International Journal of Innovative Computing, Information and Control
Volume **8**, Number **11**, November **2012**

ICIC International ©2012 ISSN 1349-4198
pp. **8019–8032**

INFORMATION SECURITY RISK ASSESSMENT: BAYESIAN PRIORITIZATION FOR AHP GROUP DECISION MAKING

Zeynep Filiz Eren-Dogu and Can Cengiz Celikoglu

Department of Statistics
Dokuz Eylül University
Buca, İzmir 35160, Turkey
zferendogu@gmail.com; cengiz.celikoglu@deu.edu.tr

Received July 2011; revised December 2011

Abstract. *Increasing complexity of risk management requires the use of more flexible approaches to measure information security risk. Adapting complex risk analysis tools in today's information systems is a very difficult task due to the shortage of reliable data. Analytic Hierarchy Process group decision making (AHP-GDM) offers a technical support for risk analysis by taking the judgements of managers and systematically calculating the relative risk values. This paper presents how Bayesian Prioritization procedure (BPP) provides a more effective way of risk assessment than proposed by the conventional approaches used in AHP-GDM.*

Keywords: Information security, Risk assessment, Analytic hierarchy process (AHP), Group decision making (GDM), Bayesian prioritization procedure (BPP)

1. Introduction.

Information security risk management is a recurrent process of identification, assessment and prioritization of risks, where risk could be defined as a possibility that a threat exploits a particular vulnerability in an asset and causes damage or loss to the asset. Risk management has two primary activities, risk assessment and risk control. Risk assessment is a very important decision mechanism which identifies the information security assets that are vulnerable to threats, calculates the quantitative or qualitative value of risk (or expected loss), and prioritizes risk incidents. In an organization, in the past, a single manager was used to be the responsible staff to protect information systems where, nowadays, a group of managers could take the responsibility of this task or participate in the risk analysis process. As risk analysis becomes a cross-functional decision making process, researchers seek ways to develop new risk analysis methods which allow a group of people to participate.

Although risk is well defined and practical for decision making, it is often difficult to calculate a priori [1]. Due to the difficulty in adapting complex risk analysis tools in today's information systems, researchers have proposed new techniques which are capable of analyzing information security risk properly. A number of quantitative and qualitative risk analysis methods have been developed.

The quantitative approaches use mathematical and statistical tools to represent risk as a function of the probability of a threat and the expected loss due to the vulnerability of the organization to this threat [2,3]. Due to the shortage of reliable data on incidents (probabilities and impacts), quantitative approaches may not yield reliable results. Consequently, security or risk management professionals mostly prefer qualitative methods rather than quantitative ones. In qualitative methods, estimated risk is calculated using only the estimated potential loss instead of the probability data. These approaches depend on the ideas of the analyst so they are subjective and might yield inconsistent results

[4]. There is not a single risk evaluation method which is best under all circumstances and for all purposes. Some researchers claimed that neither of the quantitative and qualitative approaches could properly model the assessment process alone. Alternatively, some of them developed comprehensive approaches combining both the quantitative and the qualitative approaches [2,3,5]. The Analytic Hierarchy Process (AHP), first proposed by T. L. Saaty [6], is one of the most widely used multi-criteria decision technique which can combine qualitative and quantitative factors for prioritizing, ranking and evaluating alternatives [7]. It allows multiple actors, criteria and scenarios to be involved in the analysis [8].

Previously, AHP analysis was used as support for an organization's information security system to evaluate the weights of risk factors [9], to determine the optimal allocation of a budget [10], to evaluate the weighting factors needed to combine risk measures [2], to obtain the indices' weights with respect to the final goal of the security evaluation [11], to select information security policy [12], and to establish e-commerce information security evaluation [13]. Zhang et al. [14] proposed calculating a relative risk value with Analytic Hierarchy Process group decision making (AHP-GDM) instead of calculating the actual value of the risk. They mentioned that the loss could be measured by the value of assets, and that probability of risk could be described in an equation with the danger degree of threat and vulnerability as its two variables.

The AHP method is operable and efficient as it prioritizes and orders risk incidents, which could also satisfy the aim of risk management. However, there might be some complexities when using AHP-GDM for information security risk evaluation. For instance, in AHP-GDM, it is assumed that the pairwise comparison matrices containing the judgements expressed by decision makers are complete and accurate. In real life, decision makers might provide only incomplete information due to following situations: (1) some of the decision makers may have limited expertise about the problem domain or the AHP analysis; (2) decision makers participated in the analysis would prefer to concentrate on the risk assessment itself rather than the AHP tool being implemented in the risk analysis; (3) they may have difficulties in making pairwise comparisons efficiently as the number of elements (assets, threats and vulnerabilities) in the problem increase. Moreover, the practitioner may also prefer to ignore the inconsistent or opposing judgements while keeping the consistent or homogeneous ones in order to increase the consistency or consensus among decision makers. Altuzarra et al. [15] proposed a Bayesian prioritization approach for AHP-GDM which can naturally be extended to the case of incomplete pairwise comparison matrices. Contrary to the conventional prioritization methods applied in AHP-GDM [16-18], this technique does not require intermediate filters for decision makers' initial judgements.

