Intelligent Automation & Soft Computing
DOI:10.32604/iasc.2021.016646
Article

Tech Science Press

Managing Software Security Risks through an Integrated Computational Method

Abdullah Alharbi[1], Wael Alosaimi[1], Hashem Alyami[2], Mohd Nadeem[3], Mohd Faizan[3], Alka Agrawal[3], Rajeev Kumar[3,4,*] and Raees Ahmad Khan[3]

[1]Department of Information Technology, College of Computers and Information Technology, Taif University, P. O. Box 11099, Taif 21944, Saudi Arabia
[2]Department of Computer Science, College of Computers and Information Technology, Taif University, P. O. Box 11099, Taif 21944, Saudi Arabia
[3]Department of Information Technology, Babasaheb Bhimrao Ambedkar University, Lucknow, 226025, India
[4]Department of Computer Application, Shri Ramswaroop Memorial University, Lucknow, 225003, India
*Corresponding Author: Rajeev Kumar. Email: rs0414@gmail.com

Received: 07 January 2021; Accepted: 07 February 2021

Abstract: Security risk evaluation of web-based healthcare applications is important from a design perspective. The developers as well as the users need to make sure that the applications must be secure. Citing the disastrous effects of unsecured web applications, *Accuntix Online* states that the IT industry has lost millions of dollars due to security theft and malware attacks. Protecting the integrity of patients' health data is of utmost importance. Thus, assessing the security risk of web-based healthcare applications should be accorded the highest priority while developing the web applications. To fulfill the security requirements, the developers must meticulously follow the Multi-Criteria Decision-Making (MCDM) methodology in the assortment of the most effective procedure for security assessment right from the developmental phase of the application. To address the security-related issues in web-based healthcare applications, we have followed the fuzzy-based integrated technique to assess the security risk of web-based healthcare applications. Further, the integrated technology is the combination of Analytic Hierarchy Process (F-AHP) and Technique for Order of Preference by Similarity to Ideal Solution (F-TOPSIS) techniques. The F-AHP approach gives the weights of the factors. We classified the risks into two-levels, Level one had the safety measures factors such as access control, integrity, confidentiality, and, authentication. We selected ten different web-based healthcare applications as alternatives. The calculations based on the proposed methodology ranked the *pattern system for access control* to be the most prioritized attribute. The outcomes of the study and the procedure used in this assessment would support future research and specialists' initiatives in organizing web applications through advanced supportable safety and security.

Keywords: Web-based healthcare application; fuzzy AHP; fuzzy TOPSIS; security risk; secure web design

1 Introduction

Security risk evaluation is a major concern for the Information Technology (IT) industry, specifically in the health care sector. The number of web application users has increased rapidly during the years 2012 to 2020. The security of web-based healthcare applications needs to be revised. India is ranked as one of the highest spam-sending nations on the planet [1,2]. It is shown by an analysis report that recent web based application have more loopholes than the previous ones. This means that the security of the applications is still a major problem in software development. The developers are unable to write secure code. Further, complexity is also a major concern for the developers in current scenario of designing. It is often shown that highly complex application structure has some serious fundamental issues due to its ambiguous nature. Internet of Things (IoT) devices are a significant target of malware attacks and, email spam is the common way to spread malware [3].

The external network connection makes the UK, US, and China more vulnerable [4]. 20% of the files are not protected according to the survey [5]. In the US alone, 43% of the IT industry is a victim of cyber-attacks and the resulting losses are estimated to be 214 million dollars [6]. Preventing the breach and data hijacking in any type of web based healthcare application requires industry's best practices and approaches of security [7]. However, these steps alone would not be effective enough in securing the web-based healthcare applications. We have to evaluate the design steps of web-based healthcare applications quantitatively from a design perspective to ensure optimum levels of security.

Managing the risk of security in web based healthcare application development is an important process and has a high sensitivity. Besides, every electronic device in healthcare environment has some risk associated with its security. However, these security risks can be minimized or mitigated through planned risk assessment procedures [5]. Furthermore, according to [6], security risk can be categorized into four aspects from a design perspective. On the other hand, a study classifies its security measure in terms of size for web-based healthcare applications [7]. Their definition depends on the number of lines of code in terms of the task and the number of designers involved in the process. Hence, from the perspective of achieving optimal security in the organizations, this examination proposes a consolidated F-AHP-TOPSIS methodology to ascertain the heaviness of each risk model and sub-foundation. A secure web-based healthcare application allows the patients' data to be stored as records and enables easy accessibility of data. Moreover, a secure web-based healthcare application also highlights the theft and misplacement of data.

Our quantitative research evaluation will essentially concentrate on the risk evaluation level for web-based healthcare applications. Further, the principal target of this survey is to give specialists a conclusive and systematic approach for estimating the present degree of risk evaluation.

2 Security Risk of Web-Based Healthcare Application Design

Healthcare web applications are improving the function of health services. The security and processing of patients' data is the primary concern of our research. The upsurge in the instances of healthcare data thefts poses a grave danger to the patients' health and can have fatal consequences. Security risk issues have been rising in different countries across the world. Norway and the USA report 4000 cases of ransomware per day; the spike in the cases in 2018 was estimated to be nearly 300% more than in 2017 [8]. This is creating stress worldwide. The use of smartphones, particularly in the healthcare sector, has empowered the patients as well as the doctors. Healthcare specialists use smartphones for maintaining records, process over the network, for diagnosis and medical prescription. Healthcare web-based applications or software on mobile have reported data breaches because of security measures adopted by the developers. We need to focus on the security of the web-based application. In the present study, we have formulated security at two different levels; level one has four factors F1, F2, F3 and, F4. Further, it can be classified as presented in Fig. 1 and Tab. 1.

