Computers, Materials & Continua
DOI:10.32604/cmc.2021.013579
Article

Tech Science Press

Evaluating the Impact of Software Security Tactics: A Design Perspective

Mamdouh Alenezi[1], Abhishek Kumar Pandey[2], Richa Verma[3], Mohd Faizan[2], Shalini Chandra[3], Alka Agrawal[2], Rajeev Kumar[2,4,*] and Raees Ahmad Khan[2]

[1]College of Computer and Information Sciences, Prince Sultan University, Saudi Arabia
[2]Department of Information Technology, Babasaheb Bhimrao Ambedkar University, Lucknow, Uttar Pradesh, India
[3]Department of Computer Science, Babasaheb Bhimrao Ambedkar University, Lucknow, Uttar Pradesh, India
[4]Department of Computer Application, Shri Ramswaroop Memorial University, Lucknow, Uttar Pradesh, India
[*]Corresponding Author: Rajeev Kumar. Email: rs0414@gmail.com
Received: 11 August 2020; Accepted: 05 October 2020

Abstract: Design architecture is the edifice that strengthens the functionalities as well as the security of web applications. In order to facilitate architectural security from the web application's design phase itself, practitioners are now adopting the novel mechanism of security tactics. With the intent to conduct a research from the perspective of security tactics, the present study employs a hybrid multi-criteria decision-making approach named fuzzy analytic hierarchy process-technique for order preference by similarity ideal solution (AHP-TOPSIS) method for selecting and assessing multi-criteria decisions. The adopted methodology is a blend of fuzzy analytic hierarchy process (fuzzy AHP) and fuzzy technique for order preference by similarity ideal solution (fuzzy TOPSIS). To establish the efficacy of this methodology, the results are obtained after the evaluation have been tested on fifteen different web application projects (Online Quiz competition, Entrance Test, and others) of the Babasaheb Bhimrao Ambedkar University, Lucknow, India. The tabulated outcomes demonstrate that the methodology of the Multi-Level Fuzzy Hybrid system is highly effective in providing accurate estimation for strengthening the security of web applications. The proposed study will help experts and developers in developing and managing security from any web application design phase for better accuracy and higher security.

Keywords: Web application; software security; security tactics; fuzzy AHP; fuzzy TOPSIS

1 Introduction

The digital revolution has been the harbinger of instant connectivity and easy access at viable costs and time investments. Hence, digitization in every business is not only a present-day necessity but also the best available recourse to enhance revenue generation for any business. With more and more businesses becoming digitalized, web applications at present are being designed to meet the demand and structural needs of businesses through their secured architecture [1]. However, the increasing reliance on web applications has also led to dubious growth in the instances of data breach incidents. A report on

cybersecurity assessment stated that nearly 54% of organizations accepted that they had been affected by at least a single breach last year [2]. The report also states that the ratio of this data could be even higher as many companies did not report the breaches. Most companies believe that such a disclosure could affect their clients' trust and lead to loss of revenue, in addition to marring their brand image. Another report on failures of airplanes stated that British Airways was left stranded with its web application problem in 2019. That failure led to the cancellation of about a 100 of its flights while disrupting the schedule of another 200 flights.

Such a scenario calls for foolproof mechanism to develop and maintain web applications with enhanced security to safeguard the data of the users and the organizations. The present scenario needs the design of secure web applications that are immune to infringements. Nevertheless, ensuring and maintaining an invincible security mechanism is a challenging and complex job, more so because of the multifarious aspects associated with security features [3]. Summarizing these factors to manage security in web applications is a critical task Therefore, for achieving this goal, the developers are focusing on the development of secure software from the design phase of the web application itself [4]. In the present context, the developers are trying to add security attributes and measure possible breach threats in a web application at the design phase, and thereby, develop the web application according to the constructed security standards and model from the design phase.

The defects in the web applications that gives opportunity to the attackers to exploit applications are called *vulnerabilities*. Various security experts and advisors believe that a tested and verified security strategy can provide a good environment for security maintenance and can also reduce the possibilities of vulnerabilities. Several research studies have focused on assessing and strengthening the security from the web application's development design phase itself. Alenezi et al. [5] have proposed the novel fuzzy AHP-TOPSIS based prioritization concept that enlists security guidelines and strategies. The proposed concept is an effective approach for summarizing various security attributes. The cited study discusses various factors that affects the security of a web application and then assess those factors through a scientific methodology.

The authors of this study have also summarized various security attributes or factors that affect security in web applications. Thereafter, a hierarchical model of factors has been constructed for applying the fuzzy AHP-TOPSIS methodology. The model helps in finding and assessing the priority of various factors. Such an evaluation process provides a framework of well-defined security attributes, thereby helping the practitioners to inculcate more efficient security policies and strategies. There are various multi-criteria decision making (MCDM) techniques available for solving multiple decision problems. Therefore, finding an appropriate method for evaluation requires a judicious comparison of different techniques. A number of studies conducted in this regard suggest that fuzzy AHP based MCDM approaches are comparatively more effective and accurate [6] than the other available MCDM approaches.

In particular, the reference to Dr. Garg's study becomes notable in this league. The author's study enlists and defines some implications of the AHP methodology [7]. Therefore, to tackle these implications and barriers, we have added the fuzzy approach in the existing methodology to achieve better accuracy with fewer implications in our tabulations. Furthermore, in the context of analyzing security tactics, the selection of attributes or factors that are likely to be extremely vital components contributing to security is also a very critical task. Hence, to ensure precision in choosing the most determining attributes, this study uses the fuzzy AHP-TOPSIS technique. This technique uses aggregated pair-wise comparison matrices and fuzzification as well as the de-fuzzification process to evaluate the ranking of the criteria.

