Intelligent Automation & Soft Computing
DOI:10.32604/iasc.2022.019624
Article

Multi-Level Hesitant Fuzzy Based Model for Usable-Security Assessment

Mohd Nadeem[1], Jehad F. Al-Amri[2], Ahmad F. Subahi[3], Adil Hussain Seh[1], Suhel Ahmad Khan[4], Alka Agrawal[1] and Raees Ahmad Khan[1,*]

[1]Department of Information Technology, Babasaheb Bhimrao Ambedkar University, Lucknow, 226025, India
[2]Department of Information Technology, College of Computers and Information Technology, Taif University, Taif, 21944, Saudi Arabia
[3]Department of Computer Science, University College of Al Jamoum, Umm Al Qura University, Makkah, 21421, Saudi Arabia
[4]Department of Computer Science, Indira Gandhi National Tribal University, Amarkantak, 84886, India
*Corresponding Author: Raees Ahmad Khan. Email: khanraees@yahoo.com
Received: 19 April 2021; Accepted: 20 May 2021

Abstract: Present day healthcare sector is frequently victimized by the intruders. Healthcare data industry has borne the brunt of the highest number of data breach episodes in the last few years. The key reason for this is attributed to the sensitivity of healthcare data and the high costs entailed in trading the data over the dark web. Hence, usable-security evaluation of healthcare information systems is the need of hour so as to identify the vulnerabilities and provide preventive measures as a shield against the breaches. Usable-security assessment will help the software designers and developers to prioritize usable-security attributes according to the customers' needs and bridge the security gap. This study, in particular, evaluates the usable-security of Health Information Software Systems (HISS) in design tactics perspective by using Multi Criteria Decision Making (MCDM) problem solving techniques. Hesitant fuzzy based Analytical Hierarchy Process (AHP) and Technique for Order of Preference by Similarity to Ideal-Solutions (TOPSIS) methods have been applied to conduct the quantitative analysis of usable-security of software. Five attributes and 12 sub-attributes with 6 HISS alternatives of Indian hospitals have been considered in this work for usable-security assessment. To draw a priority list from the analysis, the results of the study show that the selected usable-security attributes attained the following ranking order: User-Error protection, Learnability, Data validation, Robustness, Revoke access, Intrusion detection, Authentication, Encryption, Limit access, Reliability, Efficiency, Audit trail respectively. Furthermore, HISS-1 alternative achieved the highest satisfaction degree followed by HISS-2 and HISS-4. HISS-6 got the lowest score in the context of providing ideal usable-security mechanism. The present research endeavour will be helpful for the software designers as the findings of the study will facilitate in developing secure and usable software products from the initial stages of the software development process itself.

Keywords: Usable-security; development process; health information software systems; hesitant fuzzy based AHP-TOPSIS

This work is licensed under a Creative Commons Attribution 4.0 International License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

1 Introduction

Pervasive technologies have greatly influenced the conventional healthcare infrastructure and provided effective means to enhance the present day healthcare services. E-health has been the harbinger of the revolutionary changes in the healthcare sector. The digital health services are not only cost effective but have massive outreach [1–3]. Higher levels of accessibility to E-health services has also improved the patient-doctor interaction as patients can now contact their doctors from any remote locale without making frequent visits to the hospitals. Healthcare Information Software Systems (HISS) have gained consistent popularity in healthcare sector [4,5], and thus, healthcare data is deemed to be one of the most sensitive and confidential data in such a context [6,7]. The present day priority of the healthcare sector is to optimise the use of HISS healthcare service providers to manage and utilize health related data in an efficient way. But ensuring the security of these software systems carrying confidential data and keeping them breach-proof has become a significant issue for both the service providers and patients [8,9]. Healthcare sector recorded the highest number of data breaches in the year 2019 [3,10,11]. In the first half of the present year-2020 itself, 255 healthcare data breach cases have been reported.130 of these instances are because of hacking/IT incidents, i.e., 50.98% of the total [12,13]. These statistics prove that software systems used in healthcare sector either provide immature security services, or such complex security services that directly impact the systems' usability. Just as a flawed software system is vulnerable and prey to attacks, a software system with complex security also lacks in usability and, therefore, is of no value [14]. Such systems can lead to loss of business continuity and increase the user error rate. Moreover, the quality of HISS is significantly influenced by usable-security [15,16]. To address these issues there is a need to evaluate usable-security of HISS and prioritize the usable-security attributes.

Further, several software business studies have cited that from $37.48 billion in 2017, the software market is likely to amass $74.96 billion in 2022; an increment of 50% [16]. Hence, this expansion in demand needs to be met with ideal usable-security mechanisms. Designing and building secure software products is in itself a complex task, but the complex security mechanism of these products makes them less usable [17]. Thus, usable-security continues to be a contentious issue for the developers as they seek for the perfect amalgamation of optimum security as well as usability, without affecting the usability of the systems. Different techniques and methods have been used by the researchers to address usable-security issues. Various multi-criteria decision making techniques have been practiced to assess usable-security of software and prioritize the security and usability attributes for secure usable software development [18,19]. In this row, this research work will help the security designers to design more reliable, trustworthy, and user-friendly products. Towards reaching this objective, the present study will evaluate usable-security of healthcare software systems in design tactics perspective through hesitant fuzzy based Analytical Hierarchy Process and Technique for Order of Preference by Similarity to Ideal-Solutions (AHP-TOPSIS) approach.

While the security feature of a system mainly ensures confidentiality, integrity, and availability of web based software systems storing and processing sensitive and confidential healthcare data [18,19], usability provides the degree of easiness that facilitates the utilization of the service of a software. Thus, usable-security ensures that anyone who needs a secure software product would be able use it easily and comfortably [20,21]. In software architecture perspective, design tactics have direct impact on Software's Quality Attributes (SQA). It defines basic building blocks or predefined patterns that directly concern SQA [22] and provides guidelines to improve the overall quality attributes [23]. Therefore usable-security in design tactics perspective should be the main priority of designers and developers instead of following conventional and informal guidelines to develop the software products.

Usable-security assessment is a continuous process that is performed at regular intervals by the experts to test the usable-security preparedness of that product. This process includes the detection of software vulnerabilities and recommendations with its usability to resist against future attacks to lower down the

risk. Different usable-security attributes are set by experts' opinions while assessing the software's usable-security. Experts and researches use different Multi Criteria Decision Making (MCDM) approaches to evaluate usable-security of software [24,25]. MCDM techniques have the ability to prioritize the usable-security attributes according to their impact on the overall security and usability of the software and identify the most relevant attributes [26]. During software designing and development, a prioritization list of these security attributes will help the designers to improve and maintain usable-security of software systems from the beginning of the development lifecycle. Such a technique will also improve the lifespan of software system and reduce the time and maintenance costs entailed in the process.

Hence, this work aims to evaluate the usable-security of healthcare software systems owned by Indian hospitals through integrated AHP-TOPSIS method under the hesitant fuzzy-based environment. The work will establish guidelines to for the identification and prioritization of usable-security attributes to build more trustworthy software systems. Hesitant fuzzy based AHP-TOPSIS method has a significant ability to address MCDM problems having a hierarchical relationship [22–26]. HF-logic influences greatly where experts hesitate to make decisions about a situation and it is difficult to determine the membership of an element into a fixed set and which may be caused by a doubt among a set of different values. However, normal fuzzy logic lags to address this type of issues [27,28]. In the problem solving approach of MCDM domain, AHP with hesitant fuzzy logic has great ability to produce more accurate weights of the attributes and generate more effective results [27–29]. Moreover, the hesitant fuzzy based TOPSIS is also effective in ranking of the alternatives during solving the MCDM problem [29]. In this work, 5 usable-security attributes at 1st level and 12 sub-attributes at 2nd level have been considered with six HISS as real time alternatives.

