I.J. Intelligent Systems and Applications, **2014, 07, 60-65**
Published Online June 2014 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijisa.2014.07.08

A New Hybrid Method for Risk Management in Expert Systems

Fereshteh Mohammadi
School of Electrical and Computer Engineering, Shiraz University, Shiraz, Iran
Email: fereshteh_mohammadi@ymail.com

Mohammad bazmara
School of Electrical and Computer Engineering, Shiraz University, Shiraz, Iran
Email: Mohamad.bazmara@gmail.com

Hatef Pouryekta
Islamic Azad University of Abhar, Zanjan, Iran
Email: Pouryekta@live.com

Abstract—Information security management is a part of information management, whose main task is to determine information goals and remove obstacles on the way of achieving such goals with providing necessary strategies. Information management is responsible to implement and control the performance of the organization`s security system while tries to keep it up to date. The purpose of information security management in an organization is maintaining different sorts of resources as software, hardware, information, communication and human resources.

The organization needs an integrated program against threats such as unauthorized access to information, environmental risks and dangers caused by users. In the present paper, the IT risk in an organization was assessed through an intelligent system benefiting from fuzzy analysis and certainty factors. As most of ambiguity samples have a level of belie, so doubt and the degree of membership were calculated as a part of output in the system and a better result achieved compared to previous methods.

Index Terms— Risk Assessment, Expert Systems, Certainty Factor, Fuzzy Logic

I. INTRODUCTION

1.1 Fuzzy theory

During the past few years, we have witnessed a rapid growth in the number and variety of applications of fuzzy logic and neural networks, ranging from consumer electronics and industrial process control to decision support systems and financial trading. Thus, Neuro-Fuzzy and soft computing, with their ability to incorporate human knowledge and adapt their knowledge base via new optimization techniques, are likely to play increasingly important roles in the conception and design of hybrid intelligent systems.

From conventional AI to computational Intelligence

Humans usually employ natural language in reasoning and drawing conclusions. Conventional AI research focuses on an attempt to mimic human intelligent behavior by expressing it in language forms or symbolic rules. Conventional AI basically manipulates symbols on the assumption that such behavior can be stored in symbolically structured knowledge bases. This is the so-called physical symbol system hypothesis.

Symbolic systems provide a good basis for modeling human experts in some narrow problem areas if explicit knowledge is available. Perhaps the most successful conventional AI product is the knowledge-based system or expert system.

Calling soft computing constituents "parts of modern AI" inevitably depends on personal judgment. It is true that today many books on modern AI describe neural networks and perhaps other soft computing components.

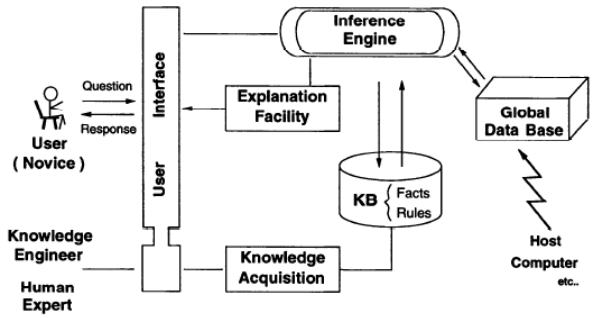

Fig.1. An expert system: one of the most successful AI products.

The long-term goal of AI research is the creation and understanding of machine intelligence. From this perspective, soft computing shares the same ultimate goal with AI. Fig.2. is a schematic representation of an intelligent system that can sense its environment (perceive) and act on its perception (react). An easy extension of ES may also result in the same ideal computationally intelligent system sought by soft computing researchers. Soft computing is apparently evolving under AI influences that sprang from cybernetics.

1.2 Fuzzy set theory

The human brain interprets imprecise and incomplete sensory information provided by perceptive organs.

Fuzzy set theory provides a systematic calculates to deal with such information linguistically, and it performs numerical computation by using linguistic labels stipulated by membership functions. Moreover, a selection of fuzzy if-then rules from the key component of a fuzzy inference system (FIS) that can effectively model human expertise in a specific application.

