Tech Science Press

Estimating Usable-Security Through Hesitant Fuzzy Linguistic Term Sets Based Technique

Abdulaziz Attaallah[1] and Raees Ahmad Khan[2,*]

[1]Department of Computer Science, Faculty of Computing and Information Technology, King Abdulaziz University, Jeddah, 21589, Saudi Arabia
[2]Department of Information Technology, Babasaheb Bhimrao Ambedkar University, Lucknow, 226025, Uttar Pradesh, India
*Corresponding Author: Raees Ahmad Khan. Email: khanraees@yahoo.com

Abstract: The apparent contradiction between usability and security has been discussed in the literature for several years. This continuous trade-off requires be acknowledging and handling whenever security solutions are introduced. However, some progressive analysts point out that present security solutions are usually very difficult for several users, and they have expressed a willingness to simplify the security product user experience. Usable security is still mostly unexplored territory in computer science. Which we are all aware with security and usability on many levels, usable security has received little operational attention. Companies have recently focused primarily on usable security. As consumers prefer to discard unsatisfactory solutions, attaining well-balanced degrees of both is a prerequisite for adequate security. Usability should be examined from the viewpoint of security to be properly assessed. The aim of this research study is to explore and discuss universally accepted and solution-independent factors influencing the perceived usable-security of institutional websites. An integrated Hesitant Fuzzy Linguistic term sets based technique was chosen as the methodology, and the experts and academicians opinion were collected. The use of predetermined selection criteria resulted in the compilation of statistical findings and were used to determine the usable-security of five different instituational websites.

Keywords: Usable security; accessibility; expert evaluation; usability criteria; fuzzy logic

1 Introduction

Technology has transformed our planet and our everyday lives over the decades. Furthermore, aging technology has provided incredible support and technologies, placing vital knowledge at our fingers. Multi-functional technologies including the smartwatch as well as smartgadgets have been made conceivable by advanced technology. Computer systems are becoming quicker, more flexible, and more prevailing than ever. Innovation has made our life easier, quicker, smarter, and more enjoyable as a result of all of these transformations. The Internet has revolutionized how we engage ourselves, interact with one another, and consume different social media platforms. It

has made interesting developments, however it has also brought significant security improvements in security systems and hospital equipment. The goal of computer or system security is to keep confidential information safe from unwanted access whilst also making it accessible to authorized people. The need for individuals to defend themselves. Users' security and valuables have always been a potential danger from intentional or unintentional destruction. Because of the increased usage of information technology, individuals and organizations now have an ever-increasing number of physical and digital assets which are at risk. To accommodate the growing demand for a secure system, the IT sector has created a variety of security methods that can be employed to considerably complicate or mitigate cyberattacks [1–4]. Conventional security comprises the use of difficult-to-understand design, engineering, and encryption. Security is one of the crucial problems of any infrastructure in an era of greater Internet spread. However, it can still be difficult for those who have technological expertise and casual online services to preserve safety. The main objective of usability is to make complicated software and hardware products simple to use for average consumers. Consequently, usability and security are still mainly different processes. Usable security necessitates a revolutionary approach to system development that guarantees both security and usability. Users are allowed to conduct security services in a usable style in this approach.

Currently, the concept of usable security has an extensive research base with hundreds of publications from social interaction, computer security, and usability to technology, finance, psychology, and sociology in dozens of peer-reviewed settings in several different fields. The discipline has prospered in making the human factor aware of how important it is to fulfill cybersecurity goals. Enterprise and creating new companies and key government activities in the United States and Europe have incorporated human awareness and understanding [5–7].

End users often regard security as an inconvenience. Incorporating security controls could influence both the functioning and the usability of the end-user. But security is similarly crucial if the program or application is to be protected from compromises. The correct balance among functionality, usability and security is, therefore, vital [8–11]. The following Fig. 1 shows the usability triangle.
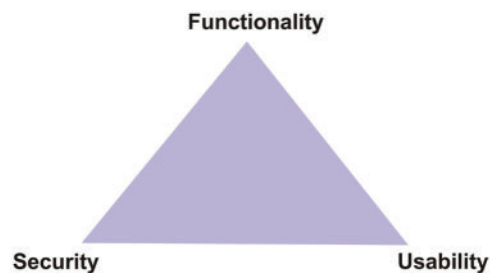
Figure 1: The usability triangle

Security checks are typically regarded overhead in an organization. More typically, there is debate amongst different stakeholders in the organization on the adoption of sustainable security rules. For instance, the entire organization would like to prioritize functionality. They rigorously wish to construct the application feature in the project's requirements stage completely as described. While end customers expect all the features to be correct, they also want to be simple to use. The easier a program may be used to satisfy end users. And afterward, security strikes. Although most security checks can be made visible to end-users, others might create overhead for

end-users like two-factor verification. However, such enhanced safety features may be necessary given the sensitive nature of the application data. Therefore, it is sometimes difficult to balance function, usability, and security, as all three are extremely and equally significant.

The rest of the paper is organized as follows. Section 2 presents related works in the usable-security domain. and Section 3 discusses the criteria selection for the usable-security evaluation. Section 4 presents an anticipated Hesitant-Fuzzy AHP TOPSIS approach to support the usable-security evaluation of institutional websites. Section 5 presents the statistical findings and comparative analysis in the study. The last Section 6 is a conclusion about the summary of the paper.

2 Related Works

The internet has evolved enormously over the last couple of decades and also has created effective communication capabilities to enhance educational and computerized information flows in the academic environment. At now, Educational institutions rely largely on online learning platforms, which offer educational material and capabilities for users as a consistent and efficient source. Academic websites may be regarded as a medium for institutional, student, and academic information as well as industry interaction. Only if overall architecture promotes characteristics of usability can educational sites make Educational institutions effective and practical. Users are impressed if the web pages fulfill the specified usability functions [12,13]. It is therefore important to evaluate the usable-security of web sites, and several scholars have made several attempts in this area.

Kumar et al. [14] evaluated the usability of two software editions over time. They used the Fuzzy-AHP methodology to analyze the priorities as well as ultimate useable security. Additionally, they quantitatively analyzed the security influence on usability & security impacts. The collected data and conclusions can be used by developers to improve the usability as well as security of software.

Kumar et al. [15] conducted rigorous literature research to identify essential factors, classify and prioritize the most essential among them using the FAHP technique, and involve targeted audiences to suggest a usability assessment tool for academic websites. They used five different websites of notable higher educational institutes (HEIs) that were examined and graded based on usability criteria to validate their proposed framework. They believed their framework would be useful in discovering real usability concerns that present in academic websites nowadays.

Muhammad et al. [16] investigated the usefulness of the software, achieving its goals, while maintaining usability, to design software with additional stability. This study primarily addressed the combination of usability and security with the qualities. They addressed usability as well as security compatibility with their contributing characteristics. They also proposed a new technique, hybrid AHP, hesitant fuzzy (HF) with TOPSIS models, to analyze usability as well as security significantly. Their usability outcomes together with the security evaluation indicate that this novel hybrid process may be the most knowledgeable strategy for deciding software security.

Agrawal et al. [17] evaluated the usable security of two different software versions labeled versions 1 and 2. The Fuzzy Analytic Hierarchy Process (Fuzzy AHP) approach was used by the researchers to evaluate usable security. Furthermore, the influence of security on usability and also the effect of usability on security were quantified in their study.

Alenezi et al. [18] defined the key security and usability variables that impact one another directly and indirectly, such as confidentiality, integrity, and availability, as well as effectiveness,

efficiency, and satisfaction. The weighting of each parameter is critical for its impact on the performance security design throughout the software development life cycle. They employed the Fuzzy AHP to assess the performance. The findings and conclusions reached can help software developers create better safe and usable applications.

Agrawal et al. [19] designed a metric for assessing the usefulness of security technologies. They suggested problem classifications for security product errors. They proposed a classification system for the usability of security properties based on this classification. Using this classification, security functions could be prioritized based on the user's capacity to prevent self-inflicted, security-critical user failures. This classification may describe possible sources of errors, as well as design choices to avoid these problems.

Although there are some recent works published in the area of usable security evaluation as summarized in Tab. 1.

