A Fuzzy Multi-Objective Covering-based Security Quantification Model for Mitigating Risk of Web based Medical Image Processing System

Abdullah Algarni[1], Abdulaziz Attaallah[3]
Faculty of Computing and Information Technology
King Abdulaziz University
Jeddah
Saudi Arabia

Masood Ahmad[2], Alka Agrawal[4]
Rajeev Kumar[5,]*,Raees Ahmad Khan[6]
Department of Information Technology
Babasaheb Bhimrao Ambedkar University
Lucknow, Uttar Pradesh, India

***Abstract*—Medical image processing is one of the most active research areas and has big impact on the health sector. With the arrival of intelligent processes, web based medical image processing has become simple and errorless. Web based application is now used extensively for medical image processing. Large amount of medical data is generated daily with more and more data being shared over public and private networks for the diagnosis of diseases through the web based image processing systems. Medical images like that of the CT (Computed Tomography) scan, MRI (Magnetic Resonance Imaging), X-Ray and Ultrasound images, etc., contain highly personal data of the patients. This data needs to be secured from intruders. Medical images are more sensitive to external interruption and manipulation in data may cause changes in the result. Data breaches in medical cases can lead to wrong diagnosis or even more fatal possibilities with life threatening results. So, security in web based medical image processing is a major issue. However, ensuring security for the medical images while preserving the characteristics of confidentiality, integrity, availability, etc., of medical images poses a major challenge. Working towards a feasible solution, in this study, authors are using a list of criteria for checking security level of the web based image processing system. We propose Fuzzy Analytic Hierarchy Process (FAHP) combined with Technique for Order Preference by Similarity to Ideal Solution (TOPSIS) in the list of criteria that affect the security assessment in medical image processing. At the results we see that FAHP-TOPSIS produce good results in security checking in web based medical image processing system. At the data analysis section all the steps showed which is involved in our model.**

***Keywords*—Web based medical image processing; fuzzy analytical hierarchy process; TOPSIS method; security management**

I. Introduction

Medical Image Processing is the most critical aspect of the diagnosis of a disease. The major benefit of the medical image processing is that it facilitates in detection of the disease in its early stages [1]. If the image processing is not done properly, it may lead to wrong diagnosis of the disease. Before the diagnosis, hospitals and doctors send the images or data for the image processing like storing, retrieving, denoising, etc. [2]. In this respect, the hospitals generate huge amount of digital data [3]. A new technology called cloud computing has emerged as one of the potential solutions for processing the medical image data [2]. Most of the hospitals do not own data storage space because medical images are large in size, making data storage an impractical alternative. Hence, most of the hospitals or labs avail of the cloud computing technology. Cloud provides the space and security of the data for which the hospitals pay the requisite tariff[4].

While the recent advancement in technologies provide new means (like cloud based image processing, web based medical image processing etc.) to handle the medical images, they also compromise their security due to easy to retrieve, manipulation and replication [5][6]. Most of these technologies are highly vulnerable in the present cyber security context because of ineffective security mechanisms. When attackers find loopholes in the existing security technology, then it is imperative to design new security technology for making the systems more secure [7] [8].

Medical image security has gained significant space in the recent endeavours of cyber security experts, practitioners and academic researchers. Security involves the following aspects: Confidentiality (only authorize users can access patient data), Availability (data available at the time of Natural damage), integrity (show that medical data hasn’t been changed) and authentication (information origin to be proven)[9]. Many methods can be applied to provide security for medical image like steganography, watermarking and encryption. Steganography and watermarking are used for authentication to prevent access to an unauthorized entity [6] [10]. There are a large number of image encryption methods because different applications require different levels of security [10] [11]. All of these securities techniques are used in transmission of data over the network [12]. Ample availability of digital data becomes an easy prey for the attackers to intrude upon, especially when the medical data is being sent over the network for processing the image, the attackers begin their attempts to trace the data [13]. Thus, the need for devising security mechanisms that afford optimum data integrity is becoming imminent by the day.

However before the use of security methods, security assessment is an even more important concern [14]. Most of the medical image systems are interlinked with Internet, and

*Corresponding Author

web applications [15]. These systems are easy targets of the attackers because limited mechanisms are applied to ensure system security and data privacy [9]. Most of the image processing devices like CT, X-RAY, MRI can also be invaded by the attackers. Medical devices also need security at the time of processing the images [11] [16]. In the present era most of the hospitals or diagnostics centers used web based application for storing the patient's data and processing on them [14] [5]. At the time of development of application, the developers do not focus on the security thereby unintentionally giving open access to the intruders [17][18].

In this context, for the assessment of cyber security risk, Pingchian Ma et al. proposed a hybrid model of AHP and FUZZY comprehensive Evaluation [16], this method is totally based on medical device security assessment. Limitation of Classical AHP is volatile scale of judgment and ranking problem in the device. In this paper author will present Fuzzy AHP- TOPSIS hybrid model to overcome the volatile scale of judgments and provide the ranks of the medical image processing system. Authors have done the comparative study with classical AHP and Fuzzy AHP and results displayed in the comparison section.

II. Literature Review

Most of the researchers are trying to find the security failure causes. In this literature review find out that security attributes shows an important role in medical image processing system security. CIA is the basic three poles of security which shows an important role in improving the security. Several factors like authentication, authorization, utility, possession and resilience remains which show an important role in medical image processing system security. Security related literatures are explained as: In 2019 A. Agrawal et.al. showing the sustainable security measurement on web application using. Agencies and development companies develop guidelines for making web applications design sustainable and secure.

