symmetry

MDPI

Article

# Fuzzy-Based Symmetrical Multi-Criteria Decision-Making Procedure for Evaluating the Impact of Harmful Factors of Healthcare Information Security

**Rajeev Kumar [1], Abhishek Kumar Pandey [1], Abdullah Baz [2,*], Hosam Alhakami [3], Wajdi Alhakami [4], Alka Agrawal [1,*] and Raees Ahmad Khan [1]**

1 Department of Information Technology, Babasaheb Bhimrao Ambedkar University, Lucknow 226025, India; rs0414@gmail.com (R.K.); abhishekkumarpanday5@gmail.com (A.K.P.); khanraees@yahoo.com (R.A.K.)
2 Department of Computer Engineering, College of Computer and Information Systems, Umm Al-Qura University, Makkah 21421, Saudi Arabia
3 Department of Computer Science, College of Computer and Information Systems, Umm Al-Qura University, Makkah 21421, Saudi Arabia; hhhakam@uqu.edu.sa
4 Department of Information Technology, College of Computers and Information Technology, Taif University, Taif 26571, Saudi Arabia; whakami@tu.edu.sa
* Correspondence: aobaz01@uqu.edu.sa (A.B.); alka_csjmu@yahoo.co.in (A.A.); Tel.: +91-9548716538 (A.A.)

Received: 22 March 2020; Accepted: 17 April 2020; Published: 22 April 2020


**Abstract:** Growing concern about healthcare information security in the wake of alarmingly rising cyber-attacks is being given symmetrical priority by current researchers and cyber security experts. Intruders are penetrating symmetrical mechanisms of healthcare information security continuously. In the same league, the paper presents an overview on the current situation of healthcare information and presents a layered model of healthcare information management in organizations. The paper also evaluates the various factors that have a key contribution in healthcare information security breaches through a hybrid fuzzy-based symmetrical methodology of AHP-TOPSIS. Furthermore, for assessing the effect of the calculated results, the authors have tested the results on local hospital software of Varanasi. Tested results of the factors are validated through the comparison and sensitivity analysis in this study. Tabulated results of the proposed study propose a symmetrical mechanism as the most conversant technique which can be employed by the experts and researchers for preparing security guidelines and strategies.

**Keywords:** healthcare security; information security; fuzzy logic; AHP-TOPSIS; data breaches

## 1. Introduction

Malware can be aptly compared to the termites preying at the healthcare data security and rendering it hollow by tampering, corrupting or pilfering the data. Attackers are targeting the largest healthcare data repositories and organizations for accessing the sensitive data and using the data for their personal profit. As per the statistics, a malware attack is exploited due to vulnerabilities in the cyber world at least once in 39 s [1]. Information security is the most compelling issue in the current era. Healthcare is another sensitive and most targeted sector for attackers due to its high information cost on dark web [1]. Any breach in healthcare information security can have detrimental effects on both the patients' wellbeing as well as the organizations' brand image. This scenario calls for remedial measures to effectively contain and neutralize the growing threats of malwares.

A investigation from 2010 observes that the growing adaptation of digital healthcare environment is a major concern for the security experts [2]. The study also tells that assuring data security and secure availability of data in between patient, doctor and healthcare service provider is a challenging

task in electronic healthcare environment. Thus, it is evident that the issue of information security is has been a contentious issue for a long time now and many researchers are working on this from different perspectives [3,4]. But the challenges and criticalness of this issue demand a more justified solution for information security assurance in healthcare [5,6]. Buoyed by this intent, the contributors of this study have tried to provide a systematic approach for the experts to understand the types of factors that are affecting the healthcare information security and create exploitation possibilities in the healthcare sector. This type of information along with a validated scientific analysis can be very useful and significant for the research community as well as security experts [7–9].

Since the authors of this study found that there are a very few research articles that discuss and dissect the reasons behind the attacks on healthcare sector [10–12], this study has tried to highlight the possible factors that are affecting healthcare information security directly. Due to its large and complex infrastructure, the healthcare information is managed and handled at various levels in any healthcare organization. For understanding the actual implication of factors that cause malware exploitation in healthcare, it is necessary to understand the working and data production/handling in the healthcare organizations [13–15].

This paper covers the previous trends and attributes of malware attacks on the healthcare services and then tries to provide some significant factors with the help of experts' opinion that are affecting the healthcare organizations rapidly [16]. The article will also provide a scientific analysis of those factors through the hybrid approach of fuzzy AHP-TOPSIS methodology [17,18]. Fuzzy AHP-TOPSIS methodology is a pre-verified and old scientific multi criteria decision making technique that gives accurate as well as effective results in multi criteria decision situation [19–21]. This type of scientific validation gives a clear and valid path to the security experts and researchers to prepare their security strategies on the basis of calculated results of this study. Authors have used the software of a local hospital in Varanasi, Uttar Pradesh, India, to apply the proposed result and discussed their finalized result in the paper for accuracy.

The entire research article is envisaged as follows: The first section of the paper discusses the various data breach trends and statistics of previous years for providing an overview of the topic and its criticalness. Thereafter, the second section of the paper talks about the common classical healthcare layered model that discusses the various data handling layers according to their use of healthcare data. After that, the authors have described the various factors that are affecting healthcare security and aligned them with previously discussed layered models according to their high infection possibilities and provide a hierarchy. In the ensuing section, the authors have performed the numerical analysis of the hierarchy through fuzzy AHP-TOPSIS methodology and evaluated the results on a local hospital's software. The last section profiles the detailed discussion while also enlisting the limitations of the study before proffering the conclusion.

### *1.1. Past Research Initiatives*

There are not many references that the authors of this study could locate in the context of various factors of information security in healthcare. Those research studies that the authors have perused in this domain are discussed below:

E. H. Park et al. provides an overview on patients' information disclosure and discusses about the factors that are affecting the patient's information like information security awareness, medical assessment, etc., as a factor [22]. The paper provides effective results that affect the healthcare sector through its results.

S. R. Kessler et al. provided a survey on information security climate in healthcare sector. Authors categorized the professional of healthcare into four categories and conducted a survey for assessing the information security status in healthcare organizations [23]. The paper provides a path for researchers through its validated results.

J. Alipour et al. provides an exhausted review on universal information system for acceptance in healthcare organizations. The paper discusses about the factors and performs a cross-section, descriptive

analysis on it. Paper provides useful information like pointing out the weak positive correlation through the review between information security of healthcare organization and organizational factors [24]. This kind of result can provide a significant way to the future research endeavors in order to perform a review.

Md. Shirdeli et al. presents a paper discussing about the outsourcing of information security services in healthcare. The paper analyzes the healthcare information technology services through the experts' opinion and finds the factors that motivate and affect the healthcare organization to borrow the services from outsources. The paper uses an analytical hierarchy process methodology for analyzing the various factors [25].

A. McLeod et al. presents a paper that discusses the factors affecting the data breaches and models them in a constructive manner to narrow down on some significant information from them. The paper provides a good literature on various data breaches and provides a model of factors that directly or indirectly affect data breaches [26].

Apart from the studies enumerated above, we perused the work of Ward Priestman et al. which is based on classifying different factors for healthcare sector [27]. This study, in particular, became the premise of our research investigations. Our study has attempted a unique and rarely undertaken research initiative. We intend to provide a thorough evaluation of the technical factors associated with the healthcare information security. Use of Multi Criteria Decision Making (MCDM) method is significantly less in healthcare information security scenario, but the result accuracy of MCDM approach is significantly very high. For achieving the accuracy in assessment procedure, the authors of the proposed study have used a hybrid MCDM (fuzzy AHP-TOPSIS) methodology.

### *1.2. Previous Attack Trends on Healthcare*

Past data records and statistics are clearly showing that the healthcare industry is the most attractive and profitable sector for attackers. Worldwide trends are showing that healthcare data breach started rising from 2010 when the Internet revolution had started all over world. Figure 1 describes the previous healthcare scenario from 2009 to 2019 [28]. Figure clearly shows that 2015 was the most terrifying year for the healthcare industry with more than 140 million data breach records.

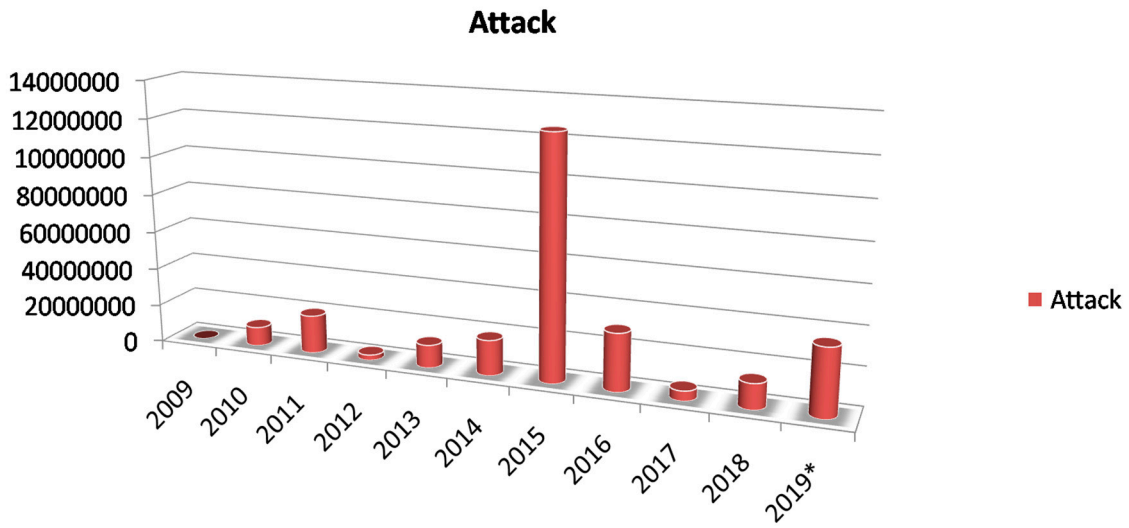



**Figure 1.** Previous data breach trend.

Another study shows that 51 big data breach incidents were reported in July 2019 worldwide. Trends of that report show that most of the incidents (count = 21) were targeted via emails in July 2019 [29]. The report also shows that 3 breaches are targeted via other platforms, 19 incidents are using network server for exploiting the healthcare industry.

Figure 2 clearly indicates that emails are targeted by most of the attackers in healthcare organizations. Phishing is the most common and widely used as well as easy and most effective approach for exploiting the system via emails. Hence, the authors assert that phishing is the new attack trend along with malware. Secondly, the network server exploitation incidents indicate that many organizations are not aware of weak and outdated security infrastructure and are currently using this kind of system and machine. The above-discussed trends of attacks and breaches in previous years are showing the criticalness and sensitivity of healthcare data security and provide a current view of the scenario.

