IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received February 13, 2020, accepted February 29, 2020, date of publication March 3, 2020, date of current version March 19, 2020.

*Digital Object Identifier 10.1109/ACCESS.2020.2978038*

# A Knowledge-Based Integrated System of Hesitant Fuzzy Set, AHP and TOPSIS for Evaluating Security-Durability of Web Applications

**RAJEEV KUMAR[1], ASIF IRSHAD KHAN[2], YOOSEF B. ABUSHARK[2], MD MOTTAHIR ALAM[3], ALKA AGRAWAL[1], AND RAEES AHMAD KHAN[1]**

[1]Department of Information Technology, Babasaheb Bhimrao Ambedkar University (A Central University), Lucknow 226025, India
[2]Computer Science Department, Faculty of Computing and Information Technology, King Abdulaziz University, Jeddah 21589, Saudi Arabia
[3]Department of Electrical and Computer Engineering, Faculty of Engineering, King Abdulaziz University, Jeddah 21589, Saudi Arabia

Corresponding author: Raees Ahmad Khan (khanraees@yahoo.com)

This work was supported by the Deanship of Scientific Research (DSR), King Abdulaziz University, Jeddah, Saudi Arabia.

**ABSTRACT** There has been a phenomenal increase in the use of web applications in every facet of human endeavor. From education, healthcare, banking, business to governance and so much more now depends on secure web applications. This accelerated growth in the use of web applications has led to increase in the complexity of security and hence the present day developers have to contribute more significantly towards meeting the users' requirements. However, the high security of web application is not yet efficacious enough because the durability of web application is not as much as it should be. In this context, it is important to consider that ensuring sustainability of security at the early stage of web application development process may reduce costs and rework entailed during the development of secure and durable web applications. Hence, there is a need to focus on increasing the life-span of a secure web application. Quantitative estimation of security-durability plays a significant role for improving the life-span of a secure web application. Thus, to optimize the security assurance effort for a specific life-span, this paper is aimed at estimating the security-durability of web application. For estimating security-durability, this paper uses a hybrid approach of Hesitant Fuzzy (HF) sets, Analytic Hierarchy Process (AHP) and Technique for Order of Preference by Similarity to Ideal Solution (TOPSIS) techniques. The effectiveness of the combined approach of HF-AHP-TOPSIS is tested for its accuracy in a web application for an academic institution, Babasaheb Bhimrao Ambedkar University in India. To check the sensitivity of outcomes, authors of the paper have taken altered forms of the University's web application. The result established contains the security-durability assessment. This work seeks to be an important contribution in enhancing the security-durability and would be beneficial for experts who are working in this domain.

**INDEX TERMS** Web application, security-durability, application development process, hesitant fuzzy, AHP, TOPSIS.

## I. INTRODUCTION

The all-pervasive use of web applications in the present digital generation has made them more vulnerable to attacks. The issues of security are increasing even more because of the absence of essential security attributes. The alarming news of the *Blur* data breach in January 2019 shocked the whole cyber security world [1]. A sensitive private file that contained the classified and private data like the users' names, e-mail addresses and its password suggestions of around 2.4 million availers of Blur was exposed. After this revelation, Albine, the corporation that manages the data, advised the anxious users to change their passwords. In another such episode, a renowned company *Dunkin' Donuts* faced a data breach on January 17, 2019, for another time in almost three months when hackers gained access to their customer's accounts

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

through credential stuffing attacks [2]. On April 17, 2019 private data of about 100 million *Just Dial* end users was found undefended on openly available servers [3]. These reports of data breach are alarm bells that signal for prompt solutions and organizations cannot wait for more instances to happen. Maintenance after these attacks costs more than its development cost. So organizations should prepare themselves for such attacks in advance. It is imperative for all security experts to concentrate more on mechanisms that afford both security and durability in the web applications.

Though significant efforts have been made to ensure security by the researchers and industry professionals, all the suggested steps are in the later stages of the development of a web application. This is one of the major flaws which render the web applications vulnerable and results in data breaches [3], [4]. The security estimation needs to be done at the initial stages of web application development. It is expected from developers to have a potentially operative method for an initial, punctual and precise assessment of security-durability throughout the web application development life cycle. At early stage of development life cycle, it is required to determine what is to be measured and establish the variables in making them adaptable and efficient, and build security-durability that works efficiently for longer services. It is trusted and well accepted that security-durability must be integrated in the web application from very early in the development life cycle and, that too, as soon as the development starts.

The web applications is neither hundred percent secure nor it can be [2]. There might be some identified security flaws present that were not fixed during its development due to time constraints or some other reason [4]. These flaws are to be looked at again, prioritized and fixed. Further, maintenance is an ongoing process and does not end until web application is completely out of use or taken over by a new web application. The time invested and the cost incurred in Security maintenance is very high, thus it is important to ensure the optimization of security [5]. Furthermore after developing a secure web application, it is even more imperative to ensure its longevity [4]. Hence, integrating security-durability during the initial phases of development of web application would prove to be cost-effective and lucrative for the organizations [4], [5]. Selecting one from a host of security-durability attributes depends on decision of experts from different academic and research fields. Thus, this leads to the problem of decision making. AHP is one of the most well-known decision aids which help to solve these decision making amorphous problems [6]. In the field of information technology, AHP has been applied for many purposes including information security, network security and computer security [6], [7].

The effects of the assessment may enable decision-makers to take reasonable judgments. Decision-makers must not only know the factors that help to make security durable, but must also identify the most justifiable and usable factors for taking the most knowledgeable decision. In this context, the contributors recommend a method of Hesitant Fuzzy (HF) analytic hierarchy process (AHP) in combination with Technique for Order of Preference by Similarity to Ideal Solution (TOPSIS) for assessing security-durability. The research team has tested the proposed methodology on an institutional website application in order to ensure the efficiency of this framework. The assessment of security-durability attributes with effective techniques is important to improve the quality of web application and its services [8].

In addition, the selection and assessment of security-durability web applications poses a decision-making problem [4]. In this research, the authors used a Hesitant-Fuzzy-based AHP-TOPSIS hybrid technique [9]. This hybrid technique helps to achieve optimal results. Several experts were able to evaluate consistent findings using Hesitant-Fuzzy-TOPSIS technology [7].However, specific guidelines have not yet been given for the quantitative assignment of qualitative weights of attributes. The technique Hesitant-Fuzzy-AHP helps decision-makers systemically weigh the attributes, thereby eliminating any uncertainties and ambiguities in the assessment. With the help of hesitant-fuzzy numbers and pair-wise comparisons, consistent weights of the factor are obtained. But, the Hesitant-Fuzzy-AHP method is inefficient because of the monotonous calculations and a huge number of pairs of comparisons for many alternatives. The authors therefore recommend that Hesitant Fuzzy AHP TOPSIS hybrid approach should be used to assess the impact of alternatives in a timely manner and without complicated estimates.

The structure of the paper is as follows: Firstly, the authors are using fuzzy with new approach of hesitant with analytic hierarchy process to evaluate weights of the factors. Through the support of these weights, the authors have categorized top noteworthy factors at each level to measure the life-span or durability of web application security. To measure the impacts of the security-durability through the hybrid methodology of hesitant fuzzy based AHP-TOPSIS, web applications of BBA University have been taken. Section 2 of this paper discusses about the work done on security, durability and Multi Criteria Decision Making (MCDM) approach. Section 3 describes about the needs and importance of security-durability. Section 4 defines the combined approach of HF-AHP-TOPSIS in details. With the help of HF-AHP-TOPSIS, security-durability of web application has been evaluated in section 5. Sensitivity analysis and comparison of the results have been evaluated in section 6 and 7. Finally, discussion and conclusion are given in section 8 and 9.

## II. RELATED WORK

There has been extensive work done in the context of the security of web application in the past. Despite all the efforts, web applications are still not secure enough. Over the years, the level of threats to web application has varied depending upon the many factors as the environment in which web application is used after development is not under con-

trol. The organizations spend lots of money in combating and solving security related challenges during web development. In addition, organizations want to enhance security to improve the working life of web apps. Security assurance of web applications is not an easy process for a longer life span [7]–[9]. It consists of some necessary steps to be taken by the developers while developing the web apps security in the early stages of Development Life Cycle. Further, hesitant fuzzy AHP and TOPSIS is one of the best techniques to solve the uncertainty problem of the choice of factors to enhance the security-durability of web applications.

Alka Agarwal et al., in 2019 presented an approach for security-durability estimation [4]. This paper assesses security-durability of software with its different factors and also uses fuzzy AHP to assessand gain the priorities for it. Results acknowledge that security-durability helps in enhancing the overall security of the system. Nathan Ensmenger in 2014 discusses about software durability [5]. The author states that software durability and its serviceability are the same things. Also, the author mentions that there is issue of longtime services and cost spent on this is more than the development. Further, the author discusses that working or durability of software decreases with the passing of time, hence for long-term software, durability plays a key role. The author also stated in this paper that longevity of software can be achieved by increasing the durability of software. J. J., Cusick in 2013 discussed durability in software for virtual toolbox [8]. The author defined durable ideas in software engineering in terms of concepts, methods, and approaches with the help of virtual toolbox. He has mentioned about the need and importance of maintaining the balance between durability and quality during the software development process. The author has addressed this issue with respect to durable software.

Chong, S., et al. in 2018 proposed a framework for vulnerability minimization [10]. Author in this work identified that the security issues are rising because of the vulnerability flaw in the design of software. Hence to improve the design of software, the author presented a framework which works on object-oriented design and resolves the issues of security which are encountered mostly due to vulnerable design. The framework presented here identifies the factors of object-oriented design flaws, analyzes it and proposes security metrics. This security metric is helpful in the development of secure software. The thorough literature review of the above research points to the fact that security is a major concern in every area these days. It also strengthens the fact that design plays a noteworthy part in promising the security of software. Complexity of design and factors such as confidentiality, integrity and availability play a foremost role in software security assurance.

A kın Özda o lu et al. in 2017 presented a work in which he mentioned that AHP is best suited for decision making problems [11]. In this research, the author compares the methods of AHP by using a case study. The case study adopted here was about selecting employee for shop floor of manufacturing platform applied in a company from food industry. In order to avoid the hazards on enactment, the AHP, a fuzzy extension of AHP, was developed to solve the hierarchical fuzzy problems. According to the research, AHP is best suited for the decision making in the applications where data is to be retrieved in linguistic values. Fuzzy logic method is capable of handling ambiguousness in the linguistic data and best suited for the applications in software industry. AHP uses linguistic values and evaluates priorities by using a weighting process within the current alternatives by pair-wise comparisons.

Liming Zhu et al., in 2015, used AHP for software architecture evaluation [12]. Authors presented a research paper on ''*Tradeoff and Sensitivity Analysis in Software Architecture Evaluation Using Analytic Hierarchy Process*''. Multiple quality-factors were assessed for software architecture evaluation using its design features. These factors typically have inherent clashes and must be measured concurrently for final development decision. In this paper, the authors proposed numerous detailed investigation methods appropriate to AHP to classify serious balances and subtle opinions in the choice procedure. Also, they validated their approach using a real world decision making problem. The outcomes helped in getting best design decisions based on changing quality factors.

Alka Agarwal et al., in 2019, proposed the fuzzy AHP-TOPSIS approach for assessing sustainable-security of web applications with focus on design perception [13]. Authors presented a new approach for sustainable-security estimation and also discussed that this estimation will help the developers to categorize high prioritized factors contributing towards sustainable-security. It can be seen that AHP is a very popular technique for estimation of the security issues. Further, it is not only a helpful technique to assess the security-durability but also the results from this technique can be helpful in real scenarios as is seen in the literature. But still there are vague and unclear results from using fuzzy AHP.

