International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-9 Issue-4, February 2020

Optimizing the Impact of Security Attributes in Requirement Elicitation Techniques using FAHP

Virendra Singh, Dhirendra Pandey, Kavita Sahu, Mohd Waris Khan

Abstract: ***Software security is a key issue in the domain of software engineering which attracts attention from both the industry and academia. Besides, due to the massive investment in software development, security is in much demand. The selection of appropriate software development model is an increasingly challenging task. Security attributes play a vital role while designing security during software development. Each attribute has its importance during requirement elicitation procedure. This is based upon the user's demand, organization resources, and sensitivity of the information. Hence, developers should understand the significance of each attribute while collecting the user requirements for developing software. In this paper, authors have proposed an approach for prioritization of these attributes using the Fuzzy Analytic Hierarchy Process (Fuzzy AHP) method. A literature survey reveals that critical security attributes such as Integrity, confidentiality, Authentication, Effectiveness, Availability, Access Control and Authorization. This will help developers to improve software security for longer.***

Keywords: Software Security, Priority Assessment, Fuzzy Analytic Hierarchy Process, Security Requirements, Security Factors

I. INTRODUCTION

Throughout the software development process, major quality factors like maintenance, a security requirement, and safety etc. are always considered. Nowadays, after delivering the code to the end-users, developers face security requirement-related issues. Software is not usable because of the high-security design as it might be [1-2]. Practitioners are trying to solve this problem. Application functionality improves if protection can be used. Although Protection refers to preventing un-authorization, security requirement ensures code formula keeping simple. The company, therefore, requires user-friendly software security products to boost revenue. Many software security requirements attribute to influence the functionality of security services, including Authentication, Authorization, and Integrity which directly and indirectly affect Effectiveness, confidentiality, Access Control, and Availability. So, developers are trying to gather quality requirements to develop secure software.

Revised Manuscript Received on February 28, 2020.

***** Correspondence Author

Virendra Singh*, Department of Inforamation Technology, Babasaheb Bhimrao Ambedkar University,Lucknow-226025, Uttar Pradesh, India

Dhirendra Pandey, Department of Inforamation Technology, Babasaheb Bhimrao Ambedkar University, Lucknow-226025, Uttar Pradesh, India

Kavita Sahu, Department of Computer Science , Dr Shankutala Misra National Rehabilation University, Lucknow-226017 Uttar Pradesh, India

Mohd Waris Khan, Department of Inforamation Technology, Babasaheb Bhimrao Ambedkar University, Lucknow-226025, Uttar Pradesh, India

Although security and security requirement makes a negative relationship with each other hence, as a result, when security requirement increases the software security also get increased [3-5]. However, some security requirement factors have a positive impact on security services, including efficiency that has a positive effect on safety. Unfortunately, no effort was made during software development to develop security requirement attributes architecture. The importance of attributes in software security architecture plays a vital role [6-7]. In the field of prioritizing security requirement attributes and security attributes, a lot of research has been done. But few effort to prioritize security requirement attributes to maximize the use of security services has been documented in the literature [1, 3-6, 9, 12, 23]. Security technology's success depends mainly on user acceptance, and security requirement attributes services are the primary needs of the user.

Analyzing the security requirement attributes variables found and prioritized is a vital task. Also, assessment of security requirement attributes should not focus solely on security services, but on software services as a whole. Also, successful attribute assessment is necessary to ensure the software's overall security services [8-9]. The decision-makers can undertake correct measures based on the output of the assessment process [10]. Nonetheless, decision-makers need to recognize not only the security requirement attributes factors that contribute to security, but also identify the most useful factors among them, to be able to take appropriate action [11-12]. Therefore, a hierarchy of security requirement attributes is specified in the next section to address the relationship between these factors and Fuzzy AHP is used to prioritize different security requirement attributes. The findings can help security designers during software development to build security requirement attributes services. The remainder of the paper is structured as follows: the second section addresses the value of security requirement, the third section evaluate the impact of security attributes through requirement elicitation process. The fourth section discusses the significance of the results. Section 5 provides the conclusion.

