Computers, Materials & Continua
DOI:10.32604/cmc.2021.014007
Article

Tech Science Press

Estimating Security Risk of Healthcare Web Applications: A Design Perspective

Fahad A. Alzahrani*

Department of Computer Engineering, Umm Al-Qura University, Mecca, 24381, Saudi Arabia
*Corresponding Author: Fahad A. Alzahrani. Email: fayzahrani@uqu.edu.sa
Received: 28 August 2020; Accepted: 20 October 2020

Abstract: In the recent years, the booming web-based applications have attracted the hackers' community. The security risk of the web-based hospital management system (WBHMS) has been increasing rapidly. In the given context, the main goal of all security professionals and website developers is to maintain security divisions and improve on the user's confidence and satisfaction. At this point, the different WBHMS tackle different types of security risks. In WBHMS, the security of the patients' medical information is of utmost importance. All in all, there is an inherent security risk of data and assets in the field of the medical industry as a whole. The objective of this study is to estimate the security risk assessment of WBHMS. The risks assessment pertains to securing the integrity of the information in alignment with the Health Insurance Portability and Accountability Act. This includes protecting the relevant financial records, as well as the identification, evaluation, and prevention of a data breach. In the past few years, according to the US-based cyber-security firm *Fire-eye*, 6.8 million data thefts have been recorded in the healthcare sector in India. The breach barometer report mentions that in the year 2019, the data breaches found were up to 48.6% as compared to the year 2018. Therefore, it is very important to assess the security risk in WBHMS. In this research, we have followed the hybrid technique fuzzy analytic hierarchy process-technique for order of preference by similarity to ideal solution (F-AHPTOPSIS) approach to assess the security risk in WBHMS. The place of this empirical database is at the local hospital of Varanasi, U.P., India. Given the affectability of WBHMS for its board framework, this work has used diverse types of web applications. The outcomes obtained and the procedure used in this assessment would support future researchers and specialists in organizing web applications through advanced support of safety and security.

Keywords: Web based hospital management system; security risk; fuzzy AHP; fuzzy TOPSIS

1 Introduction

Several surveys have cited nearly 44% increase in the number of web application users during 2012–2018 [1]. India is reckoned as one amongst the 10 highest spam-sending nations worlwide.

The data elaborates that 48% of the ruptures influenced money-related associations. 20 percent of the breaks included medical services associations. 12 percent of them affected the public division elements and 20% intrusions were on the retail and accommodation as shown in Fig. 1. Security risk has become a significant factor in the process of improving programming and the WBHMS with its broad framework plan. Several issues need to be tackled in a WBHMS including the cell phones, ransomware, and malware, among others [2]. The security risk is characterized as the "probability of enduring misfortune that portrays the effect on the venture which could be as low quality of programming arrangement, expanded costs, disappointment, or postponed finish" [3]. Thus, all of these aspects are elemental security concerns. Moreover, every information technology (IT) expert has associated security risks. However, the security risk can be reduced and mitigated through a planned assessment procedure. Furthermore, according to Jasper [4], risk can be broadly divided into two aspects, risk evaluation and risk control.

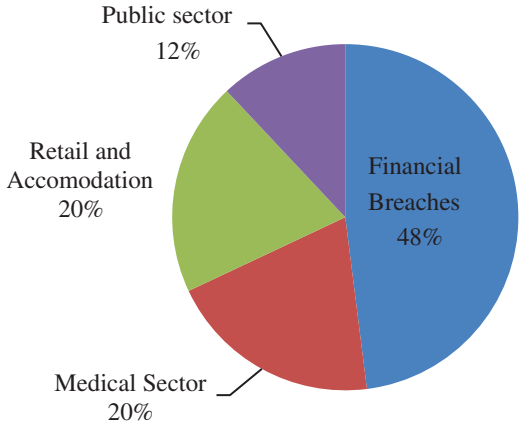

Figure 1: Pie chart of security risk

The security risk assessment of WBHMS is categorized into three sub-levels risk ID, risk investigation, and risk prioritization. Security risk has to be controlled by the developer by estimating it in two ways, security risk objective and by risk observation. On the other hand, the developers of web-based applications or software has categorized the task of development into a huge, large, and small hospital management application. Their definition depends on the number of lines of code (LOC), the term of the task, and the number of designers associated with the undertaking. According to [4], "WBHMS broadens regularly pass on the equal or more risk as do immense endeavors." Hence, from the perspective of achieving optimal security in the organizations, this examination proposes a consolidated F-AHPTOPSIS methodology to ascertain the heaviness of each security model and sub-foundation. Secure WBHMS allows patients' data to be saved as records and enables easy accessibility of data. Moreover, secure WBHMS also highlights the theft and misplacement of data.

Our paper will essentially concentrate on security risk assessment for the hospital management application developer and user framework. Further, the principal objective of this quantitative analysis is to give the developer a thoughtful approach for estimating the present degree of risk evaluation. The paper also gives data about different kinds of risk appraisal models and techniques that are found in the writing depending on the setting of risk evaluation.

The structure of this paper is as follows: Section 2 enumerates the related work done in the context of security risk assessment. Section 3 discusses different security risks based on WBHMS. Section 4 entails the methodology of F-AHPTOPSIS that we adopted for our research work. Section 5 details the calculations done on the empirical data. Section 6 presents a comparative analysis of the results with the classical method, and Section 7 of this study discusses the results. Section 8 concludes the study.

2 Related Work

Research initiatives to equate utility and practicality with assurance and security are already underway or have been attempted prievously. Moreover, several studies have been done on the creation, application, and apprising of security efforts [5,6]. Some of the noted investigations in this league are enunciated underneath:

Zech et al. [7] have presented a new approach of vulnerability detection which is useful for our study of security risk analysis of WBHMS. The authors have presented the knowledge-based security approach for vulnerability detection.

Sunitha et al. [8] present a technique for learning-based security testing by rationale programming on Web-based emergency clinic plan frameworks. This system conquers the current common spotlight on utilitarian or non-practical necessities just as the necessary elevated level of security information when performing non-useful security testing. The study shows the technique's viability in recognizing vulnerabilities in WBHMS, its incentive in making programming framework progressively secure. This component forestalls URL, XSS, and SQL infusion vulnerabilities at the customer side. The approach is useful to understand the security risk in WBHMS.

Schauer et al. [9] proposed a MITIGATE system to dissect the threat of security in the development of a web application network which gives a refreshed risk assessment of digital resources inside every partner and interconnection among those partners. This approach provides a mathematical conclusion and detects the vulnerability of different risks in web-based application security.

Kruse et al. [10] proposed a well-characterized paradigm to gauge the probability and the effect of a protection hazard. The study proposes a Fuzzy multi-criteria basic leadership way to methodically measure the seriousness of protection dangers while demonstrating the imprecision and dubiousness inborn in semantic evaluation. This paper helps us to estimate the risk assessment by the fuzzy multi-criteria decision-making process.

Ionita et al. [11] investigated issues which can be tended to by a structure that uses a hazard evaluation process, the methodology features the significance of every security highlight to item proprietors while guaranteeing that the learning and time required to actualize security necessities are made accessible to the designers.

Radanliev et al. [12] presented a model that has a structured procedure with new hazard evaluation vectors, explicit for IoT digital risk. The study shows the present holes in digital hazard guidelines and strategies and characterizes the structure standards of future digital risk sway appraisal by a model for sway evaluation of IoT digital risk.

Akinrolabu et al. [13] proposed the Cloud Supply Chain Cyber Risk Assessment model, a quantitative hazard evaluation model that is upheld by cloud provider security appraisal and cloud store network mapping. Utilizing this model, the study surveys the danger of a customer

relationship management (CRM) application, mapping for recognizing frail connections, and assessing its security dangers.

The ensuing paragraphs cites the research studies that were based on the development of fuzzy AHP and fuzzy TOPSIS. Studies that were integral to our research premise were:

Memari et al. [14] presented a not equivalent F-TOPSIS strategy to choose the privilege practical provider that worries nine criteria and thirty sub-criteria for a car extra parts producer. This methodology gives a reasonable positioning of providers and a solid answer for practical sourcing choices. This paper gave the idea of the F-TOPSIS approach in our study on WBHMS.

Dezert et al. [15] gave the methodology of the multi-criteria basic leadership strategies for positioning solid blend variables and delegate blend structure techniques. The study outlined a structure to recognize basic blend elements found from the solid blend plan strategies for superior solid by utilizing the two-stage AHP and TOPSIS approaches. In multi-criteria decision making, both (F-AHP and F-TOPSIS) are very useful.

Mokhtar et al. [16] proposed a system dependent on the F-AHP and fuzzy method for requesting execution to recognize and rank the dangers of Internet money. This examination characterized risk factors and investigated which components ought to be essentially considered. Given the examination, the study discovered that the monetary hazard is at a significant level.

Zhang et al. [17] built up a fuzzy Delphi-AHP TOPSIS system to recognize obstructions in rising innovation appropriation. This system explores the obstacles for huge information investigation to be received in the sea business.

Dao et al. [18] managed observational research on applying a blend of the F-AHP and the F-TOPSIS to gauge natural clashes developing because of titan mining in Vietnam. The approach joins the F-AHP and the F-TOPSIS to rank ecological clashes.

Solanki et al. [19] proposed a coordinated approach dependent on Strengths, Weaknesses, Opportunities, and Threats (SWOT) examination, AHP, and F-TOPSIS to assess vitality systems for supportable vitality arranging. The SWOT investigation is utilized to decide the elements and sub-factors basic for economic vitality arranging. Accordingly, AHP, a Multi-Criteria Decision Making (MCDM) strategy is utilized to decide loads of each factor and sub-factor.

