ICIC Express Letters
Volume **12**, Number **10**, October **2018**

ICIC International ©2018 ISSN 1881-803X
pp. 1053–1059

SECURITY ASSESSMENT THROUGH FUZZY-DELPHI ANALYTIC HIERARCHY PROCESS

Rajeev Kumar[1], Suhel Ahmad Khan[2], Alka Agrawal[1,*] and Raees Ahmad Khan[1]

[1]Department of Information and Technology
Babasaheb Bhimrao Ambedkar University (A Central University)
Vidya Vihar, Raebareli Road, Lucknow 226025, India
rs0414@gmail.com; khanraees@yahoo.com; *Corresponding author: alka_csjmu@yahoo.co.in

[2]Department of Computer Science
Indira Gandhi National Tribal University, Amarkantak
Amarkantak, Madhya Pradesh 484887, India
ahmadsuhel28@gmail.com

Received January 2018; accepted April 2018

Abstract. *During the software development process, selection of most appropriate attribute is the fundamental challenge for security design. To fulfill the security requirements specifications of software, selection procedure of security attributes plays a key role. Hence, selection of security attributes is a multi-criteria decision making problem. This article investigates the basic security attributes and assesses the priority through fuzzy-Delphi analytical hierarchy process method. Five most appropriate attributes have been taken from review of literature and best practices. The hybrid technique of fuzzy-Delphi and AHP helps software developers to decide the ranks of suitable security attributes in a consistent way. Further, the results may be helpful for developers to facilitate the security attributes during software development.*
Keywords: Software security, Security factors, Analytic Hierarchy Process (AHP), Fuzzy-Delphi method

1. **Introduction.** Security has always influenced the quality of software. Secure software is required for secure system because sensitive information is always at risk. Practitioners spent lots of money dealing with it, but unfortunately, most of the software is still insecure [1,2]. Developers and development organizations have very load to develop more and more software in minimum time. Thus, developers are often confused in selection of important attributes during software development. These attributes affect security design of software. In addition, to fulfill security requirements, which one will improve security more than other attributes is a big question among developers. Practitioners are always searching new techniques or methods for solving conflicting problem in selection of attributes to users' satisfaction.

It is being very hard to find the most appropriate attributes which have negative or positive impact on each other. From the review of literature and best practices, many security attributes are identified. This paper discusses five key attributes of security, i.e., confidentiality, integrity, authentication, availability and authorization [5,6,8]. To gain the individual weightages of attributes it is required to prioritize them through some methodology. In this problem there are multiple criteria of attributes to estimate the priorities of security attributes; hence in this research this problem is considered as MCDM problem. There should be a method which is based on MCDM (Multi-Criteria Decision Making) technique to prioritize the security attributes on the basis of weightages

DOI: 10.24507/icicel.12.10.1053

and ranking [3,4]. Fuzzy Delphi method is a solution to the problem of periodization of security attributes. Delphi method itself is full of vagueness and does not provide precise results to any problem. Hence hybridization of it with fuzzy is proposed here for prioritization of security attributes. Removing vagueness and imprecision from linguistic variables is the characteristic of fuzzy methods. With the help of this hybrid technique, security performance, maintenance cost minimization, and environmental flexibility of software development can be improved. With the help of hybrid technique, this paper gives the priorities and weightages of security attributes. The rest of the paper is organized as follows. In Section 2, fuzzy-Delphi analytic hierarchy process is defined. In Section 3 results of the case study for developers are given. In Section 4, conclusion is given.

2. **Fuzzy-Delphi Analytic Hierarchy Process.** During development, several security attributes influence each other. Importance of security attributes is useful to improve security design for user's satisfaction. An unsuitable selection of security attributes may outcome in failure of security of software. In addition, security failure affects output, effectiveness, and reputation of the organization's business. For right selection of security attributes, Multi-Criteria Decision Making (MCDM) is used in development organization to enhance the security of software [5-7]. It may be helpful to manage the security for longer duration. The method of MCDM includes establishing criteria, evaluating alternatives, application of a ranking system, and assessing criteria weights [6]. Different types of MCDM usually construct different results for a set of alternative decisions related to several criteria. One of the wide uses of MCDM is Analytic Hierarchy Process (AHP) [6,7].

