Information Security Risk Management of Research Information Systems: A hybrid approach of Fuzzy FMEA, AHP, TOPSIS and Shannon Entropy

M.J. Ershadi
Department of Industrial Engineering
Iranian Research Institute for Information Science & Technology (IranDoc)
1 Enghelab Ave. Felestin Intersection
Tehran 1315773314, Iran
mjershadi@gmail.com

Mehrdad Forouzandeh
Islamic Azad University, Najaf Abad Branch
Iran
forouzandeh05@gmail.com

JDIM
Journal of Digital Information Management

ABSTRACT: *The purpose of this paper is to implement information security risk management (ISRM) in research information systems (RIS). Appropriate identification and assessment of risks in different aspects such as software, communications, and human resources for RIS's besides providing efficient and effective preventive and corrective actions are other aims of this study. Furthermore, continual improvement of risk response processes in information technology environment is another aim of this study. In this study, potential risks of information security are identified using failure mode and effects analysis (FMEA). Also, detected failure modes are evaluated by multi-criteria decision-making method (MCDM) using a hybrid method of fuzzy logic, analytic hierarchy process (AHP), Shannon entropy scoring method, and technique for order preference by similarity to the ideal solution (TOPSIS). The result of this paper shows that information security software potential risks assessment by the proposed model is more accurate and reliable than non-fuzzy models. Unauthorized access to view or change the stored information of the server is the risk with the most important priority identified by MCDM approach. Confidentiality of information is more important than other information security criteria. Furthermore, failure modes in the category of the main server and internet have more priority in comparison to others.*

Subject Categories and Descriptors: [D.4.6 Security and Protection]; [I.2.3 Deduction and Theorem Proving] Uncertainty, "fuzzy," and probabilistic reasoning: **[E.4 CODING AND INFORMATION THEORY]**

General Terms: Information Security Risk Managment, Information Security, Shannon Entropy, Fuzzy Approach

Keywords: Research Information Systems, Risk Management, Information Security, Failure Modes and Effect Analysis, Fuzzy Multiple Criteria Decision Making

Received: 12 June 2019, Revised 20 September 2019, Accepted 29 September 2019

Review Metrics: Review Scale- 0/6, Review Score-4.56, Inter-reviewer Consistency- 82.2%

DOI: 10.6025/jdim/2019/17/6/321-336

1. Introduction

Nowadays, information technology has grown rapidly and information systems have a decisive and comprehensive role in the organizational business (Yuan and Chen, 2012). Therefore, the highest level of accountable management organization has the responsibility to protect the organization's information. Although information security often brings many benefits to organizations its implementing is generally so difficult.

In a study conducted by security company McAfee in 2008 was indicated that information security breaches in global companies worth more than a trillion dollars in losses within a year lead (Feledi et al., 2013).

Information security management has undertaken the task of implementing and monitoring the organization's security system which finally must try to keep the system always up to date (Panchal et al. 2018). The purpose of information security management in an organization is to preserve capital in the face of any threat and to achieve this goal required a comprehensive and integrated program.

Undoubtedly, the appearance and popularity of machine-readable databases and particularly online databases have been one of the most important recent decade's phenomena in the information industry that have grown in the field of the internet. The online database term normally used related to the digital information stored on computers that is accessible through large and small networks and the internet. The online database is an organized collection of information that is processed, stored and by the user to be searched and retrieved (Feather and Sturges, 2003).

Research information systems such as online databases from years ago are responsible for identifying, collecting, organizing and disseminating information related to various scientific documents such as theses and dissertations (Ershadi et al., 2018). In recent years due to the development of computer programs on the World Wide Web, databases are presented in this environment. Although these databases are efficient and effective for gathering and disseminating of research information, already faced with problems as follow:

• Surprise by unforeseen faults and noncompliance information security.

• Lack of a plan to improve software systems according to information security risks in the future.

• Dissatisfaction of internal and external users with the system in the field of information security.

The best way to manage aware of the current situation and make the right decision is to improve it. The most important part of risk assessment is to assess and identify the current situation. Risk management consists of four phases of identification; evaluation; planning or management and tracking risk events (Ritchie and Brindley, 2007). Nowadays, Current Research Information Systems (CRIS) has emerged to manage all materials of a research project completely up-to-date (Azeroual & Schöpfel, 2019; Azeroual, Saake & Abuosba, 2018). Also in this context data quality and especially information security are the most important dimension which should be carefully considered (Azeroual, Saake & Schallehn, 2018; Azeroual, Saake & Wastl, 2018).

The context of information security risk management is defined in two dimensions. The first one is the structure and a procedure that scope and evaluate criteria called structural dimension. The second one is process and assessment tool, which called procedural dimensions. This framework is comprised of comprehensive vision including strategy, technology, organization, people and the environment. In this regard, the assets of organizations in the fields of documentation, infrastructure, software, services, and manpower are assessed and then their potential threats and risks are identified and analyzed (Saleh and Alfantookh, 2011).

Prerequisites for successful planning in order to reduce risks are their appropriate assessment and identification then providing effective and efficient corrective and preventive actions. In this field, the method of Failure Mode and Effects Analysis (FMEA) as an effective tool could be the best tool. Although traditional FMEA methodology has been used extensively in research resources but has weaknesses and limitations as follows (Liuet al., 2013).

• Ignoring the importance weight of factors which affect risk assessment;

• Criteria have mental nature and scores are vague and imprecise,

• Scores of several risks may be the same and decision making on corrective actions would be so hard;

• The formula for calculating the rate of risks is questionable and unreliable.

In this study, to solve the above problems, the traditional FMEA method with a hybrid of fuzzy theory, Shannon entropy scoring method and multi-criteria decision making (MCDM) the method has been used. FMEA method is employed for identifying and ranking of risks. Also, MCDM techniques are used for weighting three main criteria severity, occurrence and detection. Furthermore, Shannon entropy method is used for normalizing results of MCDM approach.

As a case, an important RIS for Iranian theses and dissertations called GANJ is selected. This system involves a database for recording and dissemination of scientific research such as theses and dissertations.

The structure of this paper is as follows. Section 2 is about a literature review on the history and main newly studies on risk management on information systems. The proposed model for assessment and reducing information security risks is presented in section 3. Application of the proposed model for risk management through a case study is investigated in section 4. Section 5 provides a comparative study on different combinations of methods for application on traditional FMEA. In section 6 (discussion) similar studies and comparison of their results to the current paper are presented. Conclusion and some recommendations for future researches are presented in section 7.

2. Literature Review

In this section literature review is done based on two different parts. In subsection 2.1 a review on the main

researches of information security risk management is proposed. Then in subsection 2.2 the main newly studied researches on FMEA model and their combinations with MCDM techniques are prepared.

2.1 Information Security Risk Management (ISRM)

A systematic approach was firstly developed for issues of secure information exchange space with the advent of the first standard for information security management (Kwon et al., 2007). According to this view, the security of organizations is not achieved by replication of some physical tasks but it must be continuously done in a systematic framework during immunizations cycle, including the design, implementation, evaluation and modification, based on methodologies which are identified and planned (Broderick, 2006).

Fenz and Neubauer (2018) presented a method for formalizing information security control descriptions to improve the checking process of information security. In another study, information security risks of the organization for the internal network are identified and assessed by using the Information Security Risk Analysis Method (ISRAM). ISRAM model is a hybrid of quantitative methods and analysis of user comments (Karabacak and Sogukpinar, 2005). Chawla and Saxena (2016) following this approach assessed a knowledge management system based on factor analysis.

Aldini et al. (2017) presented a framework named opportunity-enabled risk management (OPPRIM), to support the decision-making process in access control to remote corporate assets. In an independent research, results of the Fuzzy AHP and Artificial Neural Network (ANN) method were combined for e-government information security risk assessment. In this study, the lack of systems and data management protection, technical flaws and qualitative defects of the information transmission lines were stated as the most preferred risks. FAHP method has been used for assessing and analyzing threats in independent research (Wei et al., 2010). Harrison and Jürjens (2017) studied the role of personnel in the management of information security. Also, Rebelo et al. (2017) developed a model to manage the risks of integration of management systems.

Zachman model is useful for classification of assets to determine the value of assets, threats and damage effects (Sendi et al., 2010). Silva et al. (2014) analyzed five aspects of information security, including access to information and systems, communications, infrastructure, security management, information security of systems development using fuzzy FMEA.