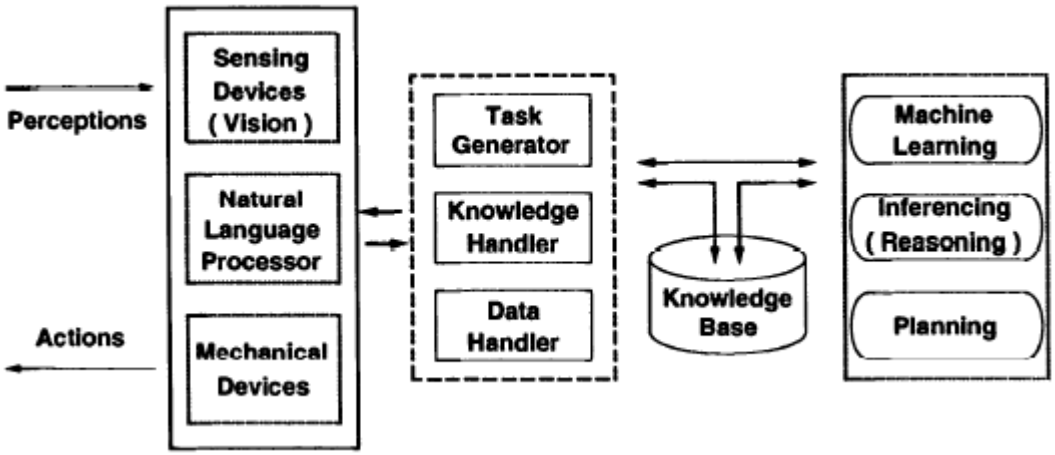

Fig. 2. An Intelligent System.

Although the fuzzy inference system has a structured knowledge representation in the form of fuzzy if-then rules, it lacks the adaptability to deal with changing external environments.

A classical set is a set with a crisp boundary. For example, a classical set A of real numbers greater than 6 can be expressed as

$$A=\{x \mid x>6\},$$

Where there is a clear, unambiguous boundary 6 such that if x is greater than this number, than x belongs to the set A; otherwise x does not belong to the set.

In contrast to a classical set, a fuzzy set, as the name implies, is a set without a crisp boundary. Let X be a space of objects and x be a generic element of X. A classical set A, $A \subseteq X$, is defined as a collection of elements or objects $x \in X$, such that each x can either belong or not belong to the set A. By defining a characteristic function for each element x in X, we can represent a classical set A by a set of ordered pairs (x,0) or (x,1), which indicates $x \notin A$ or $x \in A$, respectively.

Unlike the aforementioned conventional set, a fuzzy set [9]. Expresses the degree to which an element belongs to a set. Hence the characteristics function of a fuzzy set is allowed to have values between 0 and 1, which denotes the degree of membership of an element in a given set.

Fuzzy sets and membership functions

If X is a collection of objects denoted generically by x, then a fuzzy set A in X is defined as a set of ordered pairs:

$$A=\{(x, \mu A(x)) \mid x \in X\},$$

Where μA(x) is called the membership function (or MF for short) for the fuzzy set A.

The MF maps each element of X to a membership grade (or membership value) between 0 and 1.

Obviously, the definition of a fuzzy set is a simple extension of a classical set in which the characteristic function is permitted to have any values between 0 and 1. If the value of the membership function μA(x) is restricted to either 0 or 1, then A is reduced to a classical set and μA(x) is the characteristic function of A. For clarity, we shall also refer to classical sets as ordinary sets, crisp sets, non-fuzzy sets or just sets.

Usually X is referred to as the universe of discourse, or simply the universe and it may consist of discrete (ordered or non-ordered) objects or continuous space.

A fuzzy set is uniquely specified by its membership function. To describe membership functions more specifically, we shall define the non-enclosure used in the literature.

1.3 What is expert system

A computer program designed to model the problem-solving ability of a human expert

There are two major trails of an expert we attempt to model in our system: the expert's knowledge and reasoning. To accomplish this, the system must have two principal modules: a knowledge base and an inference engine. This simple view of an expert system is illustrated in fig.3.

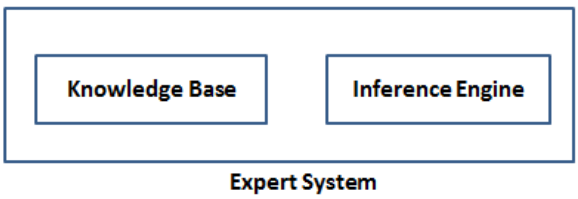

Fig. 3.Expert system block diagram

The knowledge base contains highly specialized knowledge on the problem area as provided by the expert. It includes problem facts, rules, concepts and relationships.