Elmi and Eftekhari [14] in 2020 used hesitant fuzzy based multiple criteria decision making method for selection of appropriate classifiers of dynamic ensemble selection. The experimental results showed the efficiency of hesitant fuzzy method over other. Basar [15] in one of his work used the hesitant fuzzy method for assessing the priorities of factors of time planning software. He also used a real time example of a Turkish company to determine time planning of software projects.

From the literature point of view it is clear that AHP and Fuzzy have proved to be good assessment methods for solving decision making problems that arise during the selection of factors for security-durability. Web application security is a crucial issue that needs to be addressed as soon as possible. Hence using Fuzzy AHP is the best technique for multiple criteria decision making problem. Further, TOSPSIS is used to choose the best alternative among multiple alternatives. Hesitant fuzzy is a new method for removing the hesitation while taking the decision using different values to one specific membership function. Hence this

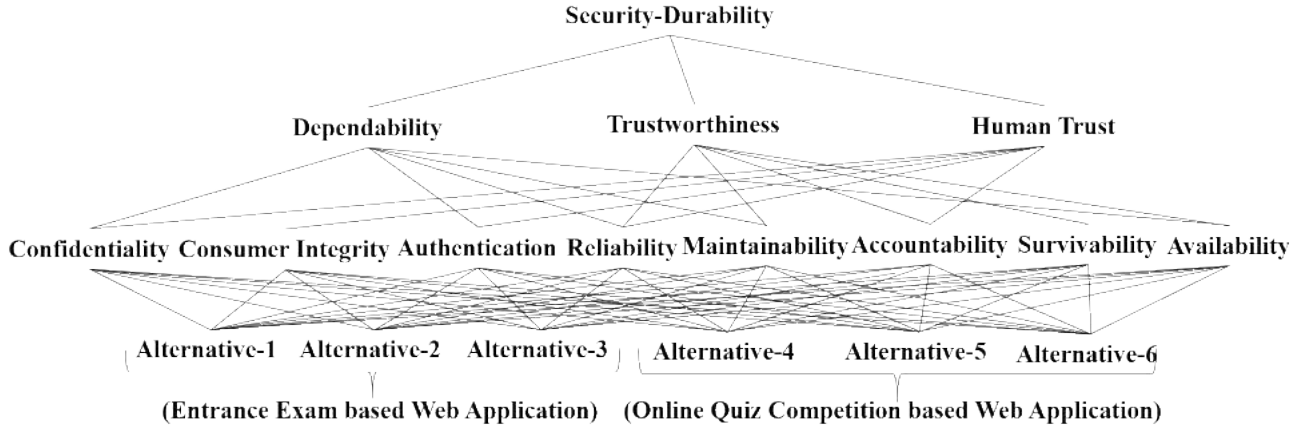


**FIGURE 1.** Security-durability factors.

paper uses hesitant fuzzy AHP TOPSIS methodology for the assessment of security-durability of a web application. CIA with other factor concurrently affects both security and durability. On the whole, this seems to be a multiple criteria decision examination problem in view of the security-durability, this is why Multiple Criteria Decision Analysis (MCDA) technique is used to assess security-durability.

## III. SECURITY-DURABILITY

The fundamental point of the innovation improvement in all web applications is to secure the clients from malignant assaults. At each phase of development life cycle, paying attention to the security of the web application may increase high reliability and user satisfaction [16]. Security of web application effectively increases the quality to meet its business requirements. Security experts say that process of identification of security factors is carried out at the time of security evaluation. Practitioners need to concentrate on security during the early stage of development; however, this is not hundred percent achievable [17]. Longer security during web application development is now becoming a difficult task for the security developers [18]. Also, consideration of security includes security factors, classifications and security measurements. Security factors must be considered as an important tool in every level of web application development. Security factors are incredibly vital facets in security engineering. Identification of security factors helps to improve security during web application development [19]. These factors formulate an essential part in the security world. In addition, the security factors are also included in producing solid cryptographic arrangements, as well as to discover an approach to give security necessities to enhance security amid web application development life cycle [6]–[9].

Web application security affects the longevity of the service life of web application [6]. This statement fortifies the fact that there must be a factor which relates to security and that is durability. In this concern, durability should be measured as one of the associating security factors. It is said that durability, in terms of software, is the time period during which software provides its services [7], [16], [17]. More so, it appears that the focus on security has inevitably led to the focus on the durability of the application. Security is straightforwardly or by implication associated with the administration life of the product. Security of web application is directly or indirectly affected by security-durability [4]. Security-durability is well defined factor of security [20], [21]. Lot of work has been done in the field of durability that has already been discussed in related work section [4]–[7], [10]–[15], [20]–[24]. The main objective of this contribution is to reduce the efforts to manage and control security and enhance life-span of web application. Security-durability assessment may be helpful to improve security and optimal maintenance for a period.

Further, durability is defined as the expected service life-span of web application. As the time passes, new threats for web applications are generated day by day. Due to the activation of these threats, security often fails and the web applications rendered dysfunctional. In this paper, authors have listed factors and sub-factors of security-durability which are already identified in their earlier work [4], [16], [23]–[24]. These factors of security-durability have been identified by thorough literature survey. In the previous work of the authors, there are plenty of factors of security-durability which is shown in figure 1.

Figure 1 include trustworthiness, dependability, and human trust that are to be used for improving security-durability that are defined as:

### A. DEPENDABILITY

According to Ensmenger [5], dependability denotes the capability to carry facility that can defensibly be reliable. From this definition it can be inferred that dependability is the factor that increases the security and the durability of web application [25]. Also, there are many factors of dependability but only a few of those affect the security-durability of web application. Dependability definition justifies the issue

of trust in security and is directly connected to security factors such as reliability, confidentiality and authentication [20]. Dependable also means that the service is reliable in its ability to avoid failures of service while it is not acceptable to the user [25]. This definition implies that dependability is related to availability and maintainability as well [4].

### B. TRUSTWORTHINESS

According to Cusick [8], the web application holds trustworthiness if it achieves what is envisioned for an exact purpose, when required, with new changes that have been done on it [21]. Security-durability is affected by few factors of trustworthiness. Further, trustworthiness depends on availability, maintainability, reliability, survivability and accountability [22]. Moreover, security-durability requirements will be strengthened when the web application work for a specified time period by consolidation of the maintainability of security of web application services, thus improving the trustworthiness of security. The measureable definition expresses that trustworthiness is also related to availability, reliability, accountability and survivability [4], [26].

### C. HUMAN TRUST

According to Agrawal *et al.* [4], human trust is typically distinct and is a subtle matter as it is the moral responsibility of the trusting party to provide reliable data and keep it confidential. In web application terms, the end users' trust on the developers is recognised as human trust. Longevity of security and human trust are the factors that complement each other and increases the other [23], [27]. Human trust has multiple factors but only a few of these factors are affected by the security-durability. Web application that has the desirable level of security-durability will enhance the human trust and in turn will improve consumer reliability on an organization's web application services [24]. Given this procedural description, it is found that there are five security factors that are affected by human trust and these are: reliability, authentication, confidentiality, consumer integrity, and accountability. Human trust always depends on these factors [22]–[23].

Security-durability assessment is based on the factors and its sub factors identified. Assessment of security-durability factors helps the decision makers to take appropriate decisions and thus improves the life-span of security [4], [8]. But to take appropriate decision, the decision makers should also know the mapping of these factors.For estimation, the factors of security-durability at level 1 are signified as D1, D2 and D3. Figure 2 shows the hierarchy of security-durability which is further classified in two levels.

In Figure 2, a factor at one level may construct its affect on higher levels but its affect on these higher levels is not the same. For assessing security-durability, factors are denoted as D1, D2, D3 at level 1, D11, D12, D13, D14, D15, D21, D22, D23, D24, D25, D31, D32, D33, D34, and D35 at level 2. The descriptions of these factors are different in different web application security situations. Further, there are eight factors at level 2 which affect security-durability and defined as:

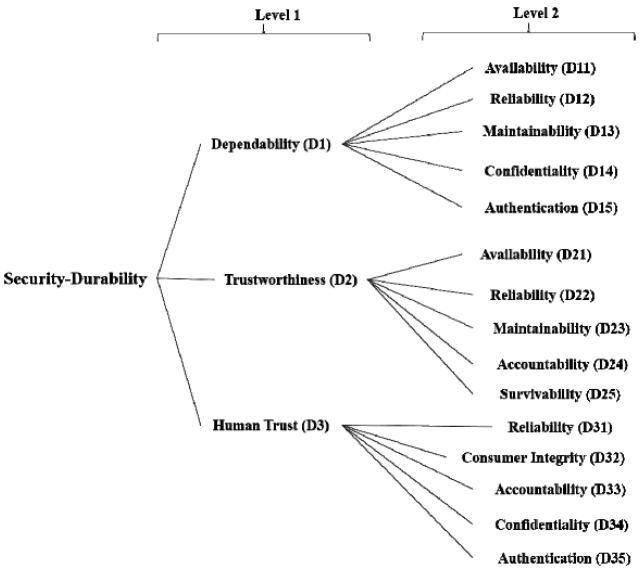


**FIGURE 2.** Hierarchy of security-durability factors.

- *Confidentiality:* Confidentiality of web application states that it is permitting authorized access to sensitive and secure data [4].
- *Consumer Integrity:* Consumer integrity of web application security is demarcated as the factor which maintains the reliability, trustworthiness, and accuracy of customer throughout the usage of web application [5].
- *Authentication:* Authentication of web application is the factor on which identity of user profile depends. Authentication is the procedure of defining whether a user is, in fact, who the user claims to be [5].
- *Reliability:* Reliability of web application is the ability of security to perform consistently for a specified period and according to its specifications [6].
- *Maintainability:* Maintainability refers to the likelihood that a web application can be maintained in a defined environment and with defined specifications [8].
- *Accountability:* Accountability specifies that every distinct user who uses web application should have precise responsibilities for security declaration [5].
- *Survivability:* Survivability is the ability of a web application to fulfill its security assignment, in an appropriate method, whether in the presence of attacks, failures, or accidents [10].
- *Availability:* Availability means the information is accessible by only authorized users. Availability, in the perspective of a web application, denotes the capability of a user to access data or resources for a specified duration [26].

Security-durability of web application will be improved when using well planned and well managed process of assessment of security-durability in Web Application Development Life Cycle (WADLC). Also deprived of an assessment of security-durability, it is not possible to improve it. Hence, this paper evaluates the security-durability through a case study of a

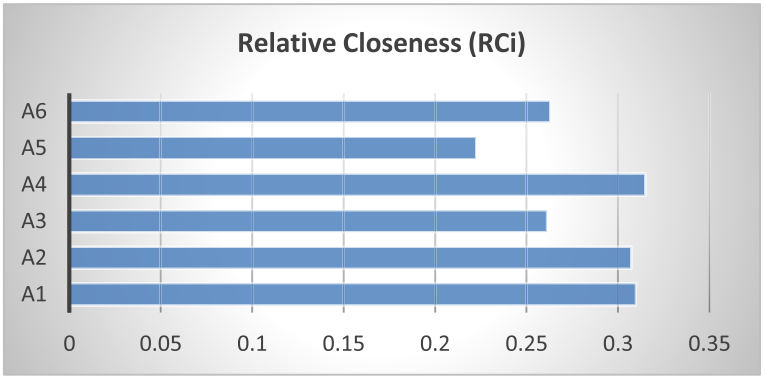


**FIGURE 3.** Graphical representation of the relative closeness.

University web application. Furthermore, this paper uses hesitant fuzzy with AHP and TOPSIS in which hesitant is used because of the hesitation that decision makers have while taking decision. Instead of the triangular fuzzy numbers, trapezoidal membership numbers are used for decision makers to take appropriate decision. Traditional methods of fuzzy cannot effectively handle problems with such imprecise information. To decide with this difficulty, the hesitant fuzzy set theory has been introduced by Torra and Narukawa in 2009 [28] and hesitant fuzzy is used where decision makers find any hesitancy in taking an appropriate decision.

