IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received December 25, 2019, accepted January 29, 2020, date of publication January 31, 2020, date of current version February 10, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.2970784

Evaluating Performance of Web Application Security Through a Fuzzy Based Hybrid Multi-Criteria Decision-Making Approach: Design Tactics Perspective

MAMDOUH ALENEZI[1], ALKA AGRAWAL[2], RAJEEV KUMAR[2], AND RAEES AHMAD KHAN[2]

[1]College of Computer and Information Sciences, Prince Sultan University, Riyadh 11586, Saudi Arabia
[2]Department of Information Technology, BBA University, Lucknow 226025, India

Corresponding author: Rajeev Kumar (rs0414@gmail.com)

This work was supported by the College of Computer and Information Sciences, Prince Sultan University, Saudi Arabia.

ABSTRACT Design of software can have a major impact on the overall security of the software. Developing a secure website design is a challenge for architectures. It depends on different and tough decisions which determine the security of website. Increasing number of vulnerabilities increase the level of security requirements. Hence, security design tactics are to be adopted to satisfy these security requirements. Security design tactics are the mechanisms to define, detect and mitigate vulnerabilities and attacks. Therefore, faults in the application of security tactics or their weakening during website maintenance could be one of the key reasons behind the emergence of new and severe vulnerabilities that can be targeted by the hackers. There is a need for in-depth analysis of security tactics and its prioritization for the sake of determining the most prioritized factor. This will further help in gaining a more secure system. In this research study, the authors have used the hybrid method of Fuzzy AHP-TOPSIS (Analytic Hierarchy Process-Technique for Order Preference by Similarity Ideal Solution) for the evaluation of security design tactics and its attributes. The efficiency of this approach has been tested on a real time web application of Babasaheb Bhimrao Ambedkar University, Lucknow, India. Further, different web applications of the University have been used to validate the obtained results. This study's evaluation of the most impactful web application design for improving security will help the architects to secure systems by using security tactics.

INDEX TERMS Web application, security assessment, security design, security tactics, Fuzzy-AHP, Fuzzy-TOPSIS.

I. INTRODUCTION

Software was designed to satisfy the business goals of organizations. Software architecture is the association between its design and desired goal [1]. There is a constant pressure on the website developers to secure website that is using its design and architecture. For the achievement of this goal, website developers work thoroughly from ground to top of security of design [2]. However, these design solutions are often not enough to compensate the problems that arise due to security thrashing. Part 3 of the manual for critical safety, IEC-61508 states that security is obtained basically from developing safety strategy in website [3].

The associate editor coordinating the review of this manuscript and approving it for publication was Luca Ardito.

According to a report published by the *Computer World India,* British Airways was stuck by website failure due to which 100 flights were cancelled and 200 were delayed [4]. This kind of website failure forces the developers to think about what went wrong during the design of website which could have led to this grave setback. Security design tactics bring the solution for security related design issues.

According to a report by Lars Lofgren, approximately 54% of the companies universally say they have experienced at least one attack within the last year. The report also highlights that just 38% of businesses were prepared to handle these cyber-attacks [5]. Website defects that disturb the security requirements are called vulnerabilities. When a defect occurs in the system, the system becomes vulnerable to other defects. Architectural solutions such as security frameworks,

tactics are available for the developers to adopt and secure website [6]. This article's contribution includes investigation of factors or attributes that contribute to security design tactics. Furthermore, this research study also analyses the prioritization of these attributes to find out the most relevant attribute among a number of attributes. This prioritization will help the security designers to primarily focus on that specific attribute of security tactics of web application which would increase security to a specified level.

In addition, the field of multiple criteria decision analysis provides several methods and tools to prioritize different attributes of a concerned problem. Prioritization of different attributes is a multiple criteria decision making problem. Hence, the results of the prioritization process may facilitate the experts in taking suitable decisions as well as in initiating the required action. Essentially though, to make an appropriate decision for tactics, decision makers not only need to know the security design tactics attributes that contribute to overall security of website but also identify the most usable attributes among them. This article takes a Fuzzy AHP-TOPSIS evaluation model for prioritization of contributing factors of security design tactics and overall security assessment with respect to alternatives. This evaluation will help the security designers in maintaining and improving web application security through weights of specific factors at the early stage of development life cycle. A good design of web application would not only reduce both the time invested and costs incurred in maintenance but also enhance the life-span of web application services [3], [4].

The hybrid technique of Fuzzy-AHP and Fuzzy-TOPSIS approach has been found to be adequate and effective in several areas [7], [8]. During monitoring, controlling, arranging, and decomposing the decision problem, features of the hybrid technique of Fuzzy AHP-TOPSIS make it more conducive than the other applied methods for assessment [9]. The authors of the present study have evaluated the weights of the security tactics through Fuzzy-AHP technique and the impacts of the factors on different alternatives have been estimated through Fuzzy-TOPSIS method. In this study, eight alternatives of institutional website applications have been taken for evaluating the impacts due to sensitive information.

The rest of the paper is arranged as follows: Review of Literature is presented in the second part of the paper. The third section presents the security tactics with its hierarchy of contributing factors. The fourth and the fifth section define the methodology and its implementation. Comparison with other methods and sensitivity analysis are shown in sixth and seventh sections. Discussion and conclusion are presented in the eighth and ninth sections, respectively.

II. RELATED WORK

Organizations put great effort in providing secure services to its end users. The most challenging task in recent years has been to fight cybercrime with the help of secure website. The main problem in reducing cybercrime is the unavailability of a single framework which can integrate security and design tactics together by considering the factors of both [10]–[12]. Several research endeavours have been proposed in the context of security [2]–[6], [10]–[16]. Some of the relevant studies being:

Santos *et al.* [10] in 2019 presented an empirical study on tactical vulnerabilities by proposing Common Architectural Weakness Enumeration. In this study, the authors categorized the vulnerabilities in two segments which were the tactical and the non-tactical. 223 different tactical vulnerabilities were found in the study and it showed how architectural weaknesses have created severe vulnerabilities.

Osses *et al.* [11] in 2019 proposed a card based selection game for selecting security tactics. These practitioners also identified some important security architectural tactics based on the objectives. Further, experimental setup was created and results showed that TaSPeR supports sponsor's participation and collaboration for security tactics selection.

Marquez *et al.* [12] in 2018 provided a comprehensive survey and review on security tactics for software vulnerabilities. In this work, the authors prepared a set of research questions related to software vulnerabilities and security tactics and searched the most appropriate answers for those. This empirical study focused on tactical and non-tactical vulnerabilities in three real time software systems. Alashqar *et al.* [13] in 2017 proposed a framework for choosing the best architectural tactic. This framework proposed the developing of transaction processing systems. To achieve the required levels of quality attributes, the framework used Choquet Integral approach with fuzzy measures and analysed the impact of quality attributes on security tactics. Further, the framework also used quality attributes to compare different probable architectures.

Osses *et al.* [14] in 2016 reviewed the literature from tactics and cleared the ambiguities about the terminologies of security tactics. A modified tactic was also given in this paper for security design.

Ryoo *et al.* [15] in 2016 examined the gap between security tactics and actual implementation of security architecture. The authors tried to achieve the goal of an effective architect's intention to use security tactics, and checking whether the tactic is manifested during designing process of open source website projects.

Ryoo *et al.* [16] in 2010 proposed a novel approach for bringing tactics from already developed design patterns. This work focused specifically on the security patterns instead of using all design patterns.

From the review of literature of the past work, it is evident that numerous researches have been done for selecting the best tactics for software security, qualitatively [15], [16]. But, there is a need for a common framework of both the qualitative and the quantitative assessment of security by estimating the impacts of security tactics and tactics attributes. However, selecting and evaluating the impact of tactics is a decision making problem [17]. Hence in this paper, the authors proposition an approach for security assessment by using an effective fuzzy based hybrid approach of AHP-TOPSIS.

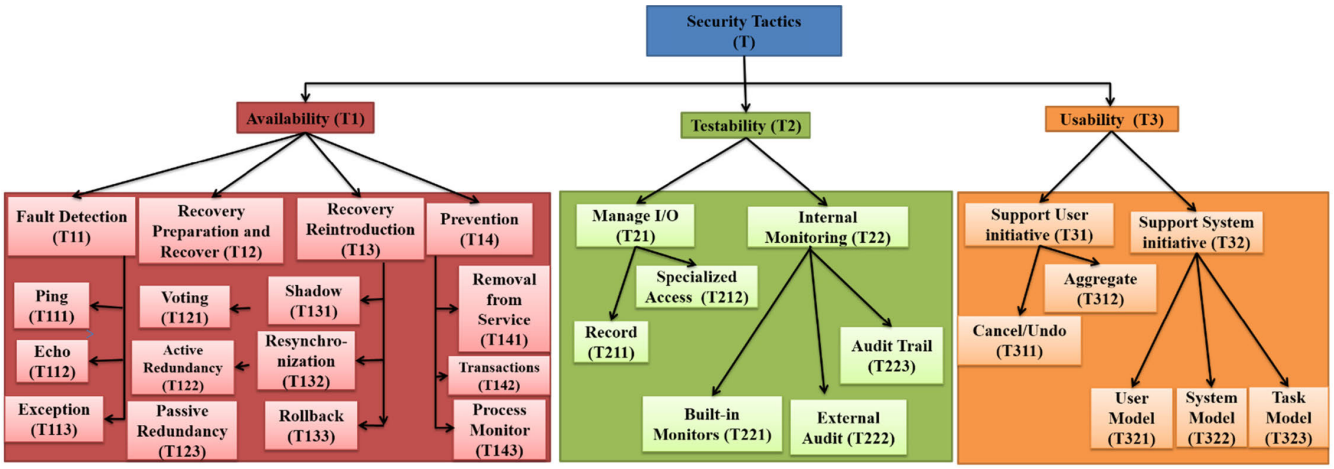

FIGURE 1. Hierarchical structure of security tactics.