After a detailed analysis of the above-mentioned studies, we found that these endeavors had worked on relevant approaches required to address the objectives of our research on security risk assessment in WBHMS. As cited in the references, many authors have mentioned different factors that affect the security of the web-based application, and they have also employed the methodology of F-AHP and F-TOPSIS which gives the weight and rank of the factors and its different alternatives. For the assessment of risk, we have used the F-AHP method to obtain the weight of the factors and by F-TOPSIS methodology we have given the different factors the privileged ranking.

3 Security Risk of WBHMS Design

There has been an abrupt and alarming increase the instances of security violence, data breaching, loss of confidentiality and integrity of patients' data in the recent years. These episodes are like cyber assault on the patients, workers, and workplaces. The digital risk on the crisis facilities has been on the rise in the world and it is not confined to any one country. Computerized violence is boundless and has affected different crisis facilities in both the significant compensation countries like the United States, or in low-focus pay countries like Kenya [20]. A report by the

US Department of Justice revealed an appalling fact about Ransomware which is only one sort of malware undermining prosperity workplaces. The report stated that nearly 4000 ransomware ambushes happened each day across different portions in 2018, an increase by 300% since 2017 [3].

The report also discovered the best three sections that were most affected by ransomware. Other than ransomware, there has also been a four-fold increase in the amount of malicious PC programming attacks over the last two years and the prosperity region has ended up being one of the most coordinated zones comprehensively. This is creating stress as centers worldwide are wrapping up their crisis facility information structures for definitive, cash related, and helpful errands along with the usage of related restorative contraptions, circulated capacity organizations, and simultaneously rising framework systems. Further, in a WBHMS design,many security risks have been shown in Fig. 2.

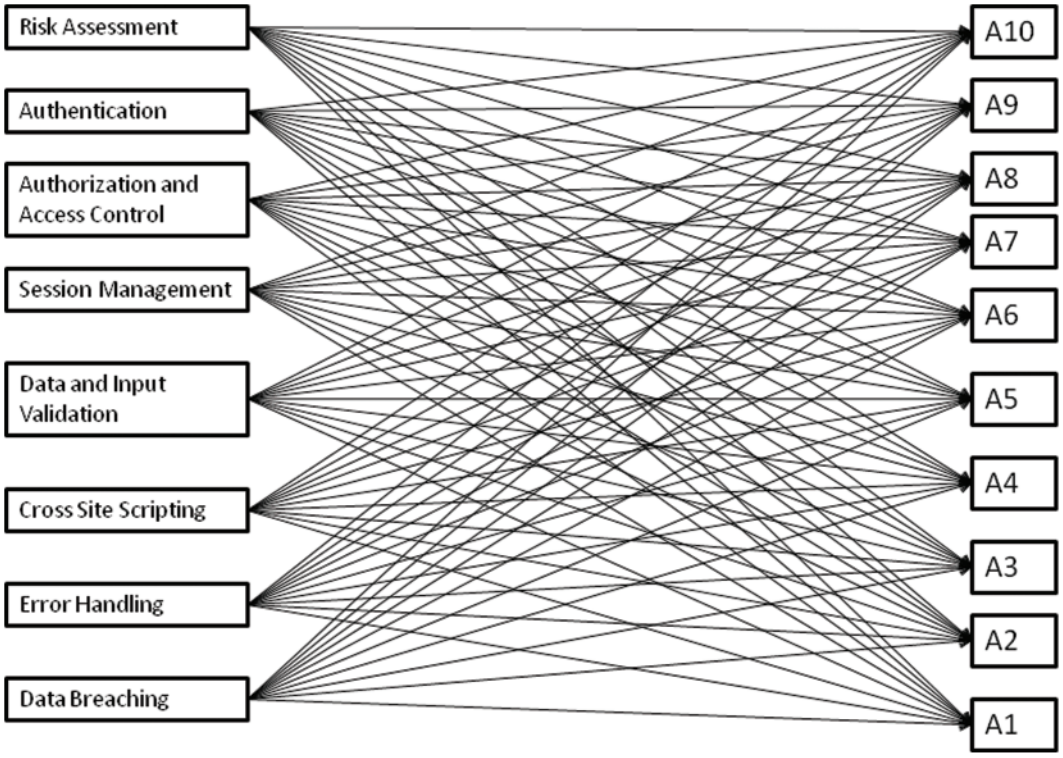

Figure 2: Different factors and alternatives to security risk

Furthermore, Fig. 2 above illustrates the security risks associated with WBHMS. Different security risks are: Risk assessment, authentication, authorization, and access control, session management, data and input validation, cross scripting, error handling, and data breaching. Each of these are connected to every individual attribute from (A1–A10 are security attribute or alternatives). Furthermore, each security risk is connected with every attribute.

Risk Assessment: Is characterized as the blend of future outcomes and related vulnerabilities, it can be viewed as perfect with the triplet meaning of security chance [21].

Authentication: In security frameworks, verification is a particular form of approval. It is a way of giving people access to framework items depending on their personality. Confirmation

simply guarantees that the individual in question is indeed who he/she professes to be, yet says nothing regarding the entrance privileges of the person [22].

Authorization and Access Control: Are fundamental and essential structural components of any application's security. WBHMS framework ought to ensure front-end and back-end information and framework assets by actualizing access control confinements to perform on the information. Access control plan ought to secure against the unapproved survey, adjustment, or duplication of information, get to control components can likewise help limit malware code execution, or unapproved activities through an assailant misusing framework conditions (DNS server, ACE server, and so on). Approval is the demonstration of verifying whether a client has the correct authorization to get to a specific record or play out a specific activity, expecting that client has effectively confirmed himself. It is particularly qualification centered and subordinate around explicit principles and access control records preset by the WBHMS [23].

Session Management: Is an instrument of essential security segment in the expansive scope of the WBHMS course of action frameworks. HTTP is a stateless convention and the session encourages the applications to extraordinarily decide a specific client over a few quantities of discrete demands just as to deal with the information which it collects about the position of the cooperation of the client with the application. It turns into the ideal objective for the security threat against the application. On the other hand, if the hackers can break the session at the board of any application, they can undoubtedly sidestep the entire confirmation controls and cover-up as different clients without having their certifications [24].

Data and Input Validation: Web-based application or software regularly upgrade numerous structures and algorithms for web components that enable the users to login and submit information. The back-end databases will execute this information. Users can, purposefully or inadvertently, enter inappropriate information that, if arrives at those back-end databases, may cause certain genuine harming issues. For appropriate User interface configuration just as for security reasons, it is significant for website specialists to consider input-approval procedures at the User interface level or as right on time as could be expected under the circumstances [25].

Cross-Site Scripting (XSS): Is a kind of infusion security assault in which an assailant infuses information, for example, malware content, into content from generally confided in sites. Cross-webpage scripting assaults happen when an untrusted source is permitted to infuse its code into a Web-based medical clinic plan framework and that pernicious code is incorporated with dynamic substance conveyed to an unfortunate casualty's program [26].

Error Handling: Inappropriate action on blunders can present a variety of security issues for a web-based application or software. One of the issues raised is that of the nitty-gritty inside error messages, for example, stack overflows, dumps of databases, and blunder codes are shown to the client (programmer). These error messages uncover usage subtleties that should not be uncovered [27].

Data Breaches: An information break is an affirmed episode of information being intruded upon or potentially revealed in an unapproved design. Information ruptures may include Personal Health Information (PHI), Personally Identifiable Information (PII), Exchange privileged insights, or protected innovation. On the off chance that any individual who is not explicitly approved to do so intrudes upon such information, the association accused of securing that data is said to have endured an information break. While programmers and cybercriminals frequently cause information ruptures, there are likewise occurrences where ventures or government offices accidentally uncover touchy or secret information on the web [28].

The different alternatives (A1–A10) are-mediXcel EMR (A1), Trio HIS (A2), Caresoft HIS (A3), GeniPulse (A4), LiveHealth For diagnostic (A5), Visual Hospital Management (A6), eHospital (A7), Medisteer (A8), HospiLogix (A9) and NextGen (A10). These are the various hospital management web-based applications that we have used as the alternatives from the location of the local hospital of Varanasi, India.

4 Methodology

The WBHMS design is highly diverse and heterogeneous due to various complex processes. Nowadays health sector is skilled with a great deal of dynamic change like data collection and its security [29–31]. Therefore, the security features in the health sector and WBHMS design have improved the different attributes such as risk assessment, authorization, etc. [32–40]. Keeping in view this background, we proposed the F-AHPTOPSIS approach for the risk assessment in WBHMS. For the proposed study, we have taken eight factors or security risks that are based on WBHMS and different applications which we have mentioned above in Section 3 (A1–A10). Each alternative is connected to each factor. We have to calculate the weights of factors which affect the WBHMS by Fuzzy-AHP [41–45]. After getting the weight, we further evaluated the rank by using Fuzzy-TOPSIS. These procedures have been explicated in Fig. 3.

Flow graph of methodology F-AHPTOPSIS is depicted in Fig. 3. There are three major categories: Pre–processing, Fuzzy-AHP, and Fuzzy-TOPSIS. From the analysis of the literature, we listed the different security risks. Then we identified the criteria and determined the risks which further passed through the risk criteria. Fuzzy-AHP was employed to select the multi-criteria decision making between different alternatives [46–50]. The four steps of the procedure included:

First, make a security matrix and compare it pair-wise.

Second, check the further assessment with the condition of the existence of a security attribute after the comparison of condition.

Third, assigning access after the Fuzzy-AHP process.

Fourth, aggregate the rating and calculate the weight of security risk and rank it [51–54].

The different factors (F1–F8) and different attributes/alternatives (A1–A10) are connected which is shown in Fig. 2. Factors are the security risks, and the alternatives are the applications being used in the hospitals of Varanasi, India. We have calculated the weight of the factors with the effect of alternatives and ranked them according to our methodology by using F-AHPTOPSIS. After this, calculated the degree of closeness.

