

## Evaluating the Impacts of Security-Durability Characteristic: Data Science Perspective

Abdullah Alharbi<sup>1</sup>, Masood Ahmad<sup>2</sup>, Wael Alosaimi<sup>1</sup>, Hashem Alyami<sup>3</sup>, Alka Agrawal<sup>2</sup>,  
Rajeev Kumar<sup>4,\*</sup>, Abdul Wahid<sup>5</sup> and Raees Ahmad Khan<sup>2</sup>

<sup>1</sup>Department of Information Technology, College of Computers and Information Technology, Taif University, Taif, 21944, Saudi Arabia

<sup>2</sup>Department of Information Technology, Babasaheb Bhimrao Ambedkar University, Lucknow, 226025, India

<sup>3</sup>Department of Computer Science, College of Computers and Information Technology, Taif University, Taif, 21944, Saudi Arabia

<sup>4</sup>Department of Computer Applications, Shri Ramswaroop Memorial University, Barabanki, 225003, India

<sup>5</sup>Department of Computer Science and Information Technology, Maulana Azad National Urdu University, Hyderabad, 500032, India

\*Corresponding Author: Rajeev Kumar. Email: rs0414@gmail.com

Received: 10 June 2021; Accepted: 11 July 2021

**Abstract:** Since the beginning of web applications, security has been a critical study area. There has been a lot of research done to figure out how to define and identify security goals or issues. However, high-security web apps have been found to be less durable in recent years; thus reducing their business continuity. High security features of a web application are worthless unless they provide effective services to the user and meet the standards of commercial viability. Hence, there is a necessity to link in the gap between durability and security of the web application. Indeed, security mechanisms must be used to enhance durability as well as the security of the web application. Although durability and security are not related directly, some of their factors influence each other indirectly. Characteristics play an important role in reducing the void between durability and security. In this respect, the present study identifies key characteristics of security and durability that affect each other indirectly and directly, *including confidentiality, integrity availability, human trust and trustworthiness*. The importance of all the attributes in terms of their weight is essential for their influence on the whole security during the development procedure of web application. To estimate the efficacy of present study, authors employed the Hesitant Fuzzy Analytic Hierarchy Process (H-Fuzzy AHP). The outcomes of our investigations and conclusions will be a useful reference for the web application developers in achieving a more secure and durable web application.

**Keywords:** Software security; durability; durability of security services; web application development process

### 1 Introduction

Major quality factors including maintainability, durability, and security, etc., are always considered during web application development [1]. Nowadays, developers are facing durability related problem



This work is licensed under a Creative Commons Attribution 4.0 International License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

after delivering the web application to the end-users [2]. Due to high-security design, the web application is not as durable as it should be [3]. This is a problem that experts are attempting to solve. The durability of web application increases if the security aspects associated with are also durable [4]. Although, security refers to the prevention of unauthorized [5], durability ensures ‘the keeping it simple’ formula of the web application. Thus, the organization wants user-friendly security services of the web application to enhance revenue. There are some attributes of durable-security that affect the durability of security services including *Confidentiality, Integrity, and Availability* (CIA) which affect [6] human trust directly, and trustworthiness indirectly [1]. Hence the developers are trying to develop a high-security design with durable-security for improving the durability of web applications [2].

Security and durability have an inverse relation with each other because increasing durability decreases the security of web application. However, there are still some factors of durability which affect the security services positively including the human trust that affects security. Unfortunately, efforts have not been made to develop durable-security design during web application development. Importance of attributes plays a key role in developing durable-security design. Sufficient research work has been done in the field of prioritizing durability attributes and security attributes [3]. Nevertheless no attempt has been reported in the literature for prioritizing durable-security attributes to improve the uses of security services yet. The user’s adoption of security technology is critical [7], and long-term security services are the user's major need [5].