Yet none of them considered the significant factors i.e., functionality, security and usability with the powerful integrated Hesitant Fuzzy AHP-TOPSIS approach for the evaluation of the usable-security. The major aim of this article is to analyse the usable-security of five distinct institutional websites. Evaluation of usable-security is a complex MCDM (multi-criteria decision making) problem and that is reason this article has utilised the Hesitant-Fuzzy AHP TOPSIS approach to assess the usable-security. The most important weighted criteria have been examined.

3 Criteria Selection for the Usable-Security Evaluation

Criteria selection is crucial step for the usable-security evaluation of different institutional websites. For this, we have selected three criteria namely Functionality, Security and Usability which are denoted as P1–P3 respectively. Fig. 2 demonstrations the hierarchy for the usable-security evaluation.

3.1 Functionality

This can be determined by the objective that something is intended to perform or is encouraged to complete. Increasing the number of functions in a program, for instance, increases the surface area which a malicious user may target when looking for a vulnerable gap.

3.2 Security

This can be considered as all of the procedures taken to safeguard a system, software, or hardware, as well as to ensure that only persons with authorization to view them can do so. A truly secure system, for instance, would be housed within a solid box without any entry points, controls, or interface and be capable of blocking all electromagnetic radiation. However, the user would be rendered ineffective because they would be unable to obtain it or use the service for its original purpose. When it comes to security, developers must keep the user perspective in mind. An investigation by IT-company and banking users discovered that many people did not intervene individually while consumers said they were motivated and aware of security. They compared work barriers to security measures. Furthermore, user behaviour was unaffected by requirements for anticipated security behaviour including awareness initiatives. However, reducing security in order to enhance functionality and usability leaves any system as well as device vulnerable to attack, thus there must be a solution to preserve the ease of use and functionality without jeopardizing security.

Table 1: Recent works on usable-security

| S. No.	Authors	Contribution	Publisher	Quartile	Reference
1.	Agrawal et al.	Multi-level fuzzy system for usable-security assessment	ICIC international	Q1	[17]
2.	Kumar et al.	A hybrid model of hesitant fuzzy decision-making analysis for estimating usable-security of software	IEEE	Q1	[14]
3.	Al-Zahrani	Evaluating the usable-security of healthcare software through unified technique of fuzzy logic, ANP and TOPSIS	IEEE	Q1	[20]
4.	Agrawal et al.	Usable-security assessment through a decision making procedure	Elsevier	Q3	[19]
5.	Alenezi et al.	Usable-security attribute evaluation using fuzzy analytic hierarchy process.	ICIC international	Q3	[18]
6.	Kumar et al.	Evaluating security tools towards usable security	TIIS	Q2	[15]
7.	Muhammad et al.	Evaluating usability of academic websites through a fuzzy analytical hierarchical process	MDPI	Q1	[16]

3.3 Usability

It can be described as the extent to which something is capable or suitable for usage. In the actual world, there is a deal between security and usability, which often results in conflict between individuals and those who manage security.

4 Hesitant-Fuzzy AHP TOPSIS Approach

Real-world decision-making challenges are typically too complicated and poorly structured to be addressed by examining a single criterion, feature, or perspective which would contribute to a

successful conclusion. In reality, such a one-dimensional approach is a misrepresentation of the true scope of the issue at hand, and it could result in irrational judgments. A more attractive strategy would be to evaluate all relevant elements linked to the challenge at the same time. Overcoming such challenges is the primary focus of multiple-criteria decision-making (MCDM). MCDM is a highly developed topic of operations research dedicated to the creation and application of decision support methods and techniques to deal with complicated choice problems containing many criteria, objectives, or targets that are in contradiction. MCDM's methods and tools are more than just statistical equations that aggregate criteria, viewpoints, or qualities; they are also decision-support dependent. As an excellent solution for such challenges, AHP is well-organized in MCDM approaches [21–25]. Typically, pair-wise comparability matrices are utilized, and the correctness is confirmed. When multiple alternatives are presented specialist decisions have a significant impact on such pair-wise evaluations. To address this issue, this study provides an integrated strategy that includes AHP to evaluate the choice criteria and TOPSIS to identify the most significant function.
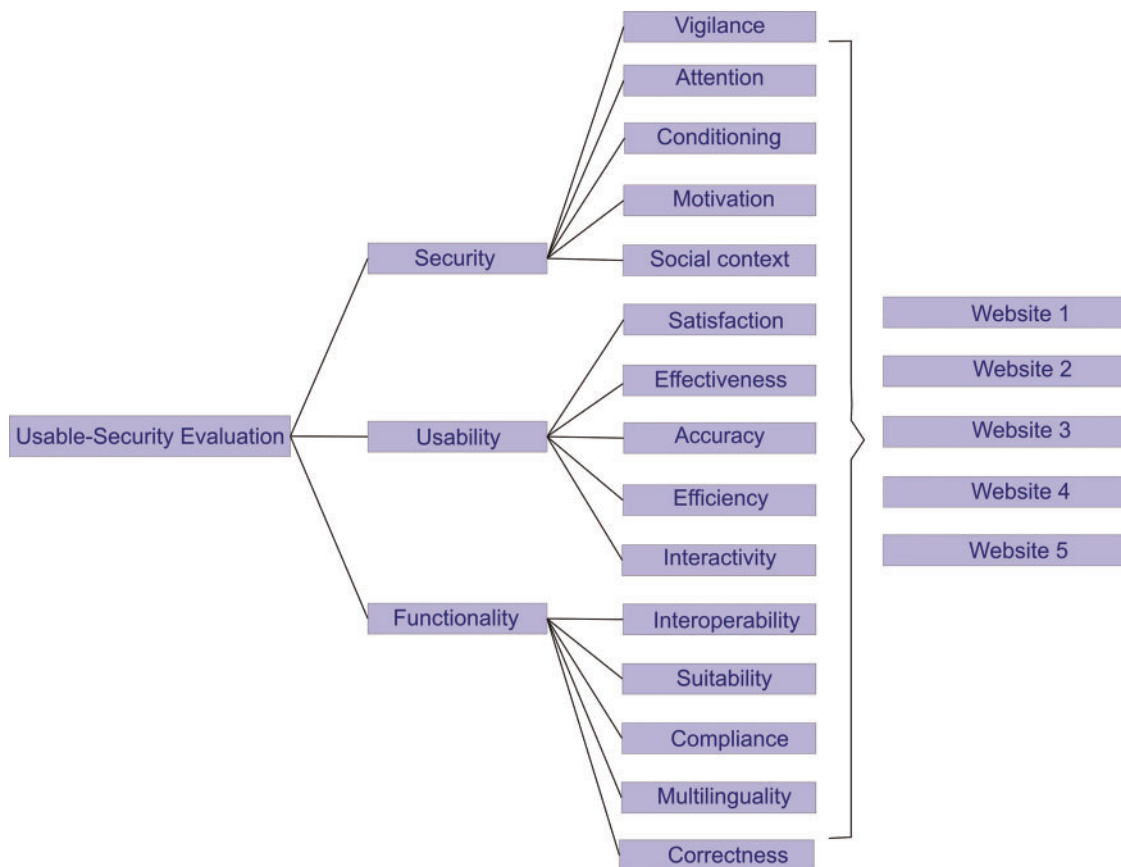
Figure 2: Hierarchy for the usable-security evaluation

To achieve more accurate assessments, the paper also employs the Hesitant-Fuzzy technique. TOPSIS comes out on top in the MCDM process because of its straightforward measuring. TOPSIS considers the excellent and optimistic outcomes when designing an efficient procedure. While these two techniques necessitate some flexibility, they are inconsistent when it approaches complicated real-world issues and must be supported by Hesitant-Fuzzy set theory. Although complication and vagueness rise, it has recently been strongly urged for the employment of type-II Hesitant-Fuzzy sets, intuitive Hesitant-Fuzzy sets, and Hesitant-Fuzzy Sets (HFS) [26–31].