In 2018 Yinghui et.al proposed a secure and privacy aware smart health system which is based on patient data privacy. Authors propose a secure resilient health system for protection and safe medical data transmission reduce risk if the private key becomes leakage. In 2018 Aqsa & Ricardo did a comprehensive study of security mapping in healthcare information systems. Authors find the issues in implementation and exploitation.

In2019 Shi & et.al develop a framework for privacy protection for health care big data management based risk access control. This is based on reliability of risk analysis of data in smart health care system patient data can be leak from three aspects: resource sensitivity, access behavior sensitivity and historical access. For risk assessment authors used fuzzy rule techniques which is used for decision making and providing guidance for improving healthcare system.

In 2018 Marwan et.al proposed a cloud based framework for securing medical image processing. Author used combined segmentation techniques and genetic algorithm for prevention of accidental disclosure of data. In 2018 Arun, Ashish & George provide a study on healthcare informatics and privacy. Author identify that not any standard body is available for identification genomic data as personal data. This method identifies and prevent from the access control.

M.Moayeri et.al(2015) done comparative study of Fuzzy AHP an TOPSIS methods for Math teachers selection. In this study authors shows that Fuzzy TOPSIS is better in comparison to classical AHP and TOPSIS.

In 2018Pingchuan Ma et al. proposed an FAHP model, for quantitative cyber security assessment, this model focusing on Medical imaging device security assessment the security in medical device and guidelines for manufacture and government to design secure devices. In 2018 M.Fatih & Gul used AHP-TOPSIS with Pythagorean Fuzzy Sets for security risk analysis. AHP Pythagorean Fuzzy used for expert judgment and TOPSIS Pythagorean Fuzzy for prioritization of identified risk. For risk analysis author used three parameters privacy, integrity and accessibility for risk analysis which shows that this methods improves effectiveness of classical risk analysis method. Alots of researcher work done in medical image secuirity but doesn't have work on medical image processing system security assessment. Ranking system in security of working system determine the longer security. In this paper author determine the ranking of security using FUZZY AHP-TOPSIS method discuss in next sections.

III. Security Assessment of Medical Image Processing System

Medical image processing system in modern medicine has become increasingly important; it is the best fit for a rapid and effective diagnosis. Actually, the medical image data provides useful information to doctors; assists in decision making and, as a result, improves treatment. Thus, any accidental change in medical image can negatively effect on the treatment [19]. Security of healthcare system/image processing system is essential part of the healthcare industry and the industry is intensifying its efforts in this direction.

All these findings of criteria satisfy the goal of assessment the security of medical image processing system. Security assessment criteria and goal show in the figure-1. For the security assessment, attributes of security assessment described below in detail.

- Confidentiality- Refers to minimal access and disclosure of data (or resource). A loss of confidentiality happens when the data is actually accessed by unauthorized user. Confidential information is not available to unauthorized access or for all users. Medical images also contain sensitive information which only the authorized person can access.

- Authentication- The main task of authentication is to validate the user, check the user's identity and match the data which is stored in the database. Authentication process provides access control for system by verifying, to see if user's given information matches with the database of the authorized users.

- Authorization- After the completion of identification and authentication process, the asset gives the permission to access the data. This process is called authorization.
- Availability- Data is said to be available if it is available in any circumstances when needed. In terms of medical image processing data should be available at over the traffic on website. The data should be manageable at any sustainable environment. Availability of data can be prevented due to power failure, hardware failure and software upgrades.
- Integrity- In terms of medical image processing, image data should not change. If the image data is changed at the processing time, then the results may be faulty. Data should not be altered in any circumstances and this is called data integrity. Data should be complete and unchanged from the original. Integrity maintains the accuracy of information.
- Utility-In the terms of medical image processing, image useful for sometime only. This is called utility. Old data is not useful for data utility purpose. Usefulness of data for a purpose is called utility of data. The difference between utility and availability is that the data is still available but no longer usable.
- Possession- Is to retaining the ownership and make data under control. If possession is lost then there would be control over the data. In terms of medical image processing, ownership of the data is imperative otherwise the original data would be lost or worst, be corrupted.
- Resilience- Resilience is the process of checking the resistance of medical image processing system to attacks. Resilience is implemented by using, OTP and encryption. Main task of resilience is to protect the entire system from attack, taking into observation all the unsafe components of the system.

Healthcare system design plays an important role in healthcare industry. While developing the healthcare system data, security should be the most prioritized concern. Through the security attributes we have designed the guidelines to develop the system. The rule set of medical image processing system security follows security attributes for assessment the security. Security assessment becomes difficult through the traditional method. To remove this difficulties and biasness, the FUZZY set theory used with AHP and TOPSIS give fruitful results.

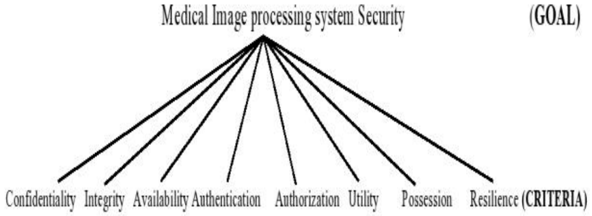

Fig. 1. Medical Image Processing System Security Attributes.

