Received: May 3, 2020. Revised: June 15, 2020.

International Journal of
Intelligent Engineering & Systems

http://www.inass.org/

Fuzzy Multi Criteria Decision Analysis Method for Assessing Security Design Tactics for Web Applications

Mamdouh Alenezi[1]* Mohammad Nadeem[2] Alka Agrawal[2]
Rajeev Kumar[2]* Raees Ahmad Khan[2]

[1]*College of Computer & Information Sciences, Prince Sultan University, Kingdom of Saudi Arabia*
[2]*Department of Information Technology, BBA University, Lucknow, Uttar Pradesh, India*
* Corresponding author's Email: rs0414@gmail.com

Abstract: Security and design tactics estimation of web application for ensuring the security, efficiency and design tactics of web applications is necessary. A survey conducted by the security research team, Micro Focus, of the USA reveals that 80% of the vulnerability defects occur due to the coding defect, validation causes 60% of the errors, 70% errors are due to encapsulation and path traversal. Such statistics call for a more efficacious design to enhance software security. The primary research goal of this study is to compute or evaluate the security threats of the software and web applications from the perspective of design tactics. Towards this intent, we have employed the methodology of Fuzzy Analytic Hierarchy Process (F-AHP) to evaluate the security factors or obtain the weight of different factors. The different design tactics of web application have also been selected according to the factors that affect the security. In this article, researchers have used a crossbreed technique of fuzzy based Multi Criteria Decision Method (MCDM) technique, i.e., F-AHP and Fuzzy Technique for Order of Preferences by Similarity to Ideal Solutions (F-TOPSIS) Technique. The results of the assessment of security will be helpful for developers or experts in designing the security tactics of software or web applications. We have also compared the results of classical and Fuzzy approach to determine the weight of alternatives or attributes and rank of the factors. This process is an effective and conclusive methodology for the developers working for more enhanced secure design tactics of software and web application design.

Keywords: Web application security, Security assessment, Security tactics, Fuzzy logic, Fuzzy-AHP, Fuzzy-TOPSIS.

1. Introduction

Web applications are one of the most predominant stages for data and administration conveyance over the internet today [1]. The Web is the essential passage to on-line information and applications. As they are progressively utilized for basic administrations, web applications have become a mainstream and important objective for security assaults. Web Based Application Safety Records tabulate vulnerabilities detected in about 10,000 scan targets in 2019. According to this report, Cross-site Scripting (XSS) vulnerabilities, Susceptible JavaScript libraries, and Word Press related troubles claimed a giant 30% of the sampled aims [2]. SQL injections, which have been wreaking havoc for years all over the internet, are yet another security issue as detected in a random sample of 10,000 efficiently scanned ambitions [3].

Evidently, web utility securities are unsafe for many reasons. Security breaches are a threat to both individual users of the web applications as well as to the organizations whose reputation and business is at stake. Certain remedial actions through rules formulated by the general data protection regulation [4] that include monetary penalties are indeed a deterrent. However, 77% of the associations concede that they don't have a formal Digital Security Occurrence Reaction Plan (DSORP) that can be relied upon, as per IBM [4]. Security is a ceaseless journey and as the systems get updated for the ease of use, the security of the systems also needs to be affected. Designers of new protective components

have been extremely vigilant in ensuring that systems have mechanisms to ward off certain assaults. Nevertheless, several vulnerabilities and issues still subsist and more continue to arise.

The most widely recognized assaults against web application in design tactics perspective that we have considered in our research as factors are: the Access control [F1], Data Protection [F2], Continuous Process to Drive Security [F3], Vulnerability Assessment [F4], Secure Code Review [F5], and Security Audit [F6]. For the purpose of our study, we intend to focus on the factors from these recognized assaults. Furthermore, we will use the F-AHP and F-TOPSIS methodology to estimate the security in web application design.

We have taken twelve alternatives denoted as A1 to A12. These alternatives are the different design methods of software and web application design tactic. The security risks are the factors from F1 to F6. The objectives of the research are mentioned below:

- To analyse the design tactics attributes with security factors, i.e., aspects of strength and weakness of the web application.
- F-AHP methodology gives the design tactics or alternatives weight with the help of security factors in the web application development.
- Sensitivity analysis corroborates the efficiency of proposed methodology.
- The comparison between AHP-TOPSIS and F-AHP F-TOPSIS further emphasises the effectiveness of the latter technique over the others.
- After comparison, the proposed methodology ensures better design tactic with different security factors.

After the Introduction, this research paper has been structured in the subsequent subsets:

- Section 2- Discusses the related studies in the given domain of design tactics
- Section 3- Explains the different alternatives of web application design.
- Section 4- Elucidates the methodology of Fuzzy AHP TOPSIS.
- Section 5- Presents the empirical data of our methodology in tabular form.
- Section 6- Tabulates a comparison of the results with usable AHP TOPSIS approach versus the results obtained through the fuzzified approach of AHP TOPSIS.
- Section 7- Enlists the sensitivity analysis.
- Section 8- Profiles a detailed discussion on our proposed methodology.
- Section 9- Concludes the study.

2. Literature review

Security estimation of web or software design tactics is an essential part of IT developer's task. According to the Micro Focus, nearly 70% of the security attacks occurred in 2019 [3]. Security estimation, moreover, has been largely ignored by the researchers, as per the data provided by the Micro Focus. The estimation of security with the reference to design tactic is our prime concern of the research in web application. The majority of web application developers want to utilize simple and faltering structures of security plan. This approach is influencing the software or web application's upgradability. Several research studies have focused on different forms of attacks in design tactics perspective. Some of the relevant studies are:

Agrawal et al. [2019] have given the idea of methodology that we have used in our research F-AHP and F-TOPSIS. The study asserts that supportable security is a multidimensional, eminent, and a final idea. Likewise, structuring supportable security of web application has many design approaches which depends on the clients' needs and association's arrangements. In this unique circumstance, the basic leadership procedure could be a powerful way to quantitatively assess practical security estimation of web application plan. In this research study, the authors have adopted a process that includes coordinating F AHP and F-TOPSIS tactics for the consideration of supportable sanctuary of web applications [1].

S. Calzavara et al. [2017] tells us about the most widely recognized assaults against web application session, that is, assaults that target legit internet browser clients building up a verified session that is confided in web application. The study presents a survey of existing security arrangements that avoids or alleviates the various assaults by assessing them along four unique indices: assurance, ease of use, similarity, and simplicity of organization [5].

M. Jazayeri [2007] gives a different model of software design tactic and the study cites that the web application will driven by propel in program innovation, web foundation, convention models, programming designing strategies, and application patterns [6].

X. Li et al. [2014] study points out the three usually observed security vulnerabilities inside web application which are: input approval vulnerability, session executives' vulnerability, and application rationale vulnerability, alongside assaults or threats that adventure these vulnerabilities [2].

P. Lous et al. [2017] tell us about the alternatives/attributes for our research and contribute a gathering of encounters on the utilization of Scrum in the worldwide programming designing. For

example, the study recognized many difficulties and provided classifications that professionals face when utilizing Scrum in particular application. Among the difficulties, scaling Scrum to application and receiving rehearses appropriately are the most prevalent ones. Authors state that most arrangement proposition target changing components of the Scrum centre procedures. Furthermore, the authors cite that despite the fact that Scrum takes into account broad change, scrum itself speaks to a boundary for worldwide programming designing, and improvement groups need to redo Scrum appropriately to profit by deft programming advancement in application [7].