III. SECURITY TACTICS

Significant efforts have been made to ensure security of the web applications, yet, even after continuous maintenance, systems remain insecure [5], [6]. Sometimes a slight and a simple change in the design may harm the web application [18]. The demand of secure website application led to the proposal of working on architectural tactics of security in design. Security tactics are a useful tool that can help to analyze and comprehend the facets of secure website design [7]. "*A security tactic is a design concept that addresses a security problem at the architectural design level*" [15], [16]. There are three main categories of security tactics. These are, the Availability based tactics, Testability based tactics and Usability based tactics [17]. Although tactics are fine grained, they are not atomic. They can be refined, so there is hierarchical structure of security tactics. After a thorough study of literature, the authors of this study have tried to build a hierarchy of security tactics which is given in figure 1.

In figure 1, security tactics are divided into three attributes of tactics which are the availability, testability and usability. This hierarchical structure and combination is taken from [10]–[13]. Availability plays an important role in building a secure system and maintaining security. Availability is the ability of the web application to deliver a service that is reliable with its requirement [2]. Testability means the ability of system to be tested for insecure attacks which is also important to maintain security [3]. Usability is the ability of the system to learn easily which ensures security from the user's end [4]. Further, availability, testability and usability are divided into their sub-attributes. The sub-attributes including fault detection, manage input/output, support user initiative, etc., have their sub-attributes in the next level of hierarchy. These attributes or tactics of availability, testability and usability are defined as follows:

- *Fault Detection (T11):* Availability tactics has four security tactics within it [3], [4]. Fault detection is one of them. Detection of failure influences the availability of data. It is influenced by three factors: Ping (T111), Echo (T112) and Exceptions (T113). Ping and echo are used to detect failure and occurrence of exceptions helps in identifying any failure.
- *Recovery Preparation and Recover (T12):* Fault recovery is one important concern while preparing availability security tactics [3]. Recovery preparation and recovering from a fault has further three factors which are Voting (T121), Active Redundancy (T122) and Passive Redundancy (T123)[3], [4]. Process of voting for a component helps in recovering from a fault. Active and passive redundancy passes the information of parallel faulty components to another component.
- *Recovery Reintroduction (T13):* Fault recovery with its reintroduction in security tactics is an important concern [4]–[10]. It has three factors within it which are Shadow (T131), Resynchronization (T132) and Rollback (T133). Shadow is when a removed fault has already been running in a shadow mode. Resynchronization is upgrading the state of component before it recovers. Rollback is after the fault recovery has been done and component is to be roll backed to the previous data.
- *Prevention (T14):* Fault prevention tactics include those tactics factors which are responsible for preventing fault from it including Removal from Service (T141), Transactions (T142) and Process Monitor (T143) [3]–[12]. Removal from Service tactic eliminates a module of the web application from procedure to undertake some activities to prevent the predicted failures. A transaction is the collection of several consecutive steps in such a manner that the entire collection can be undone at once. Process monitor can delete the nonperforming process and create a new instance of it once a fault in a process has been detected.
- *Manage I/O (T21):* This security tactics is used for managing input/output while system is in testing [4]–[13]. Manage I/O tactics includes two security tactics: Record (T211) and Specialized Access (T212). Record refers to the capturing of information and using it

as input for a testing while specialized access allows the capturing the variable values for a component through a test.

- *Internal Monitoring (T22):* Internal Monitoring is a state when a component can implement tactics based on internal state [5], [11]. It has three security tactics: Built-in Monitors (T221), External Audit (T222) and Audit Trail (T223). For doing the internal monitoring and implementing the security tactic, built-in monitors help in achieving this goal [3]. The external audit and audit trail analyse the logs of the work done in internal monitoring.
- *Support User Initiative (T31):* Supporting user initiative in maintaining is concerned with the usability which is consumermotivated [18], [19]. It contains security tactics including Cancel/Undo (T311) and Aggregate (T312).
- *Support System Initiative (T32):* This usability based security tactics is user friendly but supports the system rather than the user [20], [21]. Hence it includes tactics such as User Model (T321), System Model (T322) and Task Model (T323). Maintaining a model to support system initiative is necessary. Therefore, three models of user, system and task based tactics have been made in this.

For better understanding during the assessment process, the authors have named attributes and sub-attributes in hierarchy as T1, T2, and T3 for availability, testability and usability, respectively. Further, in the next level T11, T12, T13, T14 have been used for fault detection, recovery preparation and recover, recovery reintroduction and prevention, respectively. T21 and T22 have been used for manage input/output and internal monitoring, respectively. T31 and T32 have been used for support user initiative and support system initiative, respectively. Next level attributes have been named as T111, T112, T121, T211..... as their respective hierarchical representation.

Security tactics plays an important role in building a secure system. Further, its attributes and sub-attributes play an even more important role in building this security with their tactics [22]. For example, testability tactics is divided into two parts which is to manage input/output and internal monitoring. Building secure systems by using architectural tactics is supported by record, specialized access, build in monitors, external audit and audit trial tactics. Hence, these are also incorporated in hierarchical format of testability tactics.

This paper is focused on bringing out the single most important tactic which must be accorded the highest priority to secure the system by using security tactics. To fulfill the stated intent, this empirical study uses Fuzzy AHP. Further, Fuzzy TOPSIS method is used for evaluating the impact of these attributes. The potential of hybrid method of Fuzzy AHP-TOPSIS methodology proves to be good in measuring several qualitative attributes [9]. The next section explains the methodology of hybrid Fuzzy AHP-TOPSIS process.

IV. INTEGRATED FUZZY AHP-TOPSIS METHOD

The call for secure website development by using architecture tactics has led the architects to consider different criteria for different scenarios. Multiple attributes and sub-attributes that help in producing a secure website should have some prioritization process that would help the developers to decide the most promising tactic to be used for achieving optimum security [23], [24]. This problem contains different attributes which makes it a multi criteria decision making problem. Multiple theories have been developed for solving such kind of problems. These theories include the Fuzzy AHP, Fuzzy ANP, TOPSIS, ELECTRE, etc., [7]–[9]. Authors in the present research are using hybrid method of Fuzzy AHP-TOPSIS for this assessment.

Fuzzy-AHP is the methodology used to help with the tough choice problems because Fuzzy-AHP is objective in nature and looks for best alternative among the number of choices. The problem is divided into a hierarchical structure to solve it. The hierarchical structure for security tactics has been presented in figure 1. This hierarchy is prepared by using the experts' opinions for the concerned issue. Fuzzy membership function defines the problem into numerical values. Authors are using triangular fuzzy numbers as a membership function in this paper. The next step is to build the Triangular Fuzzy Numbers (TFN) from the hierarchal structure. With the help of effect of one attribute on various attributes, pair-wise comparison of each collection of ordered attributes is assumed to be a crucial job.

The next step now is to convert linguistic values into crisp numbers and TFN. There are various types of membership functions triangular fuzzy numbers, trapezoidal fuzzy numbers, sigmoidal, Gaussian and many more. According to this research design, the authors utilize the TFN and TFN lies somewhere in the range of 0 and 1 [25]. The reason for such selection of TFN is the computational straightforwardness of TFN enrollment capacities and their capacity to manage Fuzzy information. Triangular fuzzy numbers used in this paper range between 0 and 1 [26]. Additionally, the verbal values collected from different experts are denoted as: likely important, strongly important, etc., and crisp values are considered as 1,2,.....9. Furthermore, a fuzzy number called T on a is TFN, and its membership functions are known in equations. (1-2):

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

$$\mu_a(x) = \frac{x}{M-L} - \frac{L}{M-L} x \in [L, M] \times \frac{x}{M-U} - \frac{U}{M-U} x \in [M, U] \tag{2}$$

In the above equation L, M, and U are considered as lower limit, center farthest point, and maximum breaking point, respectively, in the triangular fuzzy number. Figure 2 portrays a TFN.

A TFN is stated here as (L, M, U). Experts elected scores to the attributes influencing the qualities in a quantitative manner as indicated by scale that is exhibited in table 1 [25].

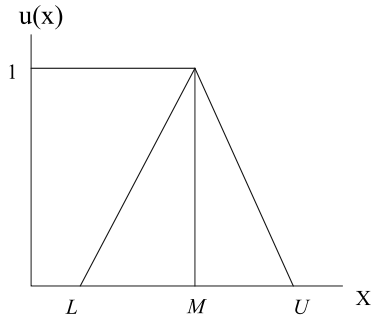

FIGURE 2. Triangular fuzzy numbers.

TABLE 1. TFN scale.

Saaty Scale Definition	Triangular Fuzzy Numbers	
1	Likely important	(1 ,1, 1)
3	Weakly important	(2 ,3, 4)
5	Fairly important	(4 ,5, 6)
7	Strongly important	(6 ,7, 8)
9	Firmly important	(9 ,9, 9)
2	Uneven principles between two adjacent measures	(1 ,2, 3)
4		(3 ,4, 5)
6		(5 ,6, 7)
8		(7 ,8, 9)

To change the linguistic values to numeric ones, equations (3-6) are used[25] that are assigned as (L_{ij}, M_{ij}, U_{ij}) where, L_{ij} is lower limit, M_{ij} is, center farthest point and U_{ij} is, and maximum breaking point values. Furthermore, TFN [η_{ij}] is said as:

$$\Phi_{ij} = (L_{ij}, M_{ij}, U_{ij}) \tag{3}$$

where $L_{ij} \leq M_{ij} \leq U_{ij}$

$$L_{ij} = min\left(J_{ijd}\right) \tag{4}$$

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

and

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

Equations (3-6), J_{ijd} show the relative importance of two attributes for each other where i and j represents the value given by practitioner or expert d. Φ_{ij} is evaluated using the geometric mean (GM) of expert's given value for a specific judgment. The geometric mean (GM) is used here because of its proficiency in correctly assessing the responses received from experts, which is also a comparative relation between two attributes.