IV. Methodology

Different authors have analyzed medical image security. Changing the medical image processing security with Fuzzy AHP-TOPSIS is a new method for achieving both high security and user satisfaction. Besides, to achieve the goals as healthcare industry wants, we have used the Multi-Criteria Group Decision Making (MCGMD). In this section, we describe an approach for security assessment in medical Image processing system using Fuzzy AHP-TOPSIS. For the assessment of security, AHP approach is very suitable. But AHP faced the criticized due to unbalanced scale of judgments and it takes an exact value for decision making. To overcome these faults we have used Fuzzy AHP techniques for security assessment and Fuzzy TOPSIS used for providing the ranks of the systems. We took the sequence of steps of Fuzzy AHP-TOPSIS method to find the results which are shown as:

a) Fuzzy AHP: Fuzzy AHP is the approach used to calculate the weights of criteria; Fuzzy AHP represents problems in the hierarchy tree form with levels (goal and criteria). The top level shows the goal and objective. Second level shows the criteria and sub-criteria. The next step is building the Triangular Fuzzy Number (TFN) from the hierarchal structure. Triangular Fuzzy value is used for creating pair-wise comparison matrix.

Triangular Fuzzy membership value for pair wise comparison was employed by Chang[20]. In this paper, we adopted TFN, because they make calculation of membership functions easy and share out with fuzzy data. The TFN lies between 0 and 1. The linguistic values are divided as equally important, weakly important etc., and crisp values are shown as numeric 1,2,………..9., its membership function values are calculated by this equation (1-2):

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

$$\mu_a(x) = \begin{cases} \frac{x}{B-A} - \frac{l}{B-A} & x \in [A,B] \\ \frac{x}{B-C} - \frac{u}{B-C} & x \in [B,C] \\ 0 & Otherwise \end{cases} \tag{2}$$

Where, assigned A as lower, B as middle, and C as upper value equally in the triangular membership function. Figure 2 represent TFN value.

A TFN is shown in figure 2. Experts assigned the quantitative value to the linguistic terms in value; values are shown in table 1.

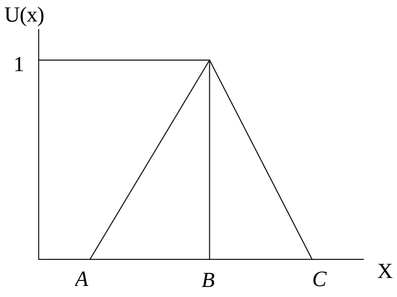

Fig. 2. Triangular Fuzzy Number.

TABLE. I. TFN SCALE

Security assessment Scale	Definitions	Membership function
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 4 6 8	Intermediate values between two adjacent scales	(1 ,2, 3) (3 ,4, 5) (5 ,6, 7) (7 ,8, 9)

The equations (3 to 6) are used for converting the numerical data into TFN [19], Φ_{ij} is calculated depend on the geometric mean of specialists' observation for a particular similarity. TFN [Φ_{ij}] is calculated as:

$$\Phi_{ij} = (A_{ij}, B_{ij}, C_{ij}) \tag{3}$$

$$where\ A_{ij} \leq Bi_{ij} \leq C_{ij}$$

$$A_{ij} = min(J_{ijd}) \tag{4}$$

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

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

The geometric mean is calculated by multiplying and adding two fuzzy numbers. Equations (7-9) used to calculate geometric mean. Consider two TFNs P1 and P2, P1= (A_1, B_1, C_1) and P2= (A_2, B_2, C_2). Calculation of Geometric means shown as:

$$(A_1, B_1, C_1) + (A_2, B_2, C_2) = (A_1 + A_2, B_1 + B_2, C_2 + C_2)$$
(7)

$$(A_1, B_1, C_1) \times (A_2, B_2, C_2) = (A_1 \times A_2, B_1 \times B_2, C_1 \times C_2) \tag{8}$$

$$(A_1, B_1, C_1)^{-1} = (\frac{1}{C_1}, \frac{1}{B_1}, \frac{1}{A1}) \tag{9}$$

A pair-wise n x n comparison matrix is created by dividing the row element with column by this equation (10).

$$\widetilde{M^d} = [\tilde{N}^d_{11} \mathrm{N}^d_{12} .. \tilde{N}^d_{1n} \tilde{N}^d_{21} \tilde{N}^d_{22} \ldots . \tilde{N}^d_{2n} \cdots \tilde{N}^d_{n1} \tilde{N}^d_{n2} \ldots \tilde{N}^d_{nn}] \tag{10}$$

Where $\widetilde{N^d_{ij}}$ shows the d^th experts give the importance of the i^th fact over the j^th fact. If more than one expert is present, then the average of each specialist is calculated by this equation (11).