## IV. HESITANT-FUZZY-AHP-TOPSIS TECHNIQUE

There are many real world problems that require MCDM approaches to solve them and to reach a suitable decision. Security-durability factors selection fits into this category. Amidst MCDM methods, AHP is proved to be well-organized than any other methods, since it provides the decision makers with an accurate solution [5], [9]. Due to the usage of pair-wise comparison matrices and checks the uniformity of results. When there are multiple numbers of alternatives available, this efficiency of pair-wise comparisons badly affects the decisions. To overcome this problem, this study proposes an integrated method hesitant fuzzy (HF) for crisp decisions consisting of AHP for weighing the decision criteria, and TOPSIS for selecting the most appropriate factor of security-durability of web application. Moreover for getting more precise results, this paper uses hesitant fuzzy mechanism. There are multiple complicated methods of MCDM but TOPSIS is the most preferred one because of its easy calculation. TOPSIS takes into account both the positive and negative ideal solution and this makes it a powerful method.

Although both of these methods fundamentally include fuzziness to a level, when it comes to complex real world complications, they lack consistency and need to be supported with fuzzy set theory. Recently in the literature, it has been strongly claimed that as the complexity and vagueness increase, ordinary fuzzy MCDM methods should be extended to the methods using type-II fuzzy sets, Intuitionistic Fuzzy Sets (IFS), and Hesitant Fuzzy Sets (HFS) [11], [28].

For the problems in which the membership degrees cannot be clearly defined or decision makers do not agree on the membership degree selection, Hesitant Fuzzy Sets should be used [15]. Hesitant fuzzy sets were introduced by Torra and Narukawa [28] and were further improved by Rodriguez *et al.* [29], [30]. Recently, the usage of HFSs has been increased in the literature. Wang *et al.* [31] recommend trapezium cloud-based TOPSIS method with interval-valued intuitionistic hesitant fuzzy linguistic information. The proposed method in this paper allowed handling vagueness and fuzziness of subjective ideas instantaneously. The proposed model was authenticated through an illustrative example which is about stock selection. Beg and Rashid [32] have also used hesitant fuzzy linguistic term sets for a projection model and compared the results with the other MCDM methods (such as maximum deviation model). A real case study was conducted for hospital information systems. Also Xia and Xu [33] proposed a novel model based on hesitant fuzzy TOPSIS and the model was authenticated for energy policy selection problem.

The proposed study in this paper opts for HF-AHP to weigh the factor within the model, and an aggregated HF-TOPSIS to select the best factor for security-durability estimation. For calculating the weights of the selected key and sub factors, steps are summarized as follows:

**Step 1:** Construct the hierarchy model of the different levels of criteria.

**Step 2:** Using the linguistic terms in Table 1, pair-wise comparisons among those criteria is made. To produce more reliable results, decision makers are given with much larger scale.

**Step 3:** Use fuzzy wrappers [29] on negotiated evaluations. Assuming that $T_0$ is the lowest value and $T_g$ is the peak value in the linguistic scale, and the evaluations are between $T_i$ and $T_j$ such that $T_0 \leq T_i \leq T_j \leq T_g$; calculate ordered weighted averaging of dimension n as in Equation (1).

$$OWA\,(a_1, a_2, \ldots a_n) = \sum_{j=1}^{n} W_j b_j \tag{1}$$

Here, $W = (w_1, w_2, \ldots . w_n)^S$ is the associated weighing vector satisfying the rule $\sum_{i=1}^{n} W = 1$ and $b_j$ takes a value equal to the largest of $a_1, a_2, \ldots . a_n$. After this calculate the fuzzy constraints of the trapezoidal numbers $\tilde{C} = (a, b, c, d)$ as in equation (2)-(5).

$$a = min\left\{a_L^i, a_M^i, a_M^{i+1}, \ldots \ldots a_M^j, a_R^j\right\} = a_L^i \tag{2}$$

$$d = max\left\{a_L^i, a_M^i, a_M^{i+1}, \ldots \ldots a_M^j, a_R^j\right\} = a_R^j \tag{3}$$

$$b = \left\{ \begin{array}{c} a_M^i, if\ i+1=j \\ OWA_w^{2\left(a_m^j, \ldots .. a_m^{\frac{i+j}{2}}\right)}, if\ \ i+j\ is\ even \\ OWA_w^{2\left(a_m^j, \ldots .. a_m^{\frac{i+j+1}{2}}\right)}, if\ \ i+j\ is\ odd \end{array} \right\} \tag{4}$$

$$c = \left\{ \begin{array}{c} a_M^{i+1}, if\ i+1=j \\ OWA_w^{2\left(a_m^j a_m^{j-1}, \ldots .. a_m^{\frac{(i+j)}{2}}\right)}, if\ \ i+j\ is\ even \\ OWA_w^{2\left(a_m^j, a_m^{j-1} \ldots .. a_m^{\frac{(i+j+1)}{2}}\right)}, if\ \ i+j\ is\ odd \end{array} \right\} \tag{5}$$

Specify 1st and 2nd type weights using $\eta$, a number within the unit interval [0, 1] using equations (6)-(7), respectively.

1st type weights ($W1 = (w_1^1, w_2^1, \ldots . . . . w_n^1)$):

$$w_1^1 = \eta_2, w_2^1 = \eta_2\left(1-\eta_2\right), \ldots . . . . w_n^1 \eta_2 (1-\eta_2)^{n-2} \tag{6}$$

2nd type weights ($W2 = (w_1^2, w_2^2, \ldots . . . . w_n^2)$) :

$$w_1^2 = \eta_1^{n-1}, \quad w_2^2 = (1-\eta_1)\,\eta_1^{n-1} \tag{7}$$

Within the equation $\eta_1 = \frac{g-(j-1)}{g-1}$s, and $\eta_2 = \frac{g-(j-1)}{g-1}$ where g is the number of the highest rank in evaluations (g is 10 according to table 1) and i and j are the ranks of the lowest and highest evaluations, respectively.

**Step 4:** Complete the pair-wise comparison matrix ($\tilde{A}$) as in equation (8)-(9).

$$\tilde{A} = \begin{bmatrix} 1 & \cdots & \tilde{c}_{1n} \\ \vdots & \ddots & \vdots \\ \tilde{c}_{n1} & \ldots & 1 \end{bmatrix} \tag{8}$$

$$\tilde{c}_{ji} = \left(\frac{1}{cij_u}, \frac{1}{cij_{m2}}, \frac{1}{cij_{m1}}, \frac{1}{cij_1}\right) \tag{9}$$

**Step 5**: Use equation (10) to defuzzify a trapezoidal fuzzy number as d = (l, $m_1$, $m_2$,h) which gives a crisp number

$$\mu_x = \frac{l + 2m_1 + 2m_2 + h}{6} \tag{10}$$

Calculate the ordinary Consistency Ratio (CR) using equations (11)-(12).

$$CI = \frac{\gamma_{max} - n}{n-1} \tag{11}$$

$$CR = \frac{CI}{RI} \tag{12}$$

where CI is the Consistency Index, $\lambda_{max}$ represents the biggest eigenvector of the matrix, n represents the number of criteria within the current evaluation, and Random Index (RI) is a randomly calculated ready-to-use index (the random index) that varies for different n values. Proceed if value of CR is lower than 0.1 otherwise go to 2nd step and restart the calculations.

**TABLE 1.** Scale for HF-AHP method.

| Rank | Linguistic Term | Abbreviation | Triangular Fuzzy Number |
|---|---|---|---|
| 10 | Absolutely High Importance | AHI | (7.0000,9.0000,9.0000) |
| 9 | Very High Importance | VHI | (5.0000,7.0000,9.0000) |
| 8 | Essentially High Importance | ESHI | (3.0000,5.0000,7.0000) |
| 7 | Weakly High Importance | WHI | (1.0000,3.0000,5.0000) |
| 6 | Equally High Importance | EHI | (1.0000,1.0000,3.0000) |
| 5 | Exactly Equal | EE | (1.0000,1.0000,1.0000) |
| 4 | Equally Low Importance | ELI | (0.3300,1.0000,1.0000) |
| 3 | Weakly Low Important | WLI | (0.2000,0.3300,1.0000) |
| 2 | Essentially Low Importance | ESLI | (0.1400, 0.2000, 0.3300) |
| 1 | Very Low Importance | VLI | (0.1100, 0.1400, 0.2000) |
| 0 | Absolutely Low Importance | ALI | (0.1100, 0.1100, 0.1400) |

**Step 6:** Next step is calculating the geometric mean for each row using equation (13).

$$\tilde{r}_i = (\tilde{c}_{i1} \otimes \tilde{c}_{i2} \ldots . . \otimes \tilde{c}_{in})^{1/n} \tag{13}$$

**Step 7:** Each main criteria weight is calculated using equation (14) given below:

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

**Step 8**: Defuzzify all the fuzzy numbers as in equation (15).

$$\mu_x = \frac{l + 2m_1 + 2m_2 + h}{6} \tag{15}$$

**Step 9:** Normalize weights are evaluated from defuzzified weights with the help of equation (16).

$$\frac{\tilde{w}_i}{\sum_i \sum_j \tilde{w}_j} \tag{16}$$

Next process is to find the best alternative using the hesitant fuzzy TOPSIS.As widely used MADM method TOPSIS helps practitioners with selecting the best preferred alternative in real world problems. The TOPSIS was firstly proposed by Lai *et al.* [34]. This method is based on the idea that the perfect alternative has the greatest level for all factors measured, whereas the negative-ideal is the one with all the worst factor values. The farthest from the negative-ideal and

the closest to the ideal alternative is the solution from TOPSIS which further is defined as the alternative. In this proposed study for security-durability estimation Beg and Rashid's hesitant fuzzy TOPSIS method is adopted by prioritizing the criteria with hesitant fuzzy AHP which clarify the procedure [32]. The methodology is based on using envelopes for computing the distance between two Hesitant Fuzzy Linguistic Term Set (HFLTS) such as H1s and H2s. Given the envelopes are env(H1s) = [$T_p$,$T_q$] and $env(H2s) = [T_p^*, T_q^*]$, the distance is defined as:

$$d\,(H1s, H2s) = \left|q^* - q\right| + \left|p^* - p\right| \tag{17}$$

The methodology can further be defined as follows:

**Step 10:** For the initial step let's assume that

- The decision under consideration has E alternatives ($C = \{C_1, C_2, \ldots..C_E\}$) and n criteria ($C = \{C_1, C_2, \ldots..C_n\}$)
- The experts are denoted with $e_x$ and the number of decision makers is K
- $\tilde{X}^l = \left[H^l_{S_{ij}}\right]_{E\times n}$ is a fuzzy decision matrix where $H^l_{S_{ij}}$ is evaluation score for alternative i($C_i$) against criteria j($A_j$) given by expert $e_x$
- The scale for hesitant fuzzy TOPSIS is given as
  Let *Scale* = {*nothing, very bad, bad, medium, good, very good, perfect*} be a verbal or linguistic term set and *CH* be the context-free grammar for generating its relative linguistic terms. Also take two expert'$e1$ and $e2$ to provide their rank for two criteria A1 and A2,
  $r_1^1$ = *between medium and good* (bt M&G)
  $r_2^1$ = *at most medium* (am M)
  $r_1^2$ = *at least good* (al G)
  $r_2^2$ = *between very bad and medium* (bt VB&M
  The fuzzy envelope for each comparative linguistic expression is computed as the following [9]:
  $env_F$ *EGH btMG*))= $T$(0.3300,0.5000,0.6700,0.8300
  $env_F$ *EGH amM*))= $T$(0.0000,0.0000,0.3500,0.6700)
  $env_F$ *EGH alG*))= $T$(0.5000,0.8500,1.0000,1.0000)
  $env_F$ *EGH btVBM*))= $T$(0.0000,0.3000,0.3700,0.6700,

**Step 11**: Aggregate the individual evaluations of experts $(\tilde{X}^1, \tilde{X}^2 \ldots\ldots \tilde{X}^K)$ and construct an aggregated decision matrix X = [$x_{ij}$] where $x_{ij}$ represents the evaluation score of $C_i$ against $A_j$ and mathematically shown as $x_{ij}$ = [$T_{pij}$, $T_{qij}$] such that

$$\begin{aligned} T_{pij} &= min\left\{min_{i=1}^K\left(maxH^x_{t_{ij}}\right), max_{i=1}^K\left(minH^x_{t_{ij}}\right)\right\} \\ T_{qij} &= max\left\{min_{i=1}^K\left(maxH^x_{t_{ij}}\right), max_{i=1}^K\left(minH^x_{t_{ij}}\right)\right\} \end{aligned} \tag{18}$$

**Step 12**: Let $\alpha_b$ represent benefit criteria where larger values in $A_j$ means higher preference and $\alpha_c$ represents cost criteria where lower values in $A_j$ indicates more preference.

