Fuzzy Multi-Criteria Decision-Making for Information Security Risk Assessment

A. Shameli-Sendi*,[1], M. Shajari[2], M. Hassanabadi[2], M. Jabbarifar[1] and M. Dagenais[1]

[1]Computer Engineering Department, Ecole Polytechnique de Montreal, Montreal, Canada

[2]Computer and Information Technology Engineering Department, Amirkabir University of Technology, Tehran, Iran

Abstract: Risk assessment is a major part of the ISMS process. In a complex organization which involves a lot of assets, risk assessment is a complicated process. In this paper, we present a practical model for information security risk assessment. This model is based on multi-criteria decision-making and uses fuzzy logic. The fuzzy logic is an appropriate model to assess risks and represents the practical results. The proposed risk assessment is a qualitative approach according to ISO/IEC 27005 standard. Main objectives and processes of business have been considered in this model and assessment of risk has been done in managerial and operational levels. This model was performed completely in the information technology section of a supply chain management company and the results show its efficiency and reliability.

Keywords: Risk assessment, information security, fuzzy logic, multi-criteria decision-making, ISO/IEC 27005.

1. INTRODUCTION

Today, many organizations and companies use information systems and network frameworks on a large scale, thus IT dependency is increasing daily. Security is one of the most important issues for the stability and development of these systems. Therefore, most organizations invest in this area and are establishing Information Security Management Systems (ISMS). Although many organizations understand the importance of security, many could not find an efficient solution to implement an ISMS.

The main process of an ISMS implementation is risk assessment [1, 2]. Risk assessment provides organizations with an accurate evaluation of the risks to their assets. It can help them prioritize and develop a comprehensive strategy to reduce risks. Information security risk assessment does not have an old history. There are some standards and methodologies for risk assessment, such as NIST and ISO27001, but while they explain general principles and guidelines, they do not give any implementation details [3]. This may cause ambiguities to the users [4]. A practical model for information security risk assessment is presented in this paper; it can be used by various organizations. Considering the limitations of quantitative approaches, this model recommends a qualitative method based on expert opinions and fuzzy techniques for information security risk assessment. The relevant knowledge from human experts is stored as rules database in order to apply fuzzy logic and infer an overall numerical value [5].

The paper is organized as follows: first, we will investigate earlier work, and several existing methods for risk assessment will be introduced. Fuzzy modeling is illustrated in Section 3. The proposed model will be discussed in Section 4. Experimental results are presented in Section 5. Section 6 concludes the paper.

2. RELATED WORK

Multi-criteria decision-making (MCDM) for risk assessment have been applied to many issues such as risk of E-business development, software development, groundwater contamination, forestry, health centers and etc. Different methods have been used in determining the level of risk, most often based on measuring the impact of risk. Likewise some proposed techniques use predefined rule-based techniques. Information security risk assessment has a recent history, and related standards and methodologies are in progress.

Zhao *et al*. [6] evaluated network security risk by using probabilities, impact severity, AHP techniques and Shannon entropy technique. Decisions were made using fuzzy logic through linguistic variables. Shannon entropy technique was also applied in weighting decision matrix. Shannon entropy technique is useful to prioritize risks but cannot be used in calculations to determine the risk level.

Guan *et al*. [7] assessed risks according to the likelihood and impact factors of threats. In this method, risk factors are determined according to standard ISO17799 categorization. Then, it is assumed that determining the likelihood of each risk is similar to determining the weights in pairwise comparisons in the AHP method. Based on this view, the likelihood or weight of each risk factor is being determined using expert opinions. On the other hand, the vulnerability of each Information asset for each risk factor is considered equal to its impact severity, which takes its relative value from experts through linguistic variables. An important point in this paper is its assumption which should be thought about. The causes of similarity between weights of risk

*Address correspondence to this author at the Computer Engineering Department, Ecole Polytechnique de Montreal, P.O. Box 6079, Succ. Downtown, Montreal, Quebec, H3C 3A7, Canada; Tel: 1 514 340 4711; E-mail: alireza.shameli-sendi@polymtl.ca

1874-110X/12 2012 Bentham Open

factors and their occurrence likelihood have not been defined in this paper. Also, the reason for considering the vulnerability of an asset to a risk factor as its impact severity is not clear. As mentioned in [1], the vulnerability is assumed to be a determining factor of likelihood of risk, rather than its severity impact.

Hwang and Yoon [8] proposed the simple additive weight (SAW) method which is the most widely used in multi-criteria decision-making. This technique obtains a weighted sum of the performance ratings of each alternative under all attributes. In the first step of this method, it scales the values of all attributes to make them comparable and eventually it sums up the values of the all attributes for each alternative [9].

Wang and Elhag [10] proposed a fuzzy TOPSIS method based on alpha level sets and applied it in bridge risk assessment. In this example, the likelihood and impact of different threats are assumed in linguistic variable forms and then are applied in bridge risk assessment by multiplying their related fuzzy values. Likewise, four effective criterion on impact severity are introduced. Experts propose their opinions in the form of these four criterions and eventually the severity impact is calculated.

Haslum *et al*. [11] proposed a fuzzy model for online risk assessment in networks. The main contribution of their paper is the fuzzy logic controllers. They were developed to quantify the various risks based on a number of variables derived from the inputs from various components.