The paper aims at providing an effective and practical group decision mechanism to prioritize the risk incidents. We propose using BPP based AHP-GDM for information security risk evaluation, which is a remedy for the complexities mentioned above. This approach provides flexibility to the group of participants when expressing their judgements, and to the risk analysts, who may not be professional AHP practitioners, by treating incomplete or inconsistent judgements properly. We compare the method with the conventional approach used in the AHP-GDM and the results show that the proposed methodology performs more robust manner and calculates the final priorities with smaller MSE than the conventional approach. Other advantages of this technique can be listed as follows: it can easily be adapted to any information security standard by updating the elements in the problem, and can be used alone or with any other information security risk analysis methods as a support.

The remainder of this paper is as follows. The relevant theoretical background of the AHP-GDM approach and the Bayesian prioritization procedure for the AHP-GDM is briefly presented in Section 2. In Section 3, an illustrative example is provided to show how the proposed method can be implemented to calculate the relative values of risk incidents. The main results of the illustrative example are also given here. Finally, Section 4 summarizes the conclusions obtained from this study.

2. Background.

2.1. AHP group decision making (AHP-GDM).

The AHP was developed by Saaty [6] in order to deal with problems which involve consideration of multiple criteria simultaneously. It has been extensively applied in complex decision-making problems of choice, prioritization and evaluation. Its ability to synthesize both tangible and intangible characteristics, to accommodate both shared and individual values and monitor the consistency with which a decision-maker makes his judgements made the AHP a widely used multiple criteria decision making (MCDM) tool [19]. The AHP has particular applications in individual and group decision making. According to many researchers AHP is an effective and flexible tool for structuring and solving complex group decision situations [15,17,19].

The AHP comprises of four stages: modeling, valuation, prioritization and synthesis. In the modeling stage, a hierarchy which describes the problem is constructed. The overall goal or mission is placed at the top of the hierarchy. The main attributes, criteria and subcriteria are placed in the subsequent levels below. In the evaluation stage, decision makers compare all the criteria with regard to goal and then all the alternatives with respect to each criterion. Their preferences are included as pairwise comparison matrices in the analysis and they are based on the fundamental scale proposed by Saaty [6]. In the prioritization stage, the local priorities are derived by calculating the eigenvalues of the comparison matrix of each element and global priorities are derived using the hierarchic composition principle. In the last stage, the global priorities for each alternative are synthesized in order to get their total priorities.

There are different methods to accommodate the judgements of decision makers in a group setting [8]. Saaty [16] suggests one of the two methods to proceed: decision makers make each paired comparison individually, or the group is required to achieve consensus on each paired comparison. If individual's paired comparison ratio judgements are gathered, the AHP literature describes different methods for the prioritization and synthesis procedures [6,20,21]. The two conventional procedures to obtain group priorities are the aggregation of individual judgements (AIJ) and the aggregation of individual priorities (AIP). Based on individual judgements, a new judgement matrix is constructed for the group as a whole in AIJ procedure and the priorities are computed from the new matrix. In the AIP method, the total priorities are obtained on the basis of individual priorities using one or other aggregation procedure. Synthesis of the model can be done using an aggregation procedure. The weighted geometric mean method is the most commonly used technique for both [22].

2.2. Bayesian prioritization procedure (BPP) for AHP-GDM.

Bayesian methods allow the treatment of missing data or incomplete information using data augmentation techniques [23]. The integration of high-dimensional functions has been the major limitation towards the wide application of Bayesian analysis before Markov Chain Monte Carlo (MCMC) methods was introduced.

There are very few references to Bayesian analysis in the AHP literature. [24] provided a Bayesian extension of their regression formulation of the AHP. [25] used MCMC methods to calculate the posterior distributions of judgements and estimated the vector of priorities and the most likely rankings. [15] provided a Bayesian prioritization procedure (BPP) for AHP group decision making that does not require filters for the initial judgements of the decision makers. This procedure is based on the prior assumption of the existence of consensus among the decision makers. Unlike the AIJ and the AIP methods, this process uses weightings that are inversely proportional to the decision makers' levels of inconsistency and is more efficient when compared to them. This method also can be extended to the case of incomplete pairwise comparison matrices, which is a common problem in complex decision making problems. For such cases, [15] showed that BPP performs much more robust manner than the conventional methods, especially with regard to consistency.

2.2.1. *Statistical model.* Assuming a single criterion, and a set of n alternatives, $A_1, \ldots, A_n$, let $D = D_1, \ldots, D_r$, $r \geq 2$ be a group of r decision makers, each express individual pairwise comparisons with regard to the criterion considered, resulting in r reciprocal judgement matrices, $R^{(k)}$, $k = 1, \ldots, r$. Their preferences are based on the fundamental scale proposed by Saaty [5]. $R^{(k)} = (r_{ij}^{(k)})$ is a positive square matrix $(n \times n)$ which validates $(r_{ii}^{(k)}) = 1$, $(r_{ij}^{(k)}) = 1/(r_{ji}^{(k)}) > 0$ for $i, j = 1, \ldots, n$. The judgements $(r_{ij}^{(k)})$ represent the preference of the decision maker, D_k, when a comparison between A_i and A_j is required.

Let $v^G = (v_1^G, \ldots, v_n^G)$ and $w^G = (w_1^G, \ldots, w_n^G)$, $w_i^G = v_i^G / \sum_{j=1}^n v_j^G$ be the group's unnormalized and normalized priorities for the alternatives, respectively.

