Analytical Hierarchy Process in Fuzzy Comprehensive Evaluation Method

Potla Revathi¹

Abstract

The use of data innovation is expanding step by step ceaselessly and quickly, concerning expanding of innovation the security episodes likewise expanding. Presently days the innovation gets to be as a part of working together. In light of this innovations the dangers to an associations are likewise expanding quickly. These advances reasons number of security episodes and dangers. These dangers are rises step by step. To diminish every one of these things we need to dissect the danger which are brought on by the dangers. Hazard examination is an imperative apparatus keeping in mind the end goal to settle on right choices. This examination for the most part used to manage the digital dangers. In danger examination, we must perform ID and valuation of advantages. If the recognizable proof and valuation of a benefits are not performed appropriately that may result wrong choices in danger investigation. Already such a variety of systems are proposed yet those are exceptionally entangled. Chain of command based resource valuation technique is proposed. The target of this system is to decrease the quantity of blunders.

Keywords : hierarchy process, fuzzy, comprehensive evaluation, data framework, data innovation, AHP.

1. Introduction

Information technologies evolved from stand alone batch applications to modern interconnected mobile systems. This evolution resulted in the widespread use of information technologies by all types of companies. info technologies became AN indivisible a part of doing business these days. 20 years ago, most of the business methods were paper primarily based in virtually each organization but virtually each process depends on info technologies these days[1-3]. Therefore, while information systems started as tools for improving operational efficiency, later on, they acquired an indispensable role for the organization's survival .Parallel to the common use of information systems in organizations, threats and attacks on the information systems also increased rapidly[4-7]. Mobile equipment attract hackers' attention because of their widespread use. Mobile systems are also vulnerable to attacks. Number of security incidents and threats rises day by day. Since most of the business operations depend

Received(June 8, 2015), Review Result(1st: June 26, 2015, 2nd: July 30, 2015), Accepted(September 10, 2015)

¹(Corresponding Author) Department of Computer Science and Engineering, KL University
email: potlarevathi02@gmail.com

on information technologies, a threat to the information technologies means a threat to the business itself. Bulgurcu et al. state that some possible results of the information security incidents could be loss of credibility and monetary damage[8-10]. Farahmand et al. believes that impact on the business is a good indicator to determine the cost of a computer security incident. Other than the financial impact, security incidents may have effects on intangibles such as: The brand image, company reputation and goodwill in the market place, The financial status will get affected, Public and customers will lose the faith in the company, Companies reputation will be in dangerous, Maintaining the revenue will be an issue, The strategy to overcome the effects, Company can't meet the customer requirements.

Security danger analysis, generally known as hazard assessment, will be basic of the security about whatever association. It is key done guaranteeing that controls Also consumption would completely similar with the dangers will which the association will be presented. However, A large number accepted strategies for performing security danger dissection are getting to be an ever increasing amount untenable As far as usability, flexibility, What's more critically.

As far as the thing that they generate for those client. This site will be expected on investigate the fundamental components of risk, What's more to present An security hazard evaluation procedure Also device around which may be Notwithstanding utilized Toward a significant number of the planets significant companies. It also embraces the utilization of the same item will help guarantee agreeability for security policies, outside norms for example, ISO 17799 and for enactment for example, information security enactment. In this paper we have used only two methods quantitative and qualitative risk analysis methods but there are so many methods are available like fuzzy, analytical hierarchy process(AHP), fuzzy logic with AHP.

1.1 Analytical hierarchy process(AHP)

AHP enables us to take effective decisions on the complex issues by simplifying , expediting our natural decision making processes. There are two approaches which are fundamental to solve the problems. They are inductive (or systems) approach and deductive approach. Basically, the approach which focuses on the parts is deductive where as the systems approach focuses on the whole. Ahp combines these two fundamental approaches in to one integrated logic framework. AHP is designed to solve the complex problems by involving multi criteria.

Analytical hierarchy Process (AHP) is a method of breaking down unstructured, complex problems in to its component parts and arranging these parts(or variables) in a hierarchical

order; assigning the numerical values to the selective judgements based on the relative importance of each of the variable and synthesizing these judgements to determine which variables have the highest priority and these should be acted upon the outcome of the situation.

The best part about AHP is it consider both qualitative and quantitative approaches of the decision , expanding the decisions with one-to-one comparisons of the criteria, objectives, alternatives or constraints in the system model. The pairwise comparisons in the Analytical Hierarchical Process assumes that the decision maker or judgement experts can compare any two elements. for example, i and j are the two elements in the same level of hierarchy in the system, provides a numerical value I, J for the ratio of their importance. To describe the preference measures a scale of 1 to 9 is generally used, but for different applications other possible scales are also presented.

The AHP process requires the decision maker to make the judgements about the relative importance of each criterion and specify a preference for each of the decision alternatives on each criterion. The output of the Analytical Hierarchical Process is a prioritized ranking which indicates the overall preference for each of the decision alternatives.

Synthesizing the AHP procedure is:

Step 1. Structure a decision problem and select the criteria

Consider a product, it may be car, refrigerator etc., and take the criteria of the aspect. for example, security. Now take three objects to have the comparisons between them with respect to the criteria.

Step 2.prepare pairwise comparison matrix

Security	Obj A	Obj B	Obj C	Obj A	1	2	8	
	Obj B	$\frac{1}{2}$	1	6	Obj C	1/8	1/6	1

Sum the values in each column

security	Obj A	Obj B	Obj C	Obj A	1	2	8
	Obj B	$\frac{1}{2}$	1	6	Obj C	1/8	1/6

Sub totals 13/8 19/6 15

Step 3. Divide each element present in the matrix by its column total (estimating the relative weights in the matrix.)

Security Obj A Obj B Obj C Obj A 8/13 12/19 8/15 Obj B 4/13 6/19 6/15 Obj C 1/13 1/19 1/15

All the columns present in the normalized pairwise comparison matrix now have the sum of

1. Now do the average of the elements present in each row

Security	Obj A	Obj B	Obj C	Row avg	Obj A	0.615	0.632	0.513	0.593	Obj B	0.308	0.316	0.400
0.341	Obj C	0.077	0.053	0.067	0.066	total 1							

The values obtained in the normalized pairwise comparison matrix have been converted in to decimal form. The result is usually represented as the priority or relative vector. Here row average column is taken as a matrix.

Step 4. Checking the consistency

One of the important consideration in terms of quality is the ultimate decision relating to the consistency of judgement that the decision makers demonstrates during the pairwise comparisons. Perfect consistency is difficult to achieve and that lack of consistency is expected to occur in any set of pairwise comparisons. To handle this type of consistency AHP provides a method for measuring the degree of consistency present among the pairwise judgements provided by the decision maker.

If the degree of consistency is acceptable according to the preference scale, then the decision process can continue. If the degree of consistency is unacceptable then the decision maker should possibly reconsider and revise the pairwise judgements before preceeding the analysis.

1.2 Fuzzy comprehensive evaluation method:

Fuzzy comprehensive evaluation method helps us to reduce inconsistency and irregularities in the system. This will do the risk assessment process by defining a group of remarks such as excellent, good, medium, low etc., and then obtaining the evaluation matrices (single, multiple) from the evaluation scores given by experts. These matrices are that point consequently translated clinched alongside should participation weights for those enrollment capacity. Finally fuzzy transform computing is performed and we get the final evaluation result.

The steps present in the fuzzy comprehensive evaluation method are as follows:

Step 1. In this step the risk factors are fuzzy by defining a group of remarks such as excellent, good, middle, bad etc i.e, we establish the element and the grade factor sets. Here grade factor set = (excellent, good, middle, bad)etc., and element set $A = (a_1, a_2, a_3, a_4, \dots, a_n)$.

Step 2. Obtain the evaluation matrices from the evaluation scores given by experts.

The evaluation statistics table we consider should be approved by a certain or more number of experts which helps in determining the evaluation factors level in the information risk security.

Evaluation statistics given by experts sample:

Level Very high High Medium low Very low X11 0 2 5 9 6 X12 1 1 4 5 4 X13 1 1 3 10 7
X14 2 3 4 4 2 X21 0 5 5 6 3 X22 1 1 3 7 5 X23 0 3 8 12 4

For each element U_j in the element set U , r_{ij} is calculated.

$r_{ij} = n/m$, where n represents the number of U_j and m is the value of number of experts who approved the statistics table for evaluation. U_j . R is the fuzzy matrix on element U_j based on scale.

R = Single factor evaluation matrices are as follows

$U = [x_1, x_2]$, $U_1 = [x_{11}, x_{12}, x_{13}, x_{14}]$, $U_2 = [x_{21}, x_{22}, x_{23}]$

R_1 , R_2 are also calculated. The obtained result in these evaluations under normalized conditions and the sum of the value present in the row vector is 1.

Step 3. To get the comprehensive results of the evaluation.

The information security risk comprehensive results in single factor evaluation are

$B_i = W_i \cdot R_i = \{b_{i1}, b_{i2}, b_{i3}, b_{i4}, b_{i5}\}$ ($i=1,2$) B_1 , B_2 are calculated.

Step 4. Multi-level fuzzy comprehensive evaluation.

As per the synthetic evaluation result B_i , of risk factors V , the cluster to V is as follows

R = The evaluation of the indices U , we can make the synthetic evaluation. Its result is recorded as follows

$B = W \cdot R = \{b_1, b_2\}$

Step 5. Get the conclusion of the evaluation.

The synthetic evaluation result B is taken in to consider under the principle of maximum subordination. Evaluation levels will be like very low, low, medium corresponding to the maximum subordination in the given sets is taken as the conclusion.

1.3 Fuzzy-analytical hierarchy process (FUZZY-AHP)

The decision makers may be uncertain about his/her level of preference due to incomplete knowledge or information, complexity, can't able to take wise decision with and lack of

appropriate measure of scale. In such cases it is difficult to measure the crisp numerical values of the comparison ratios. AHP is structured, consistent and intuitive. However, AHP has a shortcoming that it can't handle the uncertainties properly.

A natural way to cope with these uncertain judgements is to propose an evaluation tool where the experts' judgements are translated into fuzzy sets or fuzzy numbers.

Fuzzy-AHP: Fuzzy-AHP utilizes fuzzy set hypothesis to express the questionable correlation judgements similarly as fuzzy numbers. Those primary steps about Fuzzy-AHP would be as follows:

1. Structuring the decision hierarchy

Comparable to customary AHP. Those to start with step will be on breakdown the intricate choice making issue under constituent parts. Also Building a progression.

2. Developing the pairwise fuzzy comparison matrices

Think about a prioritization issue. In a sure level with n elements, the pairwise examination matrices need aid to be eventually transformed into fuzzy triangular numbers. $A_{ij} = (l_{ij}; m_{ij}; u_{ij})$. Likewise in the traditional AHP, each set of correlations to a level obliges $n(n-1)/2$ judgments, which need aid further used to develop a certain fuzzy complementary correlation grid. $A = \{a_{ij}\}$ such-and-such.

3. Checking the consistency and deriving priorities

This checks the consistency and extracts those pairwise correlation matrices necessities. Though those pairwise examination matrices pass those consistency weight, fuzzy necessities can have a chance to be ascertained with those help about accepted fuzzy AHP routines. Therefore those necessity vector can be made from those correlation grid by applying the prioritization system.

4. Aggregation the priorities and ranking alternatives

This step aggregates the local priorities obtained at different levels of the decision hierarchy into composite global priorities for alternatives on the basis of weighted sum method.

Risk assessment of the information system. Firstly the hierarchy structure is constructed. Then the risk degree is calculated.

Constructing the hierarchy structure: AHP may be a choice methods with a lot of people guidelines with methodology variables which are was troublesome on be given a esteem. It could break down the confounded circumstance under the substantially simpler progression structure in place will examine step Toward step; it camwood express Also manage people's subjective judgment in quantity, What's more manage those specific and dubious factor, and Additionally recommended if the people's subjective judgment is straight. It tumbles under four steps to purpose issue by AHP. Those to start with step may be constructing the chain of importance structure. Those second venture is constructing the judge grid Eventually Tom's perusing utilization of variable examination. The third venture is ascertaining those relative weight of the factors Toward the judge grid. The most recent venture will be figuring the entirety weight of the variables toward each layer. In this paper, the polar to start with step is applied, Toward which hazard degree will be place forward and the fluffy legitimate technique is utilized.

Right away the progressive structure structure will be constructed. Those top banana layer will be those centering of the goal, which is characterized as "the paramount degree of the hazard factor" in the danger evaluation.

We define those lead of the second layer Similarly as "risk probability", "risk sway severity" Also "uncontrollability" since each danger element ought to analyze with one another(in the probabilit the effect seriousness What's more uncontrollability.

In this paper every hazard element may be unique in relation to another according of the Contrast of the framework. For instance, it will be those progressive structure structure of the hazard appraisal of the framework.

2. Risk Analysis

2.1 Description

Risk analysis is an important tool in order to make the correct decisions and to deal with the threats. So that initially we have to find the risk which are caused by the threats. In order to find the risk we require assets, vulnerability and threats. with these requirements we have to identify the risk and gives values to the risk analysis. Without proper understanding of the assets we shouldn't find risk which leads to wrong decisions. wrong decisions on information security may directly effect corresponding business process. Risk analysis is the process of

defining and analyzing the dangers to individuals, government agencies and the business firms so that the routine human life is not disturbed. In IT, a risk analysis report can be collaborated with a company's business objectives. Risk analysis can be done either by quantitative methodology or qualitative methodology.

2.1.1 What is meant by Risk

Risk is defined as a probabilistic function of a threat successfully attacking an asset through a specific vulnerability. The probability that an actual return on an investment will be lower than the expected return. A risk is not an uncertainty where neither the probability nor the mode of occurrence is known, a peril cause of loss, or a hazard something that makes the occurrence of a peril more likely or more severe. Financial risk is divided into the following categories: Basic risk, Capital risk, Country risk, Default risk, Delivery risk, Economic risk, Exchange rate risk, Interest rate risk, Liquidity risk, Operations risk, Payment system risk, Political risk, Refinancing risk, Reinvestment risk, Settlement risk, Sovereign risk and Underwriting risk.

What is an Asset: asset is defined as anything that has value to the organizations. determining the value of an asset is a crucial part of the risk analysis. An asset may be of anything which can be touchable or not but we will those characteristic properties of assets that has value to an organization. There are many types of assets. Some of these include machines like in the factory which add value to the organization , patents and also softwares. But certain things like services, information, and people these cant come under asset directly because these wont add value to the organization directly. There are 3 types of assets are available 1.Hardware assets 2.Software assets 3.Information assets

Hardware assets: Hardware assets can be grouped into four different categories:

1. Computer assets,
2. Network assets,
3. Removable media assets, and
4. Peripheral assets

Software assets: Software Assets can be classified into four different categories: Commercial software is software which was bought by the vendors without changing its source code. QuickBooks Pro, Microsoft Word comes under commercial software. Customized software is also a type of commercial software where some changes has made to the original code so that the new software will meet the requirements perfectly. The term legacy software describes that

the aging software can be used according to the present requirements by modifying the software that has been existed before and this which will reduce the cost of software, designing which will indirectly help the organization in terms of revenue.

Homemade software is a freeware software and it is non-commercial one. But with this it is restricted to limited people.

Information assets: Anything that has worth to the agency which will be communicated or documentary material, no matter its physical type or characteristics. Includes, however isn't restricted to, paper, electronic, digital, images, and voice mail. Information technology hardware and computer code aren't info assets for classification functions.

Classification of information assets: Those end goal will be on affirm information advantages square measure known, appropriately classified, and guarded for their lifecycles. Those objective is should create Furthermore actualize all the methods that empower office will continually survey and arrange its data holdings.

Vulnerability: Vulnerability is a defect in an asset, that may be used by a threat to attack an a information system.

Vulnerability could be a defect in Associate in Nursing plus, that may be employed by a threat to attack an a system. A vulnerability could be a weakness in Associate in Nursing plus or cluster of assets. Associate in Nursing asset's weakness might permit it to be exploited and injured by one or a lot of threats. A vulnerability is additionally ordinarily outlined as a flaw in during a in Associate in Nursing exceeding in a very package element.

The previous definition is a lot of general, since it considers not solely package elements vulnerabilities however conjointly equally relevant structure aspects.

Types of vulnerabilities: Physical vulnerabilities, Natural vulnerabilities, Hardware and software vulnerabilities, Media vulnerabilities, Emanation vulnerabilities, Communication vulnerabilities, Human vulnerabilities

Threat: Any circumstance or event that can impact structure operations including mission, functions, image, reputation, structure assets, or people through associate degree data system via unauthorized access, destruction, disclosure, modification of data, and denial of service.

Also, the potential for a threat-source to with success exploit a specific data system vulnerability. So that quality, vulnerability and threat square measure the safety parameters by mistreatment that solely we've got to search out the danger.

The risk function can be given by $\text{Risk} = f(\text{asset}, \text{vulnerability}, \text{threat})$. Threats to information systems may impact confidentiality, integrity and/or availability of an asset. Threats may operate in several ways such as destruction (the asset is not recoverable), modification (changing the representation of an asset), disclosure (violation of need-to-know), and denial of service. Common threats to an information system are 1) Act of Human Error or Failure like accidents, employee mistakes 2) Compromises to Intellectual Property like piracy, copyright infringement 3) Unauthorized access and/or data collection 4) Deliberate Acts of Information Extortion 6) Deliberate Acts of Theft illegal confiscation of equipment or information 7) Software attacks like viruses, 8) Forces of Nature means fire, flood, earthquake, lightning. 9) Failures in technical Hardwares 10) Failures in technical softwares.

2.1.2 Risk analysis process:

Risk Analysis process starts with the identification of assets. Once an asset is identified, its confidentiality, integrity and availability are processed. Some assets also have legal and contractual requirements and violation of these may cause risk to an organization. Threats, that can attack an asset, are also identified along with the corresponding vulnerabilities. The requirements that are taken care of in the proposed methodology are as follows:

Confidentiality Requirement [C]: Alludes all the of the insurance for data from unapproved get alternately unintentional revelation. It may be a graded parameter. What's more will be scaled from a quality about 1 will 5. Quality about 1 will be doled out with publicly accessible benefits and to Exceedingly private benefit a quality for 5 will be doled out.

Integrity Requirement [I]: Alludes of the culmination. Also precision about majority of the data i. E. Insurance of information, data, alternately transmissions from unauthorized, uncontrolled, alternately unintentional alterations. It will be a graded parameter. Also will be scaled from a esteem about 1 will 5.

Availability Requirement [A]: Ensures that majority of the data systems, and the necessary information and services, need aid accessible will sanctioned clients for use when they would necessary. It will be An graded parameter. Also a esteem for 1 on 5 will be allocated with an benefit relying upon the level of accessibility prerequisite for that advantage.

Authenticity Requirement [Au]: Alludes of the confirmation of the legitimacy about Possibly an individual or from claiming information. Information Confirmation may be An consolidation of Confirmation Furthermore information integument. It serves as a verification that "you need aid who you say you would or what you claim will be".

2.1.3 Risk analysis methods:

Danger dissection comprises of recognizing it assets, identikit dangers with the individuals assets, and deciding the defenselessness for asset(s) will threat(s). There would a number for dissimilar methodologies on danger dissection. There are a large number methodologies presently being used that endeavor on measure those reduction presentation from claiming it possessions. These methodologies might make sorted Likewise quantitative or qualitative. In any case of the procedure used, it ought further bolstering have specific alluring properties. In it ought make adequate will management, those client community, and the data frameworks Branch. Second, despite the fact that no single danger dissection procedure might think about all risks, it ought further bolstering be as far reaching Likewise possible, What's more have the capacity will handle. New technologies Third, it should be logically sound. Fourth, it should be practical— meaning that it should deliver optimum protection for ihe cost. Fifth, it should be open to continuing evaluation from all parties. Sixth, it should be conducive to learning, accompanied by clear documentation and records of deliberations. So that The risk can be calculated by using the two methods:

1. Qualitative risk analysis method
2. Quantitative risk analysis method .

Quantitative method: Most quantitative methods are based on regarding loss exposure as a function of the vulnerability of an asset lo a threat multiplied by the probability of the threat becoming a reality. These methods are called "expected value analyses," and include annualized loss expectancy (ALE). Quantitative risk analysis methods use mathematical tools like fuzzy logic to assess the risk. Quantitative methods try to calculate annualized loss expectancy in monetary value for each threat and find the cost of a possible damage. Courtney method, Livemore Risk Analysis Methodology (LRAM), Information Security Risk Analysis Method (IS RAM), and ALE using program evaluation review technique (PERT) are instances of quantitative risk analysis methods. Quantitative methods require a solid mathematical

background to assess information security risks and implementation of these methods requires more time and effort than qualitative methods.

3. Conclusion

We talked about that in both existing strategy and also in proposed philosophy just resources are recognized utilizing different components, however in these techniques we didn't ascertain the remaining parameters like helplessness and danger. So that gauge of any danger is impractical. Now in our proposed system we figured the danger utilizing each of the three security parameters. For that we need to discover the danger component to appraise the danger. The danger element can be computed by utilizing the advantage worth and security concern. As said resource quality can be figured as the capacity of security, business and legitimate prerequisites. So that subsequent to computing the danger element we can discover the danger utilizing all accessible security parameters. So by utilizing these security parameters we can assess the danger in any space of a data framework. By consolidating the benefit values and hazard calculate the danger of any data framework can be estimate. The minimization of danger depends on the estimations of the security parameter.

References

- [1] B. Westerman, How do people really use the iPhone, Report. Create with Context, (2008).
- [2] F. Boström, P. Nurmi, P. Floréen, T. Liu, T.-K. Oikarinen, A. Vetek, and P. Boda, Capricorn - An Intelligent User Interface for Mobile Widgets, Proceedings of the 10th international conference on Human computer interaction with mobile devices and services, (2008), ACM; Amsterdam, The Netherlands
- [3] M.. Böhmer and G. Bauer, Exploiting the icon arrangement on mobile devices as information source for context-awareness, in Proceedings of the 12th international conference on Human computer interaction with mobile devices and services. (2010), ACM; Lisbon, Portugal
- [4] N. Maiden, S. Jones, K. Karlsen, R. Neill, K. Zachos, and A. Milne, Requirements engineering as creative problem solving: a research agenda for idea finding, in Requirements Engineering Conference (RE), (2010) 18th IEEE International.
- [5] T. Wasserman, Software engineering issues for mobile application development, Proceedings of the Workshop on Future of Software Engineering Research (FoSER), (2010).
- [6] T. Snowsill, I. Flaounas, T. De Bie, and N. Cristianini, Detecting events in a million New York Times articles, in Machine Learning and Knowledge Discovery in Databases: Springer, (2010).

- [7] X. Wei, X. Luo, Q. Li, J. Zhang, and Z. Xu, Online Comment-Based Hotel Quality Automatic Assessment Using Improved Fuzzy Comprehensive Evaluation and Fuzzy Cognitive Map, *IEEE Transactions on Fuzzy Systems*, **(2015)**, Vol.23, No.1, pp.72-84.
- [8] W. Li, W. Liang, L. Zhang, and Q. Tang, Performance assessment system of health, safety and environment based on experts' weights and fuzzy comprehensive evaluation, *Journal of Loss Prevention in the Process Industries*, **(2015)**, Vol.35, pp.95-103.
- [9] J. Cho and J. Lee, Development of a new technology product evaluation model for assessing commercialization opportunities using Delphi method and fuzzy AHP approach, *Expert Systems with Applications*, **(2013)**, Vol.40, pp.5314-5330.
- [10] J. F. Chen, H. N. Hsieh, and Q. H. Do, Evaluating teaching performance based on fuzzy AHP and comprehensive evaluation approach, *Applied Soft Computing*, **(2015)**, Vol.28, pp.100-108.