EVALUATION OF ELECTRONIC GOVERNMENT SECURITY ISSUES APPLIED TO COMPUTER CENTER OF BAGHDAD UNIVERSITY (CASE STUDY)

Ahmad O. Salman, Prof. Dr. Ghassan H. Abdul-Majeed, Ass. Prof. Dr. Tarik Z. Ismaeel

Abstract

Information security contributes directly to increase the level of trust between the government's departments by providing an assurance of confidentiality, integrity, and availability of sensitive governmental information. Many threats that are caused mainly by malicious acts can shutdown the e-government services. Therefore the governments are urged to implement security in e-government projects. Some modifications were proposed to the security assessment multi-layer model (*Sabri model*) to be more comprehensive model and more convenient for the Iraqi government. The proposed model can be used as a tool to assess the level of security readiness of government departments, a checklist for the required security measures and as a common security reference in the government organizations of Iraq. In order to make this model more practical, applicable and to represent the security readiness with a numerical value, evaluation modeling has been done for this model by using fuzzy logic tool of MATLAB R2010a program.

Since the risk assessment is considered as a major part in the information security management system, an effective and practical method to assess security risk is proposed by combining FEMRA (fuzzy expert model risk assessment) and Wavelet Neural Network (WNN). The fuzzy system is used to generate the training data set in order to make the required training for WNN. The proposed method is applied when a risk assessment case study is made at the computer center of Baghdad University. It is found from the numerical results that the risk levels obtained by WNN are (with maximum of 58.23) too close to these calculated from FEMRA (with maximum of 60), with an average error of 5.51%. According to these results, the proposed method is effective and reasonable and can provide the support toward establishing the e-government.

الخلاصة

تساهم أمن المعلومات بصورة مباشرة بزيادة مستوى الثقة بين الأقسام الحكومية عن طريق ضمان السرية, السلامة, وتوفير المعلومات الحكومية الحساسة.تسبب تهديدات عديدة ناشئة من أفعال خبيثة إيقاف خدمات الحكومة الألكترنية. لذلك تلح الحكومات على تنفيذ الأمنية في مشاريع الحكومة الألكترونية. تم أقتراح بعض التعديلات على نموذج تقييم أمن المعلومات ذو الطبقات المتعددة (نموذج صبري) لكي يكون نموذج شامل وملائم أكثر للحكومة العراقية. هذا النموذج من الممكن استخدامه كأداة لتقييم مستوى الأستعداد الأمني للأقسام الحكومية, وكقائمة جرد بالتدابير الأمنية المطلوبة وكمرجع عام للأمنية في المؤسسات الحكومية في العراق. لكي يتم جعل هذا النموذج عمليا وقابل للتطبيق بصورة أكثر ولكي يتم تمثيل الأستعداد الأمني بقيمة رقمية, فقد تم عمل نمذجة تقييم للنموذج المطور بأستخدام أداة المنطق المضبب في برنامج الماتلاب R2010a.

بما أن تقييم الخطر يعتبر جزء رئيسي ومهم في نظام أدارة أمن المعلومات لذا تم أقتراح طريقة فعالة وعملية لذلك عن طريق جمع تقييم الخطر بنظام الخبير المضبب مع الشبكة العصبية للمويجات.تم أستخدام النظام المضبب لتوليد مجموعة بيانات التدريب لغرض التدريب المطلوب للشبكة العصبية. تم تطبيق هذه الطريقة عندما تم عمل دراسة حالة تقييم الخطر في مركز الحاسبة لجامعة بغداد. لقد وجد من النتائج العددية لهذه الدراسة أن مستويات الخطر التي تم الحصول عليها بطريقة شبكة المويجات العصبية (أعلى مستوى خطر كان 58.23) كانت قريبة جدا لتلك النتائج التي تم حسابها بطريقة النظام المضبب (أعلى مستوى خطر كان 60) , معدل الخطأ للنتائج كانت قيمته5.51%. النتائج التي تم الحصول عليها تبين أن هذه الطريقة فعالة ومعقولة ويمكن أن توفر الدعم بأتجاه تأسيس الحكومة الالكترونية.

KEY WORDS: E-Government, Security Model, Risk Assessment, Fuzzy Expert System, Wavelet Neural Network (WNN)

1. INTRODUCTION

E-Government is a kind of governmental administration, which is based on electronic information technology. The essence of e-government is using electronic information technology to break the boundary of administrative organizations, and build up a virtual electronic government [Zhitian and Congyang,2008]. The concept of an e-government system is to provide access to government services anywhere at anytime over open networks. This leads to issues of security and privacy in the management of the information systems [Salahduddin,Lauren and Kavoos,2008]. Governments are trying to deliver their services in ways that meet citizens, employees and businesses needs effectively and efficiently. The Internet allows a quick update and access to any information any time the user wants. E-Government is the most important accomplishment of Internet [Walid and Reem, 2008]. The information system security is an essential management responsibility for e-government that has as a target to fulfil the fundamental security properties of; confidentiality, integrity, availability, accountability and information assurance. A high level of confidence and trust among all users (citizens, businesses and government) will be the foundation of a successful e-government initiative [Costas, Stefanos, Fredj and Gunther, 2003]. The objective of information system security is to optimize the performance of an organization with respect to the risks to which it is exposed [Seymour and M.E. Kabay, 2002]. Without adequate protection or network security, many individuals, businesses, and governments are at risk of losing the assets [Salah, 2009]. A *security model* is a statement that outlines the requirements necessary to properly support and implement a certain security policy [Shon, 2009]. Models in the computer security field have generally been constructed as an aid in analyzing "security" properties of interest [D. Elliott, 1988]. Information security presents a lot of challenges and concerns to governmental and commercial organizations. Models are used as the best method for illustrating new concepts or architectures. It was noticed that all existing models were developed to address one aspect or a problem in the information security field. No comprehensive model was found, which addresses all aspects of security for any organization that offers e-services over Internet or a public network. This lead to develop a new model (multi-layer information security assessment model) which contains multilayer representing the technologies, policies, competencies, operational procedures and decision layer [Sabri, 2008]. This model is named Sabri model in this paper.