Using Bayesian networks, information security risks were identified in a company's financial services and then assessed risks were ranked. In this study, the risk of network and the failure modes related to user authentication for external connections were prioritized (Feng et al., 2014).

Combined event tree analysis (ETA) with the fuzzy theory is another method for information security risk assessment which was studied by De Gusmão et al. (2016).

The following sub-section provides some main researches on FMEA model.

2.2 FMEA Model

Because information security risk assessment has a new discipline, standards and methodologies in the field of information security risk management has recently been increased.

Recent researches by combining traditional FMEA method as an efficient tool with other tools have tried to reduce restrictions and increase confidence in the obtained results. One of the most important approaches is the application of fuzzy theory on parameters of the FMEA. This method causes final results to be more accurate and clarifies the rating of the FMEA method (Wang et al, 2009).

In a different model, after determining the mutual relative importance weight of each criterion to other criteria by using the Shannon Entropy, closeness coefficient was calculated for each identified risk in the traditional FMEA method by using TOPSIS then the risks were ranked. In this model, six intended criteria were the probability of occurrence; the probability of detection; maintainability; spare parts; economic security and economic (Sachdeva et al., 2009; Ershadi and Ershadi, 2018).

In another method by FMEA, potential failure modes are detected and then identified risks were compared and assessed according to criteria of FMEA by using the paired comparison of the AHP method and finally, the risks were prioritized according to the calculated RPN (Abdelgawad and Fayek, 2010).

In another research, traditional FMEA was improved by fuzzy and gray theory. The fuzzy theory was applied for an expert rating and fuzzy scores were changed to the non-fuzzy by using gray theory then matrix utility was used to prioritize risks (Liu et al., 2011).

Also in an independent study, the combination of Decision Making Trial and Evaluation Laboratory (DEMATEL) with TOPSIS in the risks rating and prioritizing of FMEA method was used (Chang et al., 2014).

In this study, based on a comprehensive review of literature, a hybrid fuzzy theory, Shannon Entropy method, AHP, and TOPSIS is used to improve the traditional FMEA. In this approach, the fuzzy theory is employed for augmenting precision of the expert opinions. Then, Shannon Entropy method is applied for weighting of the criteria based on variance of expert opinions. Next, the AHP method is implemented for weighting the criteria according to the expert opinions and paired comparisons and finally fuzzy TOPSIS method is used for calculating the closeness coefficient and prioritized potential risks.

The applied methodology is explained in the next section.

3. Methodology

The suggested information security risk assessment is proposed in this paper includes five following steps (figure 1).

Step 1: Software aspects of the current system are studied in this step and its specifications are investigated by forming a group of experts.

It should be mentioned that the experts were including nine IT professionals of the studied system.

Step 2: Potential failure modes of software information security is identified by brainstorming meeting of the expert group in this step.

Step 3: This step is divided into two sub-steps,

Step 3-1: Identified failure modes are assessed by using three criteria, severity of effect, the probability of occurrence and degree of detection according to the expert opinions. Fuzzy numbers (as is shown in table 1) are used for scoring in FMEA.

Step 3-2: The pairwise comparison of three FMEA criteria is made for determining the importance of each criterion relative to the other according to the expert opinions by using te fuzzy number (table 2).

Step 4: This step is also divided into two parts,

Step 4-1: Weights of three criteria, the severity of effect, the probability of occurrence and degree of detection are calculated based on the pairwise comparison which is described in step 3 by using fuzzy AHP.

Step 4-2: Final weights of three criteria are determined based on the variance of expert's opinions according to the calculated criteria weights of step 4-1 by using the Shannon entropy. At the end of this step and fuzzy opinions are transformed into crisp numbers.

Step 5: In this step, first, closeness coefficients of failure modes are determined by using fuzzy TOPSIS according

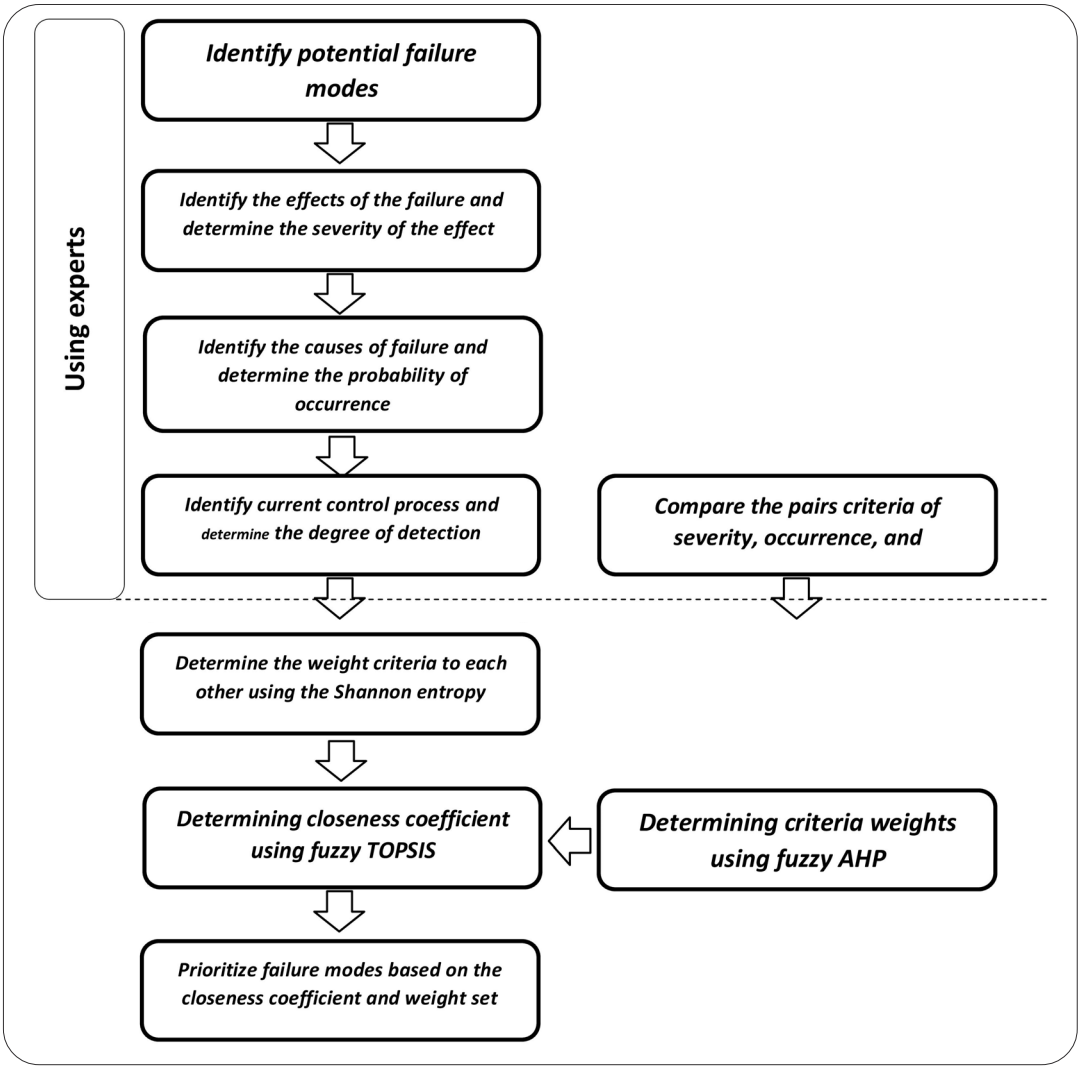

Figure 1. The evaluation process of potential failure modes based on the proposed model

to the calculated weights of step 4. Then, the identified potential failure modes prioritized based on the difference between the closeness coefficients and number one.

In the next sub-section, the applied FMEA model is explained.

3 .1 Fuzzy FMEA

Fuzzy sets are a set of imprecise objects with different degrees of membership. The membership function is a function with a range of [0, 1] (Zadeh, 1996). Fuzzy logic is extracted from fuzzy set theory for approximate arguments on the contrary precise arguments in an uncertainty environment.