The other sections of this study are organized as: the second section presents a review of the existing literature; thereafter, the material and methods of the work have been described in Section 3. Section 4 provides the results of numerical analysis of the work; thereafter the comparative results of classical and hesitant fuzzy based AHP-TOPSIS method and validation of the results through sensitivity analysis have been enlisted. After that, the discussion, then recommendations for practitioners and finally conclusion of the work have been chronicled.

2 Review of Existing Literature

Literature survey of existing relevant studies is a significant tool to find the actual research gap and identify the objectives of the proposed study. From the extensive analysis undertaken while pursuing the present research, it was found that a good number of studies have already been completed on healthcare information software system security assessment through different techniques and tools [6,8–11,13]. Different MCDM methods like fuzzy based AHP-TOPSIS and fuzzy based ANP-TOPSIS (Analytic Network Process-Technique for Order Preference by Similarity to Ideal Solution) have also been applied in different areas of interest to find out the solutions for MCDM problems. Few of the distinguished and pertinent research studies are listed below:

A unified approach of fuzzy based ANP-TOPSIS has been implemented to assess usable-security of health information systems in Agarwal et al. [4]. The analysis considers three security attributes and one usability attribute at the first level, and ten security and three usability sub-attributes at the second level with six alternatives. In addition, a fuzzy based AHP approach was used for evaluating the usable-security of the software in Agarwal et al. [10]. Results of the study show that fuzzy based adopted method is more effective and efficient than classical method. Furthermore, the user-error protection has got the highest priority in the selected attribute list.

According to Khan et al. [11], research work also undertook an in-depth analytical study of the security design tactics by using the decision making techniques. For solving the decision making problems during

software development process, integrated fuzzy based AHP-TOPSIS technique is the most popular approach. Further, fuzzy based AHP-TOPSIS technique has been applied to assess security and prioritize the design-tactics attributes for improving the security performance. In addition, an integrated approach of fuzzy-Delphi and AHP has been proposed in Refs. [12,13] to estimate usable-security of web-based Hospital Management Software System. This empirical investigation provides guidelines for the practitioners and would aid in identifying and prioritizing the usable-security factors while designing and building software products.

Sahu et al. [6] proposed a hesitant fuzzy based decision making model to evaluate software durability of web based applications. In this research study they identified trustworthiness and maintainability are two basic and fundamental attributes to preserve software durability of web applications. Kumar et al. [18] make a research endeavour to find out the applications of hesitant fuzzy sets in decision-making systems. In this study the show that generalized HF sets is fit for the situation when decision makers have a hesitation among several possible memberships with uncertainties.

Kumar et al. [16] devised a model for the selection of most pertinent renewable energy resource for electricity generation. In the research work, ANP and fuzzy based TOPSIS approaches are used to carry out the proposed experiment. The study also found wind energy to be the most appropriate option of electricity generation in Pakistan. Alzahrani et al. [21] and Attaallah et al. [22] proposed a framework based on fuzzy-TOPSIS to rank the renewable-energy supply systems of Turkey. Shannon's Entropy method was applied to evaluate the weights of attributes. The study concluded that the hydro-power station was the best renewable-energy supply system. In addition, Xia et al. [26] proposed a model for web application vulnerability estimation. The study used penetration testing as a tool to assess software's vulnerabilities. Both manual and automatic testing was performed on financial web applications for their security assessment. The study showed that almost symmetric results were obtained from both the vulnerability testing approaches. The research work conducted by Torra et al. [27] made an analytical tactic on quality of healthcare electronic-service. Data analysis and interpretations of the work have been evaluated by integrated fuzzy based AHP-TOPSIS methodology. The study also found that specialization, interactivity, service accuracy, reliability and responsiveness are the main factors for providing satisfactory and effective healthcare web services.

Further, to make an assessment for balancing the attributes of security and usability during the software's development process, Rodríguez et al. [28] used the utility function and decision tree methods. The proposed framework by Rodríguez et al. [28] is also helping the developers to design secure as well as usable software products [5,9]. Another good research work by Sahu et al. [29] estimated usable security of University's software through AHP and TOPSIS under fuzzy environment. The study provided an integration of security and usability attributes that would assist the developers in designing secure software without compromising on the usability of the software.

All in all, in the present research paper, analysis of the existing literature studies established that different techniques have been employed for evaluating the usable-security of software with respect to healthcare and design tactics. Further, MCDM techniques have been used in different domains to address MCDM problems. However, we could not find any research work that had evaluated usable-security of healthcare information system in design tactics perspective through hesitant fuzzy based AHP and TOPSIS. Hence, addressing this research query, our study aims to conduct an assessment of the usable-security of healthcare information system in design tactics perspective, a unique and hitherto unexplored facet in research.

3 Materials and Methods

Material and methods discuss the concepts and methodology used to implement these concepts as two sub-topics under the sub-headings named as "Usable-Security Design Tactics and HIS (health information system)" and "Practiced Methodology". To begin with, this section discusses the concept of

usable-security in design tactics perspective with respect to HIS. Then, a detailed explanation on the practiced methodology used to evaluate usable-security of HIS in design tactics perspective has been tabulated. Hesitant fuzzy based AHP and TOPSIS techniques are utilized to conduct an assessment of usable-security of HIS with respect to design tactics.

3.1 Usable-Security Design Tactics and HIS

Usable-security are closely associated with each other [20,21]. Security fulfills the basic requirements of confidentiality, integrity, and availability of a software product, while usable-security focuses on user-friendly and interactive development of these products. Therefore providing merely complex secure software products without usability is useless. Such products are likely to have a calamitous effect on the software market. Here our aim is to conduct a study that makes an assessment of usable-security of Health Information System (HIS) in design tactics perspective. The core intent of this empirical study is to enhance the overall quality attribute of software and develop secure software products with optimal usability.

Literally, security design tactics or design tactics define that to accomplish a specific goal there should be secure and intelligently planned strategies. In software architecture perspective, design tactics have direct impact on SQA. It defines basic building blocks or predefined patterns that concerns SQA directly [22,23] and provides guidelines to improve overall quality attributes [14]. Detection, resistance and reaction against attacks are the primary concerns of security design tactics [4]. Whereas, the usability feature ensures how these security products meet the users' satisfaction by and fulfill their demands.

To improve the usable-security and prioritize the usable-security attributes of healthcare information systems, the authors performed a case study on six healthcare information systems of the hospitals in Varanasi, India. The identification and selection of usable-security attributes for the assessment of healthcare information systems was a unanimous choice of the experts and the authors. Moreover, the existing literature survey of the pertinent studies done in this context was also a determining factor in choosing the most significant attributes of usable-security. Security tactics hierarchy tree was also alluded to for the attribute identification done in this work. Finally, five usable-security attributes at 1st level and 12 sub-attributes at 2nd level with 6 different alternatives for the usable-security evaluation of healthcare information systems were considered for this work. Health information systems of six different hospitals of Varanasi were selected as alternatives. They are symbolized as HISS-1, HISS-2, HISS-3, HISS-4, HSIS-5, and HISS-6. Fig. 1, given below represents the selected usable-security attributes and they are in a hierarchical fashion.

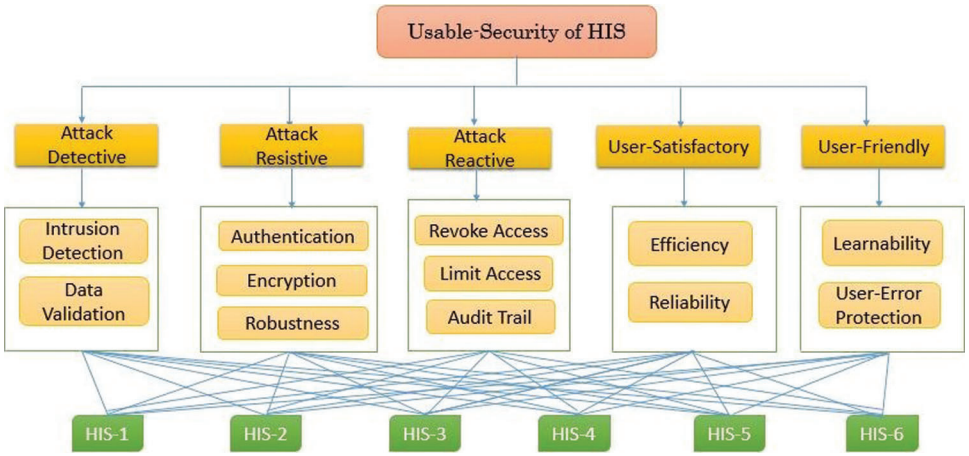

Figure 1: Healthcare information systems usable-security attributes with alternatives

The selected usable-security attributes of HISS are defined as:

Attack Detective

It is the first level attribute of the selected attribute tree. It ensures that the software security systems should possess a strong security detective mechanism to detect any kind of potential threat that could be an insider or outside attack [24]. It identifies the suspicious accesses against the system and system resources. It primarily includes Intrusion detection and data validation as sub-attributes at 2nd level.