The analysis of identifying and prioritizing the durable-security factors is a very critical task. Further, evaluation of durable-security attributes is important for both the security services and the whole web application. In this league, the assessment of trustworthiness and its associated attributes is essential to confirm the whole web application security services. Conclusions of the estimation procedure may allow the experts to create suitable judgement as well as take suitable action. Though, to be capable to take suitable action, experts not only need to distinguish the durable-security characteristics that pay to security but also recognize the utmost durable characteristics among them. Hence, to address the relationship between these factors, a ladder of durable-security characteristics is distinct in the following segment and Hesitant Fuzzy AHP is employed for prioritization of different durable-security attributes. The results may help the security designers for developing durable-security services development procedure of web application. Rest of present research work is systematized as follows: Second section deliberates the importance of durable-security; the third section evaluates durable-security attributes. The fourth section prioritizes the identified attributes and deliberates the outcomes. The final conclusion is presented in section five.

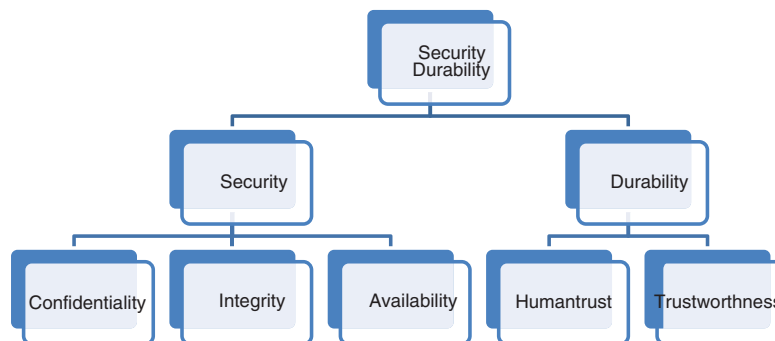
## 2 Security-Durability

Security of web application is an notion or technique that is implemented to prevent web application from malicious attacks [6]. According to G. McGraw, web application security is about building secure web applications, i.e., designing web application to be secure while educating the web application developers and architects and users about how to build secure web application [7]. Security has become a critical component during the web application development process due to the wide applicability of web applications. Indeed, web applications confront vulnerabilities from a variety of potential hostile adversaries that are always evolving, ranging from web-aware apps on PCs to complicated media communications. Assessing and maintaining the CIA during stages of web application development [6] has proved to be one of the best ways to get a more secure web application. That is why everyone is building a high-security design. However, such complex security design contains very less durability. Moreover, the complexity in design impedes the usability as the customers are not capable to practice the web applications simply and efficiently. In this context, the IEEE standard describes durability as the *degree of ease of use* by which the user can achieve the preferred outcomes without creating numerous

determinations [8]. Discussing to Jakob Nielsen, durability is a quality characteristic that depends on components containing human-trust, and trustworthiness [9].

Good web application developers are also good security-durability managers. To maintain security-durability, the main objectives of developers are to identify, address, and resolve the security issues before they become threats to success. It makes good business sense for secure web application development to incorporate security-durability as part of security-durability management. Developers need to be aware of the nature of concerned security-durability during web application development because time and cost of the development processes are greatly affected by them. Thus, identification of security-durability issues and their factors to solve the issue of security-durability during development can assist the developers in taking initial steps and suitable actions against those issues. It has been observed that the assessment of security-durability with the help of MCDM techniques can improve the software security-durability.

Although, security and durability seem to be at odds, it has been observed that improving one - affects the other. Techniques to include security goals or issues have already been developed [1], however a significant part, i.e., security-durability/durable-security still needs to be addressed. Durability in security should be incorporated into durable-security from the start and maintained until the security services are operational. The International Standard Organisation (ISO) defines durability as the ability to provide specified services with ease of use to the user including human trust and trustworthiness in a specified context of use. According to this definition, durable-security focuses on human trust, and trustworthiness. Hence, security has three major factors of durability that indirectly affect trustworthiness. Further, the CIA is the pillar of security. These five characteristics play a significant character in improving the durable-security services of web application and are discussed in details here; the hierarchy of the durability-security is depicted in Fig. 1.



