Using Fuzzy Logic to Increase the Accuracy of E-Commerce Risk Assessment Based on an Expert System

Haniyeh Beheshti
Department of Engineering
E-Campus
Islamic Azad University
Tehran, Iran
Haniyeh.beheshti@yahoo.com

Mahmood Alborzi
Department of Management and Information Technology
Science and Research Branch
Islamic Azad University
Tehran, Iran
mahmood_alborzi@yahoo.com

***Abstract*—Strong adaptive control can be exercised even without access to accurate data inputs. Such control is possible through fuzzy mathematics, which is a meta-collection of Boolean logic principles that imply relative accuracy. Fuzzy mathematics find applications in e-commerce, where different risk analysis methods are available for risk assessment and estimation. Such approaches can be quantitative or qualitative, depending on the type of examined data. Quantitative methods are grounded in statistics, whereas qualitative methods are based on expert judgments and fuzzy set theory. Given that qualitative methods are very subjective and deal with vague or inaccurate data, fuzzy logic can be used to extract useful information from data inaccuracies. In this study, a model based on the opinions of e-commerce security experts was designed and implemented by using fuzzy expert systems and MATLAB. A case study was conducted to validate the effectiveness of the Model.**

Keywords-fuzzy logic; risk assessment system; e-commerce; expert system

I. INTRODUCTION

Two of the most important components of a information security management system are risk analysis and risk assessment. These processes enable organizations to identify e-commerce assets, associated vulnerabilities and security threats, estimate vulnerability, the probability of threat occurrence and its consequences, determine, analyze, and prioritize risks and implement solutions to problems. Appropriate risk analysis and assessment methods can therefore advance the accurate and optimal implementation of security controls for e-commerce systems. Risk analysis is the process of comprehending the nature of risk and determining its level [1]. Risk assessment is the process of comparing estimated risk with presented risk criteria to determine the importance of risks [1]. Fuzzy logic is a type of logic intended to replace the methods by which human brain draws conclusions. Fuzzy logic is not only a control methodology but also a method of processing data on the basis of authorized small group membership instead of large group membership. Basic argument is that humans do not need accurate data inputs to perform strong adaptive control. Such control is possible through fuzzy mathematics, which is a meta- collection of Boolean logic principles that imply the concept of relative accuracy. Classical logic shows everything in accordance with a binary system, whereas fuzzy logic shows the accuracy of everything with a number falling between 0 and 1 [2]. Expert systems are generally defined as computer programs that simulate the manner of thinking of an expert in a specific field [3]. These programs identify logic models experts use as basis in making decisions and contain knowledge databases that human beings can refer to in making a decision about a specific issue [4]. Not all expert systems are all-purpose systems, they can simulate the human decision-making process only in a limited number of areas [5].

Authors in [6] presented a technique for analyzing software with the use of fuzzy expert systems. The authors formulated expert rules using Mamdani fuzzy reasoning for appropriate input analysis and implemented their design by using a fuzzy logic tool (MATLAB. Despite the insights provided by the study, however, its scope was limited to software security and did not cover other e-commerce elements, such as network and hardware security. The study also failed to provide a catalog of vulnerabilities and security threats. Authors in [7] described the development of a fuzzy decision support system (FDSS) to evaluate development risk in e-commerce. A prototype of a web-based FDSS was developed using MATLAB to help managers of e-commerce projects detect potential risks. The authors stated that although e-commerce provides different trade opportunities, its development is exposed to a variety of risks and that risk management is essential to coping with and preventing these problems. Appropriate risk management necessitates risk assessment, which is an important step in detecting and identifying risks. Most managers are worried about the time spent on risk identification and assessment, but such procedures can now be facilitated by computers, software, and applications. The study considered the direct and indirect risks encountered in all levels of an e-commerce system, including the planning, analysis, design, and implementation levels [7].

