Computers, Materials & Continua
DOI:10.32604/cmc.2022.020146
Article

Tech Science Press

Hesitant Fuzzy-Sets Based Decision-Making Model for Security Risk Assessment

Ahmed S. Alfakeeh[1], Abdulmohsen Almalawi[2], Fawaz Jaber Alsolami[2], Yoosef B. Abushark[2], Asif Irshad Khan[2,*], Adel Aboud S. Bahaddad[1], Alka Agrawal[3], Rajeev Kumar[4] and Raees Ahmad Khan[3]

[1]Department of Information Systems, Faculty of Computing and Information Technology, King Abdulaziz University, Jeddah, 21589, Saudi Arabia
[2]Department of Computer Science, Faculty of Computing and Information Technology, King Abdulaziz University, Jeddah, 21589, Saudi Arabia
[3]Department of Information Technology, Babasaheb Bhimrao Ambedkar University, Lucknow, 226025, Uttar Pradesh, India
[4]Department of Computer Applications, Shri Ramswaroop Memorial University, Lucknow-Deva Road, Barabanki, 225003, Uttar Pradesh, India
[*]Corresponding Author: Asif Irshad Khan. Email: aikhan@kau.edu.sa
Received: 10 May 2021; Accepted: 11 June 2021

Abstract: Security is an important component in the process of developing healthcare web applications. We need to ensure security maintenance; therefore the analysis of healthcare web application's security risk is of utmost importance. Properties must be considered to minimise the security risk. Additionally, security risk management activities are revised, prepared, implemented, tracked, and regularly set up efficiently to design the security of healthcare web applications. Managing the security risk of a healthcare web application must be considered as the key component. Security is, in specific, seen as an add-on during the development process of healthcare web applications, but not as the key problem. Researchers must ensure that security is taken into account right from the earlier developmental stages of the healthcare web application. In this row, the authors of this study have used the hesitant fuzzy-based AHP-TOPSIS technique to estimate the risks of various healthcare web applications for improving security-durability. This approach would help to design and incorporate security features in healthcare web applications that would be able to battle threats on their own, and not depend solely on the external security of healthcare web applications. Furthermore, in terms of healthcare web application's security-durability, the security risk variable is measured, and vice versa. Hence, the findings of our study will also be useful in improving the durability of several web applications in healthcare.

Keywords: Web applications; security risk; security durability; hesitant-based decision-making approach

1 Introduction

The web application development team faces many challenges in improving the functionality of healthcare web application security. Moreover, tech businesses are also looking for a viable method for enhancing the security of healthcare web applications. To effectively contain the various security threats, especially for the healthcare web applications, the practitioners keep changing their strategies to manage the security of the web applications in use. . However, risk is a threat that has particular objectives and can interrupt well-defined methods [1–3]. The procedures that are used to manage and minimise the security risk protect the healthcare web application and also help in maximizing the efficacy as well as the functionality of the application. In this context, the Risk management technology helps in risk reduction practices in the healthcare web application development process [4,5]. This technology includes security monitoring, mitigating, and maintaining which are interconnected procedures, integrated into the security design during the healthcare web application development process.

Major research work has been carried out for managing security risk [6,7]. For implementing effective security risk management procedures, it is important to handle a variety of security risks during the healthcare web application's development process. To achieve better results, all processes must be modified. To identify and minimize risks for strategic risk management, the entire healthcare web application life cycle is used. In line with the policy and oversight included in the assessment of healthcare web application security, risk management mechanisms have varying prominence; for example, they are not the results of criteria such as costs and schedules but are important components of security risk management.

This point of view has not been taken into account in the past, but it is necessary today to use the concept of integrated security. A simpler and added modernized security performance monitoring approach is risk recognition and security management systems [8,9]. Combined risk management processes use strategies and practical approaches for enhancing the security performance. In this row, the practitioners have made efforts to address and analyse different methodologies of healthcare web application security. Such an analysis helps in identifying the existing research gaps in the quest to design more secure-durable healthcare web applications.

Notably, '*compromise in designing*' has originated as one of the topmost severe security threats in several cases. It has been observed that the practitioners tend to speed up the design process to reduce "time-to-market". This means that security is not designed into a healthcare web application but remains a mere external addition, thus weakening the security. The security risk can be well-defined as the potential for failure or harm if a threat compromises susceptibility. The development team usually relies on risk management expertise and skills without sufficient risk management frameworks.

Security must be the core focus of the designers while developing the healthcare web applications. In this row, as cited by Rodriguez et al. [10], three foundations of a secure healthcare web applications that need to be prioritised are: managing security risk framework, information, and touch points. Therefore, if one wishes to enhance healthcare web application's security, management procedures of security risk are one of the key issues to focus upon.

With previous methods, characteristics quantification is very difficult during the security risk management process. Sahu et al. [11] have indicated that to evaluate the real security of any healthcare web application, adequate assessment, which is itself a very complex procedure, is essential. Kaur et al. [12] have divided the fuzzy methods into two significant forms during security risk assessment: conceptual and traditional methods concerning fuzzy sets. For managing the

security risk of the healthcare web application, many multi-criteria decision-making methods are generally addressed by practitioners because the security management process is a decision-making problem [13,14].

By using hesitant fuzzy sets, this article evaluated the healthcare web application security risks at the design phase. Schiefer [15] has employed fuzzy sets in the security risk management process. Kumar et al. [16] used the hierarchical analysis representation method of security risk to construct an empirical security risk assessment procedure. The term hesitant fuzzy has been used by some researchers to describe the procedure of ambiguity and analytical hierarchy process to determine the importance of different characteristics during healthcare web application development [17]. The security techniques, including hierarchical characterization and acceptance, were also investigated by some other researchers [8,12]. Nevertheless, with the aid of the hesitant fuzzy-based AHP-TOPSIS technique, the authors of the current research work have not found any study that emphasizes upon assessing the impact of security risk to enhance the security of healthcare web applications. That is why our research work assessed the impact of several security risk characteristics at the design phase through the hesitant fuzzy-based AHP-TOPSIS technique.

The remainder of this research work is structured as follows: The paper outlines the identification and evaluation of security risk of healthcare web applications in Section 2. Section 3 addresses the hesitant fuzzy-based AHP-TOPSIS technique and the effect of healthcare web application security risks has been assessed. Section 4 concludes this study.

2 Risk Scenario of Healthcare Web Application

The digitalization of the healthcare industry has created a huge platform for attackers who can attain valuable information from many sources and blackmail or sell this information to the buyers. In the context of the proposed paper on the durability and management of security in healthcare web applications, it is very significant to introduce the basic risks plots and situation of attacks in the healthcare domain for a better overview of a topic. A thorough understanding of the current attack trends would help in identifying effective solutions. The authors observed that the attack ratio of penetrators and hacking incidents in a healthcare organizations increased by 25% in 2020. 29 million medical records were breached in 2020 alone. Another study on attack source classification for healthcare organizations discloses that a total of 642 data breach incidents were reported in 2020 and 66.82% of breaches [18] were specifically caused by hacking and vulnerability exploitation in web platforms. A descriptive representation of incidents and their sources is discussed in the following Fig. 1.

The above statistics portray that *vulnerability exploitation* is the major cause of breach incidents and issues in the healthcare organizations. This graphical representation of 2020 statistics portrays an immense need for a standardized mechanism or procedure for managing security in digital platforms of healthcare. Moreover, a report on cyber security concerns for healthcare industry discusses that approximately $125 billion are going to be spent on security services and hardware by 2025 [19]. This huge investment prediction shows the market concerns and security issues in the healthcare domain. Thus, the demand and the need for managing the security for functionality of digital platforms cannot be overstated. This can be done more corroboratively from the design phase itself. Addressing this possibility, the proposed article works on a simplified and feasible procedure which can be adapted by the researchers aiming at enhancing the security-durability of the web applications; the same has been discussed in following headings.