Additionally, equations (7-9) are basic mathematical equations on two TFNs. Consider two TFNs N1 and N2, N1 = (L1, M1, U1) and N2 = (L2, M2, U2). The standards of activities on them are as:

$$(L_1,M_1,U_1)+(L_2,M_2,U_2) = (L_1+L_2, M_1+M_2, U_2+U_2) \tag{7}$$

TABLE 2. Linguistic scales for the rating

Linguistic Variable	Corresponding Triangular Fuzzy Number
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)

$$(L_1,M_1,U_1)\times(L_2,M_2,U_2) = (L_1\times L_2, M_1\times M_2, U_1\times U_2) \tag{8}$$

$$(L_1, M_1, U_1)^{-1} = \left(\frac{1}{U_1}, \frac{1}{M_1}, \frac{1}{L_1}\right) \tag{9}$$

Subsequent to getting the TFN esteems for each pair of examination, a Fuzzy pair-wise correlation matrix is developed as n x n lattice with the assistance of equation (10).

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

where $\tilde{k}^k_{ij}$ speaks to the d^{th} experts inclination of the i^{th} measure above the j^{th} measure. In the event that more than one alternative is available, at that point the normal of the inclinations of every expert is acquired with the assistance of equation (11).

$$\tilde{k}_{ij} = \sum\nolimits_{d=1}^{d} \tilde{k}^d_{ij} \tag{11}$$

Next stage is to refresh the pair-wise correlation matrix for all elements in the chain of importance based on the found the middle value of inclinations with the assistance of equation (12).

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

After this we utilize the GM method as appeared in equation (13) to depict the Fuzzy GM and Fuzzy weights of each factor.

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

Following step is to calculate the attribute's Fuzzy weight through the assistance of equation (14).

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

Further, to figure the normal and standardized weight criteria with the assistance of equations (15-16).

$$H_i = \frac{\tilde{w}_1 \oplus \tilde{w}_2 \ldots \oplus \tilde{w}_n}{n} \tag{15}$$

$$Nr_i = \frac{\mathrm{H}}{H_1 \oplus H_2 \oplus \ldots\ldots \oplus H_n} \tag{16}$$

Moreover, the Center of Area (COA) strategy is utilized to compute the BNP (Best Non-Fuzzy Performance) estimation

of the Fuzzy loads of each estimation with the assistance of condition (17).

$$BNPwD1 = \frac{[(U_{w1} - L_{w1}) + (M_{w1} - L_{w1})]}{3} + L_{w1} \quad (17)$$

Fuzzy TOPSIS: The fuzzy TOPSIS (Technique for Order Preference by Similarity to Ideal Situation) is used to pick one criteria when there are multiple criteria available with reference to only selected standards [26], [27]. In the TOPSIS two new approaches of FPIS and FNIS are proposed, which is to approach an alternate that is adjacent to the Fuzzy Positive Ideal Solution (FPIS) and utmost from the Fuzzy Negative Ideal Solution (FNIS) is chosen as optimum. An FPIS is the collection of the best piece of values for each alternative whereas the FNIS is the collection of the worst piece of values. Fuzzy AHP-TOPSIS procedure is as per the following:

The weights that have resulted from AHP are used in further steps. This work applies Fuzzy AHP to find out the Fuzzy weights with the support of equations (1-16) above. Additionally, by using the equation 18 and table 2 the experts create the Fuzzy matrix and give preferences for the perfect attributes as alternatives for the measures.

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

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 performance rating of the alternative A_i with respect to factor C_j estimated by the d^{th} practitioner and $\tilde{x}_{ij}^d = (L_{ij}^d, M_{ij}^d, U_{ij}^d)$.

Following stage is to standardize the Fuzzy choice matrix through the help of equation (19). The standardized Fuzzy choice matrix spoke to by $\tilde{P}$ is portrayed as follows.

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

Afterwards, the stabilization procedure can be assessed through the assistance of equation (20).

$$\tilde{p}_{ij} = \left(\frac{L_{ij}}{U_j^+}, \frac{M_{ij}}{U_j^+}, \frac{U_{ij}}{U_j^+}\right), U_j^+ = max\left\{U_{ij}, i = 1, 2, 3..n\right\} \quad (20)$$

On the other hand, we can set the best desired level U_j^+ and $j = 1, 2...n$ is equivalent to 1; generally, the most remarkably is 0. The consistent $\tilde{p}_{ij}$ keeps on being TFNs. For triangular fuzzy numbers, the normalization procedure can be performed in the similar way. The weighted Fuzzy standardized choice lattice $(\tilde{Q})$ is measured with the assistance of equations (14).

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

where, $\tilde{q}_{ij} = \tilde{p}_{ij} \otimes \tilde{w}_{ij}$ 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 $\tilde{q}_{ij}$ are constantly positive

TABLE 3. Fuzzy pair-wise comparison matrix for level 1.

	T1	T2	T3
Availability (T1)	1.0000, 1.0000, 1.0000	0.3900, 0.4300, 0.4700	0.3400, 0.4000, 0.4800
Testability (T2)	1.1100, 2.3500, 2.5900	1.0000, 1.0000, 1.0000	0.8000, 0.9700, 1.2000
Usability (T3)	2.1000, 2.5100, 2.9000	0.8400, 1.0300, 1.2500	1.0000, 1.0000, 1.0000

TFN and their extents have a place with the closed interval [0, 1]. From there on, we can depict the FPIS A^+ (goal levels) and FNIS A^- (the most exceedingly appalling levels) as appeared in equations (22-23).

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

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

where, $\tilde{q}_1^* = (1, 1, 1) \otimes \tilde{w}_{ij} = \left(Lw_j, Mw_j, Hw_j\right)$ *and* $\tilde{q}_{ij}^- = (0, 0, 0)$, $j = 1, 2, 3 \ldots n$. Determining the parting of every alternative is done from FPIS and FNIS. The parting ($\tilde{k}_i^+$ and $\tilde{k}_i^-$) of every option from A^+ and A^- can be assessed utilizing the area compensation procedure as appeared in equations (24-25).

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

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

Closeness coefficients are determined in the next step, and build up the choices to accomplish the aspired levels in each attribute. Chou *et al.* [26] recommended that this closeness coefficient $C\tilde{C}_i$ is cleared to assess the Fuzzy satisfaction degree based on the Fuzzy closeness coefficients to improve the decision on alternatives [27]. This development can be aligned with the similarities of a perfect arrangement that appeared in equation (26).

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

where, $\frac{\tilde{k}_i^-}{\tilde{k}_i^+ + \tilde{k}_i^-}$ defined as Fuzzy satisfaction degree in the i^{th} option and $\frac{\tilde{k}_i^+}{\tilde{k}_i^+ + \tilde{k}_i^-}$ characterized as fuzzy gap–degree in the i^{th} elective, based on which positions the options are achieved. The next process is to evaluate the security design tactics with the assistance of its contributing characteristics.

V. IMPLEMENTATION AND RESULTS

Mostly, qualitative assessment is appropriate for prioritizing security design tactics. It is hard to assess the security tactics quantitatively. Various criteria of security tactics and design tactics have been combined together to prioritize security design tactics in this work. Recently, researchers and developers have followed security tactics and other programs with

TABLE 4. Global weights through the hierarchy.

The first level	The weight of first level	The second level	The local weight of the second level	The third level	The local weight of the third level	The global weight of the third level	Best Non-fuzzy Performance Value (BNP)	Ranks
T1	0.14100, 0.17000, 0.21000	T11	0.14400, 0.20700, 0.29900	T111	0.11500, 0.16900, 0.24500	0.00200, 0.00600, 0.01500	0.00800	21
				T112	0.17000, 0.24900, 0.36100	0.00300, 0.00900, 0.02300	0.01200	19
				T113	0.22400, 0.32500, 0.47500	0.00500, 0.01200, 0.03000	0.01500	16
		T12	0.18700, 0.28000, 0.41800	T121	0.16600, 0.21800, 0.29000	0.00400, 0.01000, 0.02500	0.01300	18
				T122	0.26600, 0.34900, 0.46100	0.00700, 0.01700, 0.04000	0.02100	15
				T123	0.32000, 0.43300, 0.57900	0.00800, 0.02100, 0.05100	0.02700	10
		T13	0.15400, 0.22300, 0.32500	T131	0.36900, 0.52200, 0.71700	0.00800, 0.02000, 0.04900	0.02600	11
				T132	0.16600, 0.22400, 0.31000	0.00400, 0.00900, 0.02100	0.01100	20
				T133	0.18600, 0.25400, 0.36000	0.00400, 0.01000, 0.02400	0.01300	17
		T14	0.19002, 0.29000, 0.43300	T141	0.06600, 0.08800, 0.12100	0.00200, 0.00400, 0.01100	0.00600	22
				T142	0.22500, 0.31500, 0.46800	0.00600, 0.01006, 0.04200	0.02100	14
				T143	0.41000, 0.59700, 0.83800	0.01100, 0.03000, 0.07600	0.04900	7
T2	0.33100, 0.40500, 0.50100	T21	0.62200, 0.74800, 0.88800	T211	0.34200, 0.45700, 0.60400	0.07000, 0.13800, 0.26900	0.15900	3
				T212	0.41000, 0.54300, 0.72500	0.08400, 0.16500, 0.32200	0.19100	1
		T22	0.21500, 0.25200, 0.30700	T221	0.29500, 0.38009, 0.51100	0.02100, 0.04000, 0.07900	0.04600	9
				T222	0.32300, 0.43200, 0.57800	0.02300, 0.04400, 0.08900	0.05400	6
				T223	0.13400, 0.17900, 0.24100	0.01000, 0.01800, 0.03700	0.02200	13
T3	0.33500, 0.42400, 0.52900	T31	0.50200, 0.64700, 0.81600	T311	0.43900, 0.56700, 0.72100	0.07400, 0.15500, 0.31100	0.18000	2
				T312	0.34300, 0.43300, 0.55800	0.05800, 0.11900, 0.24100	0.13900	4
		T32	0.28200, 0.35300, 0.45900	T321	0.43700, 0.60400, 0.81600	0.04100, 0.09000, 0.19800	0.11000	5
				T322	0.19000, 0.25300, 0.34600	0.01800, 0.03008, 0.08400	0.04700	8
				T323	0.10900, 0.14300, 0.19500	0.01000, 0.02100, 0.04700	0.02600	12

impressive effects and efficacious performance [12]–[14]. Still architects are looking for specific security tactics for applying security in web applications. In addition, security tactics attributes impact performs a noteworthy role in security at the early stage of web application development process [17], [18]. In this paper, the authors suggest that the most apt methodology for prioritizing security design tactics is the hybrid method of Fuzzy AHP-TOPSIS. Authors have designed and discussed the security design tactics in the previous figure 1. For gathering the facts, this paper has taken suggestions of 70 specialists who are from academia and different organizations. With the help of equations (1-26), security design tactics prioritization via Fuzzy AHP-TOPSIS has been done as follows:

With the assistance of table 1 and equations number (1-9), authors have transformed the language based values into numeric values and its TFNs values. These values are used to construct AHP's pair-wise comparison matrix, further TFNs values are computed as:

$$\begin{aligned}\tilde{k}_{12}^{110} &= (1.0000, 1.0000, 1.0000)\otimes(0.1667, 0.2000, 0.2500)\\ &\quad\otimes\cdots\otimes(5.0000, 6.0000, 7.0000^{)1/110}\\ &= ((1.0000\times 0.1667\times\cdots\times 5.0000)^{1/110},\\ &\quad\times(1.0000\times 0.2000\times\cdots\times 6.0000)^{1/110},\\ &\quad\times(1.0000\times 0.2500\cdots\times 7.0000)^{1/110})\\ &= (0.3900, 0.4300, 0.4700)\end{aligned}$$

In the same way, the pair-wise comparison matrixes of the level 1 attributes is constructed with the help of equation (10) and shown in table 3.