II. NEEDS AND IMPORTANCE

The safety of data is a concept or approach applied to avoid malicious attacks on software. According to McGraw, Computer Security is about developing secure software, i.e., designing secure software, ensuring the software is stable, and informing developers and architects of software and users on how to create secure software [13]. Due to the broad applicability of the code, during the software development process,

security has become a crucial component. Indeed, software faces daily growing threats from various potential malicious opponents, from web-conscious applications running on PCs to complex media communications [14-15].

One of the best ways to get more secure software is to evaluate and retain the CIA during software development stages [16]. That's why everyone builds a high-security design, and because of many complex processes, this much security design contains much fewer security requirements. This problem generates the issues to the end of end-users. Because of the very complicated security architecture, users are unable to use the program with a great deal of ease. Also, the IEEE standard describes security requirements as the degree of user-friendliness by which users can obtain their desired results without making a great deal of effort [17].

However, the odds tend to be contained in safety and security requirements. It is revealed that it affects the other to improve one of them. Techniques have already been developed to incorporate security issues or goals, but an important aspect is missing, i.e., security-security requirement/security requirement attributes. From the very beginning, functionality in security must be integrated into functional security and it should be continued until the security services are in operation. The International Standard Organization (ISO) defines security requirements like the ability to facilitate the user's use of specified services, including efficiency, effectiveness, and satisfaction in a specified use context [18].

Security requirement attributes, according to this definition, focus on the goals of the user (effectiveness), the speed at which objectives are achieved (efficiency), and the satisfaction of the user. Safety, therefore, has three major security requirement factors that indirectly impact, including performance, effectiveness, Such seven features play a crucial role in maximizing software usable-safety services [19].

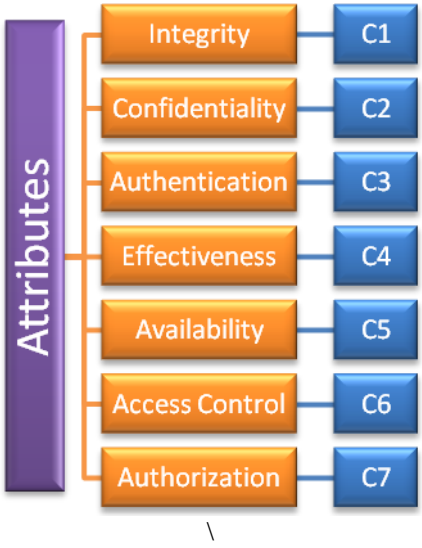

Fig 1: Hierarchy Structure of Security Attributes

Figure 1 shows that performance, Integrity, and Confidentiality are the security requirement factors that also have a positive impact on security services [20]. Authentication is the user's ability to perform a particular task. Effectiveness is captured by calculating the time required to complete a project or the number of attempts made to achieve the important objectives. Availability is essential to determine security requirements because code will fail even if it is functional if it is not acceptable to users. As specified by three security requirement factors, it is clear that these factors also affect the safety of software. Such considerations should, therefore, be included for security requirement attributes assessment.

Thus, to determine the essential attribute among these seven variables, the priorities of security requirement attributes are significant. Furthermore, the security requirement attributes the contribution of each attribute is determined. This paragraph, therefore, addresses prioritizing security requirement attributes variables to improve security services functionality. The accessible safety factors are established through a thorough review of the literature and the views of experts. As discussed earlier, the authors have demonstrated that AHP is one of the best arrangement strategies in a small-scale MCDM issue, as described in this paragraph.