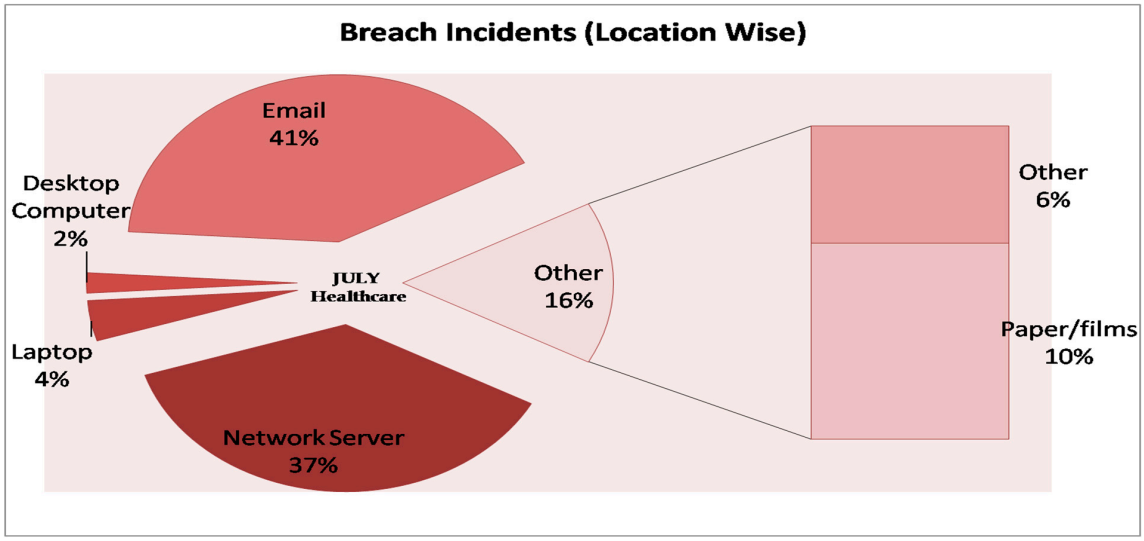



**Figure 2.** Month breach trends (location according).

The discussed findings and trends provide highly useful information like phishing being the most common approach that is used along with malware for exploiting the healthcare systems. Figure 2 describes that 84% attacks on healthcare in July month of 2019 are targeting IT infrastructure rapidly [24]. This information creates immense curiosity about finding the factors and different reasons that are creating or opening a path for attackers in healthcare services for exploitation. This situation has also motivated the contributors to evaluate the rank of the factors for providing a systematic path in order to remediate the issue or factor that is affecting the healthcare information security.

## 2. Materials and Methods

### *2.1. Classical Layered Healthcare Model: Information Perspective*

The basic and most significant objective of this paper is to provide knowledge of the factors that are affecting healthcare information security. For achieving that goal, it is important to understand the different attributes of healthcare organizations [25]. The main reason behind this is to garner a better understanding of the scenario and provide authenticated factors that are affecting different attributes in a healthcare organization [26]. Authors have categorized the healthcare organization into different layers for simple and easy understanding. Figure 3 illustrates the layered categorization of a healthcare organization in respect of information/data.

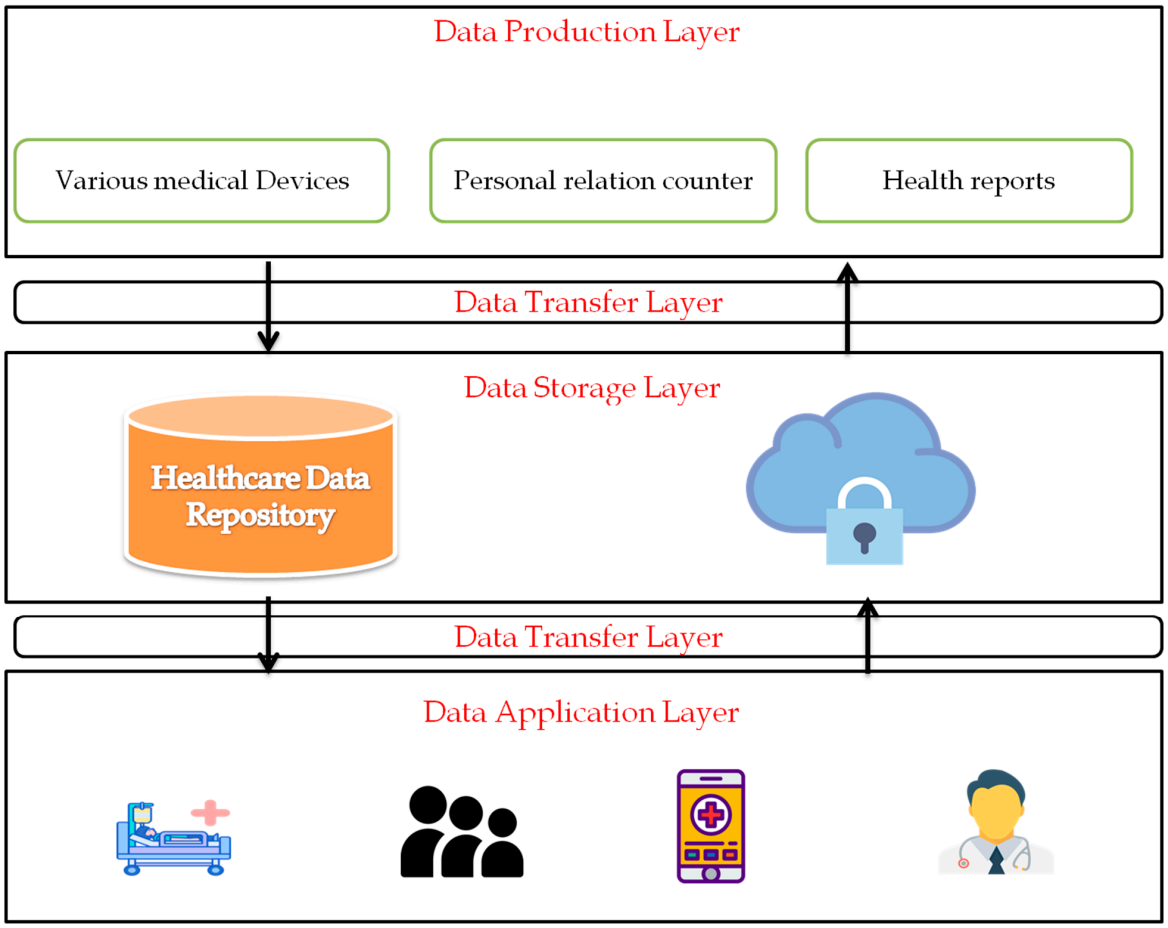



**Figure 3.** Layered structure of healthcare organization.

In the above figure, clearly describes the categorization of the healthcare organization into four different layers according to their data handling process. The first layer shows the data production layer. The second describes the data storage layer; the third layer discusses about the data Application layer; and the fourth layer illustrates the data transfer layer. The description of these different layers was elucidated in the following headings.

***Data Production Layer:*** According to the authors, this is a layer where every type of medical or health-related information is produced in a healthcare organization or service provider. This layer includes various data or information production methods and approaches that are used in different healthcare services like IoMT devices, personal relation desk information, lab report information, etc. [30]. This layer has its own various threats and factors that cause exploitation. These factors and threats are discussed in the next section of the paper. The data production layer is the first and primary entry level of any healthcare organization. Security in this layer is highly recommended and necessary for any healthcare organization.

***Data Storage Layer:*** This is a layer where all the information and data are stored by healthcare organizations according to their use in third layer. It includes various data repositories and cloud storage that are used inside the healthcare organization or outside the healthcare organization. Securing this layer needs extra efforts and sensitivity because storage and transfer layer has direct data access, i.e., if an attacker gets access to the database 1, then the possibilities are very high that he can breach the security of other databases of the organization [31]. That is the main reason why authors recommend extra security and authentication approaches in this layer.

***Data Application Layer:*** Layer three is a data application layer with various attributes like doctors, employees, patient relatives, mobile healthcare devices, etc. All these have some pieces of

information related to health of a patient or whole healthcare organization [32]. Securing this layer is as much important as the above two layers. Data application layer is also a most easily exploitable layer for attackers. The use of social engineering is effectively useful on this type of layer. Previous data breach statistics clearly shows that data application layer is the most favorite layer for attackers to exploit. This type of scenario creates an immense need for security on information application in healthcare sector.

***Data Transfer Layer:*** It is the main and significant layer in the whole healthcare structure. Many researchers and experts strongly believed that data security is hijacked or tempered mostly during data travel or data transfer. Data transfer layer holds the data during the travel period from one node to another [31,32]. It is significant and challenging to protect the information on this layer. Various types of data protection mechanisms are used for securing this layer, but previous breach ratio and explanation clearly describes that attackers are continuously exploiting the security vulnerabilities of data transfer layer.

The authors have discussed the different three layers of healthcare services from data perspective. They categorized the different attributes for analyzing the different factors that are affecting healthcare security. In the next section, the authors have discussed the various factors that are affecting the healthcare security.

### 2.2. *Various Factors: Affecting Healthcare Data Security*

Identification and categorization of the different factors that affect the healthcare data security in different ways were enumerated in this section. This was done by garnering the opinions of the experts through questionnaire generated by the research team of this study. The questionnaire was based on queries related to the healthcare information security exploitation issue. On the basis of the experts' opinion, the authors aligned every factor that is affecting a particular layer with the classical healthcare data handling model [24–27]. Figure 4 describes the different factors and their related layers.

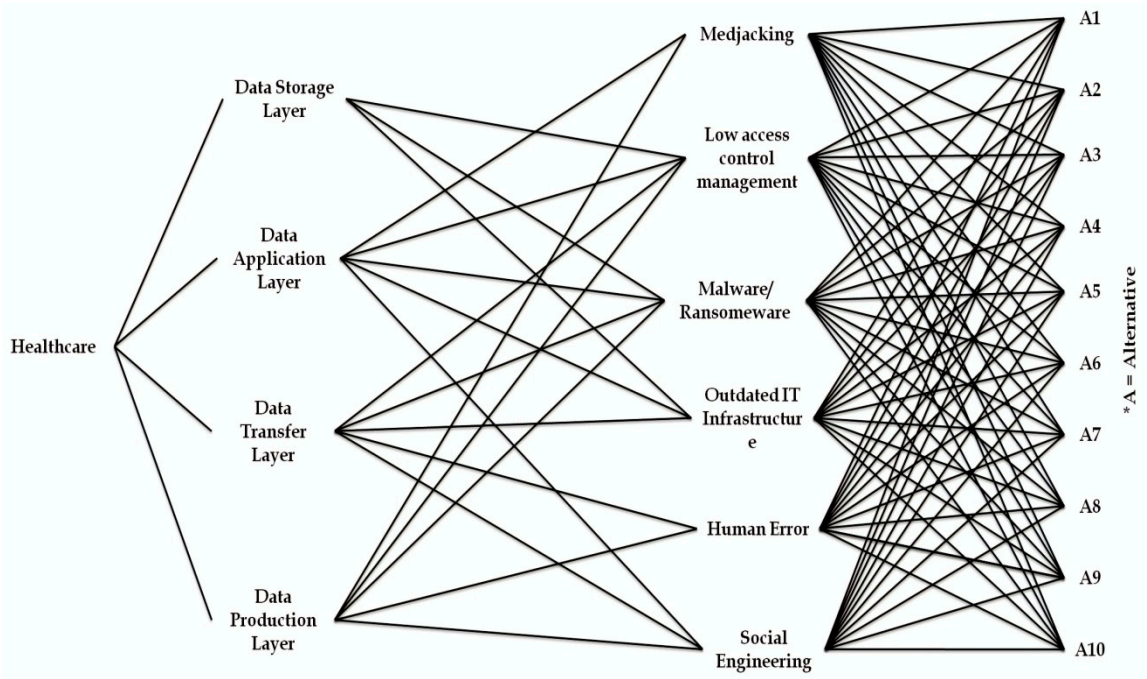



**Figure 4.** Various factors aligned with the related layer.

As we see in the above Figure 4, various factors are aligned to their relatable layers for easy and simple understanding. Figure 4 illustrates that the authors selected 10 projects of local hospital software of Varanasi as an alternative in the assessment process of the hierarchy. Varanasi is one of the oldest cities in India and revered the world over as the *city of piety*. The city is a hub of tourism that

attracts both international and domestic sightseers throughout the year. Hence, facilitating efficient, affordable and *breach-free* e-health services in such a city poses a huge challenge. This is the reason why the authors chose the local software of Varanasi hospitals as an alternative for the present study [33]. For this research, we selected 10 different projects based on the significance of the information from the various departments of the hospital. Authors choose various 10 projects of different departments of hospital. These selected 10 projects are significant and sensitive for hospital in the security perspective. Various factors that affect the healthcare information security are described below:

***Social Engineering:*** According to the classical definition of social engineering, it is a psychological or intelligence-based technique that is used to trick victims into mistakenly making security holes or extracting sensitive information from victims [27]. In the healthcare perspective social engineering is the strongest weapon against target. For example, assume that a healthcare organization employee has a habit of online betting. The attacker gets that information about employee from his behavior, environment and social media portals and in the end from a casual conversation with employee. An attacker can use this information against that particular user. An attacker can trick the employee in a phishing betting website and spot a malicious file into his computer. If the employee is using organizational system at that time, then this type of mistake can lead the whole organization into big trouble. Social engineering is the biggest threat and a grave factor that is affecting the healthcare sector through various types and ways. Authors strongly recommend a novel and strong prevention model for social engineering attacks the healthcare sector.

