ISSN 2229-5518

# Risk Assessment of a System Security on Fuzzy Logic

Rahul Choudhary, Abhishek Raghuvanshi

**Abstract**— as Information Technology (IT) has become increasingly important to the competitive position of firms, managers have grown more sensitive to their organization's overall IT risk management. In an attempt to minimize or avoid such losses, managers are employing various qualitative and quantitative risk analysis methodologies. The risk analysis literature, however, suggests that these managers typically utilize a single methodology, not combination methodologies. This paper proposes a risk analysis process that employs a combination of qualitative and quantitative methodologies.This paper will concentrate on the development of a methodology for the assessment and analysis of risk and vulnerabilities within the context of security risk management. At the end of the research a new fuzzy based risk assessment model is proposed. This process should provide managers with a better approximation of their organization's overall information technology risk posture. Practicing managers can use this proposed process as a guideline in formulating new risk analysis procedures and/or evaluating their current risk analysis procedures.

**Index Terms**— Fuzzy, Qualitative, Quantitative, Risk Assessment, Risk Analysis, Risk Assessment technique and Threats.

## 1 INTRODUCTION

However in real world environment, most of organizations do not have proper data about security breaches due to incomplete information or unreported cases. This is mainly due to financial constraints or do not have appropriate information security policies. Therefore, most of existing methods intended to estimate the probability of an identified vulnerability of security breach largely on guesswork or rough estimation. Risks can come from uncertainty in project failures, legal liabilities, accidents, natural causes and disasters as well as deliberate attacks from an adversary. Risk assessment is the determination of quantitative or qualitative value of risk related to a concrete situation and a recognized threat (also called hazard). There are four steps in a risk assessment process. First build appropriate mathematical model according to the results of risk identification. Second, obtain the necessary, basic information or data available through expert investigation, history records, extrapolation, etc., and then choose the appropriate mathematical method to quantify the information. Third, choose the appropriate model and analysis methods, process and analyze the data, and modify the model as needed. Fourth, determine risk level according to certain criteria.
We are using the fuzzy technique in the past year fuzzy logic has raised increasing attention in world scenarios. This is due to the fact that the most approaches from classical statistics assume that we deal with exact measurements. But in most, if not all world scenarios, we will never have a precise measurement. There is always going to be a degree of uncertainty. Even if we are able to measure a temperature of 32.42 degrees with two significant numbers, we will never know the exact temperature.

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

- *Rahul choudhary is currently pursuing masters degree program in information technology engineering in M.I.T. ujjain R.g.p.v., India, MOB-09098390099. E-mail:rahuldewu@gmail.com*
- *Abhishek raghuvanshi is currently Associate Professor of Computer Science Dept.in in M.I.T. ujjain R.g.p.v., India,, MOB-09827840107. E-mail:abhishek.raghuvanshi@yahoo.co.in*

## 2 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. AT&T's nationwide network suffered the most widespread malfunction in its history due to a software failure. (Communications Week. Hacker's doings are costly. January 29, 1990.14.) Robert Morris, Jr. was convicted of breaking federal I aw when he introduced a computer virus into Internet, affecting more than 6,000 computers. (Keller. J.J. Software bug closes AT&T's network, cutting phone service for millions in U.S. Wall Street Journal, January 16. 1990. A2.) Transition to a new companywide computer system introduced system errors that Caused reduced net income for the fourth quarter at Sun Microsystems Inc.( Greenstein, I. MIS snafu lost orders, could mean sun loss. Management Information Systems Week 10, 23 (June 5, 1989), 4.) American Airline's Sabre reservation system crashed for 13 hours when data from an Application program wiped out vi-

tal information. (Scheier, R.L. American Airline's still shoring up SABRE. PC Week, June 26, 1989, 65) Parker stated the importance of IT to an organization when he noted that the amount of time that an organization can go without computer services, or the' 'mean time to belly-up," was steadily decreasing (Parker, D, B. Computer Security Management. Reston VA: Reston Publishing, 1981).

.

## 3 RISK ASSESSMENT TECHNIQUE

Fuzzy metrics utilizes fuzzy descriptors. For example, assets may have values of large, medium, and small. Also, threats may have probabilities of occurrence of high, medium, and low. The simplest way for all participants in the risk analysis process to understand the descriptors is by labeling them. Participants may define' 'large" valued assets to be those from $1 million to $2 million, "medium" from $l00,000 to $ 1million, and "small" less than $100,000. Further, participants may define "high" probabilities of threats to be from 0.7 to 1.0, "medium" from 0.35 to 0.7, and' 'low" less than 0.35. The most elementary method for mathematically modeling these descriptors is to use the mean of the range of each descriptor. In our example, the mean of "large" valued assets is$L5 million, that of "medium" assets is $ 55O, OOO, and that of "small" assets is $ 50,000. The mean of "high" probabilities is 0.85, "medium" is 0.525, and "low" is 0.175. Therefore, the expected loss of a large asset under high probability of a threat equals Sl.5 million multiplied by 0.85, or $1,275 million. Another method that can be used to yield expected losses is to calculate the ranges of such losses.