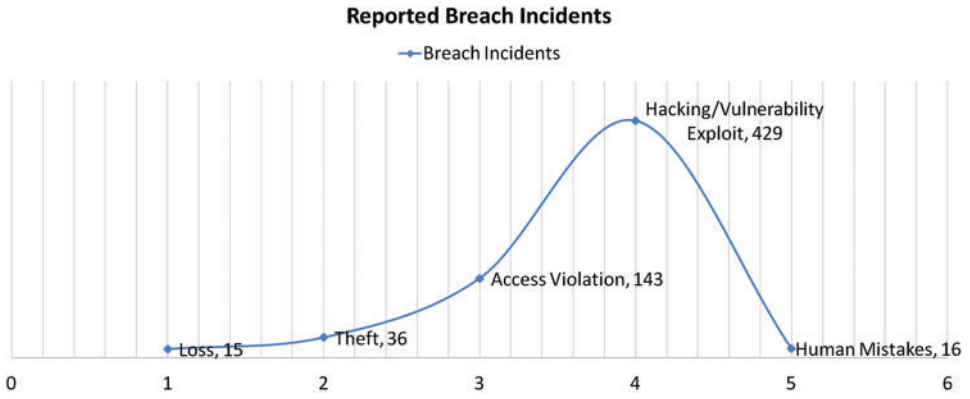

Figure 1: Healthcare reported breach incidents statistics along with their source

3 Healthcare Web Application Security Risks at Design Phase

The security designer is not inherently the best person to perform security risk estimation, because risk management itself requires technical expertise. Thorough risk estimation relies on awareness of financial impacts, including knowledge of laws, regulations, and the business model sustained by a healthcare web application. The practitioners develop certain assumptions about their systems' risks and the security experts help to test those assumptions at a reasonable level. However, all the effective techniques of security risk analysis have different advantages and disadvantages. Inspite of their best efforts, the practitioners are often unable to address the constraints that arise due to any technique, thus compromising the security of the web application and also hampering its functionality. In this context, it is important to relate traditional security risk principles to the healthcare web application design. This would help in mapping clear mitigation requirements that separate a noteworthy risk assessment from a mere average assessment process of a healthcare web application. A high-level tactic to adaptive security risk analysis will be fully combined into the development process of healthcare web applications [4]. Risk management of information security has become a vital activity. Security engineering has become important for everybody from initial education to fundamental engineering to progress into the twenty-first century. Since threats are everywhere, the healthcare web application must be extremely secure due to huge investments and users' reliance on the development process of healthcare web applications [11].

The developers of the healthcare web application should be well aware of the core of the security threats because the vulnerabilities and threats can have a momentous impact on time and costs entailed in the development process. Security threat recognition and their causes during the healthcare web application development process can also assist the practitioners in taking preliminary steps to counter these threats. It has been stated that the assessment of security risks by machine computing can considerably enhance the life span of the security of the healthcare web application. For a more effective and accurate procedure, our study identifies the key security threats that the designers must focus on and calculates the effect of these by using the hesitant fuzzy-based AHP-TOPSIS approach. The critical security risks that have been selected in this research work are based on the associated security characteristics. It has become a prerequisite for a secure healthcare web application development process to address security characteristics including access control, confidentiality, authentication, honesty, etc. Particularly, nowadays, when the users are mainly worried about the security of their data, the developers'

primary responsibility is to address this effectively. In this research study, therefore, the authors have filtered the healthcare web application security risks that may penetrate from the Common Vulnerabilities Enumeration (CWE) list into the program at the design stage [4,6]. CWE is a group that promotes the development of secure healthcare web applications by providing a list of all potential vulnerabilities in any web application. By offering a standard for detection and mitigation of different healthcare web application vulnerabilities, it acts as a security tool. As defined by the researchers, the key design-level security risks have been demonstrated in Tab. 1. Fig. 2 shows the security risks at the design phase. Further, Fig. 3 shows the relationship between security threats and security characteristics along with the concept of security risk.

Table 1: Security risks and related security characteristic

S. No.	Security risks	Description	Related security characteristic
1.	Access to critical private variable via public method	A public technique for analysis or modifying a private variable is specified by the healthcare web application [12].	Access control; Integrity
2.	Password in configuration file (PCF)	In the settings tab, a hidden password is maintained, so an attacker is vulnerable to misuse [13].	Authentication; Access control
3.	Critical variable declared public (CVDP)	Any sensitive variable/area is made available to the public when the security policy enables it to be personal [14].	Confidentiality; Integrity
4.	Unverified password change (UPC)	There is no authentication protocol until you establish a new user password [15].	Authentication; Access control
5.	Race condition within a thread (RCT)	If any resources are used simultaneously, the resources could be used while the state of the process is null and therefore undefined [16].	Integrity
6.	Untrusted search path (USP)	An externally specified search path may be used for critical resources that may lead to resources that are not directly handled by the healthcare web application [17].	Confidentiality; Integrity; Availability; Access control
7.	The download of code without integrity check (DCIC)	The executable healthcare web application program can be retrieved from any distant location without verifying the program's source and validity [5].	Integrity; Confidentiality
8.	Concurrent execution using shared resource with improper synchronization ('Race condition') [9] (RC)	A healthcare web application sequencing that may overlap with other code is included in the program and the code sequence wants instant, special access to the shared resource; though, there is a period where the shared resource may be modified with another code sequence of similarity [6].	Integrity; Confidentiality
9.	External initialization of trusted variables or data stores [10] (EITV)	To preprocess vital internal variables or database servers, the program uses inputs that can be altered by questionable actors [10].	Integrity
10.	Improperly controlled modification of dynamically determined object attributes [11]	When the object includes only internal features, vulnerability may be caused by its unintended modification [11].	Integrity

Figure 2: Healthcare web application security risks at the design phase

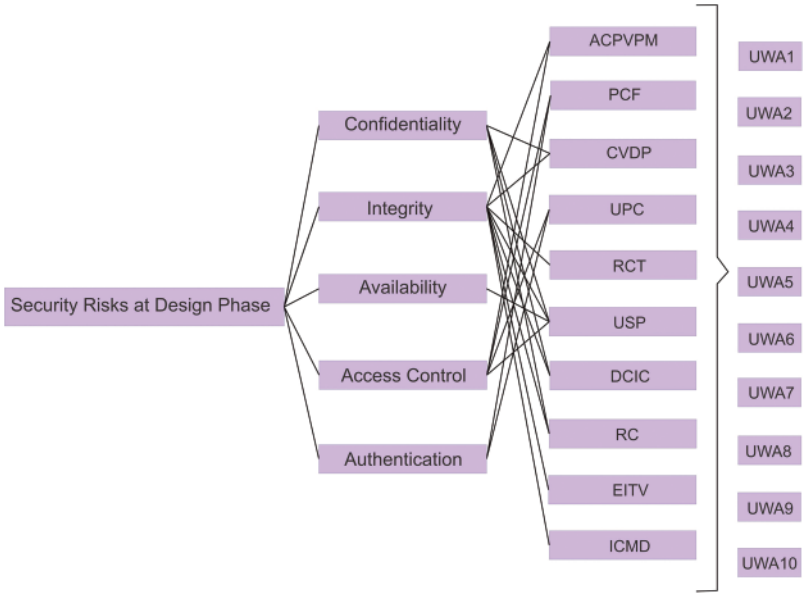

Figure 3: Healthcare web application security risk attributes concerning security durability

4 Methodology Followed

Some real-world issues demand unique or multi-choice-based solutions that are crucial for the users to choose the best from several options without any solid base. To tackle this

situation and give an ideal quantitative solution to these issues, the adopted MCDM approaches are implemented by various researchers [12–14]. Specifically adopted AHP approach combined with a fuzzy set theory is more effective and simple in comparison of others. This is evident from various previous research initiatives [15–17]. If there is more than one option available for evaluation in the technique during the computation process, then this situation influences the calculated results even more strongly. In the context of the proposed article, the authors adopt a hesitant fuzzy set-based MCDM approach that gives an extra efficiency in results in the perspective of assessment. Besides, the TOPSIS approach has been used to assess the risk impact of healthcare web application security. Moreover, to get more productive and accurate results, this study adopts the hesitant fuzzy-based TOPSIS approach. For testing the evaluated results, the adopted methodology of TOPSIS is the most appropriate approach available among the MCDM approaches. The biggest advantage of this methodology is that it gives a positive impact as well as negative impact and deliberates it in the calculation.

In our research, HF-AHP methods were enlisted to assess the priority of the security risk factors, and then we tested their approach HF-TOPSIS on alternatives for similar factors [5]. A step-by-step procedure, in brief, is deliberated below:

Step 1: The first step in the implemented approach is the hierarchy development of factors.
Step 2: In Tab. 2, examiners use linguistic terminology to create accurate and beneficial assessment criteria for the decision-makers.
Step 3: The next step in technique evaluation is the adoption of fuzzy wrappers [8] from Eq. (1).

$$OWA(a_1, a_2, \ldots a_n) = \sum_{j=1}^{n} W_j b_j \tag{1}$$

Same as experts evaluate the trapezoidal numbers $\tilde{C} = (a, b, c, d)$ by the Eqs. (2)–(5) after Eq. (1).

$$a = min\left\{a_L^i,\ a_M^i, a_M^{i+1},\ \ldots, a_M^j, a_R^j\right\} = a_L^i \tag{2}$$

$$d = max\left\{a_L^i,\ a_M^i, a_M^{i+1},\ \ldots, a_M^j, a_R^j\right\} = a_R^j \tag{3}$$

$$b = \begin{Bmatrix} a_M^i, if\ i+1 = j \\ \underset{w}{OWA}_{2\left(a_m^j, \ldots .a_m^{\frac{i+j}{2}}\right)}, if\ i+j\ is\ even \\ \underset{w}{OWA}_{2\left(a_m^j, \ldots .a_m^{\frac{i+j+1}{2}}\right)}, if\ i+j\ is\ odd \end{Bmatrix} \tag{4}$$

$$c = \begin{Bmatrix} a_M^{i+1}, if\ \ i+1 = j \\ \underset{w}{OWA}_{2\left(a_m^j a_m^{j-1}, \ldots .a_m^{\frac{(i+j)}{2}}\right)}\ , if\ i+j\ is\ even \\ \underset{w}{OWA}_{2\left(a_m^j, a_m^{j-1} \ldots .a_m^{\frac{(i+j+1)}{2}}\right)}\ , if\ i+j\ is\ odd \end{Bmatrix} \tag{5}$$

After imposing the Eqs. (3)–(5), the experts decide the first and second form of weights η, i.e., the number between [0, 1] and Eqs. (6) and (7) applied by the experts to obtain these numbers.