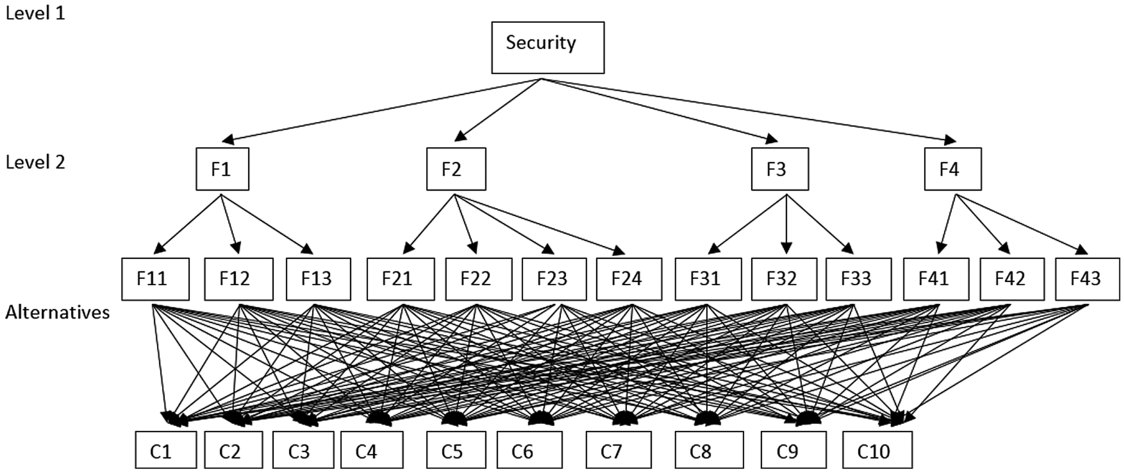

Figure 1: A structure of tree for security risks

Table 1: Security risk of web-based healthcare application factors in the design phase

	Sub-Factors	Definitions
Security Risk	Access Control [F1]	Access to Critical Private Variable via Public Method (ACPVPM) [F11] [9]
		Password in Configuration File (PCF) [F12] [10]
		A Pattern System for Access Control (APSAC) [F13] [11]
	Integrity [F2]	External Initialization of Trusted Variables or Data Stores (EITVDS) [F21] [12]
		Improperly Controlled Modification of Dynamically-determined Object Attributes (ICMDOA) [F22] [13]
		The download of Code Without Integrity Check Concurrent Execution (DCWICCE) [F23] [14]
		Shared Resource with Improper Synchronization (SRIS) [F24] [15]
	Confidentiality [F3]	Critical Variable Declared Public (CVDP) [F31] [16]
		Untrusted Search Path (USP) [F32] [5]
		Security Patterns for Web Application Development (SPWAD) [F33] [7]
	Authentication [F4]	Password in Configuration File (PCF) [F41] [8]
		Unverified Password Change (UPC) [F42] [2]
		Missing Authentication for Critical Function (MACF) [F43] [2]

The factors F1, F2 and, F3 have three different sections, F2 has four different subsections. Further, all the sub-factors are connected to ten different alternatives (web application used in a different hospital).

2.1 Factors

2.1.1 Access Control [F1]

This is the primary and important step of application on the device. Users access the application by the systematic approach of authentication, authorization, and, accountability. When the user accesses the data, authentication is checked and the location will be verified by the device.

ACPVPM [F11] - In this context, the attacker tries to modify the used variable which contains unpredicted principles. This can interrupt the further fragments of the code. Additionally, if an attacker reads the private variable, it may open up the private information, thus making it convenient for the attacker to invade further.

PCF [F12] - If the password stored in the system is accessed by the intruder, then the hacker can easily gain access to the system and pilfer the data.

APSAC [F13] - Software pattern, encapsulated in software design, explains the pattern of model to access the authorization in software or web-based application.

2.1.2 Integrity [F2]

It ensures the authenticity of the information by verifying if the source of information is genuine.

EITVDS [F21], the healthcare-based web application is hesitant to trust variables that must be initialized outside of its trust limit by the user. If the attackers are able to initialize the variables, they can do what they want with the system.

ICMDOA [F22], the object contains attributes intended for internal use. Undesirable changes cause vulnerability. The software receives input upgradation but does not have proper control over modification in attributes.

DCWICCE [F23], the hacker can execute the malicious code without checking its integrity.

Concurrent execution using SRIS [F24], the program can run with other code and, code sequence require provisional, elite access to a shared resource, but a scheduling space can alter the shared resource by alternative code arrangement that is functioning simultaneously.

2.1.3 Confidentiality [F3]

It is the set of rules which protect the information from unauthorized access. Information of the healthcare sector is sensitive and needs to be protected. Attackers can steal passwords and control network traffic. All the breaches are not intentional; some can be accidental like sending the mail to the wrong recipient, share private files in the public domain, etc. We have classified the confidentiality in its sub-factors in level 2.

CVDP [F31], web application and software define a critical field, variable to be public when security procedure is required to be private. The problem of security risks is involved in the software or web application (software development life cycle) effectively, thus affecting security by making it more difficult. It makes it easier to introduce vulnerabilities.

USP [F32], a healthcare-based application examines typical resources that are used as an external supply by the search path. This search path cannot be controlled by the application. This makes the attacker execute the malicious program and also access the authentication to modify the path of the application.

SPWAD [F33], the security patterns are the bridge between the developers and security experts. Security patterns capture security expertise for the problem. These patterns capture the strength and weaknesses of web applications and software.

2.1.4 Authentication [F4]

It is defined as the set of rules by which the authorization of access is granted. Authentication has two different levels that maintain the security risk to the web application used in the healthcare sector.

PCF [F41], web application, and healthcare software save the PIN in a configuration file that might be reachable by the attacker. The attackers use the password and make the system useless.

UPC [F42], refers to the setting a new password for the user, the change compromises the authentication of the system.