Torra [32] proposed the principle of a hesitant fuzzy set (HFS) to address the difficulties in determining the level of membership of a component in a set. HFS is represented by a variety of potential membership values that is more suited to describe indecisiveness and mathematical formalism of decision-makers between numerous values to convey their own or conflicting opinions. Currently, because of the efficient process of imprecise information, HFS typically combined with the MCDM approaches and used in various fields including analysis of decisions. The HFS approach has become more important for researchers. This novel fuzzy set extension can accommodate cases where the complexity in determining the membership level is caused by the hesitation between many a few various values rather than a boundary of error (as in linguistic variables or interval-valued fuzzy sets) or a predefined potential outcome allocation of the conceivable quantity (as in type-2 fuzzy sets). In comparison to the fuzzy set as well as many other classical variants, the hesitant fuzzy logic can more accurately represent people's uncertainty in articulating their judgments over objects. Fig. 3 shows the functional diagram of the Hesitant-Fuzzy AHP TOPSIS approach utilized in this paper to evaluate the usable security of institutional websites.

The proposed analysis provided Hesitant-Fuzzy AHP to weigh the feature inside the methodology, and an integrated Hesitant-Fuzzy TOPSIS to determine the optimal function for quantitative evaluation of usable-security in this research. To determine the values of the selected key and sub-characteristics, the assessments process are implemented as follows:

Step 1: Develop a hierarchy strategy for the many ranks of objectives.

Step 2: Pair-wise assessments of those traits are performed using the language phrases in Tab. 2. Specialists are given a much broader scope to provide more reliable results.
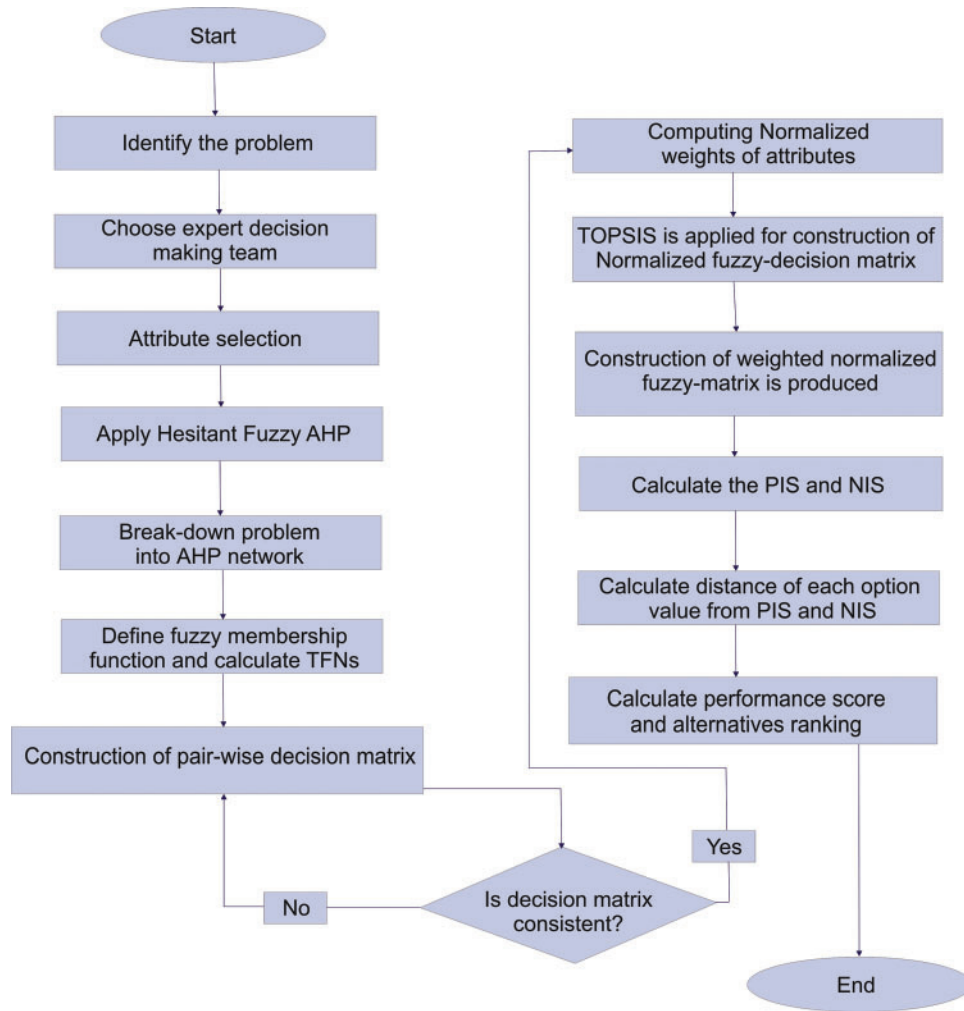
Step 3: Perform the modified statistical analysis of hesitant-fuzzy wrappers [33–35]. Assumed the T_0 is of the smallest importance and T_g is the largest importance on the linguistic scale, as well T_i and T_j have statistical assessments such as $T_0 \leq T_i \leq T_j \leq T_g$; estimate systematic weighted be an average of aspect n as in Eq. (1).

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

where OWA indicates Ordered Weighted Average. Now, $W = (w_1, w_2, \ldots . w_n)^S$ is the associated weighing vector satisfying the fomula $\sum_{i=1}^{n} W = 1$ and b_j takes significance corresponding to the highest of $a_1, a_2, \ldots . a_n$. Subsequently this calculation the HFS constraints of the trapezoidal figures $\tilde{C} = (a, b, c, d)$ as in calculation Eqs. (2)–(5).

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

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

Figure 3: Working diagram of hesitant-fuzzy AHP TOPSIS approach

$$b = \begin{cases} a_M^i, if \ i+1=j \\ \underset{w}{OWA}_2\left(a_m^j,.....a_m^{\frac{i+j}{2}}\right), if \ i+j \ is \ even \\ \underset{w}{OWA}_2\left(a_m^j,.....a_m^{\frac{i+j+1}{2}}\right), if \ i+j \ is \ odd \end{cases} \tag{4}$$

$$c = \begin{cases} a_M^{i+1}, if \ i+1=j \\ \underset{w}{OWA}_2\left(a_m^j a_m^{j-1},.....a_m^{\frac{(i+j)}{2}}\right), if \ i+j \ is \ even \\ \underset{w}{OWA}_2\left(a_m^j, a_m^{j-1}.....a_m^{\frac{(i+j+1)}{2}}\right), if \ i+j \ is \ odd \end{cases} \tag{5}$$

where L, M, and R indicate Lower, Middle and Higher values. Next step is to identify the values of 1st and 2nd types utilizing N, the unit interval numbers [0, 1] with the help of Eqs. (6), (7)

correspondingly, the values of 1st type $(W1 = (w_1^1, w_2^1, \ldots\ldots w_n^1))$:

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

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

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

With the help of Eq. $\eta_1 = \frac{g-(j-1)}{g-1}s$, and $\eta_2 = \frac{g-(j-1)}{g-1}$ where g is the greatest number in statistical modelling (g is 10 as per Tab. 2), and i and j are correspondingly the lower and the highest ranks of quantitative analysis.

Table 2: Scale for hesitant-fuzzy ahp approach

Rank	Abbreviation	Linguistic term	Triangular hesitant-fuzzy number
10	AHI	Absolutely high importance	(7, 9, 9)
9	VHI	Very high importance	(5, 7, 9)
8	ESHI	Essentially high importance	(3, 5, 7)
7	WHI	Weakly high importance	(1, 3, 5)
6	EHI	Equally high importance	(1, 1, 3)
5	EE	Exactly equal	(1, 1, 1)
4	ELI	Equally low importance	(0.33, 1, 1)
3	WLI	Weakly low important	(0.2, 0.33, 1)
2	ESLI	Essentially low importance	(0.14, 0.2, 0.33)
1	VLI	Very low importance	(0.11, 0.14, 0.2)
0	ALI	Absolutely low importance	(0.11, 0.11, 0.14)

Step 4: Take up the pairwise comparative matrix ($\tilde{A}$) as in Eqs. (8), (9).

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

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

Step 5: By using Eq. (10), defuzzify a trapezoidal Hesitant-Fuzzy number as d = (l, m$_1$, m$_2$, h) which generates a crisp number

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

Calculate the normal Consistency Ratio (CR) with the help of Eqs. (11), (12) [36–39].