- Intrusion Detection: A proactive intrusion detection module in the software system will help the system admins to identify suspicious activities performed against the system which could compromise confidentiality, integrity or availability of the system or system resources.
- Data Validation: This mechanism measures the accuracy, consistency and completeness of data transferred among legitimate entities of a connected network. It helps to identify confidentiality and integrity attacks if executed by intruders.

Attack Resistive

It ensures that whenever a suspicious entity tries to gain control on system resources, the system would combat against it and provide a defensive security mechanism to resist these attacks without compromising the confidentiality, integrity and availability [25]. It includes authentication, encryption, and robustness as sub-attributes. These three sub-attributes will primarily help the developers to build a stronger attack resistive mechanism in the software systems.

- Authentication: It ensures that the claimed entity should provide all the necessary information that will corroborate his claim [4]. For example, entering the correct username and password for successful login. Strong authentication mechanism provides access to only the authentic users of the system. This improves the confidentiality of information and information systems.
- Encryption: It is the process of transforming the normal data (plan-text) into the encrypted form, commonly known as cipher-text to protect data from illegitimate access and modification. Advanced encryption techniques ensure the improvement of overall security of a system but mainly focus on confidentiality and integrity of a system. Encrypted data is less susceptible to modification and disclosure.
- Robustness: It is the quality of a system to resist and keep working in an erroneous environment. ISO defines robustness as “a degree of smallness in variability of a system’s function in various noisy conditions”.

Attack Reactive

It ensures that the software system should have the capability of responding according to the particular situation in case of a potential threat against the system and handle resource management in a way to overcome the effect of that threat. Revoke Access, Limit access, and Audit Trail are the three sub-attributes that primarily focus on making the system attack resistive [26].

- Revoke Access: Revoke access means repealing the privileges granted to a system’s user. It ensures that whenever there is any realization of potential threat or risk against the system or system resources, administrators of the system can severely limit or revoke the access to sensitive resources.
- Limit Access: Ensures that the different users of a system should be granted different privileges according to their role and need. For system’s resource allocation, there should be a limit access protocol that provides the access of the resources to its users on the basis of users’ needs. This protocol can be implemented at the individual as well as at the group level according to the structural need of the organization.

- Audit Trail: Literally, audit trail means a systematic tracing of detailed transactions of an item or record. But in computing, audit trail maintains a record of systems activities that have been done in a file or database. Thus, the healthcare web based application system should also maintain audit trail to keep the users' actions and system records and their effects for future use, as and when necessary [4]. Maintaining audit trail will make the users of the system accountable. Hence, this will improve the non-repudiation characteristic of the system.

User-Satisfaction

ISO defines it as: "freedom from discomfort and positive attitudes towards the use of the product". It ensures that the users' expectations regarding a particular product are fulfilled by the product without any discomfort. Efficiency and reliability of a product are two important sub-attributes of user satisfaction [27].

- Efficiency: It ensures how easily and rapidly the user of the product can achieve mastery over the use of product and product's features [6]. It influences the performance of system with least amount of input for achieving the highest output.
- Reliability: Reliability defines how consistently a system performs and generates results according to its specifications within a given time frame. ISO defines it "a property of consistent intended behaviour and results".

User-Friendly

It is a usability attribute that defines how a product is easy to interact and use. In other words, it measures the degree of easy interaction of a product with its user. Learnability and Use-Error Protection are the main sub-attributes of this feature and consideration of these two sub-attributes at development phase will help the developers to build user-friendly products [27,28].

- Learnability: Learnability ensures how a product is simple and easy to learn for its users. Complex learning rate of a product will decrease the usability level of the product. Thus if the use of a new software product is easy to learn, then it impacts its memorability also. This further enhances its usability level.
- User-Error Protection: User error protection is one of the basic attributes for improving the usability level of a product. It ensures that a system should handle the errors of its users and measure the degree of it to protect its users from making errors.

3.2 Methodology

Research methodology adopted provides a systematic, step-wise procedure to carry out the experiment on healthcare information systems. For this study, hesitant fuzzy based AHP-TOPSIS has been implemented. AHP-TOPSIS is a hybrid integrated approach that comes under the umbrella of MCDM problem solving domain [4]. In this work, AHP-TOPSIS is practiced under the hesitant fuzzy logic environment that makes it efficient and effective for producing more accurate results. Fuzzy logic, as an advanced form of classical logic, has acquired utmost significance in those areas where solution of the problem may take any value from absolute true to absolute false. It can be absolutely true, partially true, absolutely false, or partially false. It comes with the ability to handle uncertainty of the information [9]. While hesitant fuzzy logic makes it apt for producing more accurate results for difficulties where membership degrees cannot be openly cleared or judgment-creators do not decide on membership selection, Torra et al. [27] presented hesitant fuzzy sets, which were further upgraded by Rodriguez et al. [28]. HF-logic influences greatly where experts hesitate to make decisions about a situation and it is difficult to determine the membership of an element into a fixed set and which may be caused by a doubt among a set of different values [29]. Hesitant fuzzy-based environment. Usually, when experts encounter a hesitation while making a decision in ANP and cannot decide on a particular value and wants to go beyond or beneath the values, but these

values are not available [21]. In this situation, hesitant fuzzy sets have got a vital role to address it. Hesitant Fuzzy Sets help in representing decision-makers' hesitant preferences. Analytical hierarchical process, which is an MCDM problem solving technique, is the most suitable technique for addressing the problems that can produce multiple solutions. It analyzes the problem in a hierarchical fashion. AHP provides accurate calculations in case of the attributes' subjective and objective values in comparison to other MCDM approaches [22]. Furthermore, it measures the attributes' strength and consistency as determined by the decisions of the experts. TOPSIS is best known for alternative ranking in the MCDM problem domain [15]. Its working concept is to find the best alternative among the set of competing alternatives and rank all the available alternatives according to their performance scores [21–25]. In this study, hesitant fuzzy based AHP is first applied to determine the weights of criteria (factors/attributes) and then hesitant fuzzy based TOPSIS is practiced to produce the ranking of alternatives. In the following sub-section, numerical formulae are provided for reference.

Hesitant Fuzzy-ANP methods have been proposed to estimate the priority of security attributes in web based applications, and later by applying HF-TOPSIS approach, we have estimate their testing and impact on alternatives for similar characteristics. A step wise depiction of the methodology in a precise ways is listed below:

Step_1: Hierarchical model development for the different attributes is initial step of proposed methodology.

Step_2: Taking help from Tab. 1, decision makers use linguistic terms and pair-wise comparisons between those attributes have been computed.

