RANKING CRITERIA OF ENTERPRISE INFORMATION SECURITY ARCHITECTURE USING FUZZY TOPSIS

Farzaneh Sadat Jalayer, Akbar Nabiollahi*

Faculty of Computer Engineering, Najafabad Branch, Islamic Azad University,
Najafabad, Iran

ABSTRACT

Information security against hacking, altering, corrupting, and divulging data is vital and inevitable and it requires an effective management in every organization. Some of the upcoming challenges can be the study of available frameworks in Enterprise Information Security Architecture (EISA) as well as criteria extraction in this field. In this study a method has been adopted in order to extract and categorize important and effective criteria in the field of information security by studying the major dimensions of EISA including standards, policies and procedures, organization infrastructure, user awareness and training, security base lines, risk assessment and compliance. Gartner's framework has been applied as a fundamental model to categorize the criteria. To assess the proposed model, a questionnaire was prepared and a group of EISA professionals completed it. The Fuzzy TOPSIS was used to quantify the data and prioritize criteria. It could be concluded that the database and database security criteria, inner software security, electronic exchange security and supervising malicious software can be high priorities.

KEYWORDS

Enterprise Information Security Architecture (EISA), Information Security Architecture's Criteria, Categorizing Criteria, Fuzzy TOPSIS

1. INTRODUCTION

Information security is a major challenge of enterprises so that design and development of a secure environment in modern organizations is a vital issue. When designing and developing an enterprise secure model, it is essential to have a thorough knowledge of different layers and criteria on information security architecture. Besides, knowledge on consequences of a system which is bugged and the most important security threats which could endanger an organization [1]. Some of these negative consequences include: income reduction and charge increase, tarnishing their credit and reputation, losing important database, process disorder, taking legal action against the organization due to lack of clients' trust, and lack of investors' trust [2].

1.1. ENTERPRISE INFORMATION SECURITY ARCHITECTURE (EISA)

Enterprise Information Security Architecture is the practice of applying a comprehensive and careful method for describing a current and/or future structure and behavior for an organization's security processes, information security systems, personnel and organizational sub-units, so that they align with the organization's main goals and strategic direction [3]. Although often

DOI:10.5121/ijcsit.2016.8504

associated strictly with information security technology, it relates more broadly to the security practice to optimize business in which it addresses business

1.2. INFORMATION SECURITIES POLICIES POSITIONING

Enterprise information security's activities and different mechanisms are placed in Figure 1. As it can be seen, policy is located on top of information security pyramid, which is derived from strategies [3]. Based on policies, standards have been defined to ensure information security specified in the basic policy. Then, implementing the process and guidelines has been identified. Having documented the organization's policies and standards, the architecture process then flows down into the specific procedure and actions to follow the security standards. Here the discrete information technology components such as software and hardware application are used to secure the data. Finally theses security mechanisms are set up in a real environment in the organization [3].

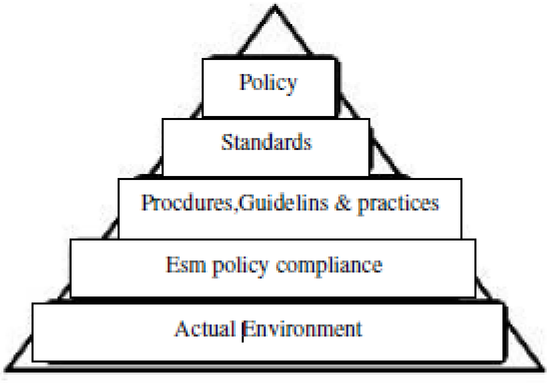


Figure 1. The rank of information security policies [3]

The importance and position of information security in enterprise architecture and enterprise information security architecture (EISA) are on top priority and importance for all organization in terms of intra-organizational and extra-organizational view [5]. In this study, important enterprise information security architecture criteria have been identified, extracted and categorized by reviewing the relevant national and international literature study. Fuzzy TOPSIS has been used to present a model in prioritizing enterprise information security architecture's criteria. The importance of the basic criterion has been realized as well. The result of the present study could be worthwhile for managers and presidents of organizations to formulate powerful secure policies and implement them to reduce the intra and inter threats toward their organization by considering the priorities.

2. REVIEW OF LITERATURE

Enterprise information security architecture was first formally presented by Gartner in his paper called "Incorporating Security into the Enterprise Architecture Process" in 2006[4]. The suggested framework was based on Zachman's architecture framework including 3 common levels of: Conceptual, Logical and Physical/implementation.

Jan Killmeyer in his book [5] "Information Security Architecture, An Integrated Approach to Security in Organization" provided five essential components to an effective architect [5]. Those are:

- Organization and Infrastructure
- Policies, Standards, and Procedures
- Baselines and risk assessments
- Users' Awareness and Training programs
- Compliance

Pulkkine and others in their article [6] "Managing information security in a business network of machinery maintenance services business - Enterprise architecture as a coordination tool" have illustrated that privacy, information security, and security policies are a roadmap for approaching integrated security management solutions in a business network of partners with heterogeneous information and communication technologies (ICT) [6]. Enterprise architecture (EA) is suggested as a means for comprehensive and coordinated planning and management of corporate ICT and the security infrastructure.

Shariati in the article [7] titled, *"Enterprise information security, a review of architectures and frameworks from interoperability perspective "*has proposed that enterprise information security architecture has been presented with the aim of combining security with enterprise architecture process, and interaction in enterprise information security framework is considered as an enterprise architecture quality which develops a close relation with information security and it can affect adversely and/or deeply [7].

Chetty and others in their article [8] titled "Towards an Information Security Framework For Service-oriented Architecture" has stated that Service-oriented architectures support distributed heterogeneous environments where business transactions occur among loosely connected services [8]. It is challenging to create a secure infrastructure for different environment. At the present time, there are currently various approaches to ensure information security, each with its own set of pros and cons. Organizations can also adopt vendor-based information security frameworks to assist them in implementing adequate information security controls. Information security components for a service-oriented architecture include a collection of developed service-oriented architecture components [8].

It was in 2011 when Roedig in his article [9] titled "Security engineering with patterns" stated that security is required by demand. As a result, system security is deeply affected by human factors in the following ways:

A. Security engineering conducted by in-experts
B. Solution to problems
C. Integrity and dependency infrastructure
D. time dependency

Zandi and others in 2012 in his article [10] titled "A fuzzy group multi-criteria enterprise architecture framework selection model" proposed that enterprise architecture is a collection of models and products which can be used to describe the organization in terms of business and information systems [10]. This unlimited number of models cannot be exploited without a proper infrastructure.