Using the equations (11-13), the fuzzy weights of factors are calculated, the computational processes are shown as the succeeding components:

$$\begin{aligned}\tilde{p}_1 &= [(1.0000, 1.0000, 1.0000)\otimes(0.3900, 0.4300, 0.4700)\\ &\quad\otimes(0.3400, 0.4000, 0.4800)]1/3\\ &= [(1.0000\times 0.3900\times 0.3400)^{1/3},\\ &\quad\times(1.0000\times 0.4300\times 0.4000)^{1/3},\\ &\quad\times(1.0000\times 0.4700\,X0.4800)^{1/3}]\\ &= (0.5100, 0.5500, 0.6100)\end{aligned}$$

Equivalently, we can obtain the remaining $\tilde{p}_i$ as: $\tilde{p}_2 = (1.1900, 1.3100, 1.4600)$; $\tilde{p}_3 = (1.2100, 1.3700, 1.5400)$

With the help of equations (14-16) we can calculate the weight of each element as follows:

$$\begin{aligned}\tilde{w}_1 &= (0.5100, 0.5500, 0.6100)\\ &\quad\otimes((0.5100,0.5500, 0.6100)\oplus(1.1900, 1.3100, 1.4600)\\ &\quad\oplus(1.2100,1.3700,1.5400)\oplus(1.2300,1.4000,1.6000))^{-1}\\ &= (0.1400, 0.1700, 0.2100)\end{aligned}$$

We also calculate the remaining weights $\tilde{w}_i$ as follows: $\tilde{w}_2 = (0.3300, 0.4100, 0.5000)$; $\tilde{w}_3 = (0.3400, 0.4200, 0.5300)$. After that, Best Non-fuzzy Performance Value (BNP) of each attribute is calculated using the equation (17) as follows:

$$BNPw1 = \frac{[(0.5000-0.3300)+(0.4100-0.3300)]}{3} + 0.3300 = 0.4133$$

Equivalently, table 4 presents computed local weights for hierarchies of level 2 and level 3. After that, the final and

global weights for the contributing factors may be computed as presented in table 4.

Table 4 shows the ranks achieved in the form of global weights from the local weights of design tactics attributes. According to the achieved results, the highest rank attribute is specialized access in testability tactics. For evaluating the impact of these ranks of the attributes, the authors have collected linguistic values from the experts for eight different alternative web applications which have been developed for BBA University. With the help of table 2 and equation (18), the authors collected and converted the linguistic values into numeric values. With the help of table 2 and equations (3-9), the numeric values were converted into TFN values. Then the TFN values were aggregated as shown in table 5. With the help of equations (19-20), normalized fuzzy-decision matrix has been constructed as shown in table 6.

Table 7 shows the weighted normalized fuzzy-decision matrix that is obtained with the help of table 4 and equation (21). Finally, with the help of equations (22-26), Fuzzy Negative Ideal Solution, Fuzzy Positive Ideal Solution, gap degree and satisfaction degree of the alternatives are obtained and shown in table 8.

The satisfaction degree is the decisive criteria for choosing the best alternative from the set of available alternatives [27]. Based on the results from the table 8, it has been inferred that alternative 7 (A7) is the best alternative among all. The worst alternative amongst all is alternative 6 (A6). This study finds that using Fuzzy AHP-TOPSIS is well suited for assessing and selecting the best security tactics for assuring a quality web application.

VI. COMPARISON BETWEEN AHP-TOPSIS METHODS

Different techniques provide different results on the same data [25]. Generally, researchers use one or more techniques to check the accuracy of the results through proposed technique [26]. In this research work, authors used classical AHP-TOPSIS technique to evaluate the accuracy of the results [27]. In classical AHP-TOPSIS, the process of data collection and assessment of that data is same as in Fuzzy AHP-TOPSIS but only difference is that there is no fuzzification required. Hence, the data is taken in its numeric form for classical AHP-TOPSIS. The differences between results of fuzzy and classical AHP-TOPSIS are shown in table 9 and figure 3. Outcomes through classical AHP-TOPSIS method have high correlation between the outcomes of fuzzy AHP-TOPSIS method. Two different methods are used in this work and one of them is the improved method of second method (Fuzzy AHP TOPSIS) because of its accuracy.

VII. SENSITIVITY ANALYSIS

Sensitivity analysis is used to check the validity of estimated results with different variations [25], [26]. In this work, last level of the hierarchy has twenty two factors and henceforth sensitivities are tested through twenty two experiments. The high weights of factor were varied and other factor weights

TABLE 5. Subjective cognition results of evaluators in linguistic terms.

	A_1	A_2	A_3	A_4	A_5	A_6	A_7	A_8
	5.3600,	4.8200,	3.9100,	4.2700,	2.4500,	2.9100,	1.4500,	1.1800,
T111	7.3600,	6.8200,	5.9100,	6.2700,	4.4500,	4.6400,	3.0000,	2.8200,
	9.0000	8.6400	7.8002	8.2700	6.4500	6.5500	4.9100	4.8200
	4.2700,	4.6400,	4.6400,	4.2700,	2.8200,	3.1800,	1.4500,	0.8200,
T112	6.2700,	6.6400,	6.6400,	6.2700,	4.8200,	5.1800,	3.0000,	2.2700,
	8.0900	8.4500	8.3600	8.0000	6.8200	7.0900	4.9100	4.2700
	6.2700,	2.6400,	3.1800,	5.3600,	3.7300,	2.4500,	0.9100,	2.4500,
T113	8.2700,	4.6400,	5.1800,	7.3600,	5.7300,	4.4500,	2.4500,	4.2700,
	9.6400	6.6400	7.0900	9.0000	7.5500	6.4500	4.4500	6.2700
	4.8200,	3.0900,	3.1800,	4.6400,	3.0000,	2.1800,	2.8200,	1.9100,
T121	6.8200,	5.0000,	5.1800,	6.6400,	5.0000,	4.0900,	4.6400,	3.7300,
	8.6400	6.9100	7.0900	8.5500	7.0000	6.0000	6.6400	5.7300
	3.7300,	3.9100,	4.2700,	3.0000,	2.4500,	3.5500,	1.8200,	1.6400,
T122	5.7300,	5.9100,	6.2700,	5.0000,	4.4500,	5.5500,	3.7300,	3.5500,
	7.6400	7.7300	8.1800	7.0000	6.4500	7.4500	5.7300	5.5500
	4.4500,	3.5500,	5.0000,	5.3600,	2.6400,	2.9000,	2.8200,	2.5500,
T123	6.4500,	5.5500,	7.0000,	7.3600,	4.6400,	4.8000,	4.6400,	4.4500,
	8.2700	7.4500	8.7300	9.0900	6.6400	6.7000	6.6400	6.4500
	4.8200,	4.8200,	4.2700,	4.8200,	2.4500,	2.3600,	1.3600,	1.3600,
T131	6.8200,	6.8200,	6.2700,	6.8200,	4.4500,	4.2700,	3.1800,	3.3600,
	8.5500	8.7300	8.0900	8.5500	6.4500	6.2700	5.1800	5.3600
	5.1800,	4.8200,	4.6000,	4.4500,	2.4500,	2.5500,	1.2000,	1.3600,
T132	7.1800,	6.8200,	6.6000,	6.4500,	4.4500,	4.4500,	3.0000,	3.3600,
	8.8200	8.6400	8.4000	8.1800	6.4500	6.4500	5.0000	5.3600
	5.1800,	4.8200,	4.6400,	4.4500,	2.3600,	2.5500,	1.0900,	0.8200,
T133	7.1800,	6.8200,	6.6400,	6.4500,	4.2700,	4.4500,	2.8200,	2.6400,
	8.9100	8.5500	8.5500	8.2700	6.1800	6.4500	4.8200	4.6400
	5.7300,	5.5500,	5.7300,	5.7300,	3.1800,	3.5500,	1.8200,	1.6400,
T141	7.7300,	7.5005,	7.7300,	7.7300,	5.1800,	5.5500,	3.7300,	3.5500,
	9.3600	9.2700	9.2700	9.2700	7.1800	7.2700	5.7300	5.5500
	5.7300,	4.2700,	4.0900,	5.1800,	2.8200,	2.0900,	1.7300,	1.1800,
T142	7.7300,	6.2700,	6.0900,	7.1800,	4.8200,	4.0900,	3.5500,	3.0000,
	9.2700	8.1800	8.0900	8.8200	6.8200	6.0900	5.5500	5.0000
	5.1800,	4.2700,	3.7300,	4.4500,	3.5500,	3.0900,	2.9100,	2.8200,
T143	7.1800,	6.2700,	5.5500,	6.4500,	5.5500,	5.0000,	4.8200,	4.8200,
	9.0000	8.0900	7.2700	8.1800	7.3600	6.8200	6.7300	6.7300
	4.4500,	5.5500,	4.0900,	4.0900,	2.2700,	4.0009,	2.0000,	1.4500,
T211	6.4500,	7.5500,	6.0900,	6.0900,	4.2700,	6.0900,	3.9100,	3.3600,
	8.3600	9.1800	8.0000	8.0900	6.2700	7.9100	5.9100	5.3600
	4.8200,	5.0000,	3.9100,	3.7300,	2.4500,	3.3600,	1.9100,	1.6400,
T212	6.8200,	7.0000,	5.9100,	5.7300,	4.4500,	5.3600,	3.7300,	3.5500,
	8.6400	8.7300	7.9100	7.6400	6.4005	7.1800	5.7300	5.5500
	4.4500,	4.4500,	4.8200,	3.1800,	2.3600,	2.2700,	1.7300,	1.4500,
T221	6.4500,	6.4500,	6.8200,	5.1800,	4.2700,	4.0900,	3.5500,	3.3600,
	8.3600	8.3600	8.5500	7.0900	6.2700	6.0000	5.5500	5.3006
	5.1800,	4.6400,	4.0900,	4.0900,	2.3600,	2.4500,	1.9100,	1.6400,
T222	7.1800,	6.6400,	6.0900,	6.0900,	4.2700,	4.2700,	3.7300,	3.5500,
	8.8200	8.3600	7.9100	7.9100	6.2700	6.2700	5.7300	5.5500
	6.2700,	5.7300,	5.3600,	6.2700,	3.9100,	3.1800,	1.6400,	1.1800,
T223	8.2700,	7.7300,	7.3600,	8.2700,	5.9100,	5.1800,	3.3600,	3.0000,
	9.4500	9.0000	8.7300	9.4500	7.5500	7.0000	5.3600	5.0000
	5.0000,	5.7300,	4.2700,	4.1800,	2.8200,	3.5500,	0.8200,	0.7300,
T311	7.0000,	7.7300,	6.2700,	6.0900,	4.8200,	5.5500,	2.4500,	2.4500,
	8.4500	9.0000	7.9100	7.6400	6.6400	7.2700	4.4500	4.4500
	5.1800,	5.3600,	5.3600,	5.0000,	2.8200,	4.8200,	1.0000,	0.6400,
T312	7.1800,	7.3600,	7.3600,	7.0000,	4.8200,	6.8200,	2.6400,	2.2700,
	8.6400	8.7300	8.7300	8.4500	6.7300	8.2700	4.6400	4.2700
	5.7300,	5.3600,	5.5500,	5.3600,	2.0900,	4.0900,	0.7300,	0.3600,
T321	7.7300,	7.3006,	7.5500,	7.3600,	3.9100,	6.0900,	2.2700,	1.7300,
	9.0900	8.7300	8.9100	8.7300	5.8200	7.7300	4.2700	3.7300
	4.4500,	6.0900,	5.5500,	4.0000,	2.0900,	3.5500,	1.0000,	0.5500,
T322	6.4500,	8.0900,	7.5500,	5.9100,	3.9100,	5.5500,	2.6400,	2.0900,
	8.0000	9.2700	8.9100	7.4500	5.8200	7.2700	4.6400	4.0900
	4.7300,	6.0900,	5.5500,	3.9100,	2.2700,	3.0000,	0.7300,	0.5500,
T323	6.6400,	8.0900,	7.5500,	5.9100,	4.0900,	5.0000,	2.2700,	2.0900,
	8.0900	9.2700	8.9100	7.5500	5.9100	6.8200	4.2700	4.0900

