A Fuzzy Based MCDM Methodology for Risk Evaluation of Cyber Security Technologies

Melike Erdoğan[1(✉)], Ali Karaşan[2], İhsan Kaya[3], Ayşenur Budak[4], and Murat Çolak[5]

[1] Duzce University, Konuralp, 81620 Düzce, Turkey
melikeerdogan@duzce.edu.tr
[2] Yildiz Technical University, Davutpasa, 34220 Istanbul, Turkey
akarasan@yildiz.edu.tr
[3] Yildiz Technical University, Besiktas, 34349 Istanbul, Turkey
ihkaya@yildiz.edu.tr
[4] Gebze Technical University, 41400 Gebze, Kocaeli, Turkey
abudak@gtu.edu.tr
[5] Kocaeli University, 41380 Izmit, Kocaeli, Turkey
colak.murat@kocaeli.edu.tr

Abstract. Cyber security that also known as information technology security is to protect computers, mobile devices, servers, electronic systems and networks from malicious digital attacks. In recent years, cyber security threats have been a growing problem for any critical digital infrastructure and various cyber-attacks created over the Internet are also becoming a big issue for the society. Therefore, the use of technologies developed to provide cyber security is very important. However, the risks of cyber security technologies should be taken into account when choosing among cyber security technologies. For this aim, we have proposed a multi-criteria decision making (MCDM) methodology based on hesitant fuzzy sets (HFSs) that gives experts extra flexibility in using linguistic terms to evaluate the criteria and alternatives to determine the best cyber security technology. For this aim, a study has also been discussed which deals with risk factors in the selection of cyber security technologies via fuzzy MCDM process.

Keywords: Cyber security technology · Hesitant fuzzy sets · Multi criteria decision making · Risk evaluation

1 Introduction

Cyber security plays an increasingly significant role as a result of the rapid development of information and industrialization. In this context, some cyber security problems have revealed with development of technology. Cyber-attacks are seen as potential threats by approximately 40% of countries in the world and therefore cyber security efforts are realized at all levels as a result of global assessment [1]. Different online applications such as online banking, e-commerce and m-commerce has become suitable for cyber-attacks because of advanced internet-computer interconnectivity. Except its different advantages, growing digital world creates important threats related to some critical departments of government like defense industry in a country.

C. Kahraman et al. (Eds.): INFUS 2019, AISC 1029, pp. 1042–1049, 2020.
https://doi.org/10.1007/978-3-030-23756-1_123

Nowadays, cyber security has become a significant concept in the world as a result of increasing cyber-crimes. It has become necessary to find reliable and robust security solutions by pioneers of information security field due to losses rooted from cyber-attacks [2]. Cyber security is a comprehensive term and there are some different definitions in the literature related to this concept. For instance, it is defined in the Merriam Webster dictionary as “measures taken to protect a computer or computer system (as on the Internet) against unauthorized access or attack”. Besides, the International Telecommunications Union (ITU) defines this term as collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be utilized to protect the cyber environment, organization and user’s assets. Connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and information existing in the cyber environment compose organization and user’s assets. Cyber security measures aim to provide perception and maintenance of security properties against security attacks in the cyber environment [3]. Cyber security includes a set of technologies and processes in order to avoid computers, networks, programs, and data from attack, unauthorized access, change, or destruction. In the cyber security systems, there are network and computer security systems and each of them must has a firewall, antivirus software and intrusion detection system (IDS). IDSs enable to determine and identify unauthorized usage, duplication, alteration and destruction of information systems. The security infringements include external and internal attacks realized against organization [4]. Adoption of cyber security technologies is very important in terms of information security. Many cyber security technologies are available in the literature. Ranking of importance for these technologies and analyzing the necessity of having the technology in the first place will provide important benefits to the companies. However, it is necessary to consider the risks caused by these technologies at the same time. Considering all these, we carry out the importance of cyber security technologies in this paper by using a MCDM methodology based on hesitant fuzzy sets (HFSs) which provide more flexibility than ordinary fuzzy sets in linguistic assessments of criteria and alternatives. We know that the fuzzy sets are also used to reflect the uncertainty of decision makers in evaluating criteria and alternatives, and to obtain results closer to reality.

The rest of the paper has been organized as follows: Sect. 2 gives a briefly information about the cyber security technologies. Section 3 presents the details of the proposed methodology based on HFS. Section 4 shows real-life analysis for the proposed method. Finally, Sect. 5 includes the obtained results and future research suggestions.