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

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

where CI denotes the consistency index, $\lambda_{\max}$ is the matrix's biggest eigenvector, denotes the number of conditions in the current quantitative evaluation and RI is a randomly decided ready-to-use index (the random index) that differs for different n values. Continue if the CR value is less than 0.1; alternatively, continue to the second stage and repeat the computational analyses.

Step 6: Determine the geometric mean for each row with the help of Eq. (13).

$$\tilde{r}_i = \left(\tilde{c}_{i1} \bigotimes \tilde{c}_{i2} \ldots \ldots \bigotimes \tilde{c}_{in} \right)^{\frac{1}{n}} \tag{13}$$

Step 7: Each highest features weight is measured with the help of Eq. (14).

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

Step8: Defuzzify all the HFS with the support of Eq. (15).

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

Step 9: With the support of Eq. (16), Normalize weights are evaluated from defuzzified weights.

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

The subsequent phase is for the Hesitant-Fuzzy TOPSIS to determine the optimal solution. TOPSIS assists specialists to choose a superior alternative to real-world situations as a frequently utilized MCDM approach [40,41]. TOPSIS has been presented by Kumar et al. [35]. TOPSIS is the traditional way to resolve the challenge of multiple criteria decision-making, the initial TOPSIS approach only addresses the problem of multi-attribute decision, when both the weight values and the attribute values are precise, in fact affecting its expertise, understanding, etc. [34–36]. This paper used a hesitant and uncertain approach to fixing the issues of not easy to evaluate and accurate the exact result of membership in simulating the complicated psychology of decision-makers, using the expanded form of fuzzy sets, dissenting fuzzyness elements [14,15], and by redefining hesitant, fuzzy distance measurements. For these concerns in this paper, this is predicated on the perception that the determining factor is the highest overall for all aspects, while the negative form has all the worse features. The technique depend on on the use of covers to evaluate the distance from H1s to H2s, for instance. Assumed the envelopes, env (H1s) = $[T_p, T_q]$ and $env(H2s) = [T_p^*, T_q^*]$, the distance is demarcated as Eq. (17):

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

The process can further be demarcated as:

Step 10: For the first step let's undertake that

- The decision under contemplation has E alternatives ($C = \{C_1, C_2, \ldots .C_E\}$) and n criteria ($C = \{C_1, C_2, \ldots .C_n\}$)
- The specialists are specified with e_x and the quantity of experts is K

- $\tilde{X}^l = \left[H_{S_{ij}}^l \right]_{E \times n}$ is a Hesitant-Fuzzy decision matrix where $H_{S_{ij}}^l$ is the mathematical analysis score for alternative i(C_i) in contradiction of criteria j(A_j) quantified by experts e_x.
- The scale for Hesitant-Fuzzy TOPSIS is indicated as:

Assume $Scale = \{nothing,\ very\ bad,\ bad,\ medium,\ good,\ very\ good,\ and\ perfect\}$ be a verbal or linguistic term set also CH be the context-free grammar for generating its relative linguistic terms. Similarly, take two specialists' e1 and e2 to deliver their level for two standards A1 and A2,

$r_1^1 = between\ medium\ and\ good$ (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)

The Hesitant-Fuzzy envelope for respective comparative linguistic expression is calculated as the succeeding [9]:

$env_F(EGH\ (btM\&G)) = T\ (0.33,\ 0.5,\ 0.67,\ 0.83)$

$env_F(EGH\ (amM)) = T\ (0,\ 0,\ 0.35,\ 0.67)$

$env_F(EGH\ (alG)) = T\ (0.5,\ 0.85,\ 1,\ 1)$

$env_F(EGH\ (btVB\&M)) = T\ (0,\ 0.3,\ 0.37,\ 0.66)$

Step 11: Compile the expert's unique statistical assessments. $\left(\tilde{X}^1, \tilde{X}^2 \ldots \ldots \tilde{X}^K \right)$ and build an accumulated decision matrix X = [x_{ij}] in which x_{ij} signifies the statistical evaluation core of C_i in contradiction of A_j and statistically characterized as $x_{ij} = [T_{pij},\ T_{qij}]$ like Eq. (18).

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

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

Step 12: Let α_b better numbers in represent assistance features where higher numbers in A_j mean greater predilection and α_c represents cost criteria where lower standards in A_j designate more predilection.

Undertake that the Hesitant-Fuzzy Linguistic Term Set (HFLTS) positive ideal solution is on condition that with $\tilde{C}^+$ and arithmetically represented as $\tilde{C}^+ = (\tilde{V}_1^+, \tilde{V}_2^+, \ldots \tilde{V}_n^+)$ where $\tilde{V}_j^+ = \left[V_{pj}^+, V_{qj}^+ \right] (j = 1, 2, 3 \ldots .n)$ and the HFLTS negative ideal solution is represented as $\tilde{C}^-$ and statistically denoted as $\tilde{C}^- = (\tilde{V}_1^-, \tilde{V}_2^-, \ldots \tilde{V}_n^-)$ where $\tilde{V}_j^- = \left[V_{pj}^-, V_{qj}^- \right] (j = 1, 2, 3 \ldots .n)$

Define $\tilde{V}_{pj}^+$, $\tilde{V}_{qj}^+$, $\tilde{V}_{pj}^-$ and $\tilde{V}_{qj}^-$ for cost as well as benefit criteria like Eqs. (19)–(22).

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

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

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

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

Step 13: With the support of Eqs. (23), (24), make the positive and negative ideal separation matrixes (D^+ and D^-), correspondingly.

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

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

Step 14: Determine the relative closeness total for each alternative under contemplation through Eqs. (25), (26).

$$CS\left(A_i\right) = \frac{D_i^+}{D_i^+ + D_i^-}, i = 1, 2, \ldots .m \qquad (25)$$

where

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

Step 15: Arrange the alternatives on the basis of associated relative closeness totals.

The subsequent section implements data analysis as well as outcomes using combined Hesitant-Fuzzy AHP-TOPSIS.

5 Data Analysis and Results

5.1 Statistical Findings

The evaluation of the security usability of five distinct institutional websites is a difficult task. The institutional websites offer dependable and efficient serviceable performance, using suitable mathematical investigation of the criteria and alternatives. The researchers have taken the symmetrical method to the results from Hesitant-Fuzzy AHP and Hesitant-Fuzzy TOP-SIS together. Tab. 2 and Eqs. (1)–(17) are utilized for the quantitative simulation of attributes. Tab. 3 generates Eq. (18) parallel matrix comparability. The linguistic numbers of the alternatives as respects the alternative were assessed; the linguistic values generated from the TFN were assessed. The standardized decision matrix Hesitant-Fuzzy has been constructed with Eqs. (19)–(23). The Hesitant-Fuzzy Comparison Matrix for Security, Usability, and Functionality is shown in Tabs. 4–6, respectively. The global weights through the hierarchy are shown in Tab. 7. Further, Tab. 8 provides additional subjective cognition conclusions of experts in language terms. Tab. 9 displays the weighted normalized fuzzy-decision matrix. Eqs. (24), (25) analyze the proximity coefficients of the variables to determine the value of d_i^+ and d_i^-. The value of closeness (CC_i^+) is assimilated with the help of Eq. (26) and present in Tab. 10 and Fig. 4. To calculate the

usable security of five some institutional websites, the different performance factors are determined by five alternative solutions; these alternatives are extremely sensitive to computational resolution.