In addition, we divide the Consistency Index by Random Index [*(RI) is generated from Saaty*] for calculating the Consistency Ratio (CR). This is shown in statement (11):

$$\tilde{N}_{ij} = \sum_{d=1}^{d} \quad \tilde{N}^d_{ij} / \mathrm{n} \qquad \text{n is the number of experts} \tag{11}$$

Next stage, Take the average of all factors in the hierarchy, here change the pair-wise comparison matrixes by this equation (12).

$$\tilde{M} = \lfloor \widetilde{\mathrm{N}_{11}} \ldots \widetilde{N_{1n}} \cdots \tilde{\mathrm{N}} \cdots \tilde{N}_{nn} \rfloor \tag{12}$$

After updating the pair-wise comparison matrix, with the help of equation (13) to calculate the fuzzy geometrical mean and fuzzy weights of every factor.

$$\tilde{O}_i = \left(\prod_{j=1}^{n} \quad \tilde{N}_{ij}\right)^{\frac{1}{n}}, i = 1,2,3 \tag{13}$$

Next stage, we add all geometric mean values to find fuzzy weights by this equation (14).

$$\tilde{\mathrm{Q}}_i = \tilde{O}_i \otimes \left(\tilde{O}_1 \oplus \tilde{O}_2 \oplus \tilde{O}_3 \ldots . \oplus \mathrm{O}_n\right)^{-1} \tag{14}$$

Next stage, we calculate the fuzzy average weight through equation (15).

$$P_i = \frac{\tilde{Q}_1 \oplus \tilde{Q}_2 \ldots . . \oplus \tilde{\mathrm{Q}}_n}{n} \tag{15}$$

Further, we normalized the fuzzy weight through the equation (16).

$$Nw_i = \frac{P_i}{P_1 \oplus P_2 \oplus \ldots \ldots \oplus P_n} \tag{16}$$

After that, we can de-fuzzify the fuzzy weights to get crisp values; the de-fuzzification methods use the Centre of Area (COA) to calculate the BNP (Best Non-fuzzy Performance) value of the fuzzy weights by equation (17).

$$BNPwD1 = \frac{\lfloor (CQ1 - AQ1) + (BQ1 - AQ1) \rfloor}{3} + AQ1 \tag{17}$$

b) Fuzzy TOPSIS: TOPSIS is used in the scenario of performance value decision. It is not used in crisp value but instead in the linguistic value given by decision maker. We used linguistic terms like very poor, poor, fair, good and very good. Without the numerical value, it is tough to assign the rank. Instead of directly assigning the linguistic value, the decision maker used Fuzzy AHP for fuzzy values for weights for each criterion. In addition, Fuzzy AHP-TOPSIS approach is totally suitable for fixing group decision-making problems in fuzzy environments. Fuzzy AHP-TOPSIS technique is as follows:

- In the first step, Fuzzy AHP is using to calculating fuzzy choice weights by mathematical statement (1-16).
- At last, by this mathematical statement (18) and table 2 we design the fuzzy decision matrix.

$$\begin{array}{ccc} & C_1 \ \ldots\ldots . & C_n \\ \tilde{M} = \begin{array}{c} A_1 \\ \ldots \\ A_m \end{array} & \left[\begin{array}{ccc} \tilde{x}_{11} & \cdots & \tilde{x}_{1n} \\ \cdots & \ddots & \cdots \\ \tilde{x}_{m1} & \cdots & \tilde{x}_{mn} \end{array}\right] \end{array} \tag{18}$$

Next stage, the standardized fuzzy decision matrix is represented by $\tilde{\mathrm{F}}$, simplified by the equation (19).

$$\tilde{F} = [\tilde{F}_{ij}]_{m \times n} \tag{19}$$

TABLE. II. LINGUISTIC SCALE FOR THE RATING

Linguistic Variable	*Corresponding Triangular Fuzzy Number*
Very poor (VP)	(0, 1, 3)
Poor (P)	(1, 3, 5)
Fair (F)	(3, 5, 7)
Good (G)	(5, 7, 9)
Very good (VG)	(7, 9,10)

After that, the standardization process can be done by the equation (20).

$$\tilde{F}_{ij} = \left(\frac{A_{ij}}{c_j^+}, \frac{B_{ij}}{c_j^+}, \frac{c_{ij}}{c_j^+}\right), \quad C_j^+ = max\{C_{ij}, i = 1,2,3..n\} \tag{20}$$

On the other hand, author opt for the supreme of C_j^+ is equal to 1 where and j = 1, 2, . . . , n; and worst case is equal to 0. The weighted fuzzy standardized decision matrix ($S\tilde{Q}$) is calculated by the equation (21).

$$\tilde{SQ} = [s\tilde{q}_{ij}]_{m\times n} i = 1,2,..m; \; j = 1,2,3 \dots n \tag{21}$$

Where, $s\tilde{q}_{ij} = \tilde{F}_{ij} \otimes \tilde{Q}_{ij}$, thereafter, author represent the Fuzzy Positive-Ideal Solution (FPIS) and Fuzzy Negative-Ideal Solution (FNIS). Here components $s\tilde{q}_{ij}$ are standardized in positive TFN, shown by the standardized weighted fuzzy decision matrix shown in table 6. And positive TFN values lie between [0, 1].The FPIS R$^+$ (Supreme) and FNIS R$^-$ (worst) are calculated by the equation (22-23).

$$R^+ = (\tilde{q}_{1,\dots\dots}^* \tilde{q}_{j,\dots\dots}^* \tilde{q}_{n,}^*) \tag{22}$$

$$R^- = (\tilde{q}_{1,\dots\dots}^* \tilde{q}_{j,\dots\dots}^* \tilde{q}_{n,}^*) \tag{23}$$

Where,

$$\tilde{q}_1^* = (1,1,1) \otimes \tilde{Q}_{ij} = (LQ_j, MQ_j, HQ_j) \; and \; s\tilde{q}_{ij}^- = (0,0,0)$$

Through the FPIS and FNIS author evaluate the distance of every alternative. The area compensation technique is used for calculating the distances ($\tilde{D}_i^+ and \; \tilde{D}_i^-$) of each alternative from R$^+$ and R$^-$ as shown by the equation (24-25).