Assume that the HFLTS positive ideal solution is donated with $\tilde{C}^+$ and mathematically represented as $\tilde{C}^+ = (\tilde{V}_1^+, \tilde{V}_2^+, \ldots \tilde{V}_n^+)$ where $\tilde{V}_j^+ = \left[V_{pj}^+, V_{qj}^+\right] (j = 1, 2, 3 \ldots .n)$ and the HFLTS negative ideal solution is denoted as $\tilde{C}^-$ and mathematically represented as $\tilde{C}^- = (\tilde{V}_1^-, \tilde{V}_2^-, \ldots \tilde{V}_n^-)$ where

$$\tilde{V}_j^- = \left[V_{pj}^-, V_{qj}^-\right] \quad (j = 1, 2, 3 \ldots .n)$$

Define $\tilde{V}_{pj}^+$, $\tilde{V}_{qj}^+$, $\tilde{V}_{pj}^-$ and $\tilde{V}_{qj}^-$ for cost and benefit criteria such that

$$\begin{aligned} \tilde{V}_{pj}^+ &= max_{i=1}^K\left(max_i\left(minH^x_{S_{ij}}\right)\right) j \in \alpha_b \quad \text{and} \\ &\quad min_{i=1}^K\left(min_i\left(minH^x_{S_{ij}}\right)\right) j \in \alpha_c) \end{aligned} \tag{19}$$

$$\begin{aligned} \tilde{V}_{qj}^+ &= max_{i=1}^K\left(max_i\left(minH^x_{S_{ij}}\right)\right) j \in \alpha_b \quad \text{and} \\ &\quad min_{i=1}^K\left(min_i\left(minH^x_{S_{ij}}\right)\right) j \in \alpha_c) \end{aligned} \tag{20}$$

$$\begin{aligned} \tilde{V}_{pj}^- &= max_{i=1}^K\left(max_i\left(minH^x_{S_{ij}}\right)\right) j \in \alpha_c \quad \text{and} \\ &\quad min_{i=1}^K\left(min_i\left(minH^x_{S_{ij}}\right)\right) j \in \alpha_b) \end{aligned} \tag{21}$$

$$\begin{aligned} \tilde{V}_{qj}^- &= max_{i=1}^K\left(max_i\left(minH^x_{S_{ij}}\right)\right) j \in \alpha_c \quad \text{and} \\ &\quad min_{i=1}^K\left(min_i\left(minH^x_{S_{ij}}\right)\right) j \in \alpha_b) \end{aligned} \tag{22}$$

**Step 13:** Construct the positive and negative ideal separation matrices ($D^+$ and $D^-$) as in equations (22)-(23) respectively,

$$D^+ = \begin{bmatrix} d\left(x_{11}, \tilde{V}_1^+\right) + & d\left(x_{12}, \tilde{V}_2^+\right) + & \ldots + d\left(x_{1n}, \tilde{V}_n^+\right) \\ d\left(x_{21}, \tilde{V}_1^+\right) + & d\left(x_{22}, \tilde{V}_2^+\right) + & \ldots + d\left(x_{21}, \tilde{V}_n^+\right) \\ d\left(x_{m1}, \tilde{V}_1^+\right) + & d\left(x_{m2}, \tilde{V}_1^+\right) + & \ldots + d\left(x_{mn}, \tilde{V}_n^+\right) \end{bmatrix} \tag{23}$$

$$D^- = \begin{bmatrix} d\left(x_{11}, \tilde{V}_1^-\right) + & d\left(x_{12}, \tilde{V}_2^-\right) + & \ldots + d\left(x_{1n}, \tilde{V}_n^-\right) \\ d\left(x_{21}, \tilde{V}_1^-\right) + & d\left(x_{22}, \tilde{V}_2^-\right) + & \ldots + d\left(x_{21}, \tilde{V}_n^-\right) \\ d\left(x_{m1}, \tilde{V}_1^-\right) + & d\left(x_{m2}, \tilde{V}_1^-\right) + & \ldots + d\left(x_{mn}, \tilde{V}_n^-\right) \end{bmatrix} \tag{24}$$

**Step 14:** Calculate the relative closeness score for each alternative under consideration using equation (24)

$$CS\,(A_i) = \frac{D_i^+}{D_i^+ + D_i^-}, \quad i = 1, 2, \ldots .m \tag{25}$$

where

$$D_i^+ = \sum_{j=1}^n d\left(x_{ij}, V_j^+\right) \text{ and } D_i^- = \sum_{j=1}^n d(x_{ij}, V_j^-) \tag{26}$$

**Step 15**: Order the alternatives based on corresponding relative closeness scores.

Security-durability estimation using a hybrid methodology of HF-AHP-TOPSIS is implemented in the next section.

## V. EMPIRICAL DATA ANALYSIS AND RESULTS

Mostly, qualitative assessment is appropriate for evaluating security-durability of web application. Quantitative

**TABLE 2.** Fuzzy envelops for factors of level 1.

| | D1 | D2 | D3 |
|---|---|---|---|
| Dependability (D1) | EE | B/W EHI and WHI | B/W ESHI and VHI |
| Trustworthiness (D2) | - | EE | B/W WHI and ESHI |
| Human Trust (D3) | - | - | EE |

assessment of security-durability is very hard. Global collective action led to the design of the durability policy. Experts from industry and academia have implemented durability policies and programs to get remarkable outcomes [35], [36]. Also, experts are trying to implement high security for reducing time and cost of security maintenance of web applications. In addition, security-durability attributes impact plays a significant role for improving security-durability [5], [20], [21]. In this row, contributors of this paper have adopted an approach for assessing security-durability of web application through HF-AHP-TOPSIS.

Contributors have categorized and deliberated the security-durability in the foregoing segments. According to figure 1, a factor of the hierarchy at a level influences one or more factor of the other level but its influence is not the same on them. It may fluctuate. For evaluating the security-durability, the contributors transformed the categorized factors into hierarchies in security-durability perspective and shown it into figure 2. For estimating security-durability, dependability factors are represented as D11, D12, D13, D14 and D15 at level 2. Trustworthiness factors are represented as D21, D22, D23, D24 and D25 at level 2. Human Trust factors are denoted as D31, D32, D33, D34 and D35 at level 2. From these orders, the contributors of the paper estimated the security-durability of web application.

To calculate the weights of factors of security-durability, pair-wise comparison matrixes are assembled in the form of opinions for each set of factors and data has been collected from 45 practitioners of various affiliations (academicians and industry persons) who were brought together in a virtual meeting environment. These academicians and industry professionals were having an 8-10 year experience in web application development and relevant expertise in using new security methods. They discussed about the factors with respect to different groups and gave the linguistic values with the help of scale. Firstly, three main factors were taken in a group as shown in figure 1 and scored after all researchers got a common decision in the meeting. After getting the score, the consistency of each evaluation was tested with the help of step 5 and equations (10-12). At the first evaluation, the consistency was found to be lower than 0.1. Therefore, the fuzzy envelops (consistent) for factors at level 1 was got that are shown in Table 2.

From table 1, table 2 and equations (1-12), contributors compute the results as following:

The fuzzy envelope (D12) was selected as ''B/W EHI and WHI''. The Triangular Fuzzy Numbers (TFN) related with the declared linguistic values are (1, 1, 3) and (1, 3, 5), respectively. With the help of equations (1-5), the trapezoidal fuzzy numbers $\tilde{C} = (a, b, c, d)$, showing the linguistic value

**TABLE 3.** Trapezoidal fuzzy pair-wise comparison matrix at level 1.

| | D1 | D2 | D3 |
|---|---|---|---|
| D1 | 1.0000, 1.0000, 1.0000, 1.0000 | 1.0000, 1.0000, 3.0000, 5.0000 | 0.3300, 1.0000, 1.0000, 3.0000 |
| D2 | 0.2000, 0.3300, 1.0000, 1.0000 | 1.0000, 1.0000, 1.0000, 1.0000 | 0.2000, 0.3300, 1.0000, 1.0000 |
| D3 | 0.3300, 1.0000, 1.0000, 3.0000 | 1.0000, 1.0000, 3.0000, 5.0000 | 1.0000, 1.0000, 1.0000, 1.0000 |

**TABLE 4.** Normalized weights of level 1 factor.

| | Geometric Means | Fuzzify Local Weights | Defuzzified Weights |
|---|---|---|---|
| D1 | 0.6900, 1.0000, 1.4400, 2.4700 | 0.1200, 0.2600, 0.5800, 1.4300 | 0.5383 |
| D2 | 0.3400, 0.4800, 1.0000, 1.0000 | 0.0600, 0.1200, 0.4000, 0.6000 | 0.2833 |
| D3 | 0.7000, 1.0000, 1.4000, 2.5000 | 0.1200, 0.2500, 0.5700, 1.4200 | 0.5300 |

is evaluated as:

$$\begin{aligned} a &= min\left\{a_L^6, a_L^7, a_M^6, a_M^7, a_R^6, a_R^7\right\} \\ &= min\{1.0000, 1.0000, 1.0000, 3.0000, 3.0000, 5.0000\} \\ &= 1.0000 \\ d &= max\left\{a_L^6, a_L^7, a_M^6, a_M^7, a_R^6, a_R^7\right\} \\ &= max\{1.0000, 1.0000, 1.0000, 3.0000, 3.0000, 5.0000\} \\ &= 5.0000 \end{aligned}$$

and then, i + 1 = j (i = 6; j = 7; then, $b = a_M^6 = 1.0000$ and $c = a_M^7 = 3.0000$. At the end, it is determined that the trapezoidal fuzzy set of this envelop is (1.0000, 1.0000, 3.0000, 5.0000). Similarly, trapezoidal fuzzy sets were calculated for other relative importance. The computed results of security-durability factors at level 1 are shown in table 3.