III. SECURITY ATTRIBUTES ASSESSMENT

The objective of this contribution is to identify the priorities of security requirement attributes factors. A questionnaire is being prepared for this. Therefore, to answer the questionnaires, it is important to have a group of experienced experts working in the field of security requirements and safety [21]. Fuzzy AHP is chosen to assess the importance of security requirement attributes factors as it is capable of controlling the participants ' vague judgmental inputs [22]. It can also turn qualitative inputs into quantitative outcomes in the form of weight and rating, which is a better assessment of functional safety. Also, the matrix for the pairwise correlation is constructed using the Fuzzy AHP technique questionnaire. Expert opinions are converted to numerical values to evaluate the weight of security requirement attributes. The formulas (1-3) are used to translate the numeric values to Triangular Fuzzy Number (TFN) [4-6] and are referred to as (l_{ij}, m_{ij}, h_{ij}) where, l_{ij} is value given to if possible, m_{ij} is most likely and h_{ij} is extreme events. Furthermore, the following TFNs are known as: The objective of this contribution is to identify the priorities of security requirement attributes factors. A questionnaire is being prepared for this. Therefore, to answer the questionnaires, it is important to have a group of experienced experts working in the field of security requirements and safety. Fuzzy AHP is chosen to assess the importance of security requirement attributes factors as it is capable of controlling the participants ' vague judgmental inputs [9]. It can also turn qualitative inputs into quantitative outcomes in the form of weight and rating, which is a better assessment of functional safety [12]. Also, the matrix for the pairwise correlation is constructed using the Fuzzy AHP technique questionnaire. Expert opinions are converted to numerical values to evaluate the weight of security requirement attributes. The formulas (1-3) are used to translate the numeric values to Triangular Fuzzy Number (TFN) and are referred to as (l_{ij}, m_{ij}, h_{ij}) where, l_{ij} is value given to if possible,

mij is most likely and hij is extreme events. Furthermore, the following TFNs are known as:

$$\eta ij = [l_{ij} m_{ij} h_{ij}]$$

$$\text{where } l_{ij} \leq m_{ij} \leq h_{ij}$$

$$lij = min(J_{ijk}) \quad (1)$$

$$mij = (J_{ij1}, J_{ij2} \ldots\ldots\ldots\ldots J_{ijk})1/k \quad (2)$$
$$hij = max(J_{ijk}) \quad (3)$$

In the above formulas, Jijk shows the comparative value given by expert k between two criteria. Where i and j are a pair of criteria that participants are judging. For a particular comparison, value is calculated based on the geometric mean of stakeholder scores. The geometric mean is capable of accurately aggregating and reflecting stakeholder consensus and represents the lowest and highest scores for the relative importance of the two parameters, respectively [23-24]. A fuzzy pair-wise comparison matrix in the form of nx n matrix is defined after obtaining the TFN value for each pair of comparison. The size of the matrix is 9x9; twenty-five participants are the group size threshold to achieve an acceptable level of consistency. Participants in this study involve researchers and developers with both security requirements and security experience. To ensure consistency of the AHP analysis, these participants are picked. TFN membership function and pair-wise comparisons are made to generate the fuzzy judgment matrix after qualitative evaluation. The matrix of 25 participants prepared by the researchers is shown in Table 1.

TABLE-I: Fuzzy Pair-Wise Comparison Matrix

	Integrity C1	Confidentiality C2	Authentication C3	Effectiveness C4	Availability C5	Access Control C6	Authorization C7
Integrity C1	1.0000, 1.0000, 1.0000	0.1100, 0.3000, 4.0000	0.1300, 0.5000, 6.0000	0.1100, 0.2200, 4.0000	0.1100, 0.4900, 8.0000	0.1100 , 0.6800, 8.0000	0.1700, 1.5400, 6.0000
Confidentiality C2	-	1.0000, 1.0000, 1.0000	0.1100, 1.2100, 8.0000	0.1100, 0.3100, 5.0000	0.1100, 0.6100, 9.0000	0.1700 , 1.6300, 9.0000	0.1700, 1.2500, 8.0000
Authentication C3	-	-	1.0000, 1.0000, 1.0000	0.1100, 0.1900, 0.5000	0.1100, 0.4400, 6.0000	0.1100, 0.4700, 6.0000	0.1700, 2.2700, 9.0000
Effectiveness C4	-	-	-	1.0000, 1.0000, 1.0000	0.1700, 2.7700, 8.0000	0.1700, 3.700, 9.0000	0.1300, 0.5300, 6.0000
Availability C5	-	-	-	-	1.0000, 1.0000, 1. 0000	0.1700, 1.8200, 9.0000	0.1700, 0.9400, 9.0000
Access Control C6	-	--	-	-	-	1.0000, 1. 0000, 1. 0000	0.1700, 1.3900, 9.0000
Authorization C7	-	--	-	-	-	-	1.0000, 1.0000, 1. 0000