**Figure 1:** Security-durability attributes

### 2.1 Confidentiality

Confidentiality refers to the attempts taken by an agency to keep the data confidential or secret. In practice, to avoid unauthorized disclosure, it's about restricting access to data. This usually means ensuring that only those who are allowed/authorized can access the specific assets and that the access is actively denied to those who are unauthorized.

### 2.2 Integrity

The "I" in the CIA triad stands for is data integrity. This is an important component of the CIA triad and is intended to protect any unauthorized party from deletion or alteration of data, and guarantees that the harm can be reversed when an approved individual makes a change that should not have been done.

### 2.3 Availability

This is the CIA triad's final portion and refers to the data's actual availability. For the information they protect, authentication mechanisms, access channels and systems all have to function properly to ensure that it is available whenever needed.

The computing tools that have architectures expressly designed to enhance availability are high availability system. This can target hardware faults, updates or power failures based on the particular system to help boost availability, or it can handle multiple network connections to route around different network failures.

### 2.4 Trustworthiness

The web application possesses trustworthiness if it works as projected for a particular reason, when required, with different improvements that have been completed newly, and without unnecessary side exploitable vulnerabilities, effects, or habits. Trustworthiness ensures that the web application will work as planned. The trustworthiness characteristics [10] that impact the life cycle of security services depend, conferring to its meaning, on integrity, availability, and confidentiality.

### 2.5 Human Trust

Human trust is commonly designated as a delicate problem in which the trustworthy party has a moral obligation towards the trusting party. In web application terms, the trust of customers in web developers is known as human trust [10]. When using the web, the confidence of consumers depends on the web's security design and that the web will operate for the predictable duration and secure their data.

All these factors depend on each other's security characteristics depending on the durability characteristics and vice versa. When the life of web application increases, then the security of the web should also increase with time. If we will not improve the security of the web application with the life of web application, then the life of the application will be worthless.

## 3 Evaluation of Durability-Security Attributes

Although Analytic Hierarchy Process (AHP) is measured well in investigating a judgement in a collection, numerous investigators have found that fuzzy AHP is more valuable for providing more accurate conclusions along with their weights [6]. AHP is an important tool and is extensively employed and approved by experts to complete the priority investigation. In order to deal with the ambiguity and uncertainties of human decision, we have come out with a modified version of AHP acknowledged as Fuzzy AHP which includes fuzzy set theory with AHP procedure [7]. This work's contributions also includes the prioritization of durable-security attributes through Fuzzy AHP with the help of the inputs of professionals. It finds out the weight and ranks of attributes for durable-security services. In this work, the authors have taken five factors of durability-security including *confidentiality*, *integrity*, *availability*, *human-trust*, and *trustworthiness* as displayed in Fig. 1.

Fig. 1 shows that human-trust and trustworthiness are the factors of durability that also affect the security services, positively. Human-trust is the capability of the user to be able to make a specific operation [11] Trustworthiness is took by measuring the time to finish a task or the number of efforts completed to accomplish required goals [12]. As per the definitions of two factors of durability, it is clear that these factors affect the web application's security as well [13]. Henceforth these characteristics should be involved for estimating the durable-security. Durable-security may be improved through a focus on the CIA with human trust and trustworthiness together. Moreover, the contribution of each attribute in durable-security is calculated. Hence, this section discusses the prioritization of durable-security factors to enhance the durability of security services [14]. The durable-security characteristics have been acknowledged through a complete literature survey and experts' views. As discussed earlier, the authors

have proven that AHP is one of the paramount procedure methods in a small-scale MCDM problem, such as the one obtainable in this segment.

The nature of web application development is accompanied by implied uncertainties, which largely rely on the thinking process of a person during web application development about security management. A framework for security management has been proposed by Saleh et al. The research evaluated the security risks of software with the help of fuzzy numbers. For example, Ming-Chang Lee has used sets in security risk management. The hierarchical breakdown structure depiction of security risk was employed by Shedden et al. to shape a framework for qualitative security risk assessment.