In 2013, Zafar and others in their article [11] titled "Human resource information systems: Information security concerns" stated that to yield much more illuminating results about human resources information systems (HRIS), as there could not be found a wide variety of research in this field, future studies could focus on electronic human resources, system security [11]. Sohrabi Safa and others in the article [12] titled "Information security conscious care behavior formation in organizations" showed that the Internet could be considered as a basic commodity, like electricity, without which many businesses simply cannot operate [12]. However, information security for both private and business aspects is important.

"Effects of virtualization on information security" is an article written by Li and others [13] in which it is shown that essential assistance to save energy and resources and also to simplify the required information management is provided by virtualization [13]. The information security issues have increasingly become a serious concern, though. In an article [14] carried out by Fezlida and others titled "Information Security: Risk, Governance and Implementation" reviewed the information security and stated that it has a key role in IT Governance (ITG) confidentiality, integrity, and availability of information [14].

3. RESEARCH METHOD, DATA COLLECTION AND ANALYSIS

Information security policies in EISA are a top priority for all organizations in terms of intra and inter organizational point of view. Killmeyer [14] in his book "Information Security Architecture, An Integrated Approach to Security in Organization" has already mentioned that information security architecture has been ignored in enterprise architecture. On the other hand, EISA owns some criteria which require prioritizing and evaluating by which the most important and essential criteria, effective on information security, can be recognized to enable the presidents and enterprise security architects to protect the organizations against data threats, corruption, perils and hacking. In this study, as a result, the tremendous challenge, recognizing its major dimensions, in EISA has been defeated by reviewing the related literature, extracting effective criteria, opting for a proper method of criteria prioritizing. Moreover, all related literature in EISA, compiled security standards to cover information security, and EISA's methodologies to be considered as specific architecture infrastructure have been reviewed in terms of intra and inter organizational point of view. With the assistance of literature review EISA's criteria have been identified and prioritized based on experts' idea and a conceptual research model has been presented. A questionnaire has been answered by a group of information security experts, who were IT or IS bachelor holder and gained a 5-year practical experience in information security, to prioritize the criteria. The data has been processed and gotten priority by running Fuzzy TOSIS. Based on the obtained result a research conceptual model has been completed and presented as EISAM which is summarized in Figure 2.

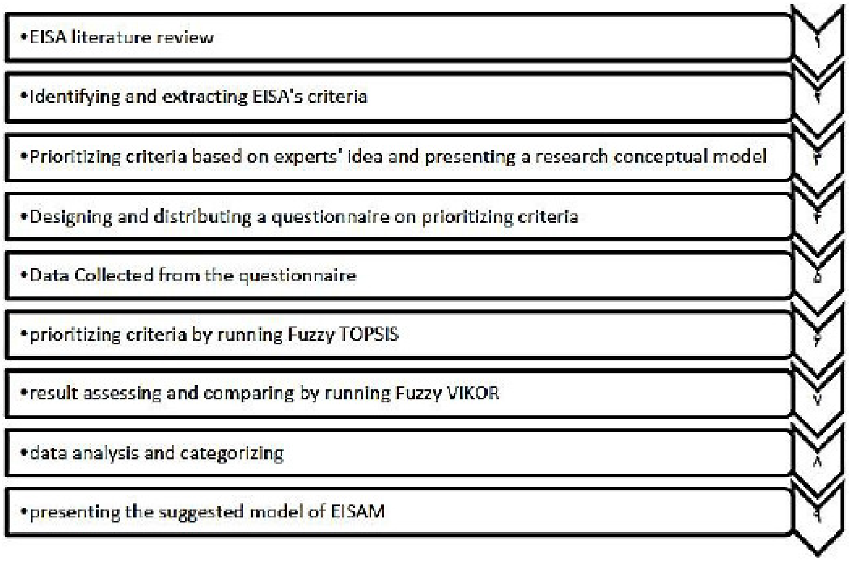

•EISA literature review
۱
•Identifying and extracting EISA's criteria
۲
•Prioritizing criteria based on experts' idea and presenting a research conceptual model
۳
•Designing and distributing a questionnaire on prioritizing criteria
۴
•Data Collected from the questionnaire
۵
•prioritizing criteria by running Fuzzy TOPSIS
۶
•result assessing and comparing by running Fuzzy VIKOR
۷
•data analysis and categorizing
۸
•presenting the suggested model of EISAM
۹

Figure 2. Research Process

On the very first step of the research, dimensions of enterprise information security architecture have been identified and the following major and effective criteria on information security have been extracted:

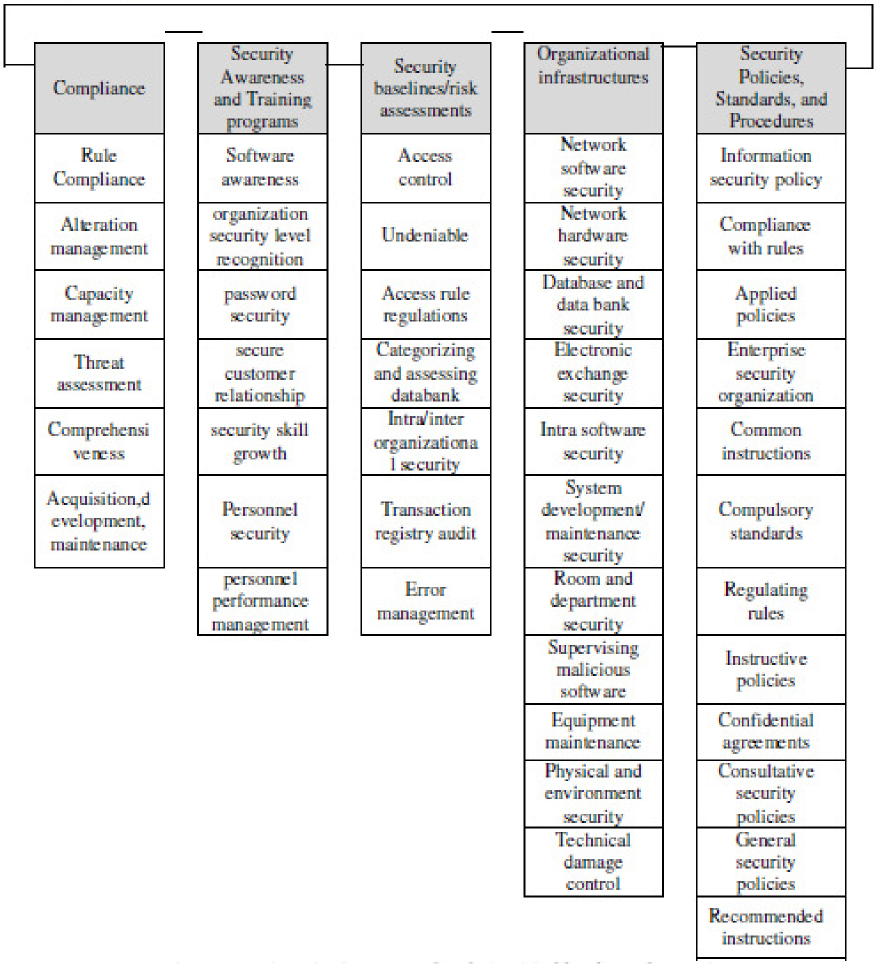

Compliance
Rule Compliance
Alteration management
Capacity management
Threat assessment
Comprehensi veness
Acquisition,d evelopment, maintenance
Security Awareness and Training programs
Software awareness
organization security level recognition
password security
secure customer relationship
security skill growth
Personnel security
personnel performance management
Security baselines/risk assessments
Access control
Undeniable
Access rule regulations
Categorizing and assessing databank
Intra/inter organizationa l security
Transaction registry audit
Error management
Organizational infrastructures
Network software security
Network hardware security
Database and data bank security
Electronic exchange security
Intra software security
System development/ maintenance security
Room and department security
Supervising malicious software
Equipment maintenance
Physical and environment security
Technical damage control
Security Policies, Standards, and Procedures
Information security policy
Compliance with rules
Applied policies
Enterprise security organization
Common instructions
Compulsory standards
Regulating rules
Instructive policies
Confidential agreements
Consultative security policies
General security policies
Recommended instructions

Figure 3. EISA criteria extracted and classified by the authors[15]

3.1. POPULATION AND SAMPLE

The population of this study includes a group of information security experts, who were bachelor holder in information security and gained a 5-year practical experience in row, to prioritize the criteria. As Fuzzy TOPSIS has been applied in order to quantify the criteria. So they could be prioritized. Questioning 15 experts in Fuzzy TOPSIS was endorsed academically and financially (a reference to 16-18 was made). 15 experts have been chosen, accordingly incompatibility level will not increase and it will facilitate the matrix comparisons. On the other hand, this number is adequate to conduct the study and lead the researcher to find the answer.

3.2. WHY FUZZY TOPSIS?

There can be found several methods to compare and prioritize different alternatives and to choose the best one among all in academic contexts; however concerning the present research's aim the followings could be used: Fuzzy Delphi [19], Fuzzy TOPSIS [20], Analytical Hierarchy Process (AHP) and Fuzzy TOPSIS [21], Fuzzy VIKOR [22]. Comparing the given techniques for prioritizing, quantifying, Fuzzy TOPSIS has been selected as the best method among all, as it facilitates extracting prioritized criteria from an individual decision-maker matrix and supporting the hierarchy process and the enormous number of criteria, as well as confronting ambiguity. Fuzzy VIKOR was used to assess the output of Fuzzy TOPSIS. Considering the circumstances in this study, as one security choice has been used, so a unit of measurement is not required. Moreover; the three-point Likert scale has been used to collect that data, so triangular fuzzy number could be reached and quantitative information gained from the questionnaire could be inverted to qualitative, definite and understandable information useful for Fuzzy TOPSIS.

3.3. Fuzzy TOPSIS Method

The word TOPSIS is a technique for order preference by similarity to ideal situation can be used to evaluate multiple alternatives against the selected criteria and it was firstly used by Chen in his article titled "Extensions of the TOPSIS for group decision-making under fuzzy environment" [20]. In this method an evaluation matrix consisting of 'm' alternatives and 'n 'criteria is created. The basic concept is that the chosen alternative should have the shortest geometric distance from the positive ideal solution and the longest geometric distance from the negative ideal solution. Actually it defines the positive and negative solution. The positive increases the profit and the negative decreases the cost criterion. According to the concept of the TOPSIS, a closeness coefficient is defined to determine the ranking order of all alternatives by calculating the distances to both the fuzzy positive-ideal solution (FPIS) and fuzzy negative-ideal solution (FNIS) simultaneous [20]. The rating of each alternative and the weight of each criterion are described by linguistic terms which can be expressed in triangular fuzzy number. So a seven-point linguistic scale was suggested to give a value to each alternative. A decision-making matrix was also used to evaluate the importance of the criteria and the ratings of alternatives by using proper techniques such as Entropy.

3.4. The Fuzzy TOPSIS Algorithm

The TOPSIS process is carried out, with a decision-making matrix consisting of 'm' alternatives and 'n 'criteria, as following [20]:

1- Create an evaluation matrix consisting of 'm' alternatives and 'n' criteria.
2- Normalize the decision matrix.
3- Calculate the weighted normalized decision matrix.
4- Determine the worst alternative (A-, FPIS) and the best alternative (A+, FPIS) for criteria.
5- Calculate the distance between the target alternative 'i' and the Fuzzy worst condition and the distance between the alternative 'i ' and the Fuzzy best condition.
6- Calculate the distance between the target alternative 'i' and ideal solution
7- Rank the alternatives.

3.5. Description of Fuzzy TOPSIS for rating EISA criteria based on Fuzzy TOPSIS Algorithm

These linguistic variables can be expressed by fuzzy numbers (Tables 1);

Table 1. Linguistic variables for ratings

Linguistic Variables	Fuzzy Number
Very Poor	(1,1,3)
poor	(1,3,5)
Fair	(3,5,7)
Medium Good	(5,7,9)
Good	(7,9,11)

Using Fuzzy TOPSIS, seven steps has been proposed to rate the criteria as the following [20];

Step 1.Creating a decision-making matrix to evaluate criteria: The result obtained from evaluating alternatives and criteria is the Fuzzy mean of experts' idea. Weight of criteria has been reached by questioning the experts.