$$\tilde{D}_i^+ = \sum_{j=1}^n \quad D(\tilde{s}\tilde{q}_{ij}, s\tilde{q}_{ij}^*) i = 1,2,..m; \; j = 1,2,3 \dots n \tag{24}$$

$$\tilde{D}_i^- = \sum_{j=1}^n \quad D(s\tilde{q}_{ij}, s\tilde{q}_{ij}^*) i = 1,2,..m; \; j = 1,2,3 \dots n \tag{25}$$

Now, Closeness coefficients ($\widetilde{CoC}_i$) are calculated by the equation (26) in this stage, and the other option is developed to achieve the desire levels in each factor.

$$C\widetilde{oC}_i = \frac{\tilde{N}_i^-}{\mathrm{N}_i^+ + \tilde{N}_i^-} = 1 - \frac{\tilde{N}_i^+}{\tilde{N}_i^+ + N_i^-}, i = 1,2, \dots, m \tag{26}$$

V. DATA ANALYSIS AND RESULTS

Mostly, Qualitative evaluation is good for evaluating the security of web based medical image processing system. It is typical to calculate web based image processing system security quantitatively. In recent years, Healthcare industries are trying to select high security medical image processing systems or devices [16]. In addition, medical image security plays an important role during processing (capture, store, retrieve, etc.) [5][10]. This research study proposes medical image security through Fuzzy AHP- TOPSIS approach[18]. The medical image security assessment attributes have been divided and explained by the authors in the previous parts of this paper shown in figure 1. We used the equations (1-26) for calculating the web based medical images processing security assessment using Fuzzy AHP-TOPSIS approaches, as was depicted through Table 1 by using equations (1 to 9). Thereafter, we performed the fuzzification where linguistic values were converted into numerical values and made the scale for linguistic terms. These values were used to construct a pair-wise comparison matrix. Equation (10) is used to calculate the pair-wise comparison matrix as shown in table 3.

In the next step, we calculate the fuzzy weights of factors with the help of the equations (11-13) shown in table(4).

In the present scenario of security assessment, it is important to analyze the effect of medical image processing security assessment in different options as per their requisite goals and criteria. Therefore, we are using 7 different web based projects pertaining to medical image processing system for hospitals in Varanasi, UP, India. Here, A1, A2, A3, and A4 show the hospital based image processing system. The remaining A5, A6, and A7 projects are web applications based diagnostic centers. Further, Hospital based project is represented by HB and diagnostic center based project represented by DC. Because of the security of the patient's data, all these web based medical projects are very sensitive. We are using table 2 for the technical data of the seven projects as shown in table 5. We calculated regularized fuzzy decision matrix by using the equations (18-20). We calculated weighted normalized fuzzy decision matrix as presented in table 6, by using the equation (21) and we calculated the closeness coefficient aspire level presented in table 7 based on the equation (22-26).

Overall satisfaction degree of project is classified in ranks; rank is obtained in between 1 to 7 as shown in Table 7. As observed, in this case study, rank order obtained in 7 alternatives finds as DS7 > HB2 > HB4 > DC6 > HB1 > DC5 > HB3.

TABLE. III. FUZZY AHP PAIR WISE MATRIX

	F1	F2	F3	F4	F5	F6	F7	F8	F9
F1	1.0000, 1.0000, 1.0000	1.0000, 1.0000, 1.1900	0.7200, 0.9000, 1.1500	0.5500, 0.7700, 1.0000	0.7700, 1.0000, 1.1500	0.7200, 0.9000, 1.1500	0.7700, 1.0000, 1.1500	0.5500, 0.7700, 1.0000	0.4500, 0.5900, 0.8500
F2	0.8700, 1.0000, 1.0000	1.0000, 1.0000, 1.0000	0.8500, 0.9000, 1.3500	0.5500, 0.7700, 1.0000	0.7700, 1.0000, 1.1500	0.7200, 0.9000, 1.1500	0.7700, 1.0000, 1.1500	0.5500, 0.7700, 1.0000	0.4700, 0.6200, 0.9000
F3	0.9000, 1.1500, 1.5000	0.7700, 1.1500, 1.3100	1.0000, 1.0000, 1.0000	0.7200, 0.9000, 1.0000	1.0000, 1.0000, 1.1500	1.0000, 1.0000, 1.0000	1.0000, 1.0000, 1.1500	0.7200, 0.9000, 1.0000	0.5900, 0.8500, 0.9000
F4	1.0000, 1.3500, 1.8500	1.0000, 1.3500, 1.8500	1.0000, 1.1500, 1.5000	1.0000, 1.0000, 1.0000	1.0000, 1.1500, 1.6500	1.0000, 1.1500, 1.5000	1.0000, 1.1500, 1.6500	1.0000, 1.0000, 1.0000	0.8000, 1.0000, 1.0000
F5	0.9000, 1.0000, 1.3500	0.9000, 1.0000, 1.3500	0.9000, 1.0000, 1.0000	0.6200, 0.9000, 1.0000	1.0000, 1.0000, 1.0000	0.9000, 1.0000, 1.0000	1.0000, 1.0000, 1.0000	0.6200, 0.9000, 1.0000	0.5300, 0.7400, 0.9000
F6	0.9000, 1.1500, 1.5000	0.9000, 1.1500, 1.5000	1.0000, 1.0000, 1.0000	0.7200, 0.9000, 1.0000	1.0000, 1.0000, 1.1500	1.0000, 1.0000, 1.0000	0.9000, 1.0000, 1.1500	0.7200, 0.9000, 1.0000	0.5900, 0.8500, 0.9000
F7	0.9000, 1.0000, 1.3500	0.9000, 1.0000, 1.3500	0.9000, 1.0000, 1.0000	0.6200, 0.9000, 1.0000	1.0000, 1.0000, 1.0000	0.9000, 1.0000, 1.1500	1.0000, 1.0000, 1.0000	0.6200, 0.9000, 1.0000	0.5100, 0.7100, 0.8500
F8	1.0000, 1.3500, 1.8500	1.0000, 1.3500, 1.8500	1.0000, 1.1500, 1.5000	1.0000, 1.0000, 1.0000	1.0000, 1.1500, 1.6500	1.0000, 1.1500, 1.5000	1.0000, 1.1500, 1.6500	1.0000, 1.0000, 1.0000	0.8000, 1.0000, 1.0000
F9	1.3100, 1.8100, 2.3100	1.1500, 1.6500, 2.1500	1.1500, 1.3100, 1.8100	1.0000, 1.0000, 1.3100	1.1500, 1.4600, 1.9600	1.1500, 1.3100, 1.8100	1.3100, 1.6200, 2.1200	1.0000, 1.0000, 1.3100	1.0000, 1.0000, 1.0000