1st type weights $(W1 = (w_1^1, w_2^1, \ldots, w_n^1))$:

$$w_1^1 = \eta_2,\ w_2^1 = \eta_2(1-\eta_2), \ldots, w_n^1 \eta_2 (1-\eta_2)^{n-2} \tag{6}$$

2nd type weights $(W2 = (w_1^2, w_2^2, \ldots\ldots..w_n^2))$:

$$w_1^2 = \eta_1^{n-1},\ w_2^2 = (1-\eta_1)\eta_1^{n-1} \tag{7}$$

The numerical form for the highest rank in the formula $\eta_1 = \frac{g-(j-1)}{g-1}$s, and $\eta_2 = \frac{g-(j-1)}{g-1}$ is g and lowest, highest rank factors are shown by i and j, respectively.

Table 2: Scale for HF-AHP technique

Rank	Linguistic term	Abbreviation	Values
10	Absolutely high importance	AHI	(7.0000, 9.0000, 9.0000)
9	Very high importance	VHI	(5.0000, 7.0000, 9.0000)
8	Essentially high importance	ESHI	(3.0000, 5.0000, 7.0000)
7	Weakly high importance	WHI	(1.0000, 3.0000, 5.0000)
6	Equally high importance	EHI	(1.0000, 1.0000, 3.0000)
5	Exactly equal	EE	(1.0000, 1. 0000, 1.0000)
4	Equally low importance	ELI	(0.3300, 1.0000, 1.0000)
3	Weakly low important	WLI	(0.2000, 0.3300, 1.0000)
2	Essentially low importance	ESLI	(0.1400, 0.2000, 0.3300)
1	Very low importance	VLI	(0.1100, 0.1400, 0.2000)
0	Absolutely low importance	ALI	(0.1100, 0.1100, 0.1400)

Step 4: Eqs. (8) and (9) are used by the experts after evaluating the entire previous approach to satisfy the remaining comparison matrix attributes. Thereafter, the experts use Eq. (10) to defuzzify the matrix to determine the comparison matrix.

$$\tilde{A} = \begin{bmatrix} 1 & \cdots & \tilde{c}_{1n} \\ \vdots & \ddots & \vdots \\ \tilde{c}_{n1} & \ldots & 1 \end{bmatrix} \tag{8}$$

$$\tilde{c}_{ji} = \left(\frac{1}{cij_u}, \frac{1}{cij_{m2}}, \frac{1}{cij_{m1}}, \frac{1}{cij_1} \right) \tag{9}$$

$$\mu_x = \frac{l + 2m_1 + 2m_2 + h}{6} \tag{10}$$

Step 5: The phase of defuzzification provides correct values. The experts examine the Consistency Ratio (CR) by applying the Eqs. (11) and (12) to analyse the CR of these values.

$$CI = \frac{\gamma_{max} - n}{n-1} \tag{11}$$

$$CR = \frac{CI}{RI} \tag{12}$$

Step 6: In this step, by Eq. (13), the experts assess the geometrical mean of the values.

$$\tilde{r}_i = (\tilde{c}_{i1} \otimes \tilde{c}_{i2} \ldots \otimes \tilde{c}_{in})^{1/n} \tag{13}$$

Step 7: The most significant criterion in the entire set is evaluated by experts by applying the Eq. (14).

$$\tilde{w}_i = \tilde{r}_1 \otimes (\tilde{r}_1 \otimes \tilde{r}_2 \ldots \tilde{r}_n)^{-1} \tag{14}$$

Step 8: Examiners analyze the defuzzified values by Eq. (15).

$$\mu_x = \frac{l + 2m_1 + 2m_2 + h}{6} \tag{15}$$

Step 9: By applying the Eq. (16), experts transform the defuzzified values into normalized values or weights.

$$\frac{\tilde{w}_i}{\sum_i \sum_j \tilde{w}_j} \tag{16}$$

Now after identifying priority list for selected attributes the second adopted methodology of TOPSIS is used for testing the effectiveness of obtained results. TOPSIS is effective as a MADM technique in recommending the most preferred option for use. The definition of the TOPSIS approach was presented by Torra et al. [14]. The synthesis of positive and negative ideas is the TOPSIS methodology; the most accurate and effective option is the most precise and reliable factor. The worst option, on the other hand, is an irrelevant factor. The authors utilized the hesitant fuzzy AHP TOPSIS approach to test and assess the security risk of healthcare web application [15–17]. The TOPSIS method associates the distance between two linguistic values such as H1s and H2s and performs its computations. Below, the procedure has been clarified (Eq. (17)):

$$d(H1s, H2s) = |q^* - q| + |p^* - p| \tag{17}$$

Step 10: The following terms are described as the starting process:

- The following written formulas are applied as $(C = \{C_1, C_2, \ldots, C_E\})$ and n criteria $(C = \{C_1, C_2, \ldots, C_n\})$ to define alternatives and criteria in TOPSIS.
- Similarly, k is used to show the numeric count of experts in TOPSIS $e\_x\ d$ enotes the experts.
- The equation $\tilde{X}^l = [H^l_{S_{ij}}]_{E \times n}$ is used in TOPSIS technique to represent HF matrix.
- The standards are written for TOPSIS to determine the criteria and effect of outcomes:

The standard for TOPSIS evaluation lies in between *very poor and very good scale,*

$r_1^1 =$ *between medium and good* (bt M&G)

$r_2^1 =$ *at most medium* (am M)

$r_1^2 =$ *at least good* (al G)

$r_2^2 =$ *between very bad and medium* (bt VB&M)

For HF matrix, the following formulas are used [9]:

$env_F(EGH\ (btM\&G)) = T\ (0.3300, 0.5000, 0.6700, 0.8300)$

$env_F(EGH\ (amM)) = T\ (0.0000, 0.0000, 0.3500, 0.6700)$

$env_F(EGH\ (alG)) = T\ (0.5000, 0.8500, 1.0000, 1.0000)$

$env_F(EGH\ (btVB\&M)) = T\ (0.0000, 0.3000, 0.3700, 0.6700)$

Step 11: By applying the Eq. (18) formula, the associated combined matrix is created:

$$T_{pij} = min\left\{min_{i=1}^{K}\left(maxH_{t_{ij}}^{x}\right), max_{i=1}^{K}\left(minH_{t_{ij}}^{x}\right)\right\}$$

$$T_{qij} = max\left\{min_{i=1}^{K}\left(maxH_{t_{ij}}^{x}\right), \quad max_{i=1}^{K}\left(minH_{t_{ij}}^{x}\right)\right\} \tag{18}$$

Step 12: The effective factor where most effective factor is indicated by Aj, is shown by alpha in the TOPSIS evaluation, and alpha shows the cost-related preferences. In addition, the latest efficient alternatives need high precision for cost related preferences. The following Eqs. (19)–(22) are used to define and compare cost as well as effective factors:

$$\tilde{V}_{pj}^{+} = max_{i=1}^{K}\left(max_i\left(minH_{S_{ij}}^{x}\right)\right) j \in \alpha_b \quad \text{and} \quad min_{i=1}^{K}\left(min_i\left(minH_{S_{ij}}^{x}\right)\right) j \in \alpha_c\ ) \tag{19}$$

$$\tilde{V}_{qj}^{+} = max_{i=1}^{K}\left(max_i\left(minH_{S_{ij}}^{x}\right)\right) j \in \alpha_b \quad \text{and} \quad min_{i=1}^{K}\left(min_i\left(minH_{S_{ij}}^{x}\right)\right) j \in \alpha_c\ ) \tag{20}$$

$$\tilde{V}_{pj}^{-} = max_{i=1}^{K}\left(max_i\left(minH_{S_{ij}}^{x}\right)\right) j \in \alpha_c \quad \text{and} \quad min_{i=1}^{K}\left(min_i\left(minH_{S_{ij}}^{x}\right)\right) j \in \alpha_b\ ) \tag{21}$$

$$\tilde{V}_{qj}^{-} = max_{i=1}^{K}\left(max_i\left(minH_{S_{ij}}^{x}\right)\right) j \in \alpha_c \quad \text{and} \quad min_{i=1}^{K}\left(min_i\left(minH_{S_{ij}}^{x}\right)\right) j \in \alpha_b\ ) \tag{22}$$

