Research Article

Multi-criteria usability evaluation of symmetric data encryption algorithms in fuzzy environment

Serkan Balli[1] · Menduh Yilmaz[2]

Received: 19 March 2020 / Accepted: 2 July 2020 / Published online: 17 July 2020

Abstract

Effective use of parameters such as time, resources, and energy is a crucial subject in daily life. These parameters directly influence the selection strategy in decision-making problems. While using encryption algorithms, it may be a problem to choose which algorithm to use according to file types in order to use resources efficiently. In this study, a C#-based program has been developed to measure various performance parameters and to compare symmetric data encryption algorithms. Accordingly, an intelligent selection system has been created that allows the most efficient encryption algorithm to be selected when encrypting text, audio, and video files. In this system, the user is presented with three profiles as "Quick," "Performance," and "Secure." Thanks to these profiles, the user can find the answer by selecting the desired profile according to the purpose. The data obtained from the program have been converted to fuzzy values using fuzzy logic. The generated fuzzy values have been evaluated separately using FAHP, TOPSIS, and PROMETHEE multi-criteria decision-making methods, and the PROMETHEE method has been found as the ranking method giving the closest result to the order created by the expert. The developed system provides efficient use of time, resources, and security.

Keywords Data encryption · Fuzzy logic · PROMETHEE · Smart choice · Cryptography

1 Introduction

Nowadays, it is inevitable to use encryption technology to prevent others from accessing the data and to prevent them from accessing the content even if they reach it [1]. The hiding process for making the content of a message unreadable is defined as encryption. Electronic communication is now a substitute for any communication made by writing on paper. This relates directly to the security and reliability of information shared via open networks that individuals/organizations/communities can make private/public/official communications via electronic communication networks [2]. Messages sent from open networks are threatened by third parties to listen and change [3]. Therefore, when sending a file over the network, it is necessary to encrypt it with any algorithm. However, using all resources efficiently and the permanence of the algorithm play a determinant role in the algorithm selection process. In this context, measuring performance is critical to make a concrete evaluation between cryptographic algorithms.

Symmetric encryption algorithms are faster than asymmetric encryption algorithms when it comes to performance management. Table 1 provides a comparison of symmetric and asymmetric encryption algorithms' characteristics. The explanations of features in Table 1 are as follows: privacy is the state of being free from observation by other persons. Integrity is the case of being whole and undivided. Authentication means identity validation. Undeniable shows that encryption and decryption processes are accurate and not be disputed. Performance means the speed of encryption and decryption processes.

✉ Serkan Balli, serkan@mu.edu.tr | [1]Department of Information Systems Engineering, Faculty of Technology, Mugla Sitki Kocman University, 48000 Mugla, Turkey. [2]Zubeyde Hanim Vocational and Technical Anatolian High School, 48000 Mugla, Turkey.

SN Applied Sciences (2020) 2:1393 | https://doi.org/10.1007/s42452-020-3170-9

Table 1 Comparison of symmetric and asymmetric encryption algorithms [4]

Feature	Symmetric encryption algorithms	Asymmetric encryption algorithms
Privacy	Good	Good
Integrity	–	Good
Authentication	–	Good
Undeniable	–	Good
Performance	Fast	Slow
Security	Dependent on key length	Dependent on key length

Security is the probability of breaking encryption and it depends on key length [4].

In this study, the performances of encryption algorithms have been measured and compared. Therefore, when the data in Table 1 is considered, "Symmetric Encryption Algorithms" has been chosen as the encryption algorithm type because it is more efficient on performance.

This work investigates the evaluation of symmetric data encryption algorithms in a fuzzy environment. The study approaches the problem with a multi-criteria perspective. Fuzzy analytic hierarchy process (FAHP), TOPSIS, and PROMETHEE multi-criteria decision-making (MCDM) methods are employed for evaluation. The problem involves different types of criteria, so fuzzy logic is ideal to combine parameters of various value forms on a single axis. Besides, the expert uses linguistic values to determine the criteria weights. In fuzzy logic, using linguistic values is inherent. Therefore, the fuzzy MCDM approach is preferred. FAHP, TOPSIS, and PROMETHEE methods are employed for selection, evaluation, ranking in the literature to solve various decision problems such as cloud service selection [5], selection of mobile health [6], service selection [7], software security estimation [8], web service selection [9], blockchain technology evaluation [10], supplier selection [11], evaluation of the network service providers [12], and other fields so on.

When the literature is examined regarding the performance of encryption algorithms; in study conducted by Guvenoglu [13], digital signature, SCAN, MLIE, CIE, BRIE image encryption algorithms have been investigated. The general structure and performance of these algorithms have been studied. In the work done by Yerlikaya [14], the structures of symmetric and asymmetric encryption algorithms commonly used today and the attacks on these algorithms have been examined. To understand the encryption algorithms, mathematical theorems and prime numbers used in the keys have been examined. The structure of RSA, ECC, DES, AES algorithms and attack techniques, performance analysis, cryptanalysis, and stenography applications on these algorithms have been investigated. In the work performed by Gunden [3], the processor, time and memory complexities of the most frequently used algorithms from symmetric and asymmetric encryption algorithms for information security have been tested and their performances have been compared. In his study, Blowfish, Twofish, IDEA, TEA, DES, AES, 3DES, RC2 encryption algorithms have been used and the RSA algorithm has been preferred from asymmetric encryption algorithms. In study conducted by Elminaam et al. [15], AES (Rijndael), DES, 3DES, RC2, Blowfish, and RC6 symmetric encryption algorithms have been compared in different settings in terms of data blocks at different sizes, different data types, battery consumption, key length, and encryption/decryption rates for each. Kumar et al. [16] have compared DES, AES, and Blowfish symmetric encryption algorithms concerning "speed, block length, and key length" parameters. Benchmarking has been designed using the Java programming language. Data encryption algorithms and performance analyses have been examined in the work done by Ciger [17]. In his study, symmetric and asymmetric algorithms have been compared in terms of the keys used. The speed and memory parameters for the encryption and decryption capabilities of RSA, DES, and AES encryption algorithms have been evaluated. Besides, encryption algorithms for audio, video, and real-time data have also been discussed. Hsiao [2] presented a neural-network-based architect for secure communications in multiple time-delay chaotic systems using the RSA algorithm and chaotic synchronization. Rajesh et al. [18] have proposed a new symmetric encryption algorithm to ensure improved security for sending text files through the IoT network by using extra keys dynamically. Al-Asli et al. [19] have proposed a new scheme on field-programmable gate arrays using symmetric encryption. Guo et al. [20] have presented dynamic multi-phrase ranked search over encrypted data with symmetric searchable encryption. Taha et al. [21] has proposed an intelligent switching method from exact encryption to short encryption considering the existent resources dynamically.

