patients' privacy and aid in their treatment but also accrue social and economic benefits. Unethical hacking is both a criminal act and a social crime which must be contained. Moreover, designing secure software would be cost-effective for both the manufacturers and the end users.
- Manufacturer can develop guidelines for developing secure software.

Through the guidelines, the government and vendors can also check the device and software.
Security assessment of third party software components in medical imaging device is very critical. Some challenges for future work:

- Third party software component security always remains a challenge as different vulnerabilities unknown to the users or the developers are prone to be under attack by the hackers.
- Our framework is based on Fuzzy ANP-TOPSIS method which is dependent on input weights. If mistakenly weights are changed, then the results may be different.
- Different methodologies can also be applied for making the medical device software more secure.

## 9. Conclusion

Patients' lives and health are dependent on medical devices that facilitate their treatment. Nowadays healthcare industry solely relies on the medical devices security. Unfortunately, the security of the medical devices has emerged as a major issue as hackers target them. Any intrusion on the device's software can change the behavior of the device. Malfunction of a medical device can threaten the patient's life. Software system is never 100% secure. Sometimes social and economic factors affect the security quality. Security checking is a core and integral issue in medical device software. At the time of decision making process, the decision makers always face problems of uncertainty and vagueness. Through the Fuzzy ANP-TOPSIS, decision makers can reach more effective decisions. In this study focused on the assessment framework with Fuzzy ANP-TOPSIS methodology for judging the security of medical imaging device software. Authors have done this assessment on 6 different medical imaging devices software. Fuzzy ANP-TOPSIS Decision makers practiced linguistic variables for the assessment of criteria; evaluation of each alternative has been done by the criteria and sub criteria. Triangular Fuzzy numbers are made by linguistic variables and fuzzy decision matrix is created. After normalizing the fuzzy decision matrix, the weighted normalized fuzzy decision matrix is created. Distance of each alternative is calculated to PIS and NIS. After that, separate calculation of each satisfaction degree for each alternative is done. With respect to the

satisfaction degree in six alternatives, A6 was the best alternative. We also recommend that the development of security guidelines for software should mainly focus on the present day security requisites. The assessment of security in medical imaging device software in our study would help the manufacturers and developers to design guidelines and through them ensure that the software is secure. Medical device vendors and software developers can opt for appropriate methods according to problem. In future, other multi-criteria decision making methods would be needed for the assessment of the software security in medical devices.

## Conflicts of Interest

The authors declare no conflict of interest.

## Author Contributions

Conceptualization, Abdullah Algarni and Masood Ahmad; methodology, Masood Ahmad; software, Abdulaziz Attaallah; validation, Masood Ahmad, Alka Agrawal, Rajeev Kumar, and Raees Ahmad Khan; formal analysis, Abdullah Algarni, Abdulaziz Attaallah, and Rajeev Kumar; investigation, Abdullah Algarni; resources, Abdulaziz Attaallah; data curation, Abdulaziz Attaallah; writing—original draft preparation, Masood Ahmad, and Rajeev Kumar; writing—review and editing, Masood Ahmad, Rajeev Kumar, and Alka Agrawal; visualization, Abdulaziz Attaallah; supervision, Raees Ahmad Khan; project administration, Alka Agrawal, and Raees Ahmad Khan; funding acquisition, Abdullah Algarni, and Abdulaziz Attaallah.

## References


[1] K. Fu and J. Blum, "Controlling for Cybersecurity Risks of Medical Device Software", *Biomedical Instrumentation & Technology*, Vol. 48, No. s1, pp. 38-41, 2014.

[2] W. Zhiqiang, M. Pingchuan, C. Yaping, and Z. Jianyi, "Medical Devices are at Risk: Information Security on Diagnostic Imaging System", In: *Proc. of International Conf. on Computer and Communications Security*, Toronto, ON, Canada, pp. 2309-2311, 2018.

[3] M. Ngamboé, B. Paul, N. Ammari, K. Dyrda, and J. Fernandez, "Risk Assessment of Cyber Attacks on Telemetry Enabled Cardiac Implantable Electronic Devices (CIED)", *arXiv:1904.11908[cs.CR]*, 2019.

[4] D. Halperin, T. S. H. Benjamin, B. Ransford, S. S. Clerk, and B. Defend, "Pacemakers and Implantable Cardiac Defibrillators: Software Radio Attacks and Zero-Power Defenses", In: *Proc. of International Conf. On Security and Privacy (sp 2008) IEEE Symposium*, Oakland, pp. 129-142, 2008.

[5] J. Sametinger, J. Rozenblit, R. Lysecky, and P. Ott, "Security Challenges for Medical Devices", *Communication of the ACM*, Vol. 58, No. 4, pp. 74-82, 2015.

[6] K. Fu and J. Blum, "Inside Risks: Controlling for Cybersecurity Risks of Medical Devices Software", *Communication of ACM*, Vol. 56, No. 10, pp. 21-23, 2013.