The inference engine is the knowledge processor which is modeled after the expert's reasoning. The engine works

with available information on a given problem, coupled with the knowledge stored in the knowledge base, to draw conclusions or recommendations. How we design this engine is the subject of inference techniques.

1.4 Replacement of expert

Stating that you are developing an expert system to replace a human produces ominous overtones. It brings forth the same resentful images envisioned by our forefathers, as they watched the march of the industrial revolution-machine replacing man. Though the potential exists, in practice the use of an expert system in place of a human has played a less foreboding role.

Some of the principal reasons expert systems are developed to replace an expert are:

- Make available expertise after hours or in other locations
- Automate a routine task requiring an expert.
- Expert is retiring or leaving.
- Expert is expensive.
- Expertise is needed in a hostile environment.

1.5 How are expert systems used?

Experts perform a generic set of tasks when solving certain types of problems such as diagnosis or planning. Regardless of the application area, given the type of problem, the expert collects and reasons with information in similar ways. Expert systems likewise are designed to accomplish generic tasks on the basis of the problem type.

1.6 Expert system structure

Expert systems solve problems using a process that is very similar to the methods used by a human expert, using a structure shown in fig.5.

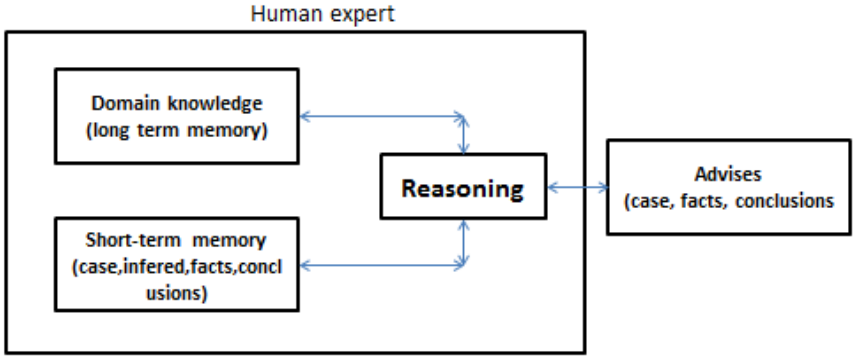

Fig. 4. Human expert problem solving

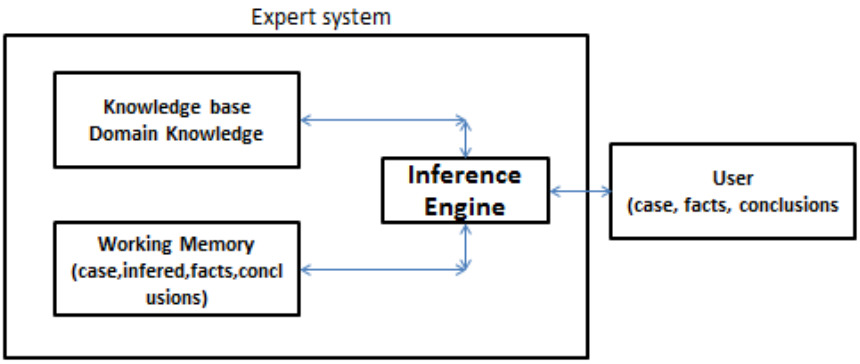

Fig. 5. Expert system problem solving

Knowledge base: an expert system maintains the expert's domain knowledge in a module known as the knowledge base that is a model for the LTM block of fig.

Working memory: contains the facts about a problem that are discovered during a conclusion. The working memory is a model for the STM block of fig.

Inference engine: the expert system models the process of human reasoning with a module known as the inference engine.

Explanation facility: a read mark of expert systems is their ability to explain their reasoning. Though not shown in figure. DOVOM. An expert system has an additional module called the explanation facility. Using this facility, an expert system can provide an explanation to the user about why it is asking question and how it reached some conclusion.

Inference: the interaction between an expert system and user is concluding in a natural language style. The interaction is also highly interactive and follows closely the conversation found between humans. To conduct this process in a manner that is acceptable to the user places special demands on you when designing the user interface.