Step 13: Experts evaluate TOPISIS +ve and -ve concepts components by applying following Eqs. (23), (24).

$$D^{+} = \begin{bmatrix} d(x_{11}, \tilde{V}_1^{+}) + d(x_{12}, \tilde{V}_2^{+}) + \ldots + d(x_{1n}, \tilde{V}_n^{+}) \\ d(x_{21}, \tilde{V}_1^{+}) + d(x_{22}, \tilde{V}_2^{+}) + \ldots + d(x_{21}, \tilde{V}_n^{+}) \\ d(x_{m1}, \tilde{V}_1^{+}) + d(x_{m2}, \tilde{V}_1^{+}) + \ldots + d(x_{mn}, \tilde{V}_n^{+}) \end{bmatrix} \tag{23}$$

$$D^- = \begin{bmatrix} d(x_{11}, \tilde{V}_1^-) + d(x_{12}, \tilde{V}_2^-) + \ldots + d(x_{1n}, \tilde{V}_n^-) \\ d(x_{21}, \tilde{V}_1^-) + d(x_{22}, \tilde{V}_2^-) + \ldots + d(x_{21}, \tilde{V}_n^-) \\ d(x_{m1}, \tilde{V}_1^-) + d(x_{m2}, \tilde{V}_1^-) + \ldots + d(x_{mn}, \tilde{V}_n^-) \end{bmatrix} \tag{24}$$

Step 14: Experts build and assess the closeness of positive and negative factors evaluated by Eqs. (25) and (26).

$$CS(A_i) = \frac{D_i^+}{D_i^+ + D_i^-}, \quad i = 1, 2, \ldots, m \tag{25}$$

where

$$D_i^+ = \sum_{j=1}^{n} d\left(x_{ij}, V_j^+\right) \quad \text{and} \quad D_i^- = \sum_{j=1}^{n} d\left(x_{ij}, V_j^-\right) \tag{26}$$

Step 15: The ranks are allocated to conclude the process, and the tabular form of options are focused on their assessment of effectiveness.

In further parts of this study, a highly detailed and evaluated numerical assessment of security risk has been conducted for improving the life span of healthcare web application security.

5 Data Analysis and Outcomes

This sub-section addresses numerous statistical results from the implementation of the integrated hesitant fuzzy-based AHP-TOPSIS method [8]. To evaluate the impact of security risk, the experts generally conduct behavior-based risk research. It is essential to recognize and characterize uncertain behaviors from large sets of signs of execution to accomplish this. The security practitioners face a daunting challenge of numerically analyzing the impact of risk. For a more simplified approach, we have used a recognized and authenticated decision-making tactic, the hesitant fuzzy-based combined methodology of AHP-TOPSIS, to achieve the goals. In the current cybersecurity environment, this hybrid method is suitable for prioritizing malware analysis techniques based on their impact assessment.

The authors of the present research work acquired opinions from 110 security practitioners from numerous sectors of education and development industries to generate a more comprehensive result. For our empirical investigations, the data outsourced from these specialists were gathered. T1, T2, T3, T4, and T5, respectively, reflect the different characteristics for assessing the security risk at the early stage of the healthcare web application development process including *access control, availability, authentication, confidentiality, and integrity*. To evaluate the impact of the above-mentioned security risks on various healthcare web applications signified by *UWA1, UWA2, UWA3, UWA4, UWA5, UWA6, UWA7, UWA8, UWA9, and UWA10.0*, the systemic tactic of hesitant fuzzy-based AHP-TOPSIS is employed.

As shown in Tab. 3, the pair-wise comparative matrix of the characteristics at level 1 is built with the help of [8]. Likewise, with the help of [9], as displayed in Tabs. 4–7, the composite pair-wise comparative matrix for level 2 has been gathered. In this research work, the authors adopted the alpha cut method for defuzzification process and Tabs. 8–12 show the calculations and local weights of the characteristics. Further, final weights of the characteristics through the hierarchy are shown in Tab. 13. In addition, Tabs. 14 and 15 displays the description of the observations, the normalised fuzzy-decision matrix and weighted normalised fuzzy-decision matrix, respectively, with the help of terminology [16]. A combination to calculate the weight of the characteristic of each point is carried out to be more detailed. In addition, Tab. 16 and Fig. 4 show, with the aid of the hierarchy, the closeness coefficients at the desired level among the various alternatives and [9].

Table 3: Combined fuzzy based pair-wise comparison matrix at level 1

Level 1	T1	T2	T3	T4	T5
T1	1.0000, 1.0000, 1.0000, 1.0000	0.0300, 0.0840, 0.0970, 0.1900	0.0320, 0.0720, 0.1040, 0.3040	0.0490, 0.1450, 0.1940, 0.4810	0.0790, 0.1980, 0.2450, 0.7440
T2		1.0000, 1.0000, 1.0000, 1.0000	0.1930, 0.2570, 0.5810, 1.0000	0.0660, 0.1240, 0.4030, 0.4910	0.1340, 0.2570, 0.5810, 0.8400
T3			1.0000, 1.0000, 1.0000, 1.0000	0.2040, 0.2910, 0.5350, 1.0000	0.1410, 0.2910, 0.3710, 0.6870
T4				1.0000, 1.0000, 1.0000, 1.0000	0.0830, 0.2010, 0.3710, 0.4760
T5					1.0000, 1.0000, 1.0000, 1.0000

Table 4: Combined fuzzy based pair-wise comparison matrix at level 2 for confidentiality

	T11	T12	T13
T11	1.0000, 1.0000, 1.0000, 1.0000	0.0460, 0.1060, 0.1420, 0.3040	0.0790, 0.1820, 0.2630, 0.5700
T12		1.0000, 1.0000, 1.0000, 1.0000	0.0410, 0.0840, 0.1040, 0.2220
T13			1.0000, 1.0000, 1.0000, 1.0000

Table 5: Combined fuzzy based pair-wise comparison matrix at level 2 for integrity

	T21	T22	T23	T24	T25	T26	T27	T28
T21	1.0000, 1.0000, 1.0000, 1.0000	0.0350, 0.0880, 0.1830, 0.3420	0.0860, 0.1720, 0.3160, 0.6740	0.1140, 0.2270, 0.4730, 1.0000	0.0580, 0.1310, 0.2400, 0.4510	0.0390, 0.0990, 0.1830, 0.4510	0.0470, 0.1370, 0.2540, 0.3550	0.1210, 0.2370, 0.5000, 1.0000

(Continued)

Table 5: Continued

	T21	T22	T23	T24	T25	T26	T27	T28
T22		1.0000, 1.0000, 1.0000, 1.0000	0.0920, 0.1800, 0.3340, 0.6990	0.0310, 0.0640, 0.1290, 0.2700	0.1140, 0.2270, 0.4730, 1.0000	0.0580, 0.1310, 0.2400, 0.4510	0.1140, 0.2270, 0.4730, 1.0000	0.0500, 0.0920, 0.1930, 0.4670
T23			1.0000, 1.0000, 1.0000, 1.0000	0.0580, 0.1310, 0.2400, 0.4510	0.0310, 0.0640, 0.1290, 0.2700	0.0580, 0.1310, 0.2400, 0.4510	0.0310, 0.0640, 0.1290, 0.2700	0.1140, 0.2270, 0.4730, 1.0000
T24				1.0000, 1.0000, 1.0000, 1.0000	0.0390, 0.0990, 0.1830, 0.4510	0.0310, 0.0640, 0.1290, 0.2700	0.1140, 0.2270, 0.4730, 1.0000	0.1140, 0.2270, 0.4730, 1.0000
T25					1.0000, 1.0000, 1.0000, 1.0000	0.0390, 0.0990, 0.1830, 0.4510	0.1140, 0.2270, 0.4730, 1.0000	0.0390, 0.0990, 0.1830, 0.4510
T26						1.0000, 1.0000, 1.0000, 1.0000	0.1140, 0.2270, 0.4730, 1.0000	0.0580, 0.1310, 0.2400, 0.4510
T27							1.0000, 1.0000, 1.0000, 1.0000	0.1140, 0.2270, 0.4730, 1.0000
T28								1.0000, 1.0000, 1.0000, 1.0000

Table 6: Combined fuzzy based pair-wise comparison matrix at level 2 for access control