Nowadays, making more productive use of time is a vital task. It is possible to encrypt the data with various encryption algorithms. However, when encrypting the data, "Which algorithm is more efficient for encryption?" question arises. Data encryption with a random algorithm regardless of any criteria can lead to negative situation management such as misuse of time, unnecessary resource, or determining the level of privacy improperly. To prevent these adversities, the creation of special profiles for the user can provide convenience to the user. In this study, different profiles are presented to offer the user a simpler choice when choosing encryption algorithms.

These profiles are in three different types as "Quick, Performance, and Secure."

In previous studies, different file types have been evaluated according to various parameters, but a system to help the user selection has not been developed. The main contribution of this study is to develop an intelligent selection system to help the user instantly decide which algorithm should be used according to profiles and the file type to be encrypted. Additionally, three multi-criteria decision-making methods: FAHP, TOPSIS, and PROMETHEE are used for selection in a fuzzy environment and their performances are compared for usability.

In the second part of this study, encryption algorithms and their types will be mentioned. Fuzzy logic will be explained in Chapter 3. In Chapter 4, multi-criteria decision making and methods will be explained. Chapter 5 will discuss the development of an intelligent selection framework for using symmetric data encryption algorithms. Results are discussed in Chapter 6 followed by the conclusion in Chapter 7.

2 Encryption algorithms

The confidentiality of encryption techniques used is just as important as an encrypted message. Third parties would not be able to decrypt the message, even though they learn encryption methods if they do not know the required key to run these methods. Despite the risk of unlocking the function of encryption algorithms, security is increased with additional information called encryption key [14]. Two types of encryption are used in encryption: symmetric and asymmetric.

2.1 Symmetric encryption

In symmetric encryption; the message to be encrypted and transmitted is subjected to a series of processes by the encryption algorithm. During these operations, the message is encrypted with the same encryption key, also found on the recipient side. The recipient decrypts the message with the encryption key found in itself when returning the encrypted message to the original. So, symmetric-key cryptography algorithms use the same keys for encryption/decryption operations [17]. Symmetric key cryptography is shown in Fig. 1.

Although there are many symmetric encryption algorithms, the main algorithms for symmetric encryption are:

- Advanced encryption standard (AES)
- Data encryption standard (DES)
- Triple data encryption standard (3DES)
- Rivest Cipher (RC2)

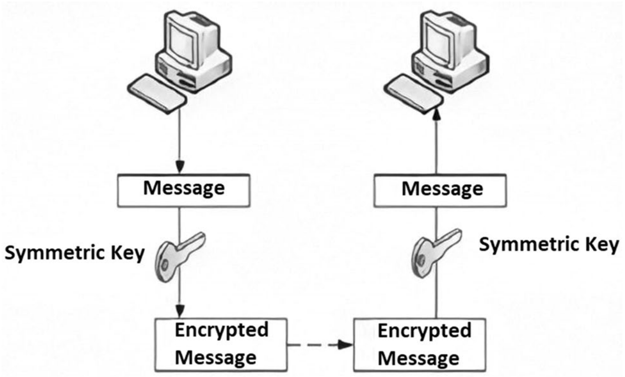


Fig. 1 Symmetric encryption [17]

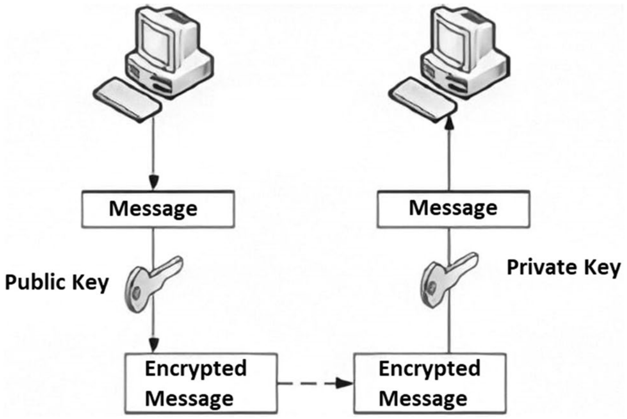


Fig. 2 Asymmetric encryption [17]

2.2 Asymmetric encryption

The encryption key used in asymmetric key cryptography is different for the sender and receiver. The key used for encrypting the message cannot be used, while the message is being decrypted. Therefore, security is high. For example, if the message encrypted by the 1st person is encrypted with the key A, the 2nd person can only decrypt the encrypted message with the key B. Similarly, message that the 2nd person encrypts with the key B can be decrypted to the 1st person with the key A. In this type of encryption algorithm, encryption–decryption keys are different [17]. Figure 2 shows the asymmetric encryption scheme. Basic asymmetric encryption algorithms are:

- Rivest–Shamir–Adleman (RSA)
- El Gamal
- Diffie–Hellman
- Digital signature algorithm (DSA)

3 Fuzzy logic

Fuzzy logic has emerged as a conclusion of the article published by Lotfi A. Zadeh [22]. In classical logic, membership values are only in the range of 0 and 1, while fuzzy logic uses intermediate values. Thus, more probability is included in the evaluation phase [23]. The basic element of fuzzy logic is the fuzzy set [24].

The usefulness of fuzzy sets is directly related to their ability to bring the appropriate membership function to different situations. The most commonly used membership functions in the literature are; triangular, trapezoidal, generalized bell-shaped, and Gaussian membership functions [25]. The triangular type of membership function is shown in Fig. 3.

The structure of the fuzzy decision-making system is given in Fig. 4 [26].

4 Multi-criteria decision making

When choosing alternatives to solve a decision problem, more than one criterion may be used to make a better decision. In this case, descriptive decision-making theory and models enable decision-makers to make effective decisions within certain areas [27]. The aim is to make a decision, not to optimize the behavior [28]. In such problems, the purpose of using MCDM methods is to provide an easy and quick decision-making process to decision-maker in cases where there are a large number of criteria and alternatives [29]. The MCDM methods used in this study are AHP, fuzzy AHP, TOPSIS, and PROMETHEE. They are described in the following subsections.