Table 1: Scale for HF-ANP technique

Rank	Abbreviation	Linguistic Term	Triangular Fuzzy Number
10	AHI	Absolutely High Importance	(7.0000,9.0000,9.0000)
9	VHI	Very High Importance	(5.0000,7.0000,9.0000)
8	ESHI	Essentially High Importance	(3.0000,5.0000,7.0000)
7	WHI	Weakly High Importance	(1.0000,3.0000,5.0000)
6	EHI	Equally High Importance	(1.0000,1.0000,3. 0000)
5	EE	Exactly Equal	(1.0000,1. 0000,1.0000)
4	ELI	Equally Low Importance	(0.3300,1.0000,1.0000)
3	WLI	Weakly Low Important	(0.2000,0.3300,1.0000)
2	ESLI	Essentially Low Importance	(0.1400, 0.2000, 0.3300)
1	VLI	Very Low Importance	(0.1100, 0.1400, 0.2000)
0	ALI	Absolutely Low Importance	(0.1100, 0.1100, 0.1400)

Step_3: Applying fuzzy wrappers [6] on transformed results. With this assuming that T0 has the lowest priority and Tg is has the highest priority in the specified linguistic scale, and the evaluations are between Ti and Tj such that $T0 \leq Ti \leq Tj \leq Tg$; attribute ordered weighted averaging has been computed as in Eq. (1).

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

where OWA specifies the method for ordered weighted averaging, W represents weight of attributes. Same way, after applying Eq. (1), experts find the trapezoidal numbers $\tilde{C} = (p, q, r, s)$ through Eqs. (2)–(5).

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

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

$$q = \left\{ \begin{array}{c} a_M^i, if\ i+1=j \\ OWA_w^2\left(a_m^j, \ldots\ldots a_m^{\frac{i+j}{2}}\right), if\ i+j\ is\ even \\ OWA_w^2\left(a_m^j, \ldots\ldots a_m^{\frac{i+j+1}{2}}\right), if\ i+j\ is\ odd \end{array} \right\} \tag{4}$$

$$r = \left\{ \begin{array}{c} a_M^{i+1}, if\ i+1=j \\ OWA_w^2\left(a_m^j a_m^{j-1}, \ldots\ldots a_m^{\frac{(i+j)}{2}}\right), if\ i+j\ is\ even \\ OWA_w^2\left(a_m^j, a_m^{j-1} \ldots\ldots a_m^{\frac{(i+j+1)}{2}}\right), if\ i+j\ is\ odd \end{array} \right\} \tag{5}$$

Taking help from Eqs. (6) and (7), 1st and 2nd type weights have been determined using η. This is a number within the unit interval [0,1], by applying Eq. (6) and (7) respectively experts achieve these numbers.

1st type weights *(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 = $(w_1^2, w_2^2, \ldots\ldots..w_n^2)$):

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

From the formula $\eta_1 = \frac{g-(j-1)}{g-1}$s, and $\eta_2 = \frac{g-(j-1)}{g-1}$ where, g represents the highest rank number in assessments (as per Tab. 1 g = 10), and i and j represents the low and high attribute assessment ranks respectively.

Step_4: By applying Eqs. (8) and (9) experts compute the pair-wise comparison matrix ($\tilde{A}$) as

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

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

Step_5: Taking help from the Eq. (10), to identify Comparision matrix experts use it for defuzzification of matrix.

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

(l,m1,m2,h) in the specified Eq. (10), represents four components of a trapezoidal number, that is lower bound, upper middle bound, lower middle bound, and higher bound. Defuzzification provides precise values.

To calculate Consistency Ratio (CR) of those values experts apply Eqs. (11) and (12) [6].

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

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

where, CI represents consistency index, RI is random index defined by Sahu et al. [6] that varies for altered n values. If value of Consistency Ration is < 0.1 then our determined matrix is consistent otherwise revise assessment from step_2.

Step_6: Here, experts of the domain apply Eq. (13) to compute the geometric mean for row values.

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

Step_7: Experts determine the most important criterion by assessing weigh of highest characteristics using Eq. (14).

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

Step_8: Analysis of the defuzzified values have been done by the experts by applying the Eq. (15).

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

Step 9: Taking help from the Eq. (16), experts of the domain defuzzified values have been transformed into Normalize weights.

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

Now, from here comes the turn of HF-TOPSIS to find out the best alternative among the available alternatives set. As a dominantly practiced MCDM technique, TOPSIS haven been proved as one of the best technique to select best alternative and help experts in real-world problems [3]. TOPSIS generated solutions are farthest away from the negative ideal solution and the nearest to the positive ideal solution [13]. The base of the proposed technique is to use the envelopes for measuring the distance between H1s and H2s, for example. Given the envelopes, envp(H1s) = [Tp,Tq] and $envp(H2s) = [T_p^*, T_q^*]$, the distance is defined as:

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

Further, the procedure can be defined as:

Step_10: Here we assume for the beginning step that the concerned problem has E alternatives $(C = \{C_1, C_2, \ldots..C_E\})$ and n criteria $(C = \{C_1, C_2, \ldots..C_n\})$

Here, ex represents the practitioners and k depicts the numeric count of experts in TOPSIS approach.

$\tilde{X}^l = \left[H^l_{S_{ij}}\right]_{E \times n}$ Is in TOPSIS technique is used to present a hesitant fuzzy decision matrix where $H^l_{S_{ij}}$ represents alternative i(Ci) estimated score against criteria j(Aj) specified by practitioners e_x.

The standards for HF-TOPSIS to assess criteria and effect of outcomes is specified as and lies between very bad and highly 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 each linguistic expression the comparative fuzzy envelope have been calculated respectively as [29]:

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

$envp_F$(EGH (amM)) = T (0.0000, 0.0000, 0.3500, 0.6700)

$envp_F$(EGH (alG)) = T (0.5000, 0.8500, 1.0000, 1.0000)

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

Step_11: The aggregation of practitioners individual assessments $\left(\tilde{X}^1, \tilde{X}^2 \ldots\ldots \tilde{X}^K\right)$ have been taken and construction of summarized decision matrix X = [xij] is completed with the help of 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: The effective factor is represented by αb in TOPSIS assessment, where Aj depicts the most effective factor, and cost characteristic is represented by αc. Further, lowest relative alternatives for cost related preferences demand high accuracy. Thus, to make cost assessment and effective characteristics, these equations have been practiced [29]:

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

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

$$min_{i=1}^{K}\left(min_i\left(minH_{S_{ij}}^{x}\right)\right) j \in \alpha_b \tag{21}$$

$$\tilde{V}_{qj}^{-} = max_{i=1}^{K}\left(max_i\left(minH_{S_{ij}}^{x}\right)\right) j \in \alpha_c$$

and

$$min_{i=1}^{K}\left(min_i\left(minH_{S_{ij}}^{x}\right)\right) j \in \alpha_b \tag{22}$$

Step_13: Experts take help from the Eqs. (22) and (23) to calculate positive and negative ideal matrixes (M^+ and M^-), respectively.

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

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

Step_14: By applying Eq. (25) the relative closeness score for each alternative have been computed.

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

where,

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

Step_15: Ordered ranking of the alternatives have been presented based on corresponding relative closeness scores.

Authors of this study applied the above discussed systematic step-wise methodology to carry out a case study on usable-security assessment of hospital software system. The next section of this work details the numerical analysis of this research endeavour.

4 Numerical Analysis and Results

Measuring quality attribute of a software system which also includes usable-security is not an easy task [6] because making quantitative evaluation of a qualitative attribute, by rationale, is a complex work. Numerical analysis of this work would provide a quantitative evaluation of usable-security of software systems. For this, a case study on 6 different healthcare information software systems was undertaken. The use of AHP-TOPSIS under the hesitant fuzzy environment made this work more effective and efficient with respect to its results.