II. MATERIALS AND METHODS

A. Uses and Advantages of Fuzzy Model Over Other Models

The management of information security risk in e-commerce is characterized by a very short history. Thus, no accurate and quantitative data have been provided on the type, probability, intensity, and consequences of e-commerce risks, as well as on data assets and any other issue related to the field [8]. Performing merely quantitative analyses in e-commerce is neither cost-effective nor accurate, and qualitative analyses suffer from disadvantages, such as overdependence on individual opinions and lack of analytical specificity. Qualitative models are appropriate only for surface analysis of risks and for the identification of priority risks (i.e., risks that require more in-depth examination). These deficiencies are popularly addressed with fuzzy models because they involve the incorporation of uncertainty in computations, the consideration for the probability of number usage to calculate risks and the use of language variables at the time of data collection. In other words, fuzzy methods encompass both quantitative and qualitative principles [9]. The effectiveness and efficiency of fuzzy theory lies in the estimation of newfound and unknown risks. Success and efficiency can also be attributed to the fact that in fuzzy theory, continuous changes are used to assign numerical inputs to several fuzzy sets with different degrees of accuracy by using recommended standard methods that satisfy the needs of each field [10]. Many researchers have compared fuzzy set and non-fuzzy set theories and the results derived with real-world situations [11, 12]. In these studies, two methods were used to prioritize several options in accordance with specified criteria. The results showed the superiority and advantages of methods based on fuzzy sets over those grounded in non-fuzzy sets [11, 12]. Authors used the Sugeno method, whose advantages include computational efficiency, appropriate performance with linear techniques, and appropriate performance with optimization and adaptive techniques. The method also guarantees continuity in output levels and is highly suitable for mathematical analysis [13].

B. Design of the Proposed Model

We used the recursive ANFIS method, which is similar to the NARX method adopted in neural networks, to design and implement our model. ANFIS inputs were created in MATLAB as follows. The neural network outputs obtained from data were used as input delay (lag) to train the model. The proposed model was developed on the basis of the NARX standard, which was designed in accordance with ANFIS. Data obtained from a questionnaire were trained as recursive components. A recursive structure can be described as oriented toward modeling. This definition therefore justifies the use of a recursive method.

In this project, the working environment of MATLAB consists of several parts, namely, anfis1, anfis2, anfis3, and plotResult. Anfis1 is related to the assessment of threat probability, anfis2 revolves around the assessment of damage probability, anfis3 is associated with final risk estimation, and plotResult has to do with drawing output graphs. The Simulink tab in MATLAB also directs a user to a number of components, such as fuzzy_sim, test_fuzzy_sim, anfis33, anfis22, and anfis11. Anfis11 pertains to the assessment of risk probability, anfis22 is associated with the assessment of damage probability, anfis33 is related to final risk estimation, fuzzy_sim revolves around the general form of the research model, and test_fuzzy_sim is related to model testing (Figure 1). In the model testing component, the main inputs taken from the questionnaire data were labeled with numbers from 1 to 4, which correspond to size, opportunity, motivation, and skill, respectively. Labels $z-1$ to $z-9$ refer to outputs with delay. The questionnaire-derived outputs were modeled as input with delay. Columns 1 to 4 contain the main data, and columns 5 to 10 consist of the outputs with delay. These delays differ from one another and were obtained by trial and error (the same parts can be found in anfis11 and anfis33).

III. DISCUSSION

The model was also designed on the basis of the design of FIS(s) and MF(s), and we approached the final step that is the output of the proposed model. For this purpose, we ran the software to examine each of the aforementioned parts. Figure 2 shows two red and black lines, which denote the network output and the target real data, respectively. The network generated the output after training. The figure can thus be described as reflecting network conditions before and after training, which includes 70% of the data. Figure 3 presents the test data, with an overview similar to that in Figure 2. The only difference between these images is that Figure 3 shows 30% of the input data and obtained output. Figures 4 and 5 show the training and test data for FIS2, while Figure 6 illustrates the data related to validation. These data, as was already explained, were selected randomly from the entirety of the examined dataset. The results shown in the Figures correspond with the expectations. Note that the data for validation account for the 70% of the entire data used. In Figure 7, the horizontal line that runs toward 550 corresponds to all the data taken from the questionnaire, and the vertical line that runs toward 5 corresponds to the defined scope. The figure features two color spectra: yellow, which denotes the reference data, and blue, which represents the training data.

A. Case Study on Model Accuracy

A case study was carried out for a more accurate examination. The required data were taken from an expert who serves as the administrator of the website Kadorangi, which is an active e-commerce platform. The required data were entered into the developed model and their reliability was ensured. The results are discussed as follows. After the data obtained from the e-commerce website were incorporated into the model, figures of the training, testing, and validation data, as well as all other data, were drawn. Each FIS was then subjected to regression. Table I shows the R2 and RMSE of each Kadorangi website component studied and the model accuracy. The values obtained, whether in the main research or the case study, indicated that the developed model is reliable and can be used to evaluate security risk in e-commerce.