2 Cyber Security Technologies

With the development of open, free, international cyber technologies, many important changes have been made to the countries of the world, to all governmental organizations, to all business organizations and to all aspects of our lives [5]. In the literature, it is possible to come across studies dealing with cyber security technologies. For example, Daley et al. [6] investigated the initiatives of Canadian Nuclear Laboratories to assess the appropriateness and effectiveness of cyber security technology and practices. Ning and Zhang [5] examined the development of cyber security technologies and its relation with other technologies. Boddy et al. [7] presented a research towards a system, which could detect unusual data behavior through the use of advanced data analytics and visualization techniques for healthcare infrastructures. Giacobe [8] searched the basic processes determined in the Joint Directors of Laboratories (JDL) data fusion process model and described them in a cyber security context. Romero-Mariona et al. [9] presented a new technology developed to secure critical infrastructures named as C-SEC (Cyber SCADA Evaluation Capability). Eom et al. [10] suggested a robust and operational cyber military strategy for cyber dominance in cyber wars. In addition to reviewing the literature related to cyber security technologies, it is necessary to consider market researches as it is closely related to companies. In this case, Gartner Company, which conducts research on information security, should be mentioned. Gartner is a global research and advisory based company centered in America [11]. It provides predictions, recommendations and tools for leaders across the world in IT, Finance, HR, Customer Service and Support, Legal and Compliance, Marketing, Sales and Supply Chain functions [11]. As a result of their research, Gartner has determined the best technologies for information security such as [12]: Cloud Workload Protection Platforms (A1), Remote Browser (A2), Deception (A3), Network Traffic Analysis (A4), Managed Detection and Response (A5), Micro segmentation (A6), Software-Defined Perimeters (A7), Cloud Access Security Brokers (A8), OSS Security Scanning and Software Composition Analysis for DevSecOps (A9), Container Security (A10).

As a result of detailed investigations both from literature and researches, these are determined as information security technologies that are established to ensure cyber security and to protect against advanced attacks. It is also important to rank these technologies and to determine which technologies should be considered first. Since this analysis requires more than one alternative and includes many different criteria to be taken into consideration in order of importance. So it can be considered as a multi-criteria decision making (MCDM) problem. Since each evaluation criterion in the analysis process cannot be expressed numerically, the use of a fuzzy logic based approach will give results that are closer to reality. As a result of these factors, a MCDM methodology based on hesitant fuzzy sets has been adopted for the comparison of cyber security technologies.

3 The Proposed Model to Evaluate Cyber Security Technologies

In this paper, we used a hesitant linguistic group decision making model for determining the best cyber security technology with fuzzy envelopes in hesitant decision making. The steps of the proposed algorithm are described as below [13, 14]:

Step 1. Define the semantics and syntax of the linguistic term set S

Step 2. Define the context-free grammar G_H

Step 3. Gather the preference relations $\tilde{p}$ and $\tilde{p}^k$ provided by experts $k \in \{1, 2, \ldots, t\}$ for both criteria weights and criteria-alternative evaluations with making experts applying linguistic term sets.

Step 4. Transform linguistic expressions into linguistic intervals [14]: The transformation function E_{GH} provides an initial basis for group decision making problems:

$$E_{GH}(\tilde{p}_{ij}^k) = Hs(\tilde{p}_{ij}^k) \tag{1}$$

$$E_{GH}(\tilde{p}_{it}) = Hs(\tilde{p}_{it}) \tag{2}$$

where i ∈ {1,…, n} n is the number of criteria, j ∈ {1,…, m} m is the number of alternatives and k ∈ {1,…, t} t is the number of experts.

Step 5. Obtain an envelope for criteria weights $\left[\tilde{p}_{it}^-, \tilde{p}_{it}^+\right]$ and alternative evaluations $\left[\tilde{p}_{ij}^{k-}, \tilde{p}_{ij}^{k+}\right]$ for each hesitant fuzzy linguistic term sets (HFLTS). The envelope for each HFLTS are obtained as follows:

$$env(Hs(\tilde{p}_{it})) = \left[\tilde{p}_{it}^-, \tilde{p}_{it}^+\right] \tag{3}$$

$$env\left(Hs\left(\tilde{p}_{ij}^k\right)\right) = \left[\tilde{p}_{ij}^{k-}, \tilde{p}_{ij}^{k+}\right] \tag{4}$$