	T41	T42	T43	T44
T41	1.0000, 1.0000, 1.0000, 1.0000	0.3090, 0.4143, 0.8980, 1.5451	0.0142, 0.0439, 0.1275, 0.4697	0.0244, 0.0754, 0.2362, 0.8881
T42		1.0000, 1.0000, 1.0000, 1.0000	0.1382, 0.2380, 0.6351, 0.6910	0.0127, 0.0348, 0.0934, 0.3430
T43			1.0000, 1.0000, 1.0000, 1.0000	0.0244, 0.0754, 0.2362, 0.8881
T44				1.0000, 1.0000, 1.0000, 1.0000

Table 7: Combined fuzzy based pair-wise comparison matrix at level 2 for authentication

	T51	T52
T51	1.0000, 1.0000, 1.0000, 1.0000	0.0093, 0.0348, 0.0871, 0.2936
T52		1.0000, 1.0000, 1.0000, 1.0000

Table 8: Combined pair-wise comparison matrix and local weights at level 1

	T1	T2	T3	T4	T5	Weights
T1	1.0000	0.2560	0.2057	0.2873	0.3933	0.0566
T2	3.9063	1.0000	0.2922	0.3125	0.2392	0.0788
T3	4.8615	3.4223	1.0000	0.2636	0.1140	0.1156
T4	3.4807	3.2000	3.7936	1.0000	0.9015	0.1661
T5	2.5426	4.1806	8.7719	1.1093	1.0000	0.5829
						C.R. = 0.05487

Table 9: Combined pair-wise comparison matrix and local weights at level 2 for confidentiality

	T1	T2	T3	Weights
T1	1.0000	0.1275	0.1741	0.0583
T2	7.8431	1.0000	0.1301	0.2088
T3	5.7438	7.6864	1.0000	0.7329
				C.R. = 0.003890

Table 10: Combined pair-wise comparison matrix and local weights at level 2 for integrity

	T21	T22	T23	T24	T25	T26	T27	T28	Weights
T21	1.0000	0.2560	0.2057	0.2873	0.3933	0.5207	1.1690	0.3430	0.0484
T22	3.9063	1.0000	0.6770	0.2560	0.2057	0.2873	0.3933	0.2150	0.0497
T23	4.8615	1.4771	1.0000	0.2922	0.3125	0.2392	0.2636	0.1140	0.0566
T24	3.4807	3.9063	3.4223	1.0000	0.1064	0.1391	1.3511	0.7319	0.1005
T25	2.5426	4.8615	3.2000	9.3990	1.0000	0.7172	1.1028	0.4350	0.2070
T26	1.9205	3.4807	4.1806	7.1891	1.3943	1.0000	2.3852	1.0473	0.2204
T27	0.8554	2.5426	3.7936	0.7401	0.9068	0.4193	1.0000	0.2621	0.0893
T28	2.9155	4.6512	8.7719	1.3663	2.2989	0.9548	3.8153	1.0000	0.2281
									C.R. = 0.045895

Table 11: Combined pair-wise comparison matrix and local weights at level 2 for availability

	T41	T42	T43	T44	Weights
T41	1.0000	0.1392	0.1933	0.1078	0.0320
T42	7.1839	1.0000	0.1922	0.1621	0.0972
T43	5.1733	5.2029	1.0000	0.1113	0.1927
T44	9.2764	6.1690	8.9847	1.0000	0.6781
					CR = 0.017850

Table 12: Combined pair-wise comparison matrix and local weights at level 2 for access control

	T51	T52	Weights
T51	1.0000	0.6261	0.3850
T52	1.5972	1.0000	0.6150
			CR = 0.00000

Table 13: Global weights through the hierarchy

Attributes at level 1	Independent weights at Level 1	Attributes at level 2	Independent weights at level 2	Dependent weights at level 2
T1	0.0566	T11	0.0583	0.0032998
		T12	0.2088	0.0118181
		T13	0.7329	0.0414821
T2	0.0788	T21	0.0484	0.0038139
		T22	0.0497	0.0039164
		T23	0.0566	0.0044601
		T24	0.1005	0.0079194
		T25	0.2070	0.0163116
		T26	0.2204	0.0173675
		T27	0.0893	0.0070368
		T28	0.2281	0.0179743
T3	0.1156	T31	-	0.1156000
T4	0.1661	T41	0.0320	0.0053152
		T42	0.0972	0.0161449
		T43	0.1927	0.0320075
		T44	0.6781	0.1126324
T5	0.5829	T51	0.3850	0.2244165
		T52	0.6150	0.3584835

Table 14: Subjective cognition results

	UWA1	UWA2	UWA3	UWA4	UWA5	UWA6	UWA7	UWA8	UWA9	UWA10
T11	2.8200,	1.5500,	1.4500,	2.8200,	1.5500,	1.4500,	2.4500,	1.5500,	1.4500,	1.6400,
	4.6400,	3.1800,	3.1800,	4.6400,	3.1800,	3.1800,	4.2700,	3.1800,	3.1800,	3.5500,
	6.6400,	5.1800,	5.1800,	6.6400,	5.1800,	5.1800,	6.2700,	5.1800,	5.1800,	5.5500,
	8.7200	6.7200	7.7200	8.7200	6.7200	7.7200	8.6200	6.7200	7.7200	6.7300
T12	2.9100,	1.4500,	1.1800,	2.9100,	1.4500,	1.1800,	2.0900,	1.4500,	1.1800,	2.5500,
	4.6400,	3.0000,	2.8200,	4.6400,	3.0000,	2.8200,	3.7300,	3.0000,	2.8200,	4.4500,
	6.0000,	4.9100,	4.8200,	6.0000,	4.9100,	4.8200,	5.7300,	4.9100,	4.8200,	6.4500,
	6.4500	5.4500	6.4500	6.4500	5.4500	6.4500	6.4500	5.4500	6.4500	7.8400
T13	2.8200,	1.5500,	1.4500,	2.4500,	1.5500,	2.8200,	1.5500,	1.4500,	2.4500,	1.5500,
	4.6400,	3.1800,	3.1800,	4.2700,	3.1800,	4.6400,	3.1800,	3.1800,	4.2700,	3.1800,
	6.6400,	5.1800,	5.1800,	6.2700,	5.1800,	6.6400,	5.1800,	5.1800,	6.2700,	5.1800,
	8.7200	6.7200	7.7200	8.6200	6.7200	8.7200	6.7200	7.7200	8.6200	6.7200
T21	2.9100,	1.4500,	1.1800,	2.0900,	1.4500,	2.9100,	1.4500,	1.1800,	2.0900,	1.4500,
	4.6400,	3.0000,	2.8200,	3.7300,	3.0000,	4.6400,	3.0000,	2.8200,	3.7300,	3.0000,
	6.0000,	4.9100,	4.8200,	5.7300,	4.9100,	6.0000,	4.9100,	4.8200,	5.7300,	4.9100,
	6.4500	5.4500	6.4500	6.4500	5.4500	6.4500	5.4500	6.4500	6.4500	5.4500
T22	3.1800,	1.4500,	0.8200,	3.0000,	1.4500,	3.1800,	1.4500,	0.8200,	3.0000,	1.4500,
	5.1800,	3.0700,	2.2700,	4.8200,	3.0700,	5.1800,	3.0700,	2.2700,	4.8200,	3.0700,
	7.1000,	4.9100,	4.2700,	6.8200,	4.9100,	7.1000,	4.9100,	4.2700,	6.8200,	4.9100,
	8.6500	5.6500	6.6500	7.6500	5.6500	8.6500	5.6500	6.6500	7.6500	5.6500
T23	1.1800,	2.9100,	1.4500,	1.1800,	2.0900,	1.1800,	2.9100,	1.4500,	1.1800,	2.0900,
	2.8200,	4.6400,	3.0000,	2.8200,	3.7300,	2.8200,	4.6400,	3.0000,	2.8200,	3.7300,
	4.8200,	6.0000,	4.9100,	4.8200,	5.7300,	4.8200,	6.0000,	4.9100,	4.8200,	5.7300,
	6.4500	6.4500	5.4500	6.4500	6.4500	6.4500	6.4500	5.4500	6.4500	6.4500
T24	1.4500,	2.4500,	1.5500,	2.8200,	1.5500,	1.4500,	2.4500,	1.5500,	2.8200,	1.5500,
	3.1800,	4.2700,	3.1800,	4.6400,	3.1800,	3.1800,	4.2700,	3.1800,	4.6400,	3.1800,
	5.1800,	6.2700,	5.1800,	6.6400,	5.1800,	5.1800,	6.2700,	5.1800,	6.6400,	5.1800,
	7.7200	8.6200	6.7200	8.7200	6.7200	7.7200	8.6200	6.7200	8.7200	6.7200
T25	1.1800,	2.9100,	1.4500,	1.1800,	2.0900,	1.1800,	2.9100,	1.4500,	1.1800,	2.0900,
	2.8200,	4.6400,	3.0000,	2.8200,	3.7300,	2.8200,	4.6400,	3.0000,	2.8200,	3.7300,
	4.8200,	6.0000,	4.9100,	4.8200,	5.7300,	4.8200,	6.0000,	4.9100,	4.8200,	5.7300,
	6.4500	6.4500	5.4500	6.4500	6.4500	6.4500	6.4500	5.4500	6.4500	6.4500
T26	1.4500,	2.4500,	1.5500,	2.8200,	1.5500,	1.4500,	2.4500,	1.5500,	2.8200,	1.5500,
	3.1800,	4.2700,	3.1800,	4.6400,	3.1800,	3.1800,	4.2700,	3.1800,	4.6400,	3.1800,
	5.1800,	6.2700,	5.1800,	6.6400,	5.1800,	5.1800,	6.2700,	5.1800,	6.6400,	5.1800,
	7.7200	8.6200	6.7200	8.7200	6.7200	7.7200	8.6200	6.7200	8.7200	6.7200
T27	1.1800,	2.0900,	1.4500,	2.9100,	1.4500,	1.1800,	2.0900,	1.4500,	2.9100,	1.4500,
	2.8200,	3.7300,	3.0000,	4.6400,	3.0000,	2.8200,	3.7300,	3.0000,	4.6400,	3.0000,
	4.8200,	5.7300,	4.9100,	6.0000,	4.9100,	4.8200,	5.7300,	4.9100,	6.0000,	4.9100,
	6.4500	6.4500	5.4500	6.4500	5.4500	6.4500	6.4500	5.4500	6.4500	5.4500
T28	1.1800,	2.9100,	1.4500,	1.1800,	2.0900,	1.1800,	2.9100,	1.4500,	1.1800,	2.0900,
	2.8200,	4.6400,	3.0000,	2.8200,	3.7300,	2.8200,	4.6400,	3.0000,	2.8200,	3.7300,
	4.8200,	6.0000,	4.9100,	4.8200,	5.7300,	4.8200,	6.0000,	4.9100,	4.8200,	5.7300,
	6.4500	6.4500	5.4500	6.4500	6.4500	6.4500	6.4500	5.4500	6.4500	6.4500
T31	1.4500,	2.4500,	1.5500,	2.8200,	1.5500,	1.4500,	2.4500,	1.5500,	2.8200,	1.5500,
	3.1800,	4.2700,	3.1800,	4.6400,	3.1800,	3.1800,	4.2700,	3.1800,	4.6400,	3.1800,
	5.1800,	6.2700,	5.1800,	6.6400,	5.1800,	5.1800,	6.2700,	5.1800,	6.6400,	5.1800,
	7.7200	8.6200	6.7200	8.7200	6.7200	7.7200	8.6200	6.7200	8.7200	6.7200