The rest of this study is organized as follows: Second section describes the security tactics. The third section details the methodology. After the evaluations, the results have been tabulated in the fourth, fifth and sixth sections. The seventh section presents the discussion, and section eight concludes this study.

2 Security Tactics for Secure Web Application

The maintenance of the security of the web applications is an extremely challenging task that needs continuous efforts to keep them secure [8,9]. Even a minor change in the web application's structure and mechanism can render it vulnerable, endangering the users' data. Thus, it is imperative to develop security tactics [10] for web applications that can be applied during the design phase of development and help in securing the application effectively. Security tactics is a significant tool that can help developers in designing exploitation-free web applications. Security tactics can best be explained as "*a concept that provides a clear and effective path for addressing the needs and problems of security at the design level of the web application*" [11,12].

There are seven important and main categories for security tactics in web applications. These are *Confidentiality, Availability, Testability, Scalability, Interoperability, Accountability, and Maintainability.* After reviewing the existing literature available on these factors, the authors have constructed the hierarchy of factors, as shown in Fig. 1.

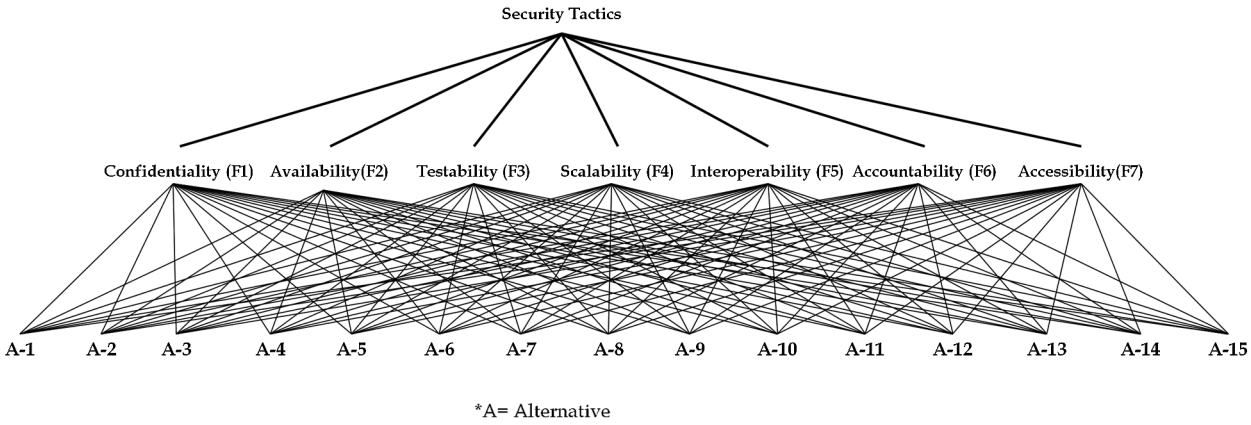

Figure 1: Tree structure of security factors

Confidentiality: Confidentiality is a process of maintaining the secrecy of data or information [13]. Web application's confidentiality is the key factor that affects the security of web applications. Thus, by the very virtue of its need, confidentiality is an important attribute.

Availability: Any data can only be useful if it is made available to the user at the required time. For instance, if at the time of extracting the required data, the search shows *unable to fetch "error 404"*, it would not only delay the outsourcing of crucial information but also stall the other related processes. Thus the factor of availability is an essential security tactic for a web application. However, the attackers are frequently targeting the availability of data to penetrate an organization or system [4]. Hence, *Availability Management* becomes an imperative aspect right from the design phase of web application development as a security tactic.

Testability: The testability of any web application is defined as its ability for testing its performance in an insecure attack situation. Testability is important for managing and validating the web application's security at any certain point in time [5].

Scalability: A functionality of any application that refers to its data adoption ability by its value growth within a particular timeframe is defined as scalability. For example, blockchain is used to carry financial transactional data and information, but currently, it is being utilized and developed [14] for healthcare data transactions that are larger and higher in volume. In terms of scalability, this change poses a great

challenge [14] for the blockchain developers. If a web application is not scalable in terms of its design, then attackers can exploit the application very easily through buffer overflow and other such advanced cyber-attacks [15]. Thus, scalability becomes an integral aspect of security tactics.

Interoperability: Compatibility of information format is a significant issue in web application development. Interoperability defines the factor or attribute of any web application that gives an additional quality to web applications in work with different non-similar data types or information formats [16]. Interoperability also becomes a vital focus in security tactics because it can cause data error and run time error at any point in the web application process.

Accountability: Web applications have many users that are responsible for data handling and security [17]. For instance, in case of a bank application, the cashier, manager and front-end executives have their own data handling and alter rights. But all of them are working on the same application that has the same connectivity. Therefore to assure information security in such an application, it is important to assign answerability for every node (user) regarding its actions within the application [15]. This type of answerability is called accountability and it is a vital component for maintaining security.

Accessibility: Information access within a web application is a matter of rights and accessibility. Accessibility is a factor or functionality of web application that provides categorization [15] related to information *read, write*, and *modify* (r/w/m) actions in web application. Managing access to data is the most significant task for the developers because wrong access rights can cause serious data modification, breach, and expose threats. Accessibility is defined in a web application through the access control model. Access management is one of the key components of any security mechanism and is also an important part of security tactics in web applications.