Shameli-Sendi *et al*. [12] presented the FEMRA model, which uses fuzzy expert systems to assess risk in organizations. The risk assessment varies considerably with the context, the metrics used as dependent variables, and the opinions of the persons involved. Asset classification has a very important role in information security management. They have designed a security cube, which is a combination of valuable and important assets from a security perspective of the organization, and the Zachman model.

The main contributions of this work is that the assessment process is divided into two levels: ***managerial*** and ***operational***. In operational level, with respect to regular categorization of Information Systems in organizations, some domains are defined and relative threats to each domain are determined. Then likelihood and impact of threat occurrence are assessed and calculated using MCDM and with each realm experts. The distinct approach of this model, compared with previous models, is that for determining likelihood and impact of each threat, effective criterions are considered for their measurement, and experts present their opinions with respect to these criterions. Therefore, assessment of likelihood and impact is based on effective criterions. It leads us to increasing accuracy and reliability of the results.

Another advantage of this model, compared with others, is that assessment of risks is not only done technically, but also the importance of Information Systems is taken into account with respect to goal and mission of organization and main procedures of business.

3. FUZZY MODEL

Human experts rely on their experience and judgement to estimate the risk. The concept of risk has a different meaning for different people. Fuzzy model is the best model to tackle this weakness. In this section, some definitions and properties used in this paper are introduced:

Definition 1) There are different fuzzy numbers, the most interesting to calculate being triangular (see Fig. **1**) and trapezoidal fuzzy numbers.

Definition 2) Fuzzy set $\bar{A} = (a, b, c)$ on real number domain is called a triangular fuzzy number if its membership function has the specifications:

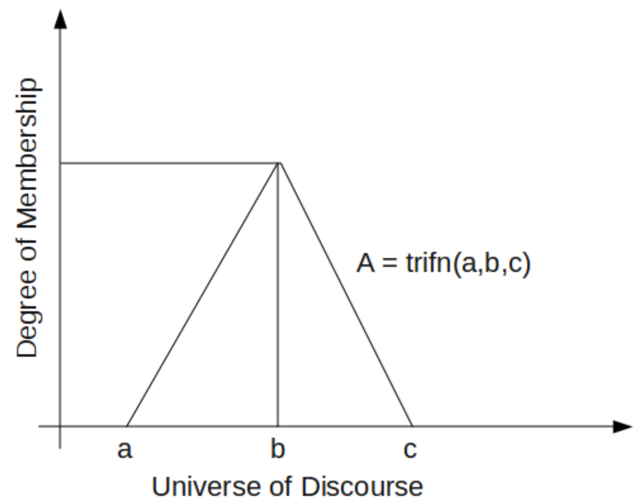

Fig. (1). Triangular fuzzy number and its membership function.

$$\gamma(X) = \begin{cases} \dfrac{(x-a)}{(b-a)} & if\ a \le x \le b \\ \dfrac{(x-c)}{(b-c)} & if\ b \le x \le c \\ 0 & otherwise \end{cases} \quad (1)$$

Property 1) Given two positive triangular fuzzy numbers A and B, the main operations on them can be expressed as follow [13]:

$$\begin{aligned} &\bar{A} = (a,b,c) \\ &\bar{B} = (d,e,f) \\ &\bar{A} + \bar{B} = (a+d, b+e, c+f) \\ &\bar{A} - \bar{B} = (a-f, b-e, c-d) \\ &\bar{A} \otimes \bar{B} = (ad, be, cf) \\ &\frac{\bar{A}}{\bar{B}} = (\frac{a}{f}, \frac{b}{e}, \frac{c}{f}) \\ &K \otimes \bar{B} = (Ka, Kb, Kc) \end{aligned} \quad (2)$$

Property 2) Yao and Chiang [14] compared Centroid and Signed distance methods and the results show that signed distance produces better results for defuzzification of triangular fuzzy numbers. The signed distance of triangular fuzzy number $\overline{A} = (a, b, c)$ is defined as follows and is used for defuzzification [15]:

$$A = \frac{a + 2b + c}{4} \tag{3}$$

Definition 3) In this model, linguistic variables are used to get experts opinion for weights of criteria and rate of alternatives, with respect to various criteria whose fuzzy equivalent is as follows [16]:

Table 1. Linguistic Variables and Fuzzy Equivalent for the Importance Weight of Each Criterion

Linguistic Variables	Fuzzy Triangular
Very low (VL)	(0, 0, 0.1)
Low (L)	(0, 0.1, 0.3)
Medium low (ML)	(0.1, 0.3, 0.5)
Medium (M)	(0.3, 0.5, 0.7)
Medium high (MH)	(0.5, 0.7, 0.9)
High (H)	(0.7, 0.9, 1.0)
Very high (VH)	(0.9, 1.0, 1.0)

Table 2. Linguistic Variables and Fuzzy Number for the Ratings

Linguistic Variables	Fuzzy Triangular
Very poor (VP)	(0, 0, 1)
Poor (P)	(0, 1, 3)
Medium poor (MP)	(1, 3, 5)
Fair (F)	(3, 5, 7)
Medium good (MG)	(5, 7, 9)
Good (G)	(7, 9, 10)
Very good (VG)	(9, 10, 10)

4. PROPOSED MODEL

Multi-criteria decision-making is a method based on decision making tables where the value of each alternative in decision making is determined by experts. The aim of multi-criteria decision-making techniques is to rate and determine the priority among different alternatives.

MCDM uses various methods, the most famous and widely used being: AHP, TOPSIS and SAW.