were constant and satisfaction degree of CC^{-i} is calculated through Fuzzy-TOPSIS technique. Table 10 shows the tested results.

In table 10 and figure 4, first row shows the original results of this work. According to original results, alternative-7 (A7) has high satisfaction degree of CC^{-i}. From T111 to T323, twenty two experiments are tested. Results show that alternative-7 (A7) still has high satisfaction degree $(CC)^{-i}$ in 12 experiments including experiment-1, 5, 7, 8, 11, 12, 14, 15, 16, 17, 18 and 21. Alternative-1 (A1) has high satisfaction degree $(CC)^{-i}$ in 6 experiments including experiment-2, 3, 6, 9, 10, 20. Alternative-2 (A2) has high satisfaction

TABLE 6. The normalized fuzzy-decision matrix.

	A_1	A_2	A_3	A_4	A_5	A_6	A_7	A_8
T111	0.5600, 0.7600, 0.9300	0.5200, 0.7400, 0.9300	0.4200, 0.6400, 0.8400	0.4500, 0.6600, 0.8800	0.3300, 0.5900, 0.8600	0.3500, 0.5600, 0.7900	0.2200, 0.4500, 0.7300	0.1800, 0.4200, 0.7200
T112	0.4400, 0.6500, 0.8400	0.5000, 0.7200, 0.9100	0.5000, 0.7200, 0.9000	0.4500, 0.6600, 0.8500	0.3700, 0.6400, 0.9000	0.3800, 0.6300, 0.8600	0.2200, 0.4500, 0.7300	0.1200, 0.3400, 0.6400
T113	0.6500, 0.8600, 1.0000	0.2800, 0.5000, 0.7200	0.3400, 0.5600, 0.7600	0.5700, 0.7800, 0.9500	0.4900, 0.7600, 1.0000	0.3000, 0.5400, 0.7800	0.1400, 0.3600, 0.6600	0.3600, 0.6400, 0.9300
T121	0.5000, 0.7100, 0.9000	0.3300, 0.5400, 0.7500	0.3400, 0.5600, 0.7600	0.4900, 0.7000, 0.9000	0.4000, 0.6600, 0.9300	0.2600, 0.4900, 0.7300	0.4200, 0.6900, 0.9900	0.2800, 0.5500, 0.8500
T122	0.3900, 0.5900, 0.7900	0.4200, 0.6400, 0.8300	0.4600, 0.6800, 0.8800	0.3200, 0.5300, 0.7400	0.3300, 0.5900, 0.8600	0.4300, 0.6700, 0.9000	0.2700, 0.5500, 0.8005	0.2400, 0.5300, 0.8200
T123	0.4600, 0.6700, 0.8600	0.3800, 0.6000, 0.8000	0.5400, 0.7500, 0.9400	0.5700, 0.7800, 0.9600	0.3500, 0.6100, 0.8800	0.3500, 0.5800, 0.8100	0.4200, 0.6900, 0.9900	0.3800, 0.6600, 0.9600
T131	0.5000, 0.7100, 0.8900	0.5200, 0.7400, 0.9400	0.4600, 0.6800, 0.8700	0.5100, 0.7200, 0.9000	0.3300, 0.5900, 0.8600	0.2900, 0.5200, 0.7600	0.2000, 0.4700, 0.7700	0.2000, 0.5000, 0.8000
T132	0.5400, 0.7500, 0.9200	0.5200, 0.7400, 0.9300	0.5000, 0.7100, 0.9100	0.4700, 0.6800, 0.8700	0.3300, 0.5900, 0.8600	0.3100, 0.5400, 0.7800	0.1800, 0.4500, 0.7400	0.2000, 0.5000, 0.8000
T133	0.5400, 0.7500, 0.9200	0.5200, 0.7400, 0.9200	0.5000, 0.7200, 0.9200	0.4700, 0.6800, 0.8800	0.3100, 0.5700, 0.8200	0.3100, 0.5400, 0.7800	0.1600, 0.4200, 0.7200	0.1200, 0.3900, 0.6900
T141	0.5900, 0.8000, 0.9700	0.6000, 0.8100, 1.0000	0.6200, 0.8300, 1.0000	0.6100, 0.8200, 0.9800	0.4200, 0.6900, 0.9500	0.4300, 0.6700, 0.8800	0.2700, 0.5500, 0.8500	0.2400, 0.5300, 0.8200
T142	0.5900, 0.8000, 0.9600	0.4600, 0.6800, 0.8800	0.4400, 0.6600, 0.8700	0.5500, 0.7600, 0.9300	0.3700, 0.6400, 0.9000	0.2500, 0.4900, 0.7400	0.2600, 0.5300, 0.8200	0.1800, 0.4500, 0.7400
T143	0.5400, 0.7500, 0.9300	0.4600, 0.6800, 0.8700	0.4000, 0.6000, 0.7800	0.4700, 0.6800, 0.8700	0.4700, 0.7300, 0.9800	0.3700, 0.6000, 0.8200	0.4300, 0.7200, 1.0000	0.4200, 0.7200, 1.0000
T211	0.4600, 0.6700, 0.8700	0.6000, 0.8100, 0.9900	0.4400, 0.6600, 0.8600	0.4300, 0.6400, 0.8600	0.3000, 0.5700, 0.8300	0.4900, 0.7400, 0.9600	0.3000, 0.5800, 0.8800	0.2200 0.5000, 0.8000
T212	0.5000, 0.7100, 0.9000	0.5400, 0.7500, 0.9400	0.4200, 0.6400, 0.8500	0.3900, 0.6100, 0.8100	0.3300, 0.5900, 0.8600	0.4100, 0.6500, 0.8700	0.2800, 0.5500, 0.8500	0.2400, 0.5300, 0.8200
T221	0.4600, 0.6700, 0.8700	0.4800, 0.7000, 0.9000	0.5200, 0.7400, 0.9200	0.3400, 0.5500, 0.7500	0.3100, 0.5700, 0.8300	0.2700, 0.4900, 0.7300	0.2600, 0.5300, 0.8200	0.2200, 0.5000, 0.8000
T222	0.5400, 0.7500, 0.9200	0.5000, 0.7200, 0.9000	0.4400, 0.6600, 0.8500	0.4300, 0.6400, 0.8400	0.3100, 0.5700, 0.8300	0.3000, 0.5200, 0.7600	0.2800, 0.5500, 0.8500	0.2400, 0.5300, 0.8200
T223	0.6500, 0.8600, 0.9800	0.6200, 0.8300, 0.9700	0.5800, 0.7900, 0.9400	0.6600, 0.8800, 1.0000	0.5200, 0.7800, 1.0000	0.3800, 0.6300, 0.8500	0.2400, 0.5000, 0.8000	0.1800, 0.4500, 0.7400
T311	0.5200, 0.7300, 0.8800	0.6200, 0.8300, 0.9700	0.4600, 0.6800, 0.8500	0.4400, 0.6400, 0.8100	0.3700, 0.6400, 0.8800	0.4300, 0.6700, 0.8800	0.1200, 0.3600, 0.6600	0.1100, 0.3600, 0.6600
T312	0.5400, 0.7500, 0.9000	0.5800, 0.7900, 0.9400	0.5800, 0.7900, 0.9400	0.5300, 0.7400, 0.8900	0.3700, 0.6400, 0.8900	0.5800, 0.8200, 1.0000	0.1500, 0.3900, 0.6900	0.0900, 0.3400, 0.6400
T321	0.5900, 0.8000, 0.9400	0.5800, 0.7900, 0.9400	0.6000, 0.8100, 0.9600	0.5700, 0.7800, 0.9200	0.2800, 0.5200, 0.7700	0.4900, 0.7400, 0.9300	0.1100, 0.3400, 0.6400	0.0500, 0.2600, 0.5500
T322	0.4600, 0.6700, 0.8300	0.6600, 0.8700, 1.0000	0.6000, 0.8100, 0.9600	0.4200, 0.6300, 0.7900	0.2800, 0.5200, 0.7700	0.4300, 0.6700, 0.8800	0.1500 ,0.3900, 0.6900	0.0800, 0.3100, 0.6100
T323	0.4900, 0.6900, 0.8400	0.6600, 0.8700, 1.0000	0.6000, 0.8100, 0.9600	0.4100, 0.6300, 0.8000	0.3000, 0.5400, 0.7800	0.3600, 0.6000, 0.8200	0.1100, 0.3400, 0.6400	0.0800, 0.3100, 0.6100