Table 3: TFN values of characteristics

	P1	P2	P3
P1	1.00000, 1.00000, 1.00000, 1.00000	3.00000, 5.00000, 7.00000, 9.00000	1.00000, 1.00000, 3.00000, 5.00000
P2	0.11000, 0.14300, 0.20000, 0.33000	1.00000, 1.00000, 1.00000, 1.00000	0.20000, 0.33000, 1.00000, 1.00000
P3	0.20000, 0.33000, 1.00000, 1.00000	1.00000, 1.00000, 3.00000, 5.00000	1.00000, 1.00000, 1.00000, 1.00000

Table 4: Pair-wise hesitant-fuzzy assessment matrix for security

	P11	P12	P13	P14	P15	Local weights
P11	1.00000, 1.00000, 1.00000, 1.00000	1.00000, 1.00000, 1.00000, 1.00000	0.20000, 0.33000, 1.00000, 1.00000	1.00000, 1.00000, 5.00000, 7.00000	1.00000, 1.00000, 5.00000, 7.00000	0.04800, 0.15700, 0.27100, 1.02500
P12	3.00000, 1.00000, 1.00000, 0.33000	1.00000, 1.00000, 1.00000, 1.00000	1.00000, 1.00000, 1.00000, 1.00000	1.00000, 3.00000, 5.00000, 7.00000	0.33000, 1.00000, 1.00000, 3.00000	0.03300, 0.12900, 0.21200, 0.78100
P13	1.00000, 1.00000, 3.00000, 5.00000	1.00000, 1.00000, 1.00000, 1.00000	1.00000, 1.00000, 1.00000, 1.00000	1.00000, 1.00000, 5.00000, 7.00000	1.00000, 1.00000, 5.00000, 7.00000	0.06400, 0.24000, 0.42600, 1.21400
P14	3.00000, 1.00000, 1.00000, 0.33000	1.00000, 1.00000, 3.00000, 5.00000	1.00000, 1.00000, 1.00000, 1.00000	1.00000, 1.00000, 1.00000, 1.00000	1.00000, 1.00000, 5.00000, 7.00000	0.05200, 0.15900, 0.29700, 1.02500
P15	0.14000, 0.20000, 1.00000, 1.00000	3.00000, 1.00000, 1.00000, 1.00000	1.00000, 1.00000, 3.00000, 5.00000	1.00000, 1.00000, 1.00000, 1.00000	1.00000, 1.00000, 1.00000, 1.00000	0.02200, 0.07300, 0.11300, 0.50300

Table 5: Pair-wise hesitant-fuzzy assessment matrix for usability

	P21	P22	P23	P24	P25	Local weights
P21	1.00000,	0.33000,	0.14000,	1.00000,	1.00000,	0.05000,
	1.00000,	1.00000,	0.20000,	1.00000,	1.00000,	0.16000,
	1.00000,	1.00000,	1.00000,	3.00000,	5.00000,	0.28000,
	1.00000	3.00000	1.00000	5.00000	7.00000	1.01000
P22	3.00000,	1.00000,	0.33000,	0.20000,	0.11000,	0.03500,
	1.00000,	1.00000,	1.00000,	0.33000,	0.14000,	0.16600,
	1.00000,	1.00000,	1.00000,	1.00000,	0.33000,	0.22600,
	0.33000	1.00000	3.00000	1.00000	1.00000	0.62000
P23	1.00000,	3.00000,	1.00000,	0.33000,	1.00000,	0.06400,
	1.00000,	1.00000,	1.00000,	1.00000,	1.00000,	0.24000,
	5.00000,	1.00000,	1.00000,	1.00000,	3.00000,	0.42600,
	7.00000	0.33000	1.00000	3.00000	5.00000	1.21400
P24	0.20000,	1.00000,	3.00000,	1.00000,	1.00000,	0.05200,
	0.33000,	1.00000,	1.00000,	1.00000,	1.00000,	0.15900,
	1.00000,	3.00000,	1.00000,	1.00000,	3.00000,	0.29700,
	1.00000	5.00000	0.33000	1.00000	5.00000	1.02500
P25	0.14000,	1.00000,	0.20000,	0.20000,	1.00000,	0.03300,
	0.20000,	3.00000,	0.30300,	0.33000,	1.00000,	0.08600,
	1.00000,	7.00000,	1.00000,	1.00000,	1.00000,	0.18000,
	1.00000	9.00000	1.00000	1.00000	1.00000	0.49800

Table 6: Pair-wise hesitant-fuzzy assessment matrix for functionality

	P31	P32	P33	P34	P35	Local weights
P31	1.00000,	1.00000,	3.00000,	1.00000,	1.00000,	0.055000,
	1.00000,	1.00000,	1.00000,	1.00000,	1.00000,	0.161000,
	1.00000,	3.00000,	1.00000,	1.00000,	3.00000,	0.282000,
	1.00000	5.00000	0.33000	1.00000	5.00000	1.012500
P32	0.14000,	1.00000,	1.00000,	1.00000,	1.00000,	0.035130,
	0.20000,	1.00000,	1.00000,	3.00000,	1.00000,	0.167400,
	1.00000,	1.00000,	1.00000,	5.00000,	1.00000,	0.225500,
	1.00000	1.00000	1.00000	7.00000	1.00000	0.615200
P33	1.00000,	3.00000,	1.00000,	1.00000,	1.00000,	0.059100,
	1.00000,	1.00000,	1.00000,	1.00000,	1.00000,	0.211000,
	5.00000,	1.00000,	1.00000,	5.00000,	3.00000,	0.351000,
	7.00000	0.33000	1.00000	7.00000	5.00000	1.262000

Table 6: Pair-wise hesitant-fuzzy assessment matrix for functionality

	P31	P32	P33	P34	P35	Local weights
P34	0.20000,	1.00000,	1.00000,	1.00000,	1.00000,	0.053500,
	0.33000,	1.00000,	1.00000,	1.00000,	1.00000,	0.131200,
	1.00000,	3.00000,	1.00000,	1.00000,	3.00000,	0.275100,
	1.00000	5.00000	1.00000	1.00000	5.00000	0.953000
P35	0.14000,	1.00000,	0.20000,	0.20000,	1.00000,	0.032610,
	0.20000,	3.00000,	0.33000,	0.33000,	1.00000,	0.086000,
	1.00000,	7.00000,	1.00000,	1.00000,	1.00000,	0.182000,
	1.00000	9.00000	1.00000	1.00000	1.00000	0.498000

Table 7: Global weights assigned to each level of the hierarchy

At level 1	Local weights at level 1	At level 2	Local weights at level 2	Global weights at level 2	Normalized global weights
	0.0317,		0.04800,	0.016058,	0.055268
	0.0782,		0.15700,	0.060500,	
	0.0472,		0.27100,	0.120520,	
	0.5745		1.02500	0.580020	
			0.03300,	0.011060,	0.011499
			0.12900,	0.060278,	
			0.21200,	0.101000,	
			0.78100	0.356100	
			0.06400,	0.019057,	0.094877
			0.24000,	0.079400,	
			0.42600,	0.156050,	
			1.21400	0.723800	
			0.05200,	0.017091,	0.046311
			0.15900,	0.049016,	
			0.29700,	0.125020,	
			1.02500	0.545070	
			0.02200,	0.010094,	0.083855
			0.07300,	0.032502,	
			0.11300,	0.080400,	
			0.50300	0.286100	
	0.0928,		0.050000,	0.004400,	0.067479
	0.1223,		0.16000,	0.019200,	
	0.1711,		0.280000,	0.046360,	
	0.2783		1.01000	0.285250	

(Continued)

Table 7: Continued

At level 1	Local weights at level 1	At level 2	Local weights at level 2	Global weights at level 2	Normalized global weights
			0.03500, 0.16600, 0.22600, 0.62000	0.003000, 0.015700, 0.036270, 0.217300	0.051999
			0.06400, 0.24000, 0.42600, 1.21400	0.005903, 0.029300, 0.072800, 0.337800	0.087872
			0.05200, 0.15900, 0.29700, 1.02500	0.004820, 0.019400, 0.050810, 0.285200	0.069030
			0.03300, 0.08600, 0.18000, 0.49800	0.002000, 0.008900, 0.019330, 0.139900	0.031811
	0.0928, 0.0223, 0.0711, 0.2783		0.055000, 0.161000, 0.282000, 1.012500	0.017910, 0.049160, 0.125200, 0.545700	0.083855
			0.035130, 0.167400, 0.225500, 0.615200	0.010940, 0.032520, 0.080400, 0.286100	0.067479
			0.059100, 0.211000, 0.351000, 1.262000	0.004400, 0.019200, 0.046360, 0.285250	0.051999
			0.053500, 0.131200, 0.275100, 0.953000	0.003000, 0.015700, 0.036270, 0.217300	0.087872
			0.032610, 0.086000, 0.182000, 0.498000	0.005930, 0.029300, 0.072800, 0.337800	0.067479