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. It is very important to make a study on the theory and practice of the assessment of security risks in the information systems [Ming, SHU and XIAO 2008]. The aim of this paper is:

- To modify the multi layer information security readiness assessment model developed by Sabri (Sabri model) and evaluate it by using fuzzy logic, in order to make it more practical and applicable to the organizations of e-government.
- To propose an effective and practical method of security risk assessment for e-government information system. This method is built by combining two engineering techniques, fuzzy expert system (FEMRA) with wavelet neural network.

2. MULTI-LAYER INFORMATION SECURITY ASSESSMENT MODEL (SABRI MODEL)

The objective of the new security model is to assist in visualizing the combination of different layers of security in order to come up with a mechanism of enhancing the security level of any e-enabled organization but specifically in using the e-governments as the research case. Having more than one dimension or layer of any model gives the model a robust structure and a better success rate in preventing organizations from various categories of threats related to a single or multiple e-services. Each layer will mitigate group of threats related to an e-services. The layers as depicted in **Fig. 1**are, the technology layer, the policy layer, the competency layer, the operational and Management layer and the decision layer. The layers were constructed from the bottom to the top based on the importance of the layers and how they complement each other.

Since each layer has more than one sub layer and to make the structure coherent and more understandable, the model evolved into a matrix oriented structure, where each layer was divided into multiple sub layers as indicated in **Fig. 2**. The division of these layers into sub layers gives the

new model a flexibility to expand into n-number of cells based on the need of the organization [Sabri , 2008].

2.1 Modifications for Sabri Model

Modifications for the Sabri model were done based on the conditions of Iraq, supervisor's experience and analysis of the published works. **Fig. 2** shows the original model of Sabri without the modifications, whereas **Fig. 3** shows the model after making the modifications (modified Sabri model). The modifications include the followingin :

1. Addition of two elements to the technology layer (***VLAN & non-repudiation***). VLANs are used to segment networks for multiple reasons, the primary reason is to group together common hosts for security purposes. VLAN can allow one broadcast domain to be split into two or more domains that restrict an access to certain network resources. This can be a handy addition to user management and security strategy for the company. [Joshura, 2008] [Todd,2003]. Non-Repudiation is an important security service needed for many e-government applications. It will increase the confidence for both citizens and the government departments on e-government applications. [Hasala, Lakshan and Rohana, 2008].
2. Dividing the competency layer into two sub layers called ***user sub layer*** and ***information security department sub layer.*** The users of an organization should be classified into two parts (common users and security specialist users). Therefore, this division for this layer will help the users to know their security tasks. Three elements have been added to the user sub Layer called:

- ***Training and awareness:*** Security awareness and training is an essential element of a comprehensive and effective security program, to keep staff aware of their responsibilities and role in implementing and maintaining security within the department [Parmar,2009].
- ***Security policies of department***: It is a set of rules and practices dictating how sensitive information is managed, protected, and distributed. Without a strong security policy that every employee must conform to, the organization may suffer from data loss, employee time loss, and productivity loss [Joseph,2005].
- ***Social engineering:*** It can be defined as any attempt to gain unauthorized access to systems or resources by means other than software or hardware hacking. A little bit of psychology and some insight into the victim's character or habits is usually enough to mount a successful attack, under the right circumstances [Todd, 2003].

Two elements have been added to the information security department sub layer called:

- ***cyber crime:*** A cyber crime is a crime like any other crime, except that in this case, the illegal act must involve a connected computing system either as an object of a crime, an instrument used to commit a crime or a repository of evidence related to a crime [Joseph, 2009].
- **Computer Security Incident Response Team (CSIRT)**: It is critical for the organization to have a fast and effective means of responding. When an incident occurs, the goal of the CSIRT is to control and minimize any damage, preserve evidence, provide quick and efficient recovery, prevent similar future events, gain insight into threats against the organization and lower the cost of recovery [Georgia, Klaus-Peter, Robin and Mark, 2003].

3. Introduce a new layer called ***physical layer***. Physical security is the term used to describe protection needed outside the computer system. Physical security is applied to prevent attackers from have a facility to gain data stored on servers, computers, or other mediums. [Charles and Shari, 2002] [Joshura , 2008]. Three elements have been added to this layer called ***site design***, ***access control devices*** and ***alarms and cameras***.
4. One element has been added to the decision layer called ***data sensitivity***. Some databases contain what is called sensitive data. Sensitive data are data that should not be made public. Obviously, some databases, such as a public library catalogue, contain no sensitive data, other databases, such as defence-related ones, are totally sensitive [Charles and Shari, 2002].
5. Replacing the element (technologies availability) in the decision layer by ***elements availability.*** Specific weight has been assigned to each layer, to take account the effect of all the layers during the decision making process, instead of depending on one layer (technology layer). Technology layer will take weight value 0.6, because it considers the important layer as recommended by Sabri model, and each of other layers will take 0.1 as a weight value. Therefore, the element (technologies

availability) is replaced by elements availability.