TABLE 7. The weighted normalized fuzzy-decision matrix.

	A_1	A_2	A_3	A_4	A_5	A_6	A_7	A_8
T111	0.00200, 0.00700, 0.02100	0.00200, 0.00600, 0.02100	0.00100, 0.00600, 0.01900	0.00200, 0.00600, 0.02000	0.00100, 0.00500, 0.01900	0.00100, 0.00500, 0.01800	0.00100, 0.00400, 0.01600	0.00100, 0.00400, 0.01600
T112	0.00200, 0.00800, 0.02500	0.00200, 0.00800, 0.02700	0.00200, 0.00800, 0.02700	0.00200, 0.00800, 0.02500	0.00200, 0.00700, 0.02700	0.00200, 0.00700, 0.02500	0.00100, 0.00500, 0.02200	0.00100, 0.00400, 0.01900
T113	0.00200, 0.00800, 0.02400	0.00100, 0.00500, 0.01700	0.00100, 0.00500, 0.01800	0.00200, 0.00700, 0.02200	0.00200, 0.00700, 0.02400	0.00100, 0.00500, 0.01800	0.00000, 0.00300, 0.01600	0.00100, 0.00600, 0.02200
T121	0.00200, 0.00700, 0.02300	0.00100, 0.00600, 0.01900	0.00200, 0.00600, 0.01900	0.00200, 0.00700, 0.02300	0.00200, 0.00700, 0.02400	0.00100, 0.00500, 0.01800	0.00200, 0.00700, 0.02500	0.00100, 0.00600, 0.02200
T122	0.00300, 0.01000, 0.03200	0.00300, 0.01100, 0.03400	0.00300, 0.01100, 0.03600	0.00200, 0.00900, 0.03000	0.00200, 0.01000, 0.03500	0.00300, 0.01100, 0.03600	0.00200, 0.00900, 0.03400	0.00200, 0.00900, 0.03300
T123	0.00400, 0.01400, 0.04400	0.00300, 0.01200, 0.04100	0.00500, 0.01600, 0.04800	0.00500, 0.01600, 0.04900	0.00300, 0.01300, 0.04500	0.00300, 0.01200, 0.04100	0.00400, 0.01400, 0.05000	0.00300, 0.01400, 0.04900
T131	0.00400, 0.01400, 0.04300	0.00400, 0.01500, 0.04600	0.00400, 0.01300, 0.04200	0.00400, 0.01400, 0.04400	0.00300, 0.01200, 0.04200	0.00200, 0.01000, 0.03700	0.00200, 0.00900, 0.03800	0.00200, 0.01000, 0.03900
T132	0.00200, 0.00600, 0.01900	0.00200, 0.00600, 0.02000	0.00200, 0.00600, 0.01900	0.00200, 0.00600, 0.01800	0.00100, 0.00500, 0.01800	0.00100, 0.00500, 0.01600	0.00100, 0.00400, 0.01600	0.00100, 0.00400, 0.01700
T133	0.00200, 0.00700, 0.02300	0.00200, 0.00700, 0.02300	0.00200, 0.00700, 0.02300	0.00200, 0.00700, 0.02100	0.00100, 0.00500, 0.02000	0.00100, 0.00500, 0.01900	0.00100, 0.00400, 0.01700	0.00000, 0.00400, 0.01700
T141	0.00100, 0.00300, 0.01100	0.00100, 0.00400, 0.01100	0.00100, 0.00400, 0.01100	0.00100, 0.00400, 0.01100	0.00100, 0.00300, 0.01000	0.00100, 0.00300, 0.01000	0.00000, 0.00200, 0.00900	0.00000, 0.00200, 0.00900
T142	0.00400, 0.01200, 0.04010	0.00300, 0.01100, 0.03700	0.00300, 0.01000, 0.03700	0.00300, 0.01200, 0.04000	0.00200, 0.01000, 0.03800	0.00200, 0.00800, 0.03100	0.00200, 0.00800, 0.03500	0.00100, 0.00700, 0.03100
T143	0.00600, 0.02200, 0.07100	0.00500, 0.02000, 0.06600	0.00400, 0.01800, 0.06000	0.00500, 0.02000, 0.06600	0.00500, 0.02200, 0.07400	0.00400, 0.01800, 0.06300	0.00500, 0.02100, 0.07600	0.00500, 0.02100, 0.07600
T211	0.03300, 0.09300, 0.23300	0.04200, 0.11300, 0.26600	0.03100, 0.09100, 0.23200	0.03000, 0.08900, 0.23000	0.02100, 0.07800, 0.22300	0.03500, 0.10200, 0.25700	0.02100, 0.08000, 0.23600	0.01500, 0.06900, 0.21400
T212	0.04020, 0.11700, 0.28900	0.04600, 0.12400, 0.30300	0.03600, 0.10500, 0.27500	0.03300, 0.10000, 0.26000	0.02700, 0.09700, 0.27600	0.03400, 0.10700, 0.28000	0.02400, 0.09100, 0.27500	0.02100, 0.08700, 0.26600
T221	0.01000, 0.02700, 0.06800	0.01000, 0.02800, 0.07100	0.01100, 0.02900, 0.07200	0.00700, 0.02200, 0.05900	0.00700, 0.02300, 0.06500	0.00600, 0.02000, 0.05700	0.00500, 0.02100, 0.06500	0.00500, 0.02000, 0.06300
T222	0.01200, 0.03300, 0.08100	0.01100, 0.03200, 0.08000	0.01000, 0.02900, 0.07600	0.01000, 0.02800, 0.07400	0.00700, 0.02500, 0.07400	0.00700, 0.02300, 0.06700	0.00700, 0.02400, 0.07600	0.00600, 0.02300, 0.07300
T223	0.00600, 0.01600, 0.03600	0.00600, 0.01500, 0.03600	0.00600, 0.01500, 0.03500	0.00600, 0.01600, 0.03700	0.00500, 0.01400, 0.03700	0.00400, 0.01100, 0.03100	0.00200, 0.00900, 0.02900	0.00200, 0.00800, 0.02700
T311	0.03800, 0.11300, 0.27300	0.04600, 0.13000, 0.30200	0.03400, 0.10500, 0.26500	0.03300, 0.10000, 0.25100	0.02800, 0.09900, 0.27400	0.03200, 0.10400, 0.27300	0.00900, 0.05700, 0.20600	0.00800, 0.05700, 0.20600
T312	0.03100, 0.08800, 0.21600	0.03300, 0.09400, 0.22700	0.03300, 0.09400, 0.22700	0.03000, 0.08800, 0.21500	0.02200, 0.07600, 0.21500	0.03400, 0.09800, 0.24100	0.00900, 0.04700, 0.16600	0.00500, 0.04000, 0.15300
T321	0.02500, 0.07200, 0.18700	0.02400, 0.07200, 0.18700	0.02500, 0.07400, 0.19000	0.02300, 0.07000, 0.18300	0.01100, 0.04700, 0.15300	0.02000, 0.06700, 0.18500	0.00400, 0.03100, 0.12600	0.00200, 0.02300, 0.11000
T322	0.00800, 0.02500, 0.07000	0.01200, 0.03300, 0.08400	0.01100, 0.03100, 0.08100	0.00800, 0.02400, 0.06600	0.00500, 0.02000, 0.06500	0.00800, 0.02500, 0.07400	0.00300, 0.01500, 0.05800	0.00100, 0.01200, 0.05100
T323	0.00500, 0.01500, 0.04000	0.00700, 0.01900, 0.04700	0.00600, 0.01700, 0.04600	0.00400, 0.01300, 0.03800	0.00300, 0.01200, 0.03700	0.00400, 0.01300, 0.03900	0.00100, 0.00700, 0.03000	0.00100, 0.00700, 0.02900

TABLE 8. Closeness coefficients to the aspired level among the different alternatives.

Alternatives		d^{+i}	d^{-i}	Gap Degree of CC^{+i}	Satisfaction Degree of CC^{-i}
Alternative 1	A1	0.043845	0.026623	0.377803	0.622197
Alternative 2	A2	0.036748	0.036243	0.496541	0.503459
Alternative 3	A3	0.035237	0.041178	0.538873	0.461127
Alternative 4	A4	0.034652	0.027023	0.438152	0.561848
Alternative 5	A5	0.038358	0.045864	0.544561	0.455439
Alternative 6	A6	0.030494	0.046557	0.604236	0.395764
Alternative 7	A7	0.043845	0.025635	0.368955	0.631045
Alternative 8	A8	0.032765	0.042353	0.563820	0.436180

TABLE 9. Comparison the results of classical and fuzzy AHP-TOPSIS methods.