***Malware/Ransomware:*** In the current decade, the healthcare sector has been upgraded to smart healthcare services. All the medical procedures, as well as administrational processes are dependent on the computers and IT infrastructures [34]. As we all know, malware is the biggest enemy and threat to any IT setup. Section 2 of this paper clearly described the involvement and the harmful impact of malware in healthcare sector. Malware is the strongest weapon of intruders against healthcare system. As shown in Figure 4, malware is a threat or factor that is affecting all the layers of healthcare model in the same way. Every entity can be exploited through malware or ransomware just by one single mistake. It is important to protect the health services from malware attacks and provide a strong prevention and protection model, specifically for healthcare.

***Human Error:*** A researcher, P. Vimalachandran, shows the importance and impact of human error in the healthcare sector. The researcher provides a novel model for maintaining data integrity in healthcare services and considers human error as a serious issue in healthcare organizations [35]. A small human error or employee error can lead the patient into a life-threatening situation. For example, if a lab technician registers a wrong diabetics value like the test result is 20.33 and instead of this value he enters the value 203.3, this type of error can be fatal for the patient and lead the organization into serious trouble [34,35]. Hence, the authors of this study iterate on creating a human error-free environment in the healthcare organizations.

***Outdated IT Infrastructure:*** Technology is a process of continuous advancement and every technocrat must work towards it. In the matter of the healthcare industry, technical IT equipment is lagging behind with outdated infrastructure of IT. Every system and equipment needs upgradation for working properly and securely. But it is often seen in the context of healthcare sector that the technical infrastructure is burdened with old IT scenario [36]. This kind of gap creates a toll-free gateway for attackers to exploit the healthcare smart services. According to the authors, this issue has become even more dangerous after the introduction of the IoMT devices in the healthcare sector. If an attacker gets to succeed in breaking the IT network of any organization, then the possibility of IoT and IoMT devices getting hacked is as high as at 80%.

***Low access control management:*** The most crucial job for any healthcare organization is to restrict information access. The U.S. Department of Health and Human Services has published a report that observes that the access to personal health records should be limited and restricted at various stages in healthcare organizations [36]. It is often seen in many healthcare organizations that they usually share their centralized database with other organizations and associates instead of a small specific one. The

main reason behind this type of situation is lack of resources and time [37]. The data breach trends, and reports of the investigations cite that usually the internal staff is involved in the breach incident. Therefore, it is necessary to restrict and reconstruct access control in the healthcare organization for low rate of data breach risk and high-security percentage.

***Medjacking:*** Exploiting medical equipment and devices via backdoors and vulnerability exploit is covered under the Medjacking. Medjacking is referred for hijacking the medical devices. A report by TrapX portrays the current criticalness of medical devices and possibilities of hijacking medical accessories in the organizations. The report disclosed that the main purpose of hijacking medical devices is stealing and tampering with the confidential medical data. There is a very vast and thriving market for medical information on the dark net. Medjacking is affecting the security of medical information. Previous trends and patterns of attacks discussed in TrapX report illustrates that medjacking attacks are associated with social engineering as well as malware attacks [38]. Thus, understanding the potential cyber threat on medical devices is not only a crucial and challenging task for medical IT staff and security experts, but it also calls forth for working on preemptive mechanisms.

### *2.3. Methodology*

Evaluating the most prioritized factor that affect the healthcare information security can provide a systematic path for the security practitioners to construct a secure and systematic healthcare information security procedure [36,37]. Contributors of this study provide a numerical evaluation of factors (described in hierarchy) through the multi criteria decision making (MCDM) method. MCDM methodology has the potential and ability to give some fresh and accurate results with validation. In order to evaluate the factors, the authors of the proposed study use Analytical Hierarchy Process (AHP) for assessing the particular weights of each factor.

Fuzzy Analytical Hierarchy Process (AHP): AHP is a useful and effective methodology that is used in multi criteria decision situation. AHP uses triangular fuzzy number for evaluating the weights of factors. The result that is evaluated through AHP methodology is crisp and effective in real time situations. Saaty proposed the AHP methodology for the first time in multi criteria decision situation [39].

For this research article, the authors have used the fuzzy AHP-TOPSIS method for assessing the weights of the elements described in Figure 4. Hierarchy described in Figure 4 shows the factors that affect the healthcare information security directly. Authors have used a tree hierarchy shown in Figure 4 for applying the fuzzy AHP-TOPSIS method. This hierarchy was prepared by experts' suggestions taken through questionnaire, research study and brainstorming. After the suggestions from experts, the authors have prepared a hierarchy of elements based on the suggestions. Furthermore, for evaluating the weights, the authors convert the linguistic values of every element into a triangular fuzzy number (TFN). For making the analysis part easy, authors use the values that stand between 0 and 1 for the TFN number [40]. Furthermore, the crisp calculated values are described as 1, 2, 3 . . . 9. Additionally, the membership function of triangular fuzzy number M on F is known in Equations (1) and (2):

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

$$\mu_a(x) = \begin{cases} \frac{x}{mi-lo} - \frac{b}{mi-lo} x \in [lo,\ mi] \\ \frac{x}{mi-up} - \frac{u}{mi-up} x \in [mi, up] \\ 0 \text{ Otherwise} \end{cases} \tag{2}$$

Here, l, mi and u are showing the lower, middle and upper limit of TFN.

TFN's are represented in Figure 5 above. Further, the authors have described the scale table for ranking the factors' score for evaluating the factors that affect in a quantitative way in Table 1 [41].

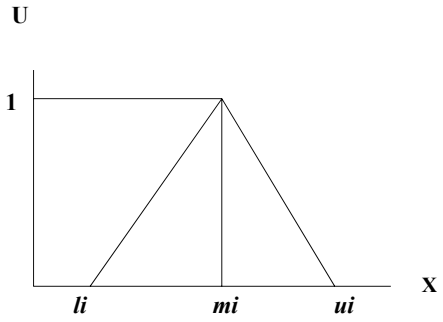



**Figure 5.** Triangular Fuzzy Number.

**Table 1.** Triangular fuzzy number scale.

| 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 | | (1, 2, 3) |
| 4 | Intermittent values between two | (3, 4, 5) |
| 6 | adjacent scales | (5, 6, 7) |
| 8 | | (7, 8, 9) |

Following Equations (3)–(6) is used for converting numeric values into triangular fuzzy numbers.

$$\eta_{ij} = (lij, miij, uij) \tag{3}$$

where lij ≤ miij ≤ uij

$$lij = (Jijd) \tag{4}$$

$$miij = (Jij1, Jij2, Jij3)1\,/ \tag{5}$$

$$and\ uij = (Jijd) \tag{6}$$

In the above conditions, *lij* is the lower worth; *mij* is the center and *uij* is the upper worth. Condition (3) shows the TFN. Conditions (7)–(9) are utilized for coordinating the diverse TFN values in the assessment procedure.

$$(l1, mi1, u1) + (l2, mi2, u2) = (l1 + l2, mi1 + mi2, u2 + u2) \tag{7}$$

$$(l1, mi1, u1) \times (l2, mi2, u2) = (l1 \times l2, mi1 \times mi2, u1 \times u2) \tag{8}$$

$$(\boldsymbol{l1}, \boldsymbol{mi1}, \boldsymbol{u1}) - \mathbf{1} = (1/u1,\ 1/\mathrm{mi}1,\ 1/l1) \tag{9}$$

Analyst now creates an *nxn* comparison matrix through Equation (10).

$$\widetilde{A^d} = \begin{bmatrix} \widetilde{k}^d_{11} & \widetilde{k}^d_{12} & \widetilde{k}^d_{1n} \\ \ldots\ldots & \ldots\ldots & \ldots\ldots \\ \widetilde{k}^d_{n1} & \widetilde{k}^d_{n2} & \widetilde{k}^d_{nn} \end{bmatrix} \tag{10}$$

If more than one preference is present in the evaluation process, then the experts use Equation (11) for calculating the average.

$$\widetilde{\mathrm{k}}_{\mathrm{ij}} = \sum\nolimits_{\mathrm{d}=1}^{\mathrm{d}} \widetilde{\mathrm{k}}_{\mathrm{ij}}^{\mathrm{d}} \tag{11}$$

In the wake of ascertaining the normal inclination in the subsequent stage of the count, the specialists update the fuzzy comparison matrix for a progressive system arranged through the experts' perspectives. For computing this progression, the specialists utilize following condition (12):

$$\widetilde{A} = \begin{bmatrix} \widetilde{k_{11}} & \cdots & \widetilde{k_{1n}} \\ \cdots & \ddots & \cdots \\ \widetilde{k_{n1}} & \cdots & \widetilde{k_{nn}} \end{bmatrix} \tag{12}$$

In the next step, the experts calculate the geometric mean and fuzzy weight of the factor through Equation (13).

$$\widetilde{P_i} = \left(\prod_{j=1}^{n} \widetilde{k_{ij}}\right)^{1/n}, \; i = 1, 2, 3, 4, \; \ldots . n \tag{13}$$

Thereafter, Equations (14)–(16) were used for concluding as well as normalizing and finding the average of the calculated fuzzy weights.

$$\widetilde{wi} = \widetilde{pi} \otimes (\widetilde{p}1 \oplus \widetilde{p}2 \oplus \widetilde{p}3 \ldots \oplus \widetilde{p}n)^{-1} \tag{14}$$

$$M_i = \frac{\widetilde{w}_1 \oplus \widetilde{w}_2 \ldots . \oplus \widetilde{w}_n}{n} \tag{15}$$

$$Nr_i = \frac{M_i}{M_1 \oplus M_2 \oplus \ldots \ldots \oplus M_n} \tag{16}$$

After all these calculations, the BNP value was evaluated through Equation (17) of COE (Center of Area method).

$$BNPwD1 = \frac{[(uw1 - lw1) + (miw1 - lw1)]}{3} + lw1 \tag{17}$$

Fuzzy TOPSIS: It calculates the factors for multi-criteria decision making in geometric arrangement of alternatives in n-dimensional space. For providing accuracy in results this TOPSIS method uses the fuzzy numbers instead of précised numbers for showing the importance of factors [42,43]. Step-by-step description of the methodology is written as follows:

In the first step of calculation, this paper used fuzzy AHP for evaluating the relevant weights through Equations (1)–(16). After that in next step, the experts prepared a comparison matrix and selected a variable with the help of Table 2 and Equation (18).

$$\widetilde{K} = \begin{bmatrix} \widetilde{x_{11}} & \cdots & \widetilde{x_{1n}} \\ \cdots & \ddots & \cdots \\ \widetilde{x_{m1}} & \cdots & \widetilde{x_{mn}} \end{bmatrix} \tag{18}$$

**Table 2.** Scale for ratings.

| Linguistic Variable | Corresponding TFN |
|---|---|
| Very Poor | (0, 1, 3) |
| Poor (P) | (1, 3, 5) |
| Fair (F) | (3, 5, 7) |
| Good (G) | (5, 7, 9) |
| Very good (VG) | (7, 9,10) |

In the following steps, the fuzzy matrix is normalized through Equation (19).

$$\widetilde{P} = \left[\widetilde{P_{ij}}\right]_{m \times n} \tag{19}$$

After a successful normalization process, a normalized fuzzy matrix is prepared through Equation (20).

$$\widetilde{Q} = \left[\widetilde{q}_{ij}\right]_{m\times n} i = 1,2,3, \ldots\ldots m; j = 1,2,3,4, \ldots\ldots n \quad (20)$$

Furthermore, in the last step the closeness gap of factors is analyzed and the alternatives for factors are evaluated. After the evaluation, the experts use Equation (21) to determine the evaluated alternatives gap of factors.

$$C\widetilde{C} = \frac{\widetilde{k_i^-}}{\widetilde{k_i^+} + \widetilde{k_i^-}} = 1 - \frac{\widetilde{k_i^+}}{\widetilde{k_i^+} + \widetilde{k_i^-}}, i = 1,2, \ldots\ldots, m \quad (21)$$

At the end of the evaluation process through the Equation (21), experts find the ranks of the factors described in hierarchy.