TABLE. IV. WEIGHTS OF FACTORS

Factors	Weights	BNP	Rank
F1	0.0700, 0.1000, 0.1400	0.0840	6
F2	0.0700, 0.1000, 0.1400	0.0810	7
F3	0.8000, 0.1100, 0.1400	0.0950	5
F4	0.0900, 0.1200, 0.1800	0.1500	2
F5	0.0700, 0.1000, 0.1400	0.0800	8
F6	0.0800, 0.1100, 0.1400	0.1100	4
F7	0.0700, 0.1000, 0.1400	0.0800	9
F8	0.0900, 0.1200, 0.1800	0.1500	3
F9	0.1000, 0.1500, 0.2200	0.1700	1

TABLE. V. Subjective Cognition Results

Alternatives/ Factors	F1	F2	F3	F4	F5	F6	F7	F8	F9
HB1	6.3800, 8.3800, 9.6900	5.0000, 7.0000, 9.0000	7.0000, 9.0000, 10.0000	7.6200, 9.3100, 10.0000	6.2400, 8.2400, 9.6200	6.2400, 8.2400, 9.6200	4.3800, 6.3800, 8.3800	5.6200, 7.6200, 9.3100	5.6200, 7.6200, 9.3100
HB2	5.0000, 7.0000, 9.0000	3.7600, 5.7600, 7.7600	4.2400, 6.2400, 8.2400	5.0000, 7.0000, 9.0000	5.6200, 7.6200, 9.3100	3.6200, 5.6200, 7.6200	4.2400, 6.2400, 8.2400	7.0000, 9.0000, 10.0000	5.6200, 7.6200, 9.3100
HB3	7.6200, 9.3100, 10.0000	5.6200, 7.6200, 9.3100	9.0000, 10.0000, 10.0000	5.6200, 7.6200, 9.3100	7.6200, 9.3100, 10.000	0.0000, 0.6200, 2.2400	5.0000, 7.0000, 9.0000	0.3100, 1.6200, 3.6200	0.6200, 2.2400, 4.2400
HB4	7.0000, 9.0000, 10.0000	5.7600, 7.7600, 9.3800	3.0000, 5.0000, 7.0000	1.7600, 3.7600, 5.7600	1.6200, 3.6200, 5.6200	3.0000, 5.0000, 7.0000	5.6200, 7.6200, 9.3100	3.0000, 5.0000, 7.0000	5.6200, 7.6200, 9.3100
DC5	3.0000, 5.0000, 7.0000	5.6200, 7.6200, 9.3100	3.0000, 5.0000, 7.0000	7.0000, 9.0000, 10.0000	6.3800, 8.3800, 9.6900	3.0000, 5.0000, 7.0000	5.0000, 7.0000, 9.0000	0.3100, 1.6200, 3.6200	3.6200, 5.6200, 7.6200
DC6	3.0000, 5.0000, 7.0000	5.0000, 7.0000, 9.0000	5.6200, 7.6200, 9.3100	6.2400, 8.2400, 9.6200	3.0000, 5.0000, 7.0000	3.0000, 5.0000, 7.0000	3.6200, 5.6200, 7.6200	7.0000, 9.0000, 10.0000	3.0000, 5.0000, 7.0000
DC7	5.0000, 7.0000, 9.0000	5.0000, 7.0000, 9.0000	3.6200, 5.6200, 7.6200	3.6200, 5.6200, 7.6200	3.7600, 5.7600, 7.7600	3.6200, 5.6200, 7.6200	7.0000, 9.0000, 10.0000	7.0000, 9.0000, 10.0000	5.7600, 7.7600, 9.3800