MACF [F43], web application and software do not execute any verification concerning functionality that needs verifiable operator characteristics or ingests a major quantity of resources. This makes the web application insecure. The cycle of the design process of web applications and software reduces the risk. Further, the factors of healthcare web applications are defined in Section 3.

2.2 Alternatives

The different alternatives (*C1 to C10) are- MediXcel EMR (C1), Trio HIS (C2), Caresoft HIS (C3), GeniPulse (C4), LiveHealth For diagnostic (C5), Visual Hospital Management (C6), eHospital (C7), Medisteer (C8), HospiLogix (C9) and NextGen (C10*). These are the various hospital management web-based applications that we are using as alternatives.

Security factors and their respective alternatives are presented in Fig. 1. The factor levels of security are classified into two-levels which maintain the cycle of calculation and achieve the desirable goal of quantitatively calculating the impact of security risk in healthcare applications. Level 1 has four factors and level two has different factors associated with level 1.

3 Unified F-AHP-TOPSIS Technique

To estimate the risk ratio in web applications of healthcare services, the authors classified and categorized various factors related to security and then evaluated these factors by a well-established fuzzy-based multi-criteria decision-making approach named, fuzzy Analytical Hierarchy Process (AHP). Further, to evaluate the risk ratio of the healthcare web applications, the adopted methodology was used to determine the weights for estimating the risk effectiveness for healthcare web applications and test the adopted results on various selected healthcare application projects as alternatives. Testing of results on various selected projects as alternatives is implemented by another similar approach called fuzzy TOPSIS. The fuzzy TOPSIS approach gives an ability to the examiner for estimating the effect of extracted results from fuzzy AHP methodology by various equations and numerical calculation.

Securing the data and maintaining risk on healthcare web applications is a problem that needs a quick and decision-based solution. Therefore, for managing this type of context, the authors and experts strongly believe that adopted fuzzy AHP-TOPSIS methodology is perfectly appropriate. There are various previous pieces of literature available that portray the significance and usefulness of results extracted from fuzzy AHP methodology. Moreover, it is also evidently drawn by experts that there are some obstacles and implications present in this evaluation methodology. Thus to tackle these implications and obstacles, authors added another effective similar approach, i.e., the fuzzy TOPSIS that gives a complementary advantage to the fuzzy AHP and its results.

Further, as a procedure to evaluate the factor's impact on healthcare web applications, the fuzzy AHP methodology was used to create a systematic tree-like model of various selected factors. Thereafter the numerical equations were applied on these factors. As a second initial step in the evaluation, the examiners converted the original weights of the factors given by experts into the triangular fuzzy set number (TFN). It is also often shown and proven that TFN values for every factor stepped in between 0 and 1 [8,9]. Moreover, to understand the adopted methodology more descriptively, the following headings are discussed:

Step 1: As an initial first step, after the creation of a successful tree model, the examiners developed a function named membership by applying the following Eqs. (1) and (2).

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

$$\mu_a(x) = \{\frac{x}{mi-l} - \frac{l}{mi-l} x \in [l, mi] \frac{x}{mi-u} - \frac{u}{mi-u} x \in [mi, u] \tag{2}$$

Here, various symbols represent various units like limit 1 denotes the upper limit, *mi* represents middle and *ui* portrays lower one.

Step 2: Now as the next step in evaluation, the examiners create the TFN numbers for factors by applying the following formulas.

For estimating the triangular numbers it is important to understand the representation mechanism as Now, the original conversation for TFN [9] is performed by Eq. (3)–(6).

$$\Phi_{ij} = \; \left(l_{ij},\; mi_{ij},\; u_{ij}\right) \tag{3}$$

$$where\ l_{ij} \leq mi_{ij} \leq u_{ij}$$

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

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

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

J_{ijd} in the above formulas represent a choice of experts that is denoted by i and j. Moreover, *d* represents the geometric mean value in the formula that is calculated by the examiners for estimating the difference between two specific factors. After calculating the GM value, Eqs. (7)–(9) described the formulas for operating the calculated GM value.

$$P + Q \;=\; (l_1 + l_2,\; mi_1 + mi_2,\; u_2 + u_2) \tag{7}$$

$$P \times Q \;=\; (l_1 \times l_2,\; mi_1 \times mi_2,\; u_1 \times u_2) \tag{8}$$

$$P^{-1} = \left(\frac{1}{u_1}, \frac{1}{mi_1}, \frac{1}{l_1}\right) \tag{9}$$

Step 3: The following Eq. (10) is used for evaluation:

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

Where $\widetilde{k^k_{ij}}$ portrays the choices of experts. In case of several experts and for representing their opinions for evaluation, the examiners apply the following Eq. (11).

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

Step 4: Further, it's time to develop a choice-based matrix by applying the following Eq. (12).

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

Step 5: The following Eq. (13) is used for calculating GM and then Eq. (14) gives an evaluation step for specific weights in tree-based model.

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

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

Step 6: Now after identifying the specific weights for every factor, the examiners apply Eqs. (15) and (16) to normalize the values.

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

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

Step 7: For estimating the best factor and ranking list of selected attributes, the following Eq. (17) is applied.

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

This concludes the evaluations done by using the fuzzy AHP methodology. After identifying the ranking list and the weights of the factors, the examiners apply another similar MCDM approach called fuzzy TOPSIS to respectively test the evaluated results. TOPSIS is a methodology that produces a testing plot in the numeric manner which is the same as real-world testing [10–12]. TOPSIS method is a perfect technique for estimating the quality and efficiency of extracted results from fuzzy AHP. To conduct the evaluation steps, the method adopts some applications related to the field of hierarchy and then uses them as an alternative in the calculation process. A brief description of the method is displayed in the following headings:

Step 1: As the first step in evaluation, the examiners assign weights for specific factors to the specific alternatives that are selected by authors.