## 3. Data Analysis and Results

Numerically analyzing risk factors for healthcare organizations is a challenging task for experts. Identification of risk factors is the most important step in order to maintain information security in any organization [44,45]. A successful identification of risk factors can provide an accurate and effective solution of problem in any organization. To achieve this goal in the proposed paper, the authors have used a well-established and verified decision making technique, the fuzzy AHP-TOPSIS for prioritizing the identified risk factors and evaluating the impact of healthcare data security. For selecting and gathering the facts and factors, the authors of this study have taken suggestion from 70 experts who are from different industries and academic background. Equations (1)–(21) are used to assess the impact of described harmful factors in Figure 4 as follows.

For assessing the factors and finding the results, the authors have used Table 1 and Equations (1)–(9) for converting linguistic values into numeric values and TFN numbers. For constructing pair-wise comparison matrix, TFNs values are computed as:

$$\begin{aligned} \widetilde{k}_{12}^{70} &= (1,\ 1,\ 1)^{1/70} \otimes (1/4,\ 1/3,\ 1/2)^{1/70} \otimes \cdots .. \otimes (1/6,\ 1/5,\ 1/4)^{1/70} \\ &= \left((1 \times 1/4 \times \cdots .. \times 1/6)^{1/70},\ (1 \times 1/3 \times \cdots .. \times 1/5)^{1/70},\ (1 \times 1/2 \cdots .. \times 1/4)^{1/70}\right) \\ &= (0.34000,\ 0.40000,\ 0.48000) \end{aligned} \quad (22)$$

In the same manner, the pair-wise comparison matrixes of the level 1 attributes is constructed with the help of Equation (10) and shown in Table 3. Similarly, Tables 4–13 present the combined pair-wise comparison matrixes for hierarchies of level 2 and level 3.

**Table 3.** Fuzzy pair-wise comparison matrix at level 1.

| | C1 | C2 | C3 | C4 |
|---|---|---|---|---|
| C1 | 1.00000, 1.00000, 1.00000 | 0.34000, 0.40000, 0.48000 | 0.56000, 0.90000, 1.37000 | 0.39000, 0.43000, 0.47000 |
| C2 | 2.08000, 2.50000, 2.94000 | 1.00000, 1.00000, 1.00000 | 0.80000, 0.97000, 1.20000 | 0.79000, 0.88000, 1.02000 |
| C3 | 0.73000, 1.11000, 1.79000 | 0.83000, 1.03000, 1.25000 | 1.00000, 1.00000, 1.00000 | 0.50000, 0.70000, 0.93000 |
| C4 | 2.13000, 2.33000, 2.57000 | 0.98000, 1.14000, 1.27000 | 1.08000, 1.43000, 2.00000 | 1.00000, 1.00000, 1.00000 |

**Table 4.** Fuzzy Pair- wise comparison matrix for data storage layer at level 2.

| | **C11** | **C12** | **C13** |
|---|---|---|---|
| C11 | 1.00000, 1.00000, 1.00000 | 0.41000, 0.55000, 0.79000 | 0.80000, 1.24000, 1.78000 |
| C12 | 1.26000, 1.81000, 2.43000 | 1.00000, 1.00000, 1.00000 | 0.38000, 0.55000, 0.84000 |
| C13 | 0.56000, 0.80000, 1.25000 | 1.19000, 1.81000, 2.63000 | 1.00000, 1.00000, 1.00000 |

**Table 5.** Fuzzy Pair- wise comparison matrix for data application layer at level 2.

| | **C21** | **C22** | **C23** | **C24** | **C25** |
|---|---|---|---|---|---|
| C21 | 1.00000, 1.00000, 1.00000 | 0.97000, 1.25000, 1.61000 | 1.06000, 1.59000, 2.22000 | 0.77000, 1.01000, 1.29000 | 0.76000, 0.91000, 1.10000 |
| C22 | 0.62100, 0.80000, 1.03000 | 1.00000, 1.00000, 1.00000 | 0.64000, 0.91000, 1.34000 | 0.43000, 0.63000, 0.97000 | 0.35000, 0.49000, 0.87000 |
| C23 | 0.45000, 0.62800, 0.94300 | 0.74600, 1.09800, 1.56000 | 1.00000, 1.00000, 1.00000 | 0.52000, 0.66000, 0.79000 | 0.52000, 0.66000, 0.92000 |
| C24 | 0.77500, 0.99000, 0.29800 | 1.03000, 1.58000, 2.32000 | 1.26000, 1.51000, 1.92000 | 1.00000, 1.00000, 1.00000 | 0.56000, 0.65000, 0.81000 |
| C25 | 0.90000, 1.09800, 1.31000 | 1.14000, 2.04000, 2.85000 | 1.08000, 1.51000, 1.92000 | 1.23000, 1.53000, 1.78000 | 1.00000, 1.00000, 1.00000 |

**Table 6.** Fuzzy Pair- wise comparison matrix for data transfer layer at level 2.

| | **C31** | **C32** | **C33** | **C34** | **C35** |
|---|---|---|---|---|---|
| C31 | 1.00000, 1.00000, 1.00000 | 1.87000, 2.60000, 3.21000 | 1.46000, 1.68000, 1.97000 | 1.45000, 2.44000, 3.39000 | 0.48000, 0.57000, 0.79000 |
| C32 | 0.31100, 0.38000, 0.53400 | 1.00000, 1.00000, 1.00000 | 0.61000, 0.78000, 1.0300 | 0.77000, 0.95000, 1.24000 | 0.16000, 0.20000, 0.25000 |
| C33 | 0.50700, 0.59500, 0.68400 | 0.97000, 1.28000, 1.63900 | 1.00000, 1.00000, 1.00000 | 0.77000, 1.05000, 1.36000 | 0.21000, 0.2500, 0.31000 |
| C34 | 0.29400, 0.40900, 0.68900 | 0.80600, 1.05200, 1.29800 | 0.73500, 0.95200, 1.29800 | 1.00000, 1.00000, 1.00000 | 0.20000, 0.23000, 0.29000 |
| C35 | 1.26500. 1.75400, 2.08300 | 4.00000, 5.00000, 6.25000 | 3.20000, 4.00000, 4.76000 | 3.44000, 4.34000, 4.00000 | 1.00000, 1.00000, 1.00000 |

**Table 7.** Fuzzy Pair- wise comparison matrix for data production layer at level 2.

| | **C41** | **C42** | **C43** | **C44** | **C45** |
|---|---|---|---|---|---|
| C41 | 1.00000, 1.00000, 1.00000 | 1.00000, 1.52000, 1.93000 | 0.49000, 0.64000, 1.00000 | 0.42000, 0.57000, 1.00000 | 0.22000, 0.29000, 0.42000 |
| C42 | 0.51800, 0.65700, 1.00000 | 1.00000, 1.00000, 1.00000 | 0.57000, 0.67000, 0.80000 | 0.31000, 0.39000, 0.56000 | 0.27000, 0.35000, 0.52000 |
| C43 | 1.00000, 1.56000, 2.04000 | 1.25000, 1.49000, 1.75000 | 1.00000, 1.00000, 1.00000 | 1.00000, 1.32000, 1.55000 | 0.30000, 0.44000, 0.80000 |
| C44 | 1.00000, 1.75000, 2.38000 | 1.78000, 2.56000, 3.22000 | 0.64500, 0.75000, 1.00000 | 1.00000, 1.00000, 1.00000 | 0.54000, 0.91000, 1.58000 |
| C45 | 2.38000, 3.44000, 4.54000 | 1.92000, 2.85000, 3.70000 | 1.25000, 2.27000, 3.33000 | 0.632000, 1.098000, 1.85000 | 1.00000, 1.00000, 1.00000 |

**Table 8.** Global weights of second level through the hierarchy.

| The First Level | The Weight of First Level | Best Non-Fuzzy Performance Value (BNP) | The Second Level | Local Weight of Second Level | The Final Weight of the Second Level | Best Non-fuzzy Performance Value (BNP) |
|---|---|---|---|---|---|---|
| C1 | 0.14600, 0.15000, 0.19000 | 0.16200 | C11 | 0.20800, 0.21500, 0.22900 | 0.03000, 0.03200, 0.04300 | 0.03500 |
| | | | C12 | 0.30200, 0.31000, 0.32800 | 0.00500, 0.04600, 0.06200 | 0.03800 |
| | | | C13 | 0.45200, 0.46300, 0.48700 | 0.06600, 0.07000, 0.09300 | 0.07600 |
| C2 | 0.28900, 0.30000, 0.35100 | 0.31100 | C21 | 0.20200, 0.22500, 0.24000 | 0.05800, 0.06700, 0.08400 | 0.07000 |
| | | | C22 | 0.22000, 0.25100, 0.55500 | 0.06300, 0.07500, 0.19000 | 0.00900 |
| | | | C23 | 0.31100, 0.35300, 0.51400 | 0.08900, 0.09900, 0.18000 | 0.09300 |
| | | | C24 | 0.11200, 0.16900, 0.21100 | 0.03200, 0.05000, 0.07400 | 0.05200 |
| | | | C25 | 0.51000, 0.57100, 0.60400 | 0.04000, 0.07000, 0.09600 | 0.07400 |
| C3 | 0.20800, 0.22600, 0.30600 | 0.20000 | C31 | 0.23300, 0.23800, 0.26400 | 0.04800, 0.05300, 0.08000 | 0.06000 |
| | | | C32 | 0.13500, 0.14100, 0.14100 | 0.02800, 0.03100, 0.04000 | 0.03300 |
| | | | C33 | 0.12500, 0.13600, 0.17700 | 0.02600, 0.03000, 0.05400 | 0.03700 |
| | | | C34 | 0.59200, 0.60200, 0.72700 | 0.12300, 0.13600, 0.22200 | 0.15000 |
| | | | C35 | 0.43100, 0.46300, 0.45900, | 0.08900, 0.10000, 0.14000 | 0.01000 |
| C4 | 0.32400, 0.34400, 0.40700 | 0.32700 | C41 | 0.23500, 0.25500, 0.26600 | 0.07600, 0.08700, 0.10800 | 0.09000 |
| | | | C42 | 0.52800, 0.53500, 0.54800 | 0.17000, 0.18000, 0.22300 | 0.06500 |
| | | | C43 | 0.40200, 0.41400, 0.42800 | 0.13000, 0.14000, 0.17400 | 0.04800 |
| | | | C44 | 0.23200, 0.24000, 0.26900 | 0.07500, 0.08000, 0.10900 | 0.04900 |
| | | | C45 | 0.27700, 0.28400, 0.28900 | 0.05100, 0.05700, 0.06400 | 0.01100 |