As traditionally employed in stochastic AHP [20,24], a multiplicative model with log-normal errors is applied in the Bayesian analysis of the model. If the decision makers express all possible judgements, the model will be

$$r_{ij}^{(k)} = \frac{v_i^G}{v_j^G} e_{ij}^{(k)},\ i, j = 1, \ldots, n,\ k = 1, \ldots, r, \tag{1}$$

with $e_{ij}^{(k)} \sim LN(0, \sigma^{(k)2})$, $i < j$. Taking the logarithms and eliminating the reciprocal judgements, a regression model with normal errors is obtained given by:

$$y_{ij}^{(k)} = (\mu_i^G - \mu_j^G) + \varepsilon_{ij}^k,\ i = 1, \ldots, n-1,\ j = 1, \ldots, n,\ k = 1, \ldots, r, \tag{2}$$

where $\varepsilon_{ij}^k \sim N(0, \sigma^{(k)2})$. Here, A_n is established as the benchmark alternative ($\mu_n = 0 \iff v_n = 1$). In matrix notation, model can be written as:

$$\boldsymbol{y}^{(k)} = \boldsymbol{X}\boldsymbol{\mu}^G + \boldsymbol{\varepsilon}^{(k)},\ \text{with}\ \boldsymbol{\varepsilon}^{(k)} \sim N_t(\boldsymbol{0}, \sigma^{(k)2}\boldsymbol{I}), \tag{3}$$

where $\boldsymbol{y}^{(k)} = (y_{12}^{(k)}, y_{13}^{(k)}, \ldots, y_{n-1n}^{(k)})'$, $\boldsymbol{X}_{t \times n-1} = (x_{pq})$ with $x_{pi} = 1$, $x_{pj} = -1$ and $x_{p\lambda} = 0$, if $\lambda \neq i, j$, $\lambda = 1, \ldots, n-1$ and $p = \frac{2n-i}{2}(i-1) + (j-1)$ with $1 \leq i < j \leq n$, $x_{pi} = 0$ and $x_{p\lambda} = 0$, if $\lambda \neq i$, $\lambda = 1, \ldots, n-1$ and $p = \frac{2n-i}{2}(i-1) + (n-i)$, $\boldsymbol{\mu}^G = (\mu_1^G, \mu_2^G, \ldots, \mu_{n-1}^G)$, $k = 1, \ldots, r$, $\boldsymbol{\varepsilon}^k = (\varepsilon_{12}^k, \varepsilon_{13}^k, \ldots, \varepsilon_{n-1n}^k)'$ and $t = n(n-1)/2$.

With a constant non-informative distribution as the prior distribution for the vector of log-priorities, $\boldsymbol{\mu}^G$, the posterior distribution of $\boldsymbol{\mu}^G$ for complete and precise information is given by:

$$\boldsymbol{\mu}^{\boldsymbol{G}} \mid \boldsymbol{y} \sim N_{n-1}(\hat{\boldsymbol{\mu}}_B, \hat{\boldsymbol{\Sigma}}_B), \tag{4}$$

where $\hat{\boldsymbol{\mu}}_B = \frac{\sum_{k=1}^r \tau^{(k)} \hat{\boldsymbol{\mu}}^{(k)}}{\sum_{k=1}^r \tau^{(k)}}$ and $\hat{\boldsymbol{\Sigma}}_B = \left(\sum_{k=1}^r \tau^{(k)}\right)^{-1} (\boldsymbol{X}'\boldsymbol{X})^{-1} \begin{pmatrix} 2/n & 1/n & \cdots & 1/n \\ 1/n & 2/n & \cdots & 1/n \\ \vdots & \vdots & \ddots & \vdots \\ 1/n & 1/n & \cdots & 2/n \end{pmatrix}$,

$\tau^{(k)} = 1/\sigma^{(k)2}$ and $\boldsymbol{y} = (\boldsymbol{y}^{(1)'}, \boldsymbol{y}^{(2)'}, \ldots, \boldsymbol{y}^{(r)'})'$.

For the conventional procedure, AIP, the most commonly used method to aggregate group judgements is the geometric mean method. It can be presented as:

$$\hat{\boldsymbol{\mu}}_{AIP} = \frac{1}{r}\sum_{k=1}^{r} \hat{\boldsymbol{\mu}}^{(k)}, \tag{5}$$

where $\hat{\boldsymbol{\mu}}^{(k)} = (\hat{\mu}_1^{(k)}, \ldots, \hat{\mu}_{n-1}^{(k)})$ with $\hat{\mu}_i^{(k)} = \bar{y}_{i.}^{(k)} - \bar{y}_{n.}^{(k)}$. The other conventional procedure, AIJ, is not mentioned in this study since [15] showed that it gives almost the same results with the AIP method. Further information and theorems can also be found in [15].