Methods/Alternatives	A1	A2	A3	A4	A5	A6	A7	A8
Fuzzy-AHP-TOPSIS	0.622197	0.503459	0.461127	0.561848	0.455439	0.395764	0.631045	0.436180
Classical-AHP-TOPSIS	0.610200	0.493960	0.448630	0.550850	0.446440	0.394260	0.625050	0.421180

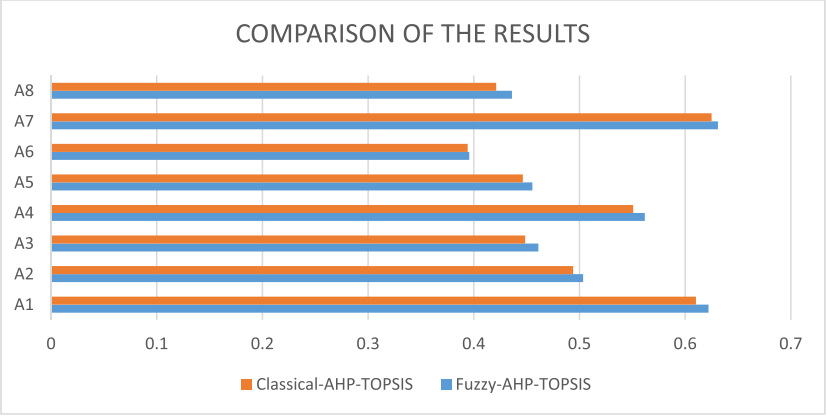

FIGURE 3. Graphical representation of the comparison between results of fuzzy and classical AHP-TOPSIS methods.

TABLE 10. Sensitivity analysis.

Experiments	Weights/Alternatives		A1	A2	A3	A4	A5	A6	A7	A8
Experiment-0	Original Weights		0.622197	0.503459	0.461127	0.561848	0.455439	0.395764	0.631045	0.436180
Experiment-1	T111		0.615500	0.498460	0.450130	0.556350	0.450440	0.395260	0.629050	0.428182
Experiment-2	T112		0.637797	0.508459	0.463127	0.567848	0.459939	0.395764	0.634045	0.444183
Experiment-3	T113		0.634197	0.513959	0.456127	0.573848	0.464439	0.397264	0.637045	0.452181
Experiment-4	T121		0.625197	0.691459	0.468727	0.583748	0.455239	0.406264	0.633745	0.429181
Experiment-5	T122		0.663997	0.546059	0.501927	0.599048	0.496839	0.435064	0.668745	0.468182
Experiment-6	T123		0.711297	0.595059	0.546727	0.642348	0.543239	0.478764	0.656045	0.521683
Experiment-7	T131	Satisfaction Degree (CC^{-i})	0.619497	0.508159	0.456927	0.549448	0.455039	0.390064	0.626045	0.416185
Experiment-8	T132		0.614997	0.512059	0.452327	0.535148	0.454839	0.384564	0.618445	0.411180
Experiment-9	T133		0.634897	0.496459	0.459127	0.563848	0.448139	0.405164	0.632045	0.437180
Experiment-10	T141		0.633197	0.507459	0.460627	0.562448	0.451839	0.400764	0.632045	0.437182
Experiment-11	T142		0.617197	0.483459	0.462127	0.560448	0.459139	0.391164	0.630545	0.435183
Experiment-12	T143		0.609597	0.478459	0.462927	0.559448	0.462439	0.386164	0.629545	0.434185
Experiment-13	T211		0.647197	0.728959	0.540627	0.658148	0.543439	0.478164	0.726545	0.527681
Experiment-14	T212		0.659897	0.535459	0.499127	0.607148	0.497439	0.444464	0.676045	0.481679
Experiment-15	T221		0.581597	0.445259	0.427127	0.521148	0.417839	0.360764	0.591045	0.398178
Experiment-16	T222		0.549197	0.407759	0.396127	0.485148	0.383839	0.329164	0.555545	0.363680
Experiment-17	T223		0.543780	0.431460	0.383627	0.486348	0.382939	0.321764	0.560045	0.360180
Experiment-18	T311		0.580797	0.466459	0.416627	0.523348	0.417939	0.357764	0.594045	0.397181
Experiment-19	T312		0.664197	0.542459	0.489627	0.672848	0.493939	0.435764	0.600045	0.477181
Experiment-20	T321		0.719197	0.582959	0.529127	0.645848	0.534939	0.477764	0.710045	0.520180
Experiment-21	T322		0.544797	0.423659	0.391127	0.492048	0.385639	0.328064	0.558045	0.340482
Experiment-22	T323		0.580797	0.463059	0.424127	0.593448	0.418039	0.359764	0.540445	0.377980

degree $(CC)^{-i}$ in 2 experiments including experiment-4 and 13. Alternative-4 (A4) has high satisfaction degree $(CC)^{-i}$ in 2 experiments including expertment-19 and 22. Therefore, the results of sensitivity analysis experiment

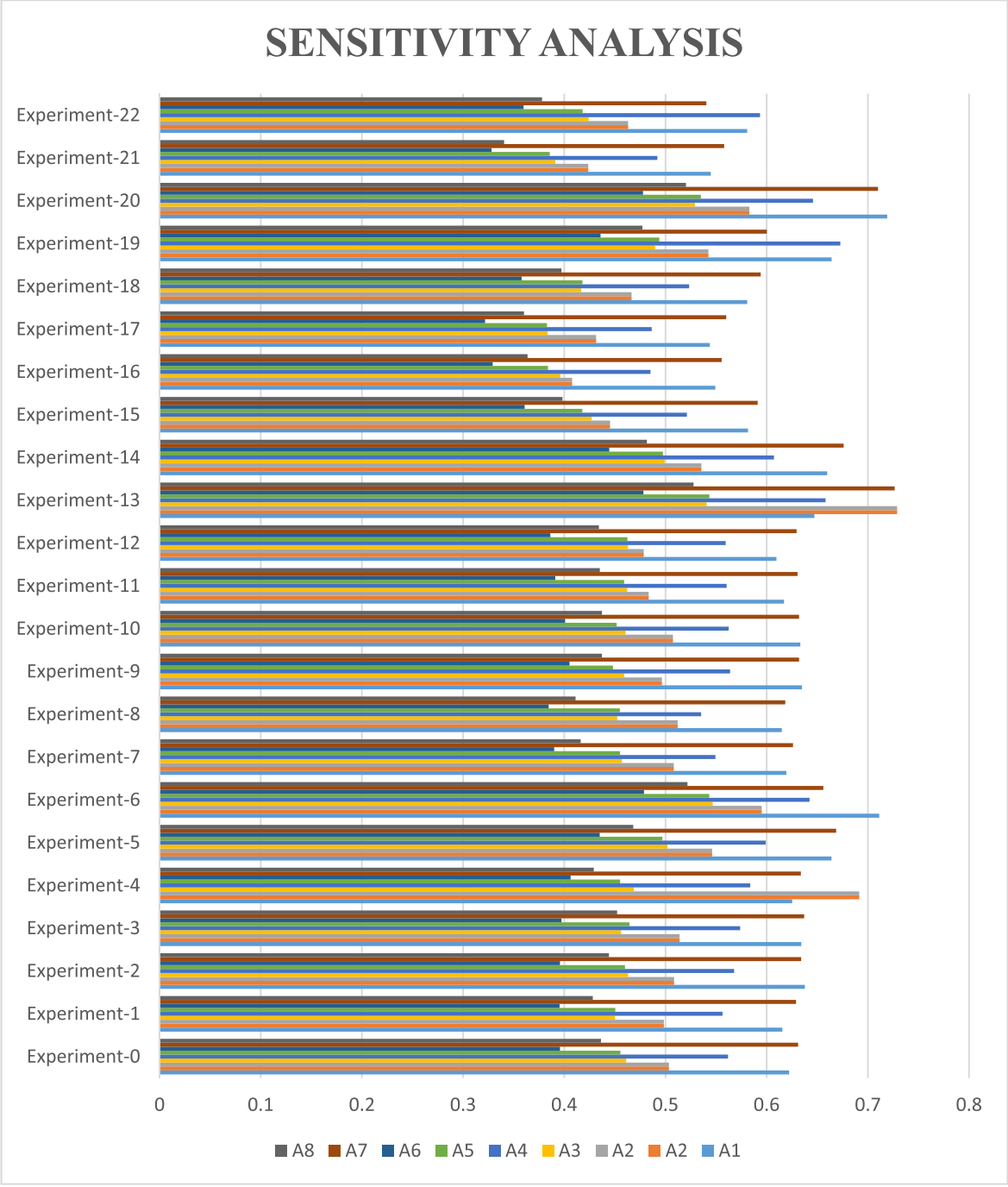

FIGURE 4. Graphical representation of the sensitivity analysis.

signified that the ranking of solutions is relatively sensitive to the barriers weights.

VIII. DISCUSSION

The importance of using architectural tactics for security was discussed in 2017 by JCS Santos [10]. This paper has presented an empirical approach to detect the vulnerabilities related to security tactics. The tactics proved to be the proper solution for every architectural issue faced during the assessment of security. All that was needed was an expert architecture or developer to implement. Thus, the assurance of security by using security tactics has emerged as a solution for making a web application secure. Garcia *et al.* [21] in 2014 gave a methodological approach to implement security tactics for proven security. A case study of *tsunami early warning system* has been taken in this study to validate the results. Still, Garcia's study lacks proper guidelines which can aid the developers and be adhered to for security tactics.