Apart from the factors mentioned above, the present study has also used some other alternatives to test the results obtained after using the fuzzy AHP method. To be specific, 15 sensitive online web application projects of Babasaheb Bhimrao Ambedkar University, Lucknow, India, were chosen as the alternatives. These projects included the *Online Quiz Competition, Entrance Test Application*, etc. A brief enumeration on the same has been described in the subsequent sections of the paper. Tab. 1 given below describes the various security factors and their contribution to security tactics for web applications.

Integrating security from the design phase, with specific reference to the tactics specified above, can be an efficacious approach for producing highly secure web applications. Moreover, to analyze and validate the technique related to web application security proposed in our study, we have adopted a hybrid methodology of Analytical Hierarchy Process and TOPSIS along with a fuzzy set theory called the fuzzy-AHP-TOPSIS approach. This is an MCDM approach that is highly effective for prioritizing and ranking various attributes for different fields or topics.

3 Methodology

Implementing security at the design phase [18–20] can enhance the security of web applications at the performance stage. For achieving this goal, preparing security tactics factors became a vital premise of the present study [10]. Furthermore, after successfully identifying the significant security tactics for web application security, the authors analyzed the impact and importance of these selected tactics. Evaluation of the significance of factors would be a useful reference for the experts and researchers in prioritizing the security tactics that need to be given more attention during web application development. For creating a priority list, we chose the most preferred methodology- the fuzzy-AHP-TOPSIS [21]. This is an MCDM approach that gives effective results in a multi-criteria selection situation. A brief description of the adopted methodology is described below:

Table 1: Key contributions of factors in security tactics concept

Factor	Key contribution to security tactics
Confidentiality	Its management can prevent various data breaches or expose related attacks like packet tracing, replay attack, session hijacking, and many others on the web application.
Availability	Its management can prevent Denial of Service (DoS), Distributed denial of services (DDoS), and its similar type of attacks that can harm availability directly.
Testability	Its management can prepare the web application to perform its testing at any point in time for insecure cyber-attacks.
Scalability	Its management can prevent the buffer overflow and similar storage level attacks that are directly related to the scalability issue of application.
Interoperability	Its management can provide a clear platform for data error related issues that are caused by interoperability issues.
Accountability	Its management provides authenticity for every node in web application architecture that helps in producing a secure web application.
Accessibility	Its management provides an assured access management mechanism from the web application design level that gives an additional and effective information security environment in web application.

Fuzzy AHP is a methodology that works on a tree-based structure through triangular fuzzy numbers (TFN) evaluation. Additionally, it creates pair-wise comparison matrices and then evaluates the assessment of these TFNs for developed hierarchy through selected tactics. The fuzzy AHP approach helped the authors to evaluate and analyze the importance of selected tactics for web application security.

To conduct this analysis, the authors developed a hierarchy after examining the relevant research literature in this domain, assimilating experts' opinions, and brainstorming. The authors chose 35 experts to analyze the value of specific factors through a questionnaire. We ensured that the panel of experts was a congregation of practitioners with enriched experience in the domain of web application and software development. The next step was to convert the original numbers given by the experts into TFN and prepare a comparison matrix. To make the analysis part simple and easy, this paper uses the TFN number that lies between 0 and 1 [22,23]. Furthermore, the calculated values are described as 1, 2, 3…..9. Additionally, the membership function of TFN, M on F is derived from Eqs. (1) and (2):

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

$$\mu_{\mathrm{a}}(\mathrm{x}) = \begin{cases} \dfrac{\mathrm{x}}{\mathrm{mi} - \mathrm{lo}} - \dfrac{\mathrm{b}}{\mathrm{mi} - \mathrm{lo}} & x \in [\mathrm{lo},\ \mathrm{mi}] \\ \dfrac{\mathrm{x}}{\mathrm{mi} - \mathrm{up}} - \dfrac{\mathrm{u}}{\mathrm{mi} - \mathrm{up}} & x \in [\mathrm{mi},\ \mathrm{up}] \\ 0 & \text{Otherwise} \end{cases} \tag{2}$$

In the above Triangular Membership Function, l, mi and u represent the lower, middle, and upper limit for TF numbers. TFN's are represented in Fig. 2.

In the above Fig. 2, l, mi, u represent the Triangular Fuzzy Numbers. Further in this paper, Tab. 2 describes the scale for ranking the factors' score for evaluating the factors that affect quantitatively. For converting the numeric values into the triangular fuzzy number, the authors have used Eqs. (3)–(6).

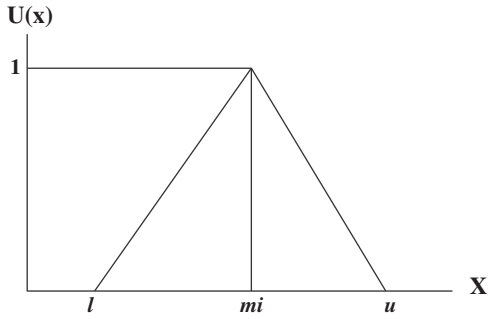

Figure 2: TFN

Table 2: TFN scale

Saaty scale definition	Scale	
1	Equally important	(1,1, 1)
3	Weakly important	(2,3, 4)
5	Fairly important	(4,5, 6)
7	Strongly important	(6,7, 8)
9	Absolutely important	(9,9, 9)

$$n_{ij} = \left(l_{ij}, m_{ij,}\, u_{ij}\right) \text{ where } l_{ij} \leq m_{ij} \leq u_{ij} \tag{3}$$

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

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

$$\text{and } u_{ij} = \left(J_{ijd}\right) \tag{6}$$

In the above equations, lij represents the lower limit; mij represents middle values and uij represents the upper value. Eq. (3) shows the TFN. Eqs. (7)–(9) have been used for integrating the different TFN values in the evaluation process.