2.2.2. *Incomplete information.* Most MCDM methods are based on the assumption that complete information about the model parameters (scores, attribute weights) need to be elicited as 'exact' point estimates [26]. According to [27], decision makers might provide only incomplete information in real life. The reasons for the incomplete information are as follows: (1) a decision might be made under pressure of limited time and lack of data; (2) many of the attributes might be intangible or non-monetary because they reflect social and environmental impacts; (3) decision makers might have limited attention and information processing capabilities; and (4) all participants might not have equal expertise about the problem domain in group settings. As a consequence, all of the decision makers may not express the $n \times (n-1)/2$ possible judgements in the reciprocal pairwise comparison matrix or may express inconsistent judgements. There are many methods proposed to overcome this problem (see [26] for more information). BPP can also naturally be extended to the case of incomplete information, where it performs more robust manner compared with the conventional methods in terms of consistency. In such cases, the equations of model (3) could be expressed as:

$$\boldsymbol{y}^{(k)} = \boldsymbol{X}\boldsymbol{\mu}^{G} + \boldsymbol{\varepsilon}^{(k)}, \tag{6}$$

with $\boldsymbol{\varepsilon}^{(k)} \sim N_{t_k}(\mathbf{0}, \sigma_k^2 \boldsymbol{I}_{t_k})$, $k = 1, \ldots, r$; and in the matrix form it can be expressed as:

$$\boldsymbol{y} = \boldsymbol{X}(\mathbf{1}_r \otimes \boldsymbol{I}_{n-1})\boldsymbol{\mu}^{G} + \boldsymbol{\varepsilon} \quad \text{with} \quad \boldsymbol{\varepsilon} \sim N_t(\mathbf{0}, \boldsymbol{D}) \tag{7}$$

where $\boldsymbol{y} = (\boldsymbol{y}^{(1)\prime}, \boldsymbol{y}^{(2)\prime}, \ldots, \boldsymbol{y}^{(r)\prime})'$, $\boldsymbol{X} = diag(\boldsymbol{X}^{(1)}, \boldsymbol{X}^{(2)}, \ldots, \boldsymbol{X}^{(r)})$, $\boldsymbol{\varepsilon} = (\boldsymbol{\varepsilon}^{(1)}, \boldsymbol{\varepsilon}^{(2)}, \ldots, \boldsymbol{\varepsilon}^{(r)})'$ and $\boldsymbol{D} = diag(\sigma^{(1)2}\boldsymbol{I}_{t_1}, \ldots, \sigma^{(r)2}\boldsymbol{I}_{t_r})$. $\mathbf{1}_r = (1, 1, \ldots, 1)'$, t_k is the number of judgements issued by each decision maker D_k, $t = t_1 + \ldots + t_r$ is the total number of judgements by all decision makers and $\otimes$ denotes the Kronecker product.

With a constant non-informative distribution as the prior distribution for the vector of log-priorities ($\boldsymbol{\mu}^G$), the posterior distribution of $\boldsymbol{\mu}^G$ for incomplete and precise information is given by:

$$\boldsymbol{\mu} \mid \boldsymbol{y} \sim N_{n-1}(\hat{\boldsymbol{\mu}}_B, \hat{\boldsymbol{\Sigma}}_B), \tag{8}$$

where

$$\begin{aligned}
\hat{\boldsymbol{\mu}}_B &= \left(\sum_{k=1}^{r} \tau^{(k)} \boldsymbol{X}^{(k)\prime} \boldsymbol{X}^{(k)}\right)^{-1} \left(\sum_{k=1}^{r} \tau^{(k)} \boldsymbol{X}^{(k)\prime} \boldsymbol{y}^{(k)}\right)^{-1} \\
&= \left((\mathbf{1}_r \otimes \boldsymbol{I}_{n-1})\left(\boldsymbol{X}'\boldsymbol{D}^{-1}\boldsymbol{X}\right)(\mathbf{1}_r \otimes \boldsymbol{I}_{n-1})\right)^{-1} (\mathbf{1}_r \otimes \boldsymbol{I}_{n-1})\left(\boldsymbol{X}'\boldsymbol{D}^{-1}\boldsymbol{y}\right), \\
\hat{\boldsymbol{\Sigma}}_B &= \left(\sum_{k=1}^{r} \tau^{(k)} \boldsymbol{X}^{k\prime} \boldsymbol{X}^{k}\right)^{-1}.
\end{aligned}$$

The estimator of μ^G obtained by means of the AIP procedure is given by:

$$\begin{aligned}\hat{\boldsymbol{\mu}}_{AIP} &= \frac{1}{r}\sum_{k=1}^{r}\hat{\boldsymbol{\mu}}^{(k)} = \frac{1}{r}\sum_{k=1}^{r}(\boldsymbol{X}^{(k)\prime}\boldsymbol{X}^{(k)})^{-1}(\boldsymbol{X}^{(k)\prime}\boldsymbol{y}^{(k)}) \\ &= \frac{1}{r}(\mathbf{1}_r \otimes \boldsymbol{I}_{n-1})(\boldsymbol{X}'\boldsymbol{X})^{-1}(\boldsymbol{X}'y). \end{aligned} \tag{9}$$

3. Information Security Risk Assessment Example.

Let us consider the group decision analysis situation on information security risk assessment taken from [14]. They defined 3 criteria ($\{C_1, C_2, C_3\}$), which are assumed to have the same weights; confidentiality, integrity and availability, and 3 key factors conducting the security risk assessment; assets ($\{A_1, \ldots, A_m\}$, $m = 5$), threats ($\{T_1, \ldots, T_s\}, s = 6$), and vulnerabilities ($\{V_1, \ldots, V_h\}, h = 6$) based on GB/T20984: Risk Assessment Specification for Information Security. The key factors are given in Table 1.