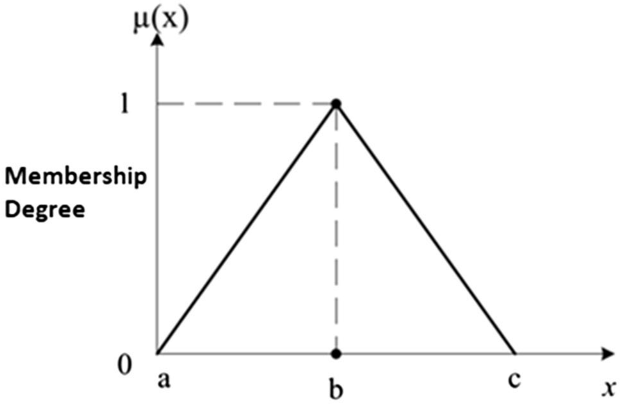


Fig. 3 Triangle membership function [25]

4.1 AHP and fuzzy AHP

The analytic hierarchy process (AHP) is used for decision making in the case of multiple criteria, multi-purpose, certainty, or uncertainty, where a large number of decision-makers can be found when selecting or sorting among multiple alternatives [30].

In daily life, expressing problems in qualitative and linguistic terms causes a relative approach to be exhibited [31]. So, for a mathematical question, one person can say it is "easy," for another, this question can be difficult. In this case, uncertainty arises [12]. Since AHP is not suited perfectly to the decision in case of uncertainty, fuzzy AHP (FAHP) is introduced by combining AHP with fuzzy logic [30].

4.2 TOPSIS

The technique for order preference by similarity to ideal solution (TOPSIS) method is one of the multi-criteria decision-making methods. It bases on Hwang and Yoon's research [32] and presented by Chen and Hwang [33]. In this method, it is necessary to compare the alternatives according to some criteria and between the minimum and maximum values that the criteria can take according to the ideal situation [34]. The solution process of the TOPSIS method consists of six basic steps [35]. These are;

- Step 1: Creating the decision matrix.
- Step 2: Creating the standard decision matrix.

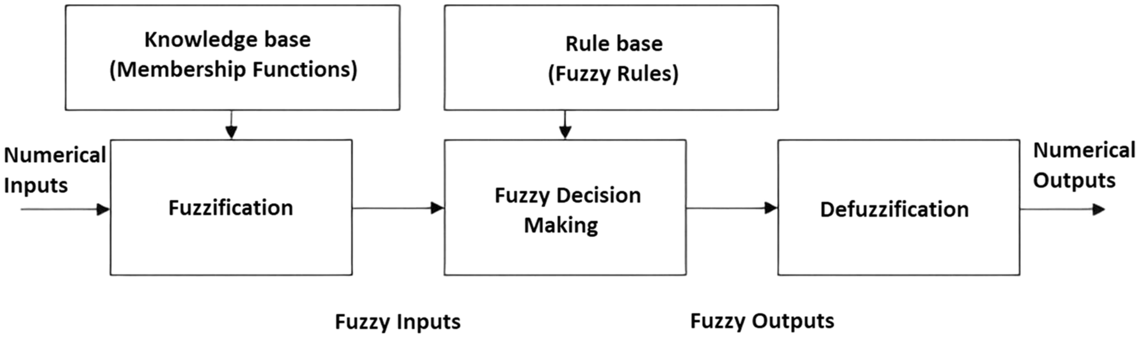


Fig. 4 Structure of the fuzzy decision-making system [26]

- Step 3: Creating the weighted standard decision matrix.
- Step 4: Creating ideal and negative ideal solutions.
- Step 5: Calculation of discrimination measure.
- Step 6: Calculating relative proximity to ideal solution.

4.3 PROMETHEE

The preference ranking organization method for enrichment evaluation (PROMETHEE) is a method developed for solving multi-criteria decision-making problems because of the difficulties in applying existing prioritization methods in the literature [36].

The geometrical analysis for interactive aid (GAIA) demonstration provides a simple explanation to the decision-maker by showing the PROMETHEE results graphically [37]. The decision-maker can make an easier and quicker evaluation by seeing the results of the problem over the GAIA geometric representation. Advantages of the PROMETHEE method are [38]:

- Direct use of data without comparisons,
- The classification accuracy according to each criterion is calculated automatically,
- Scaling can be done in the desired range, not in a fixed range,
- The problem can be visualized.

In the PROMETHEE method, positive (Phi+) and negative (Phi-) comparative values are determined for each alternative. The positive comparative values obtained indicate how superior the alternative selected is to other alternatives. Negative comparative values indicate how weak the alternative selected is to other alternatives [39]. Phi value must be determined to make a complete ranking among the alternatives [40]. Positive and negative comparative values are used to determine the Phi value. Phi formula is given in Eq. 1:

$$\text{Phi} = (\text{Phi}+) - (\text{Phi}-). \tag{1}$$

5 Development of intelligent selection system for symmetric encryption algorithms

The aim of this study to determine which encryption algorithm to use automatically in direction of the parameters determined according to the selected file type and intent of use. The flowchart of system is shown in Fig. 5.

According to Fig. 5, first, the file to be encrypted should be given to the program and the file type analysis should be done accordingly. In the next step, the criteria and alternatives to be used should be determined. Then, the data should be obtained in real time. Membership function and fuzzification should be provided at the next stage. The weights of criteria to be used afterward should be found by the FAHP method. In the next step, the FAHP, TOPSIS, and PROMETHEE methods should be used to rank the encryption algorithms appropriately per the obtained data. At the last stage, the user should be presented with the best encryption algorithm that suits the selected profile. In the following subsections, the steps in the system will be defined in detail.