**Table 9.** Dependent weights and BNP values of level 1 factor.

| S. No. | Level 1 Characteristics | Final Weights | Best Non-fuzzy Performance Value (BNP) | Ranks |
|---|---|---|---|---|
| 1 | Data Storage Layer | 0.14600, 0.15000, 0.19000 | 0.16200 | 4 |
| 2 | Data Application Layer | 0.28900, 0.30000, 0.35100 | 0.31100 | 2 |
| 3 | Data Transfer Layer | 0.20800, 0.22600, 0.30600 | 0.20000 | 3 |
| 4 | Data Production Layer | 0.32400, 0.34400, 0.40700 | 0.32700 | 1 |

**Table 10.** Dependent summarized weights and BNP values of level 2 factors.

| S. No. | Level 2 Characteristics | | Final Weights | Best Non-fuzzy Performance Value (BNP) | Ranks |
|---|---|---|---|---|---|
| 1 | Medjacking | C11+C21+C31 | 0.13600, 0.15200, 0.20700 | 0.16500 | 6 |
| 2 | Low access control management | C12+C22+C41 | 0.14400, 0.20800, 0.36000 | 0.23600 | 4 |
| 3 | Malware/Ransomware | C35+C45 | 0.14000, 0.15700, 0.20400 | 0.16700 | 5 |
| 4 | Outdated IT Infrastructure | C24+C33+C43 | 0.18800, 0.22000, 0.30200 | 0.23700 | 3 |
| 5 | Human Error | C13+C23+C32+C42 | 0.35300, 0.38000, 0.53600 | 0.42300 | 1 |
| 6 | Social Engineering | C25+C34+C44 | 0.23800, 0.28600, 0.42700 | 0.31700 | 2 |

**Table 11.** Subjective cognition results of evaluators in linguistic terms.

| | A1 | A2 | A3 | A4 | A5 | A6 | A7 | A8 | A9 | A10 |
|---|---|---|---|---|---|---|---|---|---|---|
| Medjacking | 5.36000, 7.36000, 9.00000 | 4.82000, 6.82000, 8.64000 | 3.91000, 5.91000, 7.80020 | 4.27000, 6.27000, 8.27000 | 2.45000, 4.45000, 6.45000 | 2.91000, 4.64000, 6.55000 | 1.45000, 3.00000, 4.91000 | 1.18000, 2.82000, 4.82000 | 4.82000, 6.82000, 8.55000 | 4.82000, 6.82000, 8.73000 |
| Low access control management | 4.27000, 6.27000, 8.09000 | 4.64000, 6.64000, 8.45000 | 4.64000, 6.64000, 8.36000 | 4.27000, 6.27000, 8.00000 | 2.82000, 4.82000, 6.82000 | 3.18000, 5.18000, 7.09000 | 1.45000, 3.00000, 4.91000 | 0.82000, 2.27000, 4.27000 | 5.18000, 7.18000, 8.82000 | 4.82000, 6.82000, 8.64000 |
| Malware/ Ransomware | 6.27000, 8.27000, 9.64000 | 2.64000, 4.64000, 6.64000 | 3.18000, 5.18000, 7.09000 | 5.36000, 7.36000, 9.00000 | 3.73000, 5.73000, 7.55000 | 2.45000, 4.45000, 6.45000 | 0.91000, 2.45000, 4.45000 | 2.45000, 4.27000, 6.27000 | 5.18000, 7.18000, 8.91000 | 4.82000, 6.82000, 8.55000 |
| Outdated IT Infrastructure | 4.82000, 6.82000, 8.64000 | 3.09000, 5.00000, 6.91000 | 3.18000, 5.18000, 7.09000 | 4.64000, 6.64000, 8.55000 | 3.00000, 5.00000, 7.00000 | 2.18000, 4.09000, 6.00000 | 2.82000, 4.64000, 6.64000 | 1.91000, 3.73000, 5.73000 | 5.73000, 7.73000, 9.36000 | 5.55000, 7.50500, 9.27000 |
| Human Error | 3.73000, 5.73000, 7.64000 | 3.91000, 5.91000, 7.73000 | 4.27000, 6.27000, 8.18000 | 3.00000, 5.00000, 7.00000 | 2.45000, 4.45000, 6.45000 | 3.55000, 5.55000, 7.45000 | 1.82000, 3.73000, 5.73000 | 1.64000, 3.55000, 5.55000 | 5.73000, 7.73000, 9.27000 | 4.27000, 6.27000, 8.18000 |
| Social Engineering | 4.45000, 6.45000, 8.27000 | 3.55000, 5.55000, 7.45000 | 5.00000, 7.00000, 8.73000 | 5.36000, 7.36000, 9.09000 | 2.64000, 4.64000, 6.64000 | 2.90000, 4.80000, 6.70000 | 2.82000, 4.64000, 6.64000 | 2.55000, 4.45000, 6.45000 | 5.18000, 7.18000, 9.00000 | 4.27000, 6.27000, 8.09000 |

**Table 12.** Normalized fuzzy-decision matrix.

| | A1 | A2 | A3 | A4 | A5 | A6 | A7 | A8 | A9 | A10 |
|---|---|---|---|---|---|---|---|---|---|---|
| Medjacking | 0.56000, 0.76000, 0.93000 | 0.52000, 0.74000, 0.93000 | 0.42000, 0.64000, 0.84000 | 0.45000, 0.66000, 0.88000 | 0.33000, 0.59000, 0.86000 | 0.35000, 0.56000, 0.79000 | 0.22000, 0.45000, 0.73000 | 0.18000, 0.42000, 0.72000 | 0.50000, 0.71000, 0.89000 | 0.52000, 0.74000, 0.94000 |
| Low access control management | 0.44000, 0.65000, 0.84000 | 0.50000, 0.72000, 0.91000 | 0.50000, 0.72000, 0.90000 | 0.45000, 0.66000, 0.85000 | 0.37000, 0.64000, 0.90000 | 0.38000, 0.63000, 0.86000 | 0.22000, 0.45000, 0.73000 | 0.12000, 0.34000, 0.64000 | 0.54000, 0.75000, 0.92000 | 0.52000, 0.74000, 0.93000 |
| Malware/ Ransomware | 0.65000, 0.86000, 1.00000 | 0.28000, 0.50000, 0.72000 | 0.34000, 0.56000, 0.76000 | 0.57000, 0.78000, 0.95000 | 0.49000, 0.76000, 1.00000 | 0.30000, 0.54000, 0.78000 | 0.140000, 0.36000, 0.66000 | 0.36000, 0.64000, 0.93000 | 0.54000, 0.75000, 0.92000 | 0.52000, 0.74000, 0.92000 |
| Outdated IT Infrastructure | 0.50000, 0.71000, 0.90000 | 0.33000, 0.54000, 0.75000 | 0.34000, 0.56000, 0.76000 | 0.49000, 0.70000, 0.90000 | 0.40000, 0.66000, 0.93000 | 0.26000, 0.49000, 0.73000 | 0.42000, 0.69000, 0.99000 | 0.28000, 0.55000, 0.85000 | 0.59000, 0.80000, 0.97000 | 0.60000, 0.81000, 1.00000 |
| Human Error | 0.39000, 0.59000, 0.79000 | 0.42000, 0.64000, 0.83000 | 0.46000, 0.68000, 0.88000 | 0.32000, 0.53000, 0.74000 | 0.33000, 0.59000, 0.86000 | 0.43000, 0.67000, 0.90000 | 0.27000, 0.55000, 0.80005 | 0.24000, 0.53000, 0.82000 | 0.59000, 0.80000, 0.96000 | 0.46000, 0.68000, 0.88000 |
| Social Engineering | 0.46000, 0.67000, 0.86000 | 0.38000, 0.60000, 0.80000 | 0.54000, 0.75000, 0.94000 | 0.57000, 0.78000, 0.96000 | 0.35000, 0.61000, 0.88000 | 0.35000, 0.58000, 0.81000 | 0.42000, 0.69000, 0.99000 | 0.38000, 0.66000, 0.96000 | 0.54000, 0.75000, 0.93000 | 0.46000, 0.68000, 0.87000 |

**Table 13.** Weighted normalized fuzzy-decision matrix.

| | A1 | A2 | A3 | A4 | A5 | A6 | A7 | A8 | A9 | A10 |
|---|---|---|---|---|---|---|---|---|---|---|
| Medjacking | 0.002000, 0.007000, 0.021000 | 0.002000, 0.006000, 0.021000 | 0.001000, 0.006000, 0.019000 | 0.002000, 0.006000, 0.020000 | 0.001000, 0.005000, 0.019000 | 0.001000, 0.005000, 0.018000 | 0.001000, 0.004000, 0.016000 | 0.001000, 0.004000, 0.016000 | 0.004000, 0.014000, 0.043000 | 0.004000, 0.015000, 0.046000 |
| Low access control management | 0.002000, 0.008000, 0.025000 | 0.002000, 0.008000, 0.027000 | 0.002000, 0.008000, 0.027000 | 0.002000, 0.008000, 0.025000 | 0.002000, 0.007000, 0.027000 | 0.002000, 0.007000, 0.025000 | 0.001000, 0.005000, 0.022000 | 0.001000, 0.004000, 0.019000 | 0.002000, 0.006000, 0.019000 | 0.002000, 0.006000, 0.020000 |
| Malware/ Ransomware | 0.002000, 0.008000, 0.024000 | 0.001000, 0.005000, 0.017000 | 0.001000, 0.005000, 0.018000 | 0.002000, 0.007000, 0.022000 | 0.002000, 0.007000, 0.024000 | 0.001000, 0.005000, 0.018000 | 0.000000, 0.003000, 0.016000 | 0.001000, 0.006000, 0.022000 | 0.002000, 0.007000, 0.023000 | 0.002000, 0.007000, 0.023000 |
| Outdated IT Infrastructure | 0.002000, 0.007000, 0.023000 | 0.001000, 0.006000, 0.019000 | 0.002000, 0.006000, 0.019000 | 0.002000, 0.007000, 0.023000 | 0.002000, 0.007000, 0.024000 | 0.001000, 0.005000, 0.018000 | 0.002000, 0.007000, 0.025000 | 0.001000, 0.006000, 0.022000 | 0.001000, 0.003000, 0.011000 | 0.001000, 0.004000, 0.011000 |
| Human Error | 0.003000, 0.010000, 0.032000 | 0.003000, 0.011000, 0.034000 | 0.003000, 0.011000, 0.036000 | 0.002000, 0.009000, 0.030000 | 0.002000, 0.010000, 0.035000 | 0.003000, 0.011000, 0.036000 | 0.002000, 0.009000, 0.034000 | 0.002000, 0.009000, 0.033000 | 0.004000, 0.012000, 0.040100 | 0.003000, 0.011000, 0.037000 |
| Social Engineering | 0.004000, 0.014000, 0.044000 | 0.003000, 0.012000, 0.041000 | 0.005000, 0.016000, 0.048000 | 0.005000, 0.016000, 0.049000 | 0.003000, 0.013000, 0.045000 | 0.003000, 0.012000, 0.041000 | 0.004000, 0.014000, 0.050000 | 0.003000, 0.014000, 0.049000 | 0.006000, 0.022000, 0.071000 | 0.005000, 0.020000, 0.066000 |

Through the Equations (11)–(13), authors calculate the computation of the weights as following:

$$\tilde{\mathbf{p}}_1 = [(1.00000,\ 1.00000,\ 1.00000) \otimes (0.34000,\ 0.40000,\ 0.48000) \otimes (0.56000,\ 0.90000,\ 1.37000) \otimes (0.39000,\ 0.43000,\ 0.47000)]\ 1/4$$

$$= [(1.00000 \times 0.34000 \times 0.56000 \times 0.39000)1/4,\ (1.00000 \times 0.40000 \times 0.90000 \times 0.43000)1/4, (1.00000 \times 0.48000 \times 1.37000 \times 0.47000)1/4]$$

$$= (0.07430)1/4,\ (0.15480)1/4,\ (0.30910)1/4 = (0.52200,\ 0.62700,\ 0.74560)$$

Similarly, we can obtain the remaining $\widetilde{p}_i$ as: $\widetilde{p}_2$ = (1.07700, 1.20860, 1.37730); $\widetilde{p}_3$ = (0.74180, 0.94580, 1.20100); $\widetilde{p}_4$ = (1.22530, 1.39600, 1.59840).