$$\left(l_1, m_{i1,}\, u_1\right) + \left(l_2, m_{i2,}\, u_2\right) = \left(l_1 + l_2,\ m_{i1} + m_{i2,}\, u_1 + u_2\right). \tag{7}$$

$$\left(l_1, m_{i1,}\, u_1\right) \times \left(l_2, m_{i2,}\, u_2\right) = \left(l_1 \times l_2,\ m_{i1} \times m_{i2,}\, u_1 \times u_2\right) \tag{8}$$

$$\left(l_1, m_{i1,}\, u_1\right) - 1 = \left(\frac{1}{u_1}, \frac{1}{m_{i1}}, \frac{1}{l_1}\right) \tag{9}$$

After, evaluating all the TFN values, the analysts need to construct a *n x n* fuzzy comparison matrix through Eq. (10).

$$\widetilde{A^d} = \begin{bmatrix} \tilde{k}_{11}^d & \tilde{k}_{12}^d & \tilde{k}_{1n}^d \\ \cdots\cdots & \cdots\cdots & \cdots\cdots \\ \tilde{k}_{n1}^d & \tilde{k}_{n2}^d & \tilde{k}_{nn}^d \end{bmatrix} \tag{10}$$

In case of more than one preference being present in the evaluation process, the experts used Eq. (11) for calculating the average.

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

After calculating the average preference in the next step of the calculation, the experts updated the fuzzy integrated comparison matrix for hierarchy prepared through the practitioners' views. For calculating this step, the experts used the Eq. (12):

$$\tilde{A} = \begin{bmatrix} \widetilde{k_{11}} & \cdots & \widetilde{k_{1n}} \\ \cdots & \ddots & \cdots \\ \widetilde{k_{n1}} & \cdots & \tilde{k}_{nn} \end{bmatrix} \tag{12}$$

In the next step, the specialists ascertain the geometric mean and fuzzy weights of the factor through the following (13). Further, for normalizing and concluding the evaluation, Eqs. (14)–(16) have been used.

$$\tilde{P}_i = \left(\prod_{j=1}^{n} \tilde{k}_{ij}\right)^{1/n},\ i = 1, 2, 3, 4,\ \ldots..\text{n} \tag{13}$$

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

$$\mathrm{M_i} = \frac{\tilde{\mathrm{w}}_1 \oplus \tilde{\mathrm{w}}_2 \ldots.. \oplus \tilde{\mathrm{w}}_\mathrm{n}}{\mathrm{n}} \tag{15}$$

$$\mathrm{Nr_i} = \frac{\mathrm{M_i}}{\mathrm{M}_1 \oplus \mathrm{M}_2 \oplus \ldots\ldots \oplus \mathrm{M_n}} \tag{16}$$

At the end of the fuzzy AHP method, the best non-*fuzzy* performance (BNP) value is assessed by Eq. (17).

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

Thus by adopting the Fuzzy TOPSIS methodology, we obtained the ranking of different factors. Thereafter, to establish the authenticity of the results through a scientific approach, we employed the TOPSIS method. For attaining precise results, the TOPSIS technique utilizes fuzzy numbers rather than exact numbers to demonstrate the significance of factors. A step-by-step description of this methodology is described as follows:

In the initial step of the estimation, this paper utilized fuzzy AHP for assessing the pertinent weights through Eqs. (1)–(17). After that, in the following stage, the specialists arranged a correlation lattice and chose a variable with the assistance of Tab. 3 and Eq. (18).

$$\tilde{K} = \begin{array}{c} \\ A_1 \\ \ldots \\ A_m \end{array} \begin{array}{c} \begin{array}{ccc} Cr_1 & \cdots & Cr_n \end{array} \\ \begin{bmatrix} \tilde{\alpha}_{11} & \cdots & \tilde{\alpha}_{1n} \\ \ldots & \ddots & \ldots \\ \tilde{\alpha}_{m1} & \cdots & \tilde{\alpha}_{mn} \end{bmatrix} \end{array} \tag{18}$$

In the accompanying advances, the fuzzy framework is standardized through Eq. (19), and the grid is formed by utilizing Eq. (20).

$$\tilde{P} = \left[\tilde{P}_{ij}\right]_{m \times n} \tag{19}$$

Table 3: Ranking scale

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

$$\tilde{Q} = \left[\tilde{q}_{ij}\right]_{m\times n} \; i = 1,2,3, \; \ldots\ldots m; \; j = 1,2,3,4, \; \ldots\ldots n \tag{20}$$

After the assessment, the examiners used Eq. (21) to decide the assessed elective gap degree of factors.

$$C\tilde{C} = \frac{\tilde{k}_i^-}{\tilde{k}_i^+ + \tilde{k}_i^-} = 1 - \frac{\tilde{k}_i^+}{\tilde{k}_i^+ + \tilde{k}_i^-}, \; i = 1,2, \; \ldots\ldots, \; m \tag{21}$$

At the end of the evaluation process, through Eq. (21), the experts assigned a gap degree for factors and obtained the testing results that show the performance of selected alternatives based on evaluated results from the fuzzy AHP method.

4 Results and Analysis

The hierarchy image of factors (Fig. 1) discusses different factors of security tactics for a web application. Based on Fig. 1, the authors used the fuzzy AHP-TOPSIS methodology for ranking the factors. In Fig. 1, the hierarchy has a total of seven factors that directly affect security tactics. To conduct this analysis, the authors compiled and processed the collated opinions from selected decision-makers and then, through the use of Eqs. (1)–(9) as well as according to Tab. 1, converted the linguistic values into the TFN. The evaluated calculation is described in the following Tab. 4. The authors have applied fuzzy AHP-TOPSIS methodology on all these seven factors and step-wise results are described in Tab. 4.

