Abhath Journal of Basic and Applied Sciences., 2(2) (2023) 34-37

Abhath Journal of Basic and Applied Sciences

Website:https://ojs.abhath-ye.com/index.php/OJSRJBAS/about

doi:

Research paper, Short communication, Review, Technical paper

Assessment of the Company Security System Based on Fuzzy Logic

Wadeea Ahmed Abdo Qaid[1]*, Siham Abdulmalik Mohammed Almasani[2]

[1,2]Collage of Computer Science and Engineering, Hodeidah University, Hodeidah, Yemen

***Corresponding author E-mail:* dr.wadqaid@gmail.com**

Received: 29 Oct. 2023. Accepted: 06 Sep. 2023. Published: 30 Dec. 2023.

Abstract

Company systems with low-level protection are always easy to penetrate, so assessment of the security system is essential. This paper is focused on developing a model to assess the effectiveness of security systems in a company using fuzzy logic to protect it from intrusions. There are numerous policy frameworks available to evaluate the security of a network, system or single computer. This work presents the most important criteria to assess the effectiveness of the company security system. The linguistic concepts to formalize the criteria were applied to develop a model that explains the true relationship between defensive capabilities and the probability of adversary success are given, in relation to which the experts will draw a conclusion and give an assessment of the effectiveness of the security system in a company, and that is warning the system administrator for expected threats. The proposed study shows its superiority in the area of fast response to cyber threats. To simulate the situation of a security system of the company using fuzzy logic, we use MATLAB.

Keywords: *security system; criteria, assessment; expert's knowledge; modeling; fuzzy sets.*

1. Introduction

Recently, the information security incidents are increased in the world and It has become a major threat. Many of such attacks affect a wide range of companies. Cybercriminals who attack government, financial institutions, and companies and personal users use a variety of modern IT technologies and software. The security system is a method by which something is secured through a system. Information which is stored and processed through information systems is an important resource that allows employees of the enterprise to implement their functions through it. The system will implement these functions very effectively, when the required level of control over information is implemented, and protect it from unauthorized implementation of actions on information. The security system aims to reduce or prevent threats and risks [1-3]. The best way to increase security is to focus on cyber protection of companies' systems from cyber terrorists; this paper is doing that through the assessment of the security of the system.

When any system administrator wants to assess the security of the system and increase the system's robustness, he has to consider several criteria (parameters) affecting this security. There are many criteria which allow comparing security assessments in the information system [4,5]. To achieve proper security, the criteria must be selected properly, where the business architecture of a company comprises a combination of process, people, and technology, so all three areas need to be properly addressed.

In this work, an approach has been developed to assess the security of the system using a fuzzy expert system. The proposed fuzzy expert system in this paper gives valuable information to the system administrators to improve the achievement of the system security.

The paper is structured as follows: In section 2, a review of some of the literary works to assess the effectiveness of a security system is presented. In section 3, Background on Fuzzy Logic is presented. Simulation of the proposed model and selecting the most important criteria to assess the effectiveness of a security system are shown in Section 4. The conclusions are summarized in Section 5.

2. Review of Related Research

Providing security of information and preventing threats constitutes a significant challenge for companies, so Cyber security has appeared as a significant field of research. There are many studies that have been done on cyber security, but these are mostly focused on the effects of cyber-attacks, prevention of cyber intrusion and how to evaluate information security.

In [6], this paper analyzed the cybersecurity of Energy Management System against data attacks. The results of this analysis showed how vulnerable the Energy Management System to data attacks and how.

Collaborative modeling can help to assess the vulnerability. The goal of the paper [7] was to use the proposed formalized approach, i.e. fuzzy analytic hierarchy process (AHP) to improve the method of information security management analysis. The proposed approach was used to select the most appropriate set of information security controls to meet the information security requirements of an organization. A study was done to analyze the structure of a power information management system in addition to quantifying the risk of cyber-attacks for creating secure systems, which remain poorly understood in the paper[8]. In this paper [9] compared existing Cyber Third-Party Risk Management (C-TPRM) methods created by different companies to identify the most commonly used evaluation criteria.