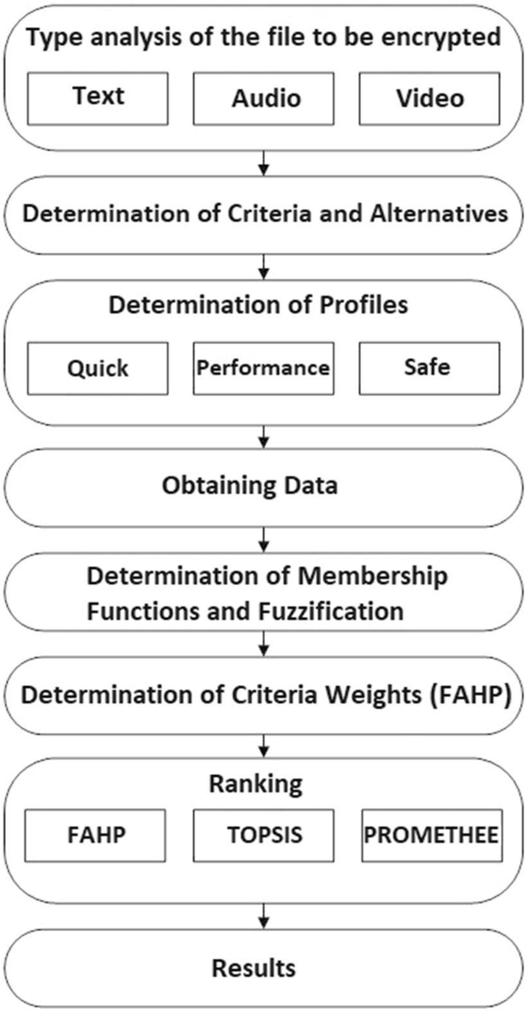

Type analysis of the file to be encrypted
Text
Audio
Video
Determination of Criteria and Alternatives
Determination of Profiles
Quick
Performance
Safe
Obtaining Data
Determination of Membership Functions and Fuzzification
Determination of Criteria Weights (FAHP)
Ranking
FAHP
TOPSIS
PROMETHEE
Results

Fig. 5 Flowchart of the system

5.1 Determination of criteria and alternatives

Criteria and alternatives to be used in the study are identified in this step. In the literature, Ciger [17] and Gunden [3] have measured the parameters "time" and "resource (RAM and CPU usage)." Accordingly, the criteria to be included in this study are given below:

1. *Time*: Encryption and decryption time of the given file in milliseconds (ms).
2. *Resource*: Measures the CPU and RAM usage during encryption and decryption by the in terms of average percentage.
3. *Privacy (Confidentiality)*: is the expression in bits of the encryption key length used during encryption.

For cryptography operations, six encryption algorithms are chosen. Four of them are stand alone, and two are hybrid algorithms. Selected algorithms are given below:

- AES
- 3DES
- RC2
- DES
- RC2 + DES
- AES + 3DES + RC2

Properties of the algorithms are given in Table 2.

Table 2 Properties of the algorithms

Algorithm number	Algorithms	Data block length (bit)	Key length	
			min (bit)	max (bit)
1	AES	128	128	256
2	3DES	64	128	192
3	RC2	64	40	128
4	DES	64	64	64
5	RC2 + DES	64	104	192
6	AES + 3DES + RC2	86	296	576

5.2 Determination of profiles

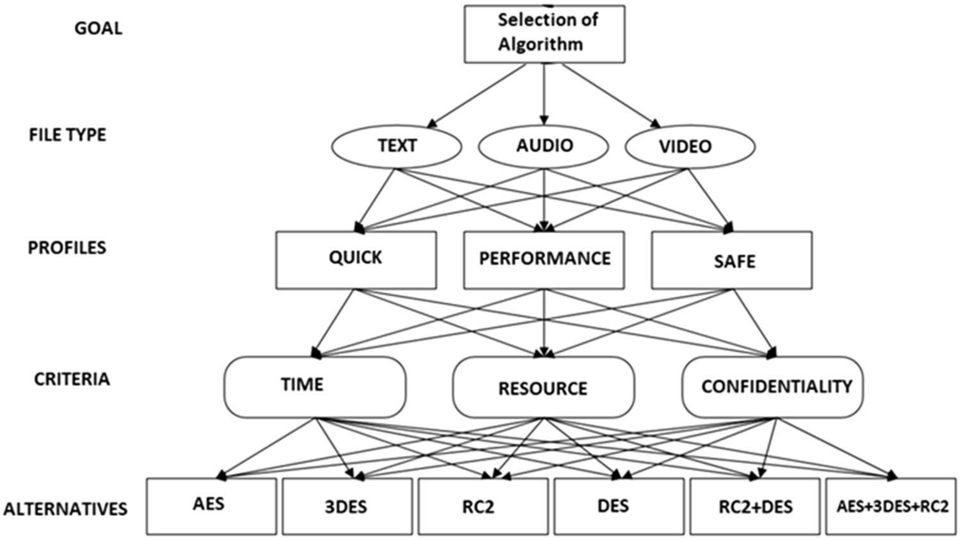
The goal of this study is to determine the most efficient encryption algorithm according to the purpose before encrypting the file and then let the users use the most efficient algorithm. The efficiency is a relative concept that varies according to profile. Although use minimal time is considered effective in one profile, a high degree of confidentiality in another profile can be regarded as effective. Three different profile options are presented to the user in this study. These profiles are "Quick," "Performance," and "Secure" and they are described in detail below.

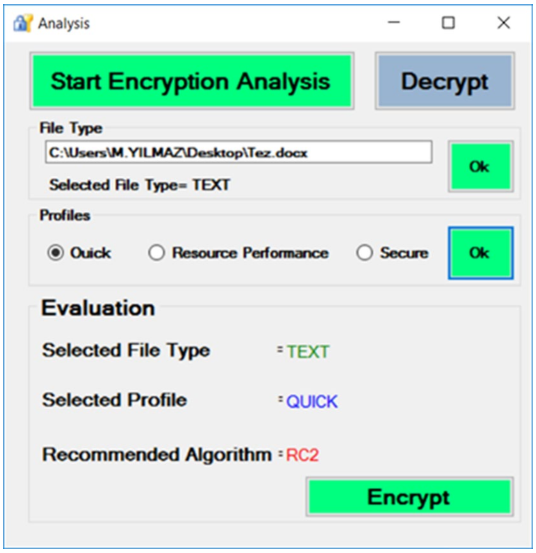
Profile-1 (Quick): In this profile, the user is given the option to find the algorithm that uses least amount of time during encryption and decryption. The importance order of the criteria in this profile; time, resources, and privacy. Although the determinant criterion in this regard seems to be the time, resource use also influences the result. The criterion that has less importance than the other two criteria is confidentiality.

Profile-2 (Performance): The purpose of this profile is to provide the algorithm that uses resources least during encryption and decryption. The order of importance for this profile is resource use, time, and privacy. Resource use is an important determinant. Therefore, time is an important measurement criterion for performance evaluation and it is one step ahead of confidentiality.

Profile-3 (Secure): This is the most determinant criterion for this profile. In this profile, the algorithm that uses the encryption key with the maximum bit length during encryption is preferred. Resource usage and time criteria are determinant after confidentiality. Here, the use of resources is more important than time.