Equations (14)–(16) is used for the calculation of weights for each factor is written as follows:

$$\widetilde{w}_1 = (0.52200,\ 0.62700,\ 0.74560) \otimes ((0.52200,\ 0.62700,\ 0.74560) \oplus (1.0770,\ 1.20860,\ 1.37730) \oplus (0.74180,\ 0.94580,\ 1.20100) \oplus (1.22530,\ 1.39600,\ 1.59840))^{-1} = (0.14640,\ 0.15000,\ 0.19000)$$

We can also calculate the remaining $\widetilde{w}_i$ as follows: $\widetilde{w}_2$ = (0.30030, 0.28920, 0.35100); $\widetilde{w}_3$ = (0.20800, 0.22630, 0.30610); $\widetilde{w}_4$ = (0.34360, 0.33400, 0.40740). Further, through the Equation (17) authors evaluate the BNP value of factors as follows:

$$\text{BNPw1} = \frac{[(0.19000 - 0.14600) + (0.15000 - 0.14600)]}{3} + 0.14600 = 0.16200 \quad (23)$$

Global weights for each second-layer factor are calculated and represented in Table 8.

Many factors are repeated in Table 8 but the influence that they give to their higher layer factor is diverse. For better sympathetic, combination is completed to assess the weights of every level's factor. Weights of alter factors at a different level are presented in Tables 6–8 with their contribution towards healthcare information security weights. Further, Table 9 shows the final dependent weights of healthcare information security through the hierarchy.

Now, we have to determine the influence of healthcare information security in alternative choices with respect to criteria. Ten successive projects of the software of a local hospital in Varanasi were taken to estimate the healthcare information security. The alternatives *1, 2, 3 . . . 10*, represent the project of hospital services, all projects are very sensitive. With the help of Table 2 and Equations (4)–(9), we took the inputs on the technological data of the six projects as shown in Table 11. With the help of Equations (18)–(20), we evaluated the regularized fuzzy decision matrix as presented in Table 12 and with the help of Equation (21), we evaluated weighted normalized fuzzy decision matrix as shown in Table 13. With the help of Equations (22)–(26), we assessed the fuzzy satisfaction degree and fuzzy gap degree as shown in Table 14.

**Table 14.** Closeness coefficients to the aspired level among the different alternatives.

| Alternatives | | d+i | d−i | Gap Degree of CC+i | Satisfaction Degree of CC−i |
|---|---|---|---|---|---|
| Alternative 1 | A1 | 0.043845 | 0.026623 | 0.377803 | 0.622197 |
| Alternative 2 | A2 | 0.036748 | 0.036243 | 0.496541 | 0.503459 |
| Alternative 3 | A3 | 0.035237 | 0.041178 | 0.538873 | 0.461127 |
| Alternative 4 | A4 | 0.034652 | 0.027023 | 0.438152 | 0.561848 |
| Alternative 5 | A5 | 0.038358 | 0.045864 | 0.544561 | 0.455439 |
| Alternative 6 | A6 | 0.030494 | 0.046557 | 0.604236 | 0.395764 |
| Alternative 7 | A7 | 0.043845 | 0.025635 | 0.368955 | 0.631045 |
| Alternative 8 | A8 | 0.032765 | 0.042353 | 0.563820 | 0.436180 |
| Alternative 9 | A9 | 0.043845 | 0.025635 | 0.368955 | 0.631045 |
| Alternative 10 | A10 | 0.032765 | 0.042353 | 0.563820 | 0.436180 |

Table 14 and Figure 6 represents that the closeness coefficients difference of all the alternatives are acceptable. Table 14 also illustrates that the sensitivity analysis of results is already achieved through the results. Figure 5 shows the graphical representation of satisfaction degrees of alternatives.

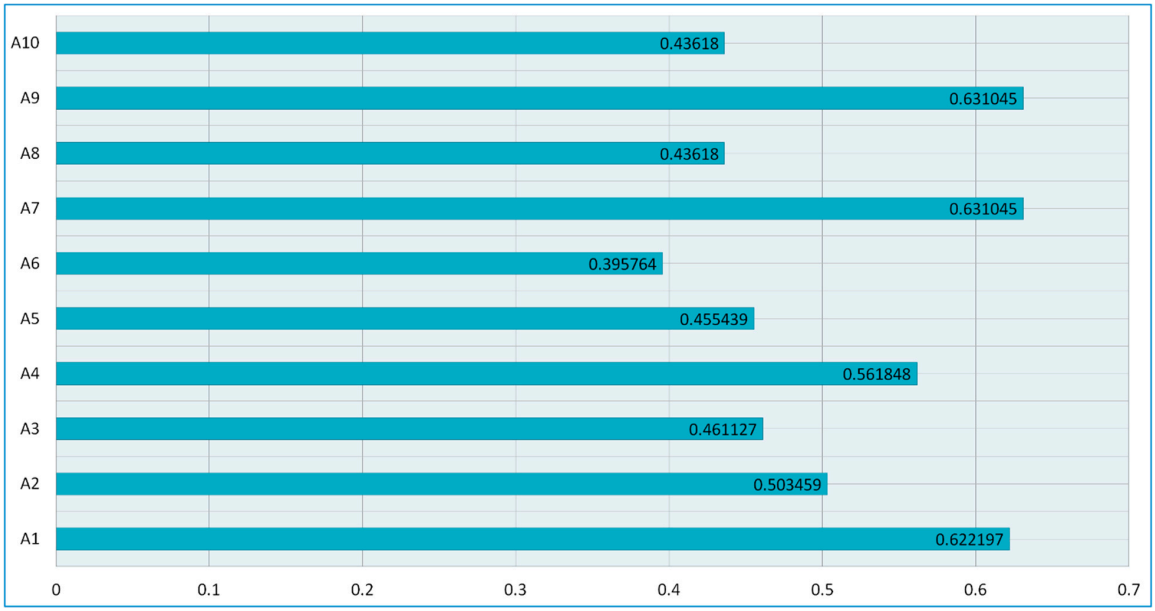



**Figure 6.** Graphical representation of satisfaction degree.

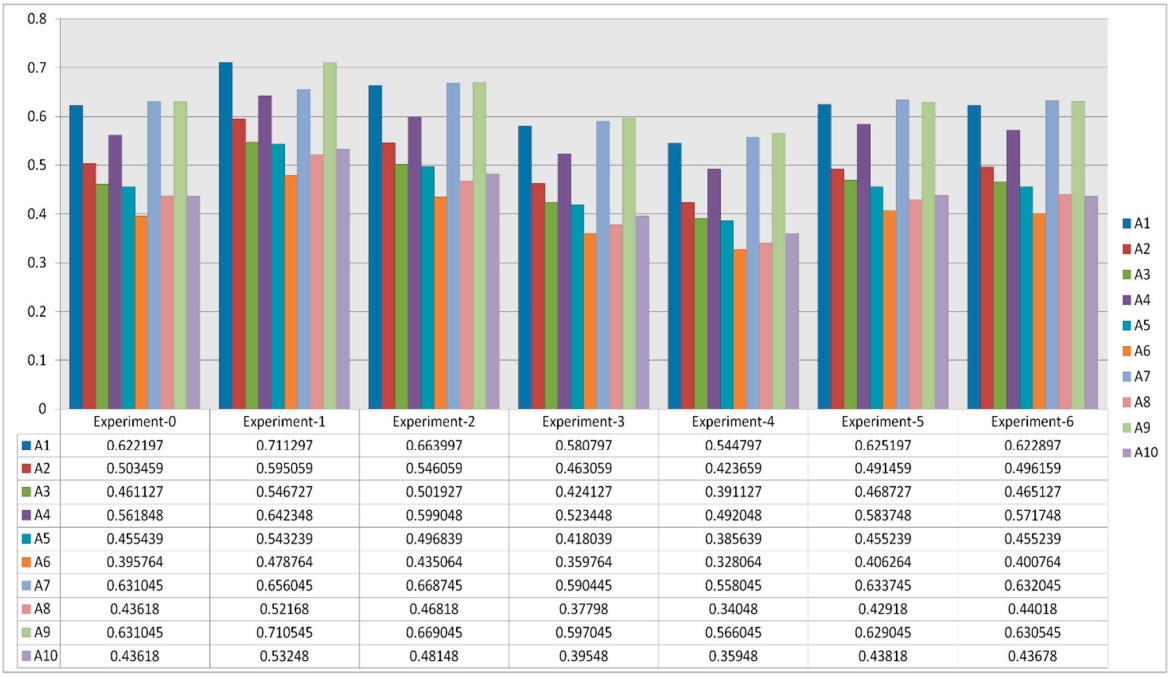
### *3.1. Sensitivity Analysis*

In any scientific paper, it is imperative to analyze the results from various perspectives. Sensitivity analysis is one of the most important and effective processes in order to motivate the accuracy and validity of results [46,47]. Sensitivity analysis provides a process for researchers to analyze their obtained results when variables are changed. The proposed study has used six experiments for sensitivity analysis because the last level of hierarchy has six factors. In order to analyze, the sensitivity weights of each factor is different at a time and the other factors weights and satisfaction degree are constant at the same time. Table 15 and Figure 7 shows the calculated results of sensitivity analysis.

From the above Table 15 and Figure 7, it is clear that alternative-9 (A9) has the highest satisfaction degree in original result. Results of sensitivity analysis also represents that A9 still has the same highest satisfaction degree in 6 experiments. The results show that alternatives are sensitive to the weights.