Based on the measured TFN values, defuzzification is performed after the creation of the comparison matrix to generate a quantifiable value. The method of defuzzification adopted in this work was derived from as formulated in equation (4-6), commonly referred to as the process of alpha slicing [25]. A fuzzy set's alpha cut is the set of all elements. The value of the alpha threshold is any value from a scale of 0 to 1. The alpha threshold value was therefore taken as 0.5. Which have an alpha threshold value that is greater than or equal to its membership value, represented by α. Alpha cutting allows one to define a fuzzy set as a crisp set composition. Crisp sets μα,β(βij) define clearly whether or not an element is a part of the set. Equations (4-6) show the method of cutting alpha.

$$\mu_{\alpha,\beta}(\eta_{ij}) = [\beta.\eta_{\alpha}(l_{ij}) + (1-\beta).\ \eta_{\alpha}(h_{ij})] \quad \ldots(4)$$

Therefore,

$$\alpha(l_{ij}) = (m_{ij} - l_{ij}).\alpha + l_{ij} \quad \ldots..(5)$$
$$\alpha(h_{ij}) = h_{ij} - (h_{ij}) = h_{ij} - (h_{ij} - m_{ij}).\alpha \quad \ldots\ldots\ldots(6)$$

α and β are used for expert preferences in these formulas. These two values range from 0 to 1. The result is shown in Table 2 by using formula (4-6) with and at 0.5.

TABLE- II: Defuzzified Pair-Wise Comparison Matrix

	Integrity C1	Confidentiality C2	Authentication C3	Effectiveness C4	Availability C5	Access Control C6	Authorization C7
Integrity C1	1	1.18	1.78	1.14	2.28	2.37	2.31
Confidentiality C2	0.85	1	2.63	1.43	2.58	3.11	2.67
Authentication C3	0.56	0.38	1	0.25	1.75	1.76	3.43
Effectiveness C4	0.88	0.7	4.08	1	3.43	4.14	1.8
Availability C5	0.44	0.39	0.57	0.29	1	3.2	2.76
Access Control C6	0.42	0.32	0.57	0.24	0.31	1	2.99
Authorization C7	0.43	0.38	0.29	0.56	0.36	0.34	1
							C.R.=0.0560

Table 2 shows that the CR value is less than 0.1, so it is right to evaluate AHP. The next step is to determine the Fuzzy pairwise comparison matrix's value and individual vector. The purpose of the matrix calculation is to determine the aggregate weight of specific criteria [24]. Assume that μ denotes the own vector while λ denotes the pair-to-pair comparison matrix of fuzzy.

$$[\mu_{\alpha,\beta}(\eta_{ij}) - \lambda I].\ \mu = 0 \qquad (7)$$

Equation (7) is based on a linear vector transformation where the unit matrix is represented. Through applying formulas (1-7), it is possible to acquire the weights for specific criteria for all other relevant criteria. The security requirement attributes attribute ranks and weights are shown in table 3.

IV. RESULT ANALYSIS

Table 3 displays the aggregated outcome in terms of weight. The results obtained were rated as follows: Integrity (0.0991), confidentiality (0.2704), Authentication (0.1132), Effectiveness (0.2963), Availability (0.0966), Access-Control (0.0670) and Authorization (0.0574). The effectiveness holds the highest priority among these seven attributes, according to the weights and priority.