The definition of fuzzy inference has also been employed by some experts to state the system of unpredictability and analytical hierarchy to establish structure and thus various rank factors included in the web development process. Some have used the clustered fuzzy decision-making procedure for risk evaluation, while others have used the security assessment of the fuzzy analytic hierarchy process.

The goal of this paper is to figure out what factors are most important in terms of long-term security. A questionnaire was created in order to create a list of the factors that were prioritised. As replies, a group of specialists in the fields of durability and security were approached. Because it can regulate fuzzy judgemental inputs from participants, Fuzzy AHP was chosen for evaluating the value of durable-security elements. It may also translate qualitative inputs into quantitative findings in the form of weight and ranking, which allows for a more accurate assessment of long-term security [15,16]. The questionnaire was also used to create a pair-wise comparison matrix for the Hesitant Fuzzy AHP approach.

#### 4 Methodology Followed

To solve and make the correct decisions, numerous real-world difficulties require MCDM explanations. This classification is included in the reliability characteristics' package. AHP is acknowledged to be well-organized in MCDM operations because it provides decision-makers with an effective solution. Normally, the pair-wise comparison matrix is used, and the system's precision is checked. These pair-wise comparisons are severely affected by the judgements of clinicians because several alternatives are available.

This study introduces an efficient approach consisting of hesitant fuzzy AHP to determine the decision requirements and choice the utmost appropriate feature to resolve the problem of choosing the suitable forecast technique for web application security-durability characteristics. Since it is hard to conclude the membership degree of characteristics, Torra [17] introduced hesitant fuzzy sets. This problem emerges from potential ideals; making it difficult for us to choose the right one. This research work also utilizes the reluctant fuzzy technique to take further precise studies. The steps of the hesitant fuzzy AHP, based on the AHP procedure of Buckley [18], are given as follows:

**Step 1:** Pair-wise comparison matrices for characteristics, sub-characteristics and alternatives are built and linguistics words are used to gather experts' assessments.

**Step 2:** Each fuzzy pair-wise matrix's consistency is tested. Pair-wise comparison to verify the accuracy of the fuzzy pair-wise comparison matrices, the grade means integration method [19] defuzzifies the value. Assume that  $\tilde{A} = [\tilde{a}_{ij}]$  is a reciprocal matrix of fuzzy positive and  $A=[a_{ij}]$  is its reciprocal matrix of defuzzified positive. If the outcome of the  $A= [a_{ij}]$  comparisons is consistent [14]. A TFN  $\tilde{A} = (l, m, u)$  can be translated into crisp number by using the equation below, according to the graded mean integration approach.

$$A = \frac{l + 4m + u}{6} \quad (1)$$

If the pair-wise comparisons are not accurate, the pair-wise comparison must be revised by experts.

**Step 3:** Conflict recognition and renewal of the tests. The expert's judgments are tested for their closeness with one another. If the assessments are not closer, then the professionals are recommended to deliberate the state and reintroduce their assessments.

**Step 4:** Fuzzy envelop procedure introduced by Liu and Rodriguez [20] is employed to integrate the experts' assessments. For conversion assessments, the third step is to use fuzzy wrappers. Assume that L0 is the lowest distinction and Lg is the uppermost linguistic scale importance, and the measurements are between Li and Lj such that  $L0 \leq Li \leq Lj \leq Lg$ ; symbol ordered constraint n weighted averaging (OrWA) [21] as shown in Eq. (2).

$$OrWA(A_1, A_2, \dots A_n) = \sum_{j=1}^n W_j B_j \tag{2}$$

Here,  $W=(w_1, w_2, \dots, w_n)$  is the related balancing vector that fulfils the law of  $\sum_{i=1}^n W_i = 1$  and  $B_j$  is relevant to the theory of  $A_1, A_2, \dots, A_n$ . The fuzzy constraints of the trapezoidal numbers  $c = (A, B, C, D)$  after this measure, as in Eqs. (3)–(6).