The Usable-security WBHMS plan framework is an accurate mechanism aand also a premise for further research [55–58]. Furthermore, Decision Making issues are consistently experienced for accomplishing the clients' targets and affectability of the data. Numerous methodologies or estimations exist in the writing that can be applied to clear up such issues. For impost of usable-security, Fuzzy-AHP is a truly appropriate technique instead of the other multi-criteria strategies. However, Fuzzy-AHP can't resolve the basic lack of clarity and imprecision of a decision inconceivably vague for research. Further, the F-AHP system is essentially founded on the unstable size of decisions. The F-AHP also has a few issues of its own [59–61]. Thus, a consolidated Fuzzy procedure of F-AHPTOPSIS is a special strategy that could help in the productive evaluation of options.

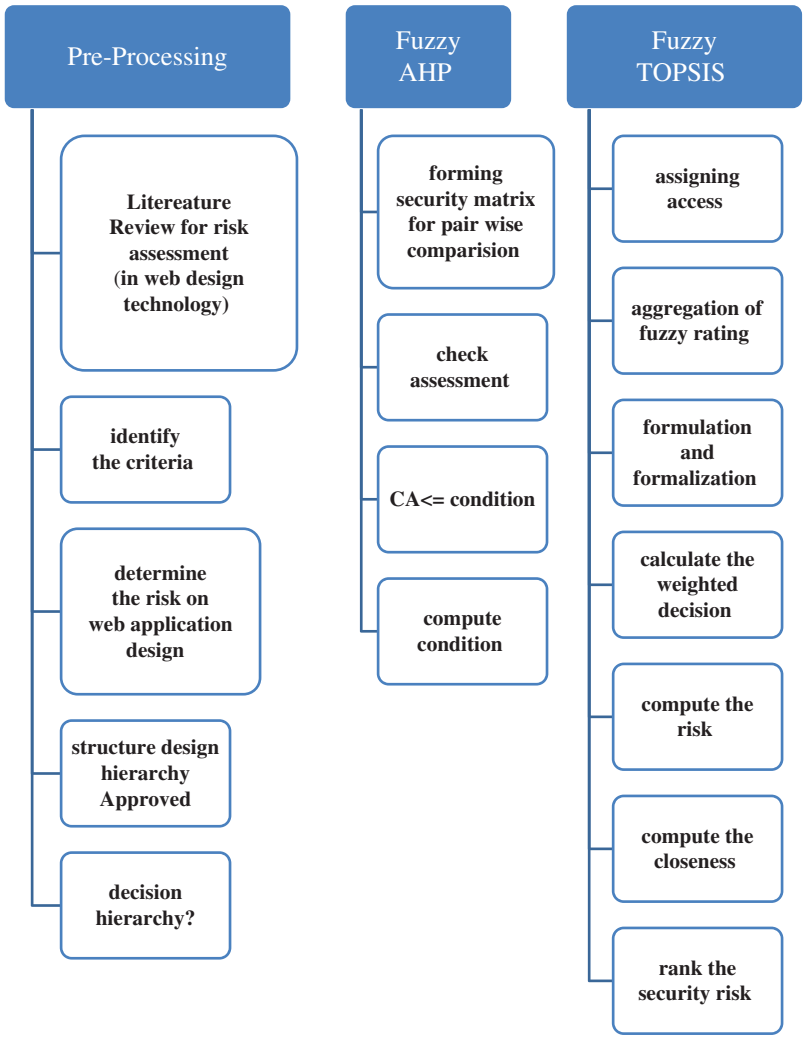

Figure 3: Flow diagram of fuzzy AHP-TOPSIS

4.1 Fuzzy-AHP

Fuzzy-AHP is the methodology used to cure hard choice issues, Fuzzy-AHP is a prized procedure and every perplexing issue might be inspected by methods for phenomenal arranged scopes of objectives, i.e., chain of command. The issue is isolated directly into a tree shape to clarify it through utilizing Fuzzy-AHP. The connectivity shape has been given in Fig. 2. This connectivity shape is prepared by utilizing experts' perspectives [62]. The following stage is building the triangular fuzzy number (TFN) from the hierarchal structure. With the help of the effect of one standard on various criteria, span examination of each gathering of ordered objectives becomes an indispensable job.

The accompanying advance is changing over etymological qualities into fresh numbers and TFN. In this investigation, creators utilize the TFN which lies somewhere in the range of 0 and 1 [63]. The reason for such selection of TFN is the computational straightforwardness of TFN enrollment capacities and their capacity to manage Fuzzy information [64,65]. Further, the phonetic qualities have been named as: *similarly significant, feebly significant*, and so forth, and

fresh qualities are classified as *1–9*. Besides this, a Fuzzy Number P on Q is called TFN, if its participation capacities are recognized in conditions (1) and (2):

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

$$\mu_a(x) = \begin{cases} \dfrac{x}{cf-l} - \dfrac{l}{cf-l} x \in [l, cf] \dfrac{x}{cf-mb} - \dfrac{mb}{cf-mb} x \in [cf, mb] \end{cases} \tag{2}$$

Here l, *cf*, and *mb* are given as a lower limit, center farthest point, and maximum breaking point, respectively, in the triangular enrollment work, Fig. 4, Portrays TFN.

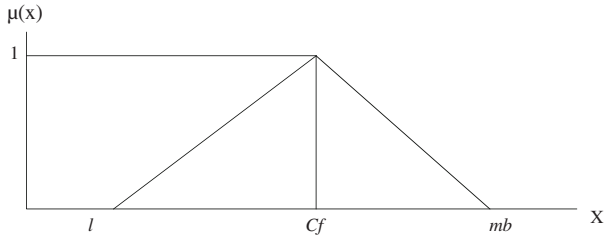

Figure 4: Triangular fuzzy numbers

TFN is denoted as (*l*, *cf*, *mb*). Specialists designated marks to the elements influencing the qualities in a computable manner as indicated by the scale that is exhibited in Tab. 1.

Table 1: TFN scale

Saaty scale definition	Fuzzy triangle scale	
1	Identical significant	(1, 1, 1)
3	Feebly significant	(2, 3, 4)
5	Justly significant	(4, 5, 6)
7	Sturdily significant	(6, 7, 8)
9	Categorically significant	(9, 9, 9)
2	Irregular tenets among two contiguous measures	(1, 2, 3)
4		(3, 4, 5)
6		(5, 6, 7)
8		(7, 8, 9)

The conditions (3)–(6) were used for changing the numeric qualities into TFN that are assigned as (l_{ij}, cf_{ij}, mb_{ij}) where l_{ij} is lower esteem, cf_{ij} is center worth and mb_{ij} is highest level occasions, the *i* and *j* are the row and column of the two-dimensional matrix. Furthermore, TFN [η_{ij}] is perceived as:

$$\Phi_{ij} = \left(l_{ij}, cf_{ij}, mb_{ij}\right) \tag{3}$$

$$where \quad l_{ij} \le cf_{ij} \le mb_{ij}$$

$$l_{ij} = cfn\left(J_{ijd}\right) \tag{4}$$

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

$$and\ mb_{ij} = max\left(J_{ijd}\right) \tag{6}$$

In the conditions (3)–(6), J_{ijd} demonstrates the near status of the qualities among two variables which is determined by professional d, where i and j imply a couple of elements being chosen by specialists. Φ_{ij} is assessed depending on the geometric mean (GM) of the master's perspectives for a particular correlation. The GM is capable of accurately joining and connoting the agreement of experts and indicates the most minimal and most elevated scores, compatibly, for the relative centrality between the two elements. Further, conditions (7)–(9) back consolidated TFN values. Consider two TFNs M1 and $M2$, $M1 = (l1, cf1, mb1)\ and\ M2 = (l2, cf2, mb2)$. The standards of activities are:

$$(l_1, cf_1, mb_1) + (l_2, cf_2, mb_2) = (l_1 + l_2, cf_1 + cf_2, mb + mb_2) \tag{7}$$

$$(l_1, cf, mb_1) \times (l_2, cf_2, mb_2) = (l_1 \times l_2, cf_1 \times cf_2, mb_1 \times mb_2) \tag{8}$$

$$(l_1, cf_1, mb_1)^{-1} = \left(\frac{1}{mb_1}, \frac{1}{cf_1}, \frac{1}{l_1}\right) \tag{9}$$

After getting the TFN esteems for each pair of examination, a Fuzzy span correlation framework is developed as $n \times n$ lattice with the assistance of condition (10).

$$\widetilde{A^d} = \left[\widetilde{k}_{11}^d \widetilde{k}_{12}^d \ldots \widetilde{k}_{1n}^d \widetilde{k}_{21}^d \widetilde{k}_{22}^d \ldots \widetilde{k}_{2n}^d \cdots \widetilde{k}_{n1}^d \widetilde{k}_{n2}^d \ldots \widetilde{k}_{nn}^d\right] \tag{10}$$

where $\widetilde{k}_{ij}^k$ represents the dth leaders' inclination of the ith criteria over the jth criteria. If more than one chief is available, at that point the normal of the inclinations of every leader is obtained with the assistance of condition (11).

$$\widetilde{k}_{ij} = \sum_{d=1}^{d} \widetilde{k}_{ij}^d \tag{11}$$

Next stage is to refresh the span correlation frameworks for all elements in the chain of importance based on the middle value of inclinations with the assistance of condition (12).

$$\widetilde{A} = \left[\widetilde{k}_{11} \ldots \widetilde{k}_{1n} \cdots \ddots \cdots \widetilde{k}_{n1} \cdots \widetilde{k}_{nn}\right] \tag{12}$$

After this, we utilized the GM method as stated in condition (13) to depict the Fuzzy GM and Fuzzy loads of each factor.

$$\widetilde{p}_i = \left(\prod_{j=1}^{n} \widetilde{k}_{ij}\right)^{\frac{1}{n}}, \quad i = 1, 2, 3 \ldots n \tag{13}$$

The following stage is to finish up the Fuzzy load of the factor with the assistance of the condition (14).

$$\widetilde{w}_i = \widetilde{p}_i \otimes (\widetilde{p}_1 \oplus \widetilde{p}_2 \oplus \widetilde{p}_3 \cdots \oplus \widetilde{p}_n)^{-1} \tag{14}$$

Further, to determine the normal and standardized weight criteria with the assistance of conditions (15) and (16).