Step 6. Select two linguistic aggregation operators φ and ϕ, which might be the same. In this case, a suitable aggregation operator will be selected to deal with linguistic intervals obtained in the previous phase. Without loss of generality and for the sake of simplicity, in the aggregation phase we use the arithmetic mean aggregation operator based on 2-tuple defined as follows:

$$\tilde{\chi}mean = \Delta\left(\frac{1}{n}\sum_{i=1}^{n} \Delta^{-1}(\tilde{s}_i, \tilde{\alpha}_i)\right) = \Delta\left(\frac{1}{n}\sum_{i=1}^{n} \tilde{\beta}_i\right) \tag{5}$$

Step 7. Obtain the pessimistic and optimistic collective preference relations P_c^- and P_c^+ through linguistic aggregation operator φ. A linguistic aggregation operator φ should be selected according to problem. It will be used to aggregate separately the right and left limits of the linguistic intervals, obtaining two collective preference relations for criteria evaluations $\tilde{P}^+$ and $\tilde{P}^-$, for alternative-criteria evaluations $\tilde{P}_C^+$ and $\tilde{P}_C^-$, respectively. These collective preferences are represented by 2-tuple linguistic values for criteria weights and for criteria-alternative evaluations preferences as follows:

$$\tilde{P}^+ = \begin{pmatrix} (\tilde{S}r, \tilde{\alpha})_{11}^+ \\ \vdots \\ (\tilde{S}r, \tilde{\alpha})_{n1}^+ \end{pmatrix} \tilde{P}^- = \begin{pmatrix} (\tilde{S}r, \tilde{\alpha})_{11}^- \\ \vdots \\ (\tilde{S}r, \tilde{\alpha})_{n1}^- \end{pmatrix} \tag{6}$$

$$(\tilde{S}r, \tilde{\alpha})_i^+ = \Delta\left(\varphi\left(\Delta^{-1}\left(\tilde{p}_{ik}^+\right)\right)\right) \; \forall k \in \{1, \ldots..t\} \tag{7}$$

$$\left(\tilde{S}r,\tilde{\alpha}\right)_{i}^{-}=\Delta\left(\varphi\left(\Delta^{-1}\left(\tilde{p}_{ik}^{-}\right)\right)\right)\ \forall k\in\{1,\ldots..t\} \tag{8}$$

$$\tilde{P}_{c}^{+}=\begin{pmatrix}\left(\tilde{S}r,\tilde{\alpha}\right)_{11}^{+} & \ldots\ldots & \left(\tilde{S}r,\tilde{\alpha}\right)_{1m}^{+}\\ \vdots & \vdots & \vdots\\ \left(\tilde{S}r,\tilde{\alpha}\right)_{n1}^{+} & \ldots\ldots & \left(\tilde{S}r,\tilde{\alpha}\right)_{mn}^{+}\end{pmatrix} \tag{9}$$

$$\tilde{P}_{c}^{-}=\begin{pmatrix}\left(\tilde{S}r,\tilde{\alpha}\right)_{11}^{-} & \ldots\ldots & \left(\tilde{S}r,\tilde{\alpha}\right)_{1m}^{-}\\ \vdots & \vdots & \vdots\\ \left(\tilde{S}r,\tilde{\alpha}\right)_{n1}^{-} & \ldots\ldots & \left(\tilde{S}r,\tilde{\alpha}\right)_{mn}^{-}\end{pmatrix} \tag{10}$$

$$\left(\tilde{S}r,\tilde{\alpha}\right)_{ij}^{+}=\Delta\left(\varphi\left(\Delta^{-1}\left(\tilde{p}_{ij}^{k+}\right)\right)\right)\ \forall k\in\{1,\ldots..t\} \tag{11}$$

$$\left(\tilde{S}r,\tilde{\alpha}\right)_{ij}^{-}=\Delta\left(\varphi\left(\Delta^{-1}\left(\tilde{p}_{ij}^{k-}\right)\right)\right)\ \forall k\in\{1,\ldots..t\} \tag{12}$$

being i ∈ {1, 2, … , n}, j ∈ {1, 2, … , m} and $Sr\in S=\{S0,\ldots,Sg\}$

Step 8. Compute a pessimistic and optimistic collective preferences for each alternative applying by using Eqs. (13) and (14).

$$p_{i}^{+}=\Delta\left(\phi\left(\Delta^{-1}(S_{r},\alpha)_{ij}^{+}\right)\right)\ \forall j\in\{1,\ldots n\} \tag{13}$$

$$p_{i}^{-}=\Delta\left(\phi\left(\Delta^{-1}(S_{r},\alpha)_{ij}^{-}\right)\right)\ \forall j\in\{1,\ldots n\} \tag{14}$$

Step 9. Build a vector of intervals $V^{R}=\left(p_{1}^{R},\ldots.,p_{N}^{R}\right)$, of collective preferences for the alternatives $p_{i}^{R}=\left[p_{i}^{+},p_{i}^{-}\right]$.