Table 4: Integrated fuzzy pair-wise comparison matrix

	F1	F2	F3	F4	F5	F6	F7
F1 (Confidentiality)	1.000, 1.000, 1.000	1.000, 1.000, 1.350	1.000, 1.190, 1.540	1.000, 1.000, 1.190	1.000, 1.190, 1.690	1.190, 1.540, 2.040	1.380, 1.880, 2.380
F2 (Availability)	0.770, 1.000, 1.000	1.000, 1.000, 1.000	0.900, 1.000, 1.350	0.900, 1.000, 1.000	1.000, 1.000, 1.350	1.000, 1.350, 1.690	1.000, 1.350, 1.850
F3 (Testability)	0.710, 0.870, 1.000	0.770, 1.000, 1.150	1.000, 1.000, 1.000	0.770, 1.000, 1.000	1.000, 1.000, 1.150	1.000, 1.000, 1.500	1.000, 1.150, 1.650

Table 4 (continued).

	F1	F2	F3	F4	F5	F6	F7
F4 (Scalability)	0.870, 1.000, 1.000	1.000, 1.000, 1.150	1.000, 1.000, 1.350	1.000, 1.000, 1.000	1.000, 1.000, 1.500	1.000, 1.350, 1.850	1.000, 1.500, 2.000
F5 (Interoperability)	0.610, 0.870, 1.000	0.770, 1.000, 1.000	0.900, 1.000, 1.000	0.670, 1.000, 1.000	1.000, 1.000, 1.000	1.000, 1.000, 1.350	1.000, 1.000, 1.500
F6 (Accountability)	0.510, 0.710, 0.870	0.650, 0.770, 1.000	0.670, 1.000, 1.000	0.550, 0.770, 1.000	0.770, 1.000, 1.000	1.000, 1.000, 1.000	1.000, 1.000, 1.150
F7 (Accessibility)	0.440, 0.570, 0.810	0.550, 0.770, 1.000	0.620, 0.900, 1.000	0.500, 0.670, 1.000	0.670, 1.000, 1.000	0.900, 1.000, 1.000	1.000, 1.000, 1.000

Tab. 4 is the matrix of the comparison of various factors that directly affect information security according to the hierarchy depicted in Fig. 1. After this step, the authors evaluated the weights and BNP values of various factors through the Eqs. (11)–(16) and (21) and tabulated their respective ranks as shown in Tab. 5.

Table 5: Weights of factors

Factors	Weights	BNP	Rank
F1 (Confidentiality)	0.1250, 0.1750, 0.2600	0.2120	1
F2 (Availability)	0.1090, 0.1530, 0.2140	0.1700	3
F3 (Testability)	0.1040, 0.1390, 0.1970	0.1420	4
F4 (Scalability)	0.1140, 0.1560, 0.2290	0.1800	2
F5 (Interoperability)	0.0980, 0.1360, 0.1820	0.1270	5
F6 (Accountability)	0.0850, 0.1240, 0.1630	0.0910	6
F7 (Accessibility)	0.0770, 0.1170, 0.1580	0.0770	7

Furthermore, to analyze and test the effect of the factors, the authors selected the web applications of Babasaheb Bhimrao Ambedkar University, Lucknow, India. Fifteen sensitive online web application projects as alternatives were chosen to map a more comprehensive empirical base. These selected alternatives are highly sensitive like the Online Quiz Competition, Entrance Test Application, etc. In the following Tabs. 6 and 7, the authors have described the subjective cognition results and their respective normalized fuzzy decision matrix through the Eqs. (18)–(21).

After these evaluations, the authors mapped the normalized fuzzy matrix in Tab. 7 through Eq. (20). Thereafter, the satisfaction degree as well as the gap degree of different alternatives among various factors through Eq. (21) was measured, as described in Tab. 8.

Table 6: Subjective cognition results

Alternatives/Factors	F1	F2	F3	F4	F5	F6	F7
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	3.0000, 5.0000, 7.0000
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	3.0000, 5.0000, 7.0000
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	3.0000, 5.0000, 7.0000
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, 10.000	9.0000, 10.000, 10.000	7.0000, 9.0000, 10.000
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	2.2400, 4.2400, 6.2400
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	7.0000, 9.0000, 10.000
A7	7.7600, 9.3800, 10.000	7.0000, 9.0000, 10.000	7.0000, 9.0000, 10.000	6.2400, 8.2400, 9.6200	5.0000, 7.0000, 9.0000	3.7600, 5.7600, 7.7600	6.2400, 8.2400, 9.6200
A8	1.0000, 3.0000, 5.0000	3.0000, 5.0000, 7.0000	7.0000, 9.0000, 10.000	5.6200, 7.6200, 9.3100	7.0000, 9.0000, 10.000	1.6200, 3.6200, 5.6200	5.6200, 7.6200, 9.3100
A9	3.0000, 5.0000, 7.0000	7.0000, 9.0000, 10.000	7.0000, 9.0000, 10.000	5.7600, 7.7600, 9.3800	3.0000, 5.0000, 7.0000	5.6200, 7.6200, 9.3100	5.7600, 7.7600, 9.3800
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	4.3800, 6.3800, 8.3800
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	3.0000, 5.0000, 7.0000
A12	7.0000, 9.0000, 10.000	5.6200, 7.6200, 9.3100	9.0000, 10.0000, 10.000	3.0000, 5.0000, 7.0000	3.0000, 5.0000, 7.0000	3.0000, 5.0000, 7.0000	3.0000, 5.0000, 7.0000
A13	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	7.0000, 9.0000, 10.000

Table 6 (continued).