**Table 15.** Sensitivity Analysis.

| Experiments | Weights/ Alternatives | | A1 | A2 | A3 | A4 | A5 | A6 | A7 | A8 | A9 | A10 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Experiment-0 | Original Weights | Satisfaction Degree (CC-i) | 0.622197 | 0.503459 | 0.461127 | 0.561848 | 0.455439 | 0.395764 | 0.631045 | 0.436180 | 0.631045 | 0.436180 |
| Experiment-1 | Medjacking | | 0.711297 | 0.595059 | 0.546727 | 0.642348 | 0.543239 | 0.478764 | 0.656045 | 0.52168 | 0.710545 | 0.53248 |
| Experiment-2 | Low access control management | | 0.663997 | 0.546059 | 0.501927 | 0.599048 | 0.496839 | 0.435064 | 0.668745 | 0.46818 | 0.669045 | 0.48148 |
| Experiment-3 | Malware/ Ransomware | | 0.580797 | 0.463059 | 0.424127 | 0.523448 | 0.418039 | 0.359764 | 0.590445 | 0.37798 | 0.597045 | 0.39548 |
| Experiment-4 | Outdated IT Infrastructure | | 0.544797 | 0.423659 | 0.391127 | 0.492048 | 0.385639 | 0.328064 | 0.558045 | 0.34048 | 0.566045 | 0.35948 |
| Experiment-5 | Human Error | | 0.625197 | 0.491459 | 0.468727 | 0.583748 | 0.455239 | 0.406264 | 0.633745 | 0.42918 | 0.629045 | 0.43818 |
| Experiment-6 | Social Engineering | | 0.622897 | 0.496159 | 0.465127 | 0.571748 | 0.455239 | 0.400764 | 0.632045 | 0.44018 | 0.630545 | 0.43678 |




| | Experiment-0 | Experiment-1 | Experiment-2 | Experiment-3 | Experiment-4 | Experiment-5 | Experiment-6 |
|---|---|---|---|---|---|---|---|
| A1 | 0.622197 | 0.711297 | 0.663997 | 0.580797 | 0.544797 | 0.625197 | 0.622897 |
| A2 | 0.503459 | 0.595059 | 0.546059 | 0.463059 | 0.423659 | 0.491459 | 0.496159 |
| A3 | 0.461127 | 0.546727 | 0.501927 | 0.424127 | 0.391127 | 0.468727 | 0.465127 |
| A4 | 0.561848 | 0.642348 | 0.599048 | 0.523448 | 0.492048 | 0.583748 | 0.571748 |
| A5 | 0.455439 | 0.543239 | 0.496839 | 0.418039 | 0.385639 | 0.455239 | 0.455239 |
| A6 | 0.395764 | 0.478764 | 0.435064 | 0.359764 | 0.328064 | 0.406264 | 0.400764 |
| A7 | 0.631045 | 0.656045 | 0.668745 | 0.590445 | 0.558045 | 0.633745 | 0.632045 |
| A8 | 0.43618 | 0.52168 | 0.46818 | 0.37798 | 0.34048 | 0.42918 | 0.44018 |
| A9 | 0.631045 | 0.710545 | 0.669045 | 0.597045 | 0.566045 | 0.629045 | 0.630545 |
| A10 | 0.43618 | 0.53248 | 0.48148 | 0.39548 | 0.35948 | 0.43818 | 0.43678 |

**Figure 7.** Graphical Description of Sensitivity Analysis.

### *3.2. Comparison with the Classical AHP-TOPSIS Method*

Validating the evaluated results is the most significant job for any researcher [48]. In order to achieve validation and provide a clear view on obtained results, the contributors of this study conducted a comparison of the results with another similar technique called the classical AHP-TOPSIS. Authors used the same data for calculation through classical AHP-TOPSIS methodology. Obtained results from both the techniques are illustrated in Table 16 and Figure 8. The results described in Table 16 show that the results calculated from both techniques are highly correlated (person correlation coefficient is) [49–51]. It is clearly portrayed in Table 16 that the fuzzy-based methodology provides improved results over the classical methodology.

**Table 16.** Comparison of the results of classical and fuzzy AHP-TOPSIS methods.

| Methods/ Alternatives | A1 | A2 | A3 | A4 | A5 | A6 | A7 | A8 | A9 | A10 |
|---|---|---|---|---|---|---|---|---|---|---|
| Fuzzy-AHP-TOPSIS | 0.622197 | 0.503459 | 0.461127 | 0.561848 | 0.455439 | 0.395764 | 0.631045 | 0.436180 | 0.631045 | 0.436180 |
| Classical-AHP-TOPSIS | 0.637897 | 0.500759 | 0.473127 | 0.602848 | 0.457439 | 0.411764 | 0.640645 | 0.464680 | 0.631045 | 0.441180 |

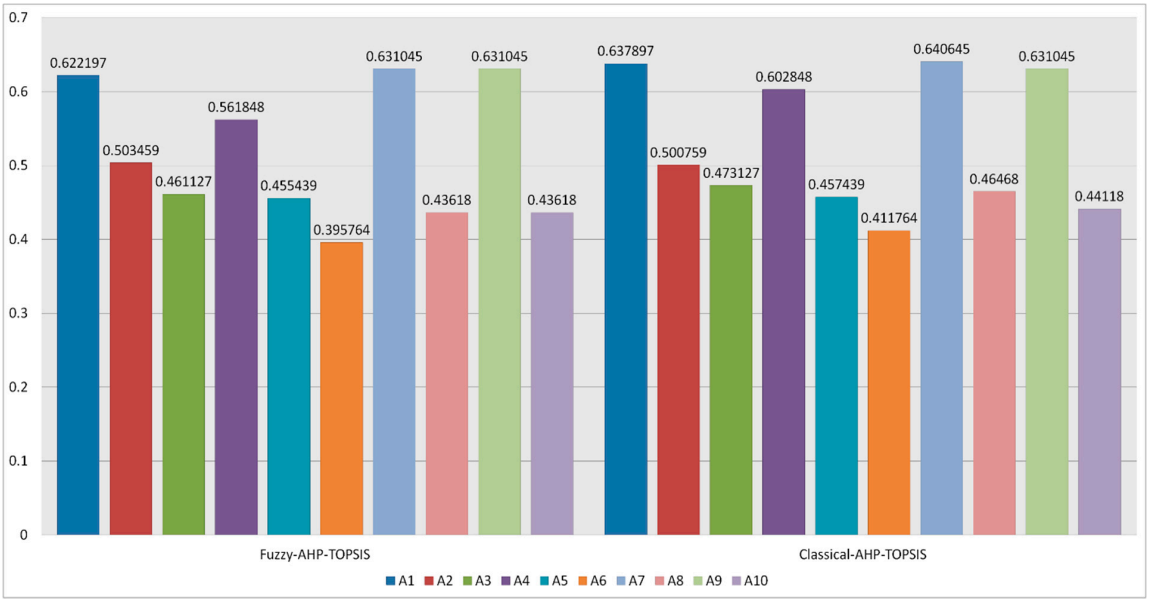



**Figure 8.** Graphical representation of comparison.

## 4. Discussion

Understanding the factors and reasons for the security backdrops and continuous data breaches are most important for better and secure environment in healthcare sector [35,36]. This paper details the various factors that are affecting the healthcare sector on different layers. Authors identified six complex and most significant factors that need to be considered in research field as well as need attention from the organizations to provide and establish better security environment. Findings are showing that every attribute of healthcare organization is under risk of exploitation and data breach.

The hierarchal structure of various layers and factors in Figure 4 describe the risk factors of healthcare organization at different layers. Factors that are discussed in this paper are internally related and depend on each other according to the results. For example, if an attacker needs to target and track an employee of healthcare organization, the attacker can employ social engineering to find sensitive information related to the employee. After this step, the attacker knows about employee's personal interests, now he creates a phishing mail containing malicious malware file for exploitation and sends to him. This type of attack contains three factors in itself. If the employee is aware of social engineering tricks, it would not be easy for the attacker to infringe upon the employer and outsource any classified information. Therefore, it is clear from the stated example that a solution of one factor can reduce the strength and risk ratio of other factors automatically.

In order to achieve this goal, the authors systematically extract and understand various data layers according to information use in healthcare organization and then analyze and classify their relevant risk factors that create the worm holes for exploitation in healthcare organizations. After identifying all these significant findings, the authors employ the universally accurate and validated fuzzy AHP-TOPSIS methodology for providing a ranking result to the constructed hierarchy in Figure 4. The analyzed result from fuzzy AHP-TOPSIS approach will help the experts to understand the process of remedying the data breach issue in healthcare by providing them a priority based systematic path. Some key findings of the proposed study are described as:

- Results of the proposed study will provide a constructive and a secure path for the experts and researchers to prepare their prevention strategies according to the evaluated result.
- Results of the proposed paper will help the experts in enhancing the current security scenario of healthcare information security by providing a scientifically evaluated priority list of affecting factors. An expert can use that result and enhance the security by preventing the factors one by one according to the results.

- The most prioritized factor is the Human Error in evaluated results, this type of evaluation attempts to draw the attention of experts and researchers on the factor and thus create future research possibilities for them.
- Contributors of this study have found six factors that affect the healthcare information security on various layers. By adopting this assessment, the future researchers can assess the web application security affecting factors and evaluate their respective weights.

However, since healthcare is a very large and complex industry in the comparison of another sector this research also has its limitations in terms of its ambit. Though a comprehensive research must cover all the technical, legal as well as administrative implications in a single manuscript, this study's focus is only on the information security scenario and its implications.

## 5. Conclusions

Data breaches and malware attacks are penetrating the healthcare industry on a large scale. Different attacking strategies pose enormous challenges for experts who are constantly working on techniques to mitigate security drawbacks. In this type of situation, healthcare sector needs a common-sense technique to tackle attack implications. The phrase "cut the problem from the root" works perfectly here, implying that if the mitigating attacks and blocking their paths are challenging and complex for experts, then instead of this, it is important to weed out the very source of the problem. In the context of healthcare, authors have discussed the factors that are playing a crucial role in exploitation and data breaches while associating them with the layers that they affect in healthcare. Thereafter, the study evaluates the ranking of factors according to their weights by hybrid MCDM approach and enlists ten projects of hospital software to assess them. Results of the proposed study will ensure that the techniques propositioned in this study would be an efficacious mechanism for the cyber security practitioners seeking solutions to make e-health data breach-proof. The analysis provides a systematic priority-based ranking result to identify which types of risk are of greater importance and first priority in terms of solutions in a healthcare organization.

**Author Contributions:** All authors contribute equally to the manuscript. All authors have read and agreed to the published version of the manuscript.

**Funding:** Deanship of Scientific Research at Umm Al-Qura University, Kingdom of Saudi Arabia.

**Acknowledgments:** The authors would like to thank the Deanship of Scientific Research at Umm Al-Qura University for supporting this work by Grant Code: 18-COM-1-01-0001.