Step 10. Use an aggregation operator for pessimistic and optimistic preferences which can be arithmetic average for this application.

Step 11. Normalize all the aggregated preferences with using linear normalization method.

Step 12. Obtain weighted normalized decision matrices by multiplying the normalized criteria weights and the decision matrix for alternatives. For example, for optimistic evaluations, weighted normalized decision matrix can be obtained as:

$$\tilde{V}^{+}=\left[\tilde{v}_{ij}^{+}\right]nxm,\quad i=1,..n;\ j=1,..m \tag{15}$$

$$\tilde{W}^{+}=\left[\tilde{w}_{i}^{+}\right]nx1,\quad i=1,..n \tag{16}$$

$$\tilde{r}_{ij}=\tilde{w}_{i}^{+}\otimes\tilde{v}_{ij}^{+} \tag{17}$$

where w_{ij} represents the importance of criterion C_i.

Step 13. Calculate final scores for each alternative by using weighted average values of criteria-alternative evaluations.

Step 14. Rank the alternatives and determine the most suitable(s).

4 Application

Cyber security threats have emerged in recent years as a growing concern for networks and computers. Most efforts to improve cyber security focus on the inclusion of new technological approaches [15]. However, these security systems collect a large amount of data, which poses a serious threat to the privacy of persons protected by system [16]. In this sense it is very important to perform risk analyzes for cyber security technologies. The privacy risks of cyber security technologies in the literature are determined as follows [16]: Data exposure, Level of identification, Data sensitivity, Level of user control. From this point of view, we conducted a risk-based prioritization study for cyber security technologies according to these identified risks. Our alternatives are the cyber security technologies determined by Gartner and our evaluation criteria are the security risks determined in the literature. After the criterion-alternative determination, the proposed method is applied as follows. Firstly, two linguistic terms sets are defined for criteria and alternatives separately. Then context-free grammar G_H and the membership values for the linguistic terms sets are defined. After that, the preference relations provided by experts for both criteria weights and criteria-alternative evaluations are gathered form experts. At this stage, the opinions of three experts are obtained in gathering the evaluations via surveys. The weights of criteria determined by expert assessments are obtained as shown in Table 1.

Table 1. Weights of criteria.

Criteria	Weight
Data exposure	0.253
Level of identification	0.330
Data sensitivity	0.276
Level of user control	0.140

According to Table 1, the most important criterion has been determined as "Level of identification". This shows that the most important factor in selecting cyber security technologies in the selection of security risks is level of identification. On the other hand, the least effective factor in the selection process has been determined as "Level of user control". After determining the criteria weights, the criteria alternative evaluations scores are calculated. Based on these evaluations, each score has been calculated for all criteria-alternative evaluation. Then, the final scores have been obtained by multiplying the criteria weights with these alternatives' scores calculated on the basis of each criterion. Table 2 shows the final scores for each alternative.

According to Table 2. The alternative "A8: Cloud Access Security Brokers" has been determined as the best alternative. This alternative should be preferred as the first in cyber security system with respect to risk factor. The latest alternative has been determined as "A5: Managed Detection and Response". If the technologies are developed according to the determined risks. The current ranking can be changed, and the technologies identified in the lower ranks may increase to the first rank.

Table 2. Final results.

	Criteria-alternative scores				Final scores	Ranking
	Data exposure	Level of identification	Data sensitivity	Level of user control		
Criteria weights	0.2400	0.3511	0.2622	0.1467		
A1	0.0915	0.1030	0.0921	0.0909	0.0965	8
A2	0.0999	0.0867	0.0915	0.1120	0.1017	3
A3	0.0861	0.0885	0.0891	0.0945	0.0954	9
A4	0.0999	0.1036	0.0951	0.0975	0.0994	6
A5	0.0921	0.0987	0.0963	0.0837	0.0942	10
A6	0.0969	0.1048	0.0975	0.0975	0.0995	5
A7	0.1114	0.1156	0.1120	0.1072	0.1057	2
A8	0.1132	0.0993	0.1180	0.1216	0.1090	1
A9	0.1023	0.0885	0.0963	0.0957	0.0975	7
A10	0.1066	0.1114	0.1084	0.0951	0.1010	4