Alternatives/Factors	F1	F2	F3	F4	F5	F6	F7
A14	7.7600, 9.3800, 10.000	7.0000, 9.0000, 10.000	7.0000, 9.0000, 10.0000	6.2400, 8.2400, 9.6200	5.0000, 7.0000, 9.0000	3.7600, 5.7600, 7.7600	6.2400, 8.2400, 9.6200
A15	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	5.6200, 7.6200, 9.3100

Table 7: Weighted normalized fuzzy-decision matrix

Alternative/Factors	F1	F2	F3	F4	F5	F6	F7
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	0.00900, 0.01400, 0.02000
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	0.00900, 0.01400, 0.02000
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	0.00900, 0.01400, 0.02000
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	0.02000, 0.02600, 0.02900
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	0.00600, 0.01200, 0.01800
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	0.03600, 0.04700, 0.05200
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	0.03200, 0.04300, 0.05000
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	0.02900, 0.03900, 0.04800
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	0.03000, 0.04000, 0.04800
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	0.02300, 0.03300, 0.04300

(Continued)

Table 7 (continued).

Alternative/Factors	F1	F2	F3	F4	F5	F6	F7
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	0.01600, 0.02600, 0.03700
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	0.01600, 0.02600, 0.03700
A13	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	0.03600, 0.04700, 0.05200
A14	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	0.03200, 0.04300, 0.05000
A15	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	0.02900, 0.03900, 0.04800

Table 8: Closeness coefficients to aspired level among different alternatives

Alternatives	di−	di+	Satisfaction degree of CCi
A1	0.7400	29.1200	0.02012
A2	0.7100	29.2100	0.02121
A3	0.7200	29.3200	0.02411
A4	0.7300	29.4200	0.02331
A5	0.6600	29.0000	0.01914
A6	0.6700	29.1400	0.02201
A7	0.6500	29.2400	0.02510
A8	0.7210	29.3100	0.02340
A9	0.7320	29.4300	0.02103
A10	0.6540	29.1400	0.02400
A11	0.7010	29.0100	0.02602
A12	0.7150	29.0500	0.02511
A13	0.6600	29.0000	0.02314
A14	0.6700	29.1400	0.02101
A15	0.6500	29.2400	0.02210

Tab. 8, above, illustrates the overall results of testing through fuzzy-TOPSIS as a satisfaction degree format. The results obtained from Tab. 8 suggest that the gap degree between different alternatives is in *good* and *very good* condition. Therefore, authors can say that security tactics are in *good* and *very good* condition for the selected web applications.

5 Sensitivity Analysis

Sensitivity Analysis assess the impact of the set of independent variables over dependent variables under some definite conditions [24]. Such an analysis establishes the robustness of tested and evaluated results, thereby authenticating the findings and making the results an accurate base for future research and reference. The given study analyzes the sensitivity of results through a method where value for one factor fluctuates by 0.05 at a particular time, while the values for the other factors remain the same [25]. Moreover, when the value of one factor fluctuates by 0.05, at the same time, the remaining factors' values must be the same as that of the original values. This evaluation provides an indication of the performance in the results when the resources or valuation of factors are changed, and also depicts the impact of fluctuation value over the results. The final results of sensitivity analysis are shown in Tab. 9 and Fig. 3.

Table 9: Sensitivity analysis

Alternatives/Factors	F1	F2	F3	F4	F5	F6	F7
A1	0.10922	0.06192	0.02128	0.05728	0.02312	0.02082	0.01292
A2	0.11281	0.06381	0.01919	0.05859	0.00921	0.01391	0.02981
A3	0.10971	0.06491	0.01289	0.04589	0.03171	0.02811	0.01531
A4	0.10381	0.06051	0.01509	0.04649	0.04521	0.03321	0.00339
A5	0.10694	0.06054	0.01826	0.05066	0.01894	0.01894	0.01854
A6	0.10501	0.06131	0.01399	0.04569	0.03251	0.02701	0.01081
A7	0.05010	0.06280	0.01550	0.0479	0.02780	0.02610	0.01250
A8	0.10890	0.05540	0.03480	0.0723	0.01640	0.02740	0.00160
A9	0.10053	0.05903	0.01297	0.04397	0.01903	0.02053	0.02283
A10	0.12030	0.06930	0.01670	0.0527	0.02600	0.02460	0.02160
A11	0.11402	0.06802	0.01158	0.04558	0.01872	0.02242	0.03302
A12	0.10751	0.07381	0.00989	0.04149	0.03451	0.03011	0.01551
A13	0.11864	0.06814	0.01686	0.05236	0.02414	0.02414	0.02164
A14	0.11251	0.06651	0.01699	0.05149	0.02201	0.02201	0.01901
A15	0.10110	0.06110	0.01490	0.04890	0.01610	0.02010	0.02810

It is evident from Fig. 3 and Tab. 9 that *Alternative 1* has the best performance in each analysis for all the 15 alternatives. Further, fluctuation in results shows that results are sensitive to resource changes that are acceptable [26] in the evaluation process. As per the sensitivity analysis test, it is observed that the variation in overall results is negligible.