Step 2: Develop a matrix by applying Eq. (18).

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

Here, $\tilde{x}_{ij} = \frac{1}{D}\left(\tilde{x}_{ij}^{1} \cdots \oplus \tilde{x}_{ij}^{d} \oplus \cdots \tilde{x}_{ij}^{D}\right)$, $\tilde{x}_{ij}^{d}-$ performance ranking of the alternative A_i concerning the factor C_J is estimated by the d^{th} practitioner or developer $\widetilde{x}_{ij}^{d} = (l_{ij}^{d}, mi_{ij}^{d},\ u_{ij}^{d})$.

Step 3: Further, after creating a systematic matrix from Eq. (18), the examiners need to normalize the values identified in the previous step and represented as in the following Eqs. (19) and (20).

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

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

Here, the value of j is considered between 1 and 0. Further, the process of normalization is frequently applied till the TFN values conversation.

Step 4: By applying the following Eq. (21), the examiner gets a numerical matrix for alternative evaluation.

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

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

As a notable point, it is often shown during the evaluation that normalized values represent TFN values that range from 0 and 1.

Step 5: To numerically quantify the +ve and –ve ideal solution value by applying Eqs. (22)–(25).

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

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

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

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

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

Step 6: In this concluding step of evaluation, the examiners apply the Eq. (26) to get the ideal gap degree of alternatives values. Calculation of coefficient gap degree needs to be evaluated for perfect alternative testing [13–16].

$$C\tilde{C}_{i} = \frac{\tilde{k}^{-}_{i}}{\tilde{k}^{+}_{i} + \tilde{k}^{-}_{i}} = 1 - \frac{\tilde{k}^{+}_{i}}{\tilde{k}^{+}_{i} + k^{-}_{i}}\ ,\ i = 1, 2, \ldots., m \tag{26}$$

where, $\frac{\tilde{k}^{-}_{i}}{\tilde{k}^{+}_{i} + \tilde{k}^{-}_{i}} -$ portray a degree of satisfaction for an alternative, and illustrates the degree of a gap for an alternative.

This abovementioned steps of the evaluation are essential for estimating the ranking and testing of the results. The next section of the paper describes the original numerical analysis of factors selected for the proposed study by applying the process discussed above.

4 Data Analysis and Results

Calculation of the security risk characteristics in the healthcare web application is a challenging job [10–13]. Estimating the quantitative impact of healthcare web application security is a critical process during building secure software or healthcare web application and to prevent the data phishing, vulnerability, and malicious attack from disintegration due to a security risk. From a healthcare perspective, security risk assessment gives successful importance to the characteristics of security as well as alternatives during the development process [14–16]. In this row, the authors of the paper opted for a fuzzy-based combined computational technique based on AHP and TOPSIS for evaluating more accurate results.

For the evaluation of the factors, we used Eqs. (1)–(9) and the scale of a triangular fuzzy number [10]. After using the TFN scale and calculating the values with the help of Eqs. (1)–(9), the authors constructed the pair-wise comparison matrix that is represented in Tab. 2 for level 1 characteristics of security risk. For level 2 each factor is connected to the respective sub factors mentioned in Fig. 1. The individual connection factors are represented by Tabs. 3 to 6. Further, the authors defuzzified the TFN values through Eqs. (7)–(11) and the results are represented in Tabs. 7 to 11. Each factor is represented by the matrix of three variables. Level 2 has F1, F3, F4 which further have 3 sub-factors and F2 has four sub-factors; the pair-wise comparison matrix is evaluated by the Eqs. (12)–(17). Thereafter, the quantitative evaluation of the weights of attributes is done; this has been shown in Tab. 12. Further, with the help of Eqs. (18)–(26), calculated subjective values in numerical form, weighted normalized fuzzy decision matrix and closeness coefficient of the different alternatives are shown in Tabs. 13 to 15, respectively.

Table 2: Aggregated fuzzy-based pairwise judgment matrix at level 1

	F1	F2	F3	F4
F1	1.0000, 1.0000, 1.0000	1.7554, 2.3458, 3.0363	1.4854, 1.9575, 2.5263	1.1298, 1.5551, 1.9895
F2	–	1.0000, 1.0000, 1.0000	0.5700, 0.7860, 1.1600	0.5600, 0.7200, 0.9699
F3	–	–	1.0000, 1.0000, 1.0000	0.6286, 0.8175, 1.0756
F4	–	–	–	1.0000, 1.0000, 1.0000

Table 3: Aggregated fuzzy-based pairwise judgment matrix for F1 at level 2

	F11	F12	F13
F11	1.0000, 1.0000, 1.0000	0.2375, 0.2879, 0.3675	0.3421, 0.4477, 0.8247
F12	–	1.0000, 1.0000, 1.0000	0.6614, 1.1725, 1.6936
F13	–	–	1.0000, 1.0000, 1.0000

Table 4: Aggregated fuzzy-based pairwise judgment matrix for F2 at level 2

	F21	F22	F23	F24
F21	1.0000, 1.0000, 1.0000	0.6941, 0.8953, 1.1124	0.2345, 0.2878, 0.3641	0.7112, 0.9541, 1.3512
F22	–	1.0000, 1.0000, 1.0000	0.4931, 0.6423, 1.2414	0.2713, 0.3515, 0.5216
F23	–	–	1.0000, 1.0000, 1.0000	1.0854, 1.3297, 1.5582
F24	–	–	–	1.0000, 1.0000, 1.0000

Table 5: Aggregated fuzzy-based pairwise judgment matrix for F3 at level 2

	F31	F32	F33
F31	1.0000, 1.0000, 1.0000	0.6653, 1.1723, 1.6974	1.1576, 1.4472, 1.7043
F32	–	1.0000, 1.0000, 1.0000	1.0077, 1.5247, 1.9343
F33	–	–	1.0000, 1.0000, 1.0000