TABLE- III: Weight and priority attributes

	Weight	Percentages	Ranks
Integrity	0.0991	9.91 %	5
Confidentiality	0.2704	27.04 %	2
Authentication	0.1132	11.32 %	3
Effectiveness	0.2963	29.63 %	1
Availability	0.0966	9.66 %	4
Access Control	0.0670	6.70 %	6
Authorization	0.0574	5.74 %	7

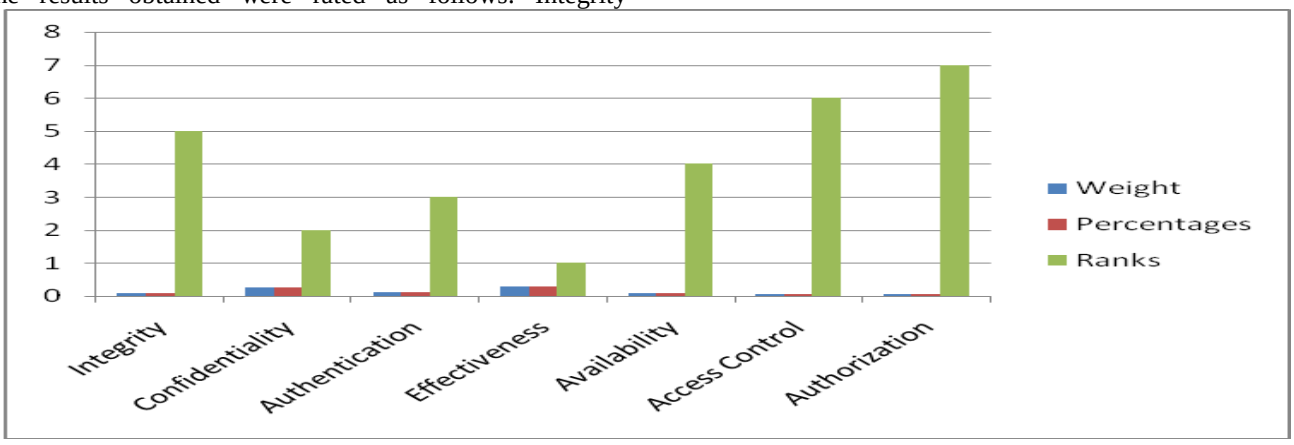

Fig. 2 Grapichal Representation of Weight And Priority Attributes

The satisfaction of the client holds the highest priority among these seven attributes, according to the weights and priority. There are different security requirement attributes in the actual scenario that are present in the process of software development. In this study, only seven security requirement attributes have been defined and prioritized, affecting security. AHP is used as another tool to verify the results. Table 4 demonstrates correlations between Fuzzy AHP and AHP methods