P. Maier et al. [2017] established secure programming advancement philosophies founded on straight models, for example, cascade and V-model, which make them inadequate for direct application in a lithe domain. This research [8] exhibits a proposition for incorporating security exercises into scrum process for creating secure Web application. The authors recognized several gaps in the existing approaches to deal with secure nimble improvement and breakdown in the built up of security designing exercises.

P. Yan & J. Guo [2010] give the idea of software development or web based application method which states that based on the hypothesis of client focused plan (CFP) and ease of use building standards, Web ease of use configuration incorporates three viewpoints: Client examine, Web structure, and Web assessment. Client research centers on target clients, and investigates client's objective, conduct and perspectives by client displaying dependent on personas. Website composition centers on data engineering structure, intelligibility configuration, search plan and page configuration to plan oneself portrayed Web UI with high-ease of use. Web assessment is an estimation that implies for iterative procedure of Web ease of use plan. The technique will be a rule to plan and improve Web ease of use for creators [9].

W. James et al. [2009] used the open source web application security instructing apparatus Web Goat for labs that train the understudies about the idea of explicit vulnerabilities like SQL infusion. These labs additionally acquaint understudies with open source web testing intermediaries. For example, Burp Suite which has been utilized all the more profoundly in later labs that give specific attention to entrance testing of a total web application. Understudies in security classes figure out how to utilize web powerlessness scanners and web application firewalls, while web programming classes centre on figuring out how to compose code without basic vulnerabilities [10].

The literature cited above tells us that the software design tactics are a difficult task and the security risks which are mentioned above are the dependent factors. Hence, it is essential for the developers to focus on the risks and be conversant with the relevant alternatives with individual weights and affecting ranks. After the ranking, the degree of closeness and sensitivity tells us about the factors that affect the design tactic of software development.

3. Materials and methods: Security factors and design tactics for web application design

Medical Securities of data are very important in every aspect of information technology and are also an integral feature of our current research area of design tactic of software and web application. To maintain the security in design is a complicated task. Due to this, our research study has opted to select six factors because the majority of security concerns arise due to these factors. The six design tactics factors are- Access control (F1), data protection (F2), Continuous Process to Drive Security (CPDS) (F3), vulnerability assessment (F4), security code review (F5), and security audits (F6). They are very important attributes for design tactics perspective in web based application or software design. We have estimated the security through different risks, i.e., cross site scripting, data breaching through the pop up, and vulnerability, etc. We have chosen the methodology F-AHP, and F-TOPSIS procedure to estimate the security. Security attributes/factors of web application design are as follows:

3.1 Access control (F1)

It is a security process that directs who can view or utilize assets in a processing domain. It is a fundamental concept in security. To secure a capability, establishments utilize electronic access control arrangements that have client details; access card readers, etc. A portion of these frameworks join access control boards to limit sections just as alerts and lock down capacities to avert unapproved access or tasks. This is a control framework that performs ID validation and approval of clients and elements by assessing required login accreditations. These sanctuary controls the exertion by distinguishing an organization or person, checking that the individual or application is who or what it professes to be, and approving the entrance level and set of activities

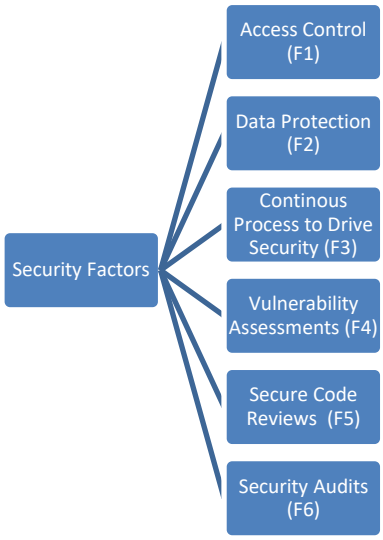

Figure. 1 Security Factors

related with the username or address. Directory service and protocol give access control to verifying and approving clients and entities and empowering them to associate with computer assets, for example, disseminated applications and web servers. Associations utilize diverse access control models relying upon their consistence prerequisites and the sanctuary levels of IT they are attempting to ensure. Two types of access control are there: somatic and coherent. Somatic access control limits access to precincts, buildings, rooms and physical IT assets [11]. Coherent access control limits acquaintances to computer network, system files and data [12].

3.2 Data protection (F2)

Many web applications do not appropriately ensure delicate information, for example, money related, human services, and so forth. Aggressors may take or change such feebly secured information to direct credit card misrepresentation, wholesale fraud, or different wrongdoings. Delicate information might be undermined without additional insurance, for example, encryption very still or in travel, requires exceptional safeguards when traded with the program. Information anonymous approaches, for example, k-namelessness, l-assorted variety, and t-closeness are utilized to protect security in distributed information [13].

3.3 Continuous process to drive security (F3)

Requires both the execution level and operational level foundations for effectively verifying web applications design tactics. When creating program based page, it is probably going to have issues in the web application. For instance, an application issue that resembles a minor bug, practically, could have antagonistic impact in the context of security [14]. Hence, the foundation of a powerful procedure for web application security is a fundamental rule.

3.4 Vulnerability assessment (F4)

A helplessness appraisal is the way towards characterizing, distinguishing, ordering and organizing vulnerabilities in computer frameworks, applications and system foundations. This process helps the association doing the evaluation with the vital learning, mindfulness and hazard foundation to comprehend the dangers to its condition and respond suitably. A vulnerability evaluation process that is planned to distinguish threats and the risk they present regularly includes the utilization of robotized testing instruments, for example, arrange security scanners, whose outcomes are recorded in a security appraisal report. Associations of any size or even people who face an expanded danger of cyber-attacks can profit by some type of helplessness evaluation. Yet, huge undertakings and different kinds of associations that are dependent upon continuous assaults will profit most from powerlessness examination. Since security vulnerabilities can empower programmers to get to IT frameworks and applications, it is basic for undertakings to distinguish and remediate shortcomings before they can be misused [15]. An exhaustive powerlessness evaluation alongside the board program can assist organizations with improving the security of their frameworks. System based sweeps are utilized to distinguish conceivable system security assaults. This sort of sweep can likewise recognize powerless frameworks on wired or remote systems. Host-based sweeps are utilized to find and recognize vulnerabilities in other systems, servers or workstations. Application sweeps can be utilized to test sites so as to recognize known programming vulnerabilities and mistaken designs in system or web applications. Database outputs can be utilized to recognize the powerless focuses in a database in order to counteract malevolent assaults, for example, SQL infusion assaults.

3.5 Secure code review (F5)

Having security code surveys, both when presenting new code just as a course evaluation, is basic. The most significant action is to build up safe practices archive that cites the best practices which every designer and activity specialist needs to pursue [13]. Besides having these just in content, it is essential to have discussions where individuals assess the past mix-ups and do a main driver evaluation for

each occurrence/botch in code so the group doesn't rehash the mistakes.

3.6 Security audits (F6)

While designing web based application, we may pursue diverse procedure models. Contingent upon the procedure model, each group may consent to pursue a lot of best practices to guarantee the safe advancement of the web application [16]. However, with time, there could be deviations from rehearses as required. Having a security review procedure mitigates the dangers of contrasts influencing in the long haul by distinguishing them as right on time as could be expected under the circumstances. These reviews could be completed with a security agenda to asses, either quarterly or every year relying upon the hierarchical prerequisites [9]. Commonly association with ISO27001 accreditations has an entrenched examining procedure as the standard norm for security.