Table 6: Aggregated fuzzy-based pairwise judgment matrix for F4 at level 2

	F41	F42	F43
F41	1.0000, 1.0000, 1.0000	1.1978, 1.5883, 2.1564	0.4911, 0.6422, 1.0099
F42	–	1.0000, 1.0000, 1.0000	0.2241, 0.2956, 0.4279
F43	–	–	1.0000, 1.0000, 1.0000

Table 7: Local weight at level 1

	F1	F2	F3	F4	Weights
F1	1.00000	2.37230	1.98190	1.55640	0.39000
F2	0.42150	1.00000	0.82430	0.74470	0.17000
F3	0.50460	1.21320	1.00000	0.83090	0.20000
F4	0.64250	1.34280	1.20350	1.00000	0.24000
					CR = 0.00154

Table 8: Local weight at level 1 for F1

	F11	F12	F13	Weights
F11	1.00000	1.17300	0.49400	0.27490
F12	0.85250	1.00000	1.17200	0.32960
F13	2.02430	0.85320	1.00000	0.39550
				CR = 0.00245

Table 9: Local weight at level 1 for F2

	F21	F22	F23	F24	Weights
F21	1.00000	0.89200	1.17300	0.99400	0.24630
F22	1.12110	1.00000	0.69100	0.37200	0.18200
F23	0.85250	1.44720	1.00000	1.29800	0.27240
F24	1.00610	2.68820	0.77040	1.00000	0.29930
					CR = 0.00254

Table 10: Local weight at level 1 for F3

	F31	F32	F33	Weights
F31	1.00000	1.17200	1.36300	0.38430
F32	0.85330	1.00000	1.49100	0.35620
F33	0.73370	0.67070	1.00000	0.25950
				CR = 0.00250

Table 11: Local weight at level 1 for F4

	F41	F42	F43	Weights
F41	1.00000	1.63300	0.69100	0.31590
F42	0.61240	1.00000	0.30300	0.17310
F43	1.44720	3.30030	1.00000	0.51100
				CR = 0.00520

Table 12: Summary of the results

Factors of Level 1	Independent Weights	Factors of Level 2	Independent Weights	Global Weights	Percentages	Final Ranking
F1	0.39000	F11	0.27490	0.107211	10.7211 %	4
		F12	0.32960	0.128544	12.8544 %	2
		F13	0.39550	0.154245	15.4245 %	1
F2	0.17000	F21	0.24630	0.041871	4.18710 %	11
		F22	0.18200	0.030940	3.09400 %	13
		F23	0.27240	0.046308	4.63080 %	10
		F24	0.29930	0.050881	5.08810 %	9
F3	0.20000	F31	0.38430	0.076860	7.68600 %	5
		F32	0.35620	0.071240	7.12400 %	7
		F33	0.25950	0.051900	5.19000 %	8
F4	0.24000	F41	0.31590	0.075816	7.58160 %	6
		F42	0.17310	0.041544	4.15440 %	12
		F43	0.51100	0.122640	12.26400 %	3

Table 13: Subjective perception outcomes in numerical form

	C1	C2	C3	C4	C5	C6	C7	C8	C9	C10
F11	5.0000, 7.0000, 8.4500	5.7300, 7.7300, 9.0000	4.2700, 6.2700, 7.9100	1.6400, 3.5500, 5.5500	4.1800, 6.0900, 7.6400	3.5500, 5.5500, 7.2700	0.8200, 2.4500, 4.4500	1.6400, 3.5500, 5.5500	4.1800, 6.0900, 7.6400	2.8200, 4.8200, 6.6400
F12	5.1800, 7.1800, 8.6400	5.3600, 7.3600, 8.7300	5.3600, 7.3600, 8.7300	1.4500, 3.3600, 5.3006	5.0000, 7.0000, 8.4500	4.8200, 6.8200, 8.2700	1.0000, 2.6400, 4.6400	1.4500, 3.3600, 5.3006	5.0000, 7.0000, 8.4500	2.8200, 4.8200, 6.7300
F13	5.7300, 7.7300, 9.0900	5.3600, 7.3006, 8.7300	5.5500, 7.5500, 8.9100	1.6400, 3.5500, 5.5500	5.3600, 7.3600, 8.7300	4.0900, 6.0900, 7.7300	0.7300, 2.2700, 4.2700	1.6400, 3.5500, 5.5500	5.3600, 7.3600, 8.7300	2.0900, 3.9100, 5.8200

(Continued)

Table 13 (continued).