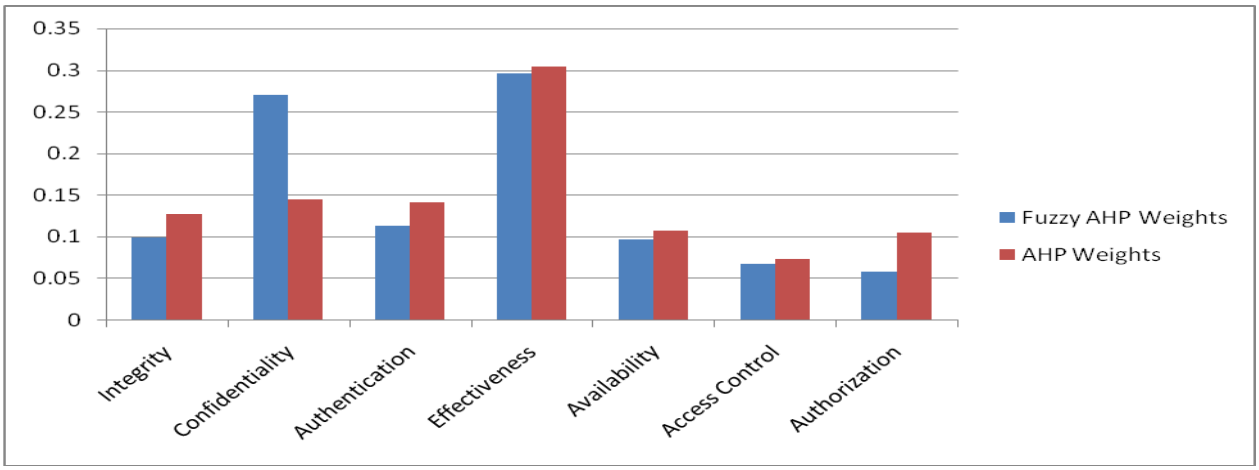

Fig. 3 Graphical Represenation of the Comparision

A comparison between the two methods is shown in Table 4. For accuracy of calculation, we compare it with AHP. The difference between these two methods is negligible. A correlation coefficient is 0.97925. This prioritization further helps to calculate the impact of these attributes on security requirement. This research also tries to provide a new methodology for calculating numeric measures from the

TABLE -IV: Difference between fuzzy AHP and AHP

Attributes	Fuzzy AHP		AHP	
	Weights	*Priority*	*Weights*	*Priority*
Integrity	0.0991	5	0.1268	4
Confidentiality	0.2704	2	0.1448	2
Authentication	0.1132	3	0.1405	3
Effectiveness	0.2963	1	0.3038	1
Availability	0.0966	4	0.1072	5
Access Control	0.067	6	0.0727	7
Authorization	0.0574	7	0.1042	6

qualitative ones while prioritizing the security attributes.

Priority wise categorization of security attributes helps developers to focus on fulfilling the user's demand and enhancing the level of security for a longer duration. The proposed work aims to establish a hierarchy that can be used in security design. It aids the security developer to identify the key security attributes essential for the successful development of stable and secure design. The gradual increase in the use of software systems has resulted in the complexity of such systems. Consequently, a more secure system is needed. The quality of software security is getting attention from both the designers and the end users. This work has examined seven security attributes while designing security during software development. This will help to easily apply the security management plan during software development. The major significances of the work are as follows.

- Working on security will enhance the security of software.
- Focusing on effectiveness, confidentiality, and authentication during software development will improve security.
- Effectiveness is the most important as well as a relevant factor of security requirement to be enhanced to get a secure service life of the software.

All in all, this contribution prioritizes security attributes, which strengthens the fact that effectiveness and confidentiality should be given top priority when designing secure software.

V. CONCLUSIONS

In this research, an extensive literature review was done to identify the significant security attributes affecting the secure software. Upon that, a hierarchical structure of attributes is proposed.

Next, the opinion of twenty experts on the seven security attributes and among them three high priority factors are i.e., effectiveness, confidentiality, and authentication. The experts are from the software industry as well as academia. Using this opinion, the weights of each factor have been calculated with the help of fuzzy AHP. It has been concluded that effectiveness is the most critical factor among the seven main security elicitation factors. For the assurance of software security, developers need to focus on effectiveness for security of the software firstly.

REFERENCES

1. Kumar R, Khan S. A. Khan R. A., (2016), Durability Challenges in Software Engineering, CrossTalk, The Journal of Defense Software Engineering Volume 42, Issue 4, pp.29-31.
2. Pressman, R.S., (2005), Software Engineering: A Practitioner's Approach, Palgrave Macmillan, London.