Fig. 6 Hierarchical structure of the problem





File Type
C:\Users\M.YILMAZ\Desktop\Tez.docx
Selected File Type= TEXT

Profiles
● Quick ○ Resource Performance ○ Secure

Evaluation
Selected File Type =TEXT
Selected Profile =QUICK
Recommended Algorithm =RC2

Fig. 7 Screenshot of the developed program

Table 3 Means of parameters for text files

Algorithms	Time (ms)	Resource (%)	Privacy (bits)
AES	0.611	29.946	192
3DES	0.698	27.375	160
RC2	0.658	20.235	84
DES	0.747	25.227	64
RC2 + DES	0.816	29.586	148
AES + 3DES + RC2	0.88	31.347	436

The hierarchical diagram of the problem involving alternatives, criteria, profiles, and file types is shown in Fig. 6.

5.3 Data analysis

Parameters of each algorithm are obtained in real time via the program developed shown in Fig. 7. To find an average value in the parameter values, 250 samples for each file type, a total of 1500 samples are obtained. When the parameter data are being generated, each parameter is evaluated in two groups as encryption and decryption via the program. For example, the "time" parameter data are obtained in the first stage as the encoding period and the decoding period. CPU and RAM usages are also measured in the "Resource" parameter, and these are handled as the two groups mentioned above (encryption–decryption). After all the parameters are obtained in this way, these groups are merged within themselves and three types of parameters have emerged as "Time, Resource and Privacy." Measurement units for parameters are milliseconds (ms) for "Time," percent (%) for "Resource," bits for "Privacy."

Table 4 Means of parameters for audio files

Algorithms	Time (ms)	Resource (%)	Privacy (bits)
AES	0.756	31.798	192
3DES	0.939	25.511	160
RC2	0.895	27.331	84
DES	1.176	28.606	64
RC2 + DES	1.298	30.749	148
AES + 3DES + RC2	1.399	33.236	436

Table 5 Means of parameters for video files

Algorithms	Time (ms)	Resource (%)	Privacy (bits)
AES	2.363	31.273	192
3DES	5.438	27.659	160
RC2	4.345	28.565	84
DES	5.377	26.863	64
RC2 + DES	8.164	31.457	148
AES + 3DES + RC2	9.511	32.114	436

The data obtained with the software are given in Tables 3, 4, and 5. These values are measured in real time for all file types. These values may vary according to the characteristics of the computer used. When these evaluations are made, a computer with Intel Core i7 2.4 GHz Processor, 8GB Memory, and 64-Bit Operating System is used.

5.4 Determination of membership functions and fuzzification

The triangle-type membership function in Fig. 8 is used to convert the obtained data to fuzzy values. The fuzzy values that belong to the parameters for three file types are given in Tables 6, 7, and 8.

5.5 Determination of criteria weights

The process to be performed at this step is to determine the criterion weights to be used for each user profile. For FAHP, triangular fuzzy numbers are used. The linguistic scale values and the corresponding triangular fuzzy values are presented in Table 9.

The fuzzy comparison matrix of the criteria set for profiles is created by the expert. The expert-generated fuzzy linguistic comparison matrix for profiles is given in Table 10. Fuzzy pairwise comparison matrix

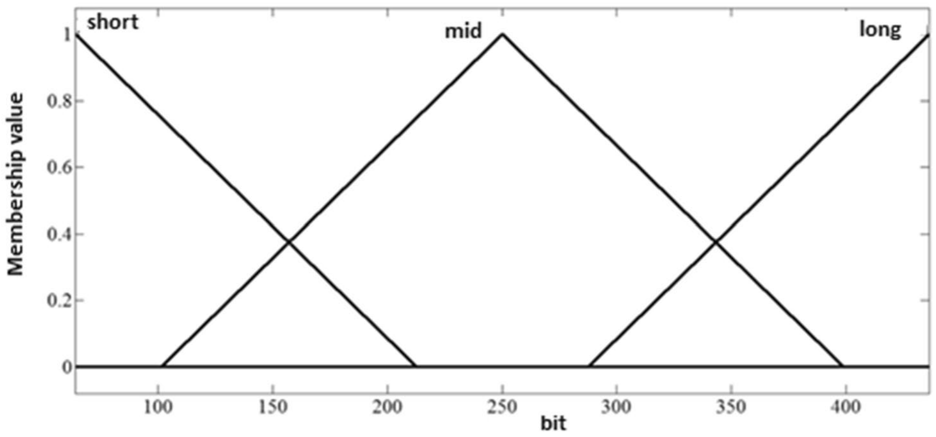


Fig. 8 Triangle-type membership function

Table 6 Fuzzy values of parameters for text files

Algorithms	Time	Resource	Privacy
AES	0.87	0.214	0.477
3DES	0.534	0.484	0.419
RC2	0.684	0.87	0.132
DES	0.5	0.5	0.13
RC2 + DES	0.399	0.287	0.386
AES + 3DES + RC2	0.13	0.131	0.87

Table 7 Fuzzy values of parameters for audio files

Algorithms	Time	Resource	Privacy
AES	0.87	0.214	0.477
3DES	0.534	0.484	0.419
RC2	0.684	0.87	0.132
DES	0.5	0.5	0.13
RC2 + DES	0.399	0.287	0.386
AES + 3DES + RC2	0.13	0.131	0.87

Table 8 Fuzzy values of parameters for video files

Algorithms	Time	Resource	Privacy
AES	0.87	0.291	0.477
3DES	0.5	0.726	0.419
RC2	0.565	0.533	0.132
DES	0.5	0.87	0.13
RC2 + DES	0.338	0.213	0.386
AES + 3DES + RC2	0.13	0.13	0.87

corresponding to linguistic values shown in Table 9 is also given in Table 11.

All criteria weight values calculated for profiles according to the FAHP method are given in Table 12.

5.6 Ranking

Taking advantage of the data in Table 2, the ranking generated by the expert is determined for each profile separately in Table 13.

The most important determining criterion for Profile-1 is speed. From the data in Table 2, the data block and key length are low, so the speed bench has come to the forefront according to expert opinion. Also, 3DES encryption is 3 times slower than DES encryption because it is the result of combining the DES cipher 3 times [3].

The determinant criterion for Profile-2 is "Performance." For the performance criterion, from the data in Table 2; data block and key length are low and the speed parameter in Profile-1 has been evaluated as a parameter directly affecting performance by the expert.

The determinant criterion for Profile-3 is "security." For the security criterion, when examining the data in Table 2, the algorithm with the highest key length is considered by the expert to be the safest. As a result of these data, the ranking in Table 13 for Profile-1, Profile-2, Profile-3 is found appropriate by the expert.