With help of equations (13-14), computing the fuzzy weights of factors as follows:

$$\begin{aligned} \tilde{r}_1 &= [(1.0000, 1.0000, 1.0000, 1.0000) \\ &\quad \otimes(1.0000, 1.0000, 3.0000, 5.0000) \\ &\quad \otimes(0.3300, 1.0000, 1.0000, 3.0000)]1/3 \\ &= [(1.0000\,X1.0000\,X0.3300)1/3, \\ &\quad (1.0000\,X1.0000\,X1.0000)1/3, \\ &\quad (1.0000\,X3.0000\,X1.0000)1/3, \\ &\quad (1.0000\,X5.0000\,X3.0000)1/3] \\ &= (0.6900, 1.0000, 1.4400, 2.4700) \end{aligned}$$

Correspondingly, remaining $\tilde{r}_i$ obtained as shown in table 4. Now, the weight of each factor can be assessed with the help of equations (14) as follows:

$$\begin{aligned} \tilde{w}_1 &= (0.6900, 1.0000, 1.4400, 2.4700) \\ &\quad \otimes((0.6900, 1.0000, 1.4400, 2.4700) \\ &\quad \oplus(0.3400, 0.4800, 1.0000, 1.0000) \\ &\quad \oplus(0.7000, 1.0000, 1.4000, 2.5000))^{-1} \\ &= (0.1200, 0.2600, 0.5800, 1.4300) \end{aligned}$$

**TABLE 5.** Global weights through the hierarchy.

| Factors of Level 1 | Local Weights | Factors of Level 2 | Local Weights | Global Weights | Defuzzified Weights | Normalized Weights |
|---|---|---|---|---|---|---|
| D1 | 0.1200, 0.2600, 0.5800, 1.4300 | D11 | 0.0500, 0.1640, 0.2830, 1.0140 | 0.0060, 0.0420, 0.1650, 1.4470 | 0.3110 | 0.0930 |
| | | D12 | 0.0345, 0.1656, 0.2256, 0.6200 | 0.0040, 0.0430, 0.1310, 0.8850 | 0.2060 | 0.0620 |
| | | D13 | 0.0590, 0.2080, 0.3480, 1.2630 | 0.0070, 0.0540, 0.2020, 1.8020 | 0.3870 | 0.1200 |
| | | D14 | 0.0540, 0.1330, 0.2810, 0.9480 | 0.0060, 0.0340, 0.1640, 1.3530 | 0.2920 | 0.0580 |
| | | D15 | 0.0330, 0.0860, 0.1810, 0.4980 | 0.0040, 0.0220, 0.1050, 0.7110 | 0.1620 | 0.0490 |
| D2 | 0.0600, 0.1200, 0.4000, 0.6000 | D21 | 0.0480, 0.1570, 0.2710, 1.0250 | 0.0060, 0.0400, 0.1570, 1.4620 | 0.3110 | 0.0910 |
| | | D22 | 0.0330, 0.1290, 0.2120, 0.7810 | 0.0040, 0.0330, 0.1230, 1.1140 | 0.2390 | 0.0720 |
| | | D23 | 0.0640, 0.2400, 0.4260, 1.2140 | 0.0080, 0.0620, 0.2480, 1.7320 | 0.3930 | 0.1140 |
| | | D24 | 0.0520, 0.1590, 0.2970, 1.0250 | 0.0060, 0.0410, 0.1730, 1.4620 | 0.3160 | 0.0930 |
| | | D25 | 0.0220, 0.0730, 0.1130, 0.5030 | 0.0030, 0.0190, 0.0660, 0.7180 | 0.1480 | 0.0440 |
| D3 | 0.1200, 0.2500, 0.5700, 1.4200 | D31 | 0.0310, 0.0780, 0.1210, 0.390 | 0.0020, 0.0100, 0.0490, 0.2250 | 0.0570 | 0.0160 |
| | | D32 | 0.1490, 0.2760, 0.7230, 1.5090 | 0.0090, 0.0340, 0.2920, 0.8730 | 0.2550 | 0.0770 |
| | | D33 | 0.0760, 0.2180, 0.4550, 1.0310 | 0.0040, 0.0270, 0.1830, 0.5960 | 0.1700 | 0.0510 |
| | | D34 | 0.0350, 0.0970, 0.1980, 0.5130 | 0.0020, 0.0120, 0.0800, 0.2970 | 0.0800 | 0.0240 |
| | | D35 | 0.0310, 0.0780, 0.1210, 0.390 | 0.0020, 0.0100, 0.0490, 0.2250 | 0.0420 | 0.0360 |

**TABLE 6.** Dependent weights of level 1 attributes.

| S. No. | Characteristics of Level 1 | Global Weights | Normalized Weights | |
|---|---|---|---|---|
| 1 | Dependability | 0.1200, 0.2600, 0.5800, 1.4300 | 0.3983 | D1 |
| 2 | Trustworthiness | 0.0600, 0.1200, 0.4000, 0.6000 | 0.2096 | D2 |
| 3 | Human Trust | 0.1200, 0.2500, 0.5700, 1.4200 | 0.3921 | D3 |

Correspondingly, remaining $\tilde{w}_i$ estimated as shown in table 4. Further, with the help of equation (15), defuzzified value of each factor is estimated as follows:

$$\tilde{w}_1 = \frac{0.1200+2\times0.2600+2\times0.5800+1.4300}{6} = 0.5383$$

Similarly, defuzzified weights of $\tilde{w}_2 = 0.2833$ and $\tilde{w}_3 = 0.5300$.

Thereafter, normalize the weights by using equation (16).

$$\begin{aligned}\tilde{w}_1 &= 0.5383\tilde{w}_2 = 0.2833;\ \tilde{w}_3 = 0.5300\\ &= 0.5383 + 0.2833 + 0.5300\\ &= 1.3516\end{aligned}$$

$$\tilde{w}_1 \textit{ in normal form is} = \frac{0.5383}{1.3516} = 0.3983$$

Similarly, normalized weights of $\tilde{w}_2 = 0.2096$ and; $\tilde{w}_3 = 0.3921$

**TABLE 7.** Dependent weights of level 2 attributes.

| S. No. | Characteristics of Level 2 | Global Weights | Normalized Weights | |
|---|---|---|---|---|
| 1 | Reliability | 0.0100, 0.0860, 0.4790, 2.2240 | 0.1500 | D12+D22 +D31 |
| 2 | Availability | 0.0120, 0.0820, 0.3220, 2.9090 | 0.1840 | D11+D21 |
| 3 | Authentication | 0.0060, 0.0320, 0.1540, 0.9360 | 0.0850 | D15+D35 |
| 4 | Maintainability | 0.0150, 0.1160, 0.4500, 3.5340 | 0.2340 | D13+D23 |
| 5 | Confidentiality | 0.0080, 0.0460, 0.2440, 1.650 | 0.0820 | D14+D34 |
| 6 | Accountability | 0.0100, 0.0680, 0.3560, 2.0580 | 0.1440 | D24+D33 |
| 7 | Consumer Integrity | 0.0090, 0.0340, 0.2920, 0.8730 | 0.0770 | D32 |
| 8 | Survivability | 0.0030, 0.0190, 0.0660, 0.7180 | 0.0440 | D25 |

Similar process is used for level 2 factors and the fuzzy local weights through the hierarchy are shown in table 5. Weights of the attributes signifies the contribution of that particular attribute in overall security-durability. Also local weights are the independent weights of attributes while global weights are calculated through the hierarchical structure of security-durability. For example reliability of the software security weighs different for its security and security-durability.With the help of previous calculations, table 5 also show the last level independent and dependent normalized weight of each factor through the hierarchy.

**TABLE 8.** Subjective cognition results of evaluators in linguistic terms.

| Security-Durability Factors/ Alternatives | A1 | A2 | A3 | A4 | A5 | A6 |
|---|---|---|---|---|---|---|
| Reliability | 3.2500, 5.1200, 7.1400, 8.7200 | 3.1500, 5.1500, 6.9100, 7.7200 | 2.8200, 4.6400, 6.6400, 8.7200 | 1.5500, 3.1800, 5.1800, 6.7200 | 1.4500, 3.1800, 5.1800, 7.7200 | 2.4500, 4.2700, 6.2700, 8.6200 |
| Availability | 4.2800, 5.3700, 6.3700, 7.7200 | 2.4500, 4.4500, 6.4500, 7.4500 | 2.9100, 4.6400, 6.0000, 6.4500 | 1.4500, 3.0000, 4.9100, 5.4500 | 1.1800, 2.8200, 4.8200, 6.4500 | 2.0900, 3.7300, 5.7300, 6.4500 |
| Authentication | 4.2700, 6.2700, 8.1400, 8.7200 | 2.8200, 4.8200, 5.8200, 6.4500 | 3.1800, 5.1800, 7.1000, 8.6500 | 1.4500, 3.0700, 4.9100, 5.6500 | 0.8200, 2.2700, 4.2700, 6.6500 | 3.0000, 4.8200, 6.8200, 7.6500 |
| Maintainability | 5.3600, 6.3600, 7.1200, 8.5100 | 3.7300, 5.7300, 7.5500, 8.6500 | 2.4500, 4.4500, 6.4500, 7.6500 | 0.9100, 2.4500, 4.4500, 5.6500 | 2.4500, 4.2700, 6.2700, 8.6500 | 3.9100, 5.9100, 7.8200, 8.6500 |
| Confidentiality | 4.6400, 5.6400, 7.5500, 8.8400 | 3.0000, 5.0000, 7.1400, 7.5100 | 2.1800, 4.0900, 6.1400, 7.5100 | 2.8200, 4.6400, 6.6400, 8.5100 | 1.9100, 3.7300, 5.7300, 7.5100 | 2.5500, 4.4500, 6.4500, 8.5100 |
| Accountability | 3.1200, 5.0000, 7.1400, 9.5100 | 2.4500, 4.4500, 6.4500, 7.7300 | 3.5500, 5.5500, 7.4500, 8.7300 | 1.8200, 3.7300, 5.7300, 6.7300 | 1.6400, 3.5500, 5.5500, 6.7300 | 3.9100, 5.9100, 7.9100, 8.7300 |
| Consumer Integrity | 5.3600, 7.3600, 9.0900, 9.7100 | 2.6400, 4.6400, 6.6400, 8.6400 | 2.9000, 4.8000, 6.7000, 7.6400 | 2.8200, 4.6400, 6.6400, 6.6400 | 2.5500, 4.4500, 6.4500, 7.8400 | 3.1800, 5.1800, 7.0900, 7.9300 |
| Survivability | 5.1200, 7.1400, 7.7200, 8.5900 | 3.1500, 5.1500, 6.9100, 7.8400 | 2.8200, 4.6400, 6.6400, 7.8400 | 1.5500, 3.1800, 5.1800, 6.5400 | 1.4500, 3.1800, 5.1800, 6.2500 | 2.4500, 4.2700, 6.2700, 8.2600 |