To determine the usable-security assessment of HISS, five usable-security attributes namely Attack detective, Attack resistive, Attack reactive, User-satisfactory, and User-friendly have been considered at 1st level of AHP hierarchical tree and are symbolized as S1, S2, S3, S4, and S5, respectively, in Fig. 1, At level 2nd, the sub-attributes of Attack detective are Intrusion detection, Data validation and are symbolized as S11, S12; sub-attributes of Attack resistive are Authentication, Encryption, Robustness and are symbolized as S21, S22 S23; sub-attributes of Attack reactive are Revoke access, Limit access, Audit trail and are symbolized as S31, S32, S33; sub-attributes of User-satisfactory are Efficiency, Reliability and are symbolized as S51, S52, and sub-attributes of User-friendly are Learnability, User-Error protection and are symbolized as S41, S42, respectively. With the help of Eqs. (1)–(26) specified in Methodology section, the usable-security assessment of healthcare information systems, by applying fuzzy based AHP-TOPSIS, has been examined as follows:

By applying Eqs. (1)–(9) and taking help from Tab. 1, conversion from linguistic terms to numeric values have been performed by the authors of this study and then into HF based crisp numeric values. After that for establishing pair-wise comparison matrix, numerical calculations are done and the final results are depicted in Tab. 2. The intermediary operations to get Tab. 2 results are the implementation of

fuzzy wrappers with the help of Eq. (1); calculations of trapezoidal numbers $\tilde{C} = (p, q, r, s)$ by applying Eqs. (2)–(5); and by practicing Eqs. (6) and (7) first and second type weights have been determined with the involvement of η, which represents a number between 0 and 1. Finally, applying Eqs. (8) and (9) experts compute the pair-wise comparison matrix. Due to the less significance of the intermediately operations, they have not been represented here and same procedure is followed in this work. For level 2nd attributes the same procedure is have been practiced to compute the values (local weights) for each attribute. Computed results of level 2nd attributes are shown in the Tab. 3, under the column "local weights" with respect to each attribute from S11 to S52. Tab. 3, also incorporates global weights computed for each 2nd level attribute with respect to corresponding level 1st attributes. With the help of Eqs. (10)–(16), defuzzified values and normalized weights of the level 2nd attributes have been computed and the final results are represented in Tab. 3 also as normalized weights. The complete process for the calculation of Tab. 3 go through the following intermediately operations: first the pair-wise comparison matrixes have been converted into combined defuzzified values through defuzzification processes with the help of Eq. (10). Then the consistency index and consistency ration have been computed using the Eqs. (11) and (12) to check matrix consistency. Our computed consistency ratio is CR = 0.05324, which is less than 0.1 that ensures our calculated matrix is consistent. After that geometric mean for row values and determination of the most important criterion have been calculated with the help of Eqs. (13) and (14). Analysis of defuzzified values and conversion of these values to normalized weights have been done with the help of Eqs. (15) and (16) respectively. On the basis of computed globally normalized weights ranking of the attributes have been determined where attribute S22 got the highest rank and attributes S33 got the lowest rank.

Table 2: Trapezoidal fuzzy pair-wise comparison matrix and normalized weights at level 1

	S1	S2	S3	S4	S5	Local Weights
S1	1.00000, 1.00000, 1.00000, 1.00000	0.33100, 1.10000, 1.12000, 3.12300	0.14100, 0.21000, 1.10000, 1.10000	1.10000, 1.10000, 3.11000, 5.11100	1.11010, 1.22010, 5.12340, 7.14100	0.05100, 0.16100, 0.28100, 1.01100
S2	3.12100, 1.11100, 1.11000, 0.33100	1.00000, 1.00000, 1.00000, 1.00000	0.33100, 1.10000, 1.10000, 3.10000	0.21000, 0.33100, 1.10000, 1.10000	0.11100, 0.14100, 0.33100, 1.10000	0.03510, 0.16610, 0.22610, 0.62100
S3	1.10000, 1.10000, 5.10000, 7.10000	3.10000, 1.10000, 1.10000, 0.33100	1.00000, 1.00000, 1.00000, 1.00000	0.33100, 1.10000, 1.10000, 3.10000	1.10000, 1.10000, 3.10000, 5.10000	0.05910, 0.21100, 0.35100, 1.26100
S4	0.21000, 0.33100, 1.10000, 1.10000	1.10000, 1.10000, 3.10000, 5.10000	3.10000, 1.10000, 1.10000, 0.33100	1.00000, 1.00000, 1.00000, 1.00000	1.10000, 1.10000, 3.10000, 5.10000	0.05410, 0.13100, 0.28100, 0.95100
S5	0.14100, 0.21000, 1.10000, 1.10000	1.10000, 3.10000, 7.10000, 9.10000	0.21000, 0.33100, 1.10000, 1.10000	0.21000, 0.33100, 1.10000, 1.10000	1.00000, 1.00000, 1.00000, 1.00000	0.03310, 0.08610, 0.18100, 0.49810

Table 3: Summarized results of level 1st and level 2nd local and global attribute weights

Main	Local Weights	Sub	Local Weights	Global Weights	Normalized Weights	Ranks
S1	0.05100, 0.16100, 0.28100, 1.01100	S11	0.05140, 0.13130, 0.28110, 0.91480	0.00610, 0.03410, 0.16140, 1.35310	0.17200	6
		S12	0.03130, 0.08160, 0.18110, 0.49810	0.00410, 0.02210, 0.10510, 0.71110	0.14900	3
S2	0.03510, 0.16610, 0.22610, 0.62100	S21	0.04180, 0.15710, 0.27110, 1.02150	0.00610, 0.04100, 0.15710, 1.46210	0.07100	7
		S22	0.03310, 0.12190, 0.21210, 0.78110	0.00410, 0.03310, 0.12310, 1.11410	0.05100	8
		S23	0.06140, 0.24100, 0.41260, 1.21140	0.00810, 0.06210, 0.24810, 1.73210	0.11400	4
S3	0.05910, 0.21100, 0.35100, 1.26100	S31	0.05210, 0.15910, 0.29710, 1.02510	0.00610, 0.04110, 0.17310, 1.46210	0.09300	5
		S32	0.02120, 0.07310, 0.11310, 0.50310	0.00310, 0.01910, 0.06610, 0.71810	0.04400	9
		S33	0.03110, 0.07180, 0.12110, 0.31910	0.00210, 0.01100, 0.04910, 0.22510	0.01100	12
S4	0.05410, 0.13100, 0.28100, 0.95100	S41	0.14910, 0.27160, 0.72130, 1.50910	0.00910, 0.03410, 0.29210, 0.87310	0.15800	2
		S42	0.07610, 0.21810, 0.45510, 1.01310	0.00410, 0.02710, 0.18310, 0.59610	0.17200	1
S5	0.03310, 0.08610, 0.18100, 0.49810	S51	0.03150, 0.09710, 0.19810, 0.51310	0.00210, 0.01210, 0.08100, 0.29710	0.02400	11
		S52	0.03110, 0.07810, 0.12110, 0.31910	0.00210, 0.01100, 0.04910, 0.22510	0.03600	10
CR = 0.05324						

This portion of the section provides a realistic assessment of evaluated results on highly sensitive healthcare web applications of Indian hospitals. After attaining the defuzzified and normalized weights of each attribute with the help of hesitant fuzzy based AHP technique, hesitant fuzzy based TOPSIS has been practiced to generate the global ranking of competitive alternatives. Taking help from standard scale in step_10 and Eq. (17) defined in the methodology sub-section, we took the inputs on the technological data of 6 health information software systems of and the combinative results are depicted in Tab. 4. To obtain alternative ranking the attribute weights produced by hesitant fuzzy based AHP are given to TOPSIS approach under fuzzy environment. Taking help from step_10 (specified in methodology section) for intermediary operations and by applying Eq. (18) normalized fuzzy decision-matrix for 12 sub-attributes and six competitive alternatives is established and presented in Tab. 5. Practicing Eqs. (19)–(22) the normalized fuzzy decision-matrix cell values (performance-values) is multiplied by every attribute weight value, and a weighted fuzzy normalized decision-matrix is to be constructed which is depicted in Tab. 6. Then by applying Eqs. (22) and (23) to calculate positive and negative idealness of each alternative with respect to each attribute have been computed and the final results are shown in Tab. 7 under column name dist+ and dist-. After that, Eqs. (25) and (26) have been applied and relative closeness score for each alternative have been computed as satisfaction degree of CC-i and the results are shown in Tab. 7.