Different design tactics are mentioned below in data analysis section as an alternative from A1 to A12 in detail. The different design tactics, A1 to A12, are used by the developers of web applications according to the requirements, applications, durability and flexibility of the application. The methodologies of F-AHP and F-TOPSIS give the degree of closeness, weight and rank of the design tactics.

4. Methodology: Integrated fuzzy AHP-TOPSIS

We have achieved the estimation of web application in design tactics perspective. In this tactic Fuzzy AHP and Fuzzy TOPSIS (FAFT), we estimate the factors of web application design, Basic decision issues that are consistently experienced for meeting the client's fulfillments and affectability of the data [17]. Many estimation procedures exist in the related work section that can be applied to understand such issues of MCDM [18]. For estimation of design security, FAFT is most suitable approach in spite of the other estimation approaches.

F-AHP can't resolve basic fuzziness and elusiveness of a decision creators' approachability of authentic measurements. Creators found that the experts have joined the Fuzzy idea with F-AHP on the grounds that the real world is unbelievably not defined for the in-depth research of the real world troubles [6]. Further, the F-AHP strategy is basically founded on very unpredictable size of decisions; moreover, the F-AHP also has few deficiencies [17] and [18]. Subsequently, a merged Fuzzy system

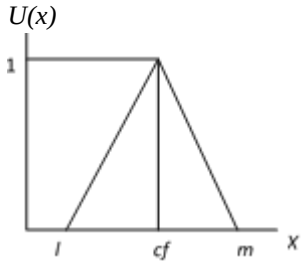

Figure 2: Triangular Fuzzy Number

FAFT is a novel strategy that could help in the proficient appraisals of option.

F-AHP is the methodology used to cure hard choice issues. F-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 F-AHP. The fuzzy stage is represented by Triangular Fuzzy Number (TFN), shown in figure 2. Here, they are classified as per the incident of occurrence in three different stages of - lower limit, centre farthest point and maximum breaking point [19]. These different stages build the structure of fuzzy logic. The logic gives the range of incidence occurrence at different levels. These are the capacities of TFN [20]. F-AHP gives the security factor's effectiveness in different design tactics. The different design tactics are arranged in the following F-TOPSIS methodology as mentioned below.

Further, the semantic qualities are named similarly significant, feebly significant and so on, and fresh esteems are sorted as 1,2,3,……..9. Furthermore, a fuzzy no. M on F is called TFN, if its participation capacity is recognized as condition (1, 2):

$$\mu_a(x) = a \rightarrow [0,1] \quad (1)$$

$$\mu_a(x) = \frac{x}{cf-l} - \frac{l}{cf-l} x \in [l, cf] \frac{x}{cf-mb} - \frac{mb}{cf-mb} x \in [cf, mb] \quad (2)$$

Here *l*, *cf*, and *mb* are denoted as the lower limit, center farthest point, and maximum breaking point, respectively. Figure 2 shows the triangle shape of fuzzy numbers in three different conditions. It may also vary for the different conditions or alternatives selected in our research as design tactics. Table 1 lists the ***Saaty*** scale for different fuzzy triangle scale.

The condition (3 to 6) is considered in varying the numeric qualities into TFN [17] 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. Further, TFN [ŋij] is perceived as:

Table 1. TFN scale

Saaty level description	Fuzzy Triangular level	
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)

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

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

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

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

Figure. 1 shows the six security factors F1, F2 …F6. And twelve alternatives A1, A2 ...A12 or methodology of web design tactic which are connected to every factor of security design tactic the alternative and factors are connected with each other. The equation 3 to 6; i, j and d can be selected by the developer or researcher and determine the variable $\left(\boldsymbol{J_{ijd}}\right)$to calculate the variable for further analysis. $\boldsymbol{\Phi_{ij}}$is the Geometric Mean (GM) of the particular correlation. The GM is to evaluate the minimum and maximum correlation of the factor in design tactics of web application. The equation or condition 7 to 9 gives different TFN values of the following variables. M1 and M2 are taken as two different TFNs.

M1= (l1, cf1, mb1) and M2= (l2, cf2, mb2).

The standards of activities on them are as:

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

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

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

After getting the TFN, M1 and M2; we evaluated the fuzzy span correlation. Fuzzy span correlation is the mathematical expression of $n \times n$ lattice which is expressed by the condition (10).

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

Here $\widetilde{k_{ij}^d}$ d is the privilege variable, i is the inclination criteria over the j criteria. In this condition there is more than one point of the normal inclination of the privilege assistance condition (11). It mentions the detail of the variable function of the F-AHP.

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

The ensuing stage of our research methodology maps out each variable of the fuzzy span correlation framework in which the middle value of the inclination is as per the condition (12).

$$\widetilde{A} = \lfloor \widetilde{k_{11}} \ \ldots \ \widetilde{k_{1n}} \cdots \ddots \cdots \widetilde{k_{n1}} \cdots \tilde{k}_{nn} \rfloor \tag{12}$$

Further, we have used the GM of condition (13), to determine the Fuzzy GM, fuzzy value of every factor.

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

Following stage is to finish up fuzzy load of the factor with the assistance of condition (14).

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

We determined the normal and standard weight criteria of the following condition (15-16). For this method we got the weight of the factors which affect the different design tactics.

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

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

The centre of area process is used to determine Best Non-fuzzy, Performance (BNP), which evaluates different factors according to the condition (17).

Table 2. Verbal scale

Verbal Variable	Equivalent TFN
Most Significant	(7, 9, 10)
Significant	(5, 7, 9)
Fair	(3, 5, 7)
Worst	(1, 3, 5)
Very Poor	(0, 1, 3)

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

F-TOPSIS: With P options as a geometrical course of action, m focuses inside the n-dimensional region of issue. TOPSIS points of view afford a multi gauges choice which can lead to major ambiguities. TOPSIS approach methodology utilized in this research is fundamentally based on the possibility that there is positive arrangement for the most limited and most distant ways whereas there is negative answer for the ideal and least perfect arrangements [21]. Researchers face problems in arranging the different values of the function in different conditions [22]. We have used the TOPSIS approach with F-TOPSIS to determine the appropriate criteria for getting the central values of the factors and alternatives. F-AHP and F-TOPSIS approach is very useful for obtaining accurate estimation in the perspective of design tactics. Fuzzy AHP and F-TOPSIS procedure, as employed in this endeavour, can be enunciated in the following steps: -

The primary step of methodology is to select the different design tactics and security factors as a criterion. The approach of FAFT in selection of design tactic is selected by the conditions (1-16). We chose the fuzzy choice of framework and got the semantic factor of the criteria with the help of matrix shown below in condition (18).

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

Where, $\tilde{x}_{ij} = \frac{1}{D}\left(\tilde{x}_{ij}^{1} \cdots \oplus \tilde{x}_{ij}^{d} \oplus \cdots \tilde{x}_{ij}^{D}\right)$, and $\tilde{x}_{ij}^{d}$ is the function of performance value of the alternative A_i (different design tactics) with respect to the following factor C_j evaluated by the factor d^{th} practitioner and $\tilde{x}_{ij}^{d} = (l_{ij}^{d}, mi_{ij}^{d}, u_{ij}^{d})$. Further we standardized our basic principle of methodology (fuzzy) in condition (19). The standard logic of fuzzy is mentioned in the matrix as:

$$\tilde{P} = \left[\tilde{p}_{ij}\right]_{m\times n} \quad (19)$$

The methodology of TOPSIS needs the realization of the function which can be mentioned by referring to equation (20).