Three different methods have been used for the ranking process to be used in the evaluation. These are FAHP, TOPSIS, and PROMETHEE methods.

6 Results and discussion

It is discussed in this section how to sort the algorithms to be used for "Profile-1, Profile-2, and Profile-3" to be presented to the user. The sorting method that gives the closest result to the order created by the expert has come to the forefront.

Table 14 shows the rank correlations between the orders of expert and the methods. Ranks of the algorithms for the FAHP and TOPSIS methods are the same, but it is

Table 9 Linguistic scaling values

Linguistic scale	Explanation	Triangular values	Reverse triangular values	Reverse linguistic scale
Equally important (EI)	Both alternatives have equal priority	(1, 1, 1)	(1, 1, 1)	REI
Less important (LI)	One alternative is slightly better than the other	(1, 3, 5)	(1/5, 1/3, 1)	RLI
Important enough (IE)	One alternative is better than the other	(3, 5, 7)	(1/7, 1/5, 1/3)	RIE
Very important (VI)	One alternative is much better than the other	(5, 7, 9)	(1/9, 1/7, 1/5)	RVI
Absolute important (AI)	One alternative is very much better than the other	(7, 9, 11)	(1/11, 1/9, 1/7)	RAI

Table 10 Fuzzy comparison matrix for three profiles

Profiles	Time	Resource	Privacy
Profile-1			
Time	EI	LI	IE
Resource	RLI	EI	LI
Privacy	RIE	RLI	EI
Profile-2			
Time	EI	RLI	LI
Resource	LI	EI	IE
Privacy	RLI	RIE	EI
Profile-3			
Time	EI	RLI	RLI
Resource	LI	EI	RLI
Privacy	LI	LI	EI

Table 11 Fuzzy pairwise comparison matrix for three profiles

Profiles	Time	Resource	Privacy
Profile-1			
Time	(1, 1, 1)	(1, 3, 5)	(3, 5, 7)
Resource	(1/5, 1/3, 1)	(1, 1, 1)	(1, 3, 5)
Privacy	(1/7, 1/5, 1/3)	(1/5, 1/3, 1)	(1, 1, 1)
Profile-2			
Time	(1, 1, 1)	(1/5, 1/3, 1)	(1, 3, 5)
Resource	(1, 3, 5)	(1, 1, 1)	(3, 5, 7)
Privacy	(1/5, 1/3, 1)	(1/7, 1/5, 1/3)	(1, 1, 1)
Profile-3			
Time	(1, 1, 1)	(1/5, 1/3, 1)	(1/5, 1/3, 1)
Resource	(1, 3, 5)	(1, 1, 1)	(1/5, 1/3, 1)
Privacy	(1, 3, 5)	(1, 3, 5)	(1, 1, 1)

Table 12 Criteria weights

Profiles	Time	Resource	Privacy
Profile-1	0.63291	0.32304	0.04406
Profile-2	0.32304	0.63291	0.04406
Profile-3	0.17987	0.34052	0.47961

Table 13 Algorithm preference order by expert

Rank	Expert rank		
	Profile-1	Profile-2	Profile-3
1	3	3	6
2	4	4	1
3	2	2	2
4	1	1	5
5	5	5	3
6	6	6	4

Table 14 Rank correlations between orders of expert and the methods

File type	FAHP	TOPSIS	PROMETHEE
Profile-1			
Text	0.48	0.48	1.00
Audio	0.48	0.48	0.82
Video	0.77	0.77	0.82
Profile-2			
Text	0.77	0.77	1.00
Audio	0.65	0.65	0.82
Video	0.82	0.82	0.82
Profile-3			
Text	0.31	0.31	1.00
Audio	0.08	0.08	1.00
Video	− 0.25	− 0.25	1.00

different for the PROMETHEE method. In Table 14, when three different methods are considered separately, PROMETHEE is the best ranking method that gives the closest result to the expert's order.

When "Correlation" between FAHP, TOPSIS, PROMETHEE methods, and expert rankings is examined in Table 14, the highest correlation is obtained by the PROMETHEE method. The ranking method to be recommended to the user in the direction of this result is the PROMETHEE method.

The Spearman rank correlation test [41] in Eq. 2 is used to measure the consistency of the results values in Table 14.

$$\rho = 1 - \frac{6\sum d_i^2}{n\left(n^2 - 1\right)} \tag{2}$$

where ρ is the Spearman rank correlation coefficient, d_i: the difference between the expected rank value and the observed rank value, n: the number of alternatives.

The hypotheses for the test are as follows:

H_0: There is no significant correlation between the two rankings.

H_1: There is a significant correlation between the two rankings.

Then, using Eq. 3, t values according to Student's t-distribution and corresponding probability values (p) (two-tailed) from T table are calculated.

$$t = \frac{\rho}{\sqrt{\left(1 - \rho^2\right)/(n-2)}}. \tag{3}$$

Since the p values calculated for the correlation values found for FAHP and TOPSIS methods are $p > 0.05$, the H_0 hypothesis cannot be rejected, so there is no significant correlation for these methods. Since p values calculated for the correlation values found for the PROMETHEE method are $p < 0.05$, it shows that there is a significant correlation by rejecting the H_0 hypothesis.

Selected methods for profiles by the PROMETHEE method are given in Table 15. According to profiles, if three file types are examined together:

Profile-1: "RC2" algorithm for text file type, "3DES" algorithm for audio file type, and "DES" algorithm for the video file type are selected in the first order. The desired feature on this profile is that the operation should be fast. Therefore, in this profile, the time and use resource parameters are more influential.

Profile-2: In this profile, the desired priority is performance. Therefore, resource use and time parameters are ultimately determinants. The "RC2" for the text file type, "3DES" for the audio type, and the "DES" algorithm for the video type are in the first order. So, a different algorithm is in the foreground for each file type.

Profile-3: The desired criterion is security in this profile. The "AES + 3DES + RC2" algorithm is the first in the text, audio, and video file types. The primary criterion is privacy for this profile; the second is resource use. The selected algorithm for three file types is "AES + 3DES + RC2."