**TABLE 9.** The normalized fuzzy-decision matrix.

| Security-Durability Factors/ Alternatives | A1 | A2 | A3 | A4 | A5 | A6 |
|---|---|---|---|---|---|---|
| Reliability | 0.3250, 0.4680, 0.5550, 0.6370 | 0.6040, 0.8120, 0.8580, 0.9690 | 0.6390, 0.8160, 0.5890, 0.9670 | 0.2310, 0.3810, 0.5480, 0.7362 | 0.3550, 0.5560, 0.6970, 0.8470 | 0.6200, 0.8720, 0.9360, 0.9890 |
| Availability | 0.2040, 0.3220, 0.4370, 0.5470 | 0.5540, 0.8040, 0.8800, 0.9580 | 0.6110, 0.7720, 0.8560, 0.9450 | 0.3800, 0.5740, 0.7220, 0.0820 | 0.4210, 0.6578, 0.7570, 0.9190 | 0.6120, 0.8500, 0.9170, 0.9680 |
| Authentication | 0.2310, 0.3580, 0.4470, 0.5700 | 0.3720, 0.5650, 0.6930, 0.8350 | 0.5740, 0.7250, 0.7920, 0.8960 | 0.2490, 0.4130, 0.5320, 0.7410 | 0.2420, 0.3970, 0.5470, 0.7430 | 0.4520, 0.6680, 0.7610, 0.8980 |
| Maintainability | 0.2574, 0.3870, 0.4370, 0.5400 | 0.0370, 0.1050, 0.2420, 0.5100 | 0.0398, 0.1000, 0.1920, 0.3840 | 0.4230, 0.6490, 0.7640, 0.8800 | 0.4610, 0.6570, 0.7650, 0.9050 | 0.2750, 0.4560, 0.5330, 0.7330 |
| Confidentiality | 0.4590, 0.6120, 0.6530, 0.6880 | 0.2940, 0.4840, 0.5630, 0.7420 | 0.4830, 0.6199, 0.7030, 0.8390 | 0.3460, 0.5530, 0.6640, 0.8170 | 0.4370, 0.6360, 0.7360, 0.8580 | 0.3340, 0.5240, 0.6180, 0.7800 |
| Accountability | 0.5400, 0.5400, 0.5400, 0.5400 | 0.2490, 0.4130, 0.5320, 0.7410 | 0.2420, 0.3970, 0.5470, 0.7430 | 0.4520, 0.6680, 0.7610, 0.8980 | 0.6110, 0.7720, 0.8560, 0.9450 | 0.6120, 0.8500, 0.9170, 0.9680 |
| Consumer Integrity | 0.5590, 0.5590, 0.5590, 0.5590 | 0.4230, 0.6490, 0.7640, 0.8800 | 0.4610, 0.6570, 0.7650, 0.9050 | 0.2750, 0.4560, 0.5330, 0.7330 | 0.5740, 0.7250, 0.7920, 0.8960 | 0.8750, 0.8750, 0.8750, 0.8750 |
| Survivability | 0.0350, 0.0350, 0.0350, 0.0350 | 0.3460, 0.5530, 0.6640, 0.8170 | 0.4370, 0.6360, 0.7360, 0.8580 | 0.3340, 0.5240, 0.6180, 0.7800 | 0.03980, 0.1000, 0.1920, 0.3840 | 0.5500, 0.5500, 0.5500, 0.5500 |

**TABLE 10.** The weighted normalized fuzzy-decision matrix.

| Security-Durability Factors/ Alternatives | A1 | A2 | A3 | A4 | A5 | A6 |
|---|---|---|---|---|---|---|
| Reliability | 0.0120, 0.0180, 0.0210, 0.0240 | 0.1250, 0.1690, 0.1850, 0.2010 | 0.1480, 0.1891, 0.2060, 0.2240 | 0.0344, 0.0570, 0.0820, 0.1100 | 0.0470, 0.0740, 0.0920, 0.1120 | 0.0434, 0.0510, 0.0660, 0.0690 |
| Availability | 0.0080, 0.0120, 0.0160, 0.0210 | 0.1150, 0.1670, 0.1830, 0.1990 | 0.1420, 0.1790, 0.1980, 0.2190 | 0.0570, 0.0850, 0.1080, 0.1310 | 0.0555, 0.0870, 0.1040, 0.1220 | 0.0428, 0.0590, 0.0640, 0.0680 |
| Authentication | 0.0087, 0.0135, 0.0170, 0.0210 | 0.0774, 0.1180, 0.1440, 0.1730 | 0.1330, 0.1680, 0.1840, 0.2080 | 0.0371, 0.0616, 0.0790, 0.1100 | 0.0320, 0.0530, 0.0720, 0.0980 | 0.0320, 0.0470, 0.0530, 0.0630 |
| Maintainability | 0.0100, 0.0150, 0.0160, 0.0200 | 0.0080, 0.0224, 0.0502, 0.1000 | 0.0090, 0.0230, 0.0450, 0.0590 | 0.0630, 0.0979, 0.1140, 0.1310 | 0.0610, 0.0870, 0.1010, 0.1200 | 0.0190, 0.0325, 0.0380, 0.0510 |
| Confidentiality | 0.0173, 0.0233, 0.0250, 0.0270 | 0.0611, 0.1010, 0.1170, 0.1540 | 0.1120, 0.1440, 0.1630, 0.1950 | 0.0516, 0.0820, 0.0990, 0.1220 | 0.0580, 0.0850, 0.0950, 0.1180 | 0.0230, 0.0370, 0.0430, 0.0550 |
| Accountability | 0.0854, 0.0930, 0.0930, 0.0986 | 0.0371, 0.0616, 0.0790, 0.1100 | 0.0320, 0.0530, 0.0720, 0.0980 | 0.0320, 0.0470, 0.0530, 0.0630 | 0.1420, 0.1790, 0.1980, 0.2190 | 0.0320, 0.0470, 0.0530, 0.0630 |
| Consumer Integrity | 0.0890, 0.0960, 0.0960, 0.1030 | 0.0630, 0.0979, 0.1140, 0.1310 | 0.0610, 0.0870, 0.1010, 0.1200 | 0.0190, 0.0325, 0.0380, 0.0510 | 0.1330, 0.1680, 0.1840, 0.2080 | 0.1430, 0.1500, 0.1500, 0.1570 |
| Survivability | 0.0010, 0.0060, 0.0060, 0.0130 | 0.0516, 0.0820, 0.0990, 0.1220 | 0.0580, 0.0850, 0.0950, 0.1180 | 0.0230, 0.0370, 0.0430, 0.0550 | 0.0090, 0.0230, 0.0450, 0.0590 | 0.0870, 0.0940, 0.0940, 0.1010 |

In table 5, numerous factors at level 2 are repetitive in hierarchy but their influence on its greater level factors is diverse. For better understanding, grouping is finalized to measure the weights of every level's factor. Weights of alter factors at a different level are presented in table 6 and 7 with their influence towards security-durability. Further, table 7 is

**TABLE 11.** Distance between alternatives and ideal solutions.

| | Positive Ideal Solutions | | | | | | Negative Ideal Solutions | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Security-Durability Factors/ Alternatives | A1 | A2 | A3 | A4 | A5 | A6 | A1 | A2 | A3 | A4 | A5 | A6 |
| Reliability | 0.9800 | 0.8300 | 0.8100 | 0.9290 | 0.9190 | 0.9400 | 0.0190 | 0.1700 | 0.1920 | 0.0710 | 0.0810 | 0.0600 |
| Availability | 0.9900 | 0.8340 | 0.8150 | 0.9050 | 0.9080 | 0.9410 | 0.0140 | 0.1660 | 0.1850 | 0.0950 | 0.0920 | 0.0590 |
| Authentication | 0.9850 | 0.8700 | 0.8270 | 0.9280 | 0.9360 | 0.9510 | 0.0150 | 0.1280 | 0.1730 | 0.0720 | 0.0640 | 0.0490 |
| Maintainability | 0.9850 | 0.9530 | 0.9580 | 0.8990 | 0.9080 | 0.9650 | 0.0150 | 0.0470 | 0.0420 | 0.1010 | 0.0920 | 0.0350 |
| Confidentiality | 0.9770 | 0.8900 | 0.8470 | 0.9110 | 0.9110 | 0.9610 | 0.0230 | 0.1080 | 0.1530 | 0.0890 | 0.0890 | 0.0390 |
| Accountability | 0.8900 | 0.9740 | 0.9410 | 0.8640 | 0.8940 | 0.8460 | 0.0450 | 0.0230 | 0.2410 | 0.1230 | 0.1420 | 0.0012 |
| Consumer Integrity | 0.8520 | 0.8920 | 0.9540 | 0.9430 | 0.8430 | 0.9420 | 0.0450 | 0.0210 | 0.0350 | 0.0400 | 0.0410 | 0.0310 |
| Survivability | 0.9290 | 0.9050 | 0.9280 | 0.8990 | 0.9110 | 0.8640 | 0.0230 | 0.0450 | 0.0120 | 0.0140 | 0.0650 | 0.0340 |

shown the final dependent weights of factors through the hierarchy.

After getting the final or dependent weights of security-durability factors, authors have to evaluate the influence of security-durability in different alternatives. In this work, six successive projects of two different Web applications have been taken to evaluate the security-durability. Where, A1, A2, A3 represent the project of entrance exam based web applications and A4, A5, A6 represent the project of quiz competition based web applications. Due to the security of the institutional information, all projects are very sensitive. With the help of step 10 and equation (1-5), authors took the inputs on the technological data of the six projects as shown in table 8. From the equations (16-18), authors estimated normalized fuzzy decision matrix and weighted normalized fuzzy decision matrix as obtained in table 9 and table 10. From the equation (18-24), authors estimated the distance between alternatives and ideal solutions as shown in table 11. From the equations (25-26), authors estimated the relative closeness as shown in table 12.

From table 12, it can be deduced that alternatives are relatively closer to each other. Hence, the security-durability of different alternatives is in good condition according to the case study. When we analyzed the values in Table 12, we observed that the Alternative A5 is performing extremely poor in security-durability of web application, while Alternative A4 is scoring extremely well in security-durability. Hence alternative A4 is best among the six alternatives.

## VI. COMPARISON BETWEEN AHP-TOPSIS METHODS

When used with different methods, similar data give different results [37]. Researchers use one or more techniques to check the accuracy of the results obtained through the proposed technique [38]. To estimate the results using a different method and to evaluate the accuracy of the results using Hesitant-Fuzzy-AHP-TOPSIS, contributors of the study used Classical AHP-TOPSIS [39], Fuzzy-AHP-SAM (Analytic Hierarchy Process-Simple Aggregation Method) [4] and Fuzzy AHP-TOPSIS methods [13]. Hesitant Fuzzy Sets (HFS) in a short time got the attention of several researchers because hesitant circumstances are very popular in widely different-world problems and this new strategy promotes the handling of ambiguity caused by hesitation. A HFS is defined as a function returning a set of membership values for each characteristic within the domain. In fuzzy set, the membership degree has one possible value in [0, 1] at any point, while in hesitant fuzzy set, the membership degree has set some values in [0, 1] at any point. Moreover, in classical AHP-TOPSIS, the data collection and estimation processes are same as in Hesitant-Fuzzy and Fuzzy based AHP-TOPSIS processing without fluctuation. Thus, data in its original numerical form is used to evaluate web application security-durability through Classical AHP-TOPSIS. The comparison of the results are shown in Table 13.

**TABLE 12.** Relative closeness of the alternatives.

| Alternatives | A1 | A2 | A3 | A4 | A5 | A6 |
|---|---|---|---|---|---|---|
| Relative Closeness (RCi) | 0.3098 | 0.3073 | 0.2612 | 0.3150 | 0.2224 | 0.2630 |

According to Table 13 and Figure 4, alternatives are ranked using four hybrid methods based on AHP. The ordering of alternatives are $A1 > A2 > A4 > A6 > A3 > A5$, $A2 > A1 > A4 > A3 > A6 > A5$, $A1 > A4 > A2 > A6 > A3 > A5$ and $A4 > A1 > A2 > A3 > A6 > A5$ using HF-AHP-TOPSIS, Fuzzy-AHP-TOPSIS, Fuzzy-AHP-SAM and Classical-AHP-TOPSIS methods, respectively. The findings produced by the approaches are highly correlated with the results attained by the methodology. With the help of statistical assessment, values of Pearson Correlation Coefficient (PCC) between HF-AHP-TOPSIS and Fuzzy-AHP-TOPSIS, Fuzzy-AHP-SAM, Classical-AHP-TOPSIS are 0.99737, 0.986636 and 0.985877, respectively. The results showed that other used methods are highly correlated with proposed approach. Further, an integration of HF-AHP and HF-TOPSIS represents its benefits in relating decision makers with opposing consensus objectives. Systematic approach is advantageous as it allows complex multi-person and multi-criteria decision problems to be solved by evaluating environmental issues and linked to alternative web applications.

