Journal of Modern Technology and Engineering
Special Issue | IECHCI2022, 2023, pp.53-58

CREATING A FUZZY MODEL THAT REALIZES THE ASSESSMENT OF INFORMATION SECURITY RISKS WITH THE APPLICATION OF COMPUTER MATHEMATICAL SYSTEMS

Rasmiyya Amiraslanova*

Department of Information Technologies, Mingachevir State University, Mingachevir, Azerbaijan

Abstract. The creation of a fuzzy models using mathematical software packages allows one the assessment of the information security risks. In the paper a model of information security risk assessment is developed in the computer system with the application of the Fuzzy Logic Toolbox package of Matlab.

Keywords: information security, threat, risk assessment, expert systems, fuzzy logic, MATLAB environment, Fuzzy Logic Toolbox package.

***Corresponding author:** Rasmiyya Amiraslanova, Department of Information Technologies, Mingachevir State University, Mingachevir, Azerbaijan, e-mail: *amiraslanova.ras@mail.ru*

Received: 10 October 2022; Revised: 19 November 2022; Accepted: 8 December 2022; Published: 13 January 2023.

1 Introduction

Ensuring information security plays an important role in the management activities of the enterprises, in the application of data collection, storage and processing technologies. These processes are based on the periodic analysis of information risk levels according to quantitative and qualitative scales, as well as a set of appropriate measures for timely identification and neutralization of information security threats and weaknesses is possible by implementation (Mikov & Buldakova, 2013). Analytical analysis of information security risks, which is a direction of artificial intelligence technologies, is carried out by the evaluation based on the neuro-fuzzy network methodology, which allows the realization of the mentioned (Alesinsky, 2021).

It is known that in the period of transition to globalized digital transformation, the possibilities of applying artificial intelligence are constantly increasing. For example, in March 2016, researchers from DeepMind, a subsidiary of Alphabet (Google's parent company), developed an AI computer program called AlphaGo is used in Apple's Siri and Amazon's Alexa voice recognition systems, Facebook's facial recognition API, Apple's 3D facial recognition hardware and software, and Tesla's "autopilot" device. use is currently successfully implemented. These indicators are reliable, it is one of the important points in the formation of flexible and stable secure information systems. For this purpose, the information security risk assessment methodology was performed with the help of the most widely used Matlab software package of computer mathematics. The evaluation was carried out in the form of internal procedures, based on the formation of a certain knowledge base, using the program's FUZZY LOGIC TOOLBOX and ANFIS library.

2 Creation of a fuzzy model that realizes the assessment of information security risks using the application of the Fuzzy Logic Toolbox Package

Developing fuzzy model using the Fuzzy Logic Toolbox package for assessing the state of a computer system in the MATLAB environment and allows assessing information security risks with many external factors occurring in the system (Azhmukhamedov, 2012).

Since the object of research is computer systems, the assessment of control input parameters that physically affect information security risks in these systems in the form of linguistic expressions is organized as follows (Buldakova, 2019):

C_1 - processor (CPU) temperature; C_2 - hard disk temperature; C_3 - body temperature; F_1 - processor cooler (CPU) rotation speed; F_2 - Body coller rotation speed; H - humidity of the system unit.

The output linguistic variables include the following:

R - information security Risk level.

The term-set for input and output linguistic variables is defined as:

C_1, F_1, F_2, H - term set low, normal, high for n input linguistic variables; For C_2, C_3 is assigned very low, low, normal, high, very high.

The term output linguistic variable describes the level of many informational risks:

$$NO\ DANGER,\ LESS\ LIKELY\ DANGER,\ LOW,\ VERY\ HIGH$$

In order to ensure that the physical capabilities of computer computing devices taken as a research object are constantly monitored, the proposed fuzzy logic inference algorithm is formed with the help of a knowledge base and serves to predict and prevent threats that may occur in the system (Baranova & Gusev, 2016; Sakhno et al., 2018; Morozov et al., 2011; Mikov & Buldakova, 2013; Otero, 2014).

It is known that the fuzzy logic inference mechanism is defined as:

$$IF\ (x_1\ is\ A)\ AND\ (x_2\ is\ B),\ THEN\ (Y\ is\ C), \tag{1}$$

Here x_1, x_2 are the antecedent (conditional) part of fuzzy rules, $X \in (x_1, x_2, ...x_n)$. Y - is the consequent (result) part of fuzzy rules; A, B - are fuzzy sets defined on the set X; C is a fuzzy set defined on Y. $\mu_{A,B}(X) \in [0, 1]$ is the affiliation function of the set A and B. $\mu_C(X) \in [0, 1]$ is the affiliation function of the set C.

If the affiliation function of sets A and B is known - $\mu_{A,B}(X)$, the composition rule of the affiliation function for a fuzzy set C is defined as follows:

$$\mu_C(Y) = \sup\{T(\mu_A(x_1), \mu_B(x_2), \mu_R(x_1, x_2, y))\}$$

Here, the function is basically defined as follows (Baranova & Gusev, 2016; Sakhno et al., 2018; Morozov et al., 2011; Mikov & Buldakova, 2013):

$$\mu_i(x) = \frac{\omega_i(x)}{\sum\limits_{i=1}^{q} \omega_i(x)}, \omega_i(x) = \prod_{j=1}^{q} x_j^i \tag{2}$$

According to expression (2), the affiliation function, which is the fuzzy term set of the j^{th} state change of the object, is described as in figure 1 (that is, it is triangular in shape).

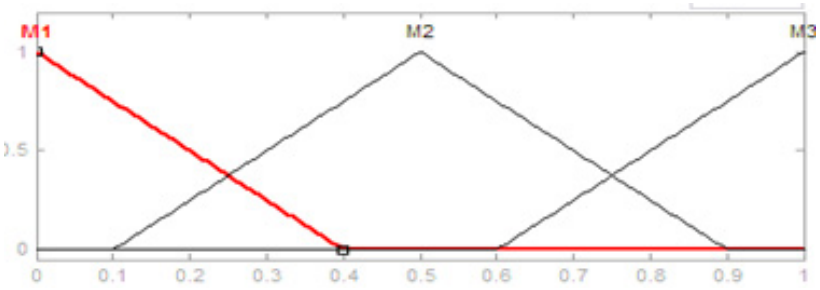

Figure 1: Description of the affiliation function of triangular type fuzzy term sets

As mentioned earlier, the process of forming a knowledge base consisting of 10 rules using the MATLAB application software package, that is, the Fuzzy Logic Toolbox packages included in its composition, was processed as follows:

IF C_1=LOW THEN R=NO DANGER
IF C_1= NORMAL THEN R=LESS LIKELY DANGER
IF C_1=HIGH THEN R=VERY HIGH
IF C_2=LOW THEN R=VERY HIGH
IF C_2=HIGH THEN R= VERY HIGH
IF C_2= LOW AND F_2= LOW THEN R= NO DANGER
IF C_3=CRITICALLY LOW THEN R= VERY HIGH
IF C_3=VERY HIGH THEN R= VERY HIGH
IF C_3=LOW AND F_2=LOW THEN R= NO DANGER
IF H=HIGH THEN R=VERY HIGH

The knowledge base processing process in the Fuzzy Logic Toolbox package was performed in the algorithmic sequence in the next section.

3 Modeling the process of assessing information security risks

Modeling of information security risk assessment process is done as follows (Castells, 2020):
1. *Matlab is started.*
2. The ***fuzzy*** command is assembled and executed in the opened ***Command Window***. In the opened window, in the ***FIS Editor Unitled*** window, from the ***File*** menu, select ***New FIS Sugeno*** fuzzy logic inference algorithm. Note that two subsystems are designed according to matrices A and B. A fuzzy subsystem with 6 inputs $(C_1, C_2, C_3, F_1, F_2, H)$ for matrices A and B and one output (R) for matrix C is designed (figure 2).

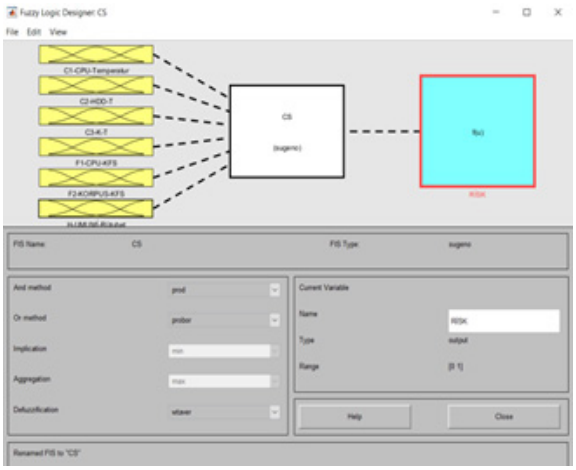

Figure 2: Fuzzy Sugeno model - subsystem design window

As can be seen from the figure, a fuzzy inference system for creating a fuzzy rule base risk assessment methodology it allows to determine the level of risk based on the development of an expert system to be implemented in the form of and subjective evaluations of all levels of information security (Morozov et al., 2011). The type of membership functions for each input variable is determined subjectively based on expert surveys. In practice, most often triangular and trapezoidal types of membership function are used. Rules for input linguistic variables are formulated as follows (Schrieber & Biglarbegian, 2014).

C_1, F_1, F_2 - the type of membership function *trimf* is selected for the input linguistic variables (figure 3):

$$trimf(3) = low,\ normal,\ high.$$

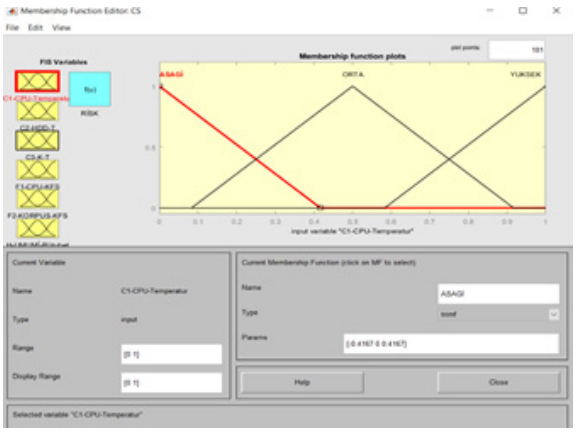

Figure 3: C_1, F_1, F_2 - determination of membership function for input linguistic variables

C_2, C_3 - type of membership function is selected for input linguistic variables *trimf* (figure 4):

$$trimf(4) = very\,low,\ low,\ normal,\ high,\ very\,high.$$

Figure 4: C_2, C_3 - definition of membership function for input linguistic variables

$R\,(RISK)$ - type of membership function is selected for output linguistic variable *trimf* (figure 5):

$$trimf(5) = bad,\ difficult,\ low,\ slightly\,high,\ very\,high.$$

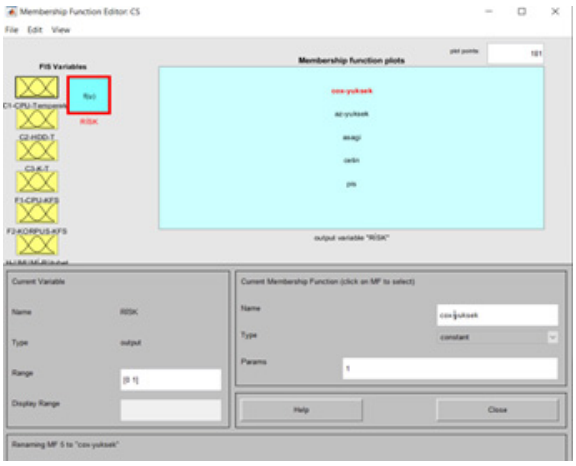

Figure 5: $R\,(RISK)$ - determination of the membership function for the output linguistic variable

After selecting the membership function of the input and output variables, it is required to create a rule base (Nassa & Yadav, 2012). Rule base *Edit-Rule* command is selected (figure 6).

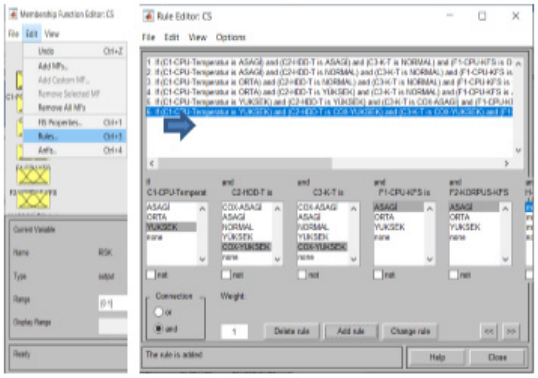

Figure 6: Rule base Edit-Rule command Rule

Rules base can be compiled n number of times depending on the set conditions (Takács, 2011). There is no limit to the formation of the rule base. However, as the number of the rule base increases, the issue of determining security risks becomes more precise (figure 7).

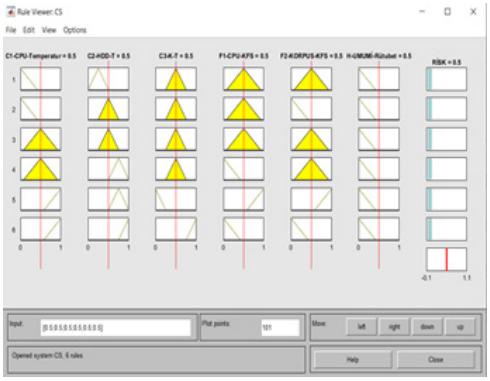

Figure 7: Information security rule base

4 Conclusion

Consequently, according to the performed calculation, the information security risk level is low in the measured parameters, which corresponds to the initial input data. In order to ensure that the physical capabilities of the computer computing devices taken as a research object are constantly monitored, the proposed fuzzy logical inference algorithm is formed with the help of the knowledge base and serves to predict and prevent threats that may occur in the system. Realization of the fuzzy model for the assessment of the state of the computer system in the MATLAB environment is adequate with the physical processes occurring in the system, and it allows to assess the information security risks whose sources are external factors that have many influences. Thus, adequate results obtained in terms of quantitative and qualitative indicators increase the risks of system security and allow to control them.

References

Alesinsky, E.I. (2021). The application of methods of fuzzy logic for the solution of a scientific task according to initial data. *Young student, 25*(367), 16-22 (in Russian).

Azhmukhamedov, I.M. (2012). Evaluation of sales safety of using the system based on a fuzzy-cognitive approach. *Issues of Information Security,* 1, 57-60 (in Russian).

Baranova, E.K., Gusev, A.M. (2016). Information security risk analysis technique using fuzzy logic based on MATLAB tools. *Educational Resources and Tech., 1*(13), 88-96 (in Russian).

Buldakova, T.I. (2019). Matlab application for information security risk analysis. II International Conference on Material Science, Smart Structures and Applications (ICMSS-2019). AIP Conference Proceedings, 2195(1), 020004. DOI:10.1063/1.5140104

Hong Xia, Li., Abubakar, B.O. (2020). Assessment of information security risks in the computer system using the Fuzzy Logic Toolbox package of the Matlab program. *International Journal of Engineering Science Invention (IJESI)*, *9*(12), 51-63.

Khazaeni, G., Khanzadi, M., Afshar, A. (2012). Fuzzy adaptive decision making model for selection balanced risk allocation. *International Journal of Project Management, 30*(4).

Morozov, D.I., Andreev, P.G., Naumova, I.Yu. (2011). Protection of radio-electronic means from the influence of climatic factors. *Radioelectronic Engineering, 1*(4), 255-261.

Mikov, D.A., Buldakova, T.I. (2013). Assessment of information risks in automated systems using a neuro-fuzzy model. *Science and Education*, 11, 295-310 (in Russian).

Nassa, V.K., Yadav, S.K. (2012). Project Management Efficiency - A Fuzzy Logic Approach. *International Journal of Engineering and Advanced Technology (IJEAT), 1*(3), 2249-8958.

Otero, A.R. (2014). Information Security Control Assessment Methodology for Organizations. *Nova Southeastern University. NSU Works.* `https://nsuworks.nova.edu/gscis_etd/266.`

Sakhno, V.V., Marshakov, D.V., Aidinyan, A.R. (2018). Application of fuzzy logic methods for solving the problem of ensuring information security. *Young researcher, 4*(13), 162-169 (in Russian).

Schrieber, M.D., Biglarbegian, M. (2014). Hardware Implementation of a Novel Inference Engine for Interval Type-2 Fuzzy Control on FPGA. *IEEE International Conference on Fuzzy Systems* (FUZZ-IEEE), Beijing, China, 640- 646

Takács, M. (2011). *Soft Computing-Based Risk Management - Fuzzy, Hierarchical Structured Decision-Making System.* Risk Management Trends. InTech.