In this study, a new approach has been developed to assess the effectiveness of the security system in a company using a fuzzy expert system. The proposed fuzzy expert system in this paper gives valuable information to system administrators to improve the security system.

3. Background of Fuzzy Logic

Fuzzy logic helps people to make decisions based on inaccurate information. Fuzzy models are mathematical means of representing ambiguous and imprecise information. These models have the ability to recognize, represent, process, interpret and use data and information those are ambiguous and lacks certainty [10-13]. The fuzzy logic system consists of four main components [14]: Fuzzy rule base, fuzzy inference engine, fuzzification and defuzzification. The fuzzy rule base consists of a collection of fuzzy IF-THEN rules .There are many fuzzy inferences system, but in this article the Mamdani inference mechanism was preferred to determine the effectiveness of a security system ,because the Mamdani is both easy and suitable to design the systems within the required limits at most of the time.

4. Materials and Methods

Information security assessment is based on the adequacy of the protective measures used to ensure the required level of information security based on the measurement and evaluation of critical elements (criteria) of the company.

Assessment models are necessary to implement the assessment process. The process of conducting an information security assessment is represented through the main components of the process: context, criteria as shown in Fig.1.

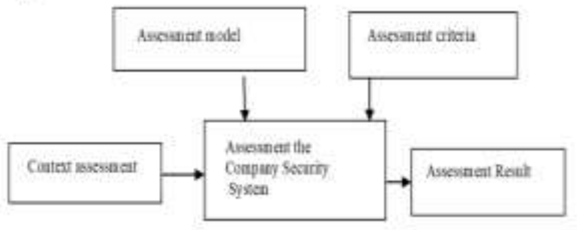


Fig.1. General view of the Company's information security assessment process

The important goal of the Information security assessment is to improve the information security. There are other goals of the Information security assessment, such as: – identification of the influence of critical elements (criteria) and their combination on the organization's information security; – comparing the maturity of various information security processes and comparing the degree of compliance of various safeguards with established requirements. The results of a company's information security assessment can also be used by any others companies to compare the level of information security of companies with the same business and comparable scale.

Depending on the selection criterion for the assessment of Information security, it is possible to divide the methods of assessing the Information security of a company (Fig. 2) into an assessment by a standard, a risk-based assessment and an assessment by economic criteria.

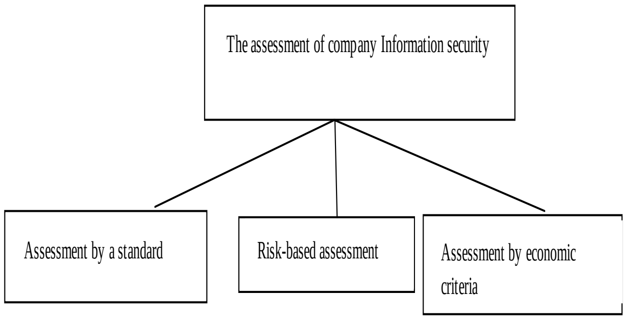

The assessment of company Information security
Assessment by a standard
Risk-based assessment
Assessment by economic criteria

fig.2. Methods for assessing the information security of a company

The method of assessing information security based on economic criteria operates with arguments that are understandable for business about the need to ensure and improve information security, so in this article, we used this method to assess the information security of a company.

To determine the effectiveness of a security system, the experts should select the criteria that determine the capabilities of the system to detect an adversary, delay an adversary long enough to engage once detected [15]. In this paper, it proposed using the most important criteria to assess the effectiveness of a security system as verbal concepts, which are defined by the experts in the form of linguistic variables:

- LV_1 – Access Controls;

Access control is a set of policies and measures for granting or revoking permission to a user to have access to the system and its resources in such a way that only authorized access is possible [16].

- LV_2 – Data Protection Force;

Data protection is paramount for the secure storage and confidential treatment of personal data. To enhance companies' operations and systems, data protection should be applied systematically throughout companies.