In AHP technique, assessment is executed through ratio-scale pairwise judgments [6-8]. It is also used for simplifying decision making by initial opinions, feelings and judgments into a multilevel categorization process that influences the domain of decisions. This is one of the best commonly used MCDM techniques, which has been applied for determining unstructured problems at early stage of software development [6,7]. Decision makers or practitioners share their knowledge in order to set up a tree of hierarchy process. Further, the security problems would make it hard for practitioners to use their information perfectly. To solve the problem, practitioners are using vague terms for acceptance of decisions. Within the scope of MCDM technique, fuzzy set theory has given a significant contribution for accepting uncertainty and inconsistent judgments, such as the nature of human decision making which was not well tackled in classical AHP [6,7].

Fuzzy sets are combined with pairwise comparison of AHP technique [6,7]. The fuzzy analytic hierarchy process allows more detailed explanation of undefined and confusing knowledge of decision makers [4,5]. The fuzzy analytic hierarchy process method is challenging to direct the decision maker's opinions. Fuzzy analytic hierarchy process method often changes traditional approaches of study by statistical methods. Delphi is a technique for configuring a cluster relationship process in a method. In addition, it allows to members of the set to be challenged [8,9]. It is an iterative process to collect and revise practitioner's judgments with the help of information gathering, analysis techniques and forecasts. Here, authors are using the hybrid technique of three methodologies including fuzzy theory, Delphi method, and AHP technique [8,10,11]. The whole description of the methodology is shown in Figure 1.

With hybrid technique of fuzzy-Delphi AHP technique, authors created a hierarchy of all the steps taken to select and prioritize the security attributes and are briefly explained. Firstly, an author defines the problem and determines the goal. On the basis of the problem identified there should be a conduction of survey which would be done on the practitioners. After the survey, there should be calculation of coefficient of variation (CV) and if CV is less than 0.5 then additional surveys are stopped and process goes to next level otherwise again expert surveys are conducted. In the next step Content Validity