Step 2. Normalizing the decision matrix: in this step the fuzzy decision matrix should be inverted to a fuzzy normalized matrix ($\widetilde{R}$). To do so, one of the following could be done:

$$\widetilde{R} = [\widetilde{r}_{ij}]_{m\times n} \qquad i = 1,2,..., m \qquad j = 1,2,..., n$$

m: alternatives, n: criteria

If the fuzzy number is considered as (a,b,c), the normalized matrix $\widetilde{R}$ is calculated as the following:

For positive criterion:

$$\widetilde{r}_{ij} = (\frac{a_{ij}}{c_j^*}, \frac{b_{ij}}{c_j^*}, \frac{c_{ij}}{c_j^*})$$

In the following relation (2-5), c_j^* is the highest value of 'C ' in 'j' criterion in all alternatives. (3-5) relation has stated this fact:

$$c_j^* = \max_i c_{ij}$$

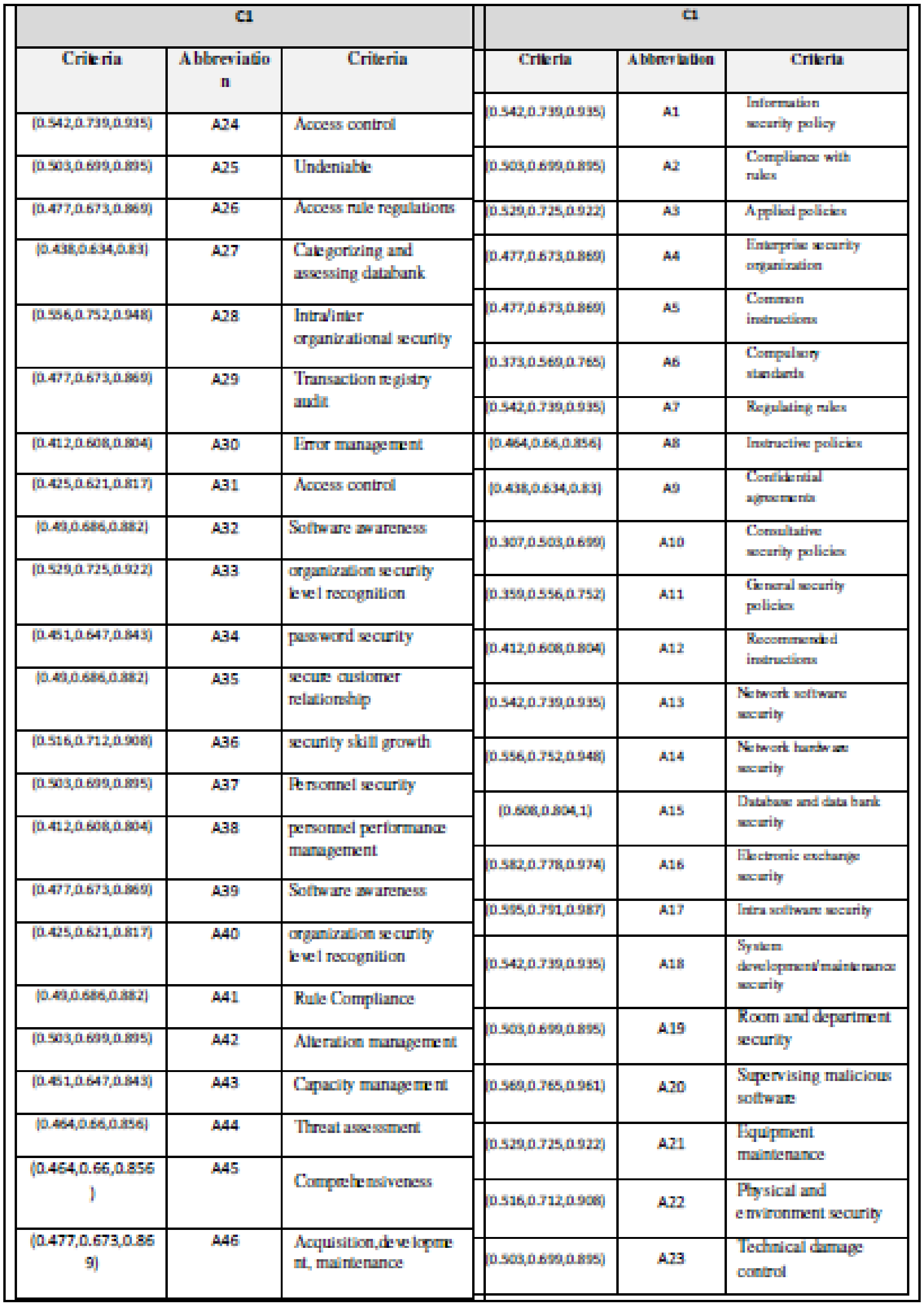
For negative criterion

$$\widetilde{r}_{ij} = (\frac{a_j^\circ}{c_{ij}}, \frac{a_j^\circ}{b_{ij}}, \frac{a_j^\circ}{a_{ij}})$$

Where $\overset{\circ}{a}_j$ is the lowest amount of a in 'j' criterion in all alternatives. It is calculated in (5-5)

$$\overset{\circ}{a}_j = \min_{i} a_{ij}$$

The calculated results of normalization have been shown in Table.2:



C1		
Criteria	Abbreviation	Criteria
(0.542,0.739,0.935)	A24	Access control
(0.503,0.699,0.895)	A25	Undeniable
(0.477,0.673,0.869)	A26	Access rule regulations
(0.438,0.634,0.83)	A27	Categorizing and assessing databank
(0.556,0.752,0.948)	A28	Intra/inter organizational security
(0.477,0.673,0.869)	A29	Transaction registry audit
(0.412,0.608,0.804)	A30	Error management
(0.425,0.621,0.817)	A31	Access control
(0.49,0.686,0.882)	A32	Software awareness
(0.529,0.725,0.922)	A33	organization security level recognition
(0.451,0.647,0.843)	A34	password security
(0.49,0.686,0.882)	A35	secure customer relationship
(0.516,0.712,0.908)	A36	security skill growth
(0.503,0.699,0.895)	A37	Personnel security
(0.412,0.608,0.804)	A38	personnel performance management
(0.477,0.673,0.869)	A39	Software awareness
(0.425,0.621,0.817)	A40	organization security level recognition
(0.49,0.686,0.882)	A41	Rule Compliance
(0.503,0.699,0.895)	A42	Alteration management
(0.451,0.647,0.843)	A43	Capacity management
(0.464,0.66,0.856)	A44	Threat assessment
(0.464,0.66,0.856)	A45	Comprehensiveness
(0.477,0.673,0.869)	A46	Acquisition,development, maintenance

C1		
Criteria	Abbreviation	Criteria
(0.542,0.739,0.935)	A1	Information security policy
(0.503,0.699,0.895)	A2	Compliance with rules
(0.529,0.725,0.922)	A3	Applied policies
(0.477,0.673,0.869)	A4	Enterprise security organization
(0.477,0.673,0.869)	A5	Common instructions
(0.373,0.569,0.765)	A6	Compulsory standards
(0.542,0.739,0.935)	A7	Regulating rules
(0.464,0.66,0.856)	A8	Instructive policies
(0.438,0.634,0.83)	A9	Confidential agreements
(0.307,0.503,0.699)	A10	Consultative security policies
(0.359,0.556,0.752)	A11	General security policies
(0.412,0.608,0.804)	A12	Recommended instructions
(0.542,0.739,0.935)	A13	Network software security
(0.556,0.752,0.948)	A14	Network hardware security
(0.608,0.804,1)	A15	Database and data bank security
(0.582,0.778,0.974)	A16	Electronic exchange security
(0.595,0.791,0.987)	A17	Intra software security
(0.542,0.739,0.935)	A18	System development/maintenance security
(0.503,0.699,0.895)	A19	Room and department security
(0.569,0.765,0.961)	A20	Supervising malicious software
(0.529,0.725,0.922)	A21	Equipment maintenance
(0.516,0.712,0.908)	A22	Physical and environment security
(0.503,0.699,0.895)	A23	Technical damage control

Step3. Constructing weighted normalized fuzzy decision matrix $(\tilde{V})$

$$\tilde{V} = [\tilde{v}_{ij}]_{m \times n} \qquad i = 1,2,..,m \qquad j = 1,2,\ldots,n$$

$$\tilde{v}_{ij} = \tilde{r}_{ij} \otimes \tilde{w}_j$$

$\tilde{r}_{ij}$ is the normalized matrix calculated in step two and $\tilde{w}_j$ is weighted fuzzy criterion of 'j'.