TABLE. VI. Weighted Standardize Fuzzy Decision

Alternative/ Factors	F1	F2	F3	F4	F5	F6	F7	F8	F9
HB1	0.00900, 0.01100, 0.01300	0.00700, 0.01000, 0.01300	0.01300, 0.01700, 0.01900	0.01200, 0.01500, 0.01600	0.00800, 0.01100, 0.01300	0.00400, 0.00600, 0.00700	0.00300, 0.00500, 0.00600	0.00500, 0.00700, 0.00800	0.00800, 0.01100, 0.01300
HB2	0.00700, 0.01000, 0.01200	0.00500, 0.00800, 0.01100	0.00800, 0.01200, 0.01500	0.00800, 0.01100, 0.01400	0.00700, 0.01000, 0.01200	0.00300, 0.00400, 0.00500	0.00300, 0.00500, 0.00600	0.00600, 0.00800, 0.00900	0.00800, 0.01100, 0.01300
HB3	0.01000, 0.01300, 0.01400	0.00800, 0.01100, 0.01400	0.01700, 0.01900, 0.01900	0.00900, 0.01200, 0.01500	0.01000, 0.01200, 0.01300	0.00000, 0.00000, 0.00200	0.00400, 0.00500, 0.00700	0.00000, 0.00100, 0.00300	0.00100, 0.00300, 0.00600
HB4	0.01000, 0.01200, 0.01400	0.00800, 0.01100, 0.01400	0.00600, 0.00900, 0.01300	0.00300, 0.00600, 0.00900	0.00200, 0.00500, 0.00700	0.00200, 0.00400, 0.00500	0.00400, 0.00600, 0.00700	0.00300, 0.00400, 0.00600	0.00800, 0.01100, 0.01300
DC5	0.00400, 0.00700, 0.01000	0.00800, 0.01100, 0.01400	0.00600, 0.00900, 0.01300	0.01100, 0.01400, 0.01600	0.00800, 0.01100, 0.01300	0.00200, 0.00400, 0.00500	0.00400, 0.00500, 0.00700	0.00000, 0.00100, 0.00300	0.00500, 0.00800, 0.01100
DC6	0.02500, 0.03900, 0.05300	0.04100, 0.05300, 0.05800	0.05200, 0.06600, 0.07400	0.03700, 0.04700, 0.05200	0.02100, 0.02900, 0.03700	0.01900, 0.02600, 0.03200	0.03500, 0.04900, 0.06300	0.02700, 0.04100, 0.05600	0.01600, 0.02400, 0.03200
DC7	0.02100, 0.03500, 0.04900	0.02900, 0.04100, 0.05300	0.04100, 0.05600, 0.06900	0.03300, 0.04300, 0.05000	0.01200, 0.02100, 0.02900	0.01000, 0.01700, 0.02400	0.02900, 0.04001, 0.05300	0.01900, 0.02900, 0.04000	0.01200, 0.01900, 0.02600

TABLE. VII. Closeness Coefficients to Aspired Level among differentalternatives

	dþi	Di	Satisfaction degree of CCi	Ranks
HB1	0.7400	29.1000	0.42300	5
HB2	0.7100	29.2000	0.52410	2
HB3	0.7200	29.3000	0.42200	7
HB4	0.7300	29.4000	0.52400	3
DC5	0.6500	29.0000	0.62220	6
DC6	0.6900	29.0012	0.62312	4
DC7	0.6600	29.1240	0.52431	1

VI. Comparison through Classical ANP-TOPSIS And FUZZY ANP-TOPSIS Method

In this paper, authors used classical AHP-TOPSIS technique and FUZZY AHP-TOPSIS for comparison[21] to verifying the accuracy of the results. In Fuzzy and classical AHP-TOPSIS, both have the same techniques to collect and assessment data[21]. No fuzzification required in classical AHP this is the main difference with Fuzzy AHP. In classical AHP-TOPSIS, data is taken in numeric form. The results difference between fuzzy and classical AHP-TOPSIS is shown in table 8. The obtained result by the classical AHP-TOPSIS method and fuzzy AHP-TOPSIS method is highly correlated. The accuracy of Fuzzy AHP TOPSIS is better than the classical AHP TOPSIS shown in results.

TABLE. VIII. Comparison the Results of Classical and FUZZY AHP-TOPSIS Methods

Alternatives	Fuzzy ANP-TOPSIS	Classical ANP-TOPSIS
HB1	0.42300	0.41100
HB2	0.52410	0.51460
HB3	0.42200	0.40950
HB4	0.52400	0.51300
DC5	0.62220	0.61320
DC6	0.62312	0.62162
DC7	0.52431	0.51832

VII. Discussion

Shocking increase in breaches of medical image has been seen by hospitals recently. In the first half of 2019 itself, 32 million health records were breached, in comparison to 15 million in the whole year of 2018. Patients' health information like date of birth, medical history, credit/debit card number and other classified details can be manipulated, corrupted and worst, sold for a high price in the market. Dismally, only 4% to 7% of revenue is invested by the healthcare industry in security. According to the Verizon Data Breach Investigation report, main source of security breaches in healthcare are insiders. The report states that 59% of the breaches in 2018 were done by insiders and 42% by external invaders. For positing an efficacious solution to this anomaly, the researchers of the present study have proposed the Fuzzy AHP-TOPSIS for security assessment. The study places an empirical evidence to suggest that affectivity of the security condition given to medical image processing system can be gauged by this methodology. The systems that are chosen for this study are being used by the hospitals and diagnostic laboratories in Varanasi. To protect the privacy of these healthcare centers, we have not enlisted their identity in this research. After collating the data from these avenues and assimilating the feedback of the practitioners about the contribution of security of medical image processing system at the time of processing, the information collected from the experts is calculated through the Fuzzy AHP- TOPSIS approach. Findings can be précised as:

- Assessment of the security of medical image will help the developers to focus on users' satisfaction.
- Through the Fuzzy AHP- TOPSIS we get the quantitative results that will support in categorizing the higher ranked factor for security assessment while developing the system.
- Development guidelines produced through this estimation will help the developers to improve their products and aid the government organizations in checking the project in the pre-market.