Table 1. List of assets, threats and vulnerabilities

Assets	Threats	Vulnerabilities
A_1-Service	T_1-Physical environment influences	V_1-Physical damages
A_2-Data	T_2-Hardware and software breakdowns	V_2-Network vulnerabilities
A_3-Software	T_3-Malicious code	V_3-Operating systems vulnerabilities
A_4-Hardware	T_4-Ultra vires	V_4-Application systems vulnerabilities
A_5-People	T_5-Cyber attacks	V_5-Application middleware vulnerabilities
	T_6-Management problems	V_6-Problems in technique and organization

We noted that the AHP-GDM analysis could contain some complexities here. For example, the decision makers participated in the analysis might have limited expertise about some of the factors in the analysis so they might express incomplete or inconsistent judgements. They also might not have sufficient information about the AHP analysis and its requirements or they might have limited attention which may result in inconsistent situations. Moreover, expressing complete and consistent judgements is difficult with a large number of attributes and alternatives, since there are 3 criteria, 5 assets, 6 threats and 6 vulnerabilities (which requires 183 different judgements for one decision maker at total) in the model. Consequently, we aimed to solve this problem with the AHP-GDM based on BPP in order to show that it would present a more practical and flexible way of information security risk assessment.

In this study, there are three AHP models to be analyzed. The first AHP model given in Figure 1 is established for calculating the priorities of assets ($A_1, \ldots, A_5$), with respect to the attributes: confidentiality (C_1), integrity (C_2) and availability (C_3). The importance of these three attributes might be different for each organization so we assumed that all

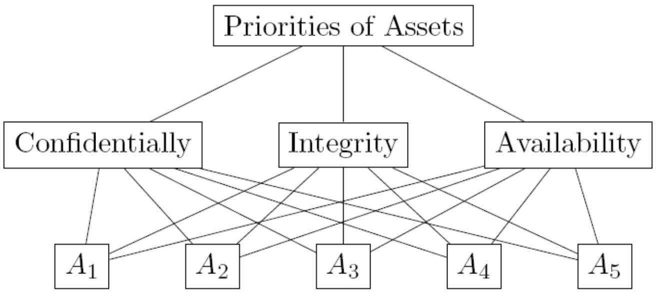

Figure 1. AHP decision tree for asset prioritization

three factors have the same importance in this study. The overall goal is placed at the top of the hierarchy. The attributes are placed in the second layer, and the assets are in the third layer, which is the "alternatives" layer.

The second and the third AHP models are constructed in order to calculate the danger degree of threats ($T_1, \ldots, T_6$) and vulnerabilities ($V_1, \ldots, V_6$) in terms of each asset respectively. Figure 2 shows the decision tree for the danger of threats model. A similar model is prepared for the vulnerabilities.

Since we assumed that the attributes in the first AHP model are equal, we did not require any comparisons for them. So, for each AHP models, we had 3, 5 and 5 different set of pairwise comparisons to be completed by each decision makers respectively. We assumed that there is a cross-functional team composed of 5 decision makers from various departments, who are not forced to give complete answers to the pairwise comparison matrices. In order to illustrate this case, we simulated data based on the fundamental scale proposed by Saaty [6] for each set of pairwise comparison matrices that are presented in Tables 2-4. In Table 2, the simulated pairwise comparisons for the first AHP model are given, where 5 assets are compared by 5 decision makers in terms of C_1, C_2 and C_3. In the first model, D_2 did not compare A_3 with A_5, and D_5 did not compare A_3 with A_5 in the second one, which resulted in incomplete judgement situations.

The opening coefficients (oc_{ij}) reflect the variability of judgements expressed by decision makers, and are calculated by: $Max_k(r_{ij}^k)/Min_k(r_{ij}^k)$, $k = 1, \ldots, 5$, $1 \le i < j \le n$. In this study we omitted the most inconsistent judgements which cause oc_{ij} to be large. In Table

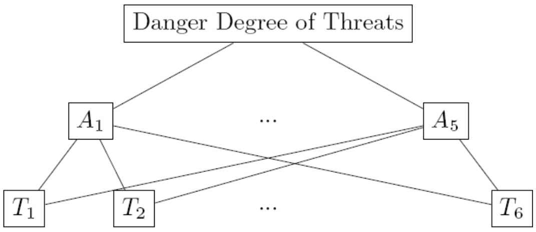

FIGURE 2. AHP decision tree for threat prioritization

TABLE 2. Simulated pairwise comparisons of 5 assets in terms of 3 attributes

$A_i - A_j$ pairs		1-2	1-3	1-4	1-5	2-3	2-4	2-5	3-4	3-5	4-5
C_1	D_1	1/4	2	5	2	7	9	5	2	1	1/3
	D_2	1/3	4	7	3	5	8	5	1	NA	1/2
	D_3	1/2	3	7	5	9	9	4	3	3	**2**
	D_4	**2**	5	9	2	7	6	2	1	1	1/4
	D_5	1/2	3	6	**1/3**	9	5	5	**1/3**	2	1/3
	$oc_{ij} \ge 8$	8			15				9		8
C_2	D_1	1/3	2	5	2	7	9	5	2	1	1/3
	D_2	1/4	3	9	2	7	6	2	1	1	1/4
	D_3	1/2	3	7	5	9	9	4	3	3	1/3
	D_4	1/3	3	6	**1/3**	9	5	5	2	2	1/3
	D_5	1/2	4	7	3	5	8	5	**1/3**	NA	**2**
	$oc_{ij} \ge 8$				15				9		8
C_3	D_1	1/4	2	5	2	7	7	5	2	1	1/3
	D_2	1/4	3	6	2	7	6	2	1	1	1/4
	D_3	1/2	4	7	5	9	7	3	3	3	1/3
	D_4	1/2	3	8	4	9	5	3	**8**	2	1/3
	D_5	1/3	4	7	3	**1**	8	4	3	2	**3**
	$oc_{ij} \ge 8$					9			8		12