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

For getting the best level mb_j^+ and j = 1, 2, .n is equivalent to 1; but it may be equivalent to 0. The normalized standard of TFN $\widetilde{p_{ij}}$ keeps the TFN in comparable way. The standard fuzzy lattice $(\widetilde{Q})$ of the weight is shown below in condition (21).

$$\tilde{Q} = \left[\tilde{q}_{ij}\right]_{m\times n} i = 1,2,..m;\ j = 1,2,3 \dots n \quad (21)$$

Where, $\tilde{q}_{ij} = \tilde{p}_{ij} \otimes \tilde{w}_{ij}$

The weight of the respective fuzzy logic is categorized in two different types: Fuzzy Positive Ideal Solution (FPIS) and Fuzzy Negative Ideal Solution (FNIS). The standardized weight of the FAFT is getting from the TFN which have a range of values from [0, 1]. Further, the researchers represent the FPIST$^+$ and FNIS R$^-$ in conditions (22-23).

$$T^+ = \left(\tilde{q}_{1,\cdots\dots}^{*}\tilde{q}_{j,\cdots\dots}^{*}\tilde{q}_{n,}^{*}\right) \quad (22)$$

$$R^- = \left(\tilde{q}_{1,\cdots\dots}^{*}\tilde{q}_{j,\cdots\dots}^{*}\tilde{q}_{n,}^{*}\right) \quad (23)$$

Where,
$\tilde{q}_1^* = (1,1,1)\otimes\tilde{w}_{ij} = \left(Lw_j, Mw_j, Hw_j\right)$ *and* $\tilde{q}_{ij}^- = (0,0,0)$, $j = 1,2,3 \dots n$.

The possible values of FPIS, FNIS differences between $(\tilde{d}_i^+, \tilde{d}_i^-)$ of every option from A^+ and A^-can be evaluated by utilizing the territory remuneration procedure, as mapped in the conditions (24-25).

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

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

Furthermore, the Closeness Coefficients $(C\tilde{C}_i)$ of following steps of the methodology can be estimated to ascertain that the proposed methodology is the most secure method of design tactic of web application. For this, the $\tilde{d}_i^+, \tilde{d}_i^-$ of all possible values can be estimated and determined by the condition (26).

$$C\tilde{C}_i = \frac{\tilde{k}_i^-}{\tilde{k}_i^+ + \tilde{k}_i^-} = 1 - \frac{\tilde{k}_i^+}{\tilde{k}_i^+ + k_i^-},$$

$$i = 1,2,\ldots,m \quad (26)$$

Where, $\frac{\tilde{k}_i^-}{\tilde{k}_i^+ + \tilde{k}_i^-}$ is defined as the fuzzy realization degree in the i^{th} option, and $\frac{\tilde{k}_i^+}{\tilde{k}_i^+ + \tilde{k}_i^-}$ is defined as fuzzy gap degree in the i^{th}elective. On the basis of their presence, we determined the degree of closeness of the data. The methodology of FAFT was used to calculate weight of the factor. After normalization with the different design tactic, we obtained the best way by the degree of closeness, to elicit the desired design tactic of web based application.

5. Data analysis and results

For the most part, subjective estimation is appropriate for evaluation of the security chance. It is typical to evaluate the design tactics in web application or software development quantitatively. Worldwide cumulative activity prompted the detailing of risk appraisal. More recently, the specialists have received risk evaluation and projects with enormous outcomes [22]. Likewise, associations are attempting to receive high security of web applications. Moreover, security variables effect assumes a critical job in web security advancement process [23]. In this subset of our study, we have contributed a path for web security structure estimation through F-AHP and F-TOPSIS. In addition, we have also discussed about the web security in the past segments. The following section details the different alternatives or design tactics of software and web based application, represented from ***A1 to A12.***

5.1 Waterfall model

[A1] in this methodology [24], the process of software or web application development is completed step-by-step. It is a linear model and according to the Waterfall, it cannot return to the previous step and this is the major drawback of the said model of software development.

5.2 Prototype methodology

[A2] this tactic of software design is different from the *waterfall* method by the solution of diversifying issues. In this method, the prototype of the required software is developed which is updated by the customers' feedback [25]. This method reduces the risk of functionality by clearly mentioning its function. The drawbacks are that due to upgradation and the feedback, the cost increases and the functionality becomes more complex.

5.3 Agile software development methodology

[A3] is a fast method to develop software or web based application. Agile means readiness for motion. This tactic maintains transparency [26]. This method has the major drawback of diversion in the results.

5.4 Rapid application development

[A4] this design tactic makes the entire developmental process effortless, assists the user, and encourages user's feedback for improvement. The drawback is that the whole developmental process needs a team [27]. Hence, only experts can solve the complexities.

5.5 Spiral model

[A5] this methodology of software or web application development is a highly sophisticated design and has low level of security risk. In this method, the developer starts the step of development and repeats the security evaluation as per spiral and reduces the risk [27]. This is a more reliable methodology of software development.

5.6 Scrum development

[A6] Scrum is the most widely used method of software development. It is a perfect approach because it enables the client to deliberately access the project. Scrum method gives direct control to the development team and paperwork is insignificant [28]. The drawbacks are not significant for the big project.

5.7 Rational unified development

[A7] it is an advanced form of software development, fastest among all, quick and responsive, but the drawback is that a large and skilled team of developers is needed and this can be expensive [28].

5.8 Dynamic System development model

[A8] this approach of software development is central responsive, feasible and has a large team [28]. Nowadays, this methodology is preferred for software development.

5.9 Extreme programming methodology

[A9] this approach is known as *XP methodology*, the software or web based applications are developed in an unbalanced environment [26]. This approach

Table-3 F-AHP aggregated pair-wise matrix

	Access Control [F1]	Data Protection [F2]	CPDS [F3]	Vulnerability Assessment [F4]	Secure Code Review [F5]	Security Audit [F6]
F1	1.0000,1.0000, 1.0000	1.0000,1.0000, 1.1900	0.8500,0.9000, 1.1900	0.6200,0.9000, 1.0000	0.8000, 1.0000, 1.0000	0.5500,0.7700, 1.0000
F2	0.8700,1.0000, 1.0000	1.0000,1.0000, 1.0000	0.8500,0.9000, 1.0000	0.5500,0.7700, 1.0000	0.6700, 1.0000, 1.0000	0.5100,0.7100, 0.8700
F3	0.8700,1.1500, 1.3100	1.0000,1.1500, 1.3100	1.0000,1.0000, 1.0000	0.7100,0.8700, 1.0000	0.7700, 1.0000, 1.1500	0.6400,0.7700, 0.8100
F4	1.0000,1.1500, 1.6500	1.0000,1.3500, 1.8500	1.0000,1.1900, 1.5400	1.0000,1.0000, 1.0000	1.0000, 1.0000, 1.3500	0.8700,1.0000, 1.0000
F5	1.0000,1.0000, 1.3100	1.0000,1.0000, 1.5000	0.9000,1.0000, 1.3500	0.7700,1.0000, 1.0000	1.0000,1.0000, 1.0000	0.7100,0.8700, 1.0000
F6	1.0000,1.3500, 1.8500	1.1900,1.5400, 2.0400	1.3800,1.5700, 1.9200	1.0000,1.0000, 1.1900	1.0000, 1.1900, 1.5400	1.0000,1.0000, 1.0000

Table 4. Weight of factors

Factors	Weight	BNP	Rank
F1	0.110,0.150,0.199	0.120	5
F2	0.102,0.145,0.183	0.090	6
F3	0.114,0.160,0.205	0.150	4
F4	0.134,0.180,0.261	0.220	2
F5	0.122,0.158,0.223	0.160	3
F6	0.150,0.206,0.297	0.260	1

enables great tractability in the design procedure. This approach reduces the cost of software essentials.