Step 4. Determining the worst alternative (A-, FPIS) and the best alternative (A+, FPIS) for criteria.

$$A^{+} = (v_1^{*}, v_2^{*}, \ldots, v_n^{*})$$

$$A^{-} = (v_1^{-}, v_2^{-}, \ldots, v_n^{-})$$

In this software, fuzzy positive ideal and fuzzy negative ideal solutions presented by Chen are used for all criteria, which are [35]:

$$v_j^{*} = (1,1,1)$$

$$v_j^{-} = (0,0,0)$$

Step 5. Calculating the distance between the target alternative 'i' and the Fuzzy positive-ideal solution ($\tilde{A} = (a_1, a_2, a_3)$= FPIS) and the distance between the alternative 'i ' and the Fuzzy negative-ideal solution ($\tilde{B} = (b_1, b_2, b_3)$=FNIS). So the distance between these two fuzzy numbers are calculated as (12-5):

$$\tilde{A} = (a_1, a_2, a_3)$$

$$\tilde{B} = (b_1, b_2, b_3)$$

$$D(\tilde{A}, \tilde{B}) = \sqrt{\frac{1}{3}[(a_2 - a_1)^2 + (b_2 - b_1)^2 + (c_2 - c_1)^2]}$$

As stated above, the distance for each variable from FPIS and FNIS can be calculated:

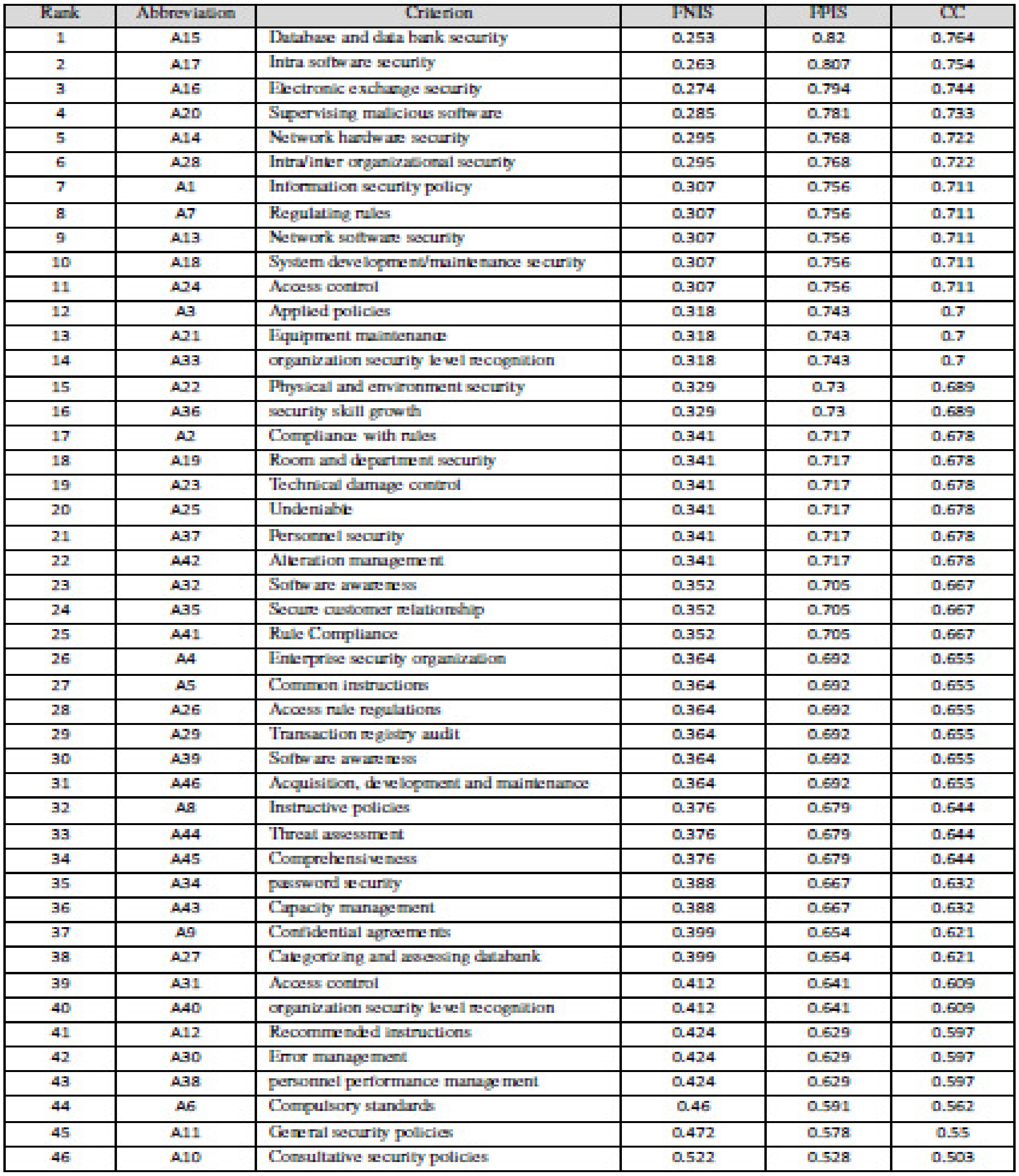
$$d_i^{*} = \sum_{j=1}^{n} d(\tilde{v}_{ij} - \tilde{v}_{ij}^{*}) \qquad i = 1,2,\ldots,m$$

$$d_i^{-} = \sum_{j=1}^{n} d(\tilde{v}_{ij} - \tilde{v}_{ij}^{-}) \qquad i = 1,2,\ldots,m$$

Step 6. Calculating the distance between the target alternative 'i' and ideal solution, which is defined as:

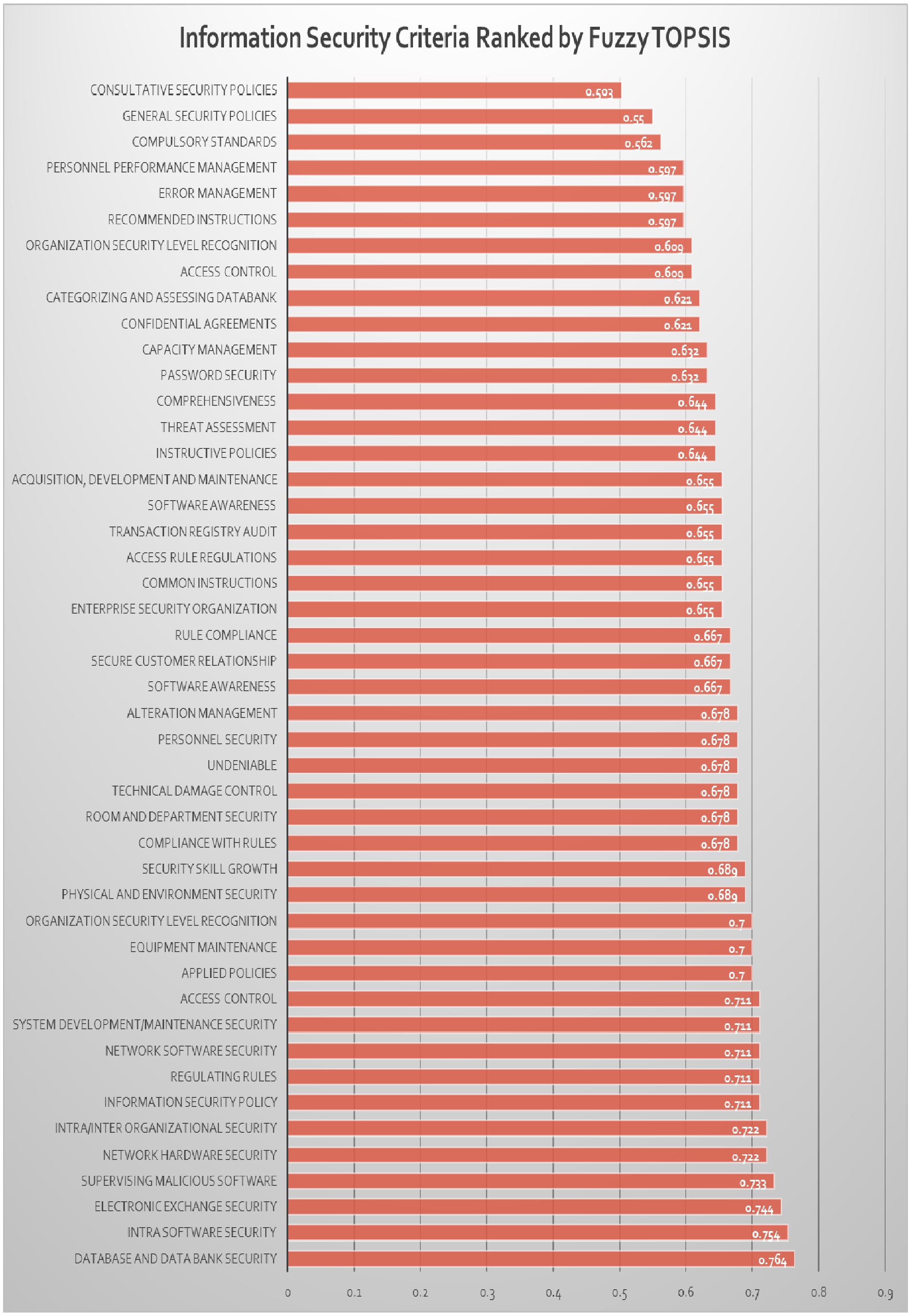
$$CC_i = \frac{d_i^{-}}{d_i^{*} + d_i^{-}} \qquad i = 1,2,\ldots,m$$

Step7. Ranking the alternatives which is descending. The bigger CC is, the better it is. The results obtained from the ranking alternatives by using Fuzzy TOPSIS are presented in Table 3.