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

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

Moreover, the center of area (COA) strategy is utilized to compute the best non-fuzzy performance (BNP) estimation of the Fuzzy loads on estimation with the assistance of condition (17).

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

4.2 Fuzzy-TOPSIS

With P options as a geometrical course of action, m focuses inside the n-dimensional region of the issue; TOPSIS points of view afford a multi gauges choice, thus creating several ambiguities. For TOPSIS, the methodology utilized in this research is fundamentally based on the possibility that a labeled open door has the most limited and is farthest from the positive perfect arrangement and the negative perfect answer for ideal and least perfect arrangements, separately [64]. Experts face problems in distributing a particular exhibition score to an option in the context of criteria [65]. For consistency with this present Fuzzy condition, TOPSIS doles out Fuzzy numbers that align with exact numbers for representing the general centrality of criteria. Also, the F-AHPTOPSIS approach is also the most conversant approach for fixing cooperative choice-making issues underneath Fuzzy situations. F-AHPTOPSIS procedure is enlisted below:

The initial step is to choose loads of the appraisal criteria. This study applies Fuzzy-AHP to finish up Fuzzy decision loads with the assistance of conditions (1)–(16). Further, the analysts make the Fuzzy choice framework and pick the perfect semantic factors as substitutions for the criteria with the help of conditions (18) and Tab. 2.

$$\widetilde{K} = \begin{array}{c} \\ A_1 \\ \cdots \\ A_m \end{array} \begin{array}{c} \begin{array}{ccc} C_1 & \cdots & C_n \end{array} \\ \begin{bmatrix} \widetilde{x}_{11} & \cdots & \widetilde{x}_{1n} \\ \cdots & \ddots & \cdots \\ \widetilde{x}_{m1} & \cdots & \widetilde{x}_{mn} \end{bmatrix} \end{array} \tag{18}$$

where, $\widetilde{x}_{ij} = \frac{1}{D}\left(\widetilde{x}_{ij}^1 \cdots \oplus \widetilde{x}_{ij}^d \oplus \cdots \widetilde{x}_{ij}^D\right)$, and $\widetilde{x}_{ij}^d$ is the performance rating of the alternative A_i concerning factor C_j estimated by the dth practitioner and $\widetilde{x}_{ij}^d = (l_{ij}^d, mi_{ij}^d, u_{ij}^d)$.

The following stage is to standardize the Fuzzy choice grid with the help of the condition (19). The standardized Fuzzy choice lattice is denoted by P as follows:

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

Table 2: Verbal scales

Verbal variable (VV)	Corresponding TFN
Very poor (VP)	(0, 1, 3)
Poor (P)	(1, 3, 5)
Fair (F)	(3, 5, 7)
Good (G)	(5, 7, 9)
Very good (VG)	(7, 9, 10)

Thereafter, the stabilization procedure can be realized with the help of Eq. (20).

$$\widetilde{p}_{ij} = \left(\frac{l_{ij}}{u_j^+}, \frac{mi_{ij}}{u_j^+}, \frac{u_{ij}}{u_j^+} \right), \quad u_j^+ = \max\{u_{ij},\, i = 1, 2, 3, \ldots, n\} \tag{20}$$

On the other hand, we can set the best-wanted level to be equivalent to 1; generally, the most noticeably awful is 0. The standardized values keep on being TFNs. For TFN, the standardization procedure can be performed comparably. The weighted Fuzzy standardized choice lattice ($\widetilde{Q}$) is measured with the assistance of the condition (21).

$$\widetilde{Q} = [\widetilde{q}_{ij}]_{m\times n} \quad i = 1, 2, \ldots, m;\, j = 1, 2, 3 \ldots n \tag{21}$$

where, $\widetilde{q}_{ij} = \widetilde{p}_{ij} \otimes \widetilde{w}_{ij}$ and after that, characterize the fuzzy positive-ideal solution (FPIS) and fuzzy negative-ideal solution (FNIS). The weighted standardized Fuzzy choice lattice shows that the components $\widetilde{q}_{ij}$ are standardized positive TFN and their extents have a place with the shut interim [0,1]. From there on, we can depict the FPIS T^+ (goal levels) and FNIS R^- (the most exceedingly awful levels) as appeared in conditions (22) and (23).

$$T^+ = \left(\widetilde{q}_1^*, \ldots \widetilde{q}_j^*, \cdots \widetilde{q}_{n,}^* \right) \tag{22}$$

$$R^- = \left(\widetilde{q}_1^*, \ldots \widetilde{q}_j^*, \ldots, \widetilde{q}_n, ^* \right) \tag{23}$$

where, $\widetilde{q}_1^* = (1, 1, 1) \bigotimes \widetilde{w}_{ij} = \left(Lw_j, Mw_j, Hw_j \right)$ *and* $\widetilde{q}_{ij}^- = (0, 0, 0)$, $j = 1, 2, 3 \ldots n$. For ascertaining the separation of every option from FPIS and FNIS, the separations ($\widetilde{d}_i^+$ and $\widetilde{d}_i^-$) of every option from A^+ and A^- can be evaluated by utilizing the territory remuneration procedure as given in the conditions (24) and (25).

$$\widetilde{d}_i^+ = \sum_{j=1}^{n} d\left(\widetilde{q}_{ij}, \widetilde{q}_{ij}^* \right) \quad i = 1, 2, \ldots, m;\, j = 1, 2, 3 \ldots n \tag{24}$$

$$\widetilde{d}_i^- = \sum_{j=1}^{n} d\left(\widetilde{q}_{ij}, \widetilde{q}_{ij}^* \right) \quad i = 1, 2, \ldots, m;\, j = 1, 2, 3 \ldots n \tag{25}$$

Closeness coefficients (relative holes' degree) are determined in the subsequent stage and build up the choices to accomplish the desire levels in each factor. The closeness coefficient is cleared to assess the Fuzzy holes' degree based on the Fuzzy nearness coefficients to progress

the options [36]. When $\widetilde{d}_i^+$ and $\widetilde{d}_i^-$ of every option have been assessed, the likenesses to the perfect arrangement are determined. This progression comprehends the similitude to a perfect arrangement as in condition (26).

$$C\widetilde{C}_i = \frac{\widetilde{k}_i^-}{\widetilde{k}_i^+ + \widetilde{k}_i^-} = 1 - \frac{\widetilde{k}_i^+}{\widetilde{k}_i^+ + k_i^-}, \quad i = 1, 2, \ldots, m \tag{26}$$

Here, $\frac{\widetilde{k}_i^-}{\widetilde{k}_i^+ + \widetilde{k}_i^-}$-defined as fuzzy satisfaction degree in the ith alternative, $\frac{\widetilde{k}_i^+}{\widetilde{k}_i^+ + \widetilde{k}_i^-}$-defined as a fuzzy gap degree in the ith alternative. Based on their positions, the options are achieved. The next procedure is to evaluate the usable-security with the assistance of its contributing characteristics.

5 Empirical Data Analysis

F-AHPTOPSIS methodology, Fuzzy-AHP process gives the weight of the risk attributes (A1–A10) which we have mentioned in Eqs. (1)–(17) from different risks which are shown in Fig. 2. Fuzzy TOPSIS process gives the ranks of security risks. After getting weights and ranks of the security risks, we determined the degree of closeness and analyzed whether this result should be used in WBHMS software application in the local hospitals of Varanasi. Though, subjective estimation is appropriate for evaluating security chance, it is hard to assess WBHMS quantitatively. In this context, the worldwide aggregate activity has prompted the detailing of hazard appraisal. Recently, the specialists have received hazard evaluation and projects, as it were, Dammak et al. [32] with enormous outcomes. Likewise, associations are attempting to receive high security of web applications. Hence, the security variables' effect assumes a critical job in the WBHMS advancement process [33]. The ensuing column tabulates a standard procedure for WBHMS structure estimation through F-AHPTOPSIS. We have already deliberated upon the WBHMS in the past segments.

As Fig. 2 shows a trait of the order at one level affects the other properties of a more significant level, yet its effect isn't the equivalent on them. It might vary. With the end goal of appraisal, we changed over the grouped properties into chains of importance and indicated it in Fig. 2. For the assurance of evaluation, variables of secrecy as for reasonable security at level 2 are denoted as F1, F2,..., F8. Properties of uprightness as for practical security at level 2 are spoken to as A1–A10. As depicted in Fig. 2, with the assistance of these chains of importance, we assessed the safe WBHMS. For gathering the information with the assistance of conditions (1)–(26), secure WBHMS through Fuzzy AHP-TOPSIS has been assessed as:

With the assistance of Tab. 1 and, conditions (1)–(9), creators changed over the etymological qualities into numeric qualities and collected TFNs values. For developing the span examination grid, TFNs qualities have been registered in Tabs. 3–8.

Tab. 3. shows the different security risk be F1–F8 and its TFN its weights and BNP have been shown in Tab. 4.

The fuzzy-AHP process gives the weight of different security risks which we have mentioned in Tab. 4. The following rank of different attributes according to the rank is-authentication (F1), risk assessment (F2), session management (F3), authorization, and access control (F4), error handling (F5), cross-site scripting (F6), data breaches (F7) and data and input validation (F8). These are the weights of different risks through Fuzzy-AHP.