The issues of access to information and security and

data protection have been the concern of rulers at a country level since long years ago and access to national and military information sometimes has caused ethnic destruction. With development of Information Technology and using information as a profitable business tool, security information takes new dimensions. In today's world information plays a key role as the capital of an organization a data protection is one of the most important components in organization survival.

Economic globalization has resulted in worldwide competition and a large number of companies have to cooperate with other companies in order to have a continued presence at global arena. Therefore, classification, rating and protecting information resources of the organization (either information systems or members of the organization) is highly essential. Information management system is a tool to implement and control software and hardware security of an information system.

The probability of a risk event is called with the results [2]. The Risk is also defined as "the analysis of the risk of loss due to a specific threat against a specific asset in relation to any protective measures is described for determining vulnerability." [3]." Risk is an inevitable activity that is a part of our daily lives. There is no universal description of the term "risk", while different specialists give different interpretation of this term.

One of the most general definitions is that risk is the "combination of the probability of an event and its consequence when there is at least the possibility of negative consequences [4]." Any way to measure, manage and reduce risk occurs, Due to the unpredictable and uncertain nature of the risk. "The level of risk associated with threats and vulnerability is influenced by the likelihood that this event can occur, the security measures in place to mitigate the risk and the impact the occurrence of this event can have on the institution."[5].

In the second section - the approach has been presented - we described our method which was the use of "membership function" in phase and "the degree of certainty" in expert system, and the level of risk was defined for credibility then three main parameters which were effective in risk creation were mentioned.

In the next section - experiences - to realize our idea, we get the help of several experts in this field in order to provide the relevant evidence of the risk event. Then the error rate obtained from the difference between the response of experts and the proposed hybrid system has been calculated by the use of formula (1).

In section three- Results –The results of experts and expert system, fuzzy system, and hybrid system have been studied and it was found that the new hybrid system acted much closer to what actually has happened.

II. THE PROPOSED APPROACH

Crisp values is not always possible; the linguistic description of the risk is due to the complex nature of risk is effectively. Considering "think of risk" must also be important. Therefore, we determined the coefficients of the fuzzy logic and certainty factor in expert systems for risk and will certainly concept. The mathematics of fuzzy sets and fuzzy logic is discussed in detail in many books and articles [**6, 7** and **8**].Today, fuzzy logic is used in different sciences such as : Identify quality soccer goalkeeper [9], Fuzzy Theory with Uncertainties in Geographic Information Systems [10] and even in agriculture [11].

And there is a lot of works about uncertainties in fuzzy logic [12].

Our logical model consists of three main sections. (Fig. 1):

- Input unit
- Inference engine
- Output unit

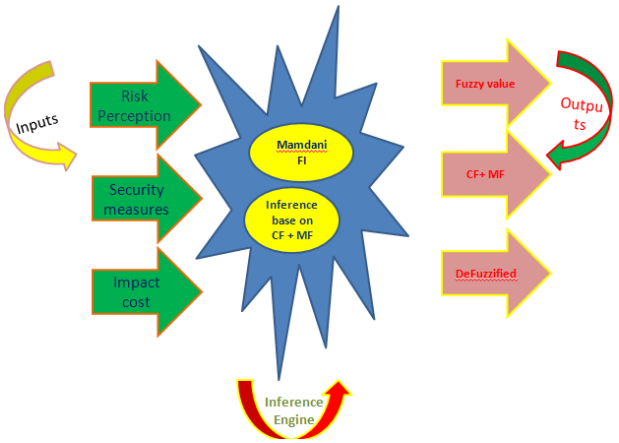

Fig. 6. Conceptual Model of System

The Input Unit:

Fig.6 illustrates the overall view of the system from a conceptual point of view Input systems, is based on the certainty factor and fuzzy. Based on the perceived risk, the potential impact of security measures to reduce risk and vulnerability assessment will happen. The input will consist of the following three groups of input data.

Risk Perception (Likelihood): Risk Perception describes the likelihood of the risk. The fuzzy set described by Table 1 is used to model the likelihood of a threat or vulnerability taking place. The linguistic variables "unlikely", "possibly" and "likely" are used to express the perceived likelihood of risk.