Table 8: Expert's subjective cognition findings in linguistic terms

	A1	A2	A3	A4	A5
P11	0.5000, 0.8500, 1.0000, 1.0000	0.0000, 0.0000, 0.3500, 0.6700	0.5000, 0.8500, 1.0000, 1.0000	0.0000, 0.0000, 0.3500, 0.6700	0.3300, 0.5000, 0.6700, 0.8300
P12	0.0000, 0.3000, 0.3700, 0.6700	0.5000, 0.8500, 1.0000, 1.0000	0.0000, 0.3000, 0.3700, 0.6700	0.0000, 0.3000, 0.3700, 0.6700	0.5000, 0.8500, 1.0000, 1.0000
P13	0.0000, 0.3000, 0.3700, 0.6700	0.0000, 0.3000, 0.3700, 0.6700	0.0000, 0.3000, 0.3700, 0.6700	0.0000, 0.3000, 0.3700, 0.6700	0.0000, 0.0000, 0.3500, 0.6700
P14	0.5000, 0.8500, 1.0000, 1.0000	0.5000, 0.8500, 1.0000, 1.0000	0.5000, 0.8500, 1.0000, 1.0000	0.0000, 0.0000, 0.3500, 0.6700	0.3300, 0.5000, 0.6700, 0.8300
P15	0.0000, 0.3000, 0.3700, 0.6700	0.0000, 0.3000, 0.3700, 0.6700	0.0000, 0.3000, 0.3700, 0.6700	0.0000, 0.3000, 0.3700, 0.6700	0.5000, 0.8500, 1.0000, 1.0000
P21	0.5000, 0.8500, 1.0000, 1.0000	0.5000, 0.8500, 1.0000, 1.0000	0.0000, 0.0000, 0.3500, 0.6700	0.3300, 0.5000, 0.6700, 0.8300	0.0000, 0.0000, 0.3500, 0.6700
P22	0.0000, 0.3000, 0.3700, 0.6700	0.0000, 0.3000, 0.3700, 0.6700	0.5000, 0.8500, 1.0000, 1.0000	0.0000, 0.0000, 0.3500, 0.6700	0.3300, 0.5000, 0.6700, 0.8300
P23	0.5000, 0.8500, 1.0000, 1.0000	0.0000, 0.0000, 0.3500, 0.6700	0.3300, 0.5000, 0.6700, 0.8300	0.0000, 0.3000, 0.3700, 0.6700	0.5000, 0.8500, 1.0000, 1.0000
P24	0.0000, 0.3000, 0.3700, 0.6700	0.0000, 0.3000, 0.3700, 0.6700	0.5000, 0.8500, 1.0000, 1.0000	0.0000, 0.0000, 0.3500, 0.6700	0.3300, 0.5000, 0.6700, 0.8300
P25	0.5000, 0.8500, 1.0000, 1.0000	0.0000, 0.0000, 0.3500, 0.6700	0.3300, 0.5000, 0.6700, 0.8300	0.0000, 0.3000, 0.3700, 0.6700	0.5000, 0.8500, 1.0000, 1.0000
P31	0.0000, 0.3000, 0.3700, 0.6700	0.0000, 0.3000, 0.3700, 0.6700	0.5000, 0.8500, 1.0000, 1.0000	0.0000, 0.0000, 0.3500, 0.6700	0.3300, 0.5000, 0.6700, 0.8300
P32	0.5000, 0.8500, 1.0000, 1.0000	0.0000, 0.0000, 0.3500, 0.6700	0.3300, 0.5000, 0.6700, 0.8300	0.0000, 0.3000, 0.3700, 0.6700	0.5000, 0.8500, 1.0000, 1.0000
P33	0.5000, 0.8500, 1.0000, 1.0000	0.0000, 0.0000, 0.3500, 0.6700	0.3300, 0.5000, 0.6700, 0.8300	0.0000, 0.0000, 0.3500, 0.6700	0.3300, 0.5000, 0.6700, 0.8300
P34	0.0000, 0.3000, 0.3700, 0.6700	0.0000, 0.3000, 0.3700, 0.6700	0.5000, 0.8500, 1.0000, 1.0000	0.0000, 0.3000, 0.3700, 0.6700	0.5000, 0.8500, 1.0000, 1.0000
P35	0.0000, 0.3000, 0.3700, 0.6700	0.0000, 0.3000, 0.3700, 0.6700	0.0000, 0.0000, 0.3500, 0.6700	0.0000, 0.3000, 0.3700, 0.6700	0.0000, 0.0000, 0.3500, 0.6700

Table 9: The weighted normalized fuzzy-decision matrix

	A1	A2	A3	A4	A5
P11	0.04192750, 0.07127675, 0.08385500, 0.08385500	0.00000000, 0.00000000, 0.02934925, 0.05618285	0.04192750, 0.07127675, 0.08385500, 0.08385500	0.04192750, 0.07127675, 0.08385500, 0.08385500	0.00000000, 0.00000000, 0.02934925, 0.05618285

(Continued)

Table 9: Continued

|	A1	A2	A3	A4	A5
P12	0.00000000, 0.02024370, 0.02496723, 0.04521093	0.00000000, 0.02024370, 0.02496723, 0.04521093	0.00000000, 0.02024370, 0.02496723, 0.04521093	0.00000000, 0.02024370, 0.02496723, 0.04521093	0.00000000, 0.02024370, 0.02496723, 0.04521093
P13	0.04192750, 0.07127675, 0.08385500, 0.08385500	0.00000000, 0.00000000, 0.02934925, 0.05618285	0.00000000, 0.02024370, 0.02496723, 0.04521093	0.04192750, 0.07127675, 0.08385500, 0.08385500	0.00000000, 0.00000000, 0.02934925, 0.05618285
P14	0.00000000, 0.02024370, 0.02496723, 0.04521093	0.00000000, 0.02024370, 0.02496723, 0.04521093	0.04192750, 0.07127675, 0.08385500, 0.08385500	0.00000000, 0.02024370, 0.02496723, 0.04521093	0.00000000, 0.02024370, 0.02496723, 0.04521093
P15	0.00000000, 0.02024370, 0.02496723, 0.04521093	0.00000000, 0.02024370, 0.02496723, 0.04521093	0.00000000, 0.02024370, 0.02496723, 0.04521093	0.00000000, 0.02024370, 0.02496723, 0.04521093	0.00000000, 0.02024370, 0.02496723, 0.04521093
P21	0.04192750, 0.07127675, 0.08385500, 0.08385500	0.00000000, 0.00000000, 0.02934925, 0.05618285	0.04192750, 0.07127675, 0.08385500, 0.08385500	0.04192750, 0.07127675, 0.08385500, 0.08385500	0.00000000, 0.00000000, 0.02934925, 0.05618285
P22	0.04192750, 0.07127675, 0.08385500, 0.08385500	0.00000000, 0.00000000, 0.02934925, 0.05618285	0.00000000, 0.02024370, 0.02496723, 0.04521093	0.04192750, 0.07127675, 0.08385500, 0.08385500	0.00000000, 0.00000000, 0.02934925, 0.05618285
P23	0.04192750, 0.07127675, 0.08385500, 0.08385500	0.00000000, 0.00000000, 0.02934925, 0.05618285	0.04192750, 0.07127675, 0.08385500, 0.08385500	0.00000000, 0.00000000, 0.02934925, 0.05618285	0.03373950, 0.05735715, 0.06747900, 0.06747900
P24	0.00000000, 0.02024370, 0.02496723, 0.04521093	0.00000000, 0.02024370, 0.02496723, 0.04521093	0.00000000, 0.02024370, 0.02496723, 0.04521093	0.00000000, 0.02024370, 0.02496723, 0.04521093	0.02767215, 0.04192750, 0.05618285, 0.06959965
P25	0.04192750, 0.07127675, 0.08385500, 0.08385500	0.00000000, 0.00000000, 0.02934925, 0.05618285	0.04192750, 0.07127675, 0.08385500, 0.08385500	0.00000000, 0.00000000, 0.02934925, 0.05618285	0.02767215, 0.04192750, 0.05618285, 0.06959965
P31	0.00000000, 0.02024370, 0.02496723, 0.04521093	0.00000000, 0.02024370, 0.02496723, 0.04521093	0.00000000, 0.02024370, 0.02496723, 0.04521093	0.00000000, 0.02024370, 0.02496723, 0.04521093	0.02767215, 0.04192750, 0.05618285, 0.06959965