3. Alka Agrawal, Mamdouh Alenezi, Rajeev Kumar, Raees Ahmad Khan, (2019), Measuring the Sustainable-Security of Web Applications through a Fuzzy-Based Integrated Approach of AHP and TOPSIS, IEEE Access, Volume 7, 2019, pp. 153936-153951, Nov-2019.
4. Alka Agrawal, Mamdouh Alenezi, Dhirendra Pandey, Rajeev Kumar, Raees Ahmad Khan, (2019), Usable-Security Assessment through a Decision Making Procedure, , ICIC Express Letters-Part B, Applications, Volume 12, Number 9, 2019.
5. Mamdouh Alenezi, Rajeev Kumar, Alka Agrawal, Raees Ahmad Khan, (2019), Usable-Security Attribute Evaluation using Fuzzy Analytic Hierarchy Process, ICIC Express Letters-An International Journal of Research and Surveys, Volume 13, Number 6, 2019.
6. Mohd Waris Khan, Dhirendra Pandey, Suhel Ahmad khan "Measuring the Security Testing Attributes through Fuzzy Analytic Network Process: A Design Perspective", Jour of Adv Research in Dynamical & Control Systems, Vol. 10, 12-Special Issue, 2018
7. Fléchais, I., (2005) Designing Secure and Usable Systems. Dissertation, University College London. ISO 9241-11:1998 (1998), Ergonomic Requirements for Office Work with Visual Display Terminals, The International Organization for Standardization, Geneva.
8. Anshul Mishra, Devendra Agrawal, M H Khan, "Confidentiality Estimation Model : Fault Perspective", International Journal of Advance Research in Computer Science,Volume 8, Issue 5, pp 2328-2332, 2017.
9. Kulyk O., Volkamer M., (2018), Usability is not Enough: Lessons Learned from' Human Factors in Security, Research for Verifiability. E-Vote-ID 2018, pp. 66.
10. Hansen, J., Porter, K., Shalaginov, A., Franke, K., (2018), Comparing Open Source Search Engine Functionality, Efficiency and Effectiveness with Respect to Digital Forensic Search, NISK 2018, Issue 108.
11. Ruoti, S., Roberts, B., Seamons, K., (2015), Authentication Melee: A Usability Analysis of Seven Web Authentication Systems, Report of the International World Wide Web Conferences Steering Committee, pp. 916-926.
12. Liu, Y., (2011), Analyzing Facebook Privacy Settings: User Expectations vs. Reality, ACM SIGCOMM.
13. Tilson, R., (1998), Factors and Principles Affecting the Usability of Four E-Commerce Sites. Proceedings of the 4th Conference on Human Factors & the Web, Basking Ridge, New Jersey.
14. Computer Hope, (2018), Availableat: http://www.computerhope.com/jargon/p/privacy.htm last visit Nov 05 2018.
15. Beckles B., Welch V., Basney J., (2005), Mechanisms for Increasing the Usability of Grid Security, International Journal of Human Computer Studies, Volume 63, Issue 12, pp.74-101.
16. Alexander I., Neil M., (2004), Scenarios, Stories and Use Cases. John Wiley.
17. Good N. S., Krekelberg A., (2003), Usability and Privacy: A Study of Kazaa P2P File Sharing, Human Factors in Computing Systems, ACM, pp. 137–144.
18. Whitten A., (2004), Making Security Usable, Ph.D. Dissertation, Carnegie Mellon University.
19. Saltzer J.H., Schroeder M.D., (1975), The Protection of Information in Computer Systems, IEEE, Volume 63, Issue 9, pp. 1278–1308.
20. McGraw G., (1999), Software Assurance for Security, IEEE Computer, Volume 32, Issue 4, pp. 103-105.
21. Mahoney M. S., (2004), What Makes the History of Software Hard, IEEE Annals of the History of Computing, Volume 30, Issue 3, pp. 8-18.
22. Technical White Paper on Reducing Security Attributes from Open Source Software, (2018) Available at: http://h20195.www2.hp.com/v2/GetPDF.aspx/4AA0-8061ENW.pdf last visit Nov 10 2018.
23. Saaty T. L., (1980), The Analytic Hierarchy Process, McGraw Hill: New York.
24. Mohd Waris Khan, D. Pandey and S. A. Khan, "Test Plan Specification using Security Attributes: A Design Perspective", ICIC Express Letters, no.12 (10), pp. 1061-1069, 2018.
25. Rajeev Kumar, Mohammad Zarour, Mamdouh Alenezi, Alka Agrawal, Raees Ahmad Khan, (2019), Measuring Security-Durability through Fuzzy Based Decision Making Process, International Journal of Computational Intelligence Systems, Volume 12, June, 2019.