Table 1. FUZZY AND CERTAINTY VALUES FOR RISK PERCEPTION

Linguistic Value	Numerical range	Certainty Factor
Unlikely	0-4	0.4
Possibly	2-8	0.6
Likely	6-10	0.8

This perception (likelihood) can be changed overtime based on the frequency of the particular vulnerability.

Security Measures (Mitigation): The measure of risk associated with a threat or vulnerability is affected by the efficacy of the mitigation measures in place to combat

that threat or vulnerability. The linguistic variables in Table 2 are used to measure the level of security. A threat with a greater measure of the security has a lower Contribution to the certainty of risk.

Table 2. FUZZY AND CERTAINTY VALUES FOR SECURITY MEASURES

Linguistic Value	Numerical range	Certainty Factor
Blow Average	0-3	0.9
Average	2-5	0.65
Good	4-7	0.3
Excellent	6-10	0.2

Impact Cost: The cost associated with the occurrence of a threat or vulnerability has a significant impact on the level of risk associated with the event. The variables in Table 3 described the values used to measure the impact. The greater the impact cost the greater the contribution to the certainty of risk.

Table 3. FUZZY AND CERTAINTY VALUES FOR IMPACT COST

Linguistic Value	Numerical range	Certainty Factor
Low Cost	0-4	0.25
Moderate Cost	3-7	0.5
Costly	6-10	0.75

Due to the number of input fuzzy sets, we have a total of 36 laws. After input fuzzy values obtained using the coefficient of certainty, the risk assessment will be carried out. If you have a rule as follows:

IF e1 AND e2 … AND en THEN h
Then the certainty factor (CF) Act will come up as follows:
*CF[h,e] = min[CF(e1),CF(e2),…,CF(en)]*CF(rule)*
CF (e) is introduction of the certainty factor.

If the number of laws are high, and Want to combine them to obtain the final coefficients, we use the following equation: CF [CF1,CF2] = CF1 + CF2(1 - CF1)
That CF1 is certainty factor of rule1 and the CF2 is certainty factor of rule2.

III. EXPRIMENT

In order to assess an expert system design, we compare obtained values from 5 individuals. These five persons include: a software engineer, a control engineer and 3 engineers working in IT security organization. 10 different test data are given separately as an expert system output to five informed persons. The results are shown in table 4.

Table 4. THE RESULTS OF ALL SYSTEMS

NO	Inputs			Results(Outputs(CF))							
	Risk Perception	Security Measures	Impact Cost	Hybrid Sys.	Fuzzy Sys.	Exp. Sys.	Exp1	Exp2	Ex3	Exp4	Exp5
1	1	2	1.5	.225	.2	.225	.175	.15	.175	.15	.05
2	4	1	3	.2	.2	.2	.175	.15	.075	.025	.075
3	5	3	4	.4	.5	.4	.1	.25	.1	.1	.35
4	2	4	3.5	.442	.375	.225	.424	.405	.405	.376	.208
5	3	1.5	8	.65	.607	.24	.483	.155	.311	.226	.422
6	6	9	1	.18	.2	.18	.18	.06	.1	.18	.02
7	7.5	8	4	.278	.2	.14	.226	.311	.154	.172	.246
8	9	2	8	.675	.8	.585	.525	.075	.225	.075	.45
9	8	7	6.5	.243	.2	.12	.154	.196	.21	.098	.229
10	8	1	9.5	.675	.8	.675	.525	.075	.225	.075	.45

In order to find out the percent error of the expert system in diagnosis of risk occurrence, the experimental inputs of the previous table need to be really tested and compared with expert system output values. Regarding the real values obtained, the percent error of each input data is calculated using the following formula:

$$\%Error = \frac{|Exact\ Value - System\ Value|}{Exact\ Value} \times 100 \qquad (1)$$

Where exact value indicates real value and System Value is indicator of expert system output. By averaging percent errors for all 10 types of data, percent error of system and consequently the success rate are obtained. We follow the same procedure to obtain the success rate of 5 other persons, which its values are given in the following table.

Table 5. EVALUATE THE SUCCESS RATE OF THE SYSTEM

Type of systems	The success rate
Hybrid system	84
Fuzzy system	80.3
Expert system	64.1
Expert1	54.7
Expert2	52.6
Expert3	46.2
Expert4	37.2
Expert5	32.2

Considering the above values, we can say that the success rate of expert system in diagnosing risk using hybrid system is considerably good compared to other individuals.