Among the various fuzzy numbers, triangular fuzzy numbers are more common, that is shown by three degrees, $A = (a_1, a_2, a_3)$, and the membership function of the numbers is as follows:

Formula 1:
$$\mu_{\tilde{A}(x)} = \begin{cases} 0, x < a_1 \\ \dfrac{x - a_1}{a_2 - a_1}, a_1 \le x \le a_2 \\ \dfrac{a_3 - x}{a_3 - a_2}, a_2 \le x \le a_3 \\ 0, a_3 < x \end{cases}$$

If two fuzzy numbers A and B as $A = (a_1, a_2, a_3)$ and $B = (b_1, b_2, b_3)$ defined, then (Zimmermann, 2001):

- Adding these two numbers which lead to number C: $C = (a_1 + b_1, a_2 + b_2, a_3 + b_3)$
- Subtract them, number D: $D = (a_1 - b_1, a_2 - b_2, a_3 - b_3)$
- Multiply them, number E: $E = (a_1 . b_1, a_2 . b_2, a_3 . b_3)$

The fuzzy theory is used for improving the traditional FMEA according to shortcomings of this method that are mental nature of criteria and vague and imprecise scores. Fuzzy FMEA allows quantitative data, as well as qualitative data, are used and the traditional method becomes more flexible (Braglia et al., 2003).

Linguistic variables specified with equivalent fuzzy values in table 1 that experts can use these variables to evaluate the criteria of FMEA (Kutlu and Ekmekçioglu, 2012). These values are imported to the FAHP method as is described in the next sub-section.

3.2 Fuzzy AHP

Fuzzy AHP is used for the first time by Laarhoven and Pedrycz in 1983 (Kutlu and Ekmekçioglu, 2012). Fuzzy theory is helping the decision maker to can freely choose a range of desired values instead of selecting the exact numbers against of mental perceptions, and uncertain judgment of the expert can be expressed (Vahidnia and Alimohammadi, 2009; Chang, 2006).

Based on extent analysis method, if $X = (x_1, x_2, ..., x_n)$ is an object set and $U = (u_1, u_2, ..., u_m)$ is a goal set, each object is selected then extent analysis is performed for each goal, respectively. m extent analysis values are achieved for each object.

Therefore, if $\tilde{M}^1_{gi}, \tilde{M}^2_{gi}, \tilde{M}^2_{gi}$ $(i = 1, 2, \ldots, n$ and $j = 1, 2, \ldots, m)$ are triangular fuzzy numbers, the steps of the extent analysis can be given as follows:

First Step: Fuzzy combined value for each object is defined as below:

Formula 2:
$$\tilde{S}_i = \Sigma_{j=1}^{m} \tilde{M}^j_{gi} \odot [\Sigma_{i=1}^{n} \Sigma_{j=1}^{m} \tilde{M}^j_{gi}]^{-1}$$

Formula 3:
$$\tilde{M}^j_{gi} = [\Sigma_{j=1}^{m} l_j, \Sigma_{j=1}^{m} m_j, \Sigma_{j=1}^{m} u_j]^{-1}$$

Formula 4:
$$\Sigma_{i=1}^{n} \Sigma_{j=1}^{m} \tilde{M}^j_{gi} = (\Sigma_{i=1}^{n} \Sigma_{i=1}^{n} m_i, \Sigma_{i=1}^{n} u_i)$$

Formula 5:
$$[\Sigma_{i=1}^{n} \Sigma_{j=1}^{m} \tilde{M}^j_{gi}]^{-1} = \left(\frac{1}{\Sigma_{i=1}^{n} u_i}, \frac{1}{\Sigma_{i=1}^{n} m_i}, \frac{1}{\Sigma_{i=1}^{l} u_i}\right)$$

The second step: $\tilde{M}_1, \tilde{M}_2$ are two triangular fuzzy numbers that possibility degree $\tilde{M}_1 \ge \tilde{M}_2$ is defined as follows:

Formula 6:
$$V(\tilde{M}_1 \ge \tilde{M}_2) = Sup_{x \ge y} [min(\mu_{\tilde{M}_1}(x), \mu_{\tilde{M}_2}(y))]$$

Abbreviation signs	Linguistic variables	Fuzzy points
VP	Very poor	(0, 0, 1)
P	Poor	(0, 1, 3)
MP	Medium poor	(1, 3, 5)
F	Fair	(3, 5, 7)
MG	Medium good	(5, 7, 9)
G	good	(7, 9, 10)
VG	Very good	(9, 10, 10)

Table 1. Fuzzy evaluation score for fuzzy FMEA (Kutlu and Ekmekçioglu, 2012)

Formula 7:

$$V(\tilde{M}_2 \geq \tilde{M}_1) = \mu(d) = \begin{cases} 1, \ if \ m_1 \geq m_2 \\ 0, \ if \ l_2 \geq u_1 \\ \dfrac{l_1 - u_2}{(m_2 - u_2) - (m_1 - l_1)}, \ otherwise \end{cases}$$

According to figure 2, d is perpendicular to point D on the intersection between $\mu_{\tilde{M}_1}$ and $\mu_{\tilde{M}_2}$ and in comparison $\tilde{M}_1$ and $\tilde{M}_2$, $V(\tilde{M}_2 \geq \tilde{M}_1)$ and $V(\tilde{M}_1 \geq \tilde{M}_2)$ are needed:

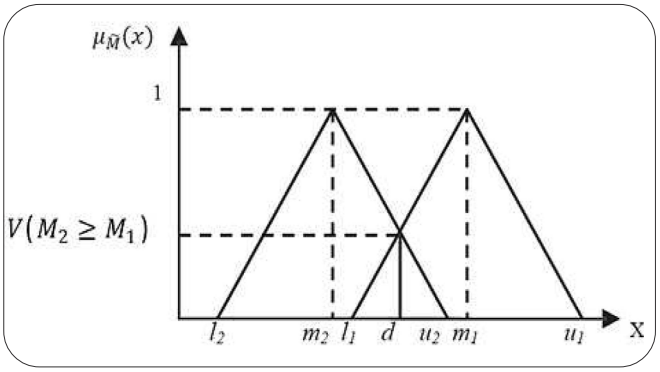

Figure 2. Possibility degree of two fuzzy numbers (Chang, 1996)

Third step: Possibility degree for the convex fuzzy number $\tilde{M} \geq \tilde{M}_1, \tilde{M}_2, ..., \tilde{M}_k$ would be:

Formula 8: $V(\tilde{M} \geq \tilde{M}_1, \tilde{M}_2, ..., \tilde{M}_k) = min V(\tilde{M} \geq \tilde{M}_i), i = 1,2,...,k$

It is assumed $\acute{d}(A_i)$ as is described in equation (9).

Formula 9: $\acute{d}(A_i) = min V(S_i \geq S_k), \quad k = 1,2,...,n, \quad k \neq i$

As a result, the weight vector for n object is equal to:

Formula 10: $\acute{W} = (\acute{d}(A_1), \acute{d}(A_2), ..., \acute{d}(A_i))^T, \quad i = 1,2,...,n$

And with normalization of weight vector equation (11) would be resulted in where number W is a non-fuzzy number.

Formula 11: $W = (d(A_1), d(A_2), ..., d(A_i))^T, \quad i = 1,2,...,n$

Paired comparisons are done using table 2. It is necessary that after comparisons, the consistency degree to be checked. To do this, the mean integration approach is used for defuzzifying the matrix. For a fuzzy number $\tilde{A} = (a_1, a_2, a_3)$ can be transformed into a crisp number by using the following equation:

Formula 12: $$P(\tilde{A}) = A = \left(\frac{a_1 + 4a_2 + a_3}{6}\right)$$

After defuzzifying values, consistency degree of the matrix could be calculated.

Because the variance of the expert opinions has a main impact on the obtained results of AHP, using methods such as Shannon entropy could be so helpful for improving final results of AHP. The next sub-section shows how this improvement could be executed.

Abbreviation signs	Linguistic variables	Fuzzy points
AS	Absolutely strong	(2, 5/2, 3)
VS	Very strong	(3/2, 2, 5/2)
FS	Fairly strong	(1, 3/2, 2)
SS	Slightly strong	(1, 1, 3/2)
E	Equal	(1, 1, 1)
SW	Slightly weak	(2/3, 1, 1)
FW	Fairly weak	(1/2, 2/3, 1)
VW	Very weak	(2/5, 1/2, 2/3)
AW	Absolutely weak	(1/3, 2/5, 1/2)

Table 2. Fuzzy evaluation point for fuzzy AHP method (Kutlu and Ekmekçioglu, 2012)

3.3 Shannon Entropy

The first time, Shannon entropy model that is taken from information theory, is presented by Claude Elwood Shannon (Bednarik et al., 2010). The main idea of this method is that the larger variance in the number of criteria shows that criteria are more important (Wang and Lee, 2009). In fact, entropy is an uncertainty criterion that is expressed by a specific probability distribution, whatever opinions of FMEA criteria are more uncertain, and the important weight of the criteria also is larger than the other criteria.