(Continued)

Table 9: Continued

	A1	A2	A3	A4	A5
P32	0.00000000, 0.02024370, 0.02496723, 0.04521093	0.00000000, 0.02024370, 0.02496723, 0.04521093	0.00000000, 0.02024370, 0.02496723, 0.04521093	0.00000000, 0.02024370, 0.02496723, 0.04521093	0.03373950, 0.05735715, 0.06747900, 0.06747900
P33	0.04192750, 0.07127675, 0.08385500, 0.08385500	0.00000000, 0.00000000, 0.02934925, 0.05618285	0.04192750, 0.07127675, 0.08385500, 0.08385500	0.00000000, 0.00000000, 0.02934925, 0.05618285	0.02767215, 0.04192750, 0.05618285, 0.06959965
P34	0.04192750, 0.07127675, 0.08385500, 0.08385500	0.00000000, 0.00000000, 0.02934925, 0.05618285	0.04192750, 0.07127675, 0.08385500, 0.08385500	0.00000000, 0.00000000, 0.02934925, 0.05618285	0.02767215, 0.04192750, 0.05618285, 0.06959965
P35	0.00000000, 0.02024370, 0.02496723, 0.04521093	0.00000000, 0.02024370, 0.02496723, 0.04521093	0.03373950, 0.05735715, 0.06747900, 0.06747900	0.00000000, 0.02024370, 0.02496723, 0.04521093	0.03373950, 0.05735715, 0.06747900, 0.06747900

Table 10: 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}
A1	0.82812547	0.00952558	0.989885747	0.010658779
A2	0.75785454	0.01798574	0.976774593	0.023885674
A3	0.82874547	0.00974574	0.989745475	0.013652411
A4	0.75755644	0.01785647	0.976745787	0.023556987
A5	0.82885477	0.00944587	0.989457489	0.015562358
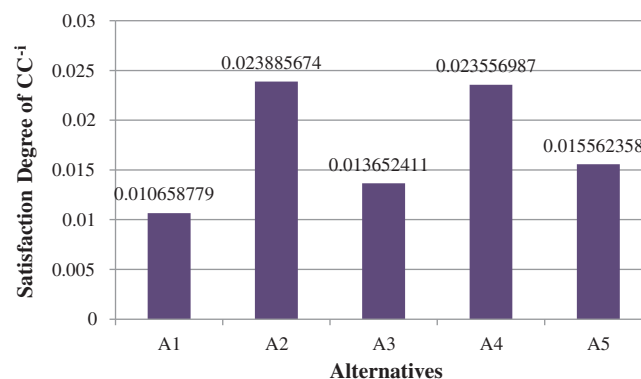
**Figure 4:** Graphical representation of satisfaction degree

5.2 Comparative Analysis

This paper uses a range of strategies for additional assessment and verification of the approach's dependability and effectiveness. In this research, the usefulness of institutional Websites

was analyzed utilizing integrated Hesitant-Fuzzy AHP and Hesitant-Fuzzy TOPSIS. The investigator compared the outcomes with four different approaches shown in Tab. 11 and Fig. 5. In a standard AHP-TOPSIS data interpretation and measured study are comparable to Hesitant-Fuzzy AHP TOPSIS, but no instability is used. Hesitant-Fuzzy TOPSIS with Hesitant-Fuzzy AHP is improved and supported in terms of dependability and performance than other approaches.

Table 11: Comparison with other fuzzy techniques

Alternatives Alternatives	Hesitant fuzzy AHP-TOPSIS	Fuzzy AHP-TOPSIS	Fuzzy ANP-TOPSIS	Classical AHP-TOPSIS	Classical ANP-TOPSIS
A1	0.010658779	0.010645441	0.010655847	0.010659658	0.010685665
A2	0.023885674	0.023854847	0.023877456	0.023885632	0.023855473
A3	0.013652411	0.013655644	0.013652545	0.013625897	0.013655471
A4	0.023556987	0.023744547	0.023554574	0.023554645	0.023545455
A5	0.015562358	0.015745645	0.015561452	0.015655455	0.015564441
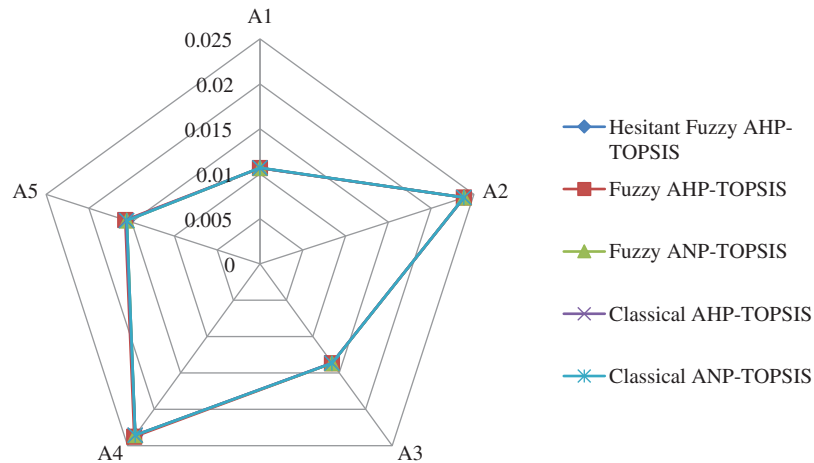
Figure 5: Radar chart representation of comparison with other fuzzy techniques

6 Conclusions

Identifying the correct balance between security as well as usability is a demanding task, from software engineers to network managers, for everyone involved in IT security. One of the primary causes of a security system failing is a lack of balance between these two components. When it approaches to harmonizing functionality, usability, with security in architecture, no functional operating system would ever be completely secure; therefore, every system/security developer and, inevitably, the user must end up settling on a negotiated settlement among appropriate functionality and usability, and acceptable security. For the security evaluation of the five different institutional sites in Uttar Pradesh, India based on sustainability factors, an integrated Hesitant-Fuzzy AHP-TOPSIS model has been designed. The investigation revealed that option A2 has

shown particularly good security usability compared to A4, A5, A3, and A1 alternatives. A relative analysis was subsequently showed to show the accuracy of the findings. The suggested technique has shown effectiveness to support decision-makers and establish confidence in assessing usable security to promote sustainable user-friendly security practice.

Key significances of this research work are as follows:

- Evaluating the usable-security would enhance productivity and user satisfaction, resulting in more secure systems for the convenience of the users.
- Throughout software development, emphasizing on usable-security qualities may increase the acceptability of secure applications.
- To improve the overall usability of programs, user error prevention is the most significant and relevant aspect of usable-security.
- Powerful methodologies like Hesitant-Fuzzy AHP TOPSIS approach appear to be more effective than classical AHP, and hence develop as a promising hybrid strategy for usable-security determination.

The majority of companies recognize quickly changing commercial and regulatory requirements as reasons to change how security (essentially preserving CIA security tried) is handled during the software development stage The present study gives a quantitative evaluation to boost the performance of security usability of applications. Overall, this work evaluates software usability and security, emphasizing the need of user error prevention and accessibility while building usable and secure systems.

Furthermore, a limitation of this research is that the security experts were clear that they were in decision making experimental situation, and because of that they were at no significant risk. A future work of this research in which security experts/participants might be encouraged to have a high motive for securing the data as if they were their personal would effectively tackle this problem.

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

References

[1] 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.

[2] M. T. J. Ansari, D. Pandey and M. Alenezi, "STORE: Security threat oriented requirements engineering methodology," *Journal of King Saud University-Computer and Information Sciences*, article in press, pp. 1–18, 2018. https://doi.org/10.1016/j.jksuci.2018.12.005.

[3] A. Attaallah, M. Ahmad, M. T. J. Ansari, A. K. Pandey, R. Kumar *et al.,* "Device security assessment of internet of healthcare things," *Intelligent Automation & Soft Computing*, vol. 27, no. 2, pp. 593–603, 2021.