(Continued)

Table 14: Continued

	UWA1	UWA2	UWA3	UWA4	UWA5	UWA6	UWA7	UWA8	UWA9	UWA10
T41	1.1800, 2.8200, 4.8200, 6.4500	2.0900, 3.7300, 5.7300, 6.4500	1.4500, 3.0000, 4.9100, 5.4500	2.9100, 4.6400, 6.0000, 6.4500	1.4500, 3.0000, 4.9100, 5.4500	1.1800, 2.8200, 4.8200, 6.4500	2.0900, 3.7300, 5.7300, 6.4500	1.4500, 3.0000, 4.9100, 5.4500	2.9100, 4.6400, 6.0000, 6.4500	1.4500, 3.0000, 4.9100, 5.4500
T42	1.5500, 3.1800, 5.1800, 6.7200	2.8200, 4.6400, 6.6400, 8.7200	1.5500, 3.1800, 5.1800, 6.7200	1.4500, 3.1800, 5.1800, 7.7200	1.5500, 3.1800, 5.1800, 6.7200	2.8200, 4.6400, 6.6400, 8.7200	1.5500, 3.1800, 5.1800, 6.7200	1.4500, 3.1800, 5.1800, 7.7200	2.4500, 4.2700, 6.2700, 8.6200	1.5500, 3.1800, 5.1800, 6.7200
T43	1.4500, 3.0000, 4.9100, 5.4500	2.9100, 4.6400, 6.0000, 6.4500	1.4500, 3.0000, 4.9100, 5.4500	1.1800, 2.8200, 4.8200, 6.4500	1.4500, 3.0000, 4.9100, 5.4500	2.9100, 4.6400, 6.0000, 6.4500	1.4500, 3.0000, 4.9100, 5.4500	1.1800, 2.8200, 4.8200, 6.4500	2.0900, 3.7300, 5.7300, 6.4500	1.4500, 3.0000, 4.9100, 5.4500
T44	1.4500, 3.0000, 4.9100, 5.4500	1.1800, 2.8200, 4.8200, 6.4500	2.0900, 3.7300, 5.7300, 6.4500	1.1800, 2.8200, 4.8200, 6.4500	1.4500, 3.0000, 4.9100, 5.4500	1.1800, 2.8200, 4.8200, 6.4500	2.0900, 3.7300, 5.7300, 6.4500	1.1800, 2.8200, 4.8200, 6.4500	2.9100, 4.6400, 6.0000, 6.4500	1.4500, 3.0000, 4.9100, 5.4500
T51	1.5500, 3.1800, 5.1800, 6.7200	2.8200, 4.6400, 6.6400, 8.7200	1.5500, 3.1800, 5.1800, 6.7200	1.4500, 3.1800, 5.1800, 7.7200	2.4500, 4.2700, 6.2700, 8.6200	1.5500, 3.1800, 5.1800, 6.7200	2.8200, 4.6400, 6.6400, 8.7200	1.4500, 3.1800, 5.1800, 7.7200	2.4500, 4.2700, 6.2700, 8.6200	1.5500, 3.1800, 5.1800, 6.7200
T52	1.4500, 3.0000, 4.9100, 5.4500	2.9100, 4.6400, 6.0000, 6.4500	1.4500, 3.0000, 4.9100, 5.4500	1.1800, 2.8200, 4.8200, 6.4500	2.0900, 3.7300, 5.7300, 6.4500	1.4500, 3.0000, 4.9100, 5.4500	2.9100, 4.6400, 6.0000, 6.4500	1.6400, 3.5500, 5.5500, 6.7300	1.6400, 3.5500, 5.5500, 6.7300	3.9100, 5.9100, 7.9100, 8.7300

Table 15: The weighted normalized fuzzy-decision matrix

	UWA1	UWA2	UWA3	UWA4	UWA5	UWA6	UWA7	UWA8	UWA9	UWA10
T11	0.1480, 0.1891, 0.2060, 0.2240	0.1420, 0.1790, 0.1980, 0.2190	0.0570, 0.0850, 0.1080, 0.1310	0.0555, 0.0870, 0.1040, 0.1220	0.1420, 0.1790, 0.1980, 0.2190	0.0570, 0.0850, 0.1080, 0.1310	0.0555, 0.0870, 0.1040, 0.1220	0.0555, 0.0870, 0.1040, 0.1220	0.1420, 0.1790, 0.1980, 0.2190	0.0570, 0.0850, 0.1080, 0.1310
T12	0.1420, 0.1790, 0.1980, 0.2190	0.1480, 0.1891, 0.2060, 0.2240	0.0344, 0.0570, 0.0820, 0.1100	0.0470, 0.0740, 0.0920, 0.1120	0.1330, 0.1680, 0.1840, 0.2080	0.1480, 0.1891, 0.2060, 0.2240	0.0344, 0.0570, 0.0820, 0.1100	0.0470, 0.0740, 0.0920, 0.1120	0.1330, 0.1680, 0.1840, 0.2080	0.1480, 0.1891, 0.2060, 0.2240
T13	0.1420, 0.1790, 0.1980, 0.2190	0.0570, 0.0850, 0.1080, 0.1310	0.1330, 0.1680, 0.1840, 0.2080	0.0371, 0.0616, 0.0790, 0.1100	0.0320, 0.0530, 0.0720, 0.0980	0.0320, 0.0470, 0.0530, 0.0630	0.0371, 0.0616, 0.0790, 0.1100	0.0371, 0.0616, 0.0790, 0.1100	0.0320, 0.0530, 0.0720, 0.0980	0.0320, 0.0470, 0.0530, 0.0630
T21	0.1330, 0.1680, 0.1840, 0.2080	0.0371, 0.0616, 0.0790, 0.1100	0.1480, 0.1891, 0.2060, 0.2240	0.0344, 0.0570, 0.0820, 0.1100	0.0470, 0.0740, 0.0920, 0.1120	0.1330, 0.1680, 0.1840, 0.2080	0.0371, 0.0616, 0.0790, 0.1100	0.0344, 0.0570, 0.0820, 0.1100	0.0470, 0.0740, 0.0920, 0.1120	0.1330, 0.1680, 0.1840, 0.2080