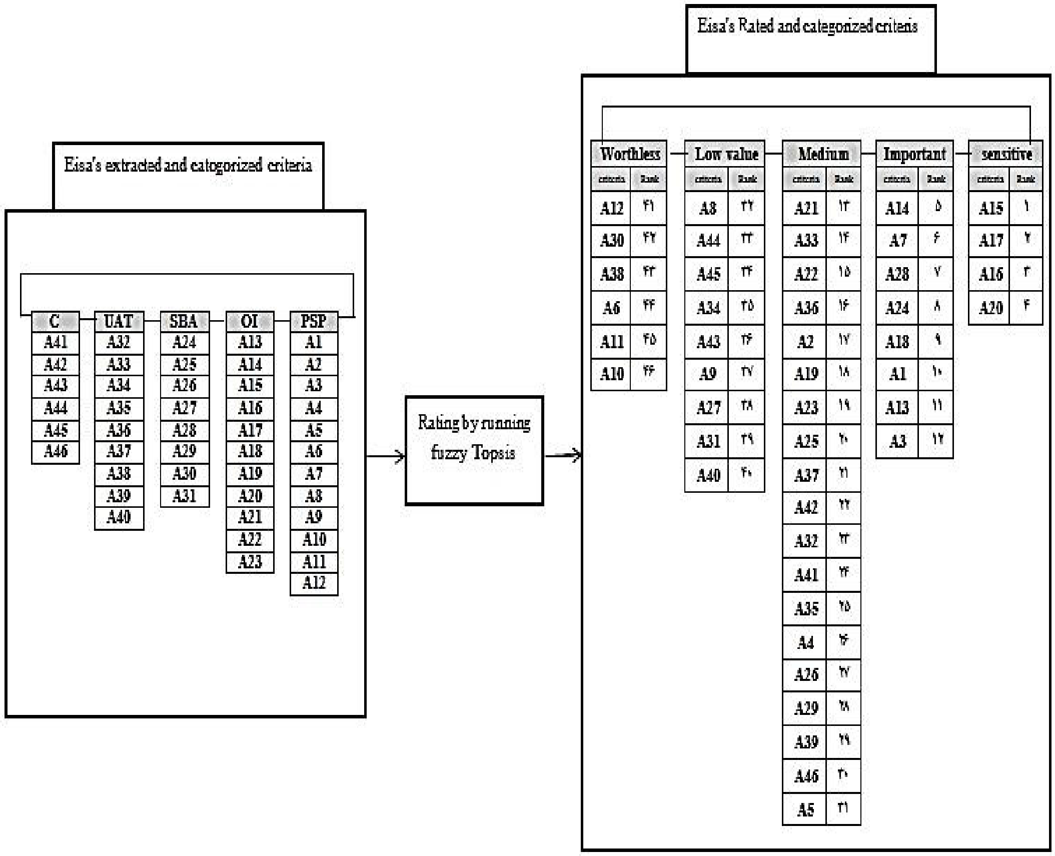


Rank	Abbreviation	Criterion	FNIS	FPIS	CC
1	A15	Database and data bank security	0.253	0.82	0.764
2	A17	Intra software security	0.263	0.807	0.754
3	A16	Electronic exchange security	0.274	0.794	0.744
4	A20	Supervising malicious software	0.285	0.781	0.733
5	A14	Network hardware security	0.295	0.768	0.722
6	A28	Intra/inter organizational security	0.295	0.768	0.722
7	A1	Information security policy	0.307	0.756	0.711
8	A7	Regulating rules	0.307	0.756	0.711
9	A13	Network software security	0.307	0.756	0.711
10	A18	System development/maintenance security	0.307	0.756	0.711
11	A24	Access control	0.307	0.756	0.711
12	A3	Applied policies	0.318	0.743	0.7
13	A21	Equipment maintenance	0.318	0.743	0.7
14	A33	organization security level recognition	0.318	0.743	0.7
15	A22	Physical and environment security	0.329	0.73	0.689
16	A36	security skill growth	0.329	0.73	0.689
17	A2	Compliance with rules	0.341	0.717	0.678
18	A19	Room and department security	0.341	0.717	0.678
19	A23	Technical damage control	0.341	0.717	0.678
20	A25	Undeniable	0.341	0.717	0.678
21	A37	Personnel security	0.341	0.717	0.678
22	A42	Alteration management	0.341	0.717	0.678
23	A32	Software awareness	0.352	0.705	0.667
24	A35	Secure customer relationship	0.352	0.705	0.667
25	A41	Rule Compliance	0.352	0.705	0.667
26	A4	Enterprise security organization	0.364	0.692	0.655
27	A5	Common instructions	0.364	0.692	0.655
28	A26	Access rule regulations	0.364	0.692	0.655
29	A29	Transaction registry audit	0.364	0.692	0.655
30	A39	Software awareness	0.364	0.692	0.655
31	A46	Acquisition, development and maintenance	0.364	0.692	0.655
32	A8	Instructive policies	0.376	0.679	0.644
33	A44	Threat assessment	0.376	0.679	0.644
34	A45	Comprehensiveness	0.376	0.679	0.644
35	A34	password security	0.388	0.667	0.632
36	A43	Capacity management	0.388	0.667	0.632
37	A9	Confidential agreements	0.399	0.654	0.621
38	A27	Categorizing and assessing databank	0.399	0.654	0.621
39	A31	Access control	0.412	0.641	0.609
40	A40	organization security level recognition	0.412	0.641	0.609
41	A12	Recommended instructions	0.424	0.629	0.597
42	A30	Error management	0.424	0.629	0.597
43	A38	personnel performance management	0.424	0.629	0.597
44	A6	Compulsory standards	0.46	0.591	0.562
45	A11	General security policies	0.472	0.578	0.55
46	A10	Consultative security policies	0.522	0.528	0.503

To show main result of Fuzzy TOPSIS ranking, a chart has been figured by CC parameter in figure 4. This chart shows how all criteria ranked based on their importance.



The result of ranking criteria belonging to five essential components in EISA which was earned by using Fuzzy TOPSIS has represented that data bank and database security as one of criteria of organizational infrastructure is the top priority. The Fuzzy TOPSIS output and Fuzzy Vikor output adjustment has admitted the accuracy of Fuzzy TOPSIS method. The proposed model of EISAM is shown in Figure 5.


Eisa's extracted and catogorized criteria
Rating by running fuzzy Topsis
Eisa's Rated and categorized criteria

C	UAT	SBA	OI	PSP
A41	A32	A24	A13	A1
A42	A33	A25	A14	A2
A43	A34	A26	A15	A3
A44	A35	A27	A16	A4
A45	A36	A28	A17	A5
A46	A37	A29	A18	A6
	A38	A30	A19	A7
	A39	A31	A20	A8
	A40		A21	A9
			A22	A10
			A23	A11
				A12

Worthless		Low value		Medium		Important		sensitive	
criteria	Rank	criteria	Rank	criteria	Rank	criteria	Rank	criteria	Rank
A12	۴۱	A8	۳۲	A21	۱۳	A14	۵	A15	۱
A30	۴۲	A44	۳۳	A33	۱۴	A7	۶	A17	۲
A38	۴۳	A45	۳۴	A22	۱۵	A28	۷	A16	۳
A6	۴۴	A34	۳۵	A36	۱۶	A24	۸	A20	۴
A11	۴۵	A43	۳۶	A2	۱۷	A18	۹		
A10	۴۶	A9	۳۷	A19	۱۸	A1	۱۰		
		A27	۳۸	A23	۱۹	A13	۱۱		
		A31	۳۹	A25	۲۰	A3	۱۲		
		A40	۴۰	A37	۲۱				
				A42	۲۲				
				A32	۲۳				
				A41	۲۴				
				A35	۲۵				
				A4	۲۶				
				A26	۲۷				
				A29	۲۸				
				A39	۲۹				
				A46	۳۰				
				A5	۳۱				

EISA's criteria, which are categorized into five essential components including PSP (Policies, Standards, and Procedures), SBA (Security Baselines/ risk assessments), SAT (Security Awareness and Training programs), OI (Organizational Infrastructure), and C (Compliance), have been ranked and quantified. Then the result has been analyzed in terms of CC (closeness coefficient that is calculating the distance between the target alternative 'i' to ideal solution). Computing the closeness coefficient of each alternative has led to 5 linguistic variables: S (sensitive), I (important), M (medium), L (low), and W (weak). Each criterion of the mentioned components based on its rank is located in these groups.