For the calculating weight of each criterion the equations (13) to (18) are employed. (m is the number of options) (Wang and Lee, 2009):

Formula 13: $$P_{ij} = \frac{a_{ij}}{\Sigma_{i=1}^{n} a_{ij}}, \forall i,j$$

Formula 14: $$k = \frac{1}{ln(m)}$$

Formula 15: $$E_j = -k \, \Sigma_{i=1}^{m} [P_{ij} ln P_{ij}], \forall j$$

E_j shows the Shannon entropy of criteria j.

Formula 16: $$d_j = 1 - E_j, \forall j$$

Value d_j expresses uncertainty or degree of deviation for j criteria and since the Shannon entropy method gives the highest weight to criteria with the highest deviation degrees, therefore:

Formula 17: $$w_j = \frac{d_j}{\Sigma_{i=1}^{n} d_j}, \forall j$$

If λ_j is calculated weight by fuzzy AHP before applying Shannon entropy then the modified weight would be as follows.

Formula 18: $$\acute{w}_j = \frac{\lambda_j w_j}{\Sigma_{j=1}^{n} \lambda_j w_j}, \forall j$$

After determining the weight of each criteria, the prioritizing of risks could be executed based on Fuzzy TOPSIS as is shown in the next sub-section.

3.4 Fuzzy TOPSIS

TOPSIS method analyzes and prioritizes the selected options, based on the shortest distance from the positive ideal solution and the farthest from the negative ideal solution. For the first time, the fuzzy theory is used in this method by Chen and Hwang in 1992 (Kutlu and Ekmekçioglu, 2012; Ershadi et al., 2019). This method can be a good alternative for traditional FMEA which prioritizes failure modes and is helpful for achieving more accurate and reliable priorities. If the decision-makers are composed of K persons, then (Chen, 2000):

Formula 19: $$\tilde{x}_{ij} = (\tilde{x}^1{}_{ij}(+)\tilde{x}^2{}_{ij}(+)...(+)\tilde{x}^k{}_{ij})$$

$\tilde{x}^k{}_{ij}$ is ratio of decision makers K, according to criterion j for case i. By using pairwise comparisons we will have:

Formula 20: $$D = \begin{array}{c} \\ A_1 \\ A_2 \\ \vdots \\ A_m \end{array} \begin{array}{c} \begin{array}{cccc} C_1 & C_2 & ... & C_n \end{array} \\ \begin{bmatrix} \tilde{x}_{11} & \tilde{x}_{12} & ... & \tilde{x}_{1n} \\ \tilde{x}_{21} & \tilde{x}_{22} & ... & \tilde{x}_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ \tilde{x}_{m1} & \tilde{x}_{m2} & ... & \tilde{x}_{mn} \end{bmatrix} \end{array}$$

Formula 21: $$W = [w_1, w_2, ..., w_j] \quad j = 1,2,....n$$

$\tilde{x}_{ij}$ is the ratio of A_i with respect to criterion C_j and w_j is weight of this criterion and $\tilde{x}_{ij}$ is a triangular fuzzy number ($\tilde{x}_{ij} = (a_{ij}, b_{ij}, c_{ij})$). The linear scale transformation is applied for converting the various criteria scales into a comparable scale. Therefore matrix $\tilde{R}$ is obtained:

Formula 22: $$\tilde{R} = [\tilde{r}_{ij}]_{m \times n}$$

If C is set of cost criteria and B is a set of benefit criteria, then:

Formula 23: $$\tilde{r} = \left(\frac{a_{ij}}{c_j^*}, \frac{b_{ij}}{c_j^*}, \frac{c_{ij}}{c_j^*}\right), j \in B; \ (c_j^* = \max_i c_{ij}, if\ j \in B)$$

Formula 24: $$\tilde{r} = \left(\frac{a_j^-}{c_{ij}}, \frac{a_j^-}{b_{ij}}, \frac{a_j^-}{a_{ij}}\right), j \in C; \ (a_j^- = \min_i a_{ij}, if\ j \in C)$$

To consider the importance weights of criteria, the fuzzy normal weight matrix can be created as is shown below.

Formula 25: $$\tilde{V} = [\tilde{v}_{ij}]_{m \times n}, \ i = 1,2,....m, \ j = 1,2,....n$$

Formula 26: $$\tilde{v}_{ij} = \tilde{r}_{ij}(.)\, d\,(C_j)$$

Fuzzy positive ideal and fuzzy negative ideal solution are defined as follows.

Formula 27: $$A^* = (\tilde{v}_1^*, \tilde{v}_2^*, ..., \tilde{v}_n^*)$$

Formula 28: $$A^- = (\tilde{v}_1^-, \tilde{v}_2^-, ..., \tilde{v}_n^-)$$

Where

Formula 29: $$\tilde{v}^*{}_1 = (1, 1, 1), \tilde{v}^*{}_1 = (0, 0, 0) \qquad j = 1,2,3...,n$$

Distance of each case A^* and A^- is calculated as follows:

Formula 30: $$d_i^* = \Sigma_{j=1}^{n} d\,(\tilde{v}_{ij}, \tilde{v}_j^*), \quad i = 1, 2, 3..., m$$

Formula 31: $$d_i^- = \Sigma_{j=1}^{n} d\,(\tilde{v}_{ij}, \tilde{v}_j^-), \quad i = 1, 2, 3..., m$$

And distance of two fuzzy numbers is calculated as follows:

Formula 32: $$d(\tilde{\rho}, \tilde{\tau}) = \sqrt{\frac{1}{3}[(\rho_1 - \tau_1)^2 + (\rho_2 - \tau_2)^2 + (\rho_3 - \tau_3)^2]}$$

That $\tilde{\rho} = (\rho_1, \rho_2, \rho_3)$ and $\tilde{\tau} = (\tau_1, \tau_2, \tau_3)$ are two fuzzy number.

Finally, the closeness coefficient is calculated as follows:

Formula 33: $$CC_i = \frac{d_j^-}{d_j^* - d_j^-}, \quad i = 1, 2, ..., m$$

Items A_i are ranked according to close to number one.

In section 4, the application of proposed methodology in a real world RIS is demonstrated.

4. Case Study

Management of identifying and evaluating the information security software potential risks is worked according to the 5-step method (figure 1). In this paper, the predefined 5 steps are described that how have been applied for risk management of online dissemination system of Iranian theses and dissertations (GANJ). For this work firstly the main processes of GANJ are investigated and documented. Then the main assets and their potential failure modes of this system are identified. After that, the identified risks are prioritized and ranked using hybrid FMEA and MCDM techniques. Finally, risks which had the main priorities are selected for defining corrective actions. The following of this section is devoted to describing the GANJ steps. These stages could be extended to any other RIS.

4.1 The Main Processes of Research Information System

GANJ system is a research information system (RIS) for Iranian scientific researches metadata. Existing processes in this system are defined into three general sections that

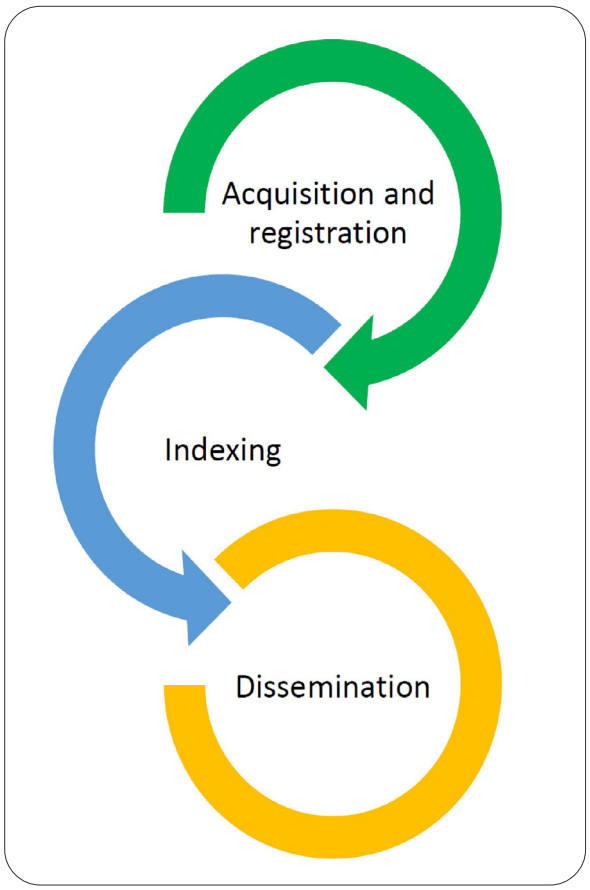

Figure 3. Three main processes of research information system

are respectively called (i) acquisition and registration of scientific document; (ii) indexing and (iii) dissemination (figure 3).