(Continued)

Table 15: Continued

	UWA1	UWA2	UWA3	UWA4	UWA5	UWA6	UWA7	UWA8	UWA9	UWA10
T22	0.0090,	0.0630,	0.1420,	0.0570,	0.0555,	0.1480,	0.0344,	0.0570,	0.0555,	0.1480,
	0.0230,	0.0979,	0.1790,	0.0850,	0.0870,	0.1891,	0.0570,	0.0850,	0.0870,	0.1891,
	0.0450,	0.1140,	0.1980,	0.1080,	0.1040,	0.2060,	0.0820,	0.1080,	0.1040,	0.2060,
	0.0590	0.1310	0.2190	0.1310	0.1220	0.2240	0.1100	0.1310	0.1220	0.2240
T23	0.0100,	0.1330,	0.0371,	0.0320,	0.0320,	0.1330,	0.0371,	0.0320,	0.0320,	0.1330,
	0.0150,	0.1680,	0.0616,	0.0530,	0.0470,	0.1680,	0.0616,	0.0530,	0.0470,	0.1680,
	0.0160,	0.1840,	0.0790,	0.0720,	0.0530,	0.1840,	0.0790,	0.0720,	0.0530,	0.1840,
	0.0200	0.2080	0.1100	0.0980	0.0630	0.2080	0.1100	0.0980	0.0630	0.2080
T24	0.0173,	0.1480,	0.0344,	0.0470,	0.0434,	0.1480,	0.0344,	0.0470,	0.1330,	0.0371,
	0.0233,	0.1891,	0.0570,	0.0740,	0.0510,	0.1891,	0.0570,	0.0740,	0.1680,	0.0616,
	0.0250,	0.2060,	0.0820,	0.0920,	0.0660,	0.2060,	0.0820,	0.0920,	0.1840,	0.0790,
	0.0270	0.2240	0.1100	0.1120	0.0690	0.2240	0.1100	0.1120	0.2080	0.1100
T25	0.0854,	0.1420,	0.0570,	0.0555,	0.0428,	0.1420,	0.0570,	0.0555,	0.1480,	0.0344,
	0.0930,	0.1790,	0.0850,	0.0870,	0.0590,	0.1790,	0.0850,	0.0870,	0.1891,	0.0570,
	0.0930,	0.1980,	0.1080,	0.1040,	0.0640,	0.1980,	0.1080,	0.1040,	0.2060,	0.0820,
	0.0986	0.2190	0.1310	0.1220	0.0680	0.2190	0.1310	0.1220	0.2240	0.1100
T26	0.1330,	0.1480,	0.0344,	0.0470,	0.1480,	0.0344,	0.0371,	0.0320,	0.0320,	0.1420,
	0.1680,	0.1891,	0.0570,	0.0740,	0.1891,	0.0570,	0.0616,	0.0530,	0.0470,	0.1790,
	0.1840,	0.2060,	0.0820,	0.0920,	0.2060,	0.0820,	0.0790,	0.0720,	0.0530,	0.1980,
	0.2080	0.2240	0.1100	0.1120	0.2240	0.1100	0.1100	0.0980	0.0630	0.2190
T27	0.1480,	0.1420,	0.0570,	0.0555,	0.1420,	0.0570,	0.0344,	0.0470,	0.1330,	0.0371,
	0.1891,	0.1790,	0.0850,	0.0870,	0.1790,	0.0850,	0.0570,	0.0740,	0.1680,	0.0616,
	0.2060,	0.1980,	0.1080,	0.1040,	0.1980,	0.1080,	0.0820,	0.0920,	0.1840,	0.0790,
	0.2240	0.2190	0.1310	0.1220	0.2190	0.1310	0.1100	0.1120	0.2080	0.1100
T28	0.1420,	0.1480,	0.0344,	0.0470,	0.1330,	0.1480,	0.0344,	0.0470,	0.1330,	0.1480,
	0.1790,	0.1891,	0.0570,	0.0740,	0.1680,	0.1891,	0.0570,	0.0740,	0.1680,	0.1891,
	0.1980,	0.2060,	0.0820,	0.0920,	0.1840,	0.2060,	0.0820,	0.0920,	0.1840,	0.2060,
	0.2190	0.2240	0.1100	0.1120	0.2080	0.2240	0.1100	0.1120	0.2080	0.2240
T31	0.1330,	0.1420,	0.0570,	0.0555,	0.1480,	0.0344,	0.0470,	0.1330,	0.0371,	0.0344,
	0.1680,	0.1790,	0.0850,	0.0870,	0.1891,	0.0570,	0.0740,	0.1680,	0.0616,	0.0570,
	0.1840,	0.1980,	0.1080,	0.1040,	0.2060,	0.0820,	0.0920,	0.1840,	0.0790,	0.0820,
	0.2080	0.2190	0.1310	0.1220	0.2240	0.1100	0.1120	0.2080	0.1100	0.1100
T41	0.0090,	0.0371,	0.0320,	0.0320,	0.1420,	0.0570,	0.0555,	0.1480,	0.0344,	0.0570,
	0.0230,	0.0616,	0.0530,	0.0470,	0.1790,	0.0850,	0.0870,	0.1891,	0.0570,	0.0850,
	0.0450,	0.0790,	0.0720,	0.0530,	0.1980,	0.1080,	0.1040,	0.2060,	0.0820,	0.1080,
	0.0590	0.1100	0.0980	0.0630	0.2190	0.1310	0.1220	0.2240	0.1100	0.1310
T42	0.1480,	0.0344,	0.0470,	0.1330,	0.0371,	0.0371,	0.0320,	0.0320,	0.1420,	0.0570,
	0.1891,	0.0570,	0.0740,	0.1680,	0.0616,	0.0616,	0.0530,	0.0470,	0.1790,	0.0850,
	0.2060,	0.0820,	0.0920,	0.1840,	0.0790,	0.0790,	0.0720,	0.0530,	0.1980,	0.1080,
	0.2240	0.1100	0.1120	0.2080	0.1100	0.1100	0.0980	0.0630	0.2190	0.1310
T43	0.1480,	0.0344,	0.0470,	0.1330,	0.1480,	0.0344,	0.0470,	0.1330,	0.0371,	0.1480,
	0.1891,	0.0570,	0.0740,	0.1680,	0.1891,	0.0570,	0.0740,	0.1680,	0.0616,	0.1891,
	0.2060,	0.0820,	0.0920,	0.1840,	0.2060,	0.0820,	0.0920,	0.1840,	0.0790,	0.2060,
	0.2240	0.1100	0.1120	0.2080	0.2240	0.1100	0.1120	0.2080	0.1100	0.2240

(Continued)

Table 15: Continued

	UWA1	UWA2	UWA3	UWA4	UWA5	UWA6	UWA7	UWA8	UWA9	UWA10
T44	0.1420, 0.1790, 0.1980, 0.2190	0.0570, 0.0850, 0.1080, 0.1310	0.0555, 0.0870, 0.1040, 0.1220	0.1480, 0.1891, 0.2060, 0.2240	0.1420, 0.1790, 0.1980, 0.2190	0.0371, 0.0616, 0.0790, 0.1100	0.0320, 0.0530, 0.0720, 0.0980	0.0320, 0.0470, 0.0530, 0.0630	0.1420, 0.1790, 0.1980, 0.2190	0.0570, 0.0850, 0.1080, 0.1310
T51	0.0371, 0.0616, 0.0790, 0.1100	0.0320, 0.0530, 0.0720, 0.0980	0.0320, 0.0470, 0.0530, 0.0630	0.1330, 0.1680, 0.1840, 0.2080	0.0371, 0.0616, 0.0790, 0.1100	0.0371, 0.0616, 0.0790, 0.1100	0.0320, 0.0530, 0.0720, 0.0980	0.0320, 0.0470, 0.0530, 0.0630	0.1420, 0.1790, 0.1980, 0.2190	0.0570, 0.0850, 0.1080, 0.1310
T52	0.0344, 0.0570, 0.0820, 0.1100	0.0470, 0.0740, 0.0920, 0.1120	0.0434, 0.0510, 0.0660, 0.0690	0.1480, 0.1891, 0.2060, 0.2240	0.0344, 0.0570, 0.0820, 0.1100	0.0344, 0.0570, 0.0820, 0.1100	0.0470, 0.0740, 0.0920, 0.1120	0.1330, 0.1680, 0.1840, 0.2080	0.0371, 0.0616, 0.0790, 0.1100	0.1480, 0.1891, 0.2060, 0.2240