As mentioned, the AHP method [7] is based on pairwise comparisons and is very accurate, but cannot easily be accepted by experts. Also, in the entropy technique, if all alternatives in a criterion have "very high" value, it leads to high decrease on weight of that criterion. In this work, we are looking for actual value of alternatives and the relative value to the "very high" case should be used for determining the value of that alternative.

In TOPSIS [10], the chosen alternative should be as close as possible to the positive ideal and as far away as possible from the negative ideal solution. Therefore, if we apply the TOPSIS technique for assessing risk, it prioritizes and ranks the risks, but this is not our goal. Thus, the TOPSIS technique cannot be used directly in our model.

The Simple Additive Weighting method (SAW) [8] is the most popular approach for multi-criteria decision-making. In SAW technique, determining the weight of criteria in decision making tables is done according to answerers' opinion. Generally, this task is done either according to values of decision making tables like for the techniques of Shanon entropy and LINMAP, or it is directly determined by the answerers like pairwise comparisons or assigning weights directly by experts.

Since a practical model for any organization is our goal, the SAW technique was chosen for implementation. Also, since risk assessment is in a domain of ambiguous topics, fuzzy logic is appropriate for evaluation in uncertain subjects, and, by using it, experts can propose their opinion in a linguistic variable form like "very high", "low", etc.

The assessment process in the proposed model is divided into two levels: managerial and operational. Then, likelihood and impact of threat occurrence are assessed and calculated using MCDM and with each realm experts. The importance of each domain of Information systems is taken into account with respect to goals and mission of organization, and main procedures of business.

4.1. Assessment in Managerial Level

In this level, different domains of Information Technology (IT) assets are identified based on standard ISO/IEC 27005:

- Network services and communication infrastructures such as network software, hardware and connections.
- Hardware such as server and client computers.
- Application software such as financial system, production system and human recourse information systems.
- Databases.
- Knowledge and skills of the Information Technology personnel.
- Security equipment such as firewall and Antivirus.
- Communication services such as Email.
- Informational services such as Intranet (Web).
- Digital document such as technical plans and future designs.

Managers of Information Technology departments and other senior and intermediate managers, who are familiar with Information Systems, determine the importance of each asset domain by using SAW technology and the four main criterions: 1) the effect on the goals and mission of the organization 2) the effect on the main procedures of the organization 3) the effect on the production quality and organization services 4) the effect on customer relationship and satisfaction.

4.2. Assessment in Operational Level

In this level, in the first step, threats relative to each domain are determined based on [17] and appendixes B and C of standard ISO/IEC 27005 [18]. The occurrence likelihood of threats and their impact intensity are two main factors in risk level estimation. Therefore, in each domain, two decision making tables are made to evaluate these two factors. Then, each expert determines the importance of each criterion and the value of each alternative in relation to each criterion using linguistic variables. Eventually, using the SAW technique, the likelihood and impact of each threat will be clarified and the risk level is calculated by multiplying these two factors. The following table shows the effective criterions for determining the likelihood and impact intensity of threats:

Table 3. Effective Criterions for Determining the Likelihood and Impact Intensity of Threats

Effective Criterion	Effective Criterion
for impact intensity	for occurrence likelihood
Financial cost	Attraction of information asset
Time cost (lost)	Simplicity of gaining profit
Credit cost	Vulnerability
Human cost	Existing control
	History of threats

4.3. Execution Stages

To implement this model, 11 steps have to be done [9, 19]):

Step 1) Obtain expert opinions in the form of linguistic variables about the importance of each domain of Section 4.1. It must be done based on decision making table (Table **1**) that shows the weight of each criteria.

Step 2) Obtain expert opinions in the form of linguistic variables to evaluate the importance of the criteria.

Step 3) Obtain expert opinions of each domain about of likelihood and impact of each threat related to each domain in the form of linguistic variables (Table **2**).

Step 4) Replace linguistic variables with fuzzy variables based on Tables **2** and **3**. Merge all expert opinions in each domain and establish a decision making matrix. $\tilde{x}_{ij}$ and $\tilde{w}_j$ are triangular fuzzy numbers and assume that our decision group has k persons:

$$\tilde{x}_{ij} = (a_{ij}, b_{ij}, c_{ij})$$
$$\tilde{w}_j = (w_{j1}, w_{j2}, w_{j3})$$
$$\tilde{x}_{ij} = \frac{1}{K}[\tilde{x}_{ij}^1(+)\tilde{x}_{ij}^2(+)..(+)\tilde{x}_{ij}^k] \tag{4}$$
$$\tilde{w}_j = \frac{1}{K}[\tilde{w}_j^1(+)\tilde{w}_j^2(+)..(+)\tilde{w}_j^k]$$

$$\tilde{D} = \begin{bmatrix} \tilde{x}_{11} & \tilde{x}_{12} & \cdots & \tilde{x}_{1n} \\ \tilde{x}_{21} & \tilde{x}_{22} & \cdots & \tilde{x}_{2n} \\ \vdots & \vdots & \cdots & \vdots \\ \tilde{x}_{m1} & \tilde{x}_{m2} & \cdots & \tilde{x}_{mn} \end{bmatrix} \tag{5}$$

$$\tilde{W} = [\tilde{w}_1, \tilde{w}_2, \ldots, \tilde{w}_n]$$

Step 5) Linear normalization of consolidated matrix through the following relationship (category B is related to incremental criteria and category C is related to decremental criteria):

$$\tilde{r}_{ij} = \begin{cases} \dfrac{a_{ij}}{c_j}, \dfrac{b_{ij}}{c_j}, \dfrac{c_{ij}}{c_j} & if\ j \in B \\ \dfrac{a_j^-}{c_{ij}}, \dfrac{a_j^-}{b_{ij}}, \dfrac{a_j^-}{a_{ij}} & if\ j \in C \end{cases} \tag{6}$$

$$c_j = max \quad c_{ij} \quad if \quad j \in B$$
$$c_j^- = min \quad a_{ij} \quad if \quad j \in C$$