Table 4: Subjective cognition results of the evaluators in linguistic terms

	HISS-1	HISS-2	HISS-3	HISS-4	HISS-5	HISS-6
S11	2.4500, 4.2700, 6.2700, 8.6500	2.4500, 4.2700, 6.2700, 8.6500	0.8200, 2.2700, 4.2700, 6.6500	2.4500, 4.2700, 6.2700, 8.6500	1.4500, 3.0700, 4.9100, 5.6500	0.8200, 2.2700, 4.2700, 6.6500
S12	3.9100, 5.9100, 7.8200, 8.6500	1.6400, 3.5500, 5.5500, 6.7300	2.4500, 4.2700, 6.2700, 8.6500	2.4500, 4.2700, 6.2700, 8.6500	0.9100, 2.4500, 4.4500, 5.6500	2.4500, 4.2700, 6.2700, 8.6500
S21	3.9100, 5.9100, 7.8200, 8.6500	2.4500, 4.2700, 6.2700, 8.6500	2.4500, 4.2700, 6.2700, 8.6500	2.4500, 4.2700, 6.2700, 8.6500	2.4500, 4.2700, 6.2700, 8.6500	3.9100, 5.9100, 7.8200, 8.6500
S22	2.4500, 4.2700, 6.2700, 8.6500	3.9100, 5.9100, 7.8200, 8.6500	1.6400, 3.5500, 5.5500, 6.7300	3.9100, 5.9100, 7.8200, 8.6500	1.6400, 3.5500, 5.5500, 6.7300	0.8200, 2.2700, 4.2700, 6.6500
S23	0.8200, 2.2700, 4.2700, 6.6500	3.9100, 5.9100, 7.8200, 8.6500	2.5500, 4.4500, 6.4500, 7.8400	3.9100, 5.9100, 7.8200, 8.6500	2.5500, 4.4500, 6.4500, 7.8400	2.4500, 4.2700, 6.2700, 8.6500
S31	2.4500, 4.2700, 6.2700, 8.6500	2.4500, 4.2700, 6.2700, 8.6500	2.4500, 4.2700, 6.2700, 8.6500	2.4500, 4.2700, 6.2700, 8.6500	2.4500, 4.2700, 6.2700, 8.6500	2.4500, 4.2700, 6.2700, 8.6500
S32	3.9100, 5.9100, 7.8200, 8.6500	0.8200, 2.2700, 4.2700, 6.6500	2.4500, 4.2700, 6.2700, 8.6500	0.8200, 2.2700, 4.2700, 6.6500	3.9100, 5.9100, 7.8200, 8.6500	1.6400, 3.5500, 5.5500, 6.7300
S33	3.2500, 5.1200, 7.1400, 8.7200	2.4500, 4.2700, 6.2700, 8.6500	2.4500, 4.2700, 6.2700, 8.6500	2.4500, 4.2700, 6.2700, 8.6500	3.9100, 5.9100, 7.8200, 8.6500	2.5500, 4.4500, 6.4500, 7.8400
S41	2.5500, 4.4500, 6.4500, 7.8400	3.9100, 5.9100, 7.8200, 8.6500	1.6400, 3.5500, 5.5500, 6.7300	3.9100, 5.9100, 7.8200, 8.6500	2.4500, 4.2700, 6.2700, 8.6500	2.4500, 4.2700, 6.2700, 8.6500
S42	3.2500, 5.1200, 7.1400, 8.7200	0.9100, 2.4500, 4.4500, 5.6500	2.4500, 4.2700, 6.2700, 8.6500	2.4500, 4.2700, 6.2700, 8.6500	0.8200, 2.2700, 4.2700, 6.6500	2.4500, 4.2700, 6.2700, 8.6500
S51	1.8200, 3.7300, 5.7300, 6.7300	2.4500, 4.2700, 6.2700, 8.6500	3.9100, 5.9100, 7.8200, 8.6500	1.6400, 3.5500, 5.5500, 6.7300	2.4500, 4.2700, 6.2700, 8.6500	2.4500, 4.2700, 6.2700, 8.6500
S52	2.8200,4.6400, 6.6400, 6.6400	2.4500, 4.2700, 6.2700, 8.6500	3.9100, 5.9100, 7.8200, 8.6500	2.5500, 4.4500, 6.4500, 7.8400	3.9100, 5.9100, .8200, 8.6500	1.6400, 3.5500, 5.5500, 6.7300

Table 5: The normalized fuzzy-decision matrix

	HISS-1	HISS-2	HISS-3	HISS-4	HISS-5	HISS-6
S11	0.5740,0.7250, 0.7920, 0.8960	0.6120, 0.8500, 0.9170, 0.9680	0.6110, 0.7720, 0.8560, 0.9450	0.6110, 0.7720, 0.8560, 0.9450	0.5740, 0.7250, 0.7920, 0.8960	0.3340, 0.5240, 0.6180, 0.7800
S12	0.6110,0.7720, 0.8560, 0.9450	0.2750, 0.4560, 0.5330, 0.7330	0.5740, 0.7250, 0.7920, 0.8960	0.8750, 0.8750, 0.8750, 0.8750	0.5740, 0.7250, 0.7920, 0.8960	0.5740, 0.7250, 0.7920, 0.8960
S21	0.5740,0.7250, 0.7920, 0.8960	0.2750, 0.4560, 0.5330, 0.7330	0.5740, 0.7250, 0.7920, 0.8960	0.6120, 0.8500, 0.9170, 0.9680	0.6110, 0.7720, 0.8560, 0.9450	0.5740, 0.7250, 0.7920, 0.8960
S22	0.6120,0.8500, 0.9170, 0.9680	0.6110, 0.7720, 0.8560, 0.9450	0.5740, 0.7250, 0.7920, 0.8960	0.2750, 0.4560, 0.5330, 0.7330	0.5740, 0.7250, 0.7920, 0.8960	0.5740, 0.7250, 0.7920, 0.8960
S23	0.5740,0.7250, 0.7920, 0.8960	0.2750, 0.4560, 0.5330, 0.7330	0.5740, 0.7250, 0.7920, 0.8960	0.6110, 0.7720, 0.8560, 0.9450	0.6120, 0.8500, 0.9170, 0.9680	0.6110, 0.7720, 0.8560, 0.9450
S31	0.6110,0.7720, 0.8560, 0.9450	0.6120, 0.8500, 0.9170, 0.9680	0.6110, 0.7720, 0.8560, 0.9450	0.5740, 0.7250, 0.7920, 0.8960	0.2750, 0.4560, 0.5330, 0.7330	0.5740, 0.7250, 0.7920, 0.8960
S32	0.5740,0.7250, 0.7920, 0.8960	0.6120, 0.8500, 0.9170, 0.9680	0.6110, 0.7720, 0.8560, 0.9450	0.6110, 0.7720, 0.8560, 0.9450	0.5740, 0.7250, 0.7920, 0.8960	0.6120, 0.8500, 0.9170, 0.9680
S33	0.6110,0.7720, 0.8560, 0.9450	0.2750, 0.4560, 0.5330, 0.7330	0.5740, 0.7250, 0.7920, 0.8960	0.6120, 0.8500, 0.9170, 0.9680	0.6110, 0.7720, 0.8560, 0.9450	0.6110, 0.7720, 0.8560, 0.9450
S41	0.5740,0.7250, 0.7920, 0.8960	0.2750, 0.4560, 0.5330, 0.7330	0.6110, 0.7720, 0.8560, 0.9450	0.2750, 0.4560, 0.5330, 0.7330	0.5740, 0.7250, 0.7920, 0.8960	0.8750, 0.8750, 0.8750, 0.8750
S42	0.6120,0.8500, 0.9170, 0.9680	0.6110, 0.7720, 0.8560, 0.9450	0.5740, 0.7250, 0.7920, 0.8960	0.2750, 0.4560, 0.5330, 0.7330	0.5740, 0.7250, 0.7920, 0.8960	0.6120, 0.8500, 0.9170, 0.9680

Table 5 (continued).