Table 16: Closeness coefficients among alternatives

Alternatives (A)	di+	di−	Gap degree of CCi+	Satisfaction degree
UWA1	0.0449124	0.0256457	0.3668565	0.6335245
UWA2	0.0358125	0.0352457	0.4695854	0.5234512
UWA3	0.0363547	0.0422556	0.5846574	0.4855467
UWA4	0.0354575	0.0260897	0.4845764	0.5745675
UWA5	0.0399578	0.0469556	0.5375487	0.4699673
UWA6	0.0446536	0.0256857	0.3667764	0.6355467
UWA7	0.0358544	0.0352559	0.4697764	0.5235641
UWA8	0.0366987	0.0422568	0.5837945	0.4852564
UWA9	0.0368858	0.0270887	0.4930124	0.5848859
UWA10	0.0382259	0.0459998	0.5135546	0.4562233

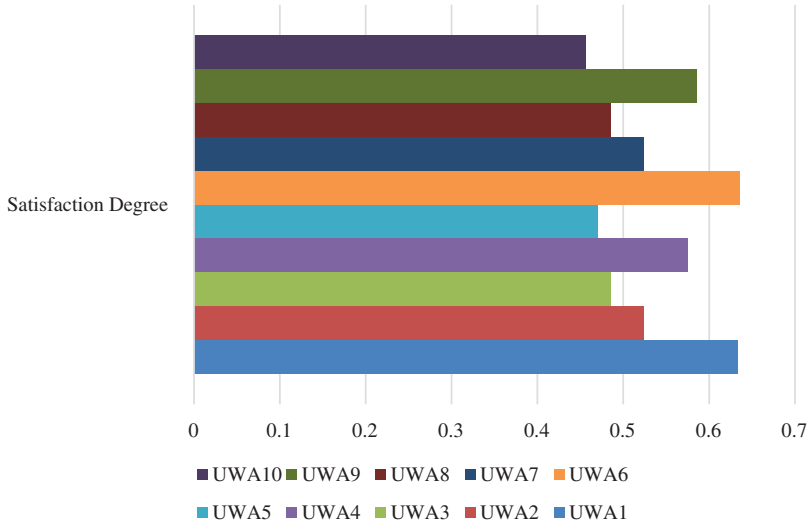

Figure 4: Graphical representation of satisfaction degrees

6 Conclusion

Security breaches can be minimized to a great extent if the issues pertaining to security-durability of web applications are resolved in their emerging phases itself. Thus, the analysis and management of security risks should be given the top priority while developing a health-care web application. Adopting such an approach would result in more productive and reliable implementations. Nowadays, where almost everything is done digitally, the use of object-oriented technology continues to grow naturally. The security characteristic is hard to ignore at the same time. Therefore, if these security risks are linked to object-focused design properties, it could be very useful for secure healthcare web application development in the future.

The researchers may also measure the connection between these threats and object-oriented design properties of healthcare web applications through hesitant fuzzy-based AHP-TOPSIS for accurate interdependence. To establish the exact mutual reliability, an effective, powerful, and secure healthcare web application can be used. In this analysis, the *Alternative (UWA6*) delivered the utmost efficient and durable security system among all the 10 competing options. The evaluation of information security in the University's web application security strategies would be a useful aid in improving the quality of healthcare web applications that can offer secure and reliable mechanisms for protection against both internal and external attacks and threats. The key conclusions of this work are:

- The security risk characteristic outcomes affecting the healthcare web applications security from a design perspective delivers an efficient and perfect priority list.
- The most prioritized alternative is the UWA6.The results drawn from the analysis will be very useful for the researchers and developers who can refer to the present study's tabulations in their efforts to choose the most secure design approach for modeling effective healthcare web applications.
- The study has found four characteristics that affect healthcare web applications. By taking the assessment procedure of this research work, the weights of the healthcare web application security risks can be elicited.

Acknowledgement: This research work was funded by Institutional Fund Projects under Grant No. (IFPHI-286-611-2020). Therefore, the authors gratefully acknowledge technical and financial support from the Ministry of Education and King Abdulaziz University, DSR, Jeddah, Saudi Arabia.

Funding Statement: Funding for this study was received from the Ministry of Education and Deanship of Scientific Research at King Abdulaziz University, Kingdom of Saudi Arabia under Grant No. IFPHI-286-611-2020.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] S. A. Khan, M. Alenezi, A. Agrawal, R. Kumar and R. A. Khan, "Evaluating performance of software durability through an integrated fuzzy-based symmetrical method of ANP and TOPSIS," *Symmetry*, vol. 12, no. 4, pp. 1–15, 2020.

[2] A. Agrawal, M. Zarour, M. Alenezi, R. Kumar and R. A. Khan, "Security durability assessment through fuzzy analytic hierarchy process," *PeerJ Computer Science*, vol. 5, no. 9, pp. 1–43, 2019.

[3] R. Kumar, M. Zarour, M. Alenezi, A. Agrawal and R. A. Khan, "Measuring security-durability through fuzzy based decision-making process," *International Journal of Computational Intelligence Systems*, vol. 12, no. 2, pp. 627–642, 2019.

[4] CWE-260: Password in configuration file, "Common weakness enumeration," 2009. [Online]. Available: https://cwe.mitre.org/data/definitions/260.html.

[5] R. Kumar, A. I. Khan, Y. B. Abushark, M. M. Alam, A. Agrawal *et al.*, "A knowledge based integrated system of hesitant fuzzy set, AHP and TOPSIS for evaluating security-durability of web applications," *IEEE Access*, vol. 8, no. 2, pp. 48870–48885, 2020.

[6] CWE-494: Download of code without integrity check, "Common weakness enumeration," 2013. [Online]. Available: https://cwe.mitre.org/data/definitions/494.html.

[7] M. Xia and Z. Xu, "Hesitant fuzzy information aggregation in decision making," *International Journal of Approximation Reason*, vol. 52, no. 5, pp. 395–407, 2011.

[8] K. Sahu, F. A. Alzahrani, R. K. Srivastava and R. Kumar, "Hesitant fuzzy sets based symmetrical model of decision-making for estimating the durability of web application," *Symmetry*, vol. 12, no. 6, pp. 1770–1792, 2020.

[9] A. Attaallah, A. Algarni and R. A. Khan, "Managing security-risks for improving security-durability of institutional web-applications: Design perspective," *Computers, Materials & Continua*, vol. 66, no. 2, pp. 1849–1865, 2021.

[10] R. M. Rodriguez, L. Martinez and F. Herrera, "Hesitant fuzzy linguistic term sets for decision making," *IEEE Transaction Fuzzy System*, vol. 20, no. 7, pp. 109–119, 2011.

[11] K. Sahu and R. K. Srivastava, "Soft computing approach for prediction of software reliability," *ICIC Express Letters*, vol. 12, no. 12, pp. 1213–1222, 2018.

[12] J. Kaur, A. I. Khan, Y. B. Abushark, M. M. Alam, S. A. Khan *et al.*, "Security risk assessment of healthcare web application through adaptive neuro-fuzzy inference system: A design perspective," *Risk Management and Healthcare Policy*, vol. 13, no. 5, pp. 355–371, 2020.

[13] K. Sahu and R. K. Srivastava, "Needs and importance of reliability prediction: An industrial perspective," *Information Sciences Letters*, vol. 9, no. 1, pp. 33–37, 2020.

[14] V. Torra, and Y. Narukawa, "On hesitant fuzzy sets and decision," in *Proc. of the 2009 IEEE Int. Conf. on Fuzzy Systems*, Jeju Island, South Korea, pp. 1378–1382, 2009.

[15] M. Schiefer, *Internet of Things: Security Evaluation of Nine Fitness Trackers*, Magdeburg, Germany, AV TEST, The Independent IT Security Institute, 2015. [Online]. Available: https://www.av-test.org/fileadmin/pdf/publications/avtest_2015-06_fitness_tracker_english-1.pdf.

[16] R. Kumar, A. K. Pandey, A. Baz, H. Alhakami, W. Alhakami *et al.*, "Fuzzy-based symmetrical multi-criteria decision-making procedure for evaluating the impact of harmful factors of healthcare information security," *Symmetry*, vol. 12, no. 664, pp. 1–23, 2020.

[17] K. Sahu and R. K. Srivastava, ""Revisiting software reliability," *Advances in Intelligent Systems and Computing*, vol. 808, pp. 221–235, 2019.

[18] S. Alder, "Healthcare data breach report," *HIPPA Journal*, vol. 1, pp. 1–10, 2020. [Online]. Available: https://www.hipaajournal.com/2020-healthcare-data-breach-report-us/.

[19] The 2020-2021 Healthcare Cybersecurity Report, "A special report from the editors at cybersecurity ventures," Herjavec Group, 2021. [Online]. Available: https://1c7fab3im83f5gqiow2qqs2k-wpengine.netdna-ssl.com/wp-content/uploads/2020/09/HG-Healthcare-Cybersecurity-Report-2021.pdf.