It is clear from this discussion that security assessment needs inventive methodologies that must be workable and accurate. Our research has worked on Fuzzy AHP- TOPSIS, yet the future challenges to reckon are:

- We have used this approach in web based medical image processing security. May be some security attributes have been missed in our empirical analysis.
- Results may be changed if the weights of inputs changed in FAHP.

VIII. Conclusion

The software industry has developed insecure system with various vulnerabilities which are non-acceptable in the medical field. This paper tests seven projects and presents a comprehensive study of security assessment of medical image processing system. The results of our tests show that most of the systems are at risks and they need to improve the security. Manually assessment of the security in medical image processing system is difficult. Proposed framework provides the quantitative assessment of security in the terms of ranking of the system. Healthcare industry does not want to invest revenue in the security. This framework will reduce the cost and time spent in the security checking. A list of criteria and Fuzzy AHP-TOPSIS methods provide rank to the system according to security check. This system provides a development guideline to improve the security at the time of software development. Thus this assessment of security will help the government and software industry to develop guidelines to make medical image processing system/tool more secure. Future challenge in our work, this technique is based on weight selection if any weight can changed by default then results can also changed.

References

[1] Jagannathan, Srinivasan&Sorini, Adam. (2015). A cybersecurity risk analysis methodology for medical devices. 1-6.

[2] Marwan, Mbarek&Kartit, Ali &Ouahmane, Hassan. (2018). A Cloud-based Framework to Secure Medical Image Processing. Journal of Mobile Multimedia. 14. 319-344.

[3] Arun, Ashish& George (2018). Healthcare Informatics and Privacy.

[4] Singh, A. & Chatterjee, K. 4ITrust: identity and trust based access control model for healthcare system security(2019) 78: 28309. https://doi.org/10.1007/s11042-019-07923.

[5] Rong, Ming &Zhi, Shuyue&Peng, Qingguo. (2016). Rayplus: A web-based platform for Medical Image Processing.

[6] Natsheh, Qamar& Li, Baihua& Gale, Alastair. (2016). Security of Multi-frame DICOM Images Using XOR Encryption Approach. Procedia Computer Science. 90. 175-181.

[7] Yinghui, Pengzhen, Dong, Menglei, &Rui (2018). A secure and privacy-Aware Smart Health system with Secret Key Leakage Resilience.

[8] Viadimir, &Marios (2019). Security and Privacy Of Medical Data: Challenges for next generation Patient-Centric Healthcare Systems.

[9] Riyaz Belgaum, Mohammad &Alansari, Zainab& Jain, Ruchin&Alshaer, Jawdat. (2018). A Framework for Evaluation of Cyber Security Challenges in Smart Cities.

[10] Bansal, Siddhant& Mehta, Garima. (2017). Comparative analysis of joint encryption and watermarking algorithms for security of biomedical images. 609-612.

[11] Wang, Zhiqiang& Ma, Pingchuan& Chi, Yaping& Zhang, Jianyi. (2018). Medical Devices are at Risk: Information Security on Diagnostic Imaging System. 2309-2311.

[12] Shanmugapriya&Kavitha (2019). Medical big data analysis: preserving security and privacy with cloud technology.

[13] Modi K.J., Kapadia N. (2019) Securing Healthcare Information over Cloud Using Hybrid Approach. In: Panigrahi C., Pujari A., Misra S., Pati B., Li KC. (eds) Progress in Advanced Computing and Intelligent Engineering. Advances in Intelligent Systems and Computing, vol 714. Springer, Singapore.

[14] Ak, MuhammetFatih&Gül, Muhammet. (2018). AHP–TOPSIS integration extended with Pythagorean fuzzy sets for information security risk analysis. Complex & Intelligent Systems.

[15] Shi, M., Jiang, R., Hu, X. et al. A privacy protection method for health care big data management based on risk access control(2019).

[16] Aqsa, & Ricardo (2018). Security aspects in healthcare information systems: A systematic mapping.

[17] Ma, Pingchuan& Wang, Zhiqiang&Hei, Xiali&Zou, Xiaoxiang& Zhang, Jianyi& Liu, Qixu&Lyu, Xin&Zhuo, Zihan. (2019). A Quantitative Approach for Medical Imaging Device Security Assessment. 5-6.

[18] A. Agrawal, M. Alenezi, R. Kumar and R. A. Khan, "Measuring the Sustainable-Security of Web Applications Through a Fuzzy-Based Integrated Approach of AHP and TOPSIS," in *IEEE Access*, vol. 7, pp. 153936-153951, 2019.

[19] Karim, Abderrahim& Hayat (2018). Big healthcare data: preserving security privacy.

[20] Chang DY. Applications of the extent analysis method on fuzzy AHP. Eur J Oper Research. 1996; 95:649–55.

[21] Moayeri, M. & Shahvarani, A. & Behzadi, M.H. & Hosseinzadeh-Lotfi, F.. (2015). Comparison of fuzzy AHP and fuzzy TOPSIS methods for math teachers selection. Indian Journal of Science and Technology. 8. 10.17485/ijst/2015/v8i13/54100.