IV. Conclusion

In the present study a hybrid system based on fuzzy reasoning and vague factor has been used in order to manage risk phase with respect to factor like vague and unexpectedness. The risk assessment phase needs to be evaluated continuously and simultaneously with emerging new threats. Risk assessment is a necessary phase in advancing in any kind of system and related data should be tangible in order to establish principles, methods and system reliability factors. The obtained results suggest that designed hybrid system can assess risk in various input conditions in an acceptable way.

References

[1] Darby, J., (2006), "Evaluating Risk from Acts of Terrorism with Belief and Fuzzy Sets", Carnahan Conferences Security Technology, Proceedings 2006 40th Annual IEEE International Oct. 2006 Page(s): 273 – 280.

[2] Anderson, K. "Intelligence-Based Threat Assessments for Information Networks and Infrastructures: A White Paper", 2005.

[3] ISO/IEC. Risk Management-Vocabulary-Guidelines for Use in Standards. ISO/IEC Guide 73, 2002.

[4] Dudeck, J., Dan, Q., (1992), *"Some Problems Related with probabilistic interpretations for certainty factor"*, Computer based Medical Systems, 1992 Proceedings, 5th Annual IEEE symposium on AI, Pages (538 -545).

[5] Heckerman, David E. , Shortliffe, Edward H. "From Certainty Factors to Belief Networks" To appear in Artificial Intelligence in Medicine, 1992.

[6] Andrew L.S. Gordon, Ivan Belik, Shahram Rahimi (2010), "A Hybrid Expert System for IT Security Risk Assessment", International conference on parallel and distributed processing techniques and applications (PDPTA'10), Las Vegas,

[7] Ruspini, E.H., P.P. Bonissone, and W. Pedrycz, Handbook of fuzzy computation. 1998: Institute of Physics Pub.

[8] Grint, K., Fuzzy management: Contemporary ideas and practices at work. 1997: Oxford University Press Oxford.

[9] Zadeh, L.A., Fuzzy sets. Information and control, 1965. 8(3): p. 338-353.

[10] M. Bazmara, S. Jafari, and F. Pasand, "A Fuzzy expert system for goalkeeper quality recognition," International Journal of Computer Science Issues, 9(5), 2012, pp. 318.

[11] F. Mohammadi, and M. Bazmara, "A New Approach of Fuzzy Theory with Uncertainties in Geographic Information Systems", *Journal of Mechatronics, Electrical and Computer Technology,* 3(6): pp. 1001-1014, 2013.

[12] Azadi, H., et al., *Sustainable rangeland management using fuzzy logic: A case study in Southwest Iran.* Agriculture, Ecosystems & Environment, 2009. 131(3): p. 193-200.

[13] F Mohammadi, M. Bazmara, A New Survey of types of Uncertainties in Nonlinear System with Fuzzy Theory. International Journal of Mechatronics, Electrical and Computer Technology, 2013. 3(7): p. 1036-1047.

Authors' Profiles

Fereshteh Mohammadi was bornin 1982 inZanjan, Iran. She has been teaching since 2009. She received the B.S. degree in Software Field from Zanjan Azad University and she received his M.Sc. degree in artificial intelligence from the School of Electrical and Computer Engineering, Shiraz University, Shiraz, Iran, in 2013. Her research interests include robotics, fuzzy logic, neural networks, expert systems and machine vision.

Mohammad Bazmara was born in 1987, he received his M.Sc. degree in artificial intelligence from the School of Electrical and Computer Engineering, Shiraz University, Shiraz, Iran, in 2013. His research interests include fuzzy logic, statistical pattern recognition, evolutionary algorithms and machine learning.

Hatef pourYekta was bornin 1983 inTehran, Iran. He receieved the B.S. degree in Electrical Engineering–Power from Abhar Azad University.

How to cite this paper: Fereshteh Mohammadi, Mohammad bazmara, Hatef Pouryekta,"A New Hybrid Method for Risk Management in Expert Systems", International Journal of Intelligent Systems and Applications(IJISA), vol.6, no.7, pp.60-65, 2014. DOI: 10.5815/ijisa.2014.07.08