[7] U.S. FDA. *Content of Premarket Submissions for Management of Cybersecurity in Medical Devices— Draft Guidance for Industry and Food and Drug Administration Staff*, Available at: http://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm356186.htm, December, 2019.

[8] D. B. Kramer, M. Baker, B. Ransford, A. M. Markhm, Q. Stewart, and K. Fu, "Security and Privacy Qualities of Medical Devices: An Analysis of FDA Postmarket Surveillance", *PLoS One*, Vol. 7, No. 7, pone.0040200, 2012.

[9] W. H. Maisel, M. Moynahan, B. D. Zuckerman, T. P. Gross, O. H. Tovar, D.-B. Tillman, and D. B. Schultz, "Pacemaker and ICD Generator Malfunctions: Analysis of Food and Drug Administration Annual Reports", *Journal of the American Medical Association*, Vol. 295, No. 16, pp. 1901–1906, 2006.

[10] J. Srinivasan and S. Adam, "A Cyber Security Risk Analysis Methodology for Medical Devices", In: *Proc. of International Conf. on IEEE Symposium Product Compliance Engineering (ISPCE, 2015)*, USA, pp. 1-6, 2015.

[11] M. Pingchuan, W. Zhiqiang , Z. Xiaoxiang, Z. Jianyi, L. Qixu, L. Xin, and W. Wentao, "Medical Imaging Device Security: An Exploratory Study", *arXiv:1904.00224v1 [cs.CR]*, 2019.

[12] M. Pingchuan, W. Zhiqiang, H. Xiali, Z. Xiaoxiang, Z. Jianyi, L. Qixu, L. Xin, and Z. Zihan, " A Quantitative Approach for Medical Imaging Device Security Assessment", In: *Proc. of International Conf. on Dependable Systems and Networks(DSN) 2019 49th IEEE/IFIP*, USA, pp. 5-6, 2019.

[13] *URGENT/11 Cybersecurity Vulnerabilities in a Widely-Used Third-Party Software Component May Introduce Risks during Use of Certain Medical Devices: FDA Safety Communication*, Available at: https://www.fda.gov/medical-

devices/safety-communications/urgent11-cybersecurity-vulnerabilities-widely-used-third-party-software-component-may-introduce, December, 2019.

[14] R. Kumar, M. Zaroor, 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.

[15] K. Sahu, and R. K. Srivastava, "Revisiting Software Reliability", *Data Management, Analytics and Innovation*, Vol. 254, pp. 221-235, 2019.

[16] 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.

[17] R. Kumar, S. A. Khan, and R. A. Khan, "Analytical Network Process for Software Security: A Design Perspective", *CSI Transactions*, Vol. 4, No. 2, pp. 255–258, 2016.

[18] C. Weaver, "Patients Put at Risk by Computer Viruses", *The Wall Street Journal*, Available at: http://online.wsj.com/article/SB10001424127887324188604578543162744943762.html, 2013.

[19] R. Kumar, A. I. Khan, Y. B. Abushark, M. M. Alam, A. Agrawal, and R. A. Khan, "An Integrated Approach of Fuzzy Logic, AHP and TOPSIS for Estimating Usable-Security of Web Applications", *IEEE Access*, Vol. 8, pp. 50944-50957, 2020.

[20] K. Sahu and R. Shree, "Stability: Abstract Roadmap of Software Security", *American International Journal of Research in Science, Technology, Engineering & Mathematics*, Vol. 15, pp. 183-186, 2015.

[21] K. Sahu, R. Shree, and R. Kumar, "Risk Management Perspective in SDLC", *International Journal of Advanced Research in Computer Science and Software Engineering*, Vol. 4, No. 3, pp. 1247-1251, 2014.

[22] R. Kumar, A. I. Khan, Y. B. Abushark, M. M. Alam, A. Agrawal, and R. A. Khan, "A Knowledge Based Integrated System of Hesitant Fuzzy Set, AHP and TOPSIS for Evaluating Security-Durability of Web Applications", *IEEE Access*, Vol. 8, pp. 48870-48885, 2020.

[23] A. Algarni, M. Ahmad, A. Attaallah, A. Agrawal, R. Kumar, and R. A. Khan, "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] 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.

Notation List

| | |
|---|---|
| $\mu_a$ | Membership function |
| a | Fuzzy set |
| Tn | Triangular Number |
| X | Universe of discourse |
| s,m,l | Small, medium, large |
| 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) |
| $TOP_{ij}$ | TOPSIS |
| $s_{ij}$ | Normalized Weighted Matrix |
| $(R^+),(R^-)$ | Positive and Negative ideal solution |
| $v_j^+$ and $v_j^-$ | $v_j^+$ is max of $s_{ij}$ if j is a advantage factor, $v_j^-$ 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 |