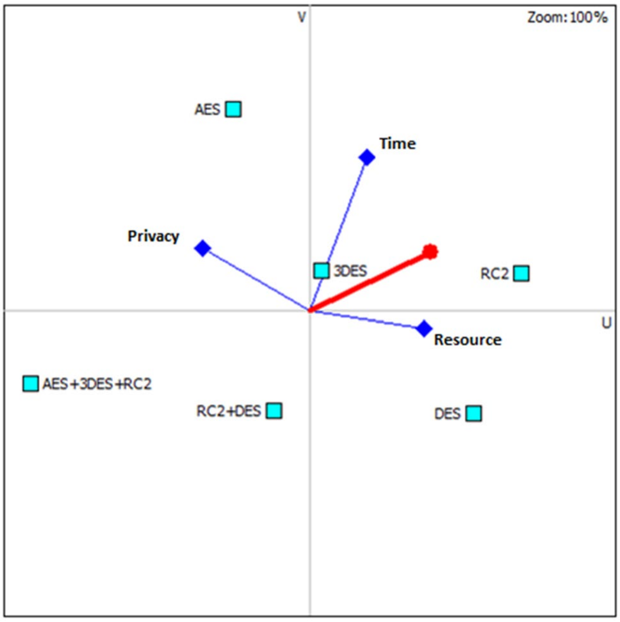


Fig. 9 GAIA of Profile-2 for text file type

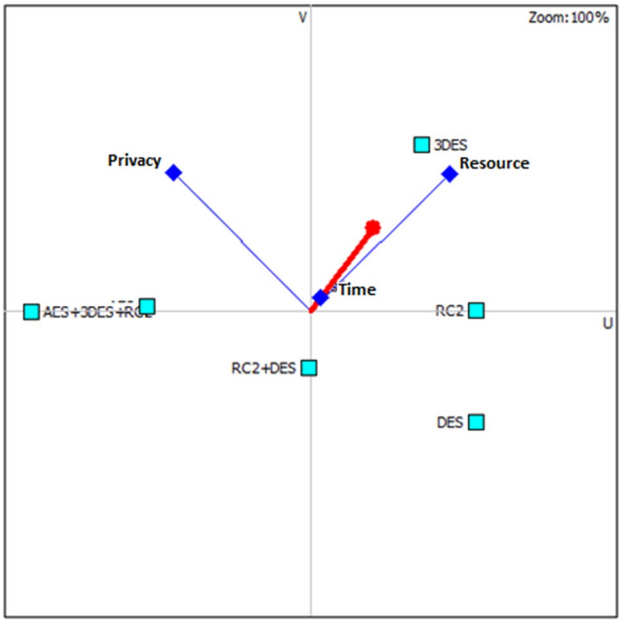


Fig. 10 GAIA of Profile-1 for audio file type

Some GAIA demonstrations are given in Figs. 9, 10, and 11. The important thing in the graph is not how far alternatives are from the axis of criteria, but how far the alternatives move in the axis direction. When the graph in Fig. 9 is examined, the "RC2" algorithm, which is in the same direction as the resource and time criterion axes, is the most efficient alternative. The most inefficient alternative is the "AES + 3DES + RC2" algorithm, which is the opposite of these criterion axes. Figure 10 shows the PROMETHEE GAIA plane graph of Profile-1 for the audio file type. According to the graph, the "3DES" algorithm is the most efficient alternative. The "AES + 3DES + RC2"

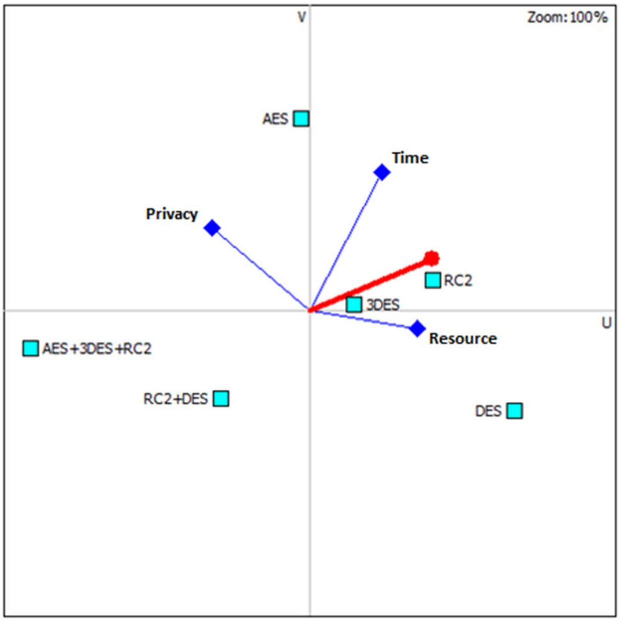


Fig. 11 GAIA of Profile-2 for video file type

Table 15 Selected methods for profiles by PROMETHEE method

File type	Profile-1	Profile-2	Profile-3
Text	RC2	RC2	AES + 3DES + RC2
Audio	3DES	3DES	AES + 3DES + RC2
Video	DES	DES	AES + 3DES + RC2

algorithm is the most inefficient alternative because it is in the opposite direction to the criterion axis. According to Fig. 11, the most efficient alternative is the "DES" algorithm for Profile-2 and video file type.

7 Conclusion

In daily life, users can encrypt each file with each encryption algorithm. In this study, six encryption algorithms selected in the profile direction determined according to file types are evaluated. Assessing a profile based on only one criterion is not always advantageous. When different criteria are included in the consideration, different results can be achieved. In this study, three different profiles are developed to include the criteria in different priorities. By applying the criteria to the different priority orders in the profiles, better results are obtained in the evaluations. While the orders of FAHP and TOPSIS methods are similar in the evaluation methods, the PROMETHEE method is different. However, when compared with expert ranking, the best method of giving results is the PROMETHEE method. The PROMETHEE approach has come to the fore since it is more flexible than other methods.

In the developed intelligent selection system, the criteria weights are calculated according to the selected profile. And the encryption algorithms are compared according to the criteria weights. Then, the most suitable algorithm is presented to the user for the selected profile. In other words, thanks to the system developed by performance evaluation, criteria such as time, resource, and security can be used efficiently. In future studies, different file types and profiles can be included in the system according to user requirements. Moreover, the system's stability can be further strengthened by using different methods and approaches to evaluation.

Compliance with ethical standards

Conflict of interest The authors declare that they have no conflict of interest.