	C1	C2	C3	C4	C5	C6	C7	C8	C9	C10
F21	5.0000, 7.0000, 8.4500	5.7300, 7.7300, 9.0000	4.2700, 6.2700, 7.9100	1.1800, 3.0000, 5.0000	4.1800, 6.0900, 7.6400	3.5500, 5.5500, 7.2700	0.8200, 2.4500, 4.4500	1.1800, 3.0000, 5.0000	4.1800, 6.0900, 7.6400	2.8200, 4.8200, 6.6400
F22	5.1800, 7.1800, 8.6400	5.3600, 7.3600, 8.7300	5.3600, 7.3600, 8.7300	0.7300, 2.4500, 4.4500	5.0000, 7.0000, 8.4500	4.8200, 6.8200, 8.2700	1.0000, 2.6400, 4.6400	0.7300, 2.4500, 4.4500	5.0000, 7.0000, 8.4500	2.8200, 4.8200, 6.7300
F23	5.7300, 7.7300, 9.0900	5.3600, 7.3006, 8.7300	5.5500, 7.5500, 8.9100	0.6400, 2.2700, 4.2700	5.3600, 7.3600, 8.7300	4.0900, 6.0900, 7.7300	0.7300, 2.2700, 4.2700	0.6400, 2.2700, 4.2700	5.3600, 7.3600, 8.7300	2.0900, 3.9100, 5.8200
F24	4.2700, 6.2700, 8.0900	3.7300, 5.5500, 7.2700	4.4500, 6.4500, 8.1800	1.6400, 3.5500, 5.5500	3.5500, 5.5500, 7.3600	2.9100, 4.8200, 6.7300	2.8200, 4.8200, 6.7300	1.6400, 3.5500, 5.5500	3.5500, 5.5500, 7.3600	3.0900, 5.0000, 6.8200
F31	4.0900, 6.0900, 7.9100	2.3600, 4.2700, 6.2700	2.4500, 4.2700, 6.2700	1.3600, 3.3600, 5.3600	4.4500, 6.4500, 8.1800	2.5500, 4.4500, 6.4500	1.2000, 3.0000, 5.0000	1.3600, 3.3600, 5.3600	4.4500, 6.4500, 8.1800	2.4500, 4.4500, 6.4500
F32	5.1800, 7.1800, 8.9100	4.8200, 6.8200, 8.5500	4.6400, 6.6400, 8.5500	0.8200, 2.6400, 4.6400	4.4500, 6.4500, 8.2700	2.5500, 4.4500, 6.4500	1.0900, 2.8200, 4.8200	0.8200, 2.6400, 4.6400	4.4500, 6.4500, 8.2700	2.3600, 4.2700, 6.1800
F33	5.7300, 7.7300, 9.3600	5.5500, 7.5005, 9.2700	5.7300, 7.7300, 9.2700	1.6400, 3.5500, 5.5500	5.7300, 7.7300, 9.2700	3.5500, 5.5500, 7.2700	1.8200, 3.7300, 5.7300	1.6400, 3.5500, 5.5500	5.7300, 7.7300, 9.2700	3.1800, 5.1800, 7.1800
F41	5.7300, 7.7300, 9.2700	4.2700, 6.2700, 8.1800	4.0900, 6.0900, 8.0900	1.1800, 3.0000, 5.0000	5.1800, 7.1800, 8.8200	2.0900, 4.0900, 6.0900	1.7300, 3.5500, 5.5500	1.1800, 3.0000, 5.0000	5.1800, 7.1800, 8.8200	2.8200, 4.8200, 6.8200
F42	5.1800, 7.1800, 9.0000	4.2700, 6.2700, 8.0900	3.7300, 5.5500, 7.2700	2.8200, 4.8200, 6.7300	4.4500, 6.4500, 8.1800	3.0900, 5.0000, 6.8200	2.9100, 4.8200, 6.7300	2.8200, 4.8200, 6.7300	4.4500, 6.4500, 8.1800	3.5500, 5.5500, 7.3600
F43	6.2700, 8.2700, 9.4500	5.7300, 7.7300, 9.0000	5.3600, 7.3600, 8.7300	1.4500, 3.3600, 5.3600	6.2700, 8.2700, 9.4500	3.1800, 5.1800, 7.0000	1.6400, 3.3600, 5.3600	1.4500, 3.3600, 5.3600	6.2700, 8.2700, 9.4500	3.9100, 5.9100, 7.5500

Table 14: The weighted normalized fuzzy decision matrix

	C1	C2	C3	C4	C5	C6	C7	C8	C9	C10
F11	0.00300, 0.01100, 0.03600	0.00200, 0.00900, 0.03000	0.00200, 0.00900, 0.03000	0.00200, 0.01000, 0.03500	0.00300, 0.01100, 0.03600	0.00100, 0.00600, 0.01900	0.00200, 0.00600, 0.02000	0.00200, 0.00600, 0.02000	0.00100, 0.00500, 0.01900	0.00100, 0.00500, 0.01800
F12	0.00400, 0.01400, 0.04400	0.00300, 0.01200, 0.04100	0.00300, 0.01200, 0.04100	0.00500, 0.01600, 0.04800	0.00500, 0.01600, 0.04900	0.00200, 0.00800, 0.02700	0.00200, 0.00800, 0.02500	0.00200, 0.00800, 0.02500	0.00200, 0.00700, 0.02700	0.00200, 0.00700, 0.02500

Table 14 (continued).