## VII. SENSITIVITY ANALYSIS

A sensitivity analysis is defined as getting the set of assumptions by changing the particular variable [4]. In other words, sensitivity analysis study is about how various values of uncertainty in a mathematical model support to the proposed work [38], [39]. In this paper sensitivity analysis was applied

**TABLE 13.** Results through different AHP-TOPSIS approaches.

| Methods/Alternatives | A1 | A2 | A3 | A4 | A5 | A6 |
|---|---|---|---|---|---|---|
| Hesitant-Fuzzy-AHP-TOPSIS | 0.3098 | 0.3073 | 0.2612 | 0.3150 | 0.2224 | 0.2630 |
| Fuzzy-AHP-TOPSIS | 0.3168 | 0.3193 | 0.2536 | 0.3171 | 0.2226 | 0.2525 |
| Fuzzy-AHP-SAM | 0.3089 | 0.2995 | 0.2548 | 0.3085 | 0.2221 | 0.2601 |
| Classical-AHP-TOPSIS | 0.3075 | 0.3020 | 0.2576 | 0.3130 | 0.2224 | 0.2575 |

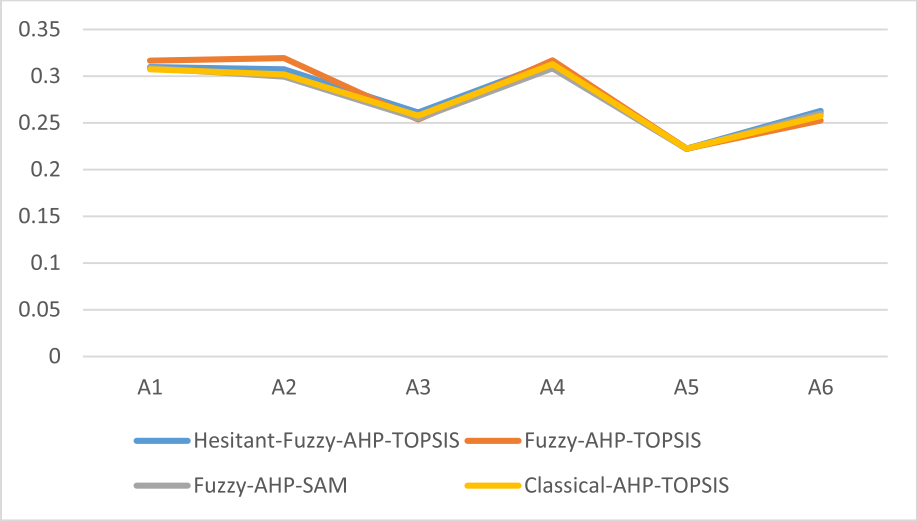


**FIGURE 4.** Graphical representation of comparisons.

**TABLE 14.** Sensitivity analysis of the results.

| Weights/Alternatives | | A1 | A2 | A3 | A4 | A5 | A6 |
|---|---|---|---|---|---|---|---|
| If No Changes in Weights (Original Weights) | Relative Closeness | 0.3098 | 0.3073 | 0.2612 | 0.3150 | 0.2224 | 0.2630 |
| If Reliability=0.1500-0.05= 0.1000 | | 0.2547 | 0.2654 | 0.2166 | 0.2789 | 0.1852 | 0.2165 |
| If Availability=0.1840-0.05= 0.134 | | 0.2233 | 0.2294 | 0.1836 | 0.2395 | 0.1528 | 0.1848 |
| If Authentication=0.0850-0.05= 0.035 | | 0.2950 | 0.2560 | 0.2780 | 0.3040 | 0.1543 | 0.2138 |
| If Maintainability=0.2340-0.05= 0.184 | | 0.3736 | 0.3959 | 0.3392 | 0.4109 | 0.3104 | 0.3355 |
| If Confidentiality=0.0820-0.05= 0.032 | | 0.2460 | 0.2533 | 0.2595 | 0.2575 | 0.2503 | 0.2247 |
| If Accountability=0.1440-0.05= 0.094 | | 0.2807 | 0.3041 | 0.2494 | 0.3240 | 0.2222 | 0.2468 |
| If Consumer Integrity=0.0770-0.05= 0.027 | | 0.2664 | 0.2996 | 0.2448 | 0.3279 | 0.2220 | 0.2413 |
| If Survivability=0.0440-0.05= -0.006 | | 0.3303 | 0.3486 | 0.2944 | 0.3619 | 0.2640 | 0.2918 |

to reveal how the changes on the importance levels of the main criteria affect the results. The authors have changed the weights of these factors by 0.05 and by shifting one factor at a time while the weights of the other factors remained correspondingly the same. Table 14 shows the results in which first no changes were made. Reliability weight is reduced by 0.05 and others were taken as stable. The results of alternatives are shown in table 14.

It should also be noted that the selection process for the best alternative is not sensitive to the changes in the importance level in Table 14. Also the figure 5 shows that the results are not sensitive to the changes. As the final observations of the sensitivity analysis, the decision makers should be informed that no matter what the factor weights are, the fourth alternative (A4) will always be the best of all alternatives.The results achieved through sensitivity analysis point towards a well-adjusted atmosphere about experts' judgments and this would ensure accuracy. It is found through the sensitivity analysis that the discrepancy between the results is negligible.

## VIII. DISCUSSION

Security of web application is required for secure system because sensitive information is always at risk. It is difficult to find the contribution of security at early stage of web application development process which has negative or positive impact on the other significant aspects. Latest report of IBM and Ponemon institute states that average total cost of a data breach has been increased and it is now 3.86 million US dollars [41], [42]. In May 2019, not only was Whats App of several users hacked, but the surveillance cameras located on these Whats App users' phone were also hacked [43]. These breaches and maintenance issues shows that need for longer security is even more compelling now due to the number of breaches happening every year. Further, security has always

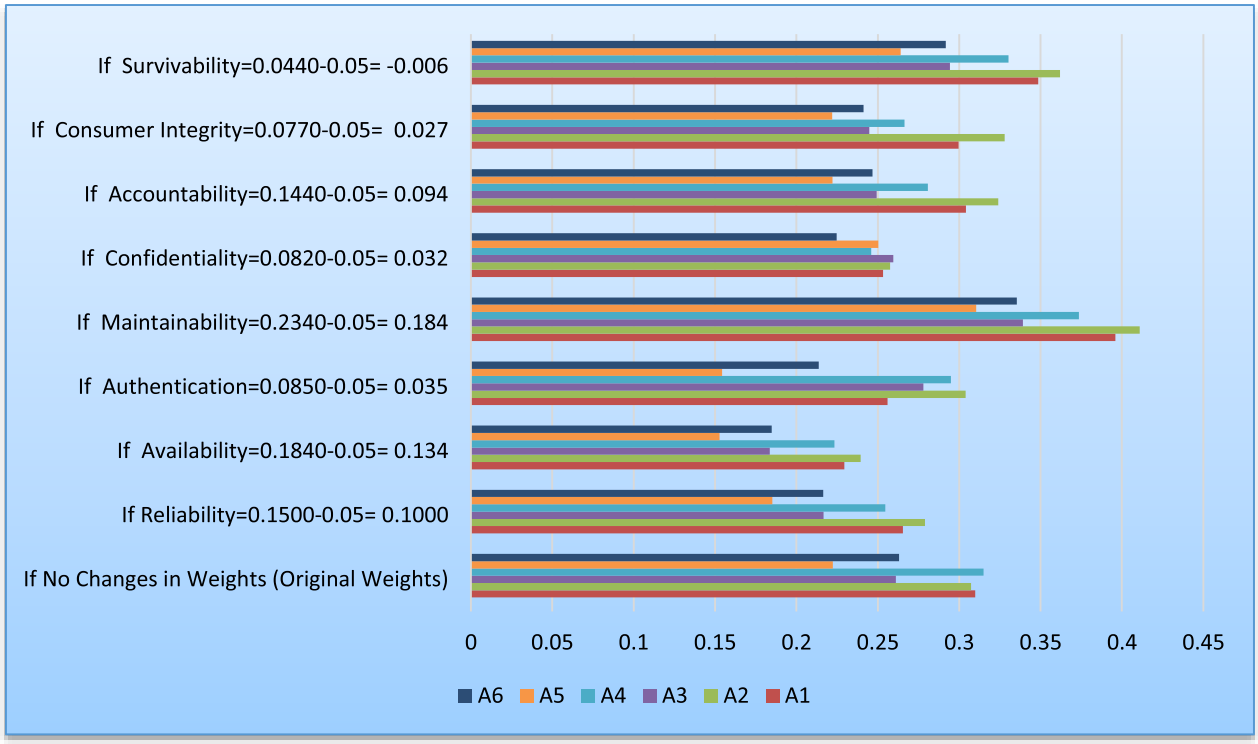


**FIGURE 5.** Graphical representation of sensitivity analysis.

influenced the quality of web application. Developers and development organizations carry loads to develop durable web application with high security. Practitioners spent lots of money to deal with long run security in web application, but unfortunately, most of the web application is still non-durable and insecure. Thus, practitioners are always exploring new techniques or methods for evaluating and estimating the security of web application services to satisfy the users and for giving them security assurance for a longer life-span. In this row, estimation of security-durability provides a novel vision for developing secure as well as durable web application.

There are a number of existing models that incorporate maintenance in the web application development life cycle. However, there is a dearth of work that focuses on longevity and security of web applications while reducing the time and cost incurred in maintenance. Security-durability estimation describes about the same problem and provides solution. After the thorough literature review of the related fields, it is found that MCDM methodology (Specifically AHP and hesitant fuzzy) not only improved the accuracy of security estimation, but is also more objective at the same time. These statements are even truer in the case of web application security because the growth of security is still in its infancy and there are very limited established references. The main aim of this work is to address the security-durability that can provide a solution with higher security for web application services that may be enhanced through the estimation. Estimation of security-durability is another approach to attain a high level of sustained security. Therefore, the approach of this report is treating various issues including durability, optimal security maintenance, reducing cost and time to maintain security for longer use. The main benefits of security-durability estimation are specified below:

- Security-durability is a persistent problem of this age and it is neglected while it needs to be remedied urgently. This assessment cum prioritization would aid the developers to understand the design of security-durability.
- As assessment is the sole method for attaining security-durability, the contribution of the article incorporates security as well as durability factors and assesses security-durability of web application.
- The most prioritized factors are the dependability in level 1 and maintainability in level 2 according to the results. This affirmation will further help in focusing on the prioritized factors for accomplishing high security-durability.
- For determining the useful and important attribute among the numbers of attributes for security-durability, the outcomes of this research work will help the developers and security practitioners.
- Authors of this research work have assessed security-durability variables. With the support of the results, security-durability considerations can be brought into focus when integrating security-durability into web application.
- The estimated weights of different factors contributing towards security-durability will also facilitate the security practitioners' task.

Quantitative analysis of security-durability is crucial to measure the impact of security-durability at early development process. The model proposed to assess the security-durability of web application uses three primary key factors including dependability, human trust and trustworthiness. However, there are a few limitations to this approach also and these are as follows:

- The data collected for website may be small as website is locally developed. Results may vary for different databases.
- There might be more significant factors that may not have been considered by the authors while estimating security- durability of this web application.
- More factors may be included with variations in results.
- Data collection tool may be changed and other methods that may give more unambiguous results can be used in future.

## IX. CONCLUSION

The latest issue regarding the development of web applications that afford security as well as durability calls for immediate attention of the researchers and practitioners. The purpose of this study is to assess the security-durability during web application development. For the determination, the method prioritizes the factors based on their impact on security-durability for developers. Furthermore, this study also recommends that security estimation must be done in the initial stages of development of web applications. The methodology proposed in the study and the results drawn from a real time project of web applications being used in BBA University will facilitate new activities and ideas for security-durability of web application development. In future, estimation of security-durability can be done with other factors that affect the security. Also different methodologies of soft computing and statistics can be further used to evaluate the security-durability.