$$A = \min\{A_L^i, A_M^i, A_M^{i+1}, \dots, A_M^j, A_R^j\} = A_L^i \tag{3}$$

$$D = \max\{A_L^i, A_M^i, A_M^{i+1}, \dots, A_M^j, A_R^j\} = A_R^j \tag{4}$$

$$B = \left\{ \begin{array}{l} A_M^i, \text{ if } i + 1 = j \\ OrWA_w \left( A_m^i, \dots, A_m^j \right), \text{ if } i+j \text{ is even} \\ OrWA_w \left( A_m^i, \dots, A_m^{\frac{i+j+1}{2}} \right), \text{ if } i+j \text{ is odd} \end{array} \right\} \tag{5}$$

$$C = \left\{ \begin{array}{l} A_M^{i+1}, \text{ if } i + 1 = j \\ OrWA_w \left( A_m^i, A_m^{i-1}, \dots, A_m^{\frac{i+j}{2}} \right), \text{ if } i+j \text{ is even} \\ OrWA_w \left( A_m^i, A_m^{i-1}, \dots, A_m^{\frac{i+j+1}{2}} \right), \text{ if } i+j \text{ is odd} \end{array} \right\} \tag{6}$$

The phase continues to use  $\mu$  to classify the first and second types of weights (which is a number found in the unit interval [0,1]) by means of Eqs. (7) and (8) separately, weights of the first kind ( $W_1 = (w_1^1, w_2^1, \dots, w_n^1)$ ):

$$w_1^1 = \mu_2, \quad w_2^1 = \mu_2(1 - \mu_2), \dots, w_n^1 \mu_2(1 - \mu_2)^{n-2} \tag{7}$$

Second type weights ( $W_2 = (w_1^2, w_2^2, \dots, w_n^2)$ ):

$$w_1^2 = \mu_1^{n-1}, \quad w_2^2 = (1 - \mu_1)\mu_1^{n-1} \tag{8}$$

Once again, with the assistance of equation  $\mu_1 = (r - (j - 1))/(r - 1)$  s, and  $\mu_2 = (r - (j - 1))/(r - 1)$  where  $r$  is the number of the highest rank in evaluations (where  $r$  is equal to 10), and  $i$  and  $j$  are correspondingly the ranks of the lowest and highest evaluations.

**Step 5:** The second step is to finish the pair-wise matrix of comparison (a) as in Eqs. (9) and (10).

$$w_1^2 = \mu_1^{n-1}, \quad w_2^2 = (1 - \mu_1)\mu_1^{n-1} \tag{9}$$

Since TFNs are the fuzzy envelops obtained in the previous steps, reciprocal principles are deliberated as follows:



$$\tilde{c}_{ji} = \left( \frac{1}{c_{ij_u}}, \frac{1}{c_{ij_{m2}}}, \frac{1}{c_{ij_{m1}}}, \frac{1}{c_{ij_1}} \right) \tag{10}$$

**Step 6:** By using Eq. (11), defuzzification procedure of a trapezoidal fuzzy number as  $d = (l, m_1, m_2, h)$  is completed, which distributes a crisp number

$$\eta_x = \frac{l + 2m_1 + 2m_2}{6} \tag{11}$$

Calculate the standard Consistency Ratio (CR) by using Eqs. (12) and (13).

$$CI = \frac{\lambda_{max} - n}{n - 1} \tag{12}$$

$$CR = \frac{CI}{RI} \tag{13}$$

Within Eq. (12) the consistency index is the CI,  $\lambda_{max}$  is the largest matrix variable,  $n$  is the number of parameters in the present estimation, and RI is the arbitrarily considered ready-to-use index (the random index) that differs for  $n$  values that have been altered. If the value of CR is lower than 0.1, the idea here is to continue with calculations otherwise go to phase 2 and start over the calculation.