2.2 Evaluation of Modified Sabri Model Using Fuzzy Logic

In this section, the modified Sabri model will be evaluated using fuzzy logic. The fuzzification of input variables is based on three major elements (*cost, data sensitivity and elements availability*) in the decision layer of the model. The design is based on the Mamdani style inference system which is very good for the representation of human reasoning and effective analysis. The implementation is done using the fuzzy logic tool of MATLAB R2010a.

The aim of this work is to assess the level of security readiness of government organizations and make decisions by using fuzzy logic instead of human reasoning. Fuzzy logic-based evaluation modeling architecture is given in **Fig. 4**.

Linguistic values are assigned for the inputs, *cost* and *data_ sensitivity* as *Low*, *Medium*, and *High*, whereas the Linguistic value for the input (*elements _availability)* is assigned as *Bad*, *Good*, and *Excellent*. The Linguistic value for the output (*trend_ level*) is assigned as *Very low, Low, Medium, Rather high, High and Very high.* The universe of discourse of the input and output variables in this case ranges from 0 to 100. **Table 1** contains the linguistic variables and their ranges.

Fig. 5 displays information about FIS editor (decision). It shows the names of input and output variables. **Fig. 6** is used to add, change or delete rules.

2.3 Determine the Value of Elements Availability

The decision of launching or not launching an e-service using the fuzzy evaluation of the modified Sabri model depends on some elements. One of these elements is (*elements availability)*. In order to determine easily the value of this element with more accurate, a function was written using the built-in editor of MATLAB R2010a. The name of this function is ***elements_avail***. It has two arguments (x1 and x2). The first argument (x1) is a row vector that represents the elements selected by security manager or designer from the modified Sabri model. The second argument (x2) is a row vector that represents the type of security service (*confidentiality, integrity, availability, authentication and non repudiation*) required for establishing an e-service. Each security service takes one value (1, 2, 3, 4 and 5 respectively) to represent it inside the function (*elements_avail)*. The output of this function is (*elements_ availability*) that represents the value of the element (*elements availability)* will be taken as input in the fuzzy model (decision).

3. SECURITY RISK ASSESSMENT

A Risk can be described as the potential of a threat to exploit a vulnerability found in an asset [Todd, 2003]. A risk exists when there is a possibility of a threat to exploit the vulnerability of a valuable asset. That is, three elements of a risk are *asset, vulnerability* and *threat*. The value of an asset makes it a target for an attacker. The vulnerability of an asset presents the opportunity of a possible asset damage or loss. A threat is a potential attack which can exploit a vulnerability to attack an asset [Nong, 2008]. The measure of risk can be determined as a product of threat, vulnerability and asset values as shown in the formula below:

$$\text{Risk} = \text{Asset} \times \text{Threat} \times \text{Vulnerability} \quad (1)$$

With the progress of the construction of the e-government information systems of different levels, the government provides management and services with higher quality and more efficient for the society. So, it is very important to make a study on the theory and practice of the assessment of security risks in information systems [Ming, 2008]. The basic steps for risk assessment are listed as follows [John, 2001] [AS/NZS, 2004]:

1. Identifying and prioritizing assets.
2. Identifying vulnerabilities.
3. Identifying threats and their probabilities.
4. Estimate level of risk
5. Developing a cost benefit analysis.
6. Developing security policies and procedures.

A powerful tool is needed to assess the risk within an organization. The WNN (wavelet neural network) has the intelligent features such as self-learn, obtaining knowledge, which is different to the conventional methods (AHP, fuzzy logical and so on), and can dissolve the uncertain problems [DONG-MEI, 2009]. In this paper, the fuzzy theory and method of Wavelet Neural Network (WNN) are combined to assess the risk level. Since the artificial neural network is suited for the quantity data processing, and poor to the qualitative analyze, therefore the fuzzy expert systems (FEMRA) method was built and applied

firstly to assess the risk factors (training data set). Secondly, the WNN was built to assess the risk level quantitatively.

3.1 Fuzzy Expert Model for Risk Assessment (FEMRA)

The steps of implementation FEMRA will be given below [Alireza, Masoume, Mehdi and Michel, 2010]:

Step 1: Assets classification and identification
Step 2: Threat Identification
Step 3: CIA Triad Evaluation

Evaluating the CIA (confidentiality, integrity and availability) triad is a key to calculate the organization's risks. The base of the CIA triad could be calculated with the following formulas:

$$W_C = \frac{\sum_{e=1}^{n} C_e}{n}, \quad W_I = \frac{\sum_{e=1}^{n} I_e}{n}, \quad W_A = \frac{\sum_{e=1}^{n} A_e}{n} \tag{2a}$$

Since authentication is important service and main part in computer security system [Mark, 2006][William, 2005][Joseph, 2005], therefore it is added to the CIA triad evaluation.

$$W_{AU} = \frac{\sum_{e=1}^{n} AU_e}{n} \tag{2b}$$

Where n represent the number of experts. C_e, I_e, A_e and AU_e represent the weights of confidentiality, integrity, availability and authentication that assigned by the experts.

Step 4: Vulnerability Identification
Step 5: Risk Identification
Step 6: Asset Value

Each expert assigns a value from 1 to 9 to each part of CIA triad based on the **Table 2**.

Table 2 Risk level range

The asset's value could be calculated with formula below:

$$asset_{value} = \sum_{(CIA+AU)=1}^{4} \left(\frac{\sum_{e=1}^{n} (CIA+AU_e)}{n} \right) * W_{(CIA+AU)} \tag{3}$$

Where n represent the number of experts, W_{CIA+AU} represent the base of the CIA triad and authentication part and $(CIA+AU)_e$ represent CIA triad and authentication values of an asset based on expert assignment.

Step 7: Vulnerability Effect

Vulnerability effects will be represented with a percentage, and for better accuracy, it is prefer to get help from n experts. The vulnerability effect could be calculated with formula below:

$$vulnerability_{effect} = \frac{\sum_{e=1}^{n} effect}{n} \tag{4}$$

Step 8: Threat Effect

The calculation method of threats is similar to the one for assets. Each expert assigns a value from 1 to 9 to each part of CIA triad plus authentication based on **Table 2**. The threat effects could be calculated with formula 5.

$$threat_{value} = \sum_{(CIA+AU)=1}^{4} \left(\frac{\sum_{e=1}^{n} (CIA+AU_e)}{n} \right) * W_{(CIA+AU)} \tag{5}$$

Risk Effects (level) modelling

The risk effects modelling are built using the fuzzy model tool of MATLAB R2010a environment. Three parameters are used as input in this modelling: *asset values, vulnerability effects* and *threat effects*. **Fig. 7** below shows the architecture of this model.

3.2 Risk Evaluation Based on Wavelet Neural Network Model

The basic structure of proposed WNN is illustrated in **Fig. 8**, which consists of three layers. The first layer is the input layer, which has three nodes (i=1, …, 3) as following: *asset value, vulnerability effect* and *threat effect*. The second layer is a hidden layer, which has *H* nodes that needs adjusting in the experiment. The third layer is an output layer, which has one node (m=1) for putting out a risk effect (risk level).

W_{hi} and W_{mh} are defined respectively as the weight coefficient of the hidden layer and the output layer. The output of a wavelon is defined as:

$$\psi_{a,b}(u) = \psi\left(\frac{u-b}{a}\right) \tag{6}$$

Where $\psi(\cdot)$, a and b are the mother wavelet function, dilation and translation parameters respectively. The activation function of the hidden layer is defined as Marr function:

$$\psi(t) = (1 - t^2)\exp(-t^2/2) \quad (7)$$

The active function of output layer is defined as a sigmoid function:

$$f(net) = 1/(1 + \exp(-net)) \quad (8)$$

4. CASE STUDY

In order to verify the validity of our proposed method (fuzzy wavelet neural network) and test its ability of risk assessment for e-government network security, experiments were carried out in the computer center at the University of Baghdad. In this study, the FEMRA method was applied firstly to assess the risk factors (training data set), then the WNN is applied to assess the risk level. Three security experts from computer center are used to do this study. The results of this case study are indicated by the following steps:

Step 1: CIA Triad Evaluation

The sum of the weights for all parts must be equal to one. Note that the authentication service is added in this step (eq. 2b), so it will be entering in the calculation of this evaluation. **Table 3** shows this evaluation.

When the eq. (2) is applied on the **Table 3**, the base of the CIA triad and authentication evaluation could be calculated. **Table 4** shows the values of the bases.

Step 2: Asset value

Table 5 shows the asset identification for computer center. Each expert assigned a value from (1 to 9) to each part (confidentiality, integrity, availability and authentication) of an asset. Then eq. (3) is applied to calculate the asset value for each asset. **Table 6** shows the asset value.

Step 3: Vulnerability effect

Table 7 shows the asset's vulnerabilities for the assets of the computer center.

Each expert assigned a value from (0 to 100) for each asset's vulnerability (**Table 8**). Then eq. (4) is applied to calculate the vulnerability effect. **Table 8** shows the vulnerability effects.

Step 4: Threat effect

Table 9 shows the threat identification for computer center.

Each expert assigned a value from (1 to 9) to each part of a threat in **Table 9**. Then eq. (5) is applied to calculate the threat effect for each threat. **Table 10** shows the threat effect.

Step 5: Risk effect (level)

Based on the previous collected data (**Tables 5**, **7** and **9**), the relationship among the assets, vulnerabilities and threats will be determined. The relationship between each vulnerability and threat is a risk. **Table 11** illustrates some risks within the computer center. Dependent on the **Table 2**, the risk effect will be divided into three levels ($1 \le$ low < 35, $35 \le$ med < 65, $65 \le$ high < 100).

The risk effect can be calculated by using the fuzzy model of FEMRM. **Table12** shows the results to assess the risks in the computer center.

4.4 Results of Risk Evaluation Based on WNN

Table 13 shows the result of comprehensive evaluating of risk level for the computer center by WNN.

Table 14 shows the contrast between the FEMRA result (desired output) and the output of WNN.

5. CONCLUSIONS

- E-Government network security is complicated process, and it requires periodically evaluation. Building secure e-government system requires a comprehensive security model.
- Modified Sabri model is an enhanced security readiness assessment model that is designed especially for e-government system. This enhanced model considers an essential tool that can be used by decision makers and designers of e-government security systems. The modified Sabri model is more effective than Sabri model, because it deals with numerical values instead of conceptual elements and all the layers of the model are contributing in making the decision instead of dependence on the technology layer only. This contribution is achieved by assigning a weight value for each layer. The modified Sabri model can help the security managers to assess the security readiness of their department with high accuracy.
- Combine two engineering techniques (fuzzy system with wavelet neural network) enables the governmental organizations to overcome the difficulty of finding the required training data set to build the wavelet neural network, and reduce the level of dependence on the experts and the time required to assess the risks in their departments.

- The numerical results from the real case study of risk assessment indicate that WNN can improve effectively the assessment accuracy and speed. The contrast result between WNN and FEMRA shows that the risk evaluation method based on the WNN can provide a credible algorithm for the risk assessment of information security.

REFERENCES

Alireza S. Sendi, M. Jabbarifar, M. Shajari and M. Dagenais, "FEMRA: Fuzzy Expert Model for Risk Assessment", Proceedings of the IEEE International Conference on Internet Monitoring and Protection, pp.48-53, 2010.

AS/NZS, "Risk Management", SAI Global, Third Edition, 2004.

Charles P. Pfleeger and Shari L. Pfleeger, "Security in Computing", Prentice Hall, third edition, 2002.

Costas Lambrinoudakis, S. Gritzalis, F. Dridi and G. Pernul, "Security Requirements for E-Government Services: A Methodological Approach for Developing A Common PKI-based Security Policy", Elsevier, Computer Communications 26, 1873–1883, 2003.

D. Elliott Bell, "Concerning Modeling of Computer Security", Proceedings of the IEEE International Symposium on Security and Privacy, pp.8-13, 1988.

Georgia Killcrece, Klaus-Peter Kossakowski, Robin Ruefle and Mark Zajicek, "Organizational Models for Computer Security Incident Respons Teams (CSIRTs)", Carnegie Mellon University, 2003.

Hasala Peiris, Lakshan Soysa and Rohana Palliyaguru, "Non-Repudiation Framework for E-Government Applications", Proceedings of the IEEE International Conference on Information and Automation forSustainability, pp.307-313, 2008.

John E. Canavan, "Fundamentals of Network Security", British Library, London, 2001.

Joseph M. Rizza, "Computer Network Security", Springer, 2005.

Joseph M. Rizza, "A Guide to Computer Network Security", Springer, 2009.

Joshura Backfield, "Network Security Model", SANS Institute, 2008.

Mark Stamp, "Information Security Principles and Practice", John Wiley & Sons, 2006.

Ming Liu, S. Sun and X. yin, " Research on The Evaluation of Security Risk for E-Government Information System" Proceedings of the IEEE International Conference on Machine Learning and Cybernetics, Vol.3, pp.1404-1409, 2008.

Nong Ye, "Secure Computer and Network Systems Modeling, Analysis and Design", john Wiley & Sons Inc., 2008.

S. K. Parmar, "Information Resource Guide Computer, Internet and Network Systems Security", security manual, sunny, Canada, June 2009.

Sabri Al-Azazi, "A Multi-layer Model for E-Government Information Security Assessment", PhD thesis, Cranfield University, 2008.

Salah Alabady, "Design and Implementation of A Network Security Model for Cooperative Network", International Arab Journal of e-Technology, Vol. 1, No. 2, June 2009.

Salahuddin Alfawaz, L. May and K. Mohanak, "E-Government Security in Developing Countries: A Managerial Conceptual Framework", International Research Society for Public Management Conference, 2008.

Seymour Bosworth and M.E. Kabay, "Computer Security Handbook", John Wiley & Sons, Fourth Edition, 2002.

Shon Harris, "CISSP All-in-One Exam Guide", McGraw Hill, Fifth Edition, 2009.

Todd King, "Security + Training Guide", Paul Boger, 2003.

Walid Al-Ahmad and R. Al-Kaabi, "An Extended Security Framework for E-Government", Proceedings of the IEEE International Conference on Intelligence and Security Informatics, pp. 294-295, 2008.

William Stallings, "Cryptography and Network Security Principles and Practices", Prentice Hall, Fourth Edition, 2005.

Zhitian Zhou and Congyang Hu, "Study on the E-Government Security Risk Management", IJCSNS International Journal of Computer Science and Network Security, Vol.8 No.5, May 2008.

NOTATION

W_C Confidentiality Base
W_I Integrity Base
W_A Availability Base
C_e Confidentiality Expert Weight
I_e Integrity Expert Weight
A_e Availability Expert Weight
w_{CIA} Base of the CIA Triad
w_{CIA+AU} Base of the CIA Triad and Authentication Part
$(CIA + AU)_e$ CIA Triad and Authentication Values of an Asset Based on Expert Assign.
net Scalar Product of the Weight and Input Vector
$\psi(u)$ Mother Wavelet
w_{hi} Weight Coefficient of the Hidden Layer
w_{mh} Weight Coefficient of the Output Layel

Table 1 Linguistic variable and their ranges

Linguistic variable	Linguistics value	Numerical range	Membership function type
Cost	Low	[0 0 20 40]	Trapezoidal
	Med	[20 60 95]	Triangular
	High	[60 90 100 100]	Trapezoidal
Data_Sensitivity	Low	[0 0 20 40]	Trapezoidal
	Med	[20 55 90]	Triangular
	High	[55 90 100 100]	Trapezoidal
Elements_availability	Bad	[0 0 25 40]	Trapezoidal
	Good	[20 60 100]	Triangular
	Excellent	[60 100 100]	Triangular
Trend_level	Very low	[0 0 30]	Triangular
	Low	[10 30 50]	Triangular
	Medium	[30 50 65]	Triangular
	Rather high	[55 65 75]	Triangular
	High	[65 75 85]	Triangular
	Very high	[75 100 100]	Triangular

Table 2 Risk level range

Level	Level	Effect
High	High	9
	Medium	8
	Low	7
Medium	High	6
	Medium	5
	Low	4
Low	High	3
	Medium	2
	Low	1

Table 3 CIA triad and authentication evaluation

Expert	Confidentiality (W_C)	Integrity (W_I)	Availability (W_A)	Authentication (W_{AU})
E1	0.3	0.3	0.1	0.3
E2	0.35	0.3	0.1	0.25
E3	0.35	0.25	0.1	0.3

Table 4 CIA base value

Base	Value
Confidentiality (W_C)	0.333
Integrity (W_I)	0.283
Availability (W_A)	0.1
Authentication (W_{AU})	0.283

Table 5 Asset identification

Id	Asset
A1	User (Instructor)
A2	Web data (questions and results of IC3 examination)
A3	License application
A4	Router
A5	Server
A6	Storage resources

Table 6 Asset value

Id	Asset	Confidentiality			Integrity			Availability			Authentication			Asset Value
		E1	E2	E3	E1	E2	E3	E1	E2	E3	E1	E2	E3	
A1	User (Instructor)	5	6	6	2	2	2	2	1	1	6	5	5	4.1
A2	Web data	7	8	8	7	7	6	5	5	4	7	6	6	6.7
A3	License Application	3	2	3	3	2	2	6	7	7	4	5	5	3.54
A4	Router	5	5	6	7	6	7	2	3	2	7	8	7	5.97
A5	Server	5	5	4	4	5	6	7	6	8	5	5	6	5.18
A6	Storage Resources	5	4	4	7	7	6	2	3	3	6	5	5	5.11

Table 7 asset's vulnerabilities

Id	Asset	Vulnerability
V1	A1 (Instructor)	User personality
V2	A2(Web data)	Administrative mistake, Poor protection
V3	A3 (License application)	Not using a mixed authentication mode
V4	A4 (Router)	Hardware defect, Configuration error
V5	A5 (Server)	Unsuitable location
V6	A6 (Storage resources)	Hardware defect, poor security

Table 8 Vulnerability effect

Asset Id	Vulnerability Id	Effect (%)			Vulnerability Effect (%)
		E1	E2	E3	
A1	V1	70	70	80	73.33
A2	V2	70	60	60	63.33
A3	V3	60	50	40	50
A4	V4	50	50	60	53.33
A5	V5	60	50	50	53.33
A6	V6	70	70	60	66.66

Table 9 Threat identification

Id	Threat
T1	Malicious Code (viruses, worms…etc.)
T2	Social engineering
T3	Hacker
T4	Equipment failure
T5	Intruder
T6	Human Errors
T7	DoS
T8	Physical theft

Table 10 Threat effect

Id	Threat	Confidentiality			Integrity			Availability			Authentication			Threat Effect
		E1	E2	E3	E1	E2	E3	E1	E2	E3	E1	E2	E3	
T1	Malicious Code	5	6	6	5	5	6	7	7	8	3	4	4	5.17
T2	Social engineering	7	7	8	3	2	2	2	2	1	7	6	6	5.07
T3	Hacker	6	6	7	6	5	5	1	2	2	7	7	6	5.67
T4	Equipment failure	2	1	2	2	2	1	7	8	6	1	1	2	2.1
T5	intruder	7	6	7	5	5	6	2	1	2	7	7	6	5.78
T6	Human Errors	5	5	4	6	5	6	2	2	1	4	5	5	4.65
T7	DoS	2	2	2	1	1	2	7	8	8	2	2	1	2.82
T8	Physical theft	5	5	4	2	2	1	6	7	7	2	1	1	3.07

Table 11 Some Risks in the computer center

Asset Id	Vulnerability Id	Threat Id	Risk Id
A1 User (Instructor)	V1 User personality	T2 Social engineering	R1 (loss of secrecy)
A2 Web data	V2 Administrative mistake	T6 Human Errors	R2 (data corruption)
A2 Web data	V2 Poor protection	T3 Hacker	R3 (company image)
A3 License application	V3 Not using mixed authentication mode	T6 Human Errors	R4 (loss of business or financial)
A4 Router	V4 Hardware defect	T4 Equipment failure	R5 (loss availability)
A4 Router	V4 Configuration error	T5 Intruder	R6 (security Compromise)
A5 Server	V5 Unsuitable location	T8 Physical theft	R7 (loss availability)
A5 (Server)	V5	T7 DoS	R8 (loss e-service)
A6 (Storage resources)	V6 Hardware defect	T4 Equipment failure	R9 (loss data)
A6 (Storage resources)	V6 poor security	T1 Malicious Code	R10 (data corruption)

Table 12 Risk effect

Risk Id	Asset Value (1-9)	Vulnerability Effect (1-100)	Threat Effect (1-9)	Risk Effect (level) (1-100)		
				low	med	high
R1	4.1	73.33	5.07		60	
R2	6.7	63.33	4.65		53.2	
R3	6.7	63.33	5.67		53.2	
R4	3.54	50	4.65		39.5	
R5	5.97	53.33	2.1	26.6		
R6	5.97	53.33	5.78		45.6	
R7	5.18	53.33	3.07		37.4	
R8	5.18	53.33	2.82	32.1		
R9	5.11	66.66	2.1		41.4	
R10	5.11	66.66	5.17		54.8	

Table 13 Risk effect using WNN

Risk Id	Input			output (Risk Level)		
	Asset Value	Vulnerability Effect	Threat Effect	Low	Med	High
R1	4.1	73.33	5.07		58.23	
R2	6.7	63.33	4.65		51.18	
R3	6.7	63.33	5.67		55.81	
R4	3.54	50	4.65		36.33	
R5	5.97	53.33	2.1	23.46		
R6	5.97	53.33	5.78		47.73	
R7	5.18	53.33	3.07		35.41	
R8	5.18	53.33	2.82	30.85		
R9	5.11	66.66	2.1		39.85	
R10	5.11	66.66	5.17		56.72	

Table 14 Contrast between desired output and output of WNN

Desired Output (FEMRA) Risk Level			WNN Risk Level			Absolute Error	Max Error	Min Error	Average Error
Low	Med	High	Low	Med	High				
	60			58.23		1.77	3.17	1.25	2.155
	53.2			51.18		2.02			
	53.2			55.81		2.61			
	39.5			36.33		3.17			
26.6			23.46			3.14			
	45.6			47.73		2.13			
	37.4			35.41		1.99			
32.1			30.85			1.25			
	41.4			39.85		1.55			
	54.8			56.72		1.92			

Fig. 1 multi layers model

Security Layers	Sub Layers / Cells					
Technology Layer	A1: Access Control	A2: Intrusion Detection Prevention	A3: Anti-Virus & Malicious Codes Signature	A4: Authentication and Passwords	A5: Files Integrity Checks	A6: Cryptography
	A7: VPN	A8: Vulnerability Scanning Tools	A9: Digital Signature and Certificate	A10: Biometrics	A11: Logical Access Control (Firewall)	A12: Security Protocols
Policy Layer	B1: Password Management	B2: Log-In Process	B3: Logs Handling	B4: Computer Viruses	B5: Intellectual Property Rights	B6: Data Privacy
	B7: Privilege Control	B8: Data Confidentiality	B9: Data Integrity	B10: Internet Connectivity	B11: Administrative Policies	B12: Encryption Policies
	B13: HR Security Policies	B14: Third Party Policies	B15: Physical Security Policies	B16: Operation Security Policies		
Competency Layer	C1: Security Operation and Management	C2: Security Architecture and Development	C3: Ethical Hacking	C4: Security Policies Development	C5: Computer Forensics	C6: Cryptography
	C7: Security Programming	C8: Laws and Regulations	C9: Security Implementation and Configuration	C10: Security Analysis		
Operation and Management Layer	D1: Operational Policies and Procedures	D2: Management Tool	D3: Correlation and Data Mining	D4: Reporting and Response	D5: Analysis and Human Intervention	
Decision Layer	F1: Cost	F2: Awareness	F3: Need	F4: Technologies Availability	F5: FUD	

Fig.2 Sabri model

Security Layers	*Sub Layers / Cells*						
Technology Layer	A1: VLAN	A2: Access Control	A3: Intrusion Detection prevention	A4: Anti-Virus & Malicious Codes Signature	A5: Authentication and passwords	A6: Files Integrity Checks	A7: cryptography
	A8: VPN	A9: Vulnerability Scanning Tools	A10: Digital Signature and Certificate	A11: Biometrics	A12: Logical Access Control (Firewall)	A13: Security Protocols	A14: non – repudiation
Policy Layer	B1: Password Management	B2: Log-In Process	B3: Logs Handling	B4: Computer Viruses	B5: Intellectual property Rights	B6: Data Privacy	B7: Privilege Control
	B8: Data Confidentiality	B9: Data Integrity	B10: Internet Connectivity	B11: Administrate policies	B12: Encryption policies	B13: HR Security Policies	B14: Third Party Policies
	B15: Physical Security Policies	B16: Operation Security Policies					
Competency Layer	User Sub Layers	C1: Training and Awareness	C2: Security Policies of Department	C3: Ethical Hacking	C4: Social Engineering		
	Information security Department	C5: Security Operation and Management	C6: Security Architecture and Development	C7: Security Policies Development	C8: Computer Forensics	C9: Cryptography	C10: Security Programming
	Sub Layers	C11: Laws and Regulations	C12: Security Implementation and Configuration	C13: Security Analysis	C14: Cyber Crime	C15: CSIRT	
Operation and Management Layer	D1: Operational Policies and Procedures	D2: Management Tool	D3: Correlation and Data Mining	D4: Reporting and Response	D5: Analysis and Human Intervention		
Physical Layer	E1: Site Design	E2: Access Control Devices	E3: Alarms and Cameras				
Decision Layer	F1: Cost	F2: Awareness	F3: Need	F4: Elements Availability	F6: FUD	F5: Data Sensitivity	

Fig. 3 Modified Sabri model

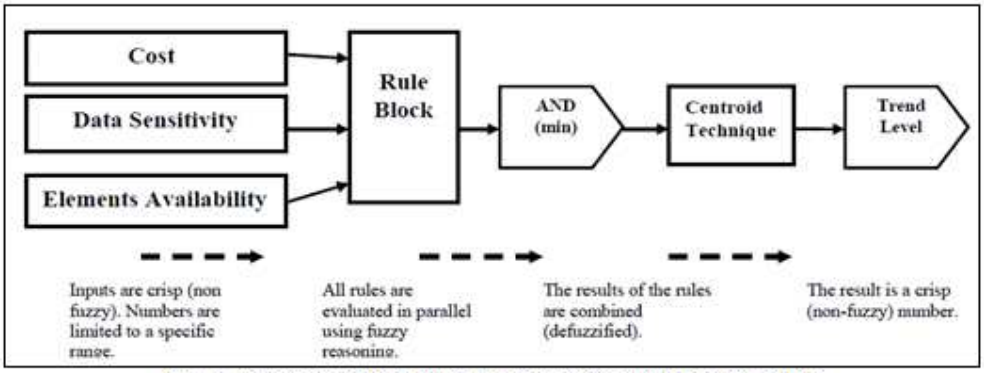

Fig. 4 Architecture for fuzzy logic-based evaluation modeling

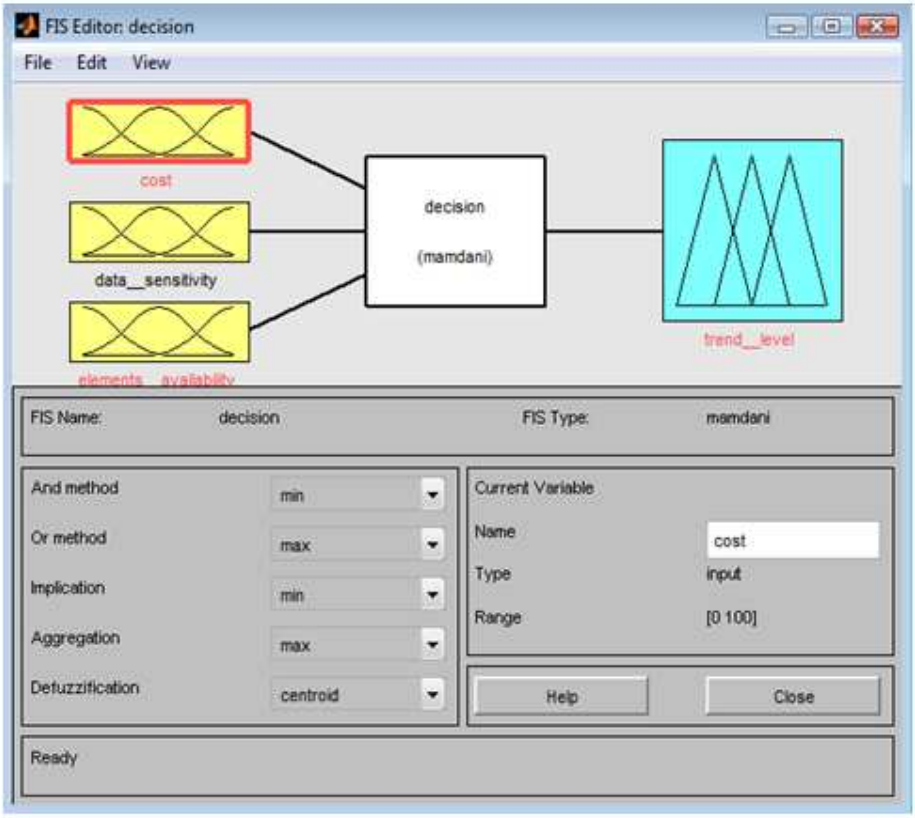

Fig. 5 FIS editor (decision)

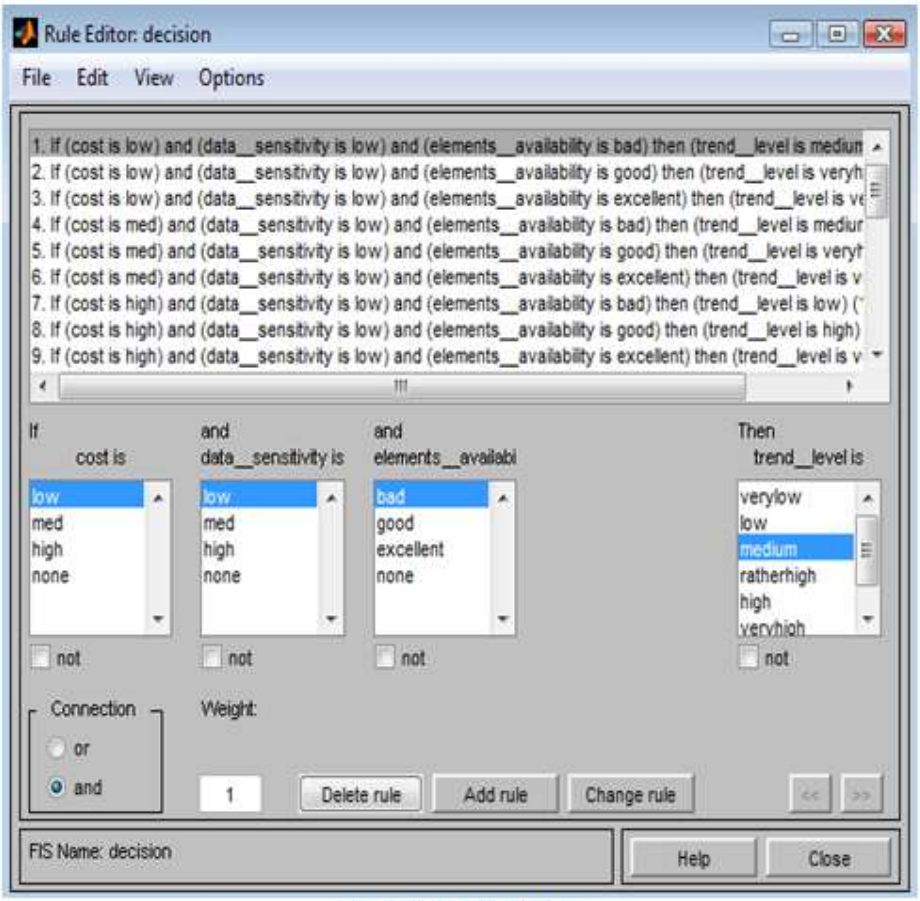

Fig. 6 Rules Editor

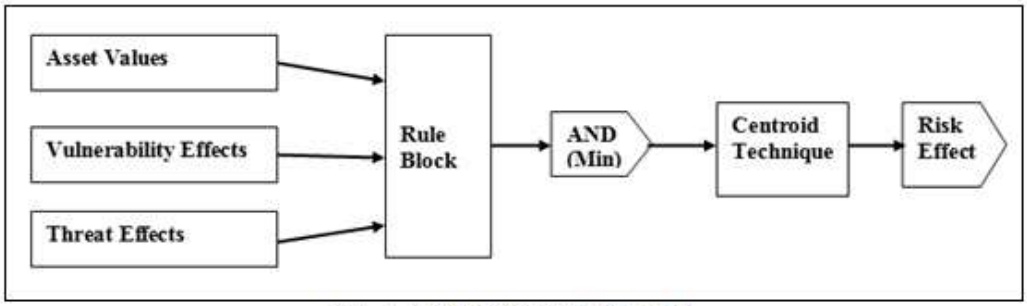

Fig. 7 Architecture of FEMRA