5 Conclusions

Cyber security technologies are important tools for protecting computers and networks against cyber-attacks. However, these systems affect the privacy of individuals by monitoring networks and computing devices [16]. Therefore, it is crucial to consider the risks they have in choosing cyber security technologies. In this paper, we conduct a study which takes into account the risks for determining the importance of cyber security technologies. Because of several evaluation criteria and alternatives in the decision process we use a multi-criteria decision-making approach for ranking alternatives. Besides, we apply to hesitant fuzzy sets that provide more flexibility than ordinary fuzzy sets in linguistic assessments of criteria and alternatives. As a result of the prioritization work, it has been determined that the criterion that should be considered first in the selection of the cyber security technologies is "Level of identification". The cyber security technology alternative determined in first place is "Cloud Access Security Brokers". As a future research suggestion it is possible to say that different MCDM methodologies can be applied in order to solve this decision problem and the results can be compared with this study. Besides, as a future research directions, different extensions of regular fuzzy sets such as intuitionistic fuzzy sets and Pythagorean fuzzy sets can be used with together MCDM methods for this problem and the obtained results can be discussed.

References

1. Alali, M., Almogren, A., Hassan, M.M., Rassan, I.A.L., Bhuiyan, M.Z.A.: Improving risk assessment model of cyber security using fuzzy logic inference system. Comput. Secur. **74**, 323–339 (2018)

2. Kour, J., Hanmandlu, M., Ansari, A.Q.: Biometrics in cyber security. Defence Sci. J. **66**(6), 600–604 (2016)
3. Von Solms, R., Van Niekerk, J.: From information security to cyber security. Comput. Secur. **38**, 97–102 (2013)
4. Buczak, A.L., Guven, E.: A survey of data mining and machine learning methods for cyber security intrusion detection. IEEE Commun. Surv. Tutorials **18**(2), 1153–1176 (2016)
5. Ning, X., Zhang, S.: Cyber Security Status and Technology Development. Nanjing University of Posts & Telecommunications (2012)
6. Daley, M., Doucet, R., Echlin, M., MacDonald, M., Mihaylov, V., Sijs, J., Trask, D.: Cyber security. Compliance to the new CSA 290.7 standard. Can. Nucl. Soc. Bull. **36**(4), 21–26 (2015)
7. Boddy, A., Hurst, W., Mackay, M., El Rhalibi, A.: A study into data analysis and visualization to increase the cyber-resilience of healthcare infrastructures. In: Proceedings of the 1st International Conference on Internet of Things and Machine Learning - IML 2017, pp. 1–7 (2017)
8. Giacobe, N.A.: Application of the JDL data fusion process model for cyber security. In: Multisensor, Multisource Information Fusion: Architectures, Algorithms, and Applications 2010, vol. 7710, pp. 77100R (2010)
9. Romero-Mariona, J., Kline, M., Miguel, J.S.: C-SEC (Cyber SCADA evaluation capability): securing critical infrastructures. In: 2015 IEEE International Symposium on Software Reliability Engineering Workshops (ISSREW), pp. 38–38 (2015)
10. Eom, JH., Kim, NU., Kim, SH., Chung, TM.: Cyber military strategy for cyberspace superiority in cyber warfare. In: Proceedings 2012 International Conference on Cyber Security. Cyber Warfare and Digital Forensic (CyberSec), pp. 295–299 (2012)
11. About Gartner. https://www.gartner.com/en/about. Accessed 5 Feb 2019
12. Gartner Identifies the Top Technologies for Security in 2017. https://www.gartner.com/en/newsroom/press-releases/2017-06-14-gartner-identifies-the-top-technologies-for-security-in-2017. Accessed 4 Feb 2019
13. Erdogan, M., Kaya, I.: Selection of the best outsourcing firm for WEEE under hesitant fuzzy environment. J. Intell. Fuzzy Syst. **35**(3), 3295–3306 (2018)
14. Rodriguez, R.M., Martinez, L., Herrera, F.: A group decision making model dealing with comparative linguistic expressions based on hesitant fuzzy linguistic term sets. Inf. Sci. **241**, 28–42 (2013)
15. Pfleeger, S.L., Caputo, D.D.: Leveraging behavioral science to mitigate cyber security risk. Comput. Secur. **31**(4), 597–611 (2012)
16. Toch, E., Bettini, C., Shmueli, E., Radaelli, L., Lanzi, A., Riboni, D., Lepri, B.: The privacy implications of cyber security systems: a technological survey. ACM Comput. Surv. **51**(2), 1–27 (2018)