For example, a large asset under high probability of a threat will yield expected losses from $700,000 to $2 million:

Low estimate = $1million x 0.7 = $700,000;

High estimate = $2 million x 1.0 = $2 million.

The difficulty of mathematically modeling fuzzy descriptors is illustrated by noting that the midpoint of the range of expected losses is $ 1.35 million. This figure is higher than that obtained above by multiplying the mean of the large asset range and the mean of the high probability range ($1,275 million). Both figures are "correct."

.

### 3.1 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 μz(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

   0 if x<-1
   μz(x) = x + 1 if -1 ≤ x <0 (1.4)
   1 –x if 0 ≤ x <1
   0 if 1≤ x

### 3.2 Fuzzy Set of operation

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

### 3.3 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)

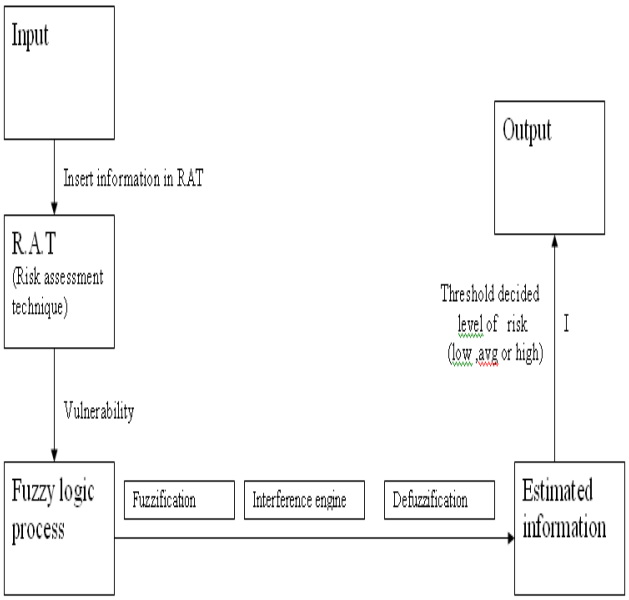
Rule 2: IF (C Score is low) and (C Ratio is bad) or (C Credit is bad)

Then (Decision is disapprove).

### 3.4 Fuzzy Interference System Editor

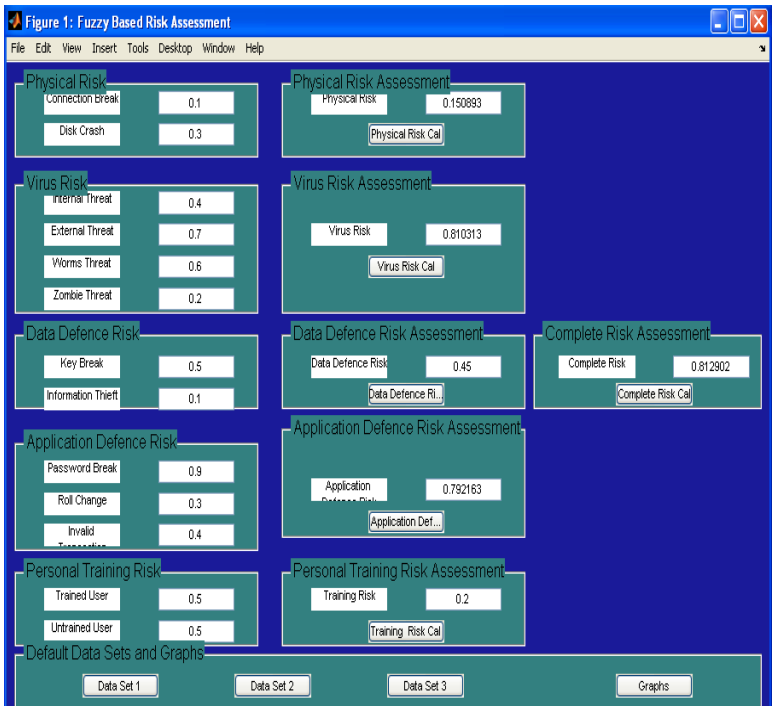
The FIS editor handles the high level issuing for the system such as the number of input and output variables an their names, types of the 'AND' and 'OR' operators, and the aggregation and defuzzification methods. The member ship function editor: The membership function editor is used to define the properties 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 fuzzy risk assessment technique is as follows:

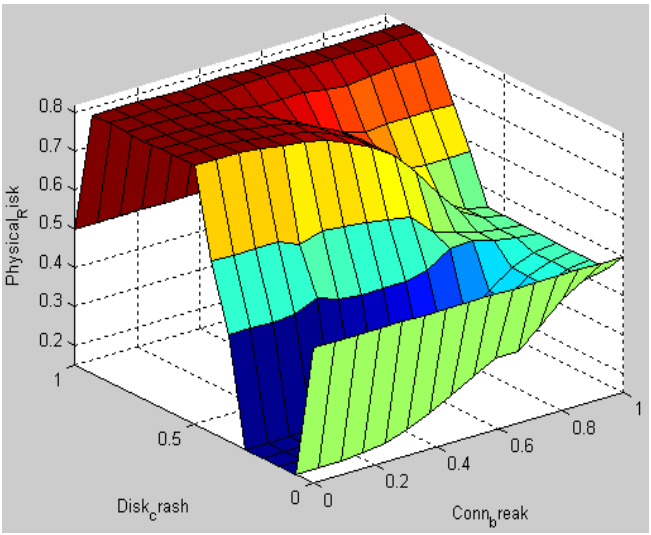



In developing the fuzzy risk assessment technique in the Appliances / Systems will be produced by adopting The Fuzzy design phase, the risk analysis methodology from ISO/IEC Risk Assessment technique. Four Level are been justified as: - 27001, ISO/IEC 27005 and shall be considered. Then the Level 1 – Goal , Level 2 – Risk Category, Level 3 – Fuzzy risk assessment technique proposed by will be adopted and Potential Category and Level 4 – Risk 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 "likely" and "resulting" of each risk done by all evaluators.

## 4 RISK ASSESSMENT TOOLS




## 5 SIMULATION



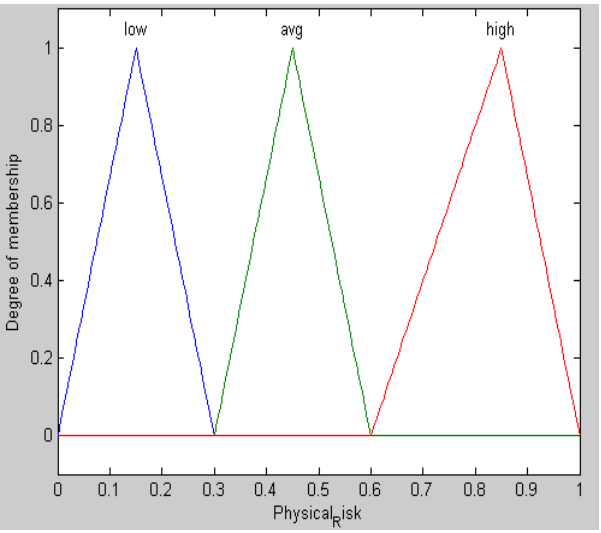



**TABLE 1**
FUZZY SET REPRESENTATION

| Likely level | Resulting level | Fuzzy triangle interval | Value varies according result |
|---|---|---|---|
| Low | Low | (0,0.15,0.3) | $0 \le x \le 0.15$ |
| Average | Average | (0.3,0.45,0.6) | $0.3 \le x \le 0.45$ |
| High | High | (0.6,0.85,1.0) | $0.6 \le x \le 0.85$ |

'x' range from 0 to 1

## 6 CONCLUSION

Fuzzy Logic provides a different way to approach a control or classification problem. In this research paper we are tried to developed the new security strategy to fight with risk and shows the level of risk which is harmful for our system or not through estimation of risk 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.

## Acknowledgment

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.

## REFERENCES

[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]. 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.
[6]. Parker, D,B. *Computer Security ManagemerU.* Rcsion, VA: Reston Publishing, 1981
[7]. 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.
[8]. Keller. J.J. Software bug closes AT&T's network, cutting phone sravice for millions in U.S. *Wall Street Journal,* January 16. 1990. A2.
[9] Risk Analysis for Information Technology Rex Kelly Rainer.Jr., Charles A. Snyder,and Houston H. Carr.1991
[10] Gary Stoneburner, Alice Goguen1, and Alexis Feringa1, Risk Management Guide for Information Technology Systems, July 2002.
[11]. Xiaohong Gan (2008) "Research on Risk Aversion of E-government Network Security". ieee research paper.
[12] Taroun, A., Yang, J.B. and Lowe, D. Construction Risk Modelling and Assessment: Insights from a LiteratureReview, 2012