Step 6) Deffuzification of combined weights through signed distance method and normalization through the following formula:

$$w_j = \frac{w_j}{\sum_j w_j} \tag{7}$$

Step 7) Calculate weighty matrix:

$$\begin{bmatrix} \tilde{x}_{11} & \tilde{x}_{12} & \cdots & \tilde{x}_{1n} \\ \tilde{x}_{21} & \tilde{x}_{22} & \cdots & \tilde{x}_{2n} \\ \vdots & \vdots & \cdots & \vdots \\ \tilde{x}_{m1} & \tilde{x}_{m2} & \cdots & \tilde{x}_{mn} \end{bmatrix} * \begin{bmatrix} w_1 \\ w_2 \\ \vdots \\ w_n \end{bmatrix} \tag{8}$$

Step 8) Multiply the fuzzy values of likelihood and impact of each threat and calculate the probability of the threat occurring in each domain.

Step 9) Deffuzification of fuzzy values by Signed Distance method for each threat and calculation of the risk level for each domain.

Step 10) Calculate the overall risk level of organization by multiplying the risk level of threat with every domain importance Coefficient.

Step 11) Match the result with Table **4** for determining how to deal with risks.

All the values of Table **4** were derived through the implementation of the 10-step risk assessment process for these individual ranges.

5. EXPERIMENTAL RESULTS

To verify the efficiency of the proposed model, it has been implemented in the IT section of a supply chain management company. In our evaluation, 81 threats [1, 20, 21] and 9 domains had been defined in advance. At first, to determine the importance of each domain, experts proposed their opinion in the form of linguistic variables, according to the managerial and operational levels. Table **5** illustrates the importance of each domain (Step1). The results are reasonable, based on the business process of this company and the relationship with its suppliers. Table **6** illustrates the threats related to the digital documents domain. We continue the presentation of our results with this domain and eventually with the results of all domains (Tables **21-28**).

Table 4. Estimated Levels of Risk Related to Different Scenarios

Estimated Levels of Risk	Range
Low-Low	0.00
Low-Medium	0.0670683
Low-High	1.9509554
Medium	14.0392099
High-Low	53.9383740
High-Medium	132.7093795
High-High	205.7530127

Table 5. Relative Importance of Different Domains in the Organization

Domain	Initial Weight	Normalized Weight	Normalized Weight *1000
Communication services	0.8594	0.137776135	137.78
Network services and communication infrastructures	0.8108	0.129984377	129.98
Informational services	0.774	0.124084642	124.08
Database	0.76515	0.122665272	122.67
Hardware	0.67612	0.108392263	108.39
Knowledge and skills of the personnel	0.65733	0.105380652	105.38
Application software	0.64724	0.103762883	103.76
Security equipments	0.52618	0.084354874	84.35
Digital documents	0.52146	0.083598903	83.6

Table 6. Digital Documents Threats

	Name
T1	Unauthorized access
T2	Unauthorized copy or send
T3	Unauthorized edit or delete

In the operational level, our goal is to indicate the likelihood and impact of each threat in each domain and, eventually, calculate the risk level. As Tables **7** and **8** illustrate, in the next step, experts compare the criterions related to likelihood and impact of threats (Step 2). The experts use the linguistic rating variables to assess the rating of threats with respect to likelihood and impact criterions as shown in Table **9** (Step3). Tables **10** and **11** show the fuzzy

Table 7. Importance Weight of Criteria Related to Likelihood of Threats

	DM1	DM2
C1: Attraction of information asset	H	H
C2: Simplicity of gaining profit	H	MH
C3: Vulnerability	MH	MH
C4: Existing control	ML	H
C5: History of threats	ML	M

Table 8. Importance Weight of Criterion Related to Impact of Threats

	DM1	DM2
C6: Financial cost	ML	M
C7: Time cost (lost)	MH	H
C8: Credit cost	VL	VL
C9: Human cost	VH	H

Table 9. The Ratings of the Three Threats of Digital Documents by Decision Makers Under All Criterions

Criteria	Threat	DM1	DM2
C1	T1	G	G
	T2	G	G
	T3	MP	F
C2	T1	MG	G
	T2	G	MG
	T3	MP	MG
C3	T1	F	G
	T2	MG	G
	T3	P	P
C4	T1	F	MG
	T2	MP	P
	T3	MG	G
C5	T1	MP	P
	T2	MP	MP
	T3	VP	VP
C6	T1	MP	MP
	T2	MP	MP
	T3	MG	F
C7	T1	G	MG
	T2	MG	G
	T3	G	VG
C8	T1	P	P
	T2	P	MP
	T3	MG	MG
C9	T1	VG	G
	T2	VG	MG
	T3	VG	MG

decision matrix and fuzzy weights of likelihood and impact of threats in digital documents domain. These tables are based on Tables **7-9**, using the conversion of the linguistic evaluation into triangular fuzzy numbers (Step4). As mentioned in Step 5, after constructing the fuzzy decision matrix, we have to create the normalized fuzzy decision matrix as Tables **12** and **13**. The results of Step 6 is related to deffuzification of combined weights as shown in these tables. Tables **14** and **15** show the weight matrices obtained based on the SAW method by multiplying each fuzzy value of Tables **12** and **13** with the related criterion weight (Step 7). We can calculate the value of likelihood and impact of each threat by adding all values related to each criterion, as in Tables **16** and **17**. The probability of a threat occurring in