	HISS-1	HISS-2	HISS-3	HISS-4	HISS-5	HISS-6
S51	0.5740,0.7250, 0.7920, 0.8960	0.2750, 0.4560, 0.5330, 0.7330	0.6120, 0.8500, 0.9170, 0.9680	0.6110, 0.7720, 0.8560, 0.9450	0.5740, 0.7250, 0.7920, 0.8960	0.2750, 0.4560, 0.5330, 0.7330
S52	0.6110,0.7720, 0.8560, 0.9450	0.6120, 0.8500, 0.9170, 0.9680	0.5740, 0.7250, 0.7920, 0.8960	0.2750, 0.4560, 0.5330, 0.7330	0.5740, 0.7250, 0.7920, 0.8960	0.6110, 0.7720, 0.8560, 0.9450
	0.5740, 0.7250, 0.7920, 0.8960	0.8750, 0.8750, 0.8750, 0.8750	0.5740, 0.7250, 0.7920, 0.8960	0.8750, 0.8750, 0.8750, 0.8750	0.03980, 0.1000, 0.1920, 0.3840	0.5500, 0.5500, 0.5500, 0.5500

Table 6: The weighted normalized fuzzy-decision matrix

	HISS-1	HISS-2	HISS-3	HISS-4	HISS-5	HISS-6
S11	0.0470,0.0740, 0.0920, 0.1120	0.0320,0.0470, 0.0530, 0.0630	0.0371,0.0616, 0.0790, 0.1100	0.1330,0.1680, 0.1840, 0.2080	0.0371,0.0616, 0.0790, 0.1100	0.0320, 0.0530, 0.0720, 0.0980
S12	0.0555,0.0870, 0.1040, 0.1220	0.0434,0.0510, 0.0660, 0.0690	0.0344,0.0570, 0.0820, 0.1100	0.1480,0.1891, 0.2060, 0.2240	0.0470,0.0740, 0.0920, 0.1120	0.0320, 0.0470, 0.0530, 0.0630
S21	0.0470,0.0740, 0.0920, 0.1120	0.0320,0.0470, 0.0530, 0.0630	0.0570,0.0850, 0.1080, 0.1310	0.0470,0.0740, 0.0920, 0.1120	0.0470,0.0740, 0.0920, 0.1120	0.0320, 0.0470, 0.0530, 0.0630
S22	0.0555,0.0870, 0.1040, 0.1220	0.0434,0.0510, 0.0660, 0.0690	0.0344,0.0570, 0.0820, 0.1100	0.0555,0.0870, 0.1040, 0.1220	0.0555,0.0870, 0.1040, 0.1220	0.0434, 0.0510, 0.0660, 0.0690
S23	0.1480,0.1891, 0.2060, 0.2240	0.0470,0.0740, 0.0920, 0.1120	0.0320,0.0470, 0.0530, 0.0630	0.0470,0.0740, 0.0920, 0.1120	0.0470,0.0740, 0.0920, 0.1120	0.0320, 0.0470, 0.0530, 0.0630
S31	0.0434,0.0510, 0.0660, 0.0690	0.0555,0.0870, 0.1040, 0.1220	0.0434,0.0510, 0.0660, 0.0690	0.0555,0.0870, 0.1040, 0.1220	0.0555,0.0870, 0.1040, 0.1220	0.0434, 0.0510, 0.0660, 0.0690

(Continued)

Table 6 (continued).

	HISS-1	HISS-2	HISS-3	HISS-4	HISS-5	HISS-6
S32	0.1330,0.1680, 0.1840, 0.2080	0.0470,0.0740, 0.0920, 0.1120	0.0320,0.0470, 0.0530, 0.0630	0.1480,0.1891, 0.2060, 0.2240	0.1480,0.1891, 0.2060, 0.2240	0.0344, 0.0570, 0.0820, 0.1100
S33	0.0470,0.0740, 0.0920, 0.1120	0.0555,0.0870, 0.1040, 0.1220	0.0434,0.0510, 0.0660, 0.0690	0.0434,0.0510, 0.0660, 0.0690	0.0434,0.0510, 0.0660, 0.0690	0.0434, 0.0510, 0.0660, 0.0690
S41	0.0555,0.0870, 0.1040, 0.1220	0.1480,0.1891, 0.2060, 0.2240	0.0344,0.0570, 0.0820, 0.1100	0.1330,0.1680, 0.1840, 0.2080	0.1330,0.1680, 0.1840, 0.2080	0.0371, 0.0616, 0.0790, 0.1100
S42	0.0320,0.0530, 0.0720, 0.0980	0.0434,0.0510, 0.0660, 0.0690	0.0434,0.0510, 0.0660, 0.0690	0.0470,0.0740, 0.0920, 0.1120	0.0470,0.0740, 0.0920, 0.1120	0.0320, 0.0470, 0.0530, 0.0630
S51	0.1480,0.1891, 0.2060, 0.2240	0.1330,0.1680, 0.1840, 0.2080	0.0371,0.0616, 0.0790, 0.1100	0.0555,0.0870, 0.1040, 0.1220	0.0555,0.0870, 0.1040, 0.1220	0.0434, 0.0510, 0.0660, 0.0690
S52	0.0080,0.0224, 0.0502, 0.1000	0.0470,0.0740, 0.0920, 0.1120	0.0320,0.0470, 0.0530, 0.0630	0.0080,0.0224, 0.0502, 0.1000	0.1480,0.1891, 0.2060, 0.2240	0.0344, 0.0570, 0.0820, 0.1100

Table 7: Closeness coefficients to the aspired level among the different alternatives

Alternatives	dist+i	dist-i	Gap Degree of CC+i	Satisfaction Degree of CC-i	Rank of Alternatives
HISS-1	0.065154	0.0356457	0.5245587	0.6443564	1
HISS-2	0.055125	0.0365887	0.3654587	0.6251254	2
HISS-3	0.047753	0.0548565	0.5698695	0.4448567	5
HISS-4	0.041251	0.0365585	0.2561568	0.5279875	3
HISS-5	0.452274	0.0558856	0.5656335	0.4678567	4
HISS-6	0.045659	0.0545547	0.6125986	0.3889969	6

Then summarized results of the numeral analysis depicts that on the basis of preference score or relative closeness scores the ranking of competitive alternatives (six health information software systems) is generated as: HISS-1, HISS-2, HISS-4, HISS-5, HISS-3, HISS-3, and HISS-6 in usable-security assessment perspective. From this analysis it has been found that the usable-security assessment performed on six different health information software systems shows HISS-1 provides better

usable-security mechanism to address main security issues and challenges on the basis of selected criteria. Further, analysis of the results shows that the identified attributes for software security assessment in this work have been prioritized on the basis of computed weights in the following sequence through hesitant fuzzy TOPSIS technique: User-Error protection (S42) 0.17200, Learnability (S41) 0.15800, Data validation (S12) 0.14900, Robustness (S23) 0.11400, Revoke access (S31) 0.09300, Intrusion detection (S11) 0.07700, Authentication (S21) 0.07100, Encryption (S22) 0.05100, Limit access (S32) 0.04400, Reliability (S52) 0.03600, Efficiency (S51) 0.02400, Audit trail S33 0.01100 respectively.

5 Discussion

Software complexity and its need in day-to-day life have seen a phenomenal growth. But inadequacy in usable-security services continues to dent this expansive rise because flawed software systems have become easy preys of intrusions and data breaches. Despite the huge investments on security tools and techniques at present, data breach incidents often remain uncontained and, sometimes, even undetected and the damage is irretrievable. According to HIPPA (2018-2019) data breach reports, there have been 2,546 healthcare data breaches between 2009 and 2018. Each breach contained more than 500 records. Those breaches have resulted in the theft/exposure of more than 189 million healthcare records [3].