Table 3: Fuzzy AHP aggregated pair-wise matrix

	F1 (Risk assessment)	F2 (Authentication)	F3 (Authorization and access control)	F4 (Session management)	F5 (Data and input validation)	F6 (Cross site scripting)	F7 (Error handling)	F8 (Data breaches)
F1	1.0000, 1.0000, 1.0000	0.9000, 1.1000, 1.4000	1.2000, 1.5000, 1.7000	0.9000, 1.0000, 1.1000	2.1000, 2.9000, 3.8000	1.1000, 1.3000, 1.6000	2.1000, 2.9000, 3.8000	0.9000, 1.1000, 1.4000
F2	0.7000, 0.9000, 1.1000	1.0000, 1.0000, 1.0000	1.1000, 1.6000, 1.9000	1.8000, 1.9000, 2.1000	2.7000, 3.4000, 4.0000	2.1000, 2.7000, 3.2000	2.7000, 3.4000, 4.0000	1.0000, 1.0000, 1.0000
F3	0.6000, 0.7000, 0.8000	0.5000, 0.6000, 0.9000	1.0000, 1.0000, 1.0000	1.4000, 1.6000, 1.9000	1.7000, 2.2000, 2.9000	1.7000, 2.1000, 2.6000	1.7000, 2.2000, 2.9000	0.5000, 0.6000, 0.9000
F4	0.9000, 1.0000, 1.2000	0.5000, 0.5500, 0.6000	0.5000, 0.6000, 0.7000	1.0000, 1.0000, 1.0000	1.9000, 2.5000, 2.7000	1.6000, 2.5000, 2.6000	1.9000, 2.5000, 2.7000	0.5000, 0.5500, 0.6000
F5	0.3000, 0.3000, 0.5000	0.3000, 0.3500, 0.4000	0.3000, 0.5000, 0.7000	0.3000, 0.4000, 0.5000	1.0000, 1.0000, 1.0000	1.0000, 1.1000, 1.3000	1.0000, 1.0000, 1.0000	0.3000, 0.3500, 0.4000
F6	0.7000, 0.8000, 1.0000	0.3000, 0.4000, 0.5000	0.4000, 0.5000, 0.6000	0.4000, 0.5000, 0.6000	0.8000, 0.9000, 1.1000	1.0000, 1.0000, 1.0000	0.8000, 0.9000, 1.1000	0.3000, 0.4000, 0.5000
F7	2.1000, 2.9000, 3.8000	2.7000, 3.4000, 4.0000	1.7000, 2.2000, 2.9000	1.9000, 2.5000, 2.7000	1.0000, 1.0000, 1.0000	0.8000, 0.9000, 1.1000	1.0000, 1.0000, 1.0000	2.7000, 3.4000, 4.0000
F8	0.9000, 1.1000, 1.4000	1.0000, 1.0000, 1.0000	0.5000, 0.6000, 0.9000	0.5000, 0.5500, 0.6000	0.5000, 0.5500, 0.6000	0.3000, 0.3500, 0.4000	0.3000, 0.4000, 0.5000	1.0000, 1.0000, 1.0000

Table 4: Weights of factors

Factors	Weights	BNP	Rank
F1	0.1500, 0.1800, 0.2100	0.1600	2
F2	0.1900, 0.2000, 0.2200	0.1900	1
F3	0.1300, 0.1600, 0.1900	0.1500	4
F4	0.1200, 0.1500, 0.1800	0.1600	3
F5	0.0600, 0.0800, 0.1000	0.0700	8
F6	0.0700, 0.0900, 0.1300	0.0900	6
F7	0.0800, 0.1000, 0.1300	0.1000	5
F8	0.0500, 0.0800, 0.1200	0.0800	7

Tabs. 5–7 are the different values of subjective cognition result mentioned in Eq. (20), normalized fuzzy decision matrix in Eq. (18), and weighted normalized decision matrix in Eqs. (24), (25). These values are taken through the Fuzzy-TOPSIS methodology.

Tab. 8. from fuzzy TOPSIS methodology, from Eq. (26), gives the degree of closeness. The degree of closeness of different attributes of security risk in WBHMS is shown in Fig. 2. The result of security risks (F1–F8) and their attributes (A1–A10) in WBHMS is in satisfactory condition due to the data of local hospitals of Varanasi, UP, India. Further, we have mentioned the degree of closeness in a bar chart as shown in Fig. 5.

Table 5: Subjective cognition results

Factors/ Alternatives	A1	A2	A3	A4	A5	A6	A7	A8	A9	A10
F1	5.0000, 7.0000, 8.9000	4.4000, 6.4000, 8.4000	4.4000, 6.4000, 8.3000	2.6000 4.6000 6.6000	4.4000 6.4000 8.4000	4.4000 6.4000 8.3000	2.6000 4.6000 6.6000	4.4000 6.4000 8.4000	4.4000, 6.4000, 8.3000	2.6000, 4.6000, 6.6000
F2	5.2000, 7.2000, 9.0000	4.6000 6.6000 8.6000	3.8000 5.8000 7.7000	2.6000 4.6000 6.6000	4.6000 6.6000 8.6000	3.8000 5.8000 7.7000	2.6000 4.6000 6.6000	4.6000, 6.6000, 8.6000	3.8000, 5.8000, 7.7000	2.6000, 4.6000, 6.6000
F3	4.6000, 6.6000, 8.6000	3.6000, 5.6000, 7.6000	4.0000 6.0000 7.9000	3.0000 5.0000 7.0000	3.6000 5.6000 7.6000	4.0000 6.0000 7.9000	3.0000 5.0000 7.0000	3.6000, 5.6000, 7.6000	4.0000, 6.0000, 7.9000	3.0000, 5.0000, 7.0000
F4	5.6000 7.6000 9.2000	4.8000, 6.8000, 8.7000	4.6000 6.6000 8.4000	3.2000 5.2000 7.2000	4.8000 6.8000 8.7000	4.6000 6.6000 8.4000	3.2000 5.2000 7.2000	4.8000, 6.8000, 8.7000	4.6000, 6.6000, 8.4000	3.2000, 5.2000, 7.2000
F5	4.8000 6.8000 8.7000	4.0000, 6.0000, 8.0000	3.8000 5.8000 7.8000	2.6000 4.6000 6.6000	4.0000 6.0000 8.0000	3.8000 5.8000 7.8000	2.6000 4.6000 6.6000	4.0000, 6.0000, 8.0000	3.8000, 5.8000, 7.8000	2.6000, 4.6000, 6.6000
F6	5.0000 7.0000 9.0000	4.4000, 6.4000, 8.4000	4.2000 6.2000 8.1000	2.5000 4.4000 6.4000	4.4000 6.4000 8.4000	4.2000 6.2000 8.1000	2.5000 4.4000 6.4000	4.4000, 6.4000, 8.4000	4.2000, 6.2000, 8.1000	2.5000, 4.4000, 6.4000
F7	4.6000 6.6000 8.6000	3.6000, 5.6000, 7.6000	4.0000 6.0000 7.9000	3.0000 5.0000 7.0000	3.6000 5.6000 7.6000	4.0000 6.0000 7.9000	3.0000 5.0000 7.0000	3.6000, 5.6000, 7.6000	4.0000, 6.0000, 7.9000	3.0000, 5.0000, 7.0000
F8	5.6000 7.6000 9.2000	4.8000, 6.8000, 8.7000	4.6000 6.6000 8.4000	3.2000 5.2000 7.2000	4.8000 6.8000 8.7000	4.6000 6.6000 8.4000	3.2000 5.2000 7.2000	4.8000, 6.8000, 8.7000	4.6000, 6.6000, 8.4000	3.2000, 5.2000, 7.2000

Table 6: Normalized fuzzy-decision matrix

Factors/ Alternatives	A1	A2	A3	A4	A5	A6	A7	A8	A9	A10
F1	0.5000, 0.8000, 1.0000	0.4800, 0.7000, 0.9000	0.4800, 0.7000, 0.9000	0.2800, 0.5000, 0.7000	0.4800, 0.7000, 0.9000	0.4800, 0.7000, 0.9000	0.2800, 0.5000, 0.7000	0.4800, 0.7000, 0.9000	0.4800, 0.7000, 0.9000	0.2800, 0.5000, 0.7000
F2	0.6000, 0.8000, 1.0000	0.5000, 0.7000, 0.9000	0.4100, 0.6000, 0.8400	0.2800, 0.5000, 0.7200	0.5000, 0.7200, 0.9400	0.4000, 0.6000, 0.8400	0.2800, 0.5000, 0.7200	0.5000, 0.7200, 0.9400	0.4100, 0.6300, 0.8400	0.2800, 0.5000, 0.7000
F3	0.5000, 0.7000, 0.9000	0.3900, 0.6000, 0.8000	0.4000, 0.6500, 0.8600	0.3300, 0.5400, 0.7600	0.3900, 0.6000, 0.8300	0.4400, 0.6500, 0.8600	0.3300, 0.5400, 0.7600	0.3900, 0.6100, 0.8300	0.4400, 0.6500, 0.8600	0.3000, 0.5000, 0.7600
F4	0.6000, 0.8000, 1.0000	0.5000, 0.7000, 0.9500	0.5000, 0.7200, 0.9000	0.3500, 0.5700, 0.7800	0.5200, 0.7400, 0.9500	0.5000, 0.7200, 0.9100	0.3500, 0.5700, 0.7800	0.5200, 0.7400, 0.9500	0.5000, 0.7200, 0.9100	0.3500, 0.5700, 0.7800
F5	0.5000, 0.7000, 1.0000	0.4000, 0.6500, 0.8700	0.4000, 0.6000, 0.8500	0.2800, 0.5000, 0.7200	0.4400, 0.6500, 0.8700	0.4100, 0.6300, 0.8500	0.2800, 0.5000, 0.7200	0.4400, 0.6500, 0.8700	0.4100, 0.6300, 0.8500	0.2800, 0.5000, 0.7000
F6	0.5000, 0.8000, 1.0000	0.4800, 0.7000, 0.9000	0.4600, 0.6700, 0.8800	0.2700, 0.4800, 0.7000	0.4800, 0.7000, 0.9100	0.4600, 0.6700, 0.8800	0.2700, 0.4800, 0.7000	0.4800, 0.7000, 0.9100	0.4600, 0.6700, 0.8800	0.2700, 0.4800, 0.7000
F7	0.5000, 0.7000, 0.9000	0.3900, 0.6000, 0.8300	0.4000, 0.6500, 0.8600	0.3300, 0.5400, 0.7600	0.3900, 0.6100, 0.8300	0.4400, 0.6500, 0.8600	0.3300, 0.5400, 0.7600	0.3900, 0.6100, 0.8300	0.4400, 0.6500, 0.8600	0.3000, 0.5400, 0.7600
F8	0.6000, 0.8000, 1.0000	0.5000, 0.7000, 0.9500	0.5000, 0.7000, 0.9100	0.3500, 0.5700, 0.7800	0.5200, 0.7400, 0.9500	0.5000, 0.7200, 0.9100	0.3500, 0.5700, 0.7800	0.5200, 0.7400, 0.9500	0.5000, 0.7200, 0.9100	0.3500, 0.5700, 0.7800