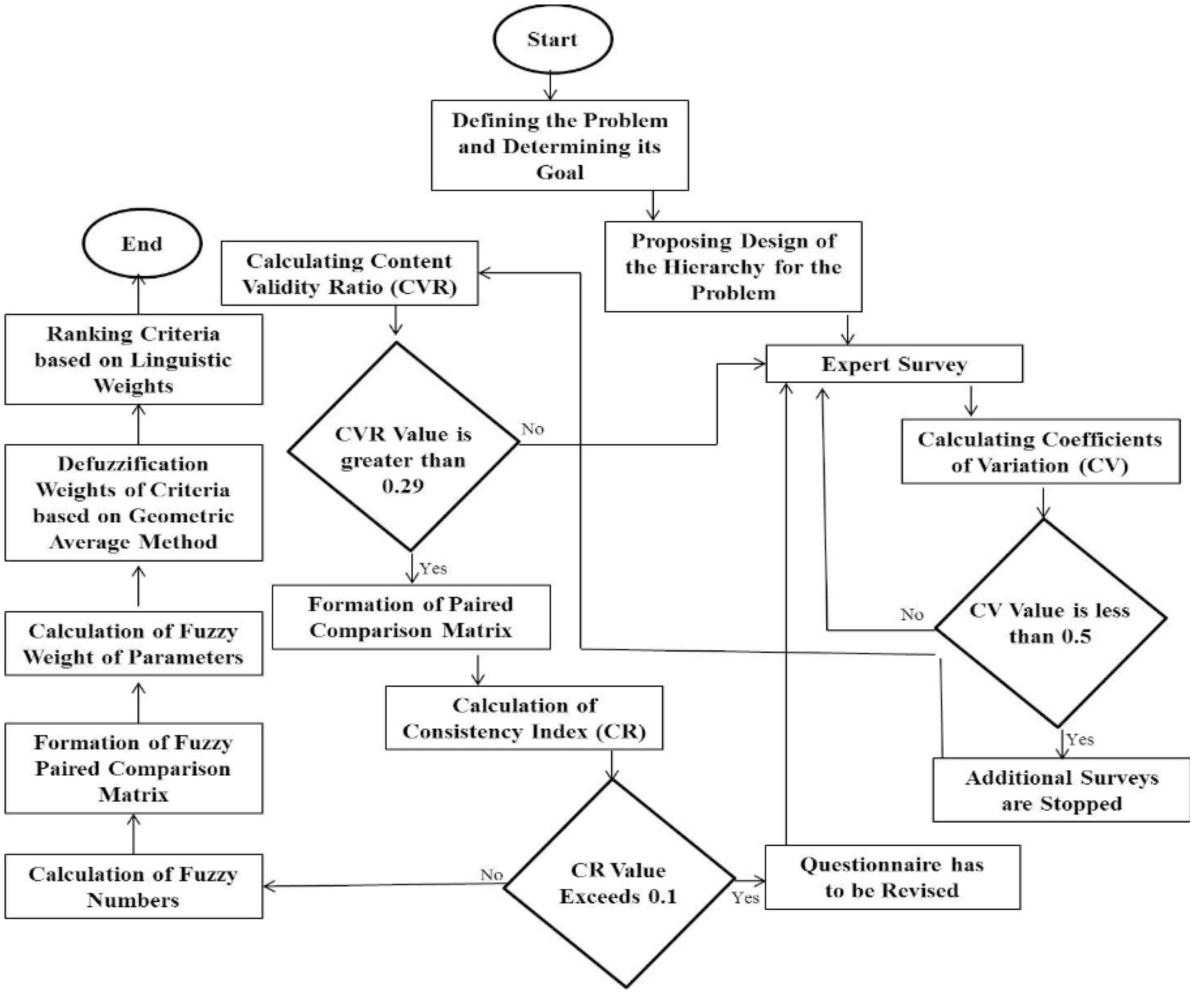

Figure 1. Fuzzy-Delphi analytic hierarchy process

Ratio (CVR) is calculated and if CVR is greater than 0.29 then formation of paired comparison matrix is done otherwise it goes back for expert surveys again. Further, there is need to calculate the CR value. If it exceeds 0.1 then questionnaire must be revised otherwise it will go to next step ahead that is calculation of fuzzy numbers. Next step is to build fuzzy paired comparison matrix and calculation of weightages. After calculation of fuzzy weightages, there is need of defuzzification. Defuzzification is done by method of geometric average. Finally, the ranking of the criteria based on linguistic values is achieved.

3. **Fuzzy-Delphi Analytic Hierarchy Process: Security Perspective.** According to previous section, the first stage in this study is proposing the hierarchy tree of security attributes [12,13]. Most of the developers as well as practitioners get confused to select the priority of security attributes according to user's requirements. There is a big problem to select most appropriate attribute of security which also influences the security design. With the help of literature survey and best practices, authors take most important attributes of security that includes confidentiality, integrity, authentication, availability and authorization. Hierarchy of attributes is shown in Figure 2 [14-16].

After the identification of security attributes, authors prepared a questionnaire and took the opinions of 22 experts, researchers, and practitioners. With the help of the opinions, authors can estimate the security by estimating the priority of attributes [17]. For integrated decision maker's uncertainty, fuzzy-Delphi AHP technique uses a choice of standard. Experts, researchers and practitioners are assigned scores to the attributes

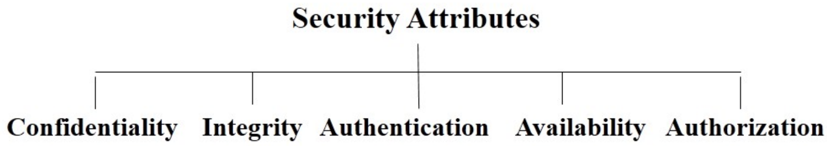

Figure 2. Security attributes hierarchy

Table 1. Scale for fuzzy-Delphi analytic hierarchy process

Symbol	Intensity of Importance	Assigned Numerical Value
WI	Without importance	1
LI	Low importance	3
MI	Moderate importance	5
SI	Strong importance	7
VEI	Very extreme importance	9

influencing the values in the quantitative way if possible according to scale which is shown in Table 1.