There has been an abrupt rise in the number of attacks on healthcare software systems in the recent years because of data sensitivity and valuable character of the data [23–26]. In the first half of the year 2020 alone, 255 healthcare data breach episodes have been reported and 130 of them are because of hacking/IT incidents [5,27–28]. Practitioners and security experts are trying to address these issues and maintain the security level of software products [24,29]. Despite the efforts made in this direction, the healthcare industry continues to targeted by the intruders because complex security service are less usable and are more user error prone. Moreover, practicing conventional and informal guidelines while addressing security issues of healthcare software systems increases software vulnerabilities [4]. Facts and figures clearly show that there is a need to estimate the HISS usable-security in design tactic perspective. Security design tactics defines basic building blocks or predefined patterns that concerns SQA directly [12,13] and provides guidelines to improve the overall quality attributes of software [14]. Practicing these guidelines instead of informal and conventional approaches will be beneficial for the practitioners in designing secure and trustworthy products. The usable-security assessment will help to examine the existing HISS usable-security mechanism, prioritize usable-security attributes, and provide new guidelines that will help designers and developers to build secure and usable products. If the prioritization of quality attributes including usable-security can be done during the software development process itself, it would be a significant achievement towards realising the goals of usable-security in design perspective. With this intent, the authors of this work conducted an assessment of HISS usable-security in design tactics perspective by using hesitant fuzzy based AHP-TOPSIS. Hesitant fuzzy logic has got utmost significance in addressing those contexts where the problem contains uncertain and imprecise information [6]. However, HF-logic influences greatly where experts hesitate to make decisions about a situation and it is difficult to determine the membership of an element into a fixed set and which may be caused by a doubt among a set of different values [29]. AHP performs very well while calculating attributes' subjective and objective values in comparison to other MCDM approaches [6]. Further, it measures the attributes' strength and consistency accurately. TOPSIS aptly ranks the alternatives [21].

The main findings of this study are:

- According to the results of the study, the Healthcare Information Software System (HISS-1) meets the maximum usable-security criteria that have been employed in this study to evaluate the security of HISSs.

- The sequential order of other alternatives according to their generated performance scores are as: HISS-1, HISS-2, HISS-4, HISS-5, HISS-3, HISS-3, and HISS-6.
- The usable-security attribute assessment through hesitant fuzzy based AHP prioritizes the usable-security attributes from higher to lower in the following order: User-Error protection (S42), Learnability (S41), Data validation (S12), Robustness (S23), Revoke access (S31), Intrusion detection (S11), Authentication (S21), Encryption (S22), Limit access (S32), Reliability (S52), Efficiency (S51), Audit trail S33 respectively.
- Our usable-security evaluation cannot be a claimant for optimality of results because research is a dynamic as well as an ongoing process, but our results are efficient and reliable. Furthermore, other MCDM techniques can be employed to produce more efficient results but we have also chosen effective techniques for this assessment.
- Attribute identification and selection for usable-security assessment is a subjective process, as per the opinions of the experts, or be need-specific. Hence, the optimality of attribute selection cannot be justified. The experimental results can vary from study to study with respect to attributes' selection. Moreover, variation in number of attributes can affect the results. Thus, it needs further investigation and research.
- It is not a conclusive fact that the Integrated HF-AHP-TOPSIS is the best technique for the evaluation of usable-security but it does provide efficient results.

6 Conclusions

Security and usability have a significant impact on the overall quality attribute of the software. While security without usability is of no value, a fragile security with high usability will also lead to disastrous outcomes. Usable-security significantly influences the HISS's quality attribute. To address both the security and usability attributes of a software system, the present endeavour assessed usable-security of HISS in design tactics perspective through MCDM problem solving techniques. The authors chose to use hesitant fuzzy based AHP-TOPSIS because these are highly effective techniques for addressing decision making problems and provide efficient results. Identification and selection of usable-security attributes used for evaluation has been done on the basis of experts' opinions and existing research outcomes. Results of the hesitant fuzzy based AHP shows that User-error protection has got the highest priority with 0.17200 attribute weight; while Audit trail got the lowest priority with 0.01100 attribute weight. Moreover, alternative ranking generated by hesitant fuzzy based TOPSIS of Healthcare information software systems shows that HISS-1 got the highest ranking with performance score of 0.6443564; while HWA-6 got lowest ranking with performance score of 0.3889969 when examined with respect to identified usable-security attributes. Identification and prioritization of usable-security attributes, as mapped in this study, are a convincing reference point for the developers in their quest to design systems that have the desired level of security while affording optimum usability.

Acknowledgement: This research was supported by Taif University Researchers Supporting Project number (TURSP-2020/211), Taif University, Taif, Saudi Arabia.

Funding Statement: This Project was funded by the Taif University Researchers Supporting Projects at Taif University, Kingdom of Saudi Arabia, under grant number: TURSP-2020/211.

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

References

[1] W. J. M. Stevens, R. V. D. Sande, L. Beijer, M. G. M. Gerritsen and W. J. J. Assendelft, "E-health apps replacing or complementing health care contacts: Scoping review on adverse effects," *Journal of Medical Internet Research*, vol. 21, no. 3, pp. 1–11, 2019.

[2] N. S. B. Nasaruddin, I. A. Aziz and N. A. Rashid, "Web-based electronic healthcare record system (EHRS) based on feedback," in *Proc. 2018 IEEE Conf. on Application, Information and Network Security*, Langkawi, Malaysia, pp. 27–32, 2018.

[3] A. H. Seh, M. Zarour, M. Alenzi, A. K. Sarkar, A. Agrawal *et al.,* "Healthcare data breaches: Insights and implications," *Healthcare*, vol. 8, no. 2, pp. 1–18, 2020.

[4] A. Agarwal, A. H. Seh, A. Baz, H. Alhakami, M. Baz *et al.,* "Software security estimation using the hybrid fuzzy ANP-TOPSIS approach: Design tactics perspective," *Symmetry*, vol. 12, no. 4, pp. 1–21, 2020.

[5] 2020 Healthcare Data Breach Report, *HIPAA Journal.* [Online]. Available: https://www.hipaajournal.com/april-2020-healthcare-data-breach-report/.

[6] 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. 11, pp. 1–20, 2020.

[7] 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.

[8] M. Zarour, M. T. J. Ansari, M. Alenezi, A. K. Sarkar, M. Faizan *et al.,* "Evaluating the impact of blockchain models for secure and trustworthy electronic healthcare records," *IEEE Access*, vol. 8, no. 8, pp. 25574–25586, 2020.

[9] M. Alenezi, A. Agrawal, R. Kumar and R. A. Khan, "Evaluating performance of web application security through a fuzzy based hybrid multi-criteria decision-making approach: Design tactics perspective," *IEEE Access*, vol. 8, no. 8, pp. 25543–25556, 2020.

[10] A. Agarwal, 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. 1–16, 2019.

[11] 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.

[12] K. Sahu and R. Shree, "Helpful and defending actions in software risk management: A security viewpoint," *Integrated Journal of British*, vol. 4, no. 5, pp. 1–7, 2015.

[13] 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.

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

[15] K. Sahu and R. Shree, "Stability: Abstract roadmap of security," *American International Journal of Research in Science, Engineering and Mathematics*, vol. 2, no. 9, pp. 183–186, 2015.

[16] 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.

[17] 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.

[18] 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.

[19] 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.

[20] 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.

[21] 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.

[22] A. Attaallah, M. Ahmad, M. Tarique, 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.

[23] K. Sahu and R. Shree, "Software security: A risk taxonomy," *International Journal of Computer Science and Engineering Technology*, vol. 7, no. 3, pp. 36–41, 2015.

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

[25] K. Sahu, R. Shree and R. Kumar, "Risk management perspective in SDLC," *International Journal of Advanced Research in Computer Science and Software Engineering*, vol. 4, no. 3, pp. 1247–1251, 2014.

[26] 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.

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

[28] R. M. Rodríguez, L. Martínez, V. Torra, Z. S. Xu and F. Herrera, "Hesitant fuzzy sets: State of the art and future directions," *International Journal of Intelligent Systems*, vol. 29, no. 6, pp. 495–524, 2019.

[29] 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.