Table 7: Weighted normalized fuzzy-decision matrix

Factors/ Alternatives	A1	A2	A3	A4	A5	A6	A7	A8	A9	A10
F1	0.0800, 0.1600, 0.2800	0.0700, 0.1500, 0.2600	0.0700, 0.1500, 0.2600	0.0400, 0.1000, 0.2100	0.0700, 0.1500, 0.2600	0.0700, 0.1500, 0.2600	0.0400, 0.1000, 0.2100	0.0700, 0.1500, 0.2600	0.0700, 0.1500, 0.2600	0.0400, 0.1000, 0.2100
F2	0.1100, 0.2000, 0.3500	0.0900, 0.1900, 0.3400	0.0800, 0.1600, 0.3000	0.0500, 0.1300, 0.2600	0.0900, 0.1900, 0.3400	0.0800, 0.1600, 0.3000	0.0500, 0.1300, 0.2600	0.0900, 0.1900, 0.3400	0.0800, 0.1600, 0.3000	0.0500, 0.1300, 0.2600
F3	0.0700, 0.1300, 0.2500	0.0500, 0.1100, 0.2200	0.0600, 0.1200, 0.2300	0.0400, 0.1000, 0.2100	0.0500, 0.1100, 0.2200	0.0600, 0.1200, 0.2300	0.0400, 0.1000, 0.2100	0.0500, 0.1100, 0.2200	0.0600, 0.1200, 0.2300	0.0400, 0.1000, 0.2100
F4	0.0800, 0.1400, 0.2300	0.0700, 0.1300, 0.2200	0.0600, 0.1200, 0.2100	0.0400, 0.1000, 0.1800	0.0700, 0.1300, 0.2200	0.0600, 0.1200, 0.2100	0.0400, 0.1000, 0.1800	0.0700, 0.1300, 0.2200	0.0600, 0.1200, 0.2100	0.0400, 0.1000, 0.1800
F5	0.0300, 0.0600, 0.1100	0.0300, 0.0500, 0.1000	0.0200, 0.0500, 0.1000	0.0200, 0.0400, 0.0900	0.0300, 0.0500, 0.1000	0.0200, 0.0500, 0.1000	0.0200, 0.0400, 0.0900	0.0300, 0.0500, 0.1000	0.0200, 0.0500, 0.1000	0.0200, 0.0400, 0.0900
F6	0.0400, 0.0700, 0.1300	0.0300, 0.0700, 0.1200	0.0300, 0.0600, 0.1200	0.0200, 0.0500, 0.0900	0.0300, 0.0700, 0.1200	0.0300, 0.0600, 0.1200	0.0200, 0.0500, 0.0900	0.0300, 0.0700, 0.1200	0.0300, 0.0600, 0.1200	0.0200, 0.0500, 0.0900
F7	0.0700, 0.1300, 0.2500	0.0500, 0.1100, 0.2200	0.0600, 0.1200, 0.2300	0.0400, 0.1000, 0.2100	0.0500, 0.1100, 0.2200	0.0600, 0.1200, 0.2300	0.0400, 0.1000, 0.2100	0.0500, 0.1100, 0.2200	0.0600, 0.1200, 0.2300	0.0400, 0.1000, 0.2100
F8	0.0800, 0.1400, 0.2300	0.0700, 0.1300, 0.2200	0.0600, 0.1200, 0.2100	0.0400, 0.1000, 0.1800	0.0700, 0.1300, 0.2200	0.0600, 0.1200, 0.2100	0.0400, 0.1000, 0.1800	0.0700, 0.1300, 0.2200	0.0600, 0.1200, 0.2100	0.0400, 0.1000, 0.1800

Table 8: Closeness coefficients to aspired level among different alternatives

Alternatives	dþi	Di	Gaps degree of CCþi	Satisfaction degree of CCi
A1 (WBHMS_A1)	0.2300	0.4900	0.6700	0.3312
A2 (WBHMS_A2)	0.8100	0.9300	0.7800	0.2224
A3 (WBHMS_A3)	0.2600	0.5100	0.6500	0.3525
A4 (WBHMS_A4)	0.3300	0.4800	0.6400	0.4055
A5 (WBHMS_A5)	0.4400	0.6100	0.5900	0.4147
A6 (WBHMS_A6)	0.2800	0.3200	0.5200	0.4849
A7 (WBHMS_A7)	0.3100	0.4200	0.5800	0.4256
A8 (WBHMS_A8)	0.4300	0.5300	0.5500	0.4551
A9 (WBHMS_A9)	0.2900	0.4400	0.5900	0.4161
A10 (WBHMS_A10)	0.3300	0.5800	0.6500	0.3589

6 Comparison with the Usual AHP TOPSIS Method

The same data results output is different when different methodologies are used [34] and the reliability and efficiency of the technique can only be verified by using different methods [35]. In this paper, we have used the F-AHPTOPSIS methodology to evaluate the efficiency and closeness

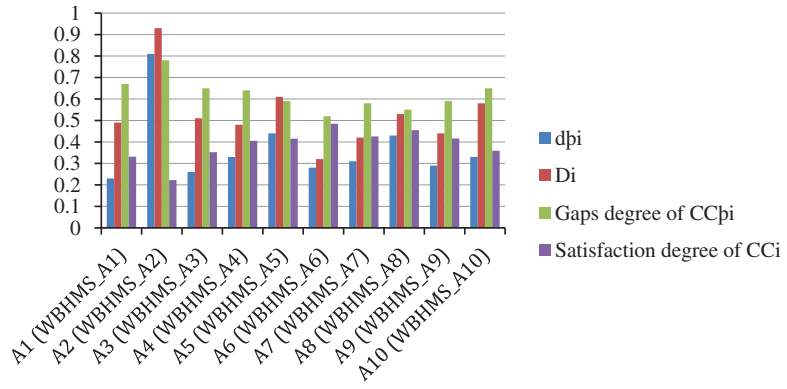

Figure 5: Graph of satisfaction degree

Table 9: The result of usual/classical methodand F-AHP and F-TOPSIS method

Methods/Alternatives	A1	A2	A3	A4	A5	A6	A7	A8	A9	A10
Fuzzy-AHP-TOPSIS	0.3312	0.2224	0.3525	0.4055	0.4147	0.4849	0.4256	0.4551	0.4161	0.3589
Classical-AHP-TOPSIS	0.3256	0.22250	0.3561	0.4058	0.4156	0.4858	0.4298	0.4660	0.4089	0.3478

or accuracy of the result obtained. In AHP-TOPSIS, the method or procedure of data compilation and estimation of that data is the same as in F-AHPTOPSIS but no fuzzification is used. Hence, for usual AHP-TOPSIS, values are taken in their real number form. The difference between the results of fuzzy and usual AHP-TOPSIS is shown in Tab. 9 and Fig. 6. The results elicited through the usual AHP-TOPSIS method are highly interrelated (Pearson correlation coefficient is 0.999176) with the results obtained through the fuzzy AHP-TOPSIS method. The reliability and efficiency of F-AHPTOPSIS is more, and it is a better procedure/method than the usual AHP TOPSIS approach.

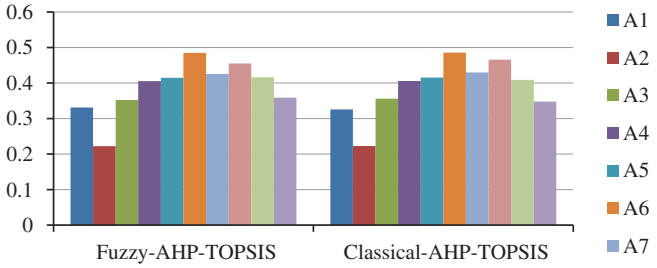

Figure 6: Variances between results

7 Sensitivity Analysis

To verify the results with each variable, we have used the sensitivity analysis [36]. This has been depicted below in Tab. 10. The sensitivity analysis is calculated by the weights of variables. In our research on WBHMS, the sensitivity analysis is verified by multiple experiments of each factor with the different experiments that showed different results, as tabulated in Tab. 10.

The satisfaction degree (CC^{-i}) is calculated by the weight of each factor (F1–F10 taken as a constant), and by F-AHPTOPSIS methodology, we calculate the (CC^{-i}).

In Tab. 10, the first row shows the original weight; Fig. 7 shows the first bunch of data. According to original weights/results, the alternative-8 (F1–F8) has a high satisfaction degree (CC^{-i}). From A1–A10, ten experiments are completed. Obtained results show that alternative-8 (F1–F8) still has a high satisfaction degree (CC^{-i}) in 10 experiments. Moreover, the alternative with least weight in each experiment is A2. The variations of results with each other show that the ratings of alternatives are sensitive to the weights.