Table 3. Simulated pairwise comparisons of 6 threats in terms of 5 assets

$T_i - T_j$ pairs		1-2	1-3	1-4	1-5	1-6	2-3	2-4	2-5	2-6	3-4	3-5	3-6	4-5	4-6	5-6
A_1	D_1	1/5	1/3	1/3	1/7	2	3	3	1/4	5	2	1/3	7	1/4	3	9
	D_2	1/4	1/3	1/2	1/5	1	3	3	1/2	6	1	1/4	3	1/3	3	9
	D_3	1/5	NA	1/5	1/5	1	5	6	1/3	5	1	1/4	4	1/2	3	**1**
	D_4	1/4	1/2	1/2	NA	2	2	3	**3**	7	1	1/7	**1/2**	1/5	2	7
	D_5	1/5	**3**	1/2	1/3	1/2	3	4	1/3	4	1	1/3	5	1/6	2	7
A_2	D_1	1/4	1/7	1/9	1/9	1/2	1/3	1/5	1/4	3	1/2	1/3	2	1	5	9
	D_2	1/3	1/6	1/9	1/9	1/2	1/2	1/3	1/5	1	1/2	1/3	2	1/2	5	7
	D_3	1/3	1/7	1/8	1/8	1	1/3	1/3	1/5	2	1	1/4	3	1/2	6	8
	D_4	1/5	1/8	**1**	1/7	2	1/2	1/4	1/3	1	1/3	1/5	1	1	**1/3**	7
	D_5	1/2	NA	1/7	1/9	1/2	1/2	**2**	1/4	3	**4**	1/5	2	1/2	4	9
A_3	D_1	1/9	1/7	1/2	1/5	1/2	2	6	3	9	4	2	6	1/2	1	3
	D_2	1/7	1/7	1	1/4	1/3	1	7	4	9	5	3	3	1/2	1	2
	D_3	1/5	**2**	1/2	1/5	NA	4	5	3	7	3	5	3	1	2	3
	D_4	1/9	1/5	1/3	1/8	1/2	**1/2**	8	2	8	7	2	5	1/3	1	3
	D_5	1/6	1/6	3	1/7	1/2	3	6	3	9	6	3	**1/3**	1	2	1
A_4	D_1	1/4	3	6	3	1/4	9	7	5	2	2	1/2	1/7	1/4	1/9	1/6
	D_2	1/5	4	7	2	1/2	9	9	4	2	1	1/3	1/5	1/4	1/9	1/3
	D_3	1/5	2	5	2	1/3	7	8	6	3	3	NA	1/6	1/3	1/7	**2**
	D_4	1/4	3	6	4	1/2	1	8	**1/2**	3	2	1/4	1/7	1/3	1/9	1/7
	D_5	1/6	**1/2**	6	3	1/3	7	9	5	2	3	1/3	**2**	1/4	1/7	1/5
A_5	D_1	5	4	1/2	5	1/3	1	1/8	1	1/9	1/5	1	1/9	**1/2**	1/4	1/9
	D_2	4	4	1	6	1/3	1	1/7	2	1/9	1/3	2	1/7	6	1/2	1/8
	D_3	4	6	1/2	7	1/4	1/2	1/5	1/2	1/6	1/4	3	1/9	7	1/3	1/7
	D_4	8	5	1/3	5	1/2	1/2	1/9	2	1/8	1/8	2	1/8	4	1	1/7
	D_5	**1**	7	1	4	1/3	2	1/8	1	1/7	**1**	3	1/9	8	1/3	1/9

2, the oc_{ij} line is presented to illustrate the omitting procedure, but the same procedure is applied for each matrix. Tables 3 and 4 give the simulated pairwise comparisons for the second and third AHP models, where 6 threats and 6 vulnerabilities are compared by 5 decision makers in terms of 5 different assets respectively.

In Tables 2-4, the incomplete judgements are written as "NA" and the judgements which are selected to be omitted are given in bold. It can be concluded that five decision makers have a consensus in general, where D_1 and D_2 are the most consistent ones and D_5 is the most inconsistent one. Some decision makers, especially D_3 and D_5 preferred not to express some of the pairwise comparisons. Looking at the oc_{ij} line, it can also be noted that D_4 and D_5 seem to pay less attention compared to others since the omitted judgements mostly belong to them.

It is assumed that consensus exists among the decision makers with regard to the priorities for each alternative. The degree of inconsistency for each decision maker ($\sigma^{(k)2}$) is assumed to be known and below the threshold. We used the inconsistency levels ($\sigma^{(k)2}$) = $(0.127, 0.043, 0.243, 0.272, 0.431)$ extracted from the first AHP model.