	C1	C2	C3	C4	C5	C6	C7	C8	C9	C10
F13	0.00400, 0.01400, 0.04400	0.00300, 0.01200, 0.04200	0.00300, 0.01200, 0.04200	0.00200, 0.01000, 0.03700	0.00200, 0.00900, 0.03800	0.00100, 0.00500, 0.01800	0.00200, 0.00700, 0.02200	0.00200, 0.00700, 0.02200	0.00200, 0.00700, 0.02400	0.00100, 0.00500, 0.01800
F21	0.00100, 0.00600, 0.01900	0.00200, 0.00600, 0.02000	0.00200, 0.00600, 0.02000	0.00100, 0.00500, 0.01900	0.00100, 0.00500, 0.01800	0.00100, 0.00600, 0.01900	0.00200, 0.00600, 0.02000	0.00200, 0.00600, 0.02000	0.00100, 0.00500, 0.01900	0.00100, 0.00500, 0.01800
F22	0.00100, 0.00500, 0.01800	0.00000, 0.00200, 0.00900	0.00200, 0.00700, 0.02200	0.00200, 0.00700, 0.02400	0.00100, 0.00500, 0.01800	0.00200, 0.00800, 0.02700	0.00200, 0.00800, 0.02500	0.00200, 0.00800, 0.02500	0.00200, 0.00700, 0.02700	0.00200, 0.00700, 0.02500
F23	0.00400, 0.01400, 0.04400	0.00300, 0.01200, 0.04100	0.00300, 0.01200, 0.04100	0.00500, 0.01600, 0.04800	0.00500, 0.01600, 0.04900	0.00100, 0.00500, 0.01800	0.00200, 0.00700, 0.02200	0.00200, 0.00700, 0.02200	0.00200, 0.00700, 0.02400	0.00100, 0.00500, 0.01800
F24	0.00400, 0.01400, 0.04400	0.00300, 0.01200, 0.04200	0.00300, 0.01200, 0.04200	0.00200, 0.01000, 0.03700	0.00200, 0.00900, 0.03800	0.00100, 0.00500, 0.01800	0.00000, 0.00200, 0.00900	0.00200, 0.00700, 0.02200	0.00200, 0.00700, 0.02400	0.00100, 0.00500, 0.01800
F31	0.00100, 0.00600, 0.01900	0.00200, 0.00600, 0.02000	0.00200, 0.00600, 0.02000	0.00100, 0.00500, 0.01900	0.00100, 0.00500, 0.01800	0.00300, 0.01100, 0.03600	0.00200, 0.00900, 0.03400	0.00200, 0.00900, 0.03000	0.00200, 0.01000, 0.03500	0.00300, 0.01100, 0.03600
F32	0.00200, 0.00800, 0.02700	0.00200, 0.00800, 0.02500	0.00200, 0.00800, 0.02500	0.00200, 0.00700, 0.02700	0.00200, 0.00700, 0.02500	0.00100, 0.00500, 0.01800	0.00000, 0.00200, 0.00900	0.00200, 0.00700, 0.02200	0.00200, 0.00700, 0.02400	0.00100, 0.00500, 0.01800
F33	0.00100, 0.00500, 0.01800	0.00200, 0.00700, 0.02200	0.00200, 0.00700, 0.02200	0.00200, 0.00700, 0.02400	0.00100, 0.00500, 0.01800	0.00300, 0.01100, 0.03600	0.00200, 0.00900, 0.03400	0.00200, 0.00900, 0.03000	0.00200, 0.01000, 0.03500	0.00300, 0.01100, 0.03600
F41	0.00100, 0.00600, 0.01900	0.00200, 0.00600, 0.02000	0.00200, 0.00600, 0.02000	0.00100, 0.00500, 0.01900	0.00100, 0.00500, 0.01800	0.00500, 0.01600, 0.04900	0.00300, 0.01300, 0.04500	0.00300, 0.01200, 0.04100	0.00500, 0.01600, 0.04800	0.00500, 0.01600, 0.04900
F42	0.00200, 0.00800, 0.02700	0.00200, 0.00800, 0.02500	0.00200, 0.00800, 0.02500	0.00200, 0.00700, 0.02700	0.00200, 0.00700, 0.02500	0.00000, 0.00400, 0.01700	0.00200, 0.00800, 0.02500	0.00200, 0.00700, 0.02700	0.00200, 0.00700, 0.02500	0.00000, 0.00400, 0.01700
F43	0.00100, 0.00500, 0.01800	0.00200, 0.00700, 0.02200	0.00200, 0.00700, 0.02200	0.00200, 0.00700, 0.02400	0.00100, 0.00500, 0.01800	0.00000, 0.00200, 0.00900	0.00200, 0.00700, 0.02200	0.00200, 0.00700, 0.02400	0.00100, 0.00500, 0.01800	0.00000, 0.00200, 0.00900

Tab. 15 shows the final values of alternatives through F-AHP-TOPSIS. Further, when we use different methodologies, the outputs of the data are different. For the examination of the accuracy of the assessment through one method, the authors have used another method called classical AHP-TOPSIS (C-AHP-TOPSIS). With the help of two or more methods, we can verify the reliability and efficiency of the obtained results through the co-relation coefficient. After the assessment through C-AHP-TOPSIS, Tab. 16 shown the outcomes.

Tab. 16 shows the difference between outcomes of F-AHP-TOPSIS and C-AHP-TOPSIS. Besides, the outcomes are highly associated (Pearson correlation coefficient is 0.96918). Obtained results through decision-making techniques may be ambiguous; hence, sensitivity analyses should be performed to verify the validity of the outcomes. In this row, the authors of this paper also evaluated the sensitivity analyses as shown in Tab. 17.

Table 15: Closeness coefficient of the different alternatives

Alternatives	d+i	d-i	Gap Degree (CC+i)	Satisfaction Degree (CC-i)
C1	0.054675	0.036545	0.365474	0.625123
C2	0.064576	0.035474	0.524574	0.644336
C3	0.046457	0.054874	0.569857	0.444224
C4	0.045164	0.036544	0.256235	0.527112
C5	0.451245	0.054574	0.565685	0.467124
C6	0.045154	0.054525	0.612545	0.387741
C7	0.056457	0.036526	0.356256	0.647356
C8	0.045127	0.045245	0.575482	0.434745
C9	0.034657	0.021547	0.553568	0.454856
C10	0.045125	0.042541	0.612366	0.397223

Table 16: Compare the result of classical and F-AHP, F-TOPSIS methods

Methods/ Alternatives	C1	C2	C3	C4	C5	C6	C7	C8	C9	C10
F-AHP-TOPSIS	0.625123	0.644336	0.444224	0.527112	0.467124	0.387741	0.647356	0.434745	0.454856	0.397223
C-AHP-TOPSIS	0.614457	0.655457	0.445427	0.545124	0.452368	0.385474	0.645287	0.436548	0.463587	0.412545