4. CONCLUSION

The Fuzzy TOPSIS procedure was exploited in order to propose a model for ranking enterprise information security architecture's criteria in this study. Reviewing the related national and international literature on EISA, extracting major criteria, and rating them in Gartner's five components, experts' ideas in this field was collected by a questionnaire. The mentioned criteria were quantified, rated and given a numerical value by Fuzzy TOPSIS, one of the most recent academic procedures. Among all 46 criteria, data bank and data base security is on top of the list and is ranked as number one. A consultative security policy which is the subset of PSP (policies, standards, procedures) with the rank of 46 is located at the bottom of the list. On the other, possessing the entire sensitive interval by four criteria; data bank and data base security electronic exchange security, intra software security, and supervising malicious software as the subsets of OI (organizational infrastructures) it was proposed that OI is the most significant of all. The conclusion carries the fact that EISA was conceptually studied in previous studies and no definite criteria were defined. Searching all aspects of EISA thoroughly, the present study has extracted the key criteria which have not been registered yet. Moreover, quantifying the above-mentioned criteria has distinguished this study from the other conducted research on the same field and it has resulted in rating EISA's criteria. It could also facilitate the process of formulating policies for those organizations that have just started developing and extending security plans. For future work it is suggested to conduct researches on following issues:

- Analyze and interpret ranked criteria
- Provide a guideline for managers to use the proposed model
- Compare the result with other ranking methods

REFERENCES

[1] Asadi Shali, A., "management information systems", Journal of Information and Documentation Center of Iran, Number IV, Volume IV, July, 2005.

[2] Nasiri Asayesh, HR., Thesis "A New Model For Enterprise Mashups Security Risk Assessment", Department of Electrical and Computer Engineering, Shahid Beheshti University, Tehran, August,2011.

[3] Shariati, M.,Thesis "Proposing an Interoperable EISA Framework in Inter / Intra Enterprise Application", Department of Electrical and Computer Engineering, Shahid Beheshti University, Tehran, February ,2011.

[4] Scholtz,T., "Structure and Content of an Enterprise Information Security Architecture Gartner Inc", (2006).

[5] Killmeyer, Tudor, Jan., "Information security architecture: an integrated approach to security in the organization", 2006, ISBN 0-8493-1549-2.

[6] Pulkkinen, Mirja., Naumenko, Anton., Luostarinen, Kari., "Managing information security in a business network of machinery maintenance services business – Enterprise architectureas a coordination tool", The Journal of Systems and Software 80 (2007) ,1607–1620.

[7] Shariatia Marzieh., Bahmani, Faezeh., Shams., Fereidoon.," Enterprise information security, a review of architectures and frameworks from interoperability perspective " , Procedia Computer Science, Vol 3 ,2011 ,PAGES 537–543.

[8] Chetty, Jacqui., Coetzee, Marijke., "Towards An Information Security Framework For Service-oriented Architecture" , University of Johannesburg, 2010.

[9] Roedig, U. , Schumacher, M., " Security engineering with patterns", PloP conference, 2011.

[10] Zandi, F., Tavana, M., "A fuzzy group multi-criteria enterprise architecture framework selection model", The Journal of Expert Systems with Applications, Vol. 39, pages [1165–1173],2012.

[11] Zafar , H. ,"Human resource information systems: Information security concerns", The Journal of Human Resource Management Review, Kennesaw State University, United States, Vol 23, Pages [105–113] , 2013 .

[12] Sohrabi Safa ,N., Sookhak, M Von Solms, R., Furnell, S., Abdul Ghani, N., Herawan, T., " Information security conscious care behavior formation in organizations", The Journal of computers & se curity, Vol 5 3, pages [6 5 -7 8] ,June 2015

[13] Li, Sh., C.Yen ,D., Chen, Sh., S. Chen, P., Lu, W., Cho, Ch., "Effects of virtualization on information security", Journal Computer Standards & Interfaces, Vol 42, pages[1–8], April 2015.

[14] Fazlida, M.R., Said, J, "Information Security: Risk, Governance and Implementation", Procedia Economics and Finance ,Vol 28, Pages [243–248], 2015.

[15] Jalayer, F., Nabiollahi ,A., "A Model for the introduceing metrics of enterprise information security architecture", Third International Conference on Applied Research in Computer Engineering, Information Technology,Tarbiat Modares University, Iran,Tehran, February 4,2016.

[16] Gu, X., Zhu, Q., "Fuzzy multi-attribute decision-making method based on eigenvector of fuzzy attribute evaluation space", The Journal of Decision Support Systems, Vol 41 (1), Pages [400–410], 2006.

[17] Mizumoto, M., Zimmermann, H.J.," Comparison of fuzzy reasoning methods", The Journal of Fuzzy Sets and Systems, Vol 8 (3), Pages [253–283], 1982.

[18] Najafi, A. and Naji,E., "Selecting Best Projects based on Fuzzy TOPSIS, Fuzzy ANP and Balanced Scorecard Approaches", The Journal of Economics and Development, Vol 2(2), Pages[15–28], February 2014.

[19] Bouzon, M., Govindan, K., Carlos M., Taboada C., Lucila M.S, "Identification and analysis of reverse logistics barriers using fuzzyDelphi method and AHP", Resources, Conservation and Recycling,January 2016 .

[20] Chen-Tung, Ch., "Extensions of the TOPSIS for group decision-making under fuzzy environment", Fuzzy Sets and Systems, Volume 114, 2000.

[21] Sun, Ch., "A performance evaluation model by integrating fuzzy AHP and fuzzy TOPSIS methods", The Journal of Expert Systems with Applications, Vol 37, Pages [7745–7754], 2010.

[22] M. Aghajani Mir, P. Taherei Ghazvinei, Sulaiman, N.M.N., Basri, N.E.A., "Application of TOPSIS and VIKOR improved versions in a multi criteria decision analysis to develop an optimized municipal solid waste management model", Journal of Environmental Management, Volume 166, 2016.

[23] Das, P.," Adaptation of fuzzy reasoning and rule generation for customers' choice in retail FMCG business", Journal of Management Research, Vol 9 (1), pages [15-26], 2009.

AUTHORS

Farzaneh Sadat Jalayer was born in Iran. She is a master student in software engineering in 2016 at faculty of computer engineering, Najafabad branch of Islamic Azad University under supervision of Dr. Akbar Nabiollahi. She defended her master thesis, “Prioritizing and Ranking EISA's Criteria by Deploying Fuzzy TOPSIS”, in February, 2016. Her research interests are software engineering, enterprise architecture, and information security.

Akbar Nabiollahi-Najafabadi was born in 1970 in Najafabad, Iran. He received his BSc in software engineering from Isfahan University of Technology in 1994. Continuing education, he received his MSc in software engineering from Islamic Azad University, Najafabad Branch in 2002. He conducted his doctoral studies in computing science, with the orientation of Information technology, in “Universiti Teknologi Malaysia (UTM)” from 2008 to 2012. His dissertation was about “A Proposed Integrated Framework for Enterprise Architecture and Information Technology Service Management”. His work experience consists of various projects in software engineering, IT service management, and information systems. Since 2012, he has been the assistant professor of the Faculty of Computer Engineering in Islamic Azad University, Najafabad Branch, Iran. His publications include many journal and conference papers. His research interests are enterprise architecture, information systems, and IT service management.