References

1. Yilmaz M, Balli S (2016) Performance evaluation of data encryption algorithms using fuzzy AHP. In: International conference on computer science and engineering. Tekirdag, Turkey, pp 20–23
2. Hsiao F-H (2018) Chaotic synchronization cryptosystems combined with RSA encryption algorithm. Fuzzy Sets Syst 342:109–137
3. Umit G (2010) Performance analysis of encryption algorithms. Master thesis, Sakarya University, Turkey
4. Kodaz H, Botsali FM (2010) Comparison of symmetric and asymmetric encryption algorithms. J Selcuk-Technic 9(1):10–23
5. Sun L, Ma J, Zhang Y, Dong H, Hussain FK (2016) Cloud-FuSeR: fuzzy ontology and MCDM based cloud service selection. Future Gener Comput Syst 57:42–45
6. Rajak M, Shaw K (2019) Evaluation and selection of mobile health (mHealth) applications using AHP and fuzzy TOPSIS. Technol Soc 101186:10–23
7. Lo C-C, Chen D-Y, Tsai C-F, Chao K-M (2010) Evaluation and selection of mobile health (mHealth) applications using AHP and fuzzy TOPSIS. In: 24th International conference on advanced information networking and applications workshops, Perth, Australia, pp 367–372
8. Agrawal A, Seh AH, Baz A, Alhakami H, Alhakami W, Baz M, Kumar R, Khan RA (2020) Software security estimation using the hybrid fuzzy ANP-TOPSIS approach: design tactics perspective. Symmetry 12(4):598
9. Karim R, Ding C, Chi C-H (2011) An enhanced PROMETHEE model for QoS-based web service selection. In: IEEE International Conference on Services Computing, Washington, USA, pp 536–543
10. Çolak M, Kaya I, Qzkan B, Budak A, Karaşan A (2020) A multi-criteria evaluation model based on hesitant fuzzy sets for blockchain technology in supply chain management. J Intell Fuzzy Syst 38(1):935–946
11. Senvar O, Tuzkaya G, Kahraman C (2014) A multi-criteria evaluation model based on hesitant fuzzy sets for blockchain

technology in supply chain management. In: Supply chain management under fuzziness. Studies in fuzziness and soft computing, vol 313. Springer, Berlin, pp 21–34

12. Balli S, Tuker M (2018) A fuzzy multi-criteria decision analysis approach for the evaluation of the network service providers in Turkey. Intell Autom Soft Comput 24(4):693–699
13. Guvenoglu E (2006) Image encryption algorithms and performance analysis. Master thesis, Trakya University, Turkey
14. Yerlikaya T (2006) The analysis of new crypto algorithms. PhD thesis, Trakya University, Turkey
15. Elminaam DSA, Kader HMA, Hadhoud MM (2010) Evaluating the performance of symmetric encryption algorithms. Int J Netw Secur 10(3):213–219
16. Kumar N, Thakur J, Kalia A (2011) Performance analysis of symmetric key cryptography algorithms: DES, AES and BLOWFISH. Int J Eng Sci 4:28–37
17. Ciger I (2012) Data encryption systems and performance analysis. Master thesis, Istanbul University, Turkey
18. Rajesh S, Paul V, Menon VG, Khosravi MR (2019) A secure and efficient lightweight symmetric encryption scheme for transfer of text files between embedded IoT devices. Symmetry 11(2):293
19. Al-Asli M, Elrabaa MES, Abu-Amara M (2018) FPGA-based symmetric re-encryption scheme to secure data processing for cloud-integrated internet of things. IEEE Internet Things J 6(1):446–457
20. Guo C, Xue C, Yingmo J, Zhangjie F, Mingchu L, Bin F (2017) Dynamic multi-phrase ranked search over encrypted data with symmetric searchable encryption. IEEE Trans Serv Comput. https://doi.org/10.1109/TSC.2017.2768045
21. Taha MB, Ould-Slimane H, Talhi C (2020) Smart offloading technique for CP-ABE encryption schemes in constrained devices. SN Appl Sci 2(2):274
22. Zadeh L (1965) Fuzzy sets. Inf Control 8:338–353
23. Baykal N, Beyan T (2004) Fuzzy logic expert systems and controllers. Bicaklar Publishing, Ankara
24. Altas I, Logic F (1999) Concept of fuzziness. Enerj Elektr Elektromekanik-3e 62:80–85
25. Yilmaz A (2015) Cancer risk analysis with using neuro-fuzzy logic model. PhD Thesis, Sakarya University, Turkey
26. Yilmaz M (2017) An intelligent selection system development for the use of symmetric encryption algorithms. Master Thesis, Mugla Sitki Kocman University, Turkey
27. Balli S, Korukoglu S (2014) Development of a fuzzy decision support framework for complex multi-attribute decision problems: a case study for the selection of skilful basketball players. Expert Syst 31(1):56–69
28. Zimmermann H-J (1987) Fuzzy sets decision making and expert systems. Kluwer Academic Publishers, Boston
29. Balli S (2010) Design and implementation of hybrid intelligent decision support systems. PhD thesis, Ege University, Turkey
30. Goksu A (2008) Fuzzy analytic hierarchy process and its application of university preference ranking. PhD thesis, Suleyman Demirel University, Turkey
31. Balli S, Korukoglu S (2009) Operating system selection using fuzzy AHP and TOPSIS methods. Math Comput Appl 14(2):119–130
32. Hwang C-L, Yoon K (1981) Multiple attribute decision making. Lecture notes in economics and mathematical systems. Springer, Berlin
33. Hwang C-L, Chen S-J (1992) Fuzzy multiple attribute decision making. Springer, New York
34. Yurdakul M, Ic YT (2003) An illustrative study aimed to measure and rank performance of Turkish automotive companies using TOPSIS. J Fac Eng Archit Gazi Univ 18(1):1–18
35. Demireli E (2010) TOPSIS multicriteria decision making method: an examination on state owned commercial banks in Turkey. J Entrep Dev 5(1):101–112
36. Dagdeviren M, Eraslan E (2008) Supplier selection using promethee sequencing method. J Fac Eng Archit Gazi Univ 23(1):69–75
37. Genc T (2013) PROMETHEE method and GAIA plane. Afyon Kocatepe Univ Fac Econ Admin Sci J 15(1):133–154
38. Balli S, Karasulu B, Korukoglu S (2007) An application of fuzzy promethee method for selecting optimal car problem. Dokuz Eylul Univ Fac Econ Adm Sci J 22(1):139–147
39. Sakarya S, Aytekin S (2013) Measurement of the relationship between deposit banks performance with stock returns in ISE: an application with PROMETHEE multi-criteria decision making method. Int J Alanya Fac Bus 5(2):99–109
40. Araz C, Ozfirat PM, Ozkarahan I (2007) An integrated multicriteria decision-making methodology for outsourcing management. Comput Oper Res 34(12):3738–3756
41. Kendall MG, Gibbons JD (1990) Rank correlation methods. Edward Arnold Publishers, London