**Step 7:** To estimate the geometric mean for each row of the pair-wise matrix by using Eq. (14).

$$\tilde{g}_i = (\tilde{c}_{i1} \otimes \tilde{c}_{i2} \dots \otimes \tilde{c}_{in})^{\frac{1}{n}} \tag{14}$$

**Step 8:**  $\tilde{w}_i$  is the fuzzy weight of each characteristic is estimated with the help of  $(\tilde{g}_i)$  values by Eq. (15).

$$\tilde{w}_i = \tilde{g}_i \otimes (\tilde{g}_1 \otimes \tilde{g}_2 \dots \tilde{g}_n)^{-1} \tag{15}$$

In this analysis,  $\tilde{g}_1 \otimes (\tilde{g}_1 \otimes \tilde{g}_2 \dots \tilde{g}_n)^{-1}$  value is accepted as the maximum parameter of the completely high importance in Tab. 2.

**Step 9:** In order to evaluate the significance ranking of the alternatives, trapezoidal fuzzy numbers are defuzzified. Using Eq. (16) defuzzification of the TFN is calculated.

$$\eta_x = \frac{l + 2m_1 + 2m_2 + h}{6} \tag{16}$$

**Step 10:** Normalize weights are estimated from defuzzified weights using the help of Eq. (17).

$$\frac{\tilde{w}_i}{\sum_i \sum_j \tilde{w}_j} \tag{17}$$

**Steps 11:** Alternatives are rated by defuzzified values and the best score alternative is chosen.

### 5 Numerical Assessment and Results

The authors measured the findings from Eqs. (1)–(12) the prediction model for Level 1 and Level 2 shows in Fig. 1 is as follows:

The fuzzy envelope (US12) was called “B/W VHI and ESHI”. The Triangular Fuzzy Numbers (TFN) associated with the defined linguistic values are (3.0, 5.0, 7.0) and (5.0, 7.0, 9.0). From Eqs. (1)–(12), the trapezoidal fuzzy numbers = (a, b, c, d) signifying the linguistic significance are determined.

In the end, the fuzzy trapezoidal set of this envelope was found to be (3.0, 5.0, 7.0, 9.0). Out of Eqs. (13) and (14), the measurement of the fuzzy weights of the models and the weight of the model can be assessed by

means of Eq. (14). The Eq. (15) is estimated by the defuzzified value of the respective model. Subsequently, normalise the weights by Eq. (16). The computed results of the level 1 durability-security prediction models are presented in Tab. 1. For checking fuzzy local weights, as shown in Tab. 1, the same method is used at level 2 for web application durability-security prediction models. As shown in Tab. 2, local or dependent weights of prediction models have been evaluated. Tabs. 1 and 2 with the aid of local weights or free weights of level 2 prediction models.

**Table 1:** Fuzzy pair-wise comparison matrix based on collection experts' judgment

	M1	M2	M3	M4	M5
M1	1.00000, 1.00000, 1.00000, 1.00000	0.03310, 0.12901, 0.21201, 0.78101	0.01094, 0.03252, 0.08040, 0.28610	0.01791, 0.04916, 0.12520, 0.54570	0.00300, 0.01570, 0.03627, 0.21730
M2	0.05210, 0.15910, 0.21970, 1.02510	1.00000, 1.00000	0.01791, 0.04916, 0.12520, 0.54570	0.00300, 0.01570, 0.03627, 0.21730	0.00300, 0.01570, 0.03627, 0.21730
M3	0.00482, 0.01940, 0.05081, 0.28520	0.01094, 0.03252, 0.08040, 0.28610	1.00000, 1.00000	0.03113, 0.12190, 0.21120, 0.78111	0.00300, 0.01570, 0.03627, 0.21730
M4	0.06140, 0.24010, 0.42160, 1.21410	0.01094, 0.03252, 0.08040, 0.28610	0.00593, 0.02930, 0.07280, 0.33780	1.00000, 1.00000	0.03130, 0.12910, 0.21210, 0.78101
M5	0.00200, 0.00890, 0.01933, 0.13990	0.00593, 0.02930, 0.07280, 0.33780	0.01791, 0.04916, 0.12520, 0.54570	0.00593, 0.02930, 0.07280, 0.33780	1.00000, 1.00000, 1.00000, 1.00000