Table 10. The Fuzzy Decision Matrix and Fuzzy Weights of Threats Likelihood in Digital Documents Domain

	C1	C2	C3	C4	C5
Weight	(0.7,0.9,1)	(0.6,0.8,0.95)	(0.5,0.7,0.9)	(0.4,0.6,0.75)	(0.2,0.4,0.6)
T1	(7,9,10)	(6,8,9.5)	(5,7,8.5)	(4,6,8)	(0.5,2,4)
T2	(7,9,10)	(6,8,9.5)	(6,8,9.5)	(0.5,2,4)	(1,3,5)
T3	(2,4,6)	(3,5,7)	(0,1,3)	(6,8,9.5)	(0,0,1)

Table 11. The Fuzzy Decision Matrix and Fuzzy Weights of Threats Impact in Digital Documents Domain

	C6	C7	C8	C9
Weight	(0.2,0.4,0.6)	(0.6,0.8,0.95)	(0,0,0.1)	(0.8,0.95,1)
T1	(1,3,5)	(6,8,9.5)	(0,1,3)	(8,9.5,10)
T2	(1,3,5)	(6,8,9.5)	(0.5,2,4)	(7,8.5,9.5)
T3	(4,6,8)	(8,9.5,10)	(5,7,9)	(7,8.5,9.5)

Table 12. The Fuzzy Normalized Decision Matrix of Threats Likelihood in Digital Documents Domain

	C1	C2	C3	C4	C5
Weight	0.26	0.23	0.21	0.17	0.12
T1	(0.7,0.9,1)	(0.63,0.84,1)	(0.53,0.74,0.89)	(0.06,0.08,0.13)	(0.1,0.4,0.8)
T2	(0.7,0.9,1)	(0.63,0.84,1)	(0.63,0.84,1)	(0.13,0.25,1)	(0.2,0.6,1)
T3	(0.2,0.4,0.6)	(0.32,0.53,0.74)	(0,0.11,0.32)	(0.05,0.06.0.08)	(0,0,0.2)

Table 13. The Fuzzy Normalized Decision Matrix of Threats Impact in Digital Documents Domain

	C6	C7	C8	C9
Weight	0.18	0.37	0.01	0.43
T1	(0.13,0.38,0.63)	(0.6,0.8,0.95)	(0,0.11,0.33)	(0.8,0.95,1)
T2	(0.13,0.38,0.63)	(0.6,0.8,0.95)	(0.06,0.22,0.44)	(0.7,0.85,0.95)
T3	(0.5,0.75,1)	(0.8,0.95,1)	(0.56,0.78,1)	(0.7,0.85,0.95)

Table 14. The Fuzzy Weighted Normalized Decision Matrix of Threats Likelihood in Digital Documents Domain

	C1	C2	C3	C4	C5
T1	(0.18,0.23,0.26)	(0.14,0.19,0.23)	(0.11,0.15,0.18)	(0.01,0.01,0.02)	(0.01,0.05,0.1)
T2	(0.18,0.23,0.26)	(0.14,0.19,0.23)	(0.13,0.18,0.21)	(0.02,0.04,0.17)	(0.02,0.07,0.12)
T3	(0.05,0.1,0.16)	(0.07,0.12,0.17)	(0,0.02,0.07)	(0,0.01.0.01)	(0,0,0.02)

Table 15. The Fuzzy Weighted Normalized Decision Matrix of Threats Impact in Digital Documents Domain

	C6	C7	C8	C9
T1	(0.02,0.07,0.11)	(0.22,0.3,0.35)	(0,0,0)	(0.34,0.41,0.43)
T2	(0.02,0.07,0.11)	(0.22,0.3,0.35)	(0,0,0)	(0.3,0.36,0.41)
T3	(0.09,0.13,0.18)	(0.3,0.35,0.37)	(0,0,0.01)	(0.3,0.36,0.41)

digital documents domain is calculated in two phases as Table **18** illustrates: 1) multiplying the fuzzy values of likelihood and impact of each threat (Step 8): 2) Deffuzification of each fuzzy triangular with Signed Distance method (Step 9). Eventually, as Table **19** illustrates, the overall risk level of threats in digital document domain is calculated by multiplying the risk level of threat in number 83.6, which is the importance coefficient of digital document based on Table **5**.

Table 16. The Value of Threats Likelihood in Digital Documents Domain as Fuzzy Numbers

Threat	Fuzzy Triangular
T1	(0.45,0.63,0.79)
T2	(0.49,0.71,0.99)
T3	(0.12,0.25,0.43)

Table 17. The Value of Threats Impact in Digital Documents Domain as Fuzzy Numbers

Threat	Fuzzy Triangular
T1	(0.58,0.7,0.89)
T2	(0.54,0.73,0.87)
T3	(0.69,0.84,0.97)

Based on Table **4**, the risk level of all threats in digital document domain are between Medium and High-Low ranges. Thus, this domain does not present a critical risk. To verify the accuracy of the proposed model, we have compared the results with TOPSIS model. We have implemented the TOPSIS model and Table **20** illustrates this comparison. As seen in Table **20**, our model has the same results. To get better results, we got help from different experts for each threat and domain.