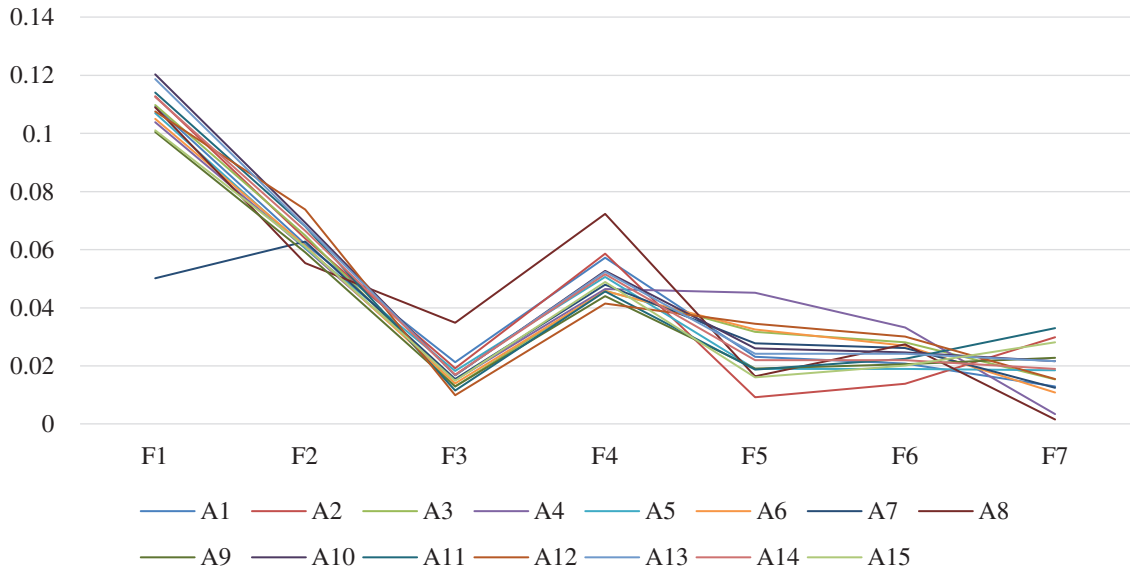

Figure 3: Sensitivity analysis

6 Comparison through Classical Approach

The comparison of the results plays a vital role in the validation and corroboration of the research analysis. To apply this statement in this study, the authors compared the adopted fuzzy AHP-TOPSIS method with the classical AHP-TOPSIS approach. For accurate comparison analysis, we conducted an evaluation of selected techniques on 15 same alternatives for selected security tactics. The authors have calculated the Pearson-correlation coefficient value for both techniques because it is a widely used statistic that measures the degree of relationship between the two variables [27]. The value is found to be 0.7681. The results of both the techniques clearly illustrate that the fuzzy-based approach provides better results as compared to the classical technique. In a nutshell, we can say that the adopted methodology is better and effective than the classical AHP-TOPSIS. A graphical and tabular description of comparative analysis is shown in Tab. 10.

Table 10: Comparison analysis

Alternatives	Fuzzy AHP-TOPSIS	Classical AHP-TOPSIS
A1	0.02012	0.02122
A2	0.02121	0.02231
A3	0.02411	0.02241
A4	0.02331	0.02211
A5	0.01914	0.01900
A6	0.02201	0.02311
A7	0.02510	0.02420
A8	0.02340	0.02230
A9	0.02103	0.02101
A10	0.02400	0.02445
A11	0.02602	0.02652

Table 10 (continued).

Alternatives	Fuzzy AHP-TOPSIS	Classical AHP-TOPSIS
A12	0.02511	0.02171
A13	0.02314	0.02354
A14	0.02101	0.02212
A15	0.02210	0.02250

7 Discussion

Implementing architectural security in web applications was first proposed by Ryoo et al. [11] in 2016. However, even in the present context, the delivery of a technical product with an ideal security mechanism continues to be a challenge for the developers. In this league, maintaining security attributes from the design or development phase of software and web application [18,19] can produce effective security measures, thereby maintaining data security effectively and minimizing the risk of data breaches. Addressing this research quest, the present study provides an overview of the need for security tactics and evaluates various security tactics for web application security. In the proposed study, the researchers have used a hybrid fuzzy AHP-TOPSIS methodology for assessing the performance of web application insecurity tactics perspective. The key contributions of this research article are:

- The evaluation of security tactics for producing secure web applications is a domain for intensive research. This study used the hybrid fuzzy based AHP-TOPSIS methodology for quantitative assessment of various security tactics in web applications.
- Selected security tactics are extremely effective for web application security and their accurate implementation, according to the calculated results, can produce a highly secure web application.
- To establish the effectiveness of the proposed scheme, the evaluation is undertaken for 15 online web applications.
- Statistical validation has been done to establish the validity of the results; the correlation coefficient is computed and found to be 0.7681.
- The comparative analysis done in the study also corroborates that fuzzy-AHP TOPSIS is an efficient method.
- According to the calculated results, it is evident that *confidentiality* is the most prioritized factor amongst all the tactics. Developers need to focus on confidentiality first to design a secure web application.

The pros and cons of the paper can be listed as-

7.1 Pros-

- Assessment of web application security as per the security-tactics perspective is a way of evaluation of security tactics about a web application.
- A thorough and prioritized implementation of security tactics can be a better result producer. The outcome of this study will help the experts and developers to concentrate on the most pertinent security tactics.
- The given approach will also help the security practitioners to assess the priority in accordance with the given rank while developing the web applications.

7.2 Cons-

- More Security tactics can be considered apart from the ones used in this paper.
- The data evaluated in this paper is from limited resources. The evaluation techniques may also be different from the approach selected for our study.
- Only the first layer of factors has been described in this study. Future research studies might consider the two-layer and three-layer architecture for evaluation.