The present research study used hybrid method of fuzzy AHP-TOPSIS for prioritizing security design tactics to secure

web application. Because of the high usage of web applications in different areas, its security has become the need of the day. In addition, exponential growth in security attacks imposes the need to develop web applications that enable high security. Further, outcomes of this research work as follows:

- TOPSIS is a method which has rationality, simplicity and good computational efficiency. When TOPSIS method is mixed with fuzzy AHP which gives unambiguous and crisp results, it becomes the most efficient method.
- Security tactics selection among available multiple tactics is a problem that should be approached for a secure web application design.
- Fuzzy AHP-TOPSIS is proved to be an efficient method as per the results achieved through comparison.
- Sensitivity of the results is achieved by changing the variables and it shows that the results are sensitive to the weights.
- Feasible application of security design tactics is a persistent problem of this era and according to its importance it should be given a top priority but is largely ignored. The prioritization of security design tactics will help the developers to pick the important one for security.
- Better empanelment of security tactics into the web application needs thorough assessment and prioritization. According to the results achieved, the most prioritized factor is the specialized access in testability tactics. This affirmation will further help in focusing on the prioritized factors for accomplishing high security.
- The results of the study will help the developers to focus on using more important security tactics for overall security of web application.

The issues and challenges that were identified during this assessment are listed as follows:

- The data collected in this paper may be limited to the resources available. Further, the data analysis can be done through different techniques. For example area compensation method has been used in the TOPSIS assessment but other approaches can also be used for the same.
- Other attributes such as modifiability and its sub-attributes have not been considered in this assessment and this might impact the security tactics in a measurable way.
- The future work in this domain might add other attributes to the hierarchy of security design tactics.

IX. CONCLUSION

Effective security and its integration with design tactics in web applications require clarifying the current perceptions of tactics and defining a concrete framework for security and it's engineering. As a first milestone, this paper presented prioritization framework with Fuzzy AHP-TOPSIS methodology for prioritization of design tactics for security of web application. Through the framework and the designed hierarchy, the most prioritized factor is the specialized access in testability. The second high prioritized tactics is Cancel/Undo tactics in support user initiative of usability. Hence, the results validate that for achieving the more secure web application, developer should use tactics of specialized access tactics in testability. The software industry has developed a large number of insecure systems with various vulnerabilities in tactics which makes the application complex and, consequently, less secure. In wake of the increasing cases of security breaches, development of security guidelines which also focus on security tactics is mandatory. Hence, prioritization of security design tactics will decidedly help the architects to make web applications more secure.

REFERENCES

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

[2] G. Marquez and H. Astudillo, "Identifying availability tactics to support security architectural design of microservice-based systems," in *Proc. Eur. Conf. Softw. Archit. (ECSA)*, Paris, France, Sep. 2019, pp. 123–129.

[3] *Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems*, Standard IEC 615038, International Electrotechnical Commission, 1998.

[4] (2019). *Top Software Failures in Recent History*. [Online]. Available: https://www.computerworld.com/article/3412197/top-software-failures-in-recent-history.html

[5] L. Lofgren. *Website Security Guide*. Accessed: Dec. 20, 2019. [Online]. Available: https://www.quicksprout.com/website-security/

[6] J. Ryoo, B. Malone, P. A. Laplante, and P. Anand, "The use of security tactics in open source software projects," *IEEE Trans. Rel.*, vol. 65, no. 3, pp. 1195–1204, Sep. 2016.

[7] A. Mardani, A. Jusoh, K. Nor, Z. Khalifah, N. Zakwan, and A. Valipour, "Multiple criteria decision-making techniques and their applications—A review of the literature from 2000 to 2014," *Econ. Res.-EkonomskaIstraživanja*, vol. 28, no. 1, pp. 516–571, 2015.

[8] J.-F. Chen, H.-N. Hsieh, and Q. H. Do, "Evaluating teaching performance based on fuzzy AHP and comprehensive evaluation approach," *Appl. Soft Comput.*, vol. 28, pp. 100–108, Mar. 2015.

[9] Y. C. Chou, H. Y. Yen, V. T. Dang, and C. C. Sun, "Assessing the human resource in science and technology for Asian countries: Application of fuzzy AHP and fuzzy TOPSIS," *Symmetry*, vol. 11, no. 2, pp. 251–262, 2019.

[10] J. C. Santos, A. Peruma, M. Mirakhorli, M. Galster, J. V. Vidal, and A. Sejfia. *Understanding Software Vulnerabilities Related to Architectural Security Tactics*. Accessed: Dec. 24, 2019. [Online]. Available: https://www.semanticscholar.org/paper/Understanding-Software-Vulnerabilities-Related-to-Santos-Peruma/4223ae9abeadb1d8c31c75db951b8b4e-5676a118

[11] F. Osses, G. Márquez, M. M. Villegas, C. Orellana, M. Visconti, and H. Astudillo, "Security tactics selection poker (TaSPeR) a card game to select security tactics to satisfy security requirements," in *Proc. 12th Eur. Conf. Softw. Archit., Companion*, 2019, Art. no. 54.

[12] G. Marquez, E. B. Fernandez, H. Astudillo, and G. Pedraza-García, "Revisiting architectural tactics for security," in *Proc. Eur. Conf. Softw. Archit.* Cham, Switzerland: Springer, 2018, pp. 55–69.

[13] A. M. Alashqar, H. M. El-Bakry, and A. A. Elfetouh, "A framework for selecting architectural tactics using fuzzy measures," *Int. J. Soft. Eng. Knowl. Eng.*, vol. 27, no. 03, pp. 475–498, Apr. 2017.

[14] G. Marquez, F. Osses, and H. Astudillo, "Review of architectural patterns and tactics for microservices in academic and industrial literature," *IEEE Latin Amer. Trans.*, vol. 16, no. 9, pp. 2321–2327, Sep. 2018.

[15] J. Ryoo, P. Laplante, and R. Kazman, "Revising a security tactics hierarchy through decomposition, reclassification, and derivation," in *Proc. IEEE 6th Int. Conf. Softw. Secur. Rel. Companion*, Jun. 2016, pp. 85–91.

[16] J. Ryoo, P. Laplante, and R. Kazman, "A methodology for mining security tactics from security patterns," in *Proc. 43rd Hawaii Int. Conf. Syst. Sci.*, 2010, pp. 1–5.

[17] U. Lechner, "Future security: Processes or properties?—Research directions in cybersecurity," in *Models, Mindsets, Meta: The What, the How, and the Why Not?* Cham, Switzerland: Springer, 2019, pp. 235–246.
[18] C. Rehn, "Software architectural tactics and patterns for safety and security," Univ. Kaiserslautern, Kaiserslautern, Germany, 2009, p. 67663.
[19] J. Parker, N. Vazou, and M. Hicks, "LWeb: Information flow security for multi-tier Web applications," in *Proc. ACM Program. Lang.*, vol. 75, 2019, pp. 1–30, doi: 10.1145/3290388.
[20] K. Sahu and R. K. Srivastava, "Soft computing approach for prediction of software reliability," *ICIC Express Lett.*, vol. 12, no. 12, pp. 1213–1222, 2018.
[21] G. P. H. Garcia Astudillo and D. Correal, "A methodological approach to apply security tactics in software architecture design," in *Proc. IEEE Colombian Conf. Commun. Comput.*, Jun. 2014, pp. 1–8.
[22] K. Sahu and R. Shree, "Stability: Abstract roadmap of software security," *Amer. Int. J. Res. Sci., Eng. Math.*, no. 15, pp. 183–186, 2015.
[23] C.-C. Sun, "A performance evaluation model by integrating fuzzy AHP and fuzzy TOPSIS methods," *Expert Syst. Appl.*, vol. 37, no. 12, pp. 7745–7754, Dec. 2010.
[24] K. Sahu, R. Shree, and R. Kumar, "Risk management perspective in SDLC," *Int. J. Adv. Res. Comput. Sci. Softw. Eng.*, vol. 4, no. 3, pp. 1247–1251, 2014.
[25] D. Pamucar, D. Bozanic, and D. Kurtov, "Fuzzification of the Saaty's scale and a presentation of the hybrid fuzzy AHP-TOPSIS model: An example of the selection of a brigade artillery group firing position in a defensive operation," *Vojnotehničkiglasnik*, vol. 64, no. 4, pp. 966–986, 2016.
[26] C.-C. Chou and K.-W. Yu, "Application of a new hybrid fuzzy AHP model to the location choice," *Math. Problems Eng.*, vol. 2013, pp. 1–12, 2013.
[27] 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.

MAMDOUH ALENEZI received the M.S. degree from DePaul University, in 2011, and the Ph.D. degree from North Dakota State University, in 2014. He is currently the Dean of the Educational Services and the Chief Information and Technology Officer (CITO) of Prince Sultan University. He has extensive experience in data mining and machine learning, where he applied several data mining techniques to solve several software engineering problems. He has conducted several research areas and development of predictive models using machine learning to predict fault-prone classes, comprehend source code, and predict the appropriate developer to be assigned to a new bug.

ALKA AGRAWAL received the Ph.D. degree from Babasaheb Bhimrao Ambedkar University, (A Central University), Vidya Vihar, Lucknow. She is currently working as an Assistant Professor with the Babasaheb Bhimrao Ambedkar University. She is a passionate researcher and has also published a number of research articles in national and international journals. She has research and teaching experience of more than 13 years. Her areas of research interests include software security and software vulnerability. She is currently working in the fields of big data security, genetic algorithms, and software security.

RAJEEV KUMAR received the master's degree in information technology and the Ph.D. degree in information technology from Babasaheb Bhimrao Ambedkar University (A Central University), Lucknow, Uttar Pradesh, India, in 2014 and 2019, respectively. He is currently working as a Guest Faculty with the Department of Information Technology, Babasaheb Bhimrao Ambedkar University (A Central University). He is young and an energetic researcher. He has more than five years of research and teaching experience. He has also published and presented articles in refereed journals and conferences. His research interests are in the areas of software security, software durability, software reliability, software sustainability, software usability, and software risk.

RAEES AHMAD KHAN is currently working as a Professor and also the Head of the Department of Information Technology and the Dean of the School for Information Science and Technology, Babasaheb Bhimrao Ambedkar University (A Central University), Vidya Vihar, Lucknow, India. He has more than 20 years of teaching and research experience. His areas of interests are software security, software quality, and software testing. He has published a number of national and international books (including Chinese Language), technical article, research articles, reviews and chapters on software security, software quality, and software testing.