Table 18. The Probability of Threat Occurring in Digital Documents Domain as Fuzzy

Threat	Fuzzification Values of Risk Level	Defuzzification Values
T1	(0.26,0.44,0.7)	0.46
T2	(0.26,0.52,0.86)	0.54
T3	(0.08,0.21,0.42)	0.23

Using this process, we can calculate the risk level of all threats related to the other domains. At the end of paper, the results for all domains are available. Table **29** shows all threats with the related risk level in ascending mode.

Table 19. Final Results of Risk Level in Digital Documents Domain in Ascending Mode

Threat	Risk Level
T2: Unauthorized copy or send	45.14
T1: Unauthorized accessing	38.46
T3: Unauthorized edit or delete	19.23

Table 20. Comparison of SAW and TOPSIS Methods

Domain	SAW	TOPSIS	Ratio (SAW/TOPSIS)
Communication services	0.859	0.209	0.2431
Network services and communication infrastructures	0.811	0.199	0.245
Informational services	0.774	0.190	0.2451
Database	0.765	0.189	0.2464
Hardware	0.676	0.168	0.2491
Knowledge and skills of the personnel	0.657	0.165	0.2507
Application software	0.647	0.162	0.2509
Security equipments	0.526	0.136	0.2583
Digital documents	0.521	0.133	0.2558

Table 21. Final Results of Risk Level in Communication Services Domain in Ascending Mode

Threat	Defuzzification Value	Risk Level
T4: Identity theft	0.51755	71.31
T5: Unauthorized access to user emails	0.37518	51.69
T6: Abuse of Service	0.37329	51.43
T7: Dictionary attack	0.24992	34.43
T8: DoS	0.20551	28.32
T9: Spam	0.19472	26.83
T10: Malicious code	0.16933	23.33

Table 22. Final Results of Risk Level in Network Services and Communication Infrastructures Domain in Ascending Mode

Threat	Defuzzification Value	Risk Level
T11: Communication disruption	0.35724	46.43
T12: Back door in system	0.35137	45.67
T13: DoS	0.34288	44.57
T14: Man-in-the-middle Attack	0.31608	41.08
T15: Damage to communication lines	0.3021	39.27
T16: Redirection Attack	0.29629	38.51
T17: Sniffing	0.26807	34.84
T18: Address theft	0.25298	32.88
T19: Password cracking	0.25231	32.8
T20: Service disruption	0.246	31.98
T21: Network hardware technical problems	0.24453	31.78
T22: Network software technical problems	0.20071	26.09
T23: User errors	0.17244	22.41
T24: Tunneling	0.15447	20.08

6. CONCLUSION

To implement an ISMS, we need a powerful tool to assess risks within an organization. In this paper, we proposed a fuzzy expert system to assess the risks of Information Systems. In the proposed model, a fuzzy technique was used to connect expert opinions with linguistic variables. These linguistic variables reflect the expert opinions more precisely. The distinct approach of this model, as compared to previous models, is that for determining the likelihood and impact of each threat, effective criterions for their measurement have been considered. Finally, experts present their opinions with respect to specific criterions leading us to increased accuracy and reliability of the results.

Table 23. Final Results of Risk Level in Informational Services Domain in Ascending Mode

Threat	Defuzzification Value	Risk Level
T25: Access to send information	0.60391	74.93
T26: SSI Injection	0.60391	74.93
T27: SQL Injection	0.60391	74.93
T28: Predictable Resource Location	0.51165	63.49
T29: Unauthorized update of web page	0.49939	61.96
T30: Cross-site Scripting	0.48285	59.91
T31: Unauthorized access to information	0.47178	58.54
T32: Insufficient Session Expiration	0.45691	56.69
T33: XPath Injection	0.45372	56.3
T34: OS Commanding	0.43106	53.49
T35: Directory Indexing	0.41741	51.79
T36: LDAP Injection	0.19492	24.19
T37: Loss of information on Web site	0.11234	13.94

Table 24. Final Results of Risk Level in Database Domain in Ascending Mode

Threat	Defuzzification Value	Risk Level
T38: Unauthorized change in fields and tables	0.419892	51.51
T39: Password cracking	0.401368	49.24
T40: SQL Injection	0.390258	47.87
T41: Unauthorized access to server	0.333465	40.91
T42: Sniffing	0.330791	40.58
T43: DoS	0.301794	37.02
T44: Loss of information	0.288905	35.44
T45: Software error	0.145757	17.88

Table 25. Final Results of Risk Level in Hardware Domain in Ascending Mode

Threat	Defuzzification Value	Risk Level
T46: Depreciation of storage media	0.23892	25.9
T47: Earthquake	0.22543	24.43
T48: Hardware theft	0.15557	16.86
T49: Maintenance error	0.14907	16.16
T50: Human error	0.13287	14.4
T51: Power fluctuations	0.11514	12.48
T52: Explosion	0.10535	11.42
T53: Flood	0.09788	10.61
T54: Unauthorized change to hardware settings	0.07267	7.88
T55: Supply disruption	0.05952	6.45
T56: Electromagnetic waves	0.05775	6.26
T57: Unauthorized access to hardware or server room	0.05772	6.26
T58: Air conditioning Problem	0.05604	6.07
T59: Fire	0.05028	5.45
T60: Pollution and dust	0.03239	3.51
T61: Temperature	0.03214	3.48