Researchers or practitioners can choose the important values that reflect their confidence from this range. Pairwise comparison process deals with subjectivity and fuzziness. Fuzzy-Delphi AHP technique is developed for solving all these selection problems of security attributes. A systematic qualitative technique is used to collect and converge expert opinions [15]. Data gathering is done using this process through a designed set of sequential questionnaire. Experts, researchers, and practitioners are from different areas of research knowledge and may define different weight vectors. During decision process, they usually cause not only the imprecise measurement but also serious judgments. Variation Constants (CV) and Content Validity Ratio (CVR) indices have been measured as shown in Equation (1) for this reason [14,15].

$$CVR = \left(SE - \frac{T}{2}\right) \Big/ \left(\frac{T}{2}\right) \tag{1}$$

where T is the total no of experts and SE is no of experts who rated the attribute essential. If CV is reached at 0.5, additional surveys are stopped. The CVR is established to validate how needed the given factor is in design of security of software. The CVR ranges from +1 to −1. A positive (+1) value is used for indicating that experts were in agreement that a factor is important. The CV is the ratio of the standard deviations and use it easier to compare the overall fuzziness of the data obtained. The calculation is stopped additional surveys for appropriate evaluation level which is shown in Table 2.

In the next step, opinions are considered directly from the experts for creating the paired comparison matrix. Further, input data satisfies a consistency check. If it is not satisfied then it goes back to previous step and revises the pairwise comparisons again. Paired comparison matrix for security attributes is shown in Table 3 for the first expert.

Table 2. CV and CVR results for final attributes assessment

Security Attributes	CV	CVR
Confidentiality	0.08	0.5
Integrity	0.10	0.2
Authentication	0.25	0.6
Availability	0.19	0.4
Authorization	0.25	0.4

TABLE 3. Paired comparison matrix for security attributes

Experts	Criteria	Confidentiality	Integrity	Authentication	Availability	Authorization
1	**Confidentiality**	1	1.29	1.80	1.29	1.80
	Integrity	0.78	1	1.40	1	1
	Authentication	0.56	0.71	1	0.72	1.40
	Availability	0.78	1	1.40	1	1.40
	Authorization	0.56	0.72	1	0.71	1

In next step, the variation of judgments can be taken using the largest eigenvalue $\tau_{\max}$. Here is given a $(n \times n)$ square matrix, a number $(\tau_{\max} - n)$ measures the deviation of the judgments from the consistent approximation. The closer max is to n, the more consistent the result is. The deviation of consistency is represented by the Consistency Index (CI) and then the Consistency Rate (CR) is calculated, which are defined in (2) and (3). The Random Index (RI) is determined by the size of n. CR is consistent in cases where it is smaller than or equal to 0.1. If it exceeds 0.1, the pairwise comparison needs to be done again or the questionnaire has to be revised [4,14,17]:

$$CI = (\tau_{\max} - n)/(n-1) \tag{2}$$

$$CR = CI/RI \tag{3}$$

Opinions of practitioners are directly taken to calculate fuzzy numbers (a_{ij}). Based on logic of Triangular Fuzzy Numbers (TFNs), maximum and minimum values of practitioners' opinions are marked as limit point. Geometrical Mean (GM) is calculated as membership degree of TFNs. In this case, a fuzzy number is defined as presented in (4) to (7). It is obvious that fuzzy number components are defined in a way that $a_{ij} \le b_{ij} \le c_{ij}$; these components vary in range $(1/9, 9)$ [4,16,18]:

$$A_{ij} = (a_{ij}, b_{ij}, c_{ij}) \tag{4}$$

$$a_{ij} = \min B_{ijk} \tag{5}$$

$$b_{ij} = \left[\prod B_{ijk}\right]^{1/n} \tag{6}$$

$$c_{ij} = \max B_{ijk} \tag{7}$$

where $k = 1, 2, 3, \ldots, n$.