Both the AIP method and the BPP have been applied for aggregating judgements in group AHP analysis respectively. After omitting the judgements given in bold, the methods are repeated and are named as AIP* and BPP*. Tables 5-7 show the priorities of assets, threats and vulnerabilities with $MSE = \Sigma^n_{1\leq i\leq j}\Sigma^r_{k=1}\varepsilon^{(k)}_{ij}/\Sigma^r_{k=1}t_k$ for each method. For different AHP models, each method gives similar weights and almost same ranking but the Bayesian estimates reflect more robust results since the priorities (w_i) does not change too much after omitting the inconsistent judgements. Out of the assets, "data" is the most important one, which is followed by "service". The order for the priorities of assets in terms of the main criteria is $A_2 > A_1 > A_5 > A_3 > A_4$. The priorities

Table 4. Simulated pairwise comparisons of 6 vulnerabilities in terms of 5 assets

$V_i - V_j$ pairs		1-2	1-3	1-4	1-5	1-6	2-3	2-4	2-5	2-6	3-4	3-5	3-6	4-5	4-6	5-6
A_1	D_1	1/4	1/3	1/9	1/8	5	1	1/3	1/2	3	1/4	1/2	2	2	8	4
	D_2	1/4	1/3	1/9	1/6	3	1	1/7	2	2	1/3	1/2	3	3	8	5
	D_3	1/3	**3**	1/8	1/5	5	1/2	1/5	1/2	4	1/4	1	1	1	9	6
	D_4	1/3	1/2	1/7	1/7	5	1/2	1/4	2	3	1/8	1/5	1/2	2	5	3
	D_5	1/5	1/4	1/7	1/8	3	2	1/8	1	**1/3**	1/3	1/3	4	3	1	5
A_2	D_1	1	1/2	1/9	1/8	1/2	1	1/3	1/2	1/2	1/2	1/2	1/2	2	4	3
	D_2	1/2	1/3	1/9	1/7	1/2	1	1/3	1/2	1/2	1/5	1/2	1/2	3	4	3
	D_3	1/2	1/3	1/8	1/8	NA	1/2	1/5	1/2	1/3	NA	1	1	1	5	4
	D_4	1	1/2	1/9	1/9	3	1/2	1/4	1/3	1/4	**3**	1/5	1/2	2	3	3
	D_5	2	1/4	1/9	1/9	1/2	2	1/8	1	1	1/3	1/3	1/8	3	**1/3**	2
A_3	D_1	1/4	1/6	1/8	1/4	1/2	1/4	1/7	1/3	1/2	1	2	3	2	4	1
	D_2	1/2	1/7	1/9	1/5	1/3	1/4	1/7	1/2	1/2	1/2	3	3	3	4	2
	D_3	NA	1/9	1/8	1/3	1/2	1/3	1/6	1/4	1	NA	1	4	4	5	3
	D_4	1/3	1/7	1/9	NA	1/5	**4**	1/8	1/3	1/2	1/2	2	**1/5**	3	6	3
	D_5	**3**	1/6	1/7	1/4	1/3	1/4	1/6	1/2	**4**	1/3	3	**1/3**	3	2	2
A_4	D_1	5	2	3	8	1/2	1	2	1	1/5	2	1	1/2	1	1/7	1/8
	D_2	4	2	5	6	1/2	1/2	2	2	1/5	3	3	1/2	1	1/9	1/9
	D_3	3	3	3	8	1	1	3	1	1/4	1	2	1/3	2	1/6	1/8
	D_4	8	1	5	7	1/3	1/2	1	3	**3**	3	3	1/4	1/2	1/8	1/6
	D_5	**1**	NA	5	9	1/3	1/3	1	2	1/2	4	**1/3**	1	1	1/9	1/9
A_5	D_1	2	1/3	2	1/2	1/6	1/5	1/4	1	1/9	2	5	1/2	3	1/3	1/9
	D_2	2	1/3	2	2	1/7	1/4	1/5	2	1/8	3	4	1/3	3	1/4	1/8
	D_3	4	**3**	4	1	1/8	1/3	1/4	2	1/8	2	6	1/2	4	1/5	1/7
	D_4	3	1/2	1	1/2	1/6	1	1/2	1	1/7	1	3	1	5	1/3	1/9
	D_5	3	1/2	**1/2**	1/2	1/7	1	NA	NA	1/9	2	7	1/3	1	**4**	1/8

Table 5. Group priorities for assets estimated by each method

	Assets	A_1	A_2	A_3	A_4	A_5
A_i of C_1	AIP	0.263	0.489	0.083	0.057	0.108
	Bayesian	0.263	0.496	0.081	0.055	0.106
	AIP*	0.332	0.418	0.079	0.068	0.104
	Bayesian*	0.305	0.448	0.078	0.061	0.108
A_i of C_2	AIP	0.241	0.511	0.091	0.052	0.105
	Bayesian	0.239	0.506	0.090	0.051	0.114
	AIP*	0.274	0.480	0.090	0.048	0.108
	Bayesian*	0.263	0.484	0.088	0.048	0.118
A_i of C_3	AIP	0.272	0.467	0.114	0.050	0.098
	Bayesian	0.257	0.480	0.104	0.050	0.110
	AIP*	0.271	0.467	0.100	0.049	0.112
	Bayesian*	0.256	0.479	0.094	0.050	0.120

of threats and vulnerabilities change for each asset. For example, T_2 (hardware and software breakdowns) is the most dangerous threat for A_1, A_3 and A_4 (service, software and hardware respectively), where it is the least dangerous threat for A_5 (people).