8 Conclusion

Frequent penetration of web applications security through massive and highly advanced cyber-attacks has created a dangerous situation for information security in web applications. The alarming scenario necessitates the implementation of security tactics more constructively, that too from the web applications' development phase itself. To apply the security tactics mechanism on the web application development phase, it is important to determine those tactics that must be prioritized during the development phase. For achieving the stated objective, the study used an MCDM approach, the fuzzy-AHP-TOPSIS. The results drawn from the evaluations were tested on 15 different web application projects of Babasaheb Bhimrao Ambedkar University. The assessed and tested results of this study are highly accurate and conclusive. Moreover, the findings of the present research investigation can be adopted by the developers for producing secure web applications. The effective security tactics evaluation tabulated in the study would be a useful empirical framework for future research pursuits. Furthermore, the study can also be extended by adding more security tactics in the proposed hierarchy for eliciting even more efficient results.

Acknowledgement: Authors are thankful to Prince Sultan University, Saudi Arabia for providing the fund to carry out the work.

Funding Statement: Prince Sultan University, Riyadh, Kingdom of Saudi Arabia.

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

References

[1] K. Sahu and R. K. Srivastava, "Revisiting software reliability," *Data Management, Analytics and Innovation, Advances in Intelligent Systems and Computing*, vol. 808, pp. 221–235, 2019.

[2] L. Lofgren, Website security guide. 2019. [Online]. Available: https://www.quicksprout.com/website-security/. (accessed 31 July 2020).

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

[4] G. Marquez and H. Astudillo, "Identifying availability tactics to support security architectural design of micro service-based systems," *European Conference on Software Architecture*, vol. 2, pp. 123–129, 2019.

[5] M. Alenezi, A. Agrawal, R. Kumar and R. A. Khan, "Evaluating performance of web application security through a fuzzy based hybrid multi-criteria decision-making approach: Design tactics perspective," *IEEE Access*, vol. 8, pp. 25543–25556, 2020.

[6] A. Agrawal, M. Zaroor, M. Alenezi, R. Kumar and R. A. Khan, "Security durability assessment through fuzzy analytic hierarchy process," *PeerJ Computer Science*, vol. 5, pp. 1–43, 2019.

[7] D. Garg, S. Luthra and A. Haleem, "Ranking of performance measures of GSCM towards sustainability: Using analytic hierarchy process," *International Journal of Social Management Economics and Business Engineering*, vol. 8, no. 3, pp. 764–770, 2014.

[8] B. Stack, Here's how much your personal information selling for on the dark web. 2017. [Online]. Available: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/. (Accessed 31 July 2020).

[9] Web application security. 2018. [Online]. Available: https://www.techopedia.com/definition/24377/web-application-security. (Accessed 31 July 2020).

[10] G. P. Garcia, H. Astudillo and D. Correal, "A methodological approach to apply security tactics in software architecture design," in *2014 IEEE Colombian Conf. on Communications and Computing, IEEE*, vol. 124, pp. 1–8, 2014.

[11] J. Ryoo, P. Laplante and R. Kazman, "Revising a security tactics hierarchy through decomposition, reclassification, and derivation," in *2012 IEEE Sixth Int. Conf. on Software Security and Reliability Companion, IEEE*, pp. 85–91, 2016.

[12] J. Ryoo, P. Laplante and R. Kazman, "A methodology for mining security tactics from security patterns," in *43rd Hawaii Int. Conf. on System Sciences, IEEE*, pp. 1–5, 2010.

[13] A. Appari and M. Eric Johnson, "Information security and privacy in healthcare: Current state of research," *International Journal of Internet and Enterprise Management*, vol. 6, no. 4, pp. 279–314, 2010.

[14] A. K. Pandey, A. I. Khan, Y. B. Abushark, M. M. Alam, A. Agrawal *et al.,* "Key issues in healthcare data integrity: Analysis and recommendations," *IEEE Access*, vol. 8, pp. 40612–40628, 2020.

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

[16] B. Sommardahl Durable Software, Awkward Coder Learning to Behave in Public 5–8. 2013. [Online]. Available: https://www.durable-north-america.com/service/duraprint-software.html (Accessed 31 July 2020).

[17] R. Kumar, A. K. Pandey, A. Baz, H. Alhakami, W. Alhakamiet *et al.,* "Fuzzy-based symmetrical multi-criteria decision-making procedure for evaluating the impact of harmful factors of healthcare information security," *Symmetry*, vol. 12, no. 4, pp. 664–688, 2020.

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

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

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

[21] A. Agrawal, M. Alenezi, S. A. Khan, R. Kumar and R. A. Khan, "Multi-level fuzzy system for usable-security assessment," *Journal of King Saud University: Computer and Information Sciences*, (In Press), pp. 1–9, 2019.

[22] 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.

[23] C. C. Sun, "A performance evaluation model by integrating fuzzy AHP and fuzzy TOPSIS methods," *Expert Systems with Applications*, vol. 37, no. 12, pp. 7745–7754, 2010.

[24] C. N. Wang, C. Y. Yang and H. C. Cheng, 'A fuzzy multicriteria decision-making (MCDM) model for sustainable supplier evaluation and selection based on triple bottom line approaches in the garment industry," *Processes*, vol. 7, no. 7, pp. 400–415, 2019.

[25] R. Kumar, A. I. Khan, Y. B. Abushark, M. M. Alam, A. Agrawal *et al.,* "An integrated approach of fuzzy logic, AHP and TOPSIS for estimating usable-security of web applications," *IEEE Access*, vol. 8, pp. 50944–50957, 2020.

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

[27] Correlation (Pearson, Kendall, Spearman), Statistics Solutions, 2018. [Online]. Available: https://www.statisticssolutions.com/correlation-pearson-kendall-spearman/. (Accessed 4 August 2020).