## ACKNOWLEDGMENT

This Project was funded by the Deanship of Scientific Research (DSR), King Abdulaziz University, Jeddah, under Grant D-234-611-1441. The authors, therefore, gratefully acknowledge DSR technical and financial support.

## REFERENCES

[1] A. Cahn, S. Alfeld, P. Barford, and S. Muthukrishnan, "An empirical study of Web cookies," in *Proc. 25th Int. Conf. World Wide Web (WWW)*, vol. 5, 2016, pp. 891–901.
[2] (2019). *Top Cybersecurity Data Breaches of (so far)*. [Online]. Available: https://www.appknox.com/blog/top-cybersecurity-data-breaches-2019
[3] A. Ullah, H. Xiao, and T. Barker, "A study into the usability and security implications of text and image based challenge questions in the context of online examination," *Edu. Inf. Technol.*, vol. 24, no. 1, pp. 13–39, Jun. 2018.
[4] A. Agrawal, M. Zarour, M. Alenezi, R. Kumar, and R. A. Khan, "Security durability assessment through fuzzy analytic hierarchy process," *PeerJ Comput. Sci.*, vol. 5, p. e215, Sep. 2019.
[5] N. Ensmenger, "When good software goes bad: The surprising durability of an ephemeral technology," in *Proc. Maintainers, Stevens Inst. Technol.*, Oct. 2016, pp. 1–14, [Online]. Available: https://larlet.fr/static/david/blog/ensmenger-maintainers-v2.pdf
[6] (2019). *Top Software Failures in Recent History*. [Online]. Available: https://www.computerworld.com/article/3412197/top-software-failures-in-recent-history.html
[7] A. Mardani, A. Jusoh, K. Nor, Z. Khalifah, N. Zakwan, and A. Valipour, "Multiple criteria decision-making techniques and their applications-a review of the literature from 2000 to 2014," *Econ. Res.-Ekonomska Istra ivanja*, vol. 28, no. 1, pp. 516–571, 2015.
[8] J. J. Cusick, *Durable Ideas in Software Engineering: Concepts, Methods and Approaches From my Virtual Toolbox*. Bentham Science, 2013, doi: 10.2174/97816080547631130101.
[9] S. Cevik Onar, B. Oztaysi, and C. Kahraman, "Strategic decision selection using hesitant fuzzy TOPSIS and interval Type-2 fuzzy AHP: A case study," *Int. J. Comput. Intell. Syst.*, vol. 7, no. 5, pp. 1002–1021, Sep. 2014.
[10] S. Chong, K. Vikram, and A. C. Myers, "SIF: Enforcing confidentiality and integrity in Web applications," in *Proc. USENIX Secur. Symp.*, 2018, pp. 1–16.
[11] A. Özdağoğlu, K. Yilmaz, and E. Çirkin, "An integration of HF-AHP and ARAS techniques in supplier selection: A case study in waste water treatment facility," *Dokuz Eylul Universitesi Iktisadi ve Idari Bilimler Dergisi*, vol. 33, no. 2, pp. 477–497, Jan. 2019.
[12] L. Zhu, A. Aurum, I. Gorton, and R. Jeffery, "Tradeoff and sensitivity analysis in software architecture evaluation using analytic hierarchy process," *Softw. Qual. J.*, vol. 13, no. 4, pp. 357–375, 2015.
[13] 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.
[14] J. Elmi and M. Eftekhari, "Dynamic ensemble selection based on hesitant fuzzy multiple criteria decision making," *Soft Comput.*, pp. 1–13, Jan. 2020.
[15] A. Basar, "An expert system methodology for planning IT projects with hesitant fuzzy effort: An application," in *Industrial Engineering in the Big Data Era*. Springer, 2019, pp. 3–18, doi: 10.1007/978-3-030-03317-0_1.
[16] R. Kumar, M. Zarour, M. Alenezi, A. Agrawal, and R. A. Khan, "Measuring security durability of software through fuzzy-based decision-making process," *Int. J. Comput. Intell. Syst.*, vol. 12, no. 2, pp. 627–642, 2019.
[17] *Introduction to Software Engineering*. [Online]. Available: http://csis.pace.edu/~marchese/SE616_New/Sum_11/Sum_11.htm
[18] *Trustworthiness in Web Design: 4 Credibility Factors*. [Online]. Available: https://www.nngroup.com/articles/trustworthy-design/
[19] *Dependability vs Survivability vs Trustworthiness*. [Online]. Available: http://webhost.laas.fr/TSF/IFIPWG/Workshops&Meetings/42/01-Laprie.pdf
[20] C. Kelty, S. Erickson, *The Durability of Software*. Berlin, Germany: Meson Press, 2015, pp. 1–13.
[21] C. Knittel, R. Feenstra, "Re-assessing the U.S. Quality adjustment to computer prices: The role of durability and changing software," in *Proc. Working Paper Dept. Econ.*, 2004, pp. 2–50.
[22] D. Linden, A. Rashid, "The effect of software warranties on cybersecurity," *ACM SIGSOFT Soft. Eng. Notices* vol. 43, no. 4, pp. 31–35, 2018.
[23] R. Kumar, S. A. Khan, R. A. Khan, "Durability challenges in software engineering," *crosstalk, J. Defense Soft. Eng.*, vol. 10, pp. 29–31, Jul. 2016.
[24] R. Kumar, S. A. Khan, and R. A. Khan, "Revisiting software security: Durability perspective," *Int. J. Hybrid Inf. Technol.* vol. 8, no. 2, pp. 311–322, 2015.
[25] E. Jonsson, "An integrated framework for security and dependability," in *Proc. Workshop New Secur. Paradigms*, 1998, pp. 22–29.
[26] D. J. Hand,"Aspects of data ethics in a changing world: Where are we now?" *Big Data*, vol. 6, no. 3, pp. 176–190, Sep. 2018.
[27] V. Mohammadi, A. M. Rahmani, A. M. Darwesh, and A. Sahafi, "Trust-based recommendation systems in Internet of Things: A systematic literature review," *Hum.-Centric Comput. Inf. Sci.*, vol. 9, no. 1, pp. 21–27, Jun. 2019.
[28] V. Torra and Y. Narukawa, "On hesitant fuzzy sets and decision," in *Proc. IEEE Int. Conf. Fuzzy Syst.*, Aug. 2009, pp. 1378–1382.
[29] R. M. Rodriguez, L. Martinez, and F. Herrera, "Hesitant fuzzy linguistic term sets for decision making," *IEEE Trans. Fuzzy Syst.*, vol. 20, no. 1, pp. 109–119, 2011.
[30] R. M. Rodríguez, L. Martínez, V. Torra, Z. S. Xu, and F. Herrera, "Hesitant fuzzy sets: State of the art and future directions," *Int. J. Intell. Syst.*, vol. 29, no. 6, pp. 495–524, Apr. 2014.
[31] F. Wang, X. Li, and X. Chen, "Hesitant fuzzy soft set and its applications in multicriteria decision making," *J. Appl. Math.*, vol. 2014, Jun. 2014, Art. no. 643785, [Online]. Available: https://www.hindawi.com/journals/jam/2014/643785/

[32] I. Beg and T. Rashid, "TOPSIS for hesitant fuzzy linguistic term sets," *Int. J. Intell. Syst.*, vol. 28, no. 12, pp. 1162–1171, Aug. 2013.
[33] M. Xia and Z. Xu, "Hesitant fuzzy information aggregation in decision making," *Int. J. Approx. Reasoning*, vol. 52, no. 3, pp. 395–407, 2011.
[34] Y.-J. Lai, T.-Y. Liu, and C.-L. Hwang, "TOPSIS for MODM," *Eur. J. Oper. Res.*, vol. 76, no. 3, pp. 486–500, Aug. 1994.
[35] K. Sahu and R. K. Srivastava, "Soft computing approach for prediction of software reliability," in *Proc. ICIC*, 2018, pp. 1213–1222.
[36] K. Sahu and Rajshree, "Stability: Abstract roadmap of security," *Amer. Int. J. Res. Sci., Eng. Math.*, vol. 2, no. 9, pp. 183–186, Dec. 2015.
[37] Z. Xiling and L. Xiangchun. (2005). *Effective User Interface Design for Consumer Trust: Two Case Studies*. [Online]. Available: http://www.diva-portal.org/smash/get/diva2:1024188/FULLTEXT01.pdf
[38] K. Sahu and R. K. Srivastava, "Revisiting software reliability," *Data Management, Analytics and Innovation, Advances in Intelligent Systems and Computing*. Springer, 2019, pp. 221–235, doi: 10.1007/978-981-13-1402-5_17.
[39] K. S. Trivedi, D. S. Kim, A. Roy, and D. Medhi, "Dependability and security models," in *Proc. 7th Int. Workshop Des. Reliable Commun. Netw.*, vol. 12, Oct. 2009, pp. 11–20.
[40] K. Sahu, R. Shree, and R. Kumar, "Risk management perspective in SDLC," *Int. J. Adv. Res. Comput. Sci. Softw. Eng.*, pp. 1247–1251, Mar. 2014.
[41] *Average Total Cost of a Data Breach Has Increased to $3.86 million—Global Study*. [Online]. Available: https://www.appknox.com/blog/cost-of-a-data-breach#
[42] *What is Reliability*. [Online]. Available: https://www.igi-global.com/dictionary/markovian-reliability-in-multiple-agv-system/25011
[43] *The Biggest Hacks Of 2019 So Far*. [Online]. Available: https://www.businessinsider.in/The-biggest-hacks-of-2019-so-far/An-unprecedented-iPhone-hack-targeted-Uighur-Muslims-in-China/slideshow/71086437.cms

**RAJEEV KUMAR** received the master's and Ph.D. degrees in information technology from Babasaheb Bhimrao Ambedkar University (A Central University), Lucknow, India, in 2014 and 2019, respectively. He is currently working as a Guest Faculty Member at the Department of Information Technology, Babasaheb Bhimrao Ambedkar University (A Central University). He is also young and energetic researcher and has worked on a Full Time Major Project funded by the University Grants Commission, New Delhi, India. He has more than five years of research and teaching experience. He has also published and presented articles in refereed journals and conferences. His research interest is in the different areas of security engineering.

**ASIF IRSHAD KHAN** is working as an assistant professor in the Computer Science Department at King Abdulaziz University, Jeddah, Saudi Arabia. He has over fifteen years of experience as a professional academician and researcher. He published several research articles in leading international journals and conferences. His current research interest includes Software Engineering with a focus on Software Security, Component-based Software Engineering and Software Product Line Engineering.

**YOOSEF B. ABUSHARK** is currently an Assistant Professor with the Computer Science Department, King Abdulaziz University (KAU). His research interests are in software engineering with a focus engineering intelligent systems and building agent-based simulations. He has been publishing several research outcomes in leading venues.

**MD MOTTAHIR ALAM** has six years of experience as a Software Engineer (quality) for leading software multinationals, where he worked on projects for companies like Pearson and Reader's Digest. He is currently an ISTQB Certified Software Tester and working as a Faculty Member with the Department of Electrical and Computer Engineering, King Abdulaziz University, Jeddah. He published several research articles in leading journals and conferences. His research interests include software engineering, especially in software product line engineering, and software reusability and component- and agent-based software engineering.

**ALKA AGRAWAL** received the Ph.D. degree from Babasaheb Bhimrao Ambedkar University, (A Central University), Lucknow. She is currently working as an Assistant Professor at Babasaheb Bhimrao Ambedkar University, (A Central University). She is also a passionate Researcher and has also published a number of research articles in national and international journals. She has research/teaching experience of more than 12 years. Her areas of research include software security and software vulnerability. She is also working in the fields of big data security, genetic algorithms, and software security.

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