In (4) to (7), B_{ijk} shows relative importance of attributes i over attributes j from viewpoint of the kth person, a_{ij} and c_{ij} are, respectively, lower and upper limits of opinions, and b_{ij} is also geometrical mean of these opinions.

In addition, paired comparison matrix of the fuzzy-Delphi has been created using (6). Further, comparison matrix for security attributes is formed as presented in (8) and matrix (9) [4,14,15]. The resulting fuzzy-Delphi comparison matrix is shown in Table 4.

$$A = [a_{ij}]_{n*n} \tag{8}$$

where $i, j = 1, 2, 3, \ldots, n$.

$$A = \left\{ \begin{array}{ccc} (1,1,1) & (a_{1j}, b_{2j}, c_{3j}) & (a_{1n}, b_{1n}, c_{1n}) \\ - & (1,1,1) & (a_{2n}, b_{2n}, c_{2n}) \\ - & - & (1,1,1) \end{array} \right. \tag{9}$$

Relative fuzzy weights of security attributes are calculated using Equation (10). After getting the final weights of each security attribute, all values obtained become non-fuzzy based on (11) [4, 17]. Table 5 shows the results of fuzzy and crisp weights and also the ranking scores for each attribute of security.

$$W_i = Z_i \oslash (Z_j \otimes \cdots Z_n) \tag{10}$$

$$W_i = \left(\prod W_{ij}\right)^{1/n} \tag{11}$$

In Table 5, the results are especially applicable for security design during software development. This means that, in this study, integrity is the most important criterion followed by authentication, availability and authorization respectively. Figure 3 shows the graphical representation of the results. The results can also be changed by changing the numbers and nature or behavior of experts. This technique can also be used in other fields of prioritization.

TABLE 4. Fuzzy-Delphi paired comparison matrix

Criteria	**Confidentiality**			**Integrity**			**Authentication**			**Availability**			**Authorization**		
	a	*b*	*c*	*a*	*b*	*c*	*a*	*b*	*c*	*a*	*b*	*c*	*a*	*b*	*c*
Confidentiality	1	1	1	1	1.36	1.80	1	1.68	3	1	1.6	1.80	1.40	2.45	3
Integrity	0.56	0.74	1	1	1	1	1	1.25	1.67	0.71	1.18	1.40	1.40	1.81	2.34
Authentication	0.34	0.59	1	0.60	0.80	1	1	1	1	0.60	0.95	1.40	1	1.45	1.67
Availability	0.56	0.63	1	0.71	0.85	1.40	0.71	1.05	1.67	1	1	1	1	1.53	2.34
Authorization	0.34	0.41	0.71	0.43	0.56	0.71	0.60	0.69	1	0.43	0.66	1	1	1	1

TABLE 5. Weightages and ranking of security attributes

Criteria	**Fuzzy Weights**			**Non-fuzzy Weights**	**Percentage**	**Ranking**
Confidentiality	0.10	0.18	0.30	0.17	17.00%	4
Integrity	0.16	0.30	0.50	0.28	28.00%	1
Authentication	0.13	0.22	0.36	0.22	22.00%	2
Availability	0.11	0.19	0.36	0.20	20.00%	3
Authorization	0.11	0.12	0.22	0.13	13.00%	5

FIGURE 3. Graphical representation of security attributes

4. **Conclusion.** Unsuitable selection of security factors may harm or cause failure of security during software use. Thus, selection and prioritization of these factors are important which are done by decision makers. Practitioners mostly select the best guidelines of development. The guidelines are based on MCDM methods. In addition, different MCDM methods regularly produce different outcomes for ranking of attributes to users' satisfaction. The results of this paper are showing the potential of the proposed fuzzy-Delphi AHP. Further, it can help practitioners obtain more strong decisions, especially in security design during software development. The results have been changed through the conditions of software industry, available development technology of the security, and their availability, etc.