4.1.1 Acquisition and Registration Process

Inputs of acquisition and registration of scientific document processes in GANJ system are metadata related to theses and dissertations of Iranian students which are recorded by MS.C and Ph.D. students of Iranian universities. This process includes quality control operations implemented in all fields of metadata.

4.1.2 Indexing Process

The providing information process includes the preparation of documents and records of information. Quality control operations will be implemented in all of these subsections and processes mentioned for ensuring the validity of information in the system.

4.1.3 Dissemination Process

Editing metadata received from the indexing process and assigning a unified code to each record is done in this process. Overview of bibliographic information is reviewed too. If there is no problem, the document is approved and disseminated.

The main role of this process is storage and dissemination of metadata, but any quality problem is identified that the record would be returned again to the indexing unit.

In the following sub-section, the assets and their related risks are identified.

4.2 Identification of Assets and their Related Risks

The vulnerability is caused by a weakness in an asset or group of assets that can be exploited by threats, and the system will get attack or damage (Kiran, Reddy and Lakshmi Haritha, 2013). In this study, information assets of the studied system are analyzed according to the related software assets. Vulnerability term is identified as weaknesses in a system that allows an attacker to interfere in the integrity of the system (Kiran, Reddy and Lakshmi Haritha, 2013).

The software structure of any online RIS is comprised of the following components:

Internal Network: Operating systems, antivirus software, firewalls, applications.

Main Server: Operating systems, antivirus software, firewalls, database software, applications.

Internet: Interface software, antivirus software, applications, email services.

Regarding different software sections, information assets related to each section is described as follows:

Identified Failure Modes	Threatened Software Assets	The Non-compliance of Information Security	Code
Unauthorized access to the secure reports of the internal network (including correspondence, software and etc.)	Internal network and Main server	confidentiality of information	A1
Unauthorized access to information of personnel	Internal network		A2
Unauthorized access to View or change the stored information of server (such as security reports, backups).	Main server		A3
Unauthorized user access to operating systems and applications of the system.	Main server		A4
Unauthorized user access to basic Information of Website.	Internet, Main server and Internal network		A5
Unauthorized user access to emails sent and received by users.	Internet		A6
Unauthorized user access to full-text files of theses.	Internet the Main server		A7
Lack of access to authorized users to software and internal network security reports.	Internal network		B1
Lack of access to authorized users according to the classification specified to view or change information of the database, security reports, backups, applications and etc.	Main server	Availability of information	B2
Lack of access to authorized users to Website's basic Information and related email.	Internet the Main server		B3
Lack of access to authorized users to theses after authentication.	Internet the Main server		B4
A non-registered user on the Website.	Internet	Integrity of information	B5
Incomplete or disarray internal organizational correspondences.	Internal network		C1
Incomplete or incorrect or disarray emails sent and received by users.	Internet		C2
Incomplete or incorrect results of the user's transactions in Website.	Internet		C3
Incomplete or disarray user's article or thesis.	Internet the Main server		C4

Table 3. Identified failure modes of GANJ system

Internal Network: Internal correspondence, financial calculations, backup files, scheduled judgments, reports, specifications of employees and referees and etc.

Main Server: Articles, theses, the profile of user and referees, backup files, reports, coding and etc.

In this step, information failure modes are identified and classified according to the related software assets (Table 3). To do this stage, five experts from the organization which were professions in RIS and FMEA framework have been consulted. The next sub-section, assessing results based on experts' opinions are presented.

4.3 Application Results of the Proposed Model

In the following, identified failure modes are assessed based on the FMEA methodology in which its criteria are weighted by a combination of FAHP and Shannon entropy.

DEGREE OF DETECTION	PROBABILITY OF OCCURENCE	SEVERITY OF EFFECT	CODE
VG, G, MG, F, MP, P, P, P, VP	VP, P, MP, MP, F, F, MG, G, G	MP, MG, MG, MG, G, G, G, VG, VG	**A1**
G, G, MG, F, F, F, MP, P, P	P, P, P, MP, F, F, MG, G, VG	P, F, F, MG, MG, MG, MG, G, G	**A2**
G, G, MG, F, MP, MP, P, P, P	P, P, P, P, MP, MP, MP, MP, F	MP, MG, G, G, G, G, VG, VG, VG	**A3**
G, G, MG, MG, F, MP, MP, P, VP	P, P, P, P, MP, MP, MP, MP, G	VP, P, F, F, G, G, G, G, VG	**A4**
VG, G, G, G, MG, MP, MP, P, P	VP, P, P, MP, F, F, G, VG, VG	VP, MP, MP, F, MG, G, G, G, G	**A5**
G, MG, MG, MP, P, P, P, P, VP	VP, VP, P, MP, F, MG, G, G, G	MP, MP, MP, MG, G, G, G, G, VG	**A6**
VG, VG, G, MG, MG, F, MP, P, P	VP, P, P, MP, MP, MG, MG, G, VG	P, P, MG, G, G, VG, VG, VG, VG	**A7**
VG, VG, VG, VG, G, G, G, MP, MP	VP, P, MP, MP, F, MG, MG, G, G	VP, P, F, MG, MG, MG, MG, G, G	**B1**
VG, VG, G, G, MG, MG, MG, F, P	VP, VP, P, MP, F, F, MG, G, G	P, MP, MP, F, MG, G, G, G, VG	**B2**
VG, VG, G, G, MG, MG, F, F, MP	P, P, MP, MP, MP, MG, MG, G, G	VP, MP, F, F, F, MG, MG, G, G	**B3**
VG, VG, G, G, MG, F, F, VP, VP	VP, VP, P, MP, F, MG, G, G, VG	MP, MP, F, MG, MG, MG, G, VG, VG	**B4**
VG, G, G, G, MG, MG, MG, F, MP	VP, MP, MP, F, MG, G, G, G, VG	VP, VP, P, F, F, F, MG, MG, G	**B5**
VG, VG, G, G, MG, MG, MG, F, MP	P, MP, MP, MP, F, MG, G, G, G	VP, P, P, F, F, MG, MG, G, VG	**C1**
VG, VG, G, G, G, MG, MG, F, MP	VP, MP, MP, MP, MP, F, MG, G, G	P, MP, MP, F, F, F, MG, G,G	**C2**
G, G, G, G, G, MG, F, P, P	VP, P, MP, MP, MP, F, MG, MG, MG	VP, MP, MP, MP, MP, MP, F, MG, G	**C3**
	VP, P, MP, MP, F, F, MG, G, VG	P, P, F, F, MG, G, G, VG, VG	**C4**

Table 4. Points of the failure modes assessment according to the FMEA criteria

Then by using the calculated closeness coefficient with TOPSIS, the risks are prioritized.

4.3.1 Assessing the Identified Risks

The identified information software risks have been evaluated based on the fuzzy numbers as is shown in table 4. In this table each expert according to three criteria severity of effect, the probability of occurrence and degree of detection judges. Table 4 shows the results collected in this regard.

4.3.2 Determining the Weights of FMEA Criteria

In order to determine the important degree of three criteria, the severity of effect, probability of occurrence and degree of detection, the relative weight of criteria calculated with a hybrid of fuzzy AHP according to the experts pairwise comparisons and Shannon entropy. The results are shown in tables 5, 6 and 7.

According to the determined weights of criteria by fuzzy AHP (table 5), the probability of occurrence parameter with the weight of 0.4 has the most important weight. After that, the parameter severity of effect and probability of detection have weights 0.38 and 0.22.

According to the determined weights of criteria by Shannon entropy (table 6), the probability of detection with the weight of 0.42 has the most weight then the probability of occurrence and severity of effect have weights 0.31 and 0.27.

In table 7 final criteria weights are shown. These criteria have been calculated by a hybrid of fuzzy AHP and Shannon entropy based on the formula 18. According to this table, the probability of occurrence has the most weight.

4.3.3 Prioritizing the Identified Risks

Prioritization of failure modes according to the previously explained model has been done based on calculating closeness coefficient of any failure mode by using the fuzzy TOPSIS method. The inputs of fuzzy TOPSIS method are the expert fuzzy opinions of failure modes (table3) and the weights of FMEA criteria by using a hybrid of AHP and Shannon entropy (table 7). The calculated closeness coefficient and priority of risks are reported in table 8.

DEGREE OF DETECTION	PROBABILITY OF OCCURRENCE	SEVERITY OF EFFECT	CRITERIA
FW, FW, E, SS, SS, FS, FS, VS, VS	VW, FW, E, E, E, SS, SS, FS, VS	-	**SEVERITY OF EFFECT**
AW, AW, E, E, SS, FS, FS, VS, VS	-	-	**PROBABILITY OF OCCURRENCE**
-	-	-	**DEGREE OF DETECTION**
0.22	**0.40**	**0.38**	**CALCULATED WEIGHT**

Table 5. Pairwise comparisons of criteria and the weights of criteria by fuzzy AHP

DEGREE OF DETECTION	PROBABILITY OF OCCURRENCE	SEVERITY OF EFFECT	CRITERIA
0.42	**0.31**	**0.27**	**CALCULATED WEIGHT**

Table 6. The weights of criteria by Shannon entropy

DEGREE OF DETECTION	PROBABILITY OF OCCURRENCE	SEVERITY OF EFFECT	CRITERIA
0.30	**0.38**	**0.32**	**CALCULATED WEIGHT**

Table 7. The final weights of criteria

Risk Priority	Closeness Coefficient	Identified and Assessed Risk	CODE
5	0.37	Unauthorized access to the secure reports of internal network (including correspondence, software and etc.)	**A1**
6	0.34	Unauthorized access to information of personnel	**A2**
1	0.49	Unauthorized access to view or change the stored information of server (such as security reports, backups).	**A3**
3	0.39	Unauthorized user access to operating systems and applications of system.	**A4**
7	0.30	Unauthorized user access to basic Information of Website.	**A5**
2	0.41	Unauthorized user access to emails sent and received by users.	**A6**
10	0.26	Unauthorized user access to full-text files of theses.	**A7**
15	0.20	Lack of access to authorized users to software and internal network security reports.	**B1**
14	0.22	Lack of access to authorized users according to the classification specified to view or change information of the database, security reports, backups, applications and etc.	**B2**
12	0.26	Lack of access to authorized users to Website's basic Information and related email.	**B3**
9	0.28	Lack of access to authorized users to theses after authentication.	**B4**
8	0.30	A non-registered user on the Website.	**B5**
13	0.26	Incomplete or disarray internal organizational correspondences.	**C1**
11	0.26	Incomplete or incorrect or disarray emails sent and received by users.	**C2**
4	0.38	Incomplete or incorrect results of user's transactions in Website.	**C3**
16	0.19	Incomplete or disarray user's article or theses.	**C4**

Table 8. Prioritization of identified and assessed risks by fuzzy TOPSIS

Table 8 shows the results of application of proposed model on risk management of GANJ system. The risks with high importance degree are selected and corrective actions for reducing the severity of each risk are defined.

As is demonstrated in figures 3 and 4, the confidentiality of information is more important than other information security criteria. Furthermore failure modes in category of main server and internet have more priority in comparison to others. Therefore, organization would completely consider the confidentiality of information in main server and internet and would strengthen the confidentiality of information in these fields by planning the appropriate preventive and corrective actions.

The next section shows how the obtained results are validated.

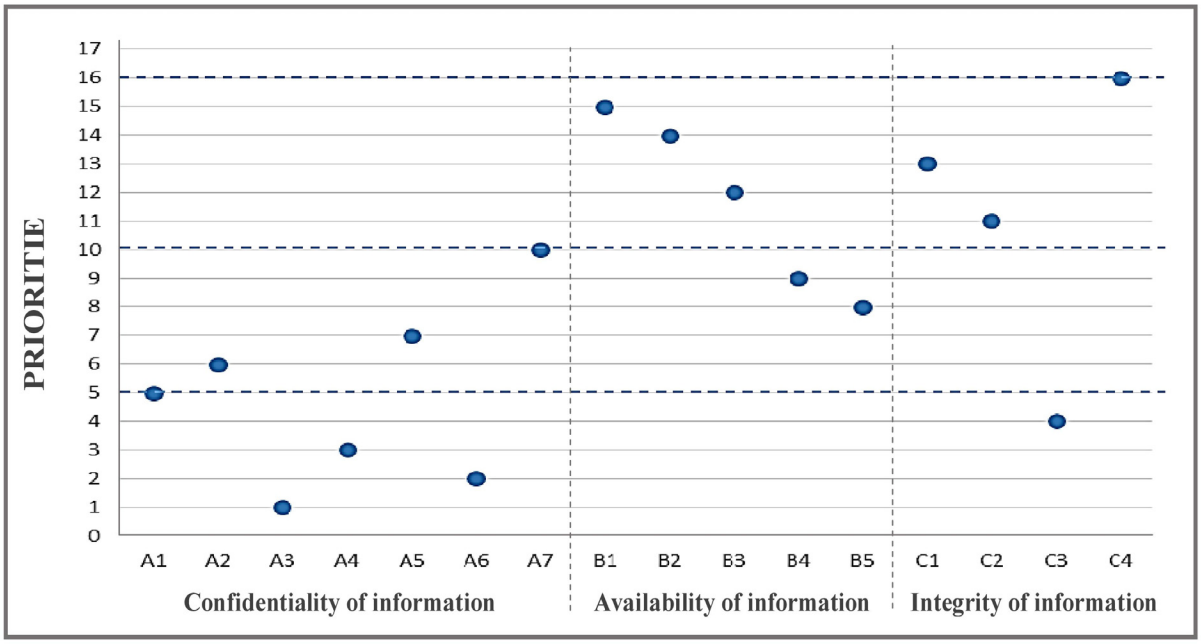

Figure 3. Prioritization of identified risks according to three criteria of information security

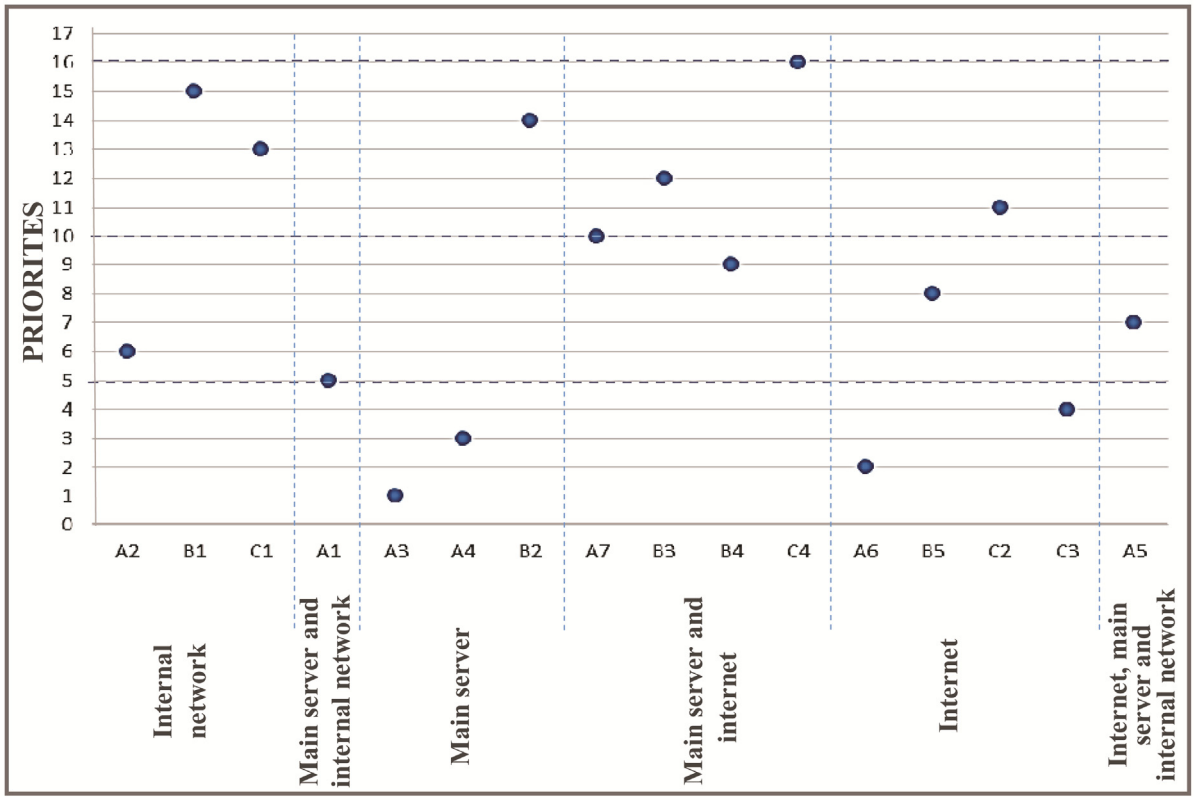

Figure 4. Prioritization of identified risks according to the software assets

5. Validation of the Framework using Comparative Study

Table 9 demonstrates a comparative study of different approaches which are applied to traditional FMEA and provides a framework to compare different combinations of methods. Results of table 8 show that the closest result to the result of the proposed model is the combination of fuzzy FMEA Shannon entropy and fuzzy TOPSIS. After that results of the combination of fuzzy FMEA with fuzzy TOPSIS is in the third rank based on nearing to the results of the developed model.

Results of table 8 show that in the risks prioritization problem of this study, the priorities of risks in four methods, fuzzy FMEA, the hybrid of fuzzy FMEA and Shannon entropy, the hybrid of fuzzy FMEA and fuzzy AHP and the hybrid of fuzzy FMEA, Shannon entropy and fuzzy AHP are the same. But the risks prioritization by adding fuzzy TOPSIS compared to results of the above four methods has been changed. Two methods, the hybrid of fuzzy FMEA and fuzzy TOPSIS and the hybrid of fuzzy FMEA, fuzzy TOPSIS and Shannon entropy are similar in nine risks prioritization and two methods, the hybrid of fuzzy FMEA and fuzzy TOPSIS and the hybrid of fuzzy FMEA, fuzzy TOPSIS and fuzzy AHP also are similar in other nine risks prioritization and the proposed approach is different with the above three methods, but in each of four methods, first priority risk is A1.

HYBRID OF F.FMEA & A.SHANNON & TOPSIS		HYBRID OF F.FMEA & TOPSIS		HYBRID OF F.FMEA & AHP& TOPSIS		HYBRID OF F.FMEA & AHP& A.SHANNON		HYBRID OF F.FMEA & AHP		HYBRID OF F.FMEA & A.SHANNON		FUZZY FMEA		PROPOSED MODEL		CODE OF RISK
PRIORITY	NEAR COFFICIET	PRIORITY	NEAR COFFICIET	PRIORITY	NEAR COFFICIET	PRIORITY	RPN	PRIORITY	RPN	PRIORITY	RPN	PRIORITY	RPN	PRIORITY	NEAR COFFICIET	
6	0.39	6	0.37	8	0.35	12	5.93	12	5.44	12	5.71	12	162.55	5	0.37	A1
7	0.36	9	0.35	9	0.34	11	5.98	11	5.48	11	5.76	11	163.96	6	0.34	A2
1	0.48	1	0.49	1	0.50	15	3.66	15	3.35	15	3.52	15	100.26	1	0.49	A3
4	0.40	5	0.39	4	0.39	16	3.62	16	3.31	16	3.48	16	99.10	3	0.39	A4
12	0.32	12	0.32	12	0.32	10	6.53	10	5.99	10	6.29	10	179.03	7	0.30	A5
2	0.44	2	0.42	5	0.39	13	4.46	13	4.09	13	4.30	13	122.21	2	0.41	A6
14	0.30	16	0.28	16	0.28	5	7.63	5	6.99	5	7.35	5	209.11	10	0.26	A7
11	0.34	11	0.32	11	0.33	2	8.74	2	8.01	2	8.42	2	239.60	15	0.20	B1
13	0.30	13	0.30	13	0.30	7	7.51	7	6.89	7	7.24	7	205.98	14	0.22	B2
10	0.34	10	0.33	10	0.34	8	7.50	8	6.87	8	7.23	8	205.57	12	0.26	B3
15	0.30	15	0.29	15	0.29	3	8.41	3	7.71	3	8.10	3	230.54	9	0.28	B4
5	0.39	4	0.40	3	0.40	6	7.56	6	6.93	6	7.28	6	207.13	8	0.30	B5
9	0.35	8	0.35	7	0.36	4	7.74	4	7.10	4	7.46	4	212.17	13	0.26	C1
8	0.35	7	0.36	6	0.36	9	7.29	9	6.68	9	7.02	9	199.75	11	0.26	C2
3	0.41	3	0.42	2	0.42	14	4.36	14	4.00	14	4.20	14	119.49	4	0.38	C3
16	0.29	14	0.29	14	0.29	1	8.85	1	8.11	1	8.53	1	242.65	16	0.19	C4

Table 9. A comparative study on prioritization of identified risks by different methods

In the next section some main discussions are provided.

6. Discussion

After application of FMEA as is seen in section 5 the most important risks of RIS are identified. Unauthorized access to view or change the stored information of server has the highest priority. This result is along with the results of Lateef and Omotayo (2019) and Gusamo et al. (2016). As is discussed by Aldini et al. (2017) unauthorized access of emails is the main risk which should be responded in ISRM. This risk faced with high priority in this study. Operating systems of information security have the main effect on risk management of RIS's as is implied in section 5, which is previously stated by Martinez-caro (2018). A trust-based opportunity-enabled risk management system (Aldini et al., 2017) could improve the efficiency of teamwork to respond promptly to the identified risks. The role and responsibilities of human resource in risk reduction as is presented in the previous section are inevitable as is illustrated by Stewart and Jurjens (2017) and also Lateef and Omatayo (2019).

Implementation of risk management systems based on FMEA is experienced in manufacturing and projected systems in previous studies (Wu et al., 2015; Panchal, 2018).On the other hand risk assessment in information systems recently is a state of the artwork (Aldini et al., 2017; De Gusamu et al., 2016). Also considering well-applied approaches in risk assessment such as FMEA in information systems are rarely studied. Hence in this paper, because of the importance of RIS's as the main category of information systems a risk management framework provided to improve the effectiveness of these systems.

In the next section some main conclusions and recommendations for future researches are provided.

7. Conclusions and some Recommendations for Future Researches

This study was prepared to identify and assess the information security software risk of an online research information system for Iranian dissertations and theses (called GANJ). In this research, potential failure modes have been identified by fuzzy FMEA which its criteria evaluated by experts than for reducing shortcomings of traditional FMEA method, the criteria are weighted by combining Shannon entropy and fuzzy AHP and failure modes are ranked by fuzzy TOPSIS. Result of application of the proposed model shows that risk priorities for improving information security of RIS's within a risk management program could be done. Comprehensive corrective actions and appropriate preventive actions to reduce the probability occurrence of non-compliance and severities of failures could be determined by applying the proposed model.

Although this study has been done regarding the risks of RIS's but can be continued and expanded to information security risks of other areas of information systems. Other risk management tools such as Bayesian networks, fault tree analysis (FTA) could be used for improving the effectiveness of FMEA method.

References

[1] Abdelgawad, M., Fayek, A. R. (2010). Risk management in the construction industry using combined fuzzy FMEA and fuzzy AHP. *Journal of Construction Engineering and Management*, 136 (9) 1028-1036.

[2] Aldini, Alessandro., Seigneur, Jean-Marc., Ballester Lafuente, Carlos., Titi, Xavier., Guislain, Jonathan. (2017). Design and validation of a trust-based opportunity-enabled risk management system, *Information & Computer Security*, 25 (1) 2-25.

[3] Azeroual, O., Saake, G., Abuosba, M. (2018). Data quality measures and data cleansing for research information systems. *Journal of Digital Information Management*, 16(1) 12–21.

[4] Azeroual, O., Saake, G., Schallehn, E. (2018). Analyzing data quality issues in research information systems via data profiling. *International Journal of Information Management*, 41, 50–56.

[5] Azeroual, O., Saake, G., Wastl, J. (2018). Data measurement in research information systems: Metrics for the evaluation of the data quality. *Scientometrics*, 115 (3) 1271–1290.

[6] Azeroual, O., Schöpfel, J. (2019). Quality Issues of CRIS data: An exploratory investigation with universities from twelve countries. *Publications*, 7 (1) 14.

[7] Bednarik, M., Magulova, B., Matys, M., Marschalko. M. (2010). Landslide Susceptibility Assessment of the Kral ovany–Liptovsky Mikulas Railway Case Study, *J. Physics and Chemistry of the Earth*, 35 (5) 162-171.

[8] Braglia, M., Frosolini, M., Montanari, R. (2003). Fuzzy criticality assessment model for failure modes and effects analysis, *International Journal of Quality & Reliability Management*, 20 (4) 503-524.

[9] Broderick, J. S. (2006). ISMS, security standards and security regulations, *Information Security Technical Report*, 11 (1) 26-31.

[10] Chang, D. Y. (1996). Applications of the extent analysis method on fuzzy AHP, *European Journal of Operational Research*, 95 (3) 649–655.

[11] Chang, K. -H., Chang, Y. -C., Lee, Y. -T. (2014). Integrating TOPSIS and DEMATEL Methods to Rank the Risk of Failure of FMEA, *International Journal of Information Technology & Decision Making*, 13 (6) 1229-1257.

[12] Chawla, A., Saxena, S. (2016). A confirmatory factor analysis of knowledge management assessment instrument in Indian higher educational institutions. *International Journal of Quality & Reliability Management*, 33 (7) 1019-1029.

[13] Chen, C. (2000). Extensions of the TOPSIS for group

decision-making under fuzzy environment, Fuzzy Sets and Systems, 114, p. 1–9.

[14] Gusmão, De., A. P. H. e Silva, L. C., Silva, M. M., Poleto, T., Costa, A. P. C. S. (2016). Information security risk analysis model using fuzzy decision theory, *International Journal of Information Management*, 36 (1) 25-34.

[15] Ershadi, M. J., Aiasi, R., Kazemi, S. (2018). Root cause analysis in quality problem solving of research information systems: a case study. *International Journal of Productivity and Quality Management*, 24 (2) 284-299.

[16] Ershadi, M. J., Ershadi, M. M. (2018). Implementation of failure modes and effects analysis in detergent production companies: A case study. *Environmental Quality Management,* 27 (3) 89-95.

[17] Ershadi, M. J., Roshanbin, N., Niaki, S. T. A. (2019). Multi-objective economic-statistical design of simple linear profiles using a combination of NSGA-II, RSM, and TOPSIS. Communications in Statistics-Simulation and Computation, 1-17.

[18] Feather, J., Sturges, P. (2003). International Encyclopedia of Information and Library Science, London: Routledge.

[19] Feledi, D., Fenz, S., Lechner, L. (2013). Toward web-based information security knowledge sharing, *Information Security Technical Report*, 17 (4) 199-209.

[20] Feng, N., Wang, H. J., Li, M. (2014). A security risk analysis model for information systems: Causal relationships of risk factors and vulnerability propagation analysis, *Information Sciences*, 256, 57-7.

[21] Rebelo, Ferreira., M., Silva, R., Santos, G. (2017). The integration of standardized management systems: managing business risk, *International Journal of Quality & Reliability Management*, 34 (3) 395-405.

[22] Stewart, Harrison., Jürjens, Jan. (2017). Information security management and the human aspect in organizations, *Information & Computer Security*, 25 (5) 494-534.

[23] Karabacaka, B., Sogukpinar, I. (2005). ISRAM: information security risk analysis method, *Computers & Security*, 24, 147-159.

[24] Kiran, K. V. D., Reddy, L. S. S., Haritha, Lakshmi., N. (2013). A Comparative Analysis on Risk Assessment Information Security Models, *International Journal of Computer Applications*, 82 (9) 41-47.

[25] Kutlu, A. C., Ekmekçioglu, M. (2012). Fuzzy failure modes and effects analysis by using fuzzy TOPSIS-based fuzzy AHP, *Expert Systems with Applications,* 39 (1) 61-67.

[26] Kwon, S., Jang, S., Lee, J., Kim, S. (2007). Common defects in information security management system of Korean companies, *Journal of Systems and Software*, 80 (10) 1631-1638.

[27] Lateef, A. and Omotayo, F.O., (2019). Information audit as an important tool in organizational management: A review of literature. *Business Information Review*, 25, 26-63.

[28] Liu, H. C., Liu, L., Bian, Q. H., Lin, Q. L., Dong, N., Xu, P. C. (2011). Failure mode and effects analysis using fuzzy evidential reasoning approach and grey theory, *Expert Systems with Applications*, 38 (4) 4403-4415.

[29] Liu, Hu-Chen, Liu, Lang, Liu, Nan. (2013). Risk evaluation approaches in failure mode and effects analysis: A literature review, *Expert Systems with Applications*, 40 (2) 828-838.

[30] Martinez-Caro, J. M., Aledo-Hernandez, A. J., Guillen-Perez, A., Sanchez-Iborra, R., Cano, M. D., (2018). A Comparative Study of Web Content Management Systems. *Information,* 9 (2) 27.

[31] Panchal, D., Mangla, S. K., Tyagi, M., Ram, M., (2018). Risk analysis for clean and sustainable production in a urea fertilizer industry. *International Journal of Quality & Reliability Management,* 35(7) 1459-1476.

[32] Ravi, V., Reddy, P. J., Zimmermann, H. J. (2001). Fuzzy rule base generation for classification and its minimization via modified threshold accepting, *Fuzzy Sets and Systems*, 120 (2) 271-279.

[33] Ritchie, B., Brindley, C. (2007). Supply chain risk management and performance: A guiding framework for future development, *International Journal of Operations & Production Management*, 27 (3) 303-322.

[34] Sachdeva, A., Kumar, D., Kumar, P. (2009). Multi-factor failure mode critically analysis using TOPSIS, J*ournal of Industrial Engineering International*, 5 (8) 1-9.

[35] Saleh, M. S., Alfantookh, A. (2011). A new comprehensive framework for enterprise information security risk management, *Applied Computing and Informatics*, 9 (2) 107-118.

[36] Sendi, A., Jabbarifar, S. M., Shajari, M., Dagenais, M. (2010). FEMRA: Fuzzy Expert Model for Risk Assessment, *In*: Fifth International Conference on Internet Monitoring and Protection, Barcelona, p. 48-53.

[37] Silva, M. M., de Gusmão, A. P. H., Poleto, T., Silva, L. C. e., Costa, A. P. C. S. (2014). A multidimensional approach to information security risk management using FMEA and fuzzy theory, *International Journal of Information Management,* 34 (6) 733-740

[38] Fenz, Stefan., Neubauer, Thomas. (2018). Ontology-based information security compliance determination and control selection on the example of ISO 27002, *Information & Computer Security,* 26 (5) 551-567.

[39] Vahidnia, M. Alesheikh, A. Abbas Alimohammadi (2009). Hospital site selection using fuzzy AHP and its derivatives, *Journal of Environmental Management,* 90 (10) 3048-3056.

[40] Wang, T., Lee, H. (2009). Developing a fuzzy TOPSIS approach based on subjective weights and objective weights. Expert Systems with Applications, 36 (5) 8980–8985.

[41] Wang, Y. M., Chin, K. S., Poon, G. K. K., Yang, J. B. (2009). Risk evaluation in failure mode and effects analysis using fuzzy weighted geometric mean, *Expert Systems with Applications*, 36 (2) 1195-1207.

[42] Wei, G., Xhang, X., Zhang, X., Huang, Z. (2010). Research on E-government Information Security Risk Assessment - Based on Fuzzy AHP and Artificial Neural Network Model, *In*: The 1st International Conference on Networking and Distributed Computing (ICNDC)

[43] Wu, X., Chen, L., Pang, S., Ding, X., (2015). A paratactic subjective-objective weighting methods and SVM risk assessment model applied in textile and apparel safety. *International Journal of Quality & Reliability Management,* 32 (5) 472-485.

[44] Yuan, T., Chen, P. (2012). International Workshop on Information and Electronics Engineering Data Mining Applications in E-Government Information Security, *Procedia Engineering*, 29, p. 235-240.

[45] Zadeh, L. A. (1996). Fuzzy logic: Computing with words, *IEEE Transactions on Fuzzy Systems*, 4 (2) 103-111.