Table 26. Final Results of Risk Level in Knowledge and Skills of the Personnel Domain in Ascending Mode

Threat	Defuzzification Value	Risk Level
T62: Dependency to personnel	0.55518	58.51
T63: Non-compliance with regulations concerning access level	0.50665	53.39
T64: Theft	0.43176	45.5
T65: Dissatisfied personnel	0.40716	42.91
T66: Shortage of skilled personnel	0.31012	32.68
T67: Human error	0.15665	16.51

Table 27. Final Results of Risk Level in Application Software Domain in Ascending Mode

Threat	Defuzzification Value	Risk Level
T68: Unauthorized update of information	0.47564	49.35
T69: Damaging by malware tools	0.4264	44.24
T70: Identity theft	0.42509	44.11
T71: Useing of the system in a abusive way	0.42499	44.1

(Table 27) contd…..

Threat	Defuzzification Value	Risk Level
T72: Unauthorized access to software	0.41248	42.8
T73: Repudiation of working with software	0.36195	37.56
T74: Entering false information into the software	0.31097	32.27
T75: Software error	0.20707	21.49
T76: Human error in the software	0.16083	16.69

Table 28. Final Results of Risk Level in Security Equipments Domain in Ascending Mode

Threat	Defuzzification Value	Risk Level
T77: Bypass security controls	0.485389	40.94
T78: Unauthorized change to device options	0.313267	26.42
T79: Unauthorized access to information	0.279961	23.61
T80: Device damage and failure	0.236998	19.99
T81: Error on device performance	0.146913	12.39

Table 29. Risk Level of All Threats in All Domain in IT Section of a Supply Chain Management Company in Ascending Mode

	Risk	Domain	Risk Level
1	T25: Access to send information	Information services	74.93
2	T26: SSI Injection	Information services	74.93
3	T27: SQL Injection	Information services	74.93
4	T4: Identity theft	Communication services	71.31
5	T28: Predictable Resource Location	Information services	63.49
6	T29: Unauthorized update of web page	Information services	61.96
7	T30: Cross-site Scripting	Information services	59.91
8	T31: Unauthorized access to information	Information services	58.54
9	T62: Dependency to personnel	Knowledge and skills of the personnel	58.51
10	T32: Insufficient Session Expiration	Information services	56.69
11	T33: XPath Injection	Information services	56.3
12	T34: OS Commanding	Information services	53.49
13	T63: Non-compliance with regulations concerning access level	0.50665	53.39
14	T35: Directory Indexing	Information services	51.79
15	T5: Unauthorized access to user emails	Communication services	51.69
16	T38: Unauthorized change in fields and tables	Database	51.51
17	T6: Abuse of Service	Communication services	51.43
18	T68: Unauthorized update of information	Application software	49.35
19	T39: Password cracking	Database	49.24
20	T40: SQL Injection	Database	47.87
21	T11: Communication disruption	Network services and communication infrastructures	46.43
22	T12: Back door in system	Network services and communication infrastructures	45.67
23	T64: Theft	Knowledge and skills of the personnel	45.5
24	T2: Unauthorized copy or send	Digital document	45.14
25	T13: DoS	Network services and communication infrastructures	44.57
26	T69: Damaging by malware tools	Application software	44.24
27	T70: Identity theft	Application software	44.11
28	T71: Useing of the system in a abusive way	application software	44.1
29	T65: Dissatisfied personnel	Knowledge and skills of the personnel	42.91
30	T72: Unauthorized access to software	Application software	42.8
31	T14: Man-in-the-middle Attack	Network services and communication infrastructures	41.08
32	T77: Bypass security controls	Security equipments	40.94
33	T41: Unauthorized access to server	Database	40.91
34	T42: Sniffing	Database	40.58
35	T15: Damage to communication lines	Network services and communication infrastructures	39.27
36	T16: Redirection Attack	Network services and communication infrastructures	38.51
37	T1: Unauthorized accessing	Digital document	38.46
38	T73: Repudiation of working with software	Application software	37.56
39	T43: DoS	Database	37.02
40	T44: Loss of information	Database	35.44
41	T17: Sniffing	Network services and communication infrastructures	34.84

(Table 29) contd…..