Table 17: Sensitivity analysis

Experiments	Weights/ Alternatives		C1	C2	C3	C4	C5	C6	C7	C8	C9	C10
Experiment-0	Original Weights	Satisfaction Degree (CC-i)	0.625123	0.644336	0.444224	0.527112	0.467124	0.387741	0.647356	0.434745	0.454856	0.397223
Experiment-1	F11		0.664197	0.542459	0.489627	0.672848	0.493939	0.435764	0.600045	0.477181	0.493939	0.435764
Experiment-2	F12		0.719197	0.582959	0.529127	0.645848	0.534939	0.477764	0.710045	0.520180	0.534939	0.477764
Experiment-3	F13		0.544797	0.423659	0.391127	0.492048	0.385639	0.328064	0.558045	0.340482	0.385639	0.328064
Experiment-4	F21		0.580797	0.463059	0.424127	0.593448	0.418039	0.359764	0.540445	0.377980	0.418039	0.359764
Experiment-5	F22		0.549197	0.407759	0.396127	0.485148	0.383839	0.329164	0.555545	0.363680	0.383839	0.329164
Experiment-6	F23		0.581597	0.445259	0.427127	0.521148	0.417839	0.360764	0.591045	0.398178	0.417839	0.360764
Experiment-7	F24		0.549197	0.407759	0.396127	0.485148	0.383839	0.329164	0.555545	0.363680	0.383839	0.329164
Experiment-8	F31		0.549197	0.407759	0.396127	0.485148	0.383839	0.329164	0.555545	0.363680	0.383839	0.329164
Experiment-9	F32		0.659897	0.535459	0.499127	0.607148	0.497439	0.444464	0.676045	0.481679	0.497439	0.444464
Experiment-10	F33		0.581597	0.445259	0.427127	0.521148	0.417839	0.360764	0.591045	0.398178	0.417839	0.360764
Experiment-11	F41		0.549197	0.407759	0.396127	0.485148	0.383839	0.329164	0.555545	0.363680	0.383839	0.329164
Experiment-12	F42		0.543780	0.431460	0.383627	0.486348	0.382939	0.321764	0.560045	0.360180	0.382939	0.321764
Experiment-13	F43		0.647197	0.728959	0.540627	0.658148	0.543439	0.478164	0.726545	0.527681	0.543439	0.478164

5 Conclusion

The combined computational technique based on AHP and TOPSIS is the most conclusive approach for verifying the impact of the selected factors in the design of healthcare web application. *Integrity, access control, confidentiality, and authentication* are primary-level factors, and the secondary level factors have been described in Fig. 1 and Tab. 1 in detail. All are important factors for secure design of web-based healthcare applications. Security concerns associated with WBHMS, and protecting the privacy of the data from different malfunctions and attacks from the design perspective is a subject of imminent attention. The present research paper selected four significant factors of security risk, four primary and three dependent factors of F1, four dependent factors of F2, three dependent factors of F3 and, three dependent factors of F4 in the secondary level, which depend healthcare applications (alternatives) being used in different hospitals. Outcomes of security risk factors represent the momentous effect on the WBHMS in healthcare applications from a design perspective. According to our estimation which was done by using F- AHP, the *pattern system for access control in the access control* got the highest rank. *eHospital* got the top rank which was determined by using F-TOPSIS technique. Thereafter, we validated the combined computational technique based on AHP and TOPSIS to deliver the impactful ranking of the security risk factors and quantitative values of alternatives.

Acknowledgement: This research was supported by Taif University Researchers Supporting Project number (TURSP-2020/231), Taif University, Taif, Saudi Arabia.

Funding Statement: Funding for this study was received from the Taif University Researchers Supporting Projects at Taif University, Kingdom of Saudi Arabia under Grant No. TURSP-2020/231.

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, “Needs and importance of reliability prediction: An industrial perspective,” *Information Sciences Letters*, vol. 9, no. 1, pp. 33–37, 2020. DOI 10.18576/isl/090105.

[2] G. McGraw, “Software security,” *IEEE Security and Privacy*, vol. 2, no. 2, pp. 80–83, 2004. DOI 10.1109/MSECP.2004.1281254.

[3] K. Sahu and R. K. Srivastava, “Soft computing approach for prediction of software reliability,” *ICIC Express Letters*, vol. 12, no. 12, pp. 1213–1222, 2018.

[4] A. S. Sodiya, S. A. Onashoga and O. B. Ajayĩ, “Towards building secure software systems,” *Issues in Informing Science and Information Technology*, vol. 3, no. 12, pp. 35–42, 2006. DOI 10.28945/920.

[5] P. Shamala, R. Ahmad and M. Yusoff, “A conceptual framework of info structure for information security risk assessment,” *Journal of Information Security and Applications*, vol. 18, no. 1, pp. 45–52, 2013. DOI 10.1016/j.jisa.2013.07.002.

[6] Z. I. Saleh, H. Refai and A. Mashhour, “Proposed framework for security risk assessment,” *Journal of Information Security*, vol. 2, no. 2, pp. 85–90, 2011. DOI 10.4236/jis.2011.22008.

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

[8] M. C. Lee, “Information security risk analysis methods and research trends: AHP and fuzzy comprehensive method,” *International Journal of Computer Science and Information Technology*, vol. 6, no. 1, pp. 29–35, 2014.

[9] P. Shedden, R. Scheepers, W. Smith and A. Ahmad, “Incorporating a knowledge perspective into security risk assessments,” *ICIC Express Letters*, vol. 12, no. 14, pp. 4567–4573, 2011.

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

[11] P. Kocher, R. Lee, G. McGraw and A. Raghunathan, “Security as a new dimension in embedded system design,” in *Proc. of the 41st Annual Design Automation Conf.*, San Diego, CA, USA, pp. 753–760, 2004.

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

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

[14] P. T. Devanbu and S. Stubblebine, “Software engineering for security: A roadmap,” in *Proc. of the Conf. on the Future of Software Engineering*, Limerick, Ireland, pp. 227–239, 2000.

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

[16] D. M. Mehta, “Effective Software Security Management,” Technical Report: OWASP, 2007. [Online]. Available: https://www. owasp.org/images/2/28/Effective_Software_Security_Management.pdf.