Acknowledgement. This work is sponsored by UGC-MRP, New Delhi, India under F. No. 43-391/2014 (SR).

REFERENCES

[1] B. P. Kiran and P. N. Rao, Life cycle assessment (LCA) and multi-criteria decision making (MCDM) for planning, designing and commissioning of green buildings, *International Journal of Advanced Trends in Computer Science and Engineering*, vol.2, no.1, pp.476-479, 2013.

[2] *How Much Is Enough? A Risk Management Approach to Computer Security*, http://iisdb.stanford.edu/pubs/11900/soohoo.pdf, 2015.

[3] *Technical White Paper on Reducing Security Risks from Open Source Software*, http://h20195.www2.hp.com/v2/GetPDF.aspx/4AA0-8061ENW.pdf, 2015.

[4] S. Kazemi, S. M. Homayouni and J. Jahangiri, A fuzzy Delphi-analytical hierarchy process approach for ranking of effective material selection criteria, *Advances in Materials Science and Engineering*, pp.1-12, 2015.

[5] H. M. Hsu and C. T. Chen, Aggregation of fuzzy opinions under group decision making, *Fuzzy Sets and Systems*, vol.79, pp.279-285, 1996.

[6] M. Ataei, *Fuzzy Multiple Criteria Decision Making (FMCDM)*, 2010.

[7] A Forrester Consulting Coverity, *The Software Security Risk Report the Road to Application Security, Begins in Development September 2012*, http://www.coverity.com/library/pdf/the-softwaresecurity-risk-report.pdf, 2015.

[8] J. J. Buckley, Ranking alternatives using fuzzy numbers, *Fuzzy Sets and Systems*, vol.15, no.1, pp.21-31, 1985.

[9] K. Reza and S. M. Vassilis, Delphi hierarchy process (DHP): A methodology for priority setting derived from the Delphi method and analytical hierarchy process, *European Journal of Operational Research*, vol.137, pp.347-354, 1988.

[10] D. B. Parker, Restating the foundation of information security, *Proc. of the 8th International Conference on Information Security*, Netherlands, pp.139-151, 1992.

[11] O. Cakir and M. S. Canbolat, A web-based decision support system for multi-criteria inventory classification using fuzzy AHP methodology, *Expert Systems with Applications*, vol.35, no.3, pp.1367-1378, 2008.

[12] B. Bulgurcu, H. Cavusoglu and I. Benbasat, Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness, *Information Security Policy Compliance*, vol.34, no.3, pp.523-548, 2010.

[13] Y. Asnar, P. Giorgini, M. Fabio and Z. Nicola, From trust to dependability through risk analysis, *Proc. of the 2nd International Conference on Availability, Reliability and Security*, pp.19-26, 2007.

[14] F. Cebi, C. Kahraman and B. Bolat, A multiattribute ABC classification model using fuzzy AHP, *Proc. of the 40th International Conference on Computers and Industrial Engineering*, Awaji, Japan, pp.25-28, 2010.

[15] R. Gupta, A. Sachdeva and A. Bhardwaj, Selection of 3pl service provider using integrated fuzzy Delphi and fuzzy TOPSIS, *Proc. of the World Congress on Engineering and Computer Science*, San Francisco, USA, pp.24-31, 2010.

[16] A. Ishikawa, M. Amagasa, T. Shiga, G. Tomizawa, R. Tatsuta, and H. Mieno, The max-min Delphi method and fuzzy Delphi method via fuzzy integration, *Fuzzy Sets and Systems*, vol.55, no.3, pp.241-253, 1993.

[17] L. Mikhailov, Deriving priorities from fuzzy pairwise comparison judgements, *Fuzzy Sets and Systems*, vol.134, no.3, pp.365-385, 2003.

[18] R. Kumar, S. A. Khan, A. Agrawal and R. A. Khan, Measuring the security attributes through fuzzy analytic hierarchy process: Durability perspective, *ICIC Express Letters*, vol.12, no.6, pp.615-620, 2018.