	Risk	Domain	Risk Level
42	T7: Dictionary attack	Communication services	34.43
43	T18: Address theft	Network services and communication infrastructures	32.88
44	T19: Password cracking	Network services and communication infrastructures	32.8
45	T66: Shortage of skilled personnel	Knowledge and skills of the personnel	32.68
46	T74: Entering false information into the software	Application software	32.27
47	T20: Service disruption	Network services and communication infrastructures	31.98
48	T21: Network hardware technical problems	Network services and communication infrastructures	31.78
49	T8: DoS	Communication services	28.32
50	T9: Spam	Communication services	26.83
51	T78: Unauthorized change to device options	Security equipments	26.42
52	T22: Network software technical problems	Network services and communication infrastructures	26.09
53	T46: Depreciation of storage media	Hardware	25.9
54	T47: Earthquake	Hardware	24.43
55	T36: LDAP Injection	Information services	24.19
56	T79: Unauthorized access to information	Security equipments	23.61
57	T10: Malicious code	Communication services	23.33
58	T23: User errors	Network services and communication infrastructures	22.41
59	T75: Software error	Application software	21.49
60	T24: Tunneling	Network services and communication infrastructures	20.08
61	T80: Device damage and failure	Security equipments	19.99
62	T3: Unauthorized edit or delete	Digital document	19.23
63	T45: Software error	Database	17.88
64	T48: Hardware theft	Hardware	16.86
65	T76: Human error in the software	Application software	16.69
66	T67: Human error	Knowledge and skills of the personnel	16.51
67	T49: Maintenance error	Hardware	16.16
68	T50: Human error	hardware	14.4
69	T37: Loss of information on Web site	Information services	13.94
70	T51: Power fluctuations	hardware	12.48
71	T81: Error on device performance	Security equipments	12.39
72	T52: Explosion	hardware	11.42
73	T53: Flood	hardware	10.61
74	T54: Unauthorized change to hardware settings	hardware	7.88
75	T55: Supply disruption	hardware	6.45
76	T56: Electromagnetic waves	hardware	6.26
77	T57: Unauthorized access to hardware or server room	hardware	6.26
78	T58: Air conditioning Problem	hardware	6.07
79	T59: Fire	hardware	5.45
80	T60: Pollution and dust	hardware	3.51
81	T61: Temperature	hardware	3.48

ACKNOWLEDGEMENT

The support of the Natural Sciences and Engineering Research Council of Canada (NSERC) is gratefully acknowledged.

CONFLICT OF INTEREST

Declared none.

REFERENCES

[1] International Standard Organization, ISO/IEC 27005, Information Security Risk Management, 2008.

[2] G. Stoneburner, A. Goguen, and A. Feringa, "Risk management guide for information technology systems," 2002. [Online] Available: http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf .

[3] A. Shameli-Sendi, N. Ezzati-Jivan, M. Jabbarifar, and M. Dagenais, "Intrusion response systems: survey and taxonomy," *Int. J. Comput. Sci. Netw.Secur.*, vol. 12, no. 1, pp.1-14, 2012.

[4] ENISA, "Risk Management: Implementation principles and Inventories for Risk Management/Risk Assessment methods and tools," Technical Department of European Network and Information Security Agency, 2006.

[5] L. Zadeh, "Fuzzy sets," *Inf. Control.*, pp. 338-353, 1965.

[6] D. M. Zhao, J. H. Wang, and J.F. Ma, "Fuzzy Risk Assessment of Network Security," In: *Fifth International Conference on Machine Learning and Cybernetics,* Dalian: China, 2006, pp. 4400-4405.

[7] B. C. Guan, C. C. Lo, P. Wang, and J. S. Hwang, "Evaluation of information security related risk of an organization: the application of multi criteria decision making method," In: *IEEE 37th Annual International Carnahan Conference*, Taipei: Taiwan,2003, pp. 168-175.

[8] C. L. Hwang and K. Yoon, *Multiple Attribute Decision Making - Method and Applications*, SpringerVerlag: New York, 1981.

[9] S. Y. Chou, Y. H. Chang, and C. Y. Shen, "A fuzzy simple additive weighting system under group decision-making for facility location selection with objective/subjective attributes," *Oper.Res.*, vol. 189, pp.132-145, 2008.

[10] Y. M. Wang and T. M. Elhag, "Fuzzy TOPSIS method based on alpha level sets with an application to bridge risk assessment," *Expert Sys. Appl.*, pp. 309-319, 2006.

[11] K. Haslum, A. Abraham, and S. Knapskog, "Fuzzy Online Risk Assessment for Distributed Intrusion Prediction and Prevention Systems," In: *Tenth International Conference on Computer Modeling and Simulation*, Cambridge: IEEE Computer Society Press, 2008, pp. 216-223.

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

[13] A. Kaufmann and M. M. Gupta, *Introduction to Fuzzy Arithmetic: Theory and Applications*, Van Nostrand Reinhold: New York, 1985.

[14] J. S. Yao and J. Chiang, "Inventory without backorder with fuzzy total cost and fuzzy storing cost defuzzified by centroid and signed distance," *Oper. Res.,* vol. 148, pp. 401-409, 2003.

[15] J. S. Yao and K. Wu, "Ranking fuzzy numbers based on decomposition principle and signed distance," *Fuzzy Set Syst.,* vol. 116, pp. 75-88, 2000.

[16] S. H. Ghyym, "A semi linguistic fuzzy approach to multi actor decision making: application to aggregation of experts' judgments," *Ann. Nucl. Energy*, vol. 26, pp. 1097-1112, 1999.

[17] Web Application Security Consortium: Threat Classification. Available: http://www.webappsec.org/projects/threat .

[18] D. J. Landoll, "The security Risk Assessment Handbook," Auerbach Publications: USA, 2006.

[19] C. T. Chen, "A fuzzy approach to select the location of the distribution center," *Fuzzy Set Syst.,* vol. 118, pp. 65-73, 2001.

[20] National Institute of Standards and Technology (NIST), Special Publication 800-12, An Introduction to Computer Security:The NIST Handbook,1995.

[21] International Standard Organization, ISO/IEC TR 15446, Information technology – Security techniques - Guide for the production of Protection Profiles and Security Targets, 2004.

Received: January 2, 2012 Revised: May 2, 2012 Accepted: May 2, 2012