[4]   M. T. J. Ansari, A. Baz, H. Alhakami, W. Alhakami, R. Kumar *et al.,* "P-STORE: Extension of store methodology to elicit privacy requirements," *Arabian Journal for Science and Engineering*, article in press, pp. 1–24, 2021. https://doi.org/10.1007/s13369-021-05476-z.

[5]   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.

[6]   M. T. J. Ansari and D. Pandey, "An integration of threat modeling with attack pattern and misuse case for effective security requirement elicitation," *International Journal of Advanced Research in Computer Science*, vol. 8, no. 3, pp. 1–18, 2017.

[7]   R. Kumar, M. Alenezi, M. T. J. Ansari, B. Gupta, A. Agrawal *et al.,* "Evaluating the impact of malware analysis techniques for securing web applications through a decision-making framework under fuzzy environment," *International Journal of Intelligent Engineering and Systems*, vol. 13, no. 6, pp. 94–109, 2020.

[8]   F. A. Alzahrani, M. Ahmad, M. Nadeem, R. Kumar and R. A. Khan, "Integrity assessment of medical devices for improving hospital services," *Computers, Materials & Continua*, vol. 67, no. 3, pp. 3619–3633, 2021.

[9]   W. Alosaimi, R. Kumar, A. Alharbi, H. Alyami, A. Agrawal *et al.,* "Computational technique for effectiveness of treatments used in curing sars-cov-2," *Intelligent Automation & Soft Computing*, vol. 28, no. 3, pp. 617–628, 2021.

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

[11] K. Sahu, F. A. Alzahrani, R. K. Srivastava and R. Kumar, "Evaluating the impact of prediction techniques: Software reliability perspective," *Computers, Materials & Continua*, vol. 67, no. 2, pp. 1471–1488, 2021.

[12] R. Kumar, S. A. Khan and R. A. Khan, "Fuzzy analytic hierarchy process for software durability: Security risks perspective," *Advances in Intelligent Systems and Computing*, vol. 508, pp. 469–478, 2017.

[13] R. Kumar, S. A. Khan and R. A. Khan, "Secure serviceability of software: Durability perspective," *Communications in Computer and Information Science*, vol. 628, pp. 104–110, 2016.

[14] R. Kumar, A. I. Khan, Y. B. Abushark, M. M. Alam, A. Agrawal *et al.,* "An integrated approach of fuzzy logic, AHP and TOPSIS for estimating usable-security of web applications," *IEEE Access*, vol. 8, no. 8, pp. 50944–50957, 2020.

[15] R. Kumar, M. T. J. Ansari, A. Baz, H. Alhakami, A. Agrawal *et al.,* "A multi-perspective benchmarking framework for estimating usable-security of hospital management system software based on fuzzy logic, ANP and TOPSIS methods," *KSII Transactions on Internet and Information Systems*, vol. 15, no. 1, pp. 240–263, 2021.

[16] A. Muhammad, A. Siddique, Q. N. Naveed, U. Khaliq, A. M. Aseere *et al.,* "Evaluating usability of academic websites through a fuzzy analytical hierarchical process," *Sustainability*, vol. 13, no. 4, pp. 1–21, 2021.

[17] A. Agrawal, M. Alenezi, D. Pandey, R. Kumar and R. A. Khan, "Usable-security assessment through a decision making procedure," *ICIC Express Letters*, vol. 10, no. 8, pp. 665–672, 2019.

[18] M. Alenezi, R. Kumar, A. Agrawal and R. A. Khan, "Usable-security attribute evaluation using fuzzy analytic hierarchy process," *ICIC Express Letters*, vol. 13, no. 6, pp. 453–460, 2018.

[19] A. Agrawal, M. Alenezi, S. A. Khan, R. Kumar and R. A. Khan, "Multi-level fuzzy system for usable-security assessment," *Journal of King Saud University-Computer and Information Sciences*, article in press, pp. 1–9, 2019. https://doi.org/10.1016/j.jksuci.2019.04.007.

[20] F. A. Alzhrani, "Evaluating the usable-security of healthcare software through unified technique of fuzzy logic, ANP and TOPSIS," *IEEE Access*, vol. 8, no. 8, pp. 109905–109916, 2020.

[21] R. Kumar, S. A. Khan and R. A. Khan, "Durability challenges in software engineering," *Crosstalk*, vol. 42, no. 4, pp. 29–31, 2016.

[22] R. Kumar, S. A. Khan and R. A. Khan, "Durable security in software development: Needs and importance," *CSI Communications*, vol. 10, no. 10, pp. 34–36, 2015.

[23] 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.

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

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

[26] R. Kumar, S. A. Khan and R. A. Khan, "Revisiting software security: Durability perspective," *International Journal of Hybrid Information Technology*, vol. 8, no. 2, pp. 311–322, 2015.

[27] W. Alosaimi, A. Alharbi, H. Alyami, M. Ahmad, A. K. Pandey *et al.,* "Impact of tools and techniques for securing consultancy services," *Computer Systems Science and Engineering*, vol. 37, no. 3, pp. 347–360, 2021.

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

[29] M. T. J. Ansari, F. A. Alzahrani, D. Pandey and A. Agrawal, "A fuzzy TOPSIS based analysis toward selection of effective security requirements engineering approach for trustworthy healthcare software development," *BMC Medical Informatics and Decision Making*, vol. 20, no. 1, pp. 1–13, 2021.

[30] R. Kumar, S. A. Khan and R. A. Khan, "Durable security in software development: Needs and importance," *CSI Communications*, vol. 10, no. 10, pp. 34–36, 2015.

[31] R. Kumar, S. A. Khan and R. A. Khan, "Revisiting software security risks," *Journal of Advances in Mathematics and Computer Science*, vol. 11, no. 6, pp. 1–10, 2015.

[32] V. Torra, "Hesitant fuzzy sets," *International Journal of Intelligent Systems*, vol. 25, no. 6, pp. 529–539, 2010.

[33] W. Alosaimi, M. T. J. Ansari, A. Alharbi, H. Alyami, A. H. Seh *et al.,* "Evaluating the impact of different symmetrical models of ambient assisted living systems," *Symmetry*, vol. 13, no. 3, pp. 1–21, 2021.

[34] A. Attaallah, M. Ahmad, M. T. J. Ansari, A. K. Pandey, R. Kumar *et al.,* "Device security assessment of internet of healthcare things," *Intelligent Automation & Soft Computing*, vol. 27, no. 2, pp. 593–603, 2020.

[35] 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. 8, pp. 48870–48885, 2020.

[36] W. Alhakami, A. Binmahfoudh, A. Baz, H. Alhakami, M. T. J. Ansari *et al.,* "Atrocious impinging of covid-19 pandemic on software development industries," *Computer Systems Science and Engineering*, vol. 36, no. 2, pp. 323–338, 2021.

[37] K. Sahu and R. K. Srivastava, "'Predicting software bugs of newly and large datasets through a unified neuro-fuzzy approach: Reliability perspective," *Advances in Mathematics: Scientific Journal*, vol. 10, no. 1, pp. 543–555, 2021.

[38] R. Kumar, S. A. Khan and R. A. Khan, "Analytical network process for software security: A design perspective," *CSI Transactions on ICT*, vol. 4, no. 2, pp. 255–258, 2016.

[39] R. Kumar, S. A. Khan, A. Agrawal and R. A. Khan, "Measuring the security attributes through fuzzy analytic hierarchy process: Durability perspective," *ICIC Express Letters*, vol. 12, no. 6, pp. 615–620, 2018.

[40] R. Kumar, S. A. Khan and R. A. Khan, "Software security testing: A pertinent framework," *Journal of Global Research in Computer Science*, vol. 5, no. 3, pp. 23–27, 2014.

[41] R. Kumar, A. Baz, H. Alhakami, W. Alhakami, A. Agrawal *et al.,* "A hybrid fuzzy rule-based multi-criteria framework for sustainable-security assessment of web application," *Ain Shams Engineering Journal*, article in press, pp. 1–21, 2021. https://doi.org/10.1016/j.asej.2021.01.003.