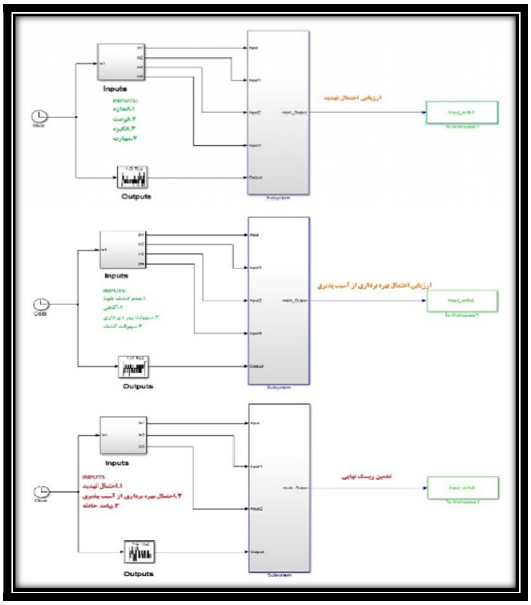

Fig. 1. Overview of anfis11, anfis22, anfis33 in MATLAB Simulink

TABLE I. RESULTS ON MODEL RELIABILITY IN THE CASE STUDY

Acceptable / Unacceptable	*R2*	RMSE	Parts	FIS
Acceptable	0.95645	0.22275	Training data	FIS1
Acceptable	0.97507	0.2374	Test data	
Acceptable	0.96655	0.22724	All data	
Acceptable	0.95941	0.23397	Validation data	
Acceptable	0.98727	0.21559	Training data	FIS2
Acceptable	0.9755	0.1797	Test data	
Acceptable	0.97512	0.20548	All data	
Acceptable	0.98193	0.20636	Validation data	
Acceptable	0.97589	0.20278	Training data	FIS3
Acceptable	0.98096	0.17774	Test data	
Acceptable	0.98089	0.19561	All data	
Acceptable	0.9815	0.19359	Validation data	

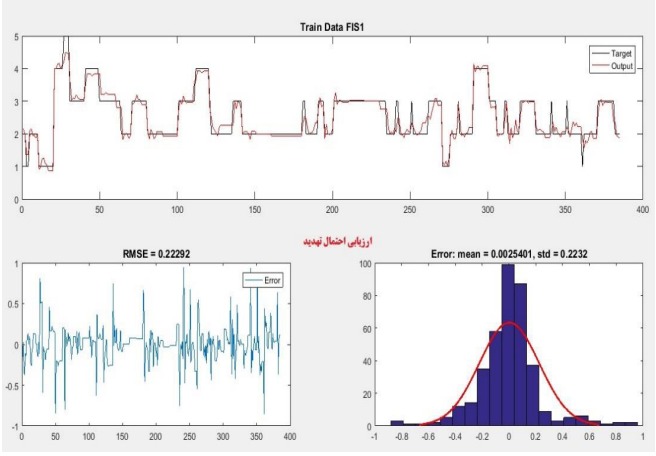

Fig. 2. Training data for FIS1

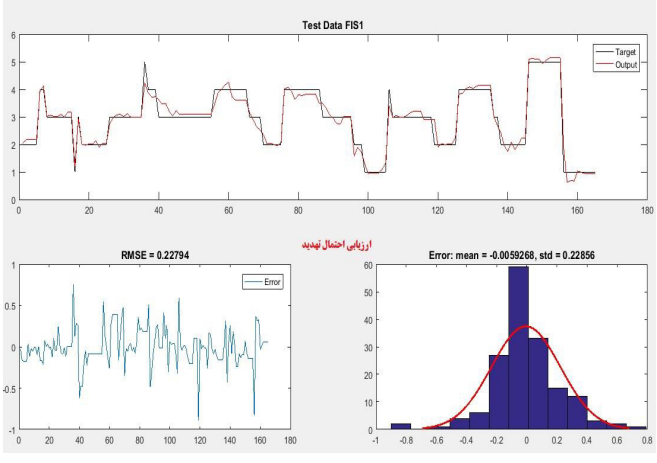

Fig. 3. Test data for FIS1

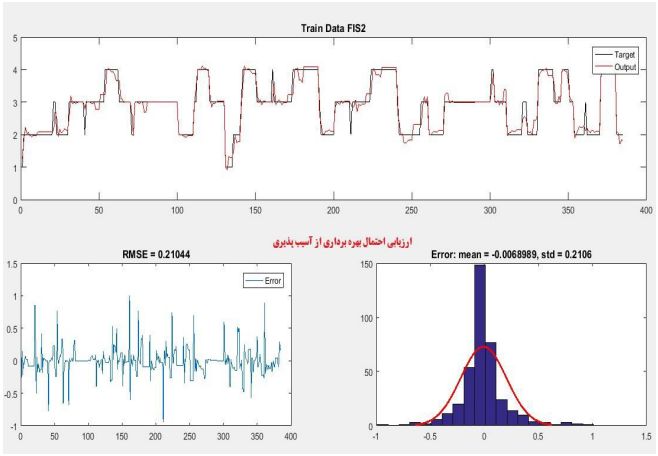

Fig. 4. Training data for FIS2

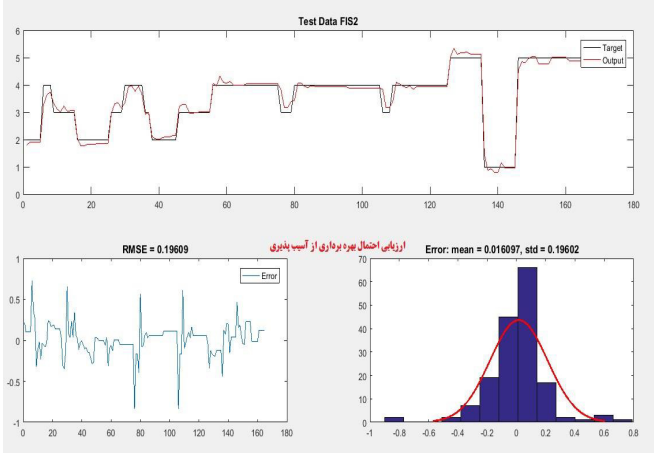

Fig. 5. Test data for FIS2

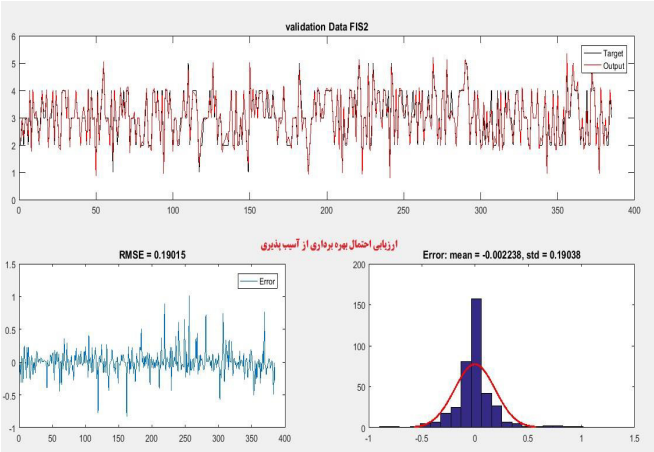

Fig. 6. Validation data for FIS2

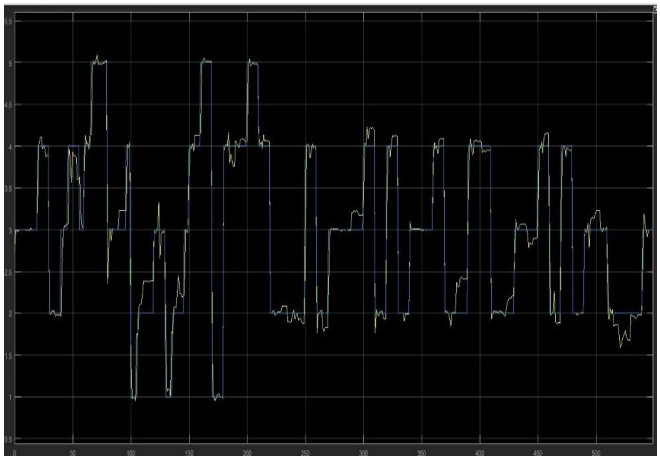

Fig. 7. A view of scope–final output of the model

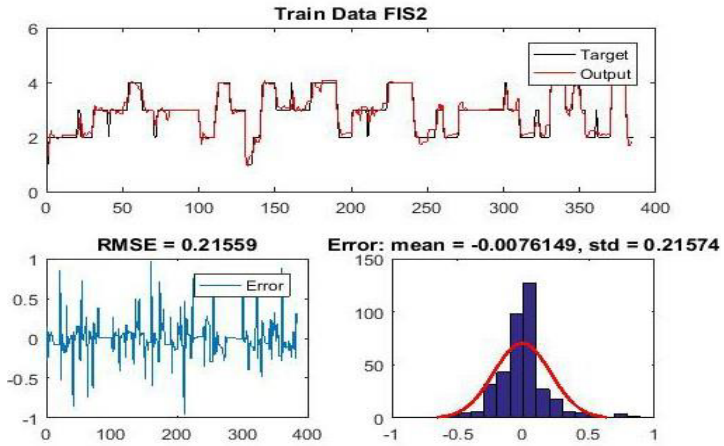

Fig. 8. Training data for FIS2

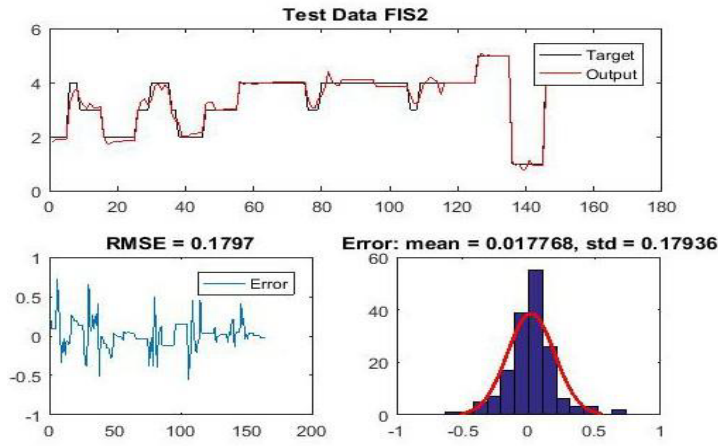

Fig. 9. Test data for FIS2

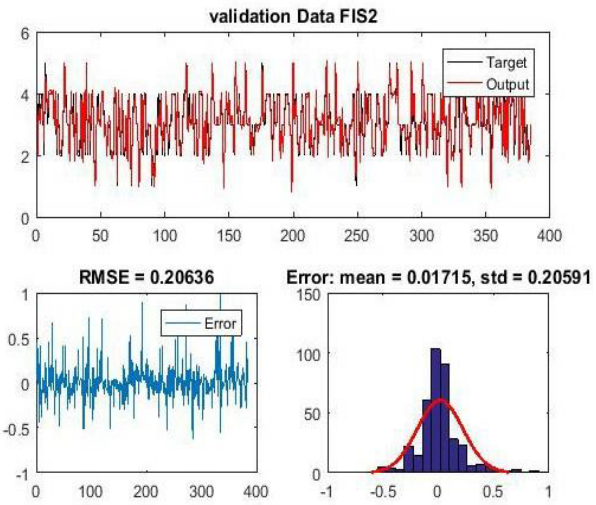

Fig. 10. Validation data for FIS2

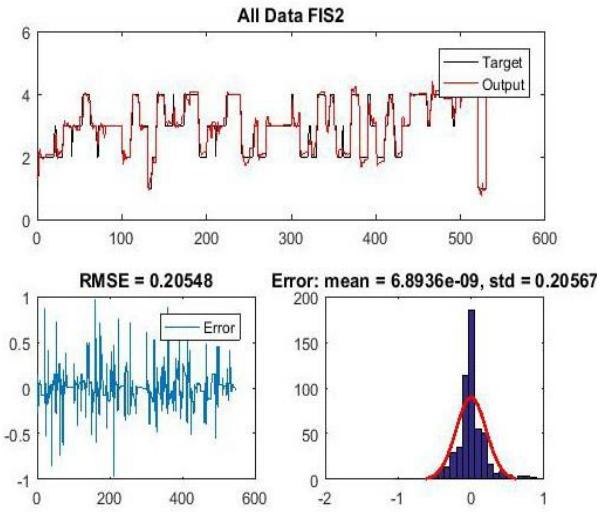

Fig. 11. All data for FIS2

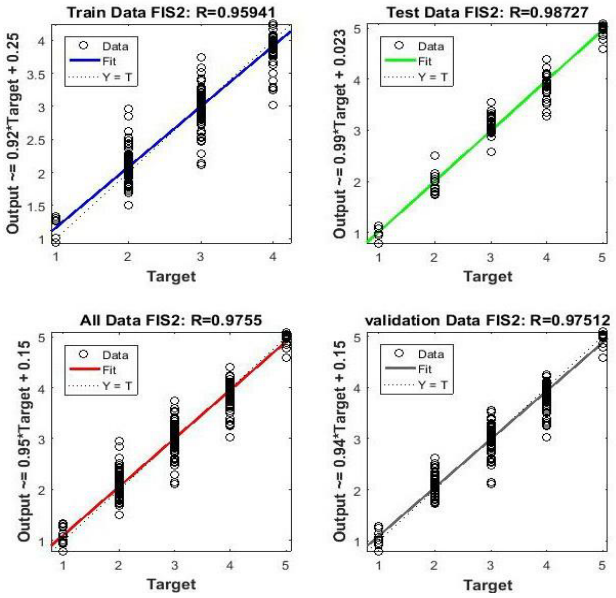

Fig. 12. Regression of FIS2

IV. CONCLUSION

Risk is an uncertain phenomenon that can never be completely eliminated, even in the e-commerce domain. Fuzzy logic substantially contributes to risk analysis in uncertain conditions and thereby enables appropriate decision making supported by risk evaluation and analysis. Different methods are used to assess and estimate risk in e-commerce, and these can be categorized as quantitative or qualitative in nature, depending on the type of the examined data. Quantitative methods are statistical in nature, whereas qualitative methods are grounded in expert judgments and fuzzy set theory. Using a fuzzy method to ensure e-commerce security can increase the accuracy of risk assessment systems that are based on the evaluations of experts in the field. It also provides optimal and reliable results. To address these issues, this study developed a model and implemented it on the basis of the opinions of e-commerce experts. The model development and implementation were accomplished using fuzzy expert systems and MATLAB.

REFERENCES

[1] ISO/IEC, ISO/IEC Guide 73:2003: Risk management - Principles and guidelines, International Organization for Standardization, Switzerland, 2003

[2] M. R. Gupta, S. Sarkar, S. Ghosh, M. Debnath, M. Khan, "Effect of nonadiabaticity of dust charge variation on dust acoustic waves: Generation of dust acoustic shock waves", Physical Review E, Vol. 63, No. 4, pp.046406, 2001

[3] W. Jiang, Z. Li, J. Jia, D. Liu, "Evaluating E-Commerce System Security Using Fuzzy Multi-criterion Decision-Making", IEEE Seventh International Conference on Semantic Computing, pp. 438-443, 2013

[4] E. W. T. Ngai, F. K. T. Wat, "Fuzzy decision support system for risk analysis in e-commerce development" Decision support systems, Vol. 40, No. 2, pp.235-255, 2005

[5] K. Darlington, The essence of expert systems, Prentice Hall, 2000

[6] A. S. Sodiya, H. O. D. Longe, O. M. Fasan, "Software security risk analysis using fuzzy expert system", INFOCOMP Journal of Computer Science, Vol. 7, No. 3, pp.70-77, 2008

[7] M. H. Zirakja, R. Samizadeh, "Risk Analysis in E-commerce via Fuzzy Logic", International Journal of Management and Business Research, Vol. 1, No. 3, pp.99-112, 2011

[8] A. S. Sendi, M. Jabbarifar, M. Shajari, M. Dagenais, "FEMRA: Fuzzy Expert Model for Risk Assessment", Fifth International Conference on Internet Monitoring and Protection, pp. 48-53, 2010

[9] W. L. McGill, B. M. Ayyub, "Multicriteria security system performance assessment using fuzzy logic", The Journal of Defense Modeling and Simulation: Applications, Methodology, Technology, Vol. 4, No. 4, pp.356-376, 2007

[10] K. Shang, Inconsistent Inference in Qualitative Risk Assessment, Available at http://crocouncil.org/images/Inconsistent_Inference_in_Qualitative_Risk_Assessment_v2_-_clean.pdf, 2013

[11] A. Ozdagoglu, G. Ozdagoglu, "Comparison of AHP and Fuzzy AHP for the Multi Criteria Decision Making Processes with Linguistic Evaluations", Istanbul Ticaret Universitesi Fen Bilimleri Dergisi, Vol. 6, No.11, pp. 65-85, 2007

[12] D. Y. Chang, "Applications of The Extent Analysis Method on Fuzzy- AHP", European Journal of Operational Research, Vol. 95, No. 3,pp. 649-655, 1996

[13] K. Mostafa, Fuzzy logic in MATLAB, Tehran: Kian university press, 2011

[14] N. Kasuan, N. Ismail, M. N. Taib, M. H. Fazalul Rahiman, "Recurrent adaptive neuro-fuzzy inference system for steam temperature estimation in distillation of essential oil extraction process", IEEE 7th International Colloquium on Signal Processing and its Applications, pp. 1-6, 2011