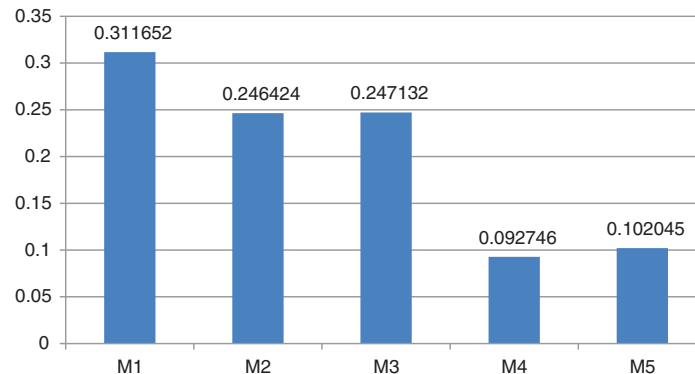
**Table 2:** Weight and priority of attributes

Models	Weights at level 2	Defuzzified weights	Normalized weights	Final rank
M1	0.011957, 0.071940, 0.151650, 0.721380	0.32141	0.311652	1
M2	0.003100, 0.015710, 0.036217, 0.217130	0.25414	0.246424	3
M3	0.017191, 0.049116, 0.125210, 0.545701	0.25487	0.247132	2
M4	0.001482, 0.019140, 0.050181, 0.285210	0.09565	0.092746	5
M5	0.002100, 0.008910, 0.019313, 0.139910	0.10524	0.102045	4

Defuzzification is used after the comparison matrix is built to produce a quantifiable value based on the calculated TFN values. The defuzzification approach employed in this research work was developed from Eqs. (4)–(6), also known as the alpha cut technique. The set of all items in a fuzzy set is called the alpha cut. Any number between 0 and 1 is used as the alpha threshold value. Further, the alpha threshold value has been set to 0.5; the membership value is larger than or equal to the alpha threshold value, which is signified by with alpha cut technique, a fuzzy set can be described as a collection of crisp sets. Crisp sets, (ij) simply state whether or not a given element is a member of the set. The alpha cut approach is shown in Eqs. (4)–(6).



The combined outcome in terms of weight is tabulated in Tab. 2 and the ranks determined according to the obtained weights have been depicted in Fig. 2. The results - according to the ranking are: *Confidentiality* (0.311652), *Integrity* (0.247132), *Availability* (0.246424), *Human trust* (0.092746), and *trustworthiness* (0.102045). According to the weights and priority, *confidentiality* of the user holds the highest priority among these five characteristics. In actual scenario, there are numerous durable-security characteristics, in this research, only five attributes of durable-security that affect security have been identified as well as prioritized. For validation of the results, Hesitant Fuzzy AHP is used as another method.



**Figure 2:** Ranks of the attributes

## 6 Conclusion

The purpose of this research work is to prioritize durable-security attributes during development process. For this purpose, the model security characteristics and durability characteristics produces outcomes which are supportive for experts in providing the durable-security services of the web application. The different security models are helpful for generating quantitative values including object-oriented and service-oriented perspective but there is yet no such mechanism for measuring security-durability. The framework suggested here will help to estimate the durable-security of web application services. In our study, the M1 has obtained the highest rank to give the durable security web application among others. By evaluating the security of the web applications, the researchers can develop a more durable and secure web application that offers human trust and trustworthiness web application for protection against the internal and outsider attacks.

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

**Funding Statement:** This Project was funded by the Taif University Researchers Supporting Projects at Taif University, Kingdom of Saudi Arabia, under Grant Number: TURSP-2020/231.

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

## References

- [1] R. Kumar, S. A. Khan and R. A. Khan, "Durability challenges in software engineering," *CrossTalk*, vol. 42, no. 4, pp. 29–31, 2016.
- [2] R. S. Pressman, "Software engineering: A practitioner's approach," in *Palgrave Macmillan*, London, McGraw Hill Education, 2005.