Table 8 shows the mean square errors (MSE) of different prioritization methods for each of the AHP models, in which the value of assets and then the danger degree of threats and vulnerabilities are evaluated. $WMSE$ is the weighted average of MSE's, which could be calculated as: $WMSE = \Sigma_{i=1}^{m} w_i MSE_i/m$, where w_i is the weight of the attribute and MSE_i is the MSE of the group when comparing the alternatives in terms

Table 6. Group priorities for threats estimated by each method

	Threats	T_1	T_2	T_3	T_4	T_5	T_6
T_j of A_1	AIP	0.082	0.309	0.120	0.180	0.234	0.076
	Bayesian	0.072	0.293	0.121	0.159	0.297	0.058
	AIP*	0.084	0.278	0.146	0.229	0.177	0.085
	Bayesian*	0.074	0.275	0.141	0.182	0.268	0.059
T_j of A_2	AIP	0.041	0.110	0.158	0.305	0.314	0.072
	Bayesian	0.037	0.098	0.155	0.287	0.359	0.065
	AIP*	0.040	0.099	0.211	0.316	0.260	0.075
	Bayesian*	0.036	0.092	0.185	0.305	0.319	0.063
T_j of A_3	AIP	0.048	0.427	0.244	0.073	0.136	0.072
	Bayesian	0.046	0.422	0.259	0.070	0.135	0.069
	AIP*	0.050	0.473	0.201	0.103	0.108	0.065
	Bayesian*	0.047	0.457	0.227	0.085	0.116	0.068
T_j of A_4	AIP	0.142	0.411	0.062	0.034	0.108	0.243
	Bayesian	0.144	0.412	0.054	0.033	0.101	0.257
	AIP*	0.154	0.395	0.040	0.040	0.127	0.243
	Bayesian*	0.148	0.397	0.040	0.034	0.108	0.273
T_j of A_5	AIP	0.187	0.047	0.057	0.226	0.042	0.442
	Bayesian	0.190	0.047	0.057	0.222	0.042	0.442
	AIP*	0.203	0.044	0.070	0.189	0.059	0.435
	Bayesian*	0.197	0.044	0.064	0.212	0.047	0.437

Table 7. Group priorities for vulnerabilities estimated by each method

	Vulnerabilities	V_1	V_2	V_3	V_4	V_5	V_6
V_k of A_1	AIP	0.059	0.129	0.107	0.432	0.225	0.049
	Bayesian	0.056	0.131	0.111	0.443	0.213	0.045
	AIP*	0.056	0.128	0.147	0.469	0.137	0.062
	Bayesian*	0.054	0.131	0.139	0.465	0.160	0.051
V_k of A_2	AIP	0.054	0.103	0.129	0.365	0.221	0.129
	Bayesian	0.051	0.101	0.122	0.378	0.221	0.127
	AIP*	0.054	0.099	0.156	0.354	0.240	0.097
	Bayesian*	0.051	0.098	0.139	0.369	0.234	0.108
V_k of A_3	AIP	0.044	0.077	0.294	0.337	0.149	0.100
	Bayesian	0.041	0.073	0.292	0.353	0.144	0.097
	AIP*	0.036	0.092	0.368	0.254	0.141	0.109
	Bayesian*	0.035	0.082	0.337	0.311	0.135	0.100
V_k of A_4	AIP	0.276	0.114	0.128	0.060	0.080	0.342
	Bayesian	0.273	0.100	0.131	0.056	0.062	0.377
	AIP*	0.277	0.115	0.117	0.056	0.094	0.342
	Bayesian*	0.273	0.100	0.123	0.054	0.069	0.381
V_k of A_5	AIP	0.114	0.071	0.216	0.155	0.080	0.364
	Bayesian	0.105	0.060	0.211	0.126	0.059	0.440
	AIP*	0.113	0.076	0.228	0.119	0.131	0.333
	Bayesian*	0.105	0.064	0.220	0.112	0.082	0.418

Table 8. MSE values for each method

	Methods	AIP	BPP	AIP*	BPP*
A_i	Con.	0.391	0.392	0.281	0.235
	Int.	0.348	0.351	0.183	0.188
	Ava.	0.348	0.352	0.265	0.281
	$WMSE$	0.362	0.365	0.243	0.235
T_j	A_1	0.578	0.414	0.510	0.317
	A_2	0.450	0.402	0.321	0.199
	A_3	0.382	0.379	0.312	0.222
	A_4	0.431	0.435	0.286	0.211
	A_5	0.293	0.293	0.330	0.266
	$WMSE$	0.466	0.394	0.377	0.245
V_k	A_1	0.486	0.478	0.301	0.190
	A_2	0.740	0.736	0.661	0.602
	A_3	0.510	0.514	0.513	0.396
	A_4	0.388	0.340	0.371	0.245
	A_5	0.516	0.452	0.645	0.378
	$WMSE$	0.604	0.593	0.568	0.461

of the i^{th} attