Volume 2, Issue 9, September 2012 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

# Fuzzy Based Evaluation Model of a Systems Security

**Rahul Choudhary**
*Dept. of C.S. / I.T.*
*M.I.T. Ujjain (m.p.) India*

**Abhishek Raghuvanshi**
*Associate Professor of computer science dept.*
*M.I.T. Ujjain (m.p.) India*

***Abstract— Modern security management methods now acknowledge that most threats cannot be completely eliminated and that they need to be managed in a cost effective manner. This paper will concentrate on the development of a methodology for the assessment and analysis of threats and vulnerabilities within the context of security risk management. At the end of the research a new fuzzy based threat assessment model is proposed. Due to dynamic and continuous threats on network security, policy makers need to perform evaluation on existing security strategy as to deliver trusted and confidence services. This paper presents a threat evaluation framework based on fuzzy logic techniques to help policy makers conduct comprehensive assessment of security strategy.***
***Keywords—Threat, Threat Impact, Fuzzy, Threat Assessment, Threat Analysis***.

## I. INTRODUCTION

Recently, the issue of security has evolved and government has recorded around 787 cases of security breach into the government network reported from January 2001 to July 2007. From this figure 90.5% are intrusion attacks [1]. Even though security features has been implemented and put in place, there are still spaces and potential threats which could lead to these attacks.

Securing the network infrastructure itself does not solve the security issues as a whole. These new tools, systems and appliance should also be secured in a way where it is possible to avoid threats and vulnerability in order to avoid the risk of failure towards the agency. This is where risk assessment comes into the picture. Threat assessment which is a part of risk analysis plays a significant role in security management efforts [2]. There is a demand for a threat analysis model and tool to support the assessment of risk management in network security field for government agencies. The main idea of this study is to answer the research question: "Can fuzzy logic approach be performed in threat analysis for network security systems and appliances in the government networking scenario?"

The research will focus on risk assessment analysis using fuzzy base approach for network security appliances and systems assessment in government agencies.

## II. BACKGROUND

As it was realized, all the different methodologies (Brewer, 2000; Katzke, 1988; Reid and Floyd, 2001; Carroll, 1996; Nosworthy, 2000; Pfleeger, 2000; Icove, Seger, VonStorch, 1995; Summers, 1977; CCTA, 1993) were assuming that the user knew about the threats and the threat agents his system had to face, and do not attempt to examine their sources. In today's ever-changing world a threat assessment cannot and should not make that mistake. All of the examined methodologies and models are following the waterfall method (Pressman, 2001) for calculating and producing results. That means that they are not flexible enough and cannot cope with the amount of changes their inputs have to go thought. Furthermore, they are using probabilities for calculating the likelihood of the threat, without examining the likelihood of the agent. Just the concept of using probabilities greatly undermines the validity of the methods. None of the methods is trying to model the system in the business environment hence various assumptions are made. Most of the models think of the threat impact as only causing a financial loss. A threat though can have an impact on various levels and aspects of a business (Kalakota and Whinston, 1997; Daughtrey, 2001; Computer Fraud & Security, 2002; Johnson and Scholes, 1999). We not only need to consider these various levels, but we also need to examine combinations of impacts and how catastrophic they might be towards the survivability of the business.

## III. METHODOLOGY

Fuzzy Logic introduced by Zadeh (1965) gives us a language, with syntax and local semantics, in which we can translate our qualitative knowledge about the problem to be solved. Fuzzy logic is a powerful problem-solving methodology with a myriad of applications in embedded control and information processing. Fuzzy provides a remarkably simple way to draw definite conclusions from vague, ambiguous or imprecise information. In a sense, fuzzy logic resembles human decision making with its ability to work from approximate

data and find precise solutions. There are many factors which account for the increase in question but the most prominent among them is the rapidly growing use of soft computing and especially fuzzy logic in the conception and design of intelligent systems .As one of the principal constituents of soft computing, fuzzy logic is playing a key role in the conception and design of various systems. There are two concepts within fuzzy logic which play a central role in its applications. The first is that of a linguistic variable, i.e., a variable whose values are words or sentences in a natural or

 

synthetic language. The other is that of a fuzzy if-then rule in which the antecedent and consequent are propositions containing linguistic variables. The essential function served by linguistic variables is that of granulation of variables and their dependencies. In effect, the use of linguistic variables and fuzzy if-then rules results -through granulation in soft data compression which exploits the tolerance for imprecision and uncertainty. In this respect, fuzzy logic mimics the crucial ability of the human mind to summarize data and focus on decision-relevant information since decision making mostly involve fuzzy logic techniques and alternative to consider altogether, this framework implement fuzzy logic techniques approach to view security strategy from managerial perspective. Fuzzy set theory is applied to complement the framework in order to capture fuzziness in the form of inconsistencies and vagueness coming from subjective judgments by decision makers.

*A. Different Membership Function:*

1. Straight line**:** The simplest membership function is formed by straight line.
2. Trapezoidal**:** The function is often represented by "trapmf".
3. Gaussian**:** Let say a fuzzy set Z which represent "number close to zero". The possible Membership function for Z is $\mu z(x) = e \exp(-x^2)$ (1.3)
4. Triangular**:** This is formed by the combination of straight lines. The function is name as "trimf" .We considers the above case i.e. fuzzy set Z to represent the "number close to zero". So mathematically we can also represent it as

$$\mu z(x) = \begin{cases} 0 \text{ if } x<-1 \\ x + 1 \text{ if } -1 \le x <0 \\ 1 - x \text{ if } 0 \le x <1 \\ 0 \text{ if } 1 \le x \end{cases} \quad (1.4)$$

*B. Fuzzy Set of Operation:*

1. Fuzzy intersection
2. Fuzzy union
3. Fuzzy complement.

*C. Fuzzy Rule Base:*

A fuzzy rule-based model of human problem solving is described. The model is presented in its general form and then adapted to fit data from a simulated fault diagnosis task. The model was able to match 50% of human subjects' actions exactly while using the same rules approximately 70% of the time. Problem solving rules were selected by the model according to measures of recall, usefulness, applicability, and simplicity. Rules were further discriminated by their use of symptomatic information for pattern recognition or topographic information for information seeking. A production rule consists of two parts: condition (antecedent) part and conclusion (action, consequent) part,

IF (conditions) THEN (actions)

Rule 1: IF (C Score is high) and (C Ratio is good) and (C Credit is good)

Then (Decision is approve)

Rule 2: IF (C Score is low) and (C Ratio is bad) or (C Credit is bad)

Then (Decision is disapprove).

*D. Fuzzy Interference System Editor:*

The FIS editor handles the high level issuing for the system such as the number of input and output variables an their names, types of the 'AND' and 'OR' operators, and the aggregation and defuzzification methods. The member ship function editor: The membership function editor is used to define the properties of the membership function for the systems variables. · The rule editor: The rule editor enables the user to define and edit the of rules that describe the behavior of the system. The rule viewer: The rule viewer is a read only tool that displays the whole fuzzy inference diagram. The surface viewer: The surface viewer is also a read only tool. it is used to display how an output is dependent on any one or two of the input. The proposed model is as follows:

In developing the fuzzy threat assessment model in the Appliances / Systems will be produced by adopting The Fuzzy design phase, the risk analysis methodology from ISO/IEC Risk Analysis Model . Four Level are been justified as:- 27001, ISO/IEC 27005 and shall be considered. Then the Level 1 – Goal , Level 2 – Threat Category, Level 3 – Threat fuzzy risk analysis model proposed by will be adopted and Potential Category and Level 4 – Threat Descriptions. Modified accordingly Data aggregation can be defined as any process in which information is gathered and expressed in a summary form, for the purposes of such statistical analysis (SearchSQLServer.com Definitions). In this case, the process is to get a value to complete the fuzzification process. A common aggregation purpose is to get more information about particular groups based on specific variables such as in this study, the "likelihood" and the "consequences" of the threats. More than one, n evaluator will be involved in the threat assessment process. The Triangular Average Formula will be used to get the value from the average of each assessment done by each evaluator as the process of obtaining mean value. The fuzzy average value is obtained based on the selection of "likelihood" and "consequence" of each threat done by all evaluators.

 

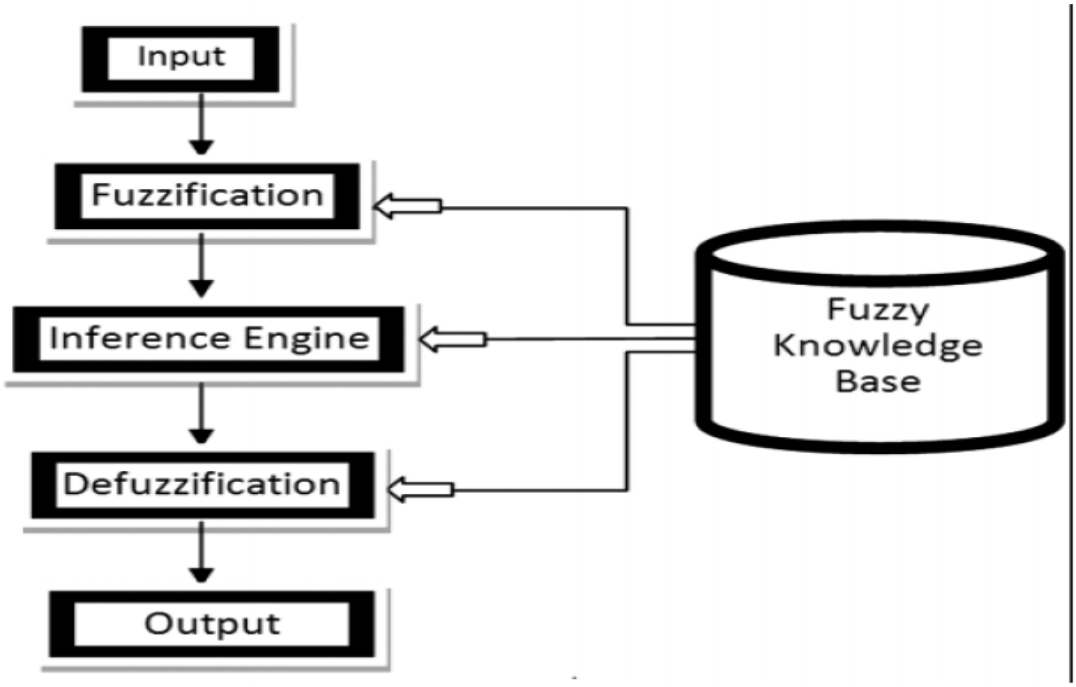


**Fig :** Proposed Fuzzy Threat Assessment Model

## IV.**CONCLUSION**

In this research paper we tried to developed the security strategy by using fuzzy logic expert system because each and every department need the absolutely flaw less performance of the security strategies, and using fuzzy technology evaluation of security strategies on the basis of various key performance attributes that have been validated. For obtaining the desired level of performance, we take input value for various attributes applied different membership functions and applied to the same linguistic variables, triangular and trapezoidal, more of less similar and compared the performance and we got the performance of absolute security parameters. The fuzzy scale has been designed to map and control the input data values from absolute truth to absolute false. The qualitative variables are mapped in to numeric results by implementing the fuzzy export system model through various input examples and provide a basis to evaluate government system security strategy

## **ACKNOWLEDGMENTS**

First of all I would like to express my heartiest to my guide Mr. Abhishek Raghuvanshi, for his all time guidance, support, and valuable suggestion.

I would like to express my gratitude towards Prof. Shweta yadav, Head of the Department, Information Technology engg., M.I.T. Ujjain.

REFRENCES

[1]. L.A. Zadeh, Fuzzy Sets, Information and Control, 1965
[2]. L.A. Zadeh, Outline of A New Approach to the Analysis of of Complex Systems and Decision Processes, 1973
[3]. L.A. Zadeh, ”Fuzzy algorithms,” Info. & Ctl., Vol. 12, 1968, pp. 94-102.
[4]. L.A. Zadeh, ”Making computers think like people,” IEEE. Spectrum, 8/1984, pp. 26-32.
[5]. S. Korner, ”Laws of thought,” Encyclopedia of Philosophy, Vol. 4, MacMillan, NY: 1967, pp. 414- 417.
[6]. C. Lejewski, ”Jan Lukasiewicz,” Encyclopedia of Philosophy, Vol. 5, MacMillan, NY: 1967, pp. 104- 107.
[7]. J.F. Baldwin, ”Fuzzy logic and fuzzy reasoning,” in Fuzzy Reasoning and Its Applications, E.H.Mamdani and B.R. Gaines (eds.), London: Academic Press, 1981.
[8]. W. Bandler and L.J. Kohout, ”Semantics of implication operators and fuzzy relational products,” in Fuzzy Reasoning and Its Applications, E.H. Mamdani and B.R. Gaines (eds.), London: Academic Press, 1981.
[9]. M. Eschbach and J. Cunnyngham, ”The logic of fuzzy Bayesian influence,” paper presented at the International Fuzzy Systems Association Symposium of Fuzzy information Processing in Artificial Intelligence and Operational Research, Cambridge, England: 1984.
[10]. F. Esragh and E.H. Mamdani, ”A general approach to linguistic approximation,” in Fuzzy Reasoning and Its Applications, E.H. Mamdani and B.R. Gaines (eds.), London: Academic Press, 1981.

 

[11]. Xiaohong Gan (2008) ”Research on Risk Aversion of E-government Network Security”. ieee research paper.
[12]. WANG Jin-fu (2009) “E-government Security Management: Key Factors and Countermeasures”. ieee research paper.
[13]. Irfan Syamsuddin, Junseok Hwang Bertucci ,(2010) “A New Fuzzy MCDM Framework to Evaluate
[14]. E-Government Security Strategy” ieee research paper.
[15]. “INFORMATION SYSTEMS SECURITY COMPLIANCE IN E-GOVERNMENT”(2009)
[16]. Goncalves, M. (1999), Firewalls A Complete Guide, McGraw Hill, NEW DELHI

 