- [3] R. Kumar, S. A. Khan, A. Agrawal and R. A. Khan, "Measuring the security attributes through fuzzy analytic hierarchy process: Durability perspective," *ICIC Express Letters*, vol. 12, no. 6, pp. 615–620, 2018.
- [4] M. Anwar, M. S. A. Malik and A. Siddiq, "Usability and security issues of the user interface design," *International Journal of Computer Science and Network Security*, vol. 18, no. 8, pp. 105–111, 2018.
- [5] O. Kulyk and M. Volkamer, "Usability is not enough: Lessons learned from human factors in security," *Research for Verifiability*, vol. 12, no. 6, pp. 66–67, 2018.
- [6] A. Abdullah, M. Ahmad, A. Attaallah, A. Agrawal, R. Kumar *et al.*, "A hybrid fuzzy-based multi-criteria framework for security assessment of medical device software," *International Journal of Intelligent Engineering & Systems*, vol. 13, no. 5, pp. 51–62, 2020.
- [7] A. Abdullah, A. Attaallah, M. Ahmad, A. Agrawal, R. Kumar *et al.*, "A fuzzy multi-objective covering-based security quantification model for mitigating risk of web based medical image processing system," *International Journal of Advanced Commuter Science and Applications*, vol. 11, no. 1, pp. 481–489, 2020.
- [8] B. Beckles, V. Welch and J. Basney, "Mechanisms for increasing the usability of grid security," *International Journal of Human Computer Studies*, vol. 63, no. 12, pp. 74–101, 2005.
- [9] H. Hoodat and H. Rashidi, "Classification and analysis of risks in software engineering," *World Academy of Science, Engineering and Technology*, vol. 56, no. 32, pp. 446–452, 2009.
- [10] 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.
- [11] N. S. Good and A. Kregelberg, "Usability and privacy: A study of kazaa P2P files sharing, human factors in computing systems," *ACM*, vol. 12, no.2, pp. 627–642, 2013.
- [12] J. H. Saltzer and M. D. Schroeder, "The protection of information in computer systems," *IEEE Access*, vol. 63, no.9, pp. 1278–1308, 1975.
- [13] G. McGraw, "Software assurance for security," *IEEE Computer*, vol. 32, no.4, pp. 103–105, 1999.
- [14] P. Shamla, 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.
- [15] S. Gemmiti, 'How to manage open source risks using black duck SCA', Software Integrity Blog: Synopsys, [Online]. Available: <https://www.synopsys.com/blogs/software-security/manage-open-source-black-duck/>, 2021.
- [16] 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. 251–263, 2019.
- [17] V. Torra, "On hesitant fuzzy sets," *International Journal of Intelligence System*, vol. 25, no.2, pp. 529–539, 2010.
- [18] B. Zhu and Z. Xu, "Analytic hierarchy process-hesitant group decision making," *European Journal of Operational Research*, vol. 239, no.2, pp. 794–801, 2014.
- [19] D. J. Yu, Y. Y. Wu and W. Zhou, "Generalized hesitant fuzzy Bonferroni mean and its application in multi-criteria decision making," *IEEE Transaction on Fuzzy System*, vol. 20, no. 2, pp. 109–119, 2012.
- [20] L. Liu and R. M. Rodriguez, "A fuzzy envelop for hesitant fuzzy linguistic term set and its application to multi criteria decision making," *Information Sciences*, vol. 258, no.2, pp. 220–238, 2014.
- [21] D. Filev and R. R. Yager, "On the issue of obtaining OWA operator weights," *Fuzzy Sets and Systems*, vol. 94, no. 2, pp. 157–169, 1998.

**Appendix A**

Symbols	Definition
(OrWA)	Ordered constraint n weighted averaging
$A = \min A(L)$	Lower bound
$A = \max A(L)$	Upper bound
$A = \frac{l+4m+u}{6}$	Crisp number computation
W1, W2	First and second type of weights
$\tilde{c}_{ji}$	Trapezoidal fuzzy number
CI, CR	Consistency index and ratio
$\tilde{g}_i$	Geo metric means
$\tilde{w}_i$	Fuzzy weights
$\eta_x$	Defuzzification trapezoidal fuzzy numbers