5.10 Feature driven development (FDD)

[A10] FDD approach of software development is user centric and agile development process in which the users' specifications are very important for software development iteration process. It deals with large projects with pre-planned steps, regular updates and is a costly method [28].

5.11 Joint application development

[A11] it is a client centric approach of software development. This approach brings the user, developer and manager face to face with the plan for software development. This approach tackles group requirements for the development [29].

5.12 Lean development methodology

[A12] this approach is very easy as compared to the other agile development approaches. It is less costly and even the time taken by this approach is one third in comparison to the other approaches. However, in spite of its merits, this method entails a security risk [30].

Figure. 1 shows the list of factors affecting the design of web application security at first level. The factors affect one or more property of the other significant level also, yet their effect isn't equivalent on them. It might vary. With the end goal of appraisal, we changed over the grouped properties into chains of importance as indicated in figure. 1. For the assurance of evaluation, ***variables of secrecy*** as for reasonable security at level 2 are spoken of as ***F1, F2… F6***. ***Properties of uprightness*** as for practical security at level 2 are spoken of as ***A1, A2, A3, A4, to A12***. As appeared in figure 1 and table 5, with the assistance of these chains of importance, we assessed the safe web application design. For gathering the information, with the assistance of conditions (1-26), secure web application through FAFT has been assessed as entailed below:

With the assistance of table 1, equation (1-9), the creators changed over the etymological qualities into numeric qualities and collected TFNs values. For developing span examination grid, TFNs qualities are registered as shown in Table 3. In Table 4 shows the matrix of aggregation according to equation 18. And the weight factors as per equation 17. Table 5 shows the cognition result of fuzzy. Table 7 shows normalize fuzzy decision matrix on equation 21. Table 8 evaluates the closeness coefficient of alternatives on equation 24, which we have mentioned as the rank of different levels.

Table 5 and table 6 enlist the different values of subjective cognition result mentioned in equation 20, normalized fuzzy decision matrix in equation 18, and weighted normalized decision matrix in equation 24, 25. These values are taken through the F-TOPSIS.

The table 7 depicts the degree of closeness as elicited through the fuzzy TOPSIS methodology, based on the Equation 26. Degree of closeness of different attributes of security factors of design tactics used in web application and software development and the different security factors are shown in figure. 1. The results of security factors (*F1* to *F6*) and their alternatives (*A1* to *A12*) in security estimation of web application and software

Table 5. Subjective cognition result

Factors/Alternative	F1	F2	F3	F4	F5	F6
Waterfall Model [A1]	4.3800, 6.3800, 8.3800	4.2400, 6.2400, 8.2400	5.0000, 7.0000, 8.6900	3.0000, 5.0000, 7.0000	5.7600, 7.7600, 9.3800	3.0000, 5.0000, 7.0000
Prototype Model [A2]	3.6200, 5.6200, 7.6200	3.7600, 5.7600, 7.7600	3.0000, 5.0000, 7.0000	3.0000, 5.0000, 7.0000	5.6200, 7.6200, 9.3100	4.2400, 6.2400, 8.2400
Agile Model [A3]	0.3100, 1.6200, 3.6200	0.0000, 1.0000, 3.0000	0.3800, 1.7600, 3.7600	3.0000, 5.0000, 7.0000	0.6200, 2.2400, 4.2400	0.6200, 2.2400, 4.2400
Rapid App. Model [A4]	3.7600, 5.7600, 7.7600	0.6900, 2.3800, 4.3800	0.0000, 0.3100, 1.6200	7.0000, 9.0000, 10.0000	7.0000, 9.0000, 10.0000	9.0000, 10.000, 10.0000
Spiral Model [A5]	0.6200, 2.2400, 4.2400	0.0000, 1.0000, 3.0000	0.0000, 0.0000, 1.0000	2.2400, 4.2400, 6.2400	3.0000, 5.0000, 7.0000	5.6200, 7.6200, 9.3100
Scrum Model [A6]	5.7600, 7.7600, 9.3800	6.3800, 8.3800, 9.6900	4.3800, 6.3800, 8.3800	7.0000, 9.0000, 10.0000	3.0000, 5.0000, 7.0000	3.0000, 5.0000, 7.0000
Rational Unified Development Model[A7]	7.7600, 9.3800, 10.0000	7.0000, 9.0000, 10.0000	7.0000, 9.0000, 10.0000	6.2400, 8.2400, 9.6200	5.0000, 7.0000, 9.0000	3.7600, 5.7600, 7.7600
Dynamic System Development Model [A8]	1.0000, 3.0000, 5.0000	3.0000, 5.0000, 7.0000	7.0000, 9.0000, 10.0000	5.6200, 7.6200, 9.3100	7.0000, 9.0000, 10.0000	1.6200, 3.6200, 5.6200
Extreme Development Model [A9]	3.0000, 5.0000, 7.0000	7.0000, 9.0000, 10.0000	7.0000, 9.0000, 10.0000	5.7600, 7.7600, 9.3800	3.0000, 5.0000, 7.0000	5.6200, 7.6200, 9.3100
Feature Driven Development [A10]	0.6200, 2.2400, 4.2400	5.6200, 7.6200, 9.3100	3.7600, 5.7600, 7.7600	4.3800, 6.3800, 8.3800	3.0000, 5.0000, 7.0000	5.0000, 7.0000, 9.0000
Joint Application Development [A11]	2.3800, 4.3800, 6.3800	5.6200, 7.6200, 9.3100	8.3800, 9.6900, 10.0000	3.0000, 5.0000, 7.0000	3.0000, 5.0000, 7.0000	4.3800, 6.3800, 8.3800
Lean Development Model [A12]	7.0000, 9.0000, 10.0000	5.6200, 7.6200, 9.3100	9.0000, 10.000, 10.000	3.0000, 5.0000, 7.0000	3.0000, 5.0000, 7.0000	3.0000, 5.0000, 7.0000

development are satisfactory. We have mentioned the degree of closeness in a bar chart as shown in figure 3.

6. Sensitivity analysis

To verify the results with each variable, we have used the sensitivity analysis [21]. This has been depicted below in table 8. The sensitivity analysis is calculated by the weight of variables. In our research based on security in design tactics of web application, the sensitivity analysis is verified by multiple experiments of each factor with the different experiments. The results have been shown in table 8. The *satisfaction degree* (CC^{-i}) is calculated by the weight of each factors (A1 to A12 taken as a constant), and by F-AHP and F-TOPSIS methodology, we calculated the $CC^{-I.}$

Table 8 depicts the sensitivity analysis and figure 4 is the bar graph representation of the sensitivity analysis. The first row of table 8 shows the original weight and fig. 4 shows the first bar graph of data. With the real weights, the security factor (F1 to F6) has the highest satisfaction degree. For different design tactic methods, denoted as alternatives A1 to A12, ten different experiments are done. The result of secure design tactic A3 is determined with the help of degree of closeness. The different ratings of A1 to A12 are sensitive to the weights.

Table 6. Weight normalized fuzzy decision matrix

Alternative/ Factors	F1	F2	F3	F4	F5	F6
A1	0.00400, 0.00600, 0.00700	0.00500, 0.00700, 0.00900	0.00400, 0.00600, 0.00800	0.00900, 0.01400, 0.02000	0.02600, 0.03400, 0.04200	0.02000, 0.03300, 0.04600
A2	0.00300, 0.00500, 0.00700	0.00400, 0.00600, 0.00800	0.00300, 0.00400, 0.00600	0.00900, 0.01400, 0.02000	0.02500, 0.03400, 0.04100	0.02800, 0.04100, 0.05400
A3	0.00000, 0.00100, 0.00300	0.00000, 0.00100, 0.00300	0.00000, 0.00200, 0.00300	0.00900, 0.01400, 0.02000	0.00300, 0.01000, 0.01900	0.00400, 0.01500, 0.02800
A4	0.00300, 0.00500, 0.00700	0.00100, 0.00300, 0.00500	0.00000, 0.00000, 0.00100	0.02000, 0.02600, 0.02900	0.03100, 0.04000, 0.04400	0.05900, 0.06600, 0.06600
A5	0.00100, 0.00200, 0.00400	0.00000, 0.00100, 0.00300	0.00000, 0.00000, 0.00100	0.00600, 0.01200, 0.01800	0.01300, 0.02200, 0.03100	0.03700, 0.05000, 0.06100
A6	0.00800, 0.01000, 0.01300	0.01100, 0.01400, 0.01600	0.01400, 0.02000, 0.02700	0.03600, 0.04700, 0.05200	0.01100, 0.01800, 0.02500	0.01200, 0.02000, 0.02800
A7	0.01000, 0.01300, 0.01300	0.01200, 0.01500, 0.01700	0.02200, 0.02900, 0.03200	0.03200, 0.04300, 0.05000	0.01800, 0.02500, 0.03200	0.01500, 0.02300, 0.03100
A8	0.00100, 0.00400, 0.00700	0.00500, 0.00800, 0.01200	0.02200, 0.02900, 0.03200	0.02900, 0.03900, 0.04800	0.02500, 0.03200, 0.03500	0.00700, 0.01500, 0.02300
A9	0.00400, 0.00700, 0.00900	0.01200, 0.01500, 0.01700	0.02200, 0.02900, 0.03200	0.03000, 0.04000, 0.04800	0.01100, 0.01800, 0.02500	0.02300, 0.03100, 0.03800
A10	0.00100, 0.00300, 0.00600	0.01000, 0.01300, 0.01600	0.01200, 0.01800, 0.02500	0.02300, 0.03300, 0.04300	0.01100, 0.01800, 0.02500	0.02000, 0.02800, 0.03600
A11	0.01700, 0.03100, 0.04500	0.03300, 0.04400, 0.05400	0.06200, 0.07100, 0.07400	0.01600, 0.02600, 0.03700	0.01200, 0.02100, 0.02900	0.01500, 0.02200, 0.02800
A12	0.04900, 0.06300, 0.07000	0.03300, 0.04400, 0.05400	0.06600, 0.07400, 0.07400	0.01600, 0.02600, 0.03700	0.01200, 0.02100, 0.02900	0.01000, 0.01700, 0.02400

Table 7. Closeness coefficients of aspired level among different alternative

	di	Di	Satisfaction degree	Ranks
A1	0.7400	29.1200	0.02312	6
A2	0.7100	29.2100	0.02421	2
A3	0.7200	29.3200	0.02211	11
A4	0.7300	29.4200	0.02431	1
A5	0.6600	29.0000	0.02214	10
A6	0.6700	29.1400	0.02301	8
A7	0.6500	29.2400	0.02410	5
A8	0.7210	29.3100	0.02240	9
A9	0.7320	29.4300	0.02403	4
A10	0.6540	29.1400	0.02200	12
A11	0.7010	29.0100	0.02302	7
A12	0.7150	29.0500	0.02411	3

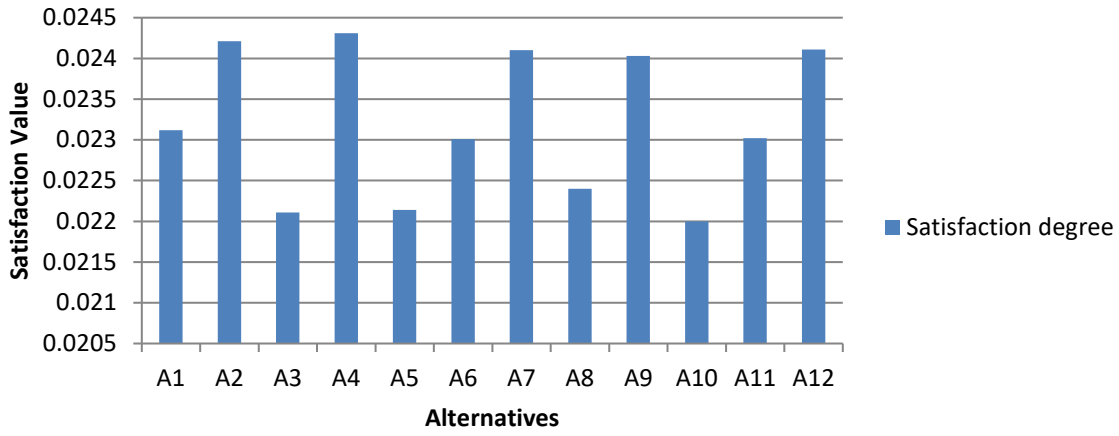

Figure. 3 Satisfaction degre

Table 8. Sensitivity analysis

Alternatives/ Experiments	Experiment -0	Experiment -1	Experiment -2	Experiment -3	Experiment -4	Experiment -5	Experiment -6
	Satisfaction Degree (CC-i)						
A1	0.02312	0.02418	0.02654	0.02568	0.02641	0.02996	0.02294
A2	0.02421	0.02479	0.02789	0.02490	0.03240	0.03279	0.02395
A3	0.02211	0.02269	0.02166	0.02536	0.02494	0.02448	0.01836
A4	0.02431	0.01899	0.02547	0.02931	0.02807	0.02664	0.02233
A5	0.02214	0.02426	0.01852	0.02226	0.02222	0.02220	0.01528
A6	0.02301	0.02069	0.02165	0.02525	0.02468	0.02413	0.01848
A7	0.02410	0.03680	0.01777	0.02183	0.02133	0.02057	0.01453
A8	0.02240	0.03110	0.02138	0.02720	0.02520	0.02470	0.01763
A9	0.02403	0.01747	0.02060	0.02400	0.02410	0.02418	0.01750
A10	0.02200	0.02900	0.02090	0.02497	0.02483	0.02473	0.01730
A11	0.02302	0.02298	0.02247	0.02623	0.02660	0.02693	0.01907
A12	0.02411	0.00959	0.02073	0.02423	0.02377	0.02327	0.01757

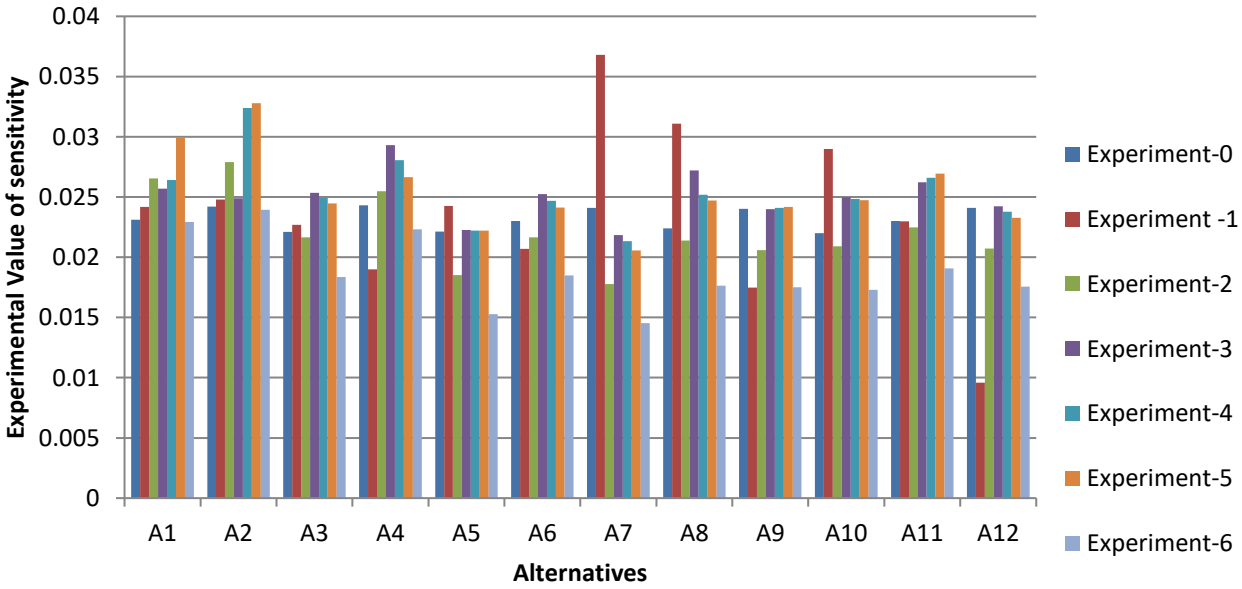

Figure. 4 Graphical Representation of Sensitivity Analysis

Table 9. Comparison table of classical AHP TOPSIS and FAFT approach

Methods/Alternative	FAFT	Classical-AHP-TOPSIS[31],[32]
A1	0.02312	0.02052
A2	0.02421	0.02251
A3	0.02211	0.02101
A4	0.02431	0.02251
A5	0.02214	0.01942
A6	0.02301	0.02161
A7	0.00241	0.02210
A8	0.02240	0.02060
A9	0.02403	0.02243
A10	0.02200	0.02230
A11	0.02302	0.02242
A12	0.02411	0.02141

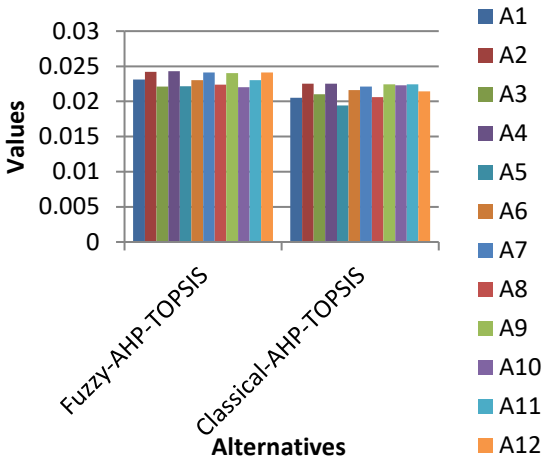

Figure. 5 Variation between results

7. Comparison of AHP-TOPSIS and FAFT

Same data, when used in two different methodologies of AHP-TOPSIS and FAFT gives different outputs. To estimate the accuracy of the results output collected by the given technique, we used more than one technique for our result because we wanted the exact estimation of our research work. The other technique is called the classical approach of AHP-TOPSIS. The main difference between FAFT and the classical AHP-TOPSIS is that of fuzzification. The classical approach and fuzzified approach of AHP-TOPSIS in numeric form are shown in table 9 and figure 5 shows its bar graph. Figure 4 shows the bar graph of degree satisfaction. The result obtained is highly correlated with 0.999176 by employing the FAFT methodology.

The reliability and efficiency of F-AHP, F-TOPSIS is improved and it is a better procedure/method than the usual AHP TOPSIS approach.

8. Discussion

F-AHP along with F-TOPSIS technique for security estimation on the basis of design tactics perspective is the most significant procedure for verifying security estimation of web application. As pointed out in the introductory section of this study, for the protected structure of web application in the design metric perspective, the Executives' Framework is the need of the time. As web applications have turned into a convincing need, their use and multifaceted nature are developed in stages. What's more, exponential development in security assaults forces the need to create web applications that empower the applications with high security. Evaluation and estimation are the best way to accomplish Security Estimation of Web Application the board framework.

This paper incorporates security factors and assesses these factors in a systematic framework. The consequences of the examination will assist the engineers in integrating the online secure administration framework along with structuring Security Estimation of Web Application with the reference of design tactics during its improvement. There are now numerous estimation models in design tactics perspective or strategies propositioned in several research resources for evaluating security independently. However, the accessibility of models or techniques which coordinate security on F-AHP strategy is altogether less. In this research paper, we reserved six alternatives of security risk of web based applications as per the opinions of the experts. These opinions necessarily centred on the contributing risk plan, mitigation plan and security attributes of the particular web based application.

Information has been taken from the *Micro Focus*, USA, for applying F-AHP and F-TOPSIS. Results of the work can be considered as the security estimation of web application system which will help the developers or experts to plan the security risk mitigation and other associated plans for major security issues, which provide secure web application design. The quantifiable outcomes accomplished by FAFT will bolster the specialists in classifying higher positioned components of security estimation of web application in design tactics perspective the board framework.

Security estimation of web application in design tactics perspective of the board framework is as yet overlooked. This evaluation would assist the engineers to gain knowledge about the structure of security.

Improvement rules can be delivered along with the assessment to help the engineers in refining the

structure of securities so as to suit the requirement of the systems. This estimation may have a few limits which can be addressed in ensuing research initiatives in future. Limitation, as reckoned by the researchers, is that the information gathered for website architecture is noteworthy, however, little. The results may contrast if the information is enormous. Moreover, there may be extra security configuration factors/attributes other than those recognized in this work.

9. Conclusion

This paper examined the different categories of threats to the security of web application, more specifically, in the context of design tactics perspective. Further, it checked on a portion of the security countermeasures for these kinds of threats. This paper propositions a novel methodology of employing F-AHP and F-TOPSIS to assess the security of a given web application. The effectivity of this technique was analyzed empirically and the results corroborate that this hybrid methodology would suit the specific security estimation in web design. This research gives the ranking of different design methodologies. The rapid application development method got the first priority in the analysis. To counter and contain the trajectory of threats emerging at present, the security experts can consider more alternatives for accurate assessment of security mechanisms from the perspective of design tactics.

Conflicts of Interest

The authors declare no conflict of interest.

Author Contributions

Conceptualization, Mamdouh Alenezi and Mohammad Nadeem; methodology, Mohammad Nadeem; software, Mohammad Nadeem; validation, Mohammad Nadeem, Alka Agrawal, Rajeev Kumar, and Raees Ahmad Khan; formal analysis, Alka Agrawal,Mohammad Nadeem, and Rajeev Kumar; investigation, Mamdouh Alenezi; resources, Mohammad Nadeem; data curation, Alka Agrawal; writing—original draft preparation, Mohammad Nadeem, and Rajeev Kumar; writing—review and editing, Mohammad Nadeem, Rajeev Kumar, and Alka Agrawal; visualization, Mohammad Nadeem; supervision, Raees Ahmad Khan; project administration, Alka Agrawal, and Raees Ahmad Khan; funding acquisition, Mamdouh Alenezi.

References

[1] 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.

[2] X. Li and Y. Xue, "A survey on server-side approaches to securing web applications" *ACM Computing Surveys (CSUR)*, vol. 46, no. 4, pp.1-29, 2014

[3] T. Demirel, N. Ç. Demirel, and C. Kahraman, "Fuzzy analytic hierarchy process and its application." In *Fuzzy multi-criteria decision making*, *Springer, Boston, MA*, Vol. 16, pp. 53-83, 2008.

[4] V. Roussev, "Hashing and data fingerprinting in digital forensics." *IEEE Security & Privacy*, Vol. 7, No. 2, pp.49-55, 2009.

[5] S. Calzavara, R. Focardi, M. Squarcina, and M. Tempesta. "Surviving the Web: A Journey into Web Session Security." *ACM Computing Survey 50*, Vol. 13, No. 1, pp. 1-34, 2017.

[6] M. Jazayeri, "Some Trends in Web Application Development." *Future of Software Engineering (FOSE '07). IEEE Computer Society*, USA, pp.199–213, 2007.

[7] P. Lous, M. Kuhrmann, and P. Tell, "Is Scrum Fit for Global Software Engineering?", In: *Proc. of IEEE 12th International Conference on Global Software Engineering (ICGSE)*, Buenos, Aires, pp. 1-10, 2017.

[8] P. Maier, Z. Ma, and R. Bloem, "Towards a Secure SCRUM Process for Agile Web Application Development", In: *Proc. of 12th International Conference on Availability, Reliability and Security (ARES) Association for Computing Machinery*, New York, NY, USA, pp.1–8, 2017.

[9] P. Yan and J. Guo, "The research of Web usability design," In: *Proc. of The 2nd International Conference on Computer and Automation Engineering (ICCAE)*, Singapore, pp. 480-483, 2010.

[10] J. Walden, M. Doyle, and G. Welch, M. Whelan, "Security of Open Source Web Applications", *3rd International Symposium on Empirical Software Engineering and Measurement IEEE*, pp. 545-553, 2009.

[11] J. A. De Guzman, K. Thilakarathna, and A. Seneviratne, "Security and Privacy Approaches in Mixed Reality: A Literature Survey", *ACM Comput. Surv.*, pp.1-36, 2019.

[12] T. Ishikawa and K. Sakurai, "Parameter manipulation attack prevention and detection by

using web application deception proxy", In: *Proc. of 11th International Conference on Ubiquitous Information Management and Communication (IMCOM '17). Association for Computing Machinery*, New York, NY, USA, pp.1–9, 2017.

[13] H. J. Schellnhuber and V. Wenzel, "Earth System Analysis: Integrating Science for Sustainability", *Springer*, 2012.

[14] C. Calero, G. R. D. Guzmán, M. A. Moraga, and F. García, "Is software sustainability considered in the CSR of software industry?" *Int. J. Sustain. Develop. World Ecol.*, Vol. 26, No. 5, pp. 439-459, 2019.

[15] R. Kumar, Z. Mohammad, A. Mamdouh, 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 pp.627–642, 2019.

[16] A. Ishizaka and P. Nemery, "Multi-Criteria Decision Analysis: Methods and Software", Hoboken, NJ, USA, *Wiley*, 2013.

[17] F. Khorramrouz, N. P. Kajabadi, and M. R. Galankashi, "Application of fuzzy analytic hierarchy process (FAHP) in failure investigation of knowledge-based business plans", *SN Appl. Sci*., Vol. 1, pp.1386, 2019.

[18] C. Balusa and A. K. Gorai, "Sensitivity analysis of fuzzy-analytic hierarchical process (FAHP) decision-making model in selection of underground metal mining method", *Journal of Sustainable Mining*, Vol.18, No.1, pp.8-17, 2019.

[19] M. Akram, W. Dudek, and F. Ilyas, "Group decision-making based on pythagorean fuzzy TOPSIS method", *International Journal Intelligence System* Vol.34, pp.1455-1475, 2019.

[20] K. Aliyeva "Facility location problem by using fuzzy topsis method", *Chemical Technology, Control and Management*, Vol.1, No.3, pp.55-59, 2018.

[21] H. Kanj and P. E. AbiChar, "A New Fuzzy-TOPSIS Based Risk Decision Making Framework for Dangerous Good Transportation", In: *Proc. of IEEE 21st International Conference on High Performance Computing and Communications; IEEE 17th International Conference on Smart City; IEEE 5th International Conference on Data Science and Systems (HPCC/SmartCity/DSS), Zhangjiajie*, China, pp. 2666-2672, 2019.

[22] K. Petersen, C. Wohlin, and D. Bacan, "The Waterfall Model in Large-Scale Development", In: *Proc. of International Conference on Product-Focused Software Process Improvement*, Springer, Berlin, Heidelberg, pp. 386-400, 2009.

[23] D. Y. Kim, "A Design Methodology Using Prototyping Based on the Digital-Physical Models in the Architectural Design Process", *Sustainability* Vol.11, No.16, pp.1-23, 2019.

[24] G. Kumar and P. Bhatia, "Impact of Agile Methodology on Software Development Process", *International Journal of Computer Technology and Electronics Engineering (IJCTEE)*, Vol.2, No.4, pp.46-50, 2012.

[25] W. Boehm, "A Spiral Model of Software Development and Enhancement", *Computer*, Vol. 21, No. 5, pp. 61-72, 1988.

[26] R. Dixit and B. Bhushan, "Scrum: An Agile Software Development Process and Metrics", *Journal on Today's Ideas Tomorrow's Technologies* Vol. 7, No. 1, pp. 73-87, 2019.

[27] P. B. Davies, C. Carne, H. Mackay, and D. Tudhope, "Rapid application development (RAD): An empirical review", *European Journal of Information Systems*. Vol. 8, No. 3, pp. 211-223, 1999.

[28] Z. Nawaz, S. Aftab, and F. Anwer, "Simplified FDD Process Model", *International Journal of Modern Education and Computer Science* Vol. 9, No. 9, pp. 53, 2017.

[29] E. Carmel, R. Whitaker, and J. George, "PD and Joint Application Design: A Transatlantic Comparison", *Communications of the ACM* Vol. 36, No. 6, pp. 40-48, 1993.

[30] O. Cawley, X. Wang, and I. Richardson, "Lean Software Development – What Exactly Are We Talking About?", In: *Proc. of International Conference on Lean Enterprise Software and Systems, Springer*, Berlin, Heidelberg, vol. 167, pp. 16-31, 2013.

[31] B. Oztaysi, "A decision model for information technology selection using AHP integrated TOPSIS-Grey: The case of content management systems", *Knowledge Based Systems*, Vol. *70*, pp. 44-54, 2014.

[32] A. Shaout and M. K. Yousif, "Performance evaluation–Methods and techniques survey", *International Journal of Computer and Information Technology*, Vol. 3, No. 5, pp. 966-979,2014.

Sr No.	Notation	Explanation
1.	$\mu_a\ (x)$	Fuzzy TFN
2.	l	Lower limit
3.	cf	Center farthest point
4.	mb	Maximum breaking point
5.	Φ_{ij}	TFN matrix
6.	M1 and M2	Two different TFN
7.	A^d	Fuzzy span correlation
8.	$\widetilde{k_{ij}^d}$	Privilege variable
9.	$\tilde{p}_i$	Fuzzy geometric mean
10	$\widetilde{w}_i$	Fuzzy weight
11	M_i	Normal weight criteria
12	Nr_i	Standard weight criteria
13	$\widetilde{K}$	Fuzzy matrix
14	T^+	Fuzzy positive ideal solution
15	R^-	Fuzzy negative ideal solution
16	$\tilde{p}_{ij}$	Realization function
17	$C\tilde{C}_i$	Degree of closeness
18	$\tilde{Q}$	Standard fuzzy lattice