**Conflicts of Interest:** The authors declare no conflict of interest.

## References

1. Pandey, A.K.; Tripathi, A.K.; Kapil, G.; Singh, V.; Khan, M.W.; Agrawal, A.; Kumar, R.; Khan, R.A. Trends in Malware Attacks. In *Critical Concepts, Standards, and Techniques in Cyber Forensics*; IGI Global: Hershey, PA, USA, 2020; pp. 47–60. [CrossRef]
2. Appari, A.; Johnson, M.E. Information security and privacy in healthcare: Current state of research. *Int. J. Internet Enterp. Manag.* **2010**, *6*, 279. [CrossRef]
3. Kruse, C.; Smith, B.; Vanderlinden, H.; Nealand, A. Security Techniques for the Electronic Health Records. *J. Med. Syst.* **2017**, *41*, 127. [CrossRef]
4. Slamanig, D.; Stingl, C. The Degree of Privacy in Web-based Electronic Health Records. In Proceedings of the World Congress on Medical Physics and Biomedical Engineering, Seoul, Korea, 27 August–1 Septmber 2006; Springer: Berlin/Heidelberg, Germany, 2009; Volume 22, pp. 974–977.
5. Toll, E.T.; A Alkureishi, M.; Lee, W.W.; Babbott, S.F.; A Bain, P.; Beasley, J.W.; Frankel, R.M.; A Loveys, A.; Wald, H.S.; Woods, S.S.; et al. Protecting healing relationships in the age of electronic health records: Report from an international conference. *JAMIA Open* **2019**, *2*, 282–290. [CrossRef]

6. Al-Zubaidie, M.; Zhang, Z.; Zhang, J. PAX: Using Pseudonymization and Anonymization to Protect Patients' Identities and Data in the Healthcare System. *Int. J. Environ. Res. Public Health* **2019**, *16*, 1490. [CrossRef]
7. Señor, I.C.; Fernández-Alemán, J.L.; Toval, A. Usable Privacy and Security in Personal Health Records. In *Computer Vision*; Springer: Berlin/Heidelberg, Germany, 2011; Volume 6949, pp. 36–43. [CrossRef]
8. Thigpen, B.L. Strategies to Lower Security Risks Involving Medical Devices in Patient Care. 2020. Available online: https://scholarworks.waldenu.edu/cgi/viewcontent.cgi?article=9698&context=dissertations (accessed on 15 February 2020).
9. Ronquillo, J.G.; Winterholler, J.E.; Cwikla, K.; Szymanski, R.; Levy, C. Health IT, hacking, and cybersecurity: National trends in data breaches of protected health information. *JAMIA Open* **2018**, *1*, 15–19. [CrossRef]
10. Hai, N.K.; Lawpoolsri, S.; Jittamala, P.; Huong, P.T.T.; Kaewkungwal, J. Practices in security and confidentiality of HIV/AIDS patients' information: A national survey among staff at HIV outpatient clinics in Vietnam. *PLoS ONE* **2017**, *12*, e0188160. [CrossRef]
11. Sahu, K.; Srivastava, R.K. Needs and Importance of Reliability Prediction: An Industrial Perspective. *Inf. Sci. Lett. Natural Sci. Publ.* **2020**, *9*, 33–37.
12. Peikari, H.R.; Ramayah, T.; Shah, M.H.; Lo, M.C. Patients' perception of the information security management in health centers: The role of organizational and human factors. *BMC Med. Inform. Decis. Mak.* **2018**, *18*, 102. [CrossRef]
13. Lyon, A.R.; Lewis, C.C.; Melvin, A.; Boyd, M.; Nicodimos, S.; Liu, F.F.; Jungbluth, N. Health Information Technologies—Academic and Commercial Evaluation (HIT-ACE) methodology: Description and application to clinical feedback systems. *Implement Sci.* **2015**, *11*, 128. [CrossRef]
14. Sahu, K.; Srivastava, R.K. Revisiting Software Reliability. In *Advances in Intelligent Systems and Computing*; Springer: Berlin/Heidelberg, Germany, 2018; pp. 221–235. [CrossRef]
15. Yeratziotis, A.; Pottas, D.; Van Greunen, D. A Usable Security Heuristic Evaluation for the Online Health Social Networking Paradigm. *Int. J. Hum.-Comput. Interact.* **2012**, *28*, 678–694. [CrossRef]
16. Sahu, K.; Rajshree, P.; Kumar, R. Risk management perspective in SDLC. *Int. J. Adv. Res. Comput. Sci. Softw. Eng.* **2014**, *4*, 1247–1251.
17. Kumar, R.; Khan, A.I.; Abushark, Y.B.; Alam, M.; Agrawal, A.; Khan, R.A. A Knowledge-Based Integrated System of Hesitant Fuzzy Set, AHP and TOPSIS for Evaluating Security-Durability of Web Applications. *IEEE Access* **2020**, *8*, 48870–48885. [CrossRef]
18. Kumar, R.; Khan, A.I.; Abushark, Y.B.; Alam, M.; Agrawal, A.; Khan, R.A. An Integrated Approach of Fuzzy Logic, AHP and TOPSIS for Estimating Usable-Security of Web Applications. *IEEE Access* **2020**, *8*, 50944–50957. [CrossRef]
19. Teles, S.; Napolskij, M.S.; Paúl, C.; Ferreira, A.; Seeher, K. Training and support for caregivers of people with dementia: The process of culturally adapting the World Health Organization iSupportprogramme to Portugal. Dementia. *Dementia* **2020**. [CrossRef]
20. Kumar, R.; Zarour, M.; Alenezi, M.; Agrawal, A.; Khan, R.A. Measuring Security Durability of Software through Fuzzy-Based Decision-Making Process. *Int. J. Comput. Intell. Syst.* **2019**, *12*, 627–642. [CrossRef]
21. Peng, P. A Measurement Approach to Understanding the Data Flow of Phishing from Attacker and Defender Perspectives (Doctoral Dissertation, Virginia Tech). 2019. Available online: https://vtechworks.lib.vt.edu/bitstream/handle/10919/96401/Peng_P_T_2020.pdf?sequence=1&isAllowed=y (accessed on 22 March 2020).
22. Park, E.H.; Kim, J.; Wiles, L.L.; Park, Y.S.; Wile, L.L. Factors affecting intention to disclose patients' health information. *Comput. Secur.* **2019**, *87*, 101340. [CrossRef]
23. Kessler, S.R.; Pindek, S.; Kleinman, G.; A Andel, S.; Spector, P.E. Information security climate and the assessment of information security risk among healthcare employees. *Heal. Inform. J.* **2019**. [CrossRef]
24. Alipour, J.; Mehdipour, Y.; Karimi, A. Factors Affecting Acceptance of Hospital Information Systems in Public Hospitals of Zahedan University of Medical Sciences: A Cross-Sectional Study. *J. Med. Life* **2020**, *12*, 403–410.
25. Shirdeli, M.; Zare, S.; Kharazmi, E.; Rezaee, R.; Maher, M.H. Presenting a Model to Evaluate Factors Affecting Outsourcing of Health Information Technology Services. *Acta Inform. Medica* **2018**, *26*, 190–194. [CrossRef]
26. McLeod, A.; Dolezel, D. Cyber-analytics: Modeling factors associated with healthcare data breaches. *Decis. Support Syst.* **2018**, *108*, 57–68. [CrossRef]
27. Priestman, W.; Anstis, T.; Sebire, I.G.; Sridharan, S.; Sebire, N.J. Phishing in healthcare organisations: Threats, mitigation and approaches. *BMJ Health Care Inform.* **2019**, *26*. [CrossRef] [PubMed]

28. Healthcare Data Breach Statistics. Available online: https://www.hipaajournal.com/healthcare-data-breach-statistics/ (accessed on 11 January 2020).
29. Healthcare Data Breach Report. 2019. Available online: https://www.hipaajournal.com/july-2019-healthcare-data-breach-report/ (accessed on 11 January 2020).
30. Palanisamy, V.; Thirunavukarasu, R. Implications of big data analytics in developing healthcare frameworks—A review. *J. King Saud Univ.-Comput. Inf. Sci.* **2017**, *31*, 415–425. [CrossRef]
31. El Aboudi, N.; Benhlima, L. Big Data Management for Healthcare Systems: Architecture, Requirements, and Implementation. *Adv. Bioinform.* **2018**, *2018*, 1–10. [CrossRef] [PubMed]
32. Clarke, J.; Bourn, S.; Skoufalos, A.; Beck, E.H.; Castillo, D.J. An Innovative Approach to Health Care Delivery for Patients with Chronic Conditions. *Popul. Health Manag.* **2016**, *20*, 23–30. [CrossRef]
33. University Repositorty. 2019. Available online: http://www.bbau.ac.in/new/index.aspx (accessed on 1 March 2020).
34. Dang, L.M.; Piran, J.; Han, D.; Min, K.; Moon, H. A Survey on Internet of Things and Cloud Computing for Healthcare. *Electronics* **2019**, *8*, 768. [CrossRef]
35. Vimalachandran, P.; Wang, H.; Zhang, Y.; Heyward, B.; Zhao, Y. Preserving patient-centered controls in electronic health record systems: A reliance-based model implication. In Proceedings of the 2017 International Conference on Orange Technologies (ICOT), Singapore, 8–10 December 2017. Available online: https://arxiv.org/ftp/arxiv/papers/1802/1802.00575.pdf (accessed on 11 January 2020).
36. Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients; Department of Health and Human Services: USA. 2018. Available online: https://www.phe.gov/Preparedness/planning/405d/Pages/hic-practices.aspx (accessed on 1 March 2020).
37. Pandey, A.K.; Khan, A.I.; Abushark, Y.B.; Alam, M.; Agrawal, A.; Kumar, R.; Khan, R.A. Key Issues in Healthcare Data Integrity: Analysis and Recommendations. *IEEE Access* **2020**, *8*, 40612–40628. [CrossRef]
38. MEDJACK. Medical Device Hijacking; TrapX Research Lab. 2018. Available online: https://www.trustdimension.com/wp-content/uploads/2015/02/MedJack.4-ilovepdf-compressed.pdf (accessed on 1 March 2020).
39. Saaty, T.L. How to make a decision: The analytic hierarchy process. *Eur. J. Oper. Res.* **1990**, *48*, 9–26. [CrossRef]
40. Saaty, T.L. Transport planning with multiple criteria: The analytic hierarchy process applications and progress review. *J. Adv. Transp.* **1995**, *29*, 81–126. [CrossRef]
41. Hahn, W.J.; Seaman, S.L.; Bikel, R. Making decisions with multiple attributes: A case in sustainability planning. *Graziadio Bus. Rev.* **2012**, *15*, 365–381.
42. Zavadskas, E.K.; Govindan, K.; Antuchevičiene, J.; Turskis, Z. Hybrid multiple criteria decision-making methods: A review of applications for sustainability issues. *Econ. Res.-Ekon. Istraživanja* **2016**, *29*, 857–887. [CrossRef]
43. Syamsuddin, I. Multicriteria Evaluation and Sensitivity Analysis on Information Security. *Int. J. Comput. Appl.* **2013**, *69*, 22–25. [CrossRef]
44. Mi, X.; Wu, X.; Tang, M.; Liao, H.; Al-Barakati, A.; Altalhi, A.H.; Herrera, F. Hesitant Fuzzy Linguistic Analytic Hierarchical Process with Prioritization, Consistency Checking, and Inconsistency Repairing. *IEEE Access* **2019**, *7*, 44135–44149. [CrossRef]
45. Srivastava, P.R.; Singh, A.P.; Vageesh, V.K. Assessment of Software Quality: A Fuzzy Multi-Criteria Approach. In *Evolutionary Computation and Optimization Algorithms in Software Engineering*; IGI Global: Hershey, PA, USA, 2010; pp. 200–219. [CrossRef]
46. How to Build a Sustainable Cyber Security Plan. 2019. Available online: https://www.cigniti.com/blog/sustainable-cybersecurity-strategy-plan/ (accessed on 7 February 2020).
47. Mikhailov, L. Deriving priorities from fuzzy pairwise comparison judgements. *Fuzzy Sets Syst.* **2003**, *134*, 365–385. [CrossRef]
48. Dymova, L.; Sevastjanov, P.; Tikhonenko, A. An interval type-2 fuzzy extension of the TOPSIS method using alpha cuts. *Knowl.-Based Syst.* **2015**, *83*, 116–127. [CrossRef]
49. Pearson Product-Moment Correlation. 2017. Available online: https://statistics.laerd.com/statistical-guides/pearson-correlation-coefficient-statistical-guide.php (accessed on 1 March 2020).

50. Agrawal, A.; Seh, A.H.; Baz, A.; Alhakami, H.; Alhakami, W.; Baz, M.; Kumar, R.; Khan, R.A. Software Security Estimation Using the Hybrid Fuzzy ANP-TOPSIS Approach: Design Tactics Perspective. *Symmetry* **2020**, *12*, 598. [CrossRef]
51. Kumar, R.; Baz, A.; Alhakami, H.; Alhakami, W.; Baz, M.; Agrawal, A.; Khan, R.A. A Hybrid Model of Hesitant Fuzzy Decision- Making Analysis for Estimating Usable- Security of Software. *IEEE Access (Early Access)* **2020**, *8*. [CrossRef]