Table 10: Sensitivity analysis

Experiments	Weights/ Alternatives	A1	A2	A3	A4	A5	A6	A7	A8	A9	A10
		Satisfaction degree (CC-i)									
Experiment-0	Original Weights	0.3312	0.2224	0.3525	0.4055	0.4147	0.4849	0.4256	0.4551	0.4161	0.3589
Experiment-1	F1	0.3523	0.2375	0.3671	0.4213	0.4206	0.4963	0.43179	0.471	0.4294	0.3697
Experiment-2	F2	0.33	0.2275	0.3541	0.4098	0.4111	0.4958	0.4268	0.4615	0.4289	0.3648
Experiment-3	F3	0.3336	0.222	0.3611	0.4038	0.4066	0.4943	0.4238	0.457	0.4274	0.3618
Experiment-4	F4	0.3426	0.0445	0.3485	0.3939	0.4158	0.4853	0.4271	0.4662	0.4184	0.3651
Experiment-5	F5	0.3038	0.1899	0.3153	0.3786	0.3742	0.4565	0.3921	0.4246	0.3896	0.3301
Experiment-6	F6	0.2565	0.1409	0.2705	0.3353	0.3278	0.4128	0.4048	0.3782	0.3459	0.3428
Experiment-7	F7	0.3483	0.2278	0.3603	0.4282	0.416	0.5015	0.4348	0.4664	0.4346	0.3728
Experiment-8	F8	0.3329	0.2395	0.3581	0.4138	0.4229	0.4864	0.4288	0.4733	0.4195	0.3668

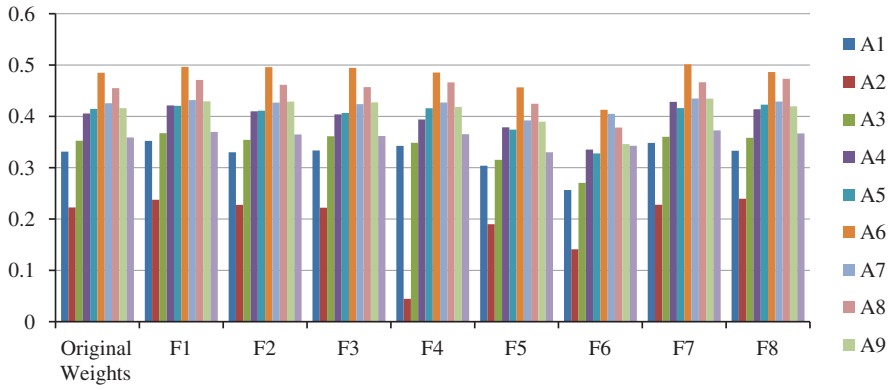

Figure 7: Graphical representation of sensitivity analysis

8 Discussion

In the context of security risk assessment, F-AHPTOPSIS technique is considered to be the most significant procedure for verifying web-based healthcare applications. The study undertook an empirical investigation of local hospitals of Varanasi in India to corroborate that the developer's framework is essential for protecting the WBHMS. The present security concerns have changed to maintainable and secure website composition and medical clinic's-the developer

framework. This examination centers on these two concerns and has made a various leveled structure which at last brings up the significant and contributing variables in the supportable security plan of the medical clinic the developer framework. With the web applications becoming a convincing need, their use and multifaceted nature are developing step by step. Moreover, the exponential development in security assessment forces the need to create a digital medical clinic the developer submits and empower it with high security and effective supportability.

Estimation and evaluation of security risk is the best way to accomplish feasible security. This exploration paper coordinates security just as maintainability factors and assesses reasonable security in a systematic manner. The consequences of the examination will assist the engineers in integrating supportable security with planning web application during its advancement. In this paper, we have taken tasks of the emergency clinic of different WBHMS and made feelings out of experts about the causative supportability, plan, and security variables of the particular WBHMS. Information examined from the experts has been incorporated by using Fuzzy AHP-TOPSIS.

A broad framework of research mentions the development and estimation of secure WBHMS. This paper mentions the security factors and their alternatives according to the case study of the different hospital which uses the different hospital management system application in Varanasi, India. Our research will help the engineers in developing the web application with proper improvement in the development life cycle of WBHMS. There are now numerous estimation models or strategies accessible in the writing for evaluating security independently however the accessibility of models or techniques that coordinate security on the Fuzzy-AHP strategy is altogether less. In this work, we have taken ten alternatives of the security risk of web-based applications. These alternatives were chosen after consulting the experts and collating their opinions about the contributing risk plan, mitigation plan, and security attributes of the particular web-based application.

Discoveries of this work can be enumerated as:

- The quantitative outcomes accomplished by F-AHPTOPSIS will bolster the specialists in classifying higher positioned components of an electronic emergency clinic in the board framework.
- F-AHP method gives the weight of risk attributes; F-TOPSIS gives the rank of the following attributes.
- Comparison of F-AHPTOPSIS with usual AHP TOPSIS gives the betterment of methodologies.
- Sensitivity analysis gives the degree of satisfaction for WBHMS.
- Web-based emergency clinic the board framework must be the foremost priority for both future investigations and present endeavors to optimize the efficacy of WBHMS. This evaluation would assist the engineers in gaining knowledge about the structure of security.

Improvement rules can be delivered over this assessment to help the engineers in refining the structure of security by utilizing high organized aspects in concern. This estimation may have a few delimits which can be defeated later in future studies. Delimits of the results are the following:

- The information gathered for website architecture is noteworthy, however, little. The results may contrast if the information is enormous.
- There may be extra security configuration factors other than those recognized in this work

9 Conclusion

This paper examined the security dangers that are threatening the web applications, more specifically, WBHMS. The study also analyzed a portion of the security countermeasures for these kinds of dangers. From writing, security dangers are viewed as the most significant countermeasures. As a solution to minimise the possibility of data breaches in WBHMS, this study undertook the estimation of risk assessment and employed the novel methodology of AHP TOPSIS for delivering new technique that suits the specific emergency clinic industry. This system gives distinctive security dangers credits to be decided by the AHP TOPSIS technique. Our research paper also gives the weights and the ranks of security factors. Hence, the validated and highly conclusive results drawn in the study will help the software or web application developers to consider the stated risks while developing the web-based application.

Acknowledgement: The work is funded by Grant No. 12-INF2970-10 from the National Science, Technology and Innovation Plan (MAARIFAH), the King Abdul-Aziz City for Science and Technology (KACST), Saudi Arabia. We thank the Science and Technology Unit at Um Al-Qura University for their continued logistics support.

Funding Statement: King Abdul-Aziz City for Science and Technology (KACST), Saudi Arabia.

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

References

[1] U. J. Butt, M. Abbod, A. Lors, H. Jahankhani, A. Jamalet *et al.,* "Ransomware threat and its impact on SCADA," in *IEEE 12th Int. Conf. on Global Security, Safety and Sustainability*, London, USA, pp. 205–212, 2019.

[2] P. Patel, F. G. Fall, R. Sullivan and R. Irwin, "Documenting attacks on health workers and facilities in armed conflicts," *Bulletin of the World Health Organization*, vol. 95, no. 1, pp. 79–81, 2017.

[3] S. T. Argaw, J. R. T. Pastoriza, D. Lacey, M. V. Florin, F. Calcavacchia *et al.,* "Cybersecurity of hospitals: Discussing the challenges and working towards mitigating the risks," *BMC Med Information and Decision Making*, vol. 20, no. 2, pp. 146, 2020.

[4] S. E. Jasper, "U.S. cyber threat intelligence sharing frameworks," *International Journal of Intelligence and Counter Intelligence*, vol. 30, no. 1, pp. 53–65, 2017.

[5] P. A. Williams and A. J. Woodward, "Cyber security vulnerabilities in medical devices: A complex environment and multifaceted problem," *Medical Devices (Auckland N.Z.)*, vol. 8, pp. 305–316, 2015.

[6] R. Susło, J. Trnka and J. Drobnik, "Current threats to medical data security in family doctors' practices," *Family Medicine & Primary Care Review*, vol. 3, no. 1, pp. 313–318, 2017.

[7] P. Zech, M. Felderer and R. Breu, "Towards risk driven security testing of service centric systems," in *12th Int. Conf. on Quality Software*, Xi'an, China, pp. 140–143, 2012.

[8] K. V. N. Sunitha and M. Sridevi, "Automated detection system for SQL injection attack," *International Journal of Computer Science and Security*, vol. 4, no. 4, pp. 426, 2009.

[9] S. Schauer, M. Stamer, C. Bosse, M. Pavlidis, H. Mouratidis *et al.,* "An adaptive supply chain cyber risk management methodology," in *Hamburg Int. Conf. of Logistics*, Hamburg, Germany, pp. 15–19, 2017.

[10] C. S. Kruse, B. Frederick, T. Jacobson and D. K. Monticone, "Cybersecurity in healthcare: A systematic review of modern threats and trends," *Technology and Health Care*, vol. 25, no. 1, pp. 1–10, 2017.

[11] D. Ionita, J. Bullee and R. J. Wieringa, "Argumentation-based security requirements elicitation: The next round," in *IEEE 1st Int. Workshop on Evolving Security and Privacy Requirements Engineering*, Karlskrona, pp. 7–12, 2014.
[12] P. Radanliev, D. C. D. Roure, R. Nicolescu, M. Huth, R. M. Montalvo *et al.,* "Future developments in cyber risk assessment for the internet of things," *Computers in Industry*, vol. 102, no. 1, pp. 14–22, 2018.
[13] O. Akinrolabu, S. New and A. Martin, "CSCCRA: A novel quantitative risk assessment model for SaaS cloud service providers," *Computers*, vol. 8, no. 66, pp. 15–23, 2019.
[14] A. Memari, A. Dargi, M. R. A. Jokar, R. Ahmad, A. Rahman *et al.,* "Sustainable supplier selection: A multi-criteria intuitionistic fuzzy TOPSIS method," *Journal of Manufacturing Systems*, vol. 50, no. 1, pp. 9–24, 2019.
[15] J. Dezert, D. Han and J. Tacnet, "Multi-criteria decision making with imprecise scores and BF-TOPSIS," in *20th Int. Conf. on Information Fusion (Fusion)*, Xi'an, China, pp. 1–8, 2017.
[16] M. R. Mokhtar, M. P. Abdullah, M. Y. Hassan and F. Hussin, "Combination of AHP-PROMETHEE and TOPSIS for selecting the best demand side management (DSM) options," in *IEEE Student Conf. on Research and Development*, Kuala Lumpur, pp. 367–372, 2015.
[17] Q. Zhang, X. Zhu, Q. Li and X. Han, "Empirical study on evaluating value creation strategy performance based on GRA and Fuzzy TOPSIS," in *Sixth Int. Conf. on Fuzzy Systems and Knowledge Discovery*, Tianjin, China, pp. 79–84, 2009.
[18] M. T. Dao, A. T. Nguyen, T. K. Nguyen, H. T. Pham, D. T. Nguyen *et al.,* "A hybrid approach using fuzzy AHP-TOPSIS assessing environmental conflicts in the titan mining industry along central coast Vietnam," *Appllied Sciences*, vol. 9, no. 14, pp. 1–24, 2019.
[19] R. Solanki, G. Gulati, A. Tiwari and Q. M. D. Lohani, "A correlation based Intuitionistic fuzzy TOPSIS method on supplier selection problem, *IEEE Int. Conf. on Fuzzy Systems*, Vancouver, BC, pp. 2106–2112, 2016.
[20] M. S. Jalali, S. Razak, W. Gordon, E. Perakslis and S. Madnick, "Health care and cybersecurity: Bibliometric analysis of the literature," *Journal of Medical Internet Research*, vol. 21, no. 2, pp. 52–57, 2019.
[21] A. M. Sharif and M. Z. A. Rozan, "Design and implementation of project time management risk assessment tool for SME projects using oracle application express," *World Academy of Science Engineering, and Technology*, vol. 65, no. 54, pp. 1221–1226, 2010.
[22] M. A. Sharif and S. Basri, "Software Risk Assessment: A review on small and medium software projects, Software Engineering and Computer Systems," in *ICSECS 2011, Communications in Computer and Information Science*. vol. 180. Berlin, Heidelberg: Springer, pp. 54–59, 2011.
[23] M. Habiba, M. R. Islam and A. B. M. S. Ali, "Access control management for Cloud," in *12th IEEE Int. Conf. on Trust, Security and Privacy in Computing and Communications*, Melbourne, VIC, pp. 485–492, 2013.
[24] G. Pujolle, A. Serhrouchni and I. Ayadi, "Secure session management with cookies," in *7th Int. Conf. on Information, Communications and Signal Processing (ICICS)*, Macau, pp. 1–6, 2009.
[25] I. Alsmadi and I. Alazzam, "Websites' input validation and input misuse based attacks," in *Cybersecurity and Cyberforensics Conf.*, Amman, pp. 113–116, 2016.
[26] S. K. Mahmoud, M. Alfonse, M. I. Roushdy and A. M. Salem, "A comparative analysis of cross site scripting (XSS) detecting and defensive techniques," in *8th Int. Conf. on Intelligent Computing and Information Systems (ICICIS)*, Cairo, pp. 36–42, 2017.
[27] G. B. de Pádua and W. Shang, "Revisiting exception handling practices with exception flow analysis," in *IEEE 17th Int. Working Conf. on Source Code Analysis and Manipulation*, Shanghai, pp. 11–20, 2017.
[28] R. Barona and E. A. M. Anita, "A survey on data breach challenges in cloud computing security: Issues and threats," in *Int. Conf. on Circuit, Power and Computing Technologies*, Kollam, pp. 1–8, 2017.
[29] A. Keikha and H. M. Nehi, "A complex method based on TOPSIS and choquet integral to solve multi attribute group decision making problems with interval type-2 fuzzy numbers," in *4th Iranian Joint Congress on Fuzzy and Intelligent Systems*, Zahedan, pp. 1–5, 2015.

[30] S. Chen, S. Cheng and T. Lan, "A new multicriteria decision making method based on the topsis method and similarity measures between intuitionistic fuzzy sets," in *Int. Conf. on Machine Learning and Cybernetics*, Jeju, South Korea, pp. 692–696, 2016.

[31] S. Zhou, W. Chang, S. Zhou and W. Liu, "The method of risk evaluation for equipment development based on triangular fuzzy number and TOPSIS," in *The 26th Chinese Control and Decision Conf.*, Changsha, China, pp. 2272–2276, 2014.

[32] F. Dammak, L. Baccour and A. M. Alimi, "The impact of criterion weights techniques in TOPSIS method of multi-criteria decision making in crisp and intuitionistic fuzzy domains," in *IEEE International Conf. on Fuzzy Systems*, Istanbul, pp. 1–8, 2015.

[33] L. W. Lee and S. M. Chen, "Fuzzy multiple attributes group decision-making based on the extension of TOPSIS method and interval type-2 fuzzy sets," in *Int. Conf. on Machine Learning and Cybernetics*, Kunming, 8, pp. 3260–3265, 2008.

[34] W. Hadikurniawati, E. Winarno, D. B. Santoso and Purwatiningtyas, "A mixed method using AHP-TOPSIS for dryland agriculture crops selection problem," in *3rd Int. Conf. on Informatics and Computational Sciences*, Semarang, Indonesia, pp. 1–5, 2019.

[35] M. Alenezi, M. Nadeem, A. Agrawal, R. Kumar and R. A. Khan, "Fuzzy multi criteria decision analysis method for assessing security design tactics for web applications," *International Journal of Intelligent Engineering and Systems*, vol. 13, no. 5, pp. 181–196, 2020.

[36] M. A. Zytoon, "A decision support model for prioritization of regulated safety inspections using integrated delphi, AHP and double hierarchical TOPSIS approach," *IEEE Access*, vol. 8, pp. 83444–83464, 2020.

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

[38] R. Kumar, M. Zaroor, 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.

[39] A. Agrawal, M. Alenezi, R. Kumar and R. A. Khan, "Measuring the sustainable-security of web applications through a fuzzy-based integrated approach of AHP and TOPSIS," *IEEE Access*, vol. 7, pp. 153936–153951, 2019.

[40] K. Sahu, Rajshree 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.

[41] 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.

[42] 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, pp. 50944–50957, 2020.

[43] 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.

[44] 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.

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

[46] K. Sahu and R. K. Srivastava, "Revisiting software reliability," in *Data Management, Analytics and Innovation (Advances in Intelligent Systems and Computing)*, vol. 802, pp. 221–235, Springer, 2019.

[47] R. Kumar, S. A. Khan and R. A. Khan, "Durable security in software development: Needs and importance," *CSI Communication*, vol. 39, no. 7, pp. 34–36, 2015.

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

[49] K. Sahu and Rajshree, "Helpful and defending actions in software risk management: A security viewpoint," *Integrated Journal of British*, vol. 4, pp. 1–7, 2015.

[50] R. Kumar, S. A. Khan and R. A. Khan, "Durability challenges in software engineering," *Crosstalk*, vol. 29, no. 5, pp. 29–31, 2016.

[51] 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.

[52] 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*, pp. 1–9, 2019.

[53] 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—An International Journal of Research and Surveys*, vol. 12, no. 6, pp. 615–620, 2018.

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

[55] M. Alenezi, R. Kumar, A. Agrawal and R. A. Khan, "Usable-security attribute evaluation using fuzzy analytic hierarchy process," *ICIC Express Letters—An International Journal of Research and Surveys*, vol. 13, no. 6, pp. 453–460, 2019.

[56] 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.

[57] A. Agrawal, M. Alenezi, R. Kumar and R. A. Khan, "A unified fuzzy-based symmetrical multi-criteria decision-making method for evaluating sustainable-security of web applications," *Symmetry*, vol. 12, no. 3, pp. 1–23, 2020.

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

[59] 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. 1, pp. 25543–25556, 2020.

[60] R. Kumar, S. A. Khan, A. Agrawal and R. A. Khan, "Security assessment through fuzzy Delphi analytic hierarchy process," *ICIC Express Letters—An International Journal of Research and Surveys*, vol. 12, no. 10, pp. 1053–1060, 2018.

[61] Q. Li, "An Improved fuzzy AHP approach to evaluating conductor joint alternatives," in *7th Int. Conf. on Fuzzy Systems and Knowledge Discovery*, Yantai, China, pp. 811–814, 2010.

[62] B. Öztaysi, S. Ç. Onar, E. Boltürk and C. Kahraman, "Hesitant fuzzy analytic hierarchy process," in *IEEE Int. Conf. on Fuzzy Systems (FUZZ-IEEE)*, Istanbul, pp. 1–7, 2015.

[63] A. Agrawal, A. Pandey, A. Baz, H. Alhakami, W. Alhakami *et al.,* "Evaluating the security impact of healthcare web applications through fuzzy based hybrid approach of multi criteria decision making analysis," *IEEE Access*, vol. 8, pp. 135770–135783, 2020.

[64] 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, pp. 48870–48885, 2020.

[65] A. Agrawal, M. Alenezi, R. Kumar and R. A. Khan, "Measuring the sustainable security of web applications through a fuzzy based integrated approach of AHP and TOPSIS," *IEEE Access*, vol. 7, pp. 153936–153951, 2019.