- LV_3 – Security Culture in the Company;

The concept of the Security Culture in the Company aims to be concerned with making information security considerations an integral part of an employee's job, habits and conduct, embedding them in their day-to-day actions[17].

- LV_4 – Reaction Force.

A reaction force is a force that acts in the opposite direction to an action force. Reaction forces and reaction moments are usually the result of heavy weapons, which the company to neutralize an identified threat.

Experts consider each of the criteria as a linguistic variable (LV), define a set $<\alpha_i, T(\alpha_i), X_i, G_i, M_i>$, $i = 1 , n$, where α_i – name of *LV; $T(\alpha_i)$* - term-set *LV* α_i; *Xi* – domain *LV* α_i , G_i - syntactic rule; M_i - semantic rule [8].

For each *LV* α_i experts give the term-set $T(\alpha_i)$ as sets of fuzzy variables $\alpha_i^j, i=\overline{1,n}, j=\overline{1,m_i}$ where m_i – domain of term-set $T(\alpha_i)$. Fuzzy variables α_i^j are defined by the sets $<\alpha_i^j, \tilde{C}(\alpha_i^j), X_i>$, where $\tilde{C}(\alpha_i^j)=\{<\mu_{C(\alpha_i^j)}(x_i)/x_i>\}$, $x_i \in X_i$ – fuzzy subset of sets X_i, $\mu_{C(\alpha_i^j)}(x_i)$ - membership function elements of $x_i \in X_i$ in fuzzy $\tilde{C}(\alpha_i^j)$.

In this work, the selected criteria will be determined at the verbal level by the following linguistic variables (LV) and term-sets as inputs for fuzzy logic:

- LV_1 – Access Controls has base-sets $T(LV_1)$={ LV_1^1 - Low; LV_1^2 - Medium; LV_1^3 - High};
- LV_2 – Data Protection Force has base-sets $T(LV_2)$={ LV_2^1 - Weak; LV_2^2- Medium; LV_2^3- Strong };
- LV_3 – Security Culture in the Company has base-sets $T(LV_3)$={ LV_3^1 - low; LV_3^2- Medium; LV_3^3- Strong};
- LV_4 – Reaction Force has base-sets $T(LV_4)$={ LV_4^1 - Slow; LV_4^2 - Medium; LV_4^3- Fast }.

To build this form, a set of rules is developed to evaluate input and produce the proper output. The results show the satisfactory performance of the proposed algorithm and more accuracy with respect to comparing methods. To assess the effectiveness of a security system, the program has been developed in the Matlab environment [18]. The program operation algorithm is shown in Fig. 3. The algorithm shows the process of identifying the effectiveness of the security system: measurement of criteria, fuzzification, fuzzy inference, defuzzification and the effectiveness of a security system.

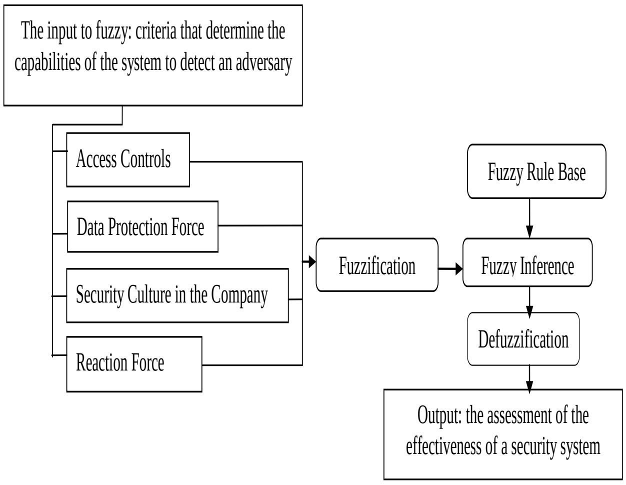

The input to fuzzy: criteria that determine the capabilities of the system to detect an adversary
Access Controls
Data Protection Force
Security Culture in the Company
Reaction Force
Fuzzification
Fuzzy Rule Base
Fuzzy Inference
Defuzzification
Output: the assessment of the effectiveness of a security system

Fig 3. The proposed fuzzy logic algorithm to assess the effectiveness of a security system

The output of the fuzzy model is the assessment of the effectiveness of a security system and it will take the following fuzzy sets: Weak, Medium, Strong, and Very Strong. After the determination of all LVs and FVs, the membership functions of FV are given for a logical decision conclusion regarding the effectiveness of a security system. The experts are putting the correspondence table "criteria - the effectiveness of a security system", as shown in Table.1.

TABLE I The correspondence table "situation-solution"

№ rule	LV_1	LV_2	LV_3	LV_4	Solution
1	High	Strong	Strong	Fast	Very Strong
2	High	Strong	Medium	Fast	Very Strong
3	High	Medium	Strong	Fast	Strong
4	Medium	Strong	Strong	Fast	Strong
	…	…	…	…	...
79	High	Strong	Medium	Medium	Medium
80	Medium	Weak	low	Slow	Weak
81	High	Weak	low	Slow	Weak

The decision-making algorithm according to the situation - action" correspondence table works in determining the degree of truth of the fuzzy rule [19-22] for each partition class. For the moment of decision making *t0*, the degrees of *FV* membership in the base sets are determined so that the coordinates of the input factors are obtained $(x_1^o x_2^o ,...,x_R^o) \in X_1 \times X_2 \times ... \times X_R = X$. Then the values of the membership degrees are given into the decision rules. The values of the membership degrees are calculated by $\mu_{L_i}(x_1^o ,x_2^o ,...,x_R^o),\ \ i=\overline{1,R}$. Among all the meanings μ_{L_l} the maximum value is found by

$$\mu_{L_S} = \max_j \mu_{L_j}(x_1^o ,x_2^o ,...,x_R^o) \qquad (1)$$

The input and output parameters in the Fuzzy Logic Toolbox environment are inserted as shown in Fig. 4.

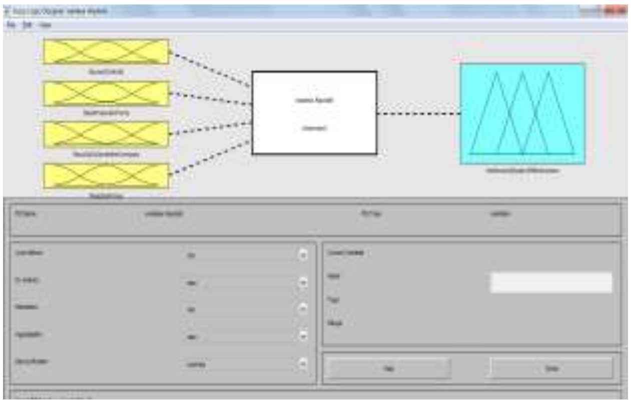


Fig.4, The input and output parameters in the Fuzzy Logic Toolbox

In Fig. 4 shows the membership functions forms of the fuzzy variables

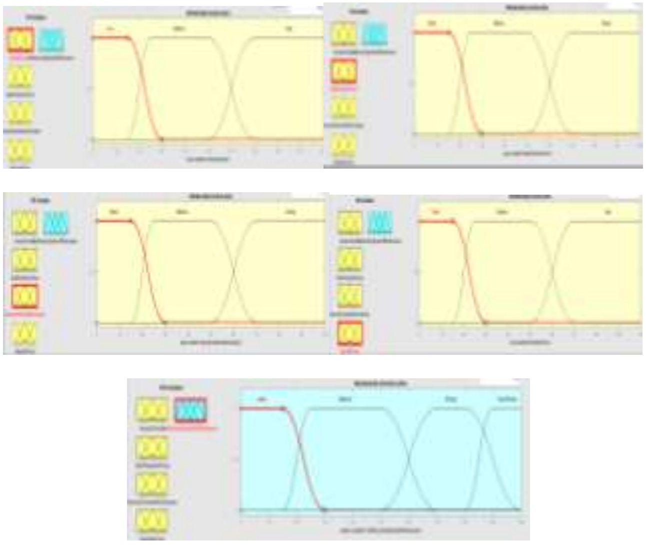
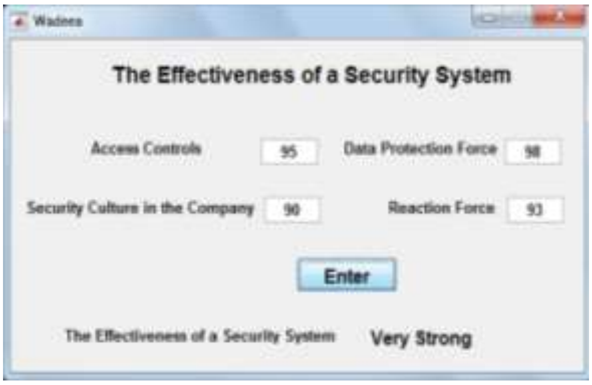


Fig.5. The membership functions forms

The experts have analyzed and processed the criteria. Fore example of the analysis and processing results, the following values in the program: Access Controls was determined by the value 95 %, Data Protection Force 98%, Security Culture in the Company 90%, Reaction Force 93% as shown in Fig. 6. After the values of the belonging degree of all FVs are determined, the program determines the effectiveness of a security system as shown in Fig. 6. As shown in Fig. 6, the effectiveness of a security system was very strong depending on the criteria values.



Wadees

The Effectiveness of a Security System

Access Controls 95 Data Protection Force 98

Security Culture in the Company 90 Reaction Force 93

The Effectiveness of a Security System Very Strong

Fig.6.The result of effectiveness of a security system

5. Conclusions

In the article, the urgency of assessing the effectiveness of a security system in a company has been substantiated. The method to assess the effectiveness of a security system in a company was developed. To determine the effectiveness of a security system, the experts determine the criteria that determine the capabilities of the system to detect an adversary, delay an adversary long enough to engage once detected. The article proposed using these criteria as verbal concepts, which are defined by the experts in the form of linguistic variables and determine the fuzzy reference states to assess the effectiveness of a security system. The proposed method gave an accurate assessment of the effectiveness of a security system.

Data Availability

No data were used to support this study.

Conflicts of Interest

The authors declare that they have no conficts of interest.

How to Cite : Wadeea Ahmed Abdo Qaid and Siham Abdulmalik Mohammed Almasani (2023). Assessment Of The Company Security System Based On Fuzzy Logic, *Abhath Journal of Basic and Applied Sciences*, 2(2), 34-37.

References

[1] D. Leon, S. Tomasz, M. Ireneusz, “Risk Assessment Methodology in Public Financial Institutions, ” IntechOpen ,Risk Management and Assessment, May 22nd, 2020.

[2] L. Manco, H. Medina, S. Botero, F. Legendre, “Risk assessment methodology: implementation of duration gap in corporate portfolios in order to reduce the systemic risk”, Estudios Gerenciales, vol. 34, no. 146,pp 34-41, 2018.

[3] H. Beheshti and M. Alborzi, “Using Fuzzy Logic to Increase the Accuracy of E-Commerce Risk Assessment Based on an Expert System”, Eng. Technol. Appl. Sci. Res., vol. 7, no. 6, pp. 2205–2209, Dec. 2017. https://doi.org/10.48084/etasr.1479

[4] L. Al-Qaisi, “Evaluation of E-Commerce Website Functionality Using **a Mamdani Fuzzy System”, Eng.** Technol. Appl. Sci. Res., vol. 5, no. 5, pp. 860–863, Oct. 2015. https://doi.org/10.48084/etasr.594

[5] W. McGill, B. Ayyub, M. Kaminskiy, “Risk Analysis for Critical Asset Protection,” Risk Analysis, vol. 27, no. 5,pp. 1265-1281, 2007.

[6] K. Pan, A. Teixeira, C. Lopez, P. Palensky, “Cosimulation for cyber security analysis: Data attacks against energy management system,” in 2017 IEEE International Conference on Smart Grid Communications, SmartGridComm, pp. 253-258.

[7] M. Tariq, S. Ahmed, N. Memon, S. Tayyaba, M. Ashraf , M. Nazi, A. Hussain, V. Balas, M. Balas, , “Prioritization of information security controls through fuzzy AHP for cloud computing networks and wireless sensor networks,” Sensors, vol. 20, no. 5, pp. 13-10, 2020.

[8] P. Woo, S. Hwang, S. Hwang, B. Kim, “Risk assessment for the security of power information control systems,” International Journal of Smart Grid and Clean Energy, vol. 8, no. 4, pp. 488-494, 2019.

[9] O. Keskin, K. Caramancion, I. Tatar, O. Raza, U.Tatar ,“Cyber third-party risk management: A comparison of non-intrusive risk scoring reports,” Electronics, vol. 10, no. 10, 1168, 2021.

[10] A. A. Alghamdi, “Computerised Information Security Using Texture Based Fuzzy Cryptosystem”, Eng. Technol. Appl. Sci. Res., vol. 8, no. 6, pp. 3598–3602, Dec. 2018. https://doi.org/10.48084/etasr.2353

[11] S.A.M Almasani, V.I. Finaev, W.A.A. Qaid W, A.V. Tychinsky, “Assessing the Current State of the Stock Market Under Uncertainty”, Journal of Theoretical and Applied Information Technology. vol.89, no.1, 2016.

[12] S.A.M Almasani, V.I. Finaev, W.A.A. Qaid, A.V. Tychinsky, “ The Decision-making Model for the Stock Market Under Uncertainty”, International Journal of Electrical and Computer Engineering, vol.7, no. 5, pp. 2782 – 2790, 2017.

[13] S.A.M. Almasani, V.I Finaev, “ Information support for decision making under uncertainty in the securities market” , in 2016 , International Conference «Innovative technologies and didactics in teaching (ITDT-2016)», Spain. From 2 till 3 May. La Laguna, pp. 153 – 161.

[14] L.A.Zadeh. Fuzzy sets and their application to pattern classification and clustering analysis. Published in: Book: Fuzzy sets, fuzzy logic, and fuzzy systems. World Scientific Publishing Co., Inc. River Edge, NJ, USA. 1996.Pages 355 – 393.

[15] G. Stoneburner, A. Goguen, A. Feringa “Risk Management Guide for Information Technology Systems”, NIST Special Publication 800-30 ,Gaithersburg, USA, 2002,page 54.

[16] M. Shabnam, M. Nasser, ” Criteria Specifications for the Comparison andEvaluation of Access Control Models”, I. J. Computer Network and Information Security,vol. 5, 19-29, 2013.

[17] Špela Orehek and Gregor Petrič, 2021, “A systematic review of scales for measuring information security culture”, Information & Computer Security,Vol. 29 No. 1, pp. 133-158.

[18] J. S. Roger Jang, “ Matlab fuzzy logic toolbox user guide”, Math Works, 1997, Pages: 64.

[19] M. Biswaranjan, “Decision making in Inventory Management: Benefit Potential of Inventory Control Theory”, Publisher: LAP LAMBERT Academic Publishing, 2011, P – 184.

[20] S.A.M. Almasani, W.A.A. Qaid, J.A.M. Saif, I.A.A. Alqubati, “ Fuzzy rule based sentiment analysis for finding University Studentn Satisfaction in Yemen”. Indian Journal of Science and Technology,vol. 14, no.44, pp. 3264-3269, 2021.

[21] V.I. Finaev, W.A.A. Qaid, “ Decision-making Strategies Within the Format of Initial Information Uncertainty in the Problems of Investments” , World Applied Sciences Journal, vo. 26, no. 11, pp. 1444-1450, 2013.

[22] W.A.A. Qaid. V.I. Finaev, A.V Tychinsky, “Algorithmization of the Process of Preparation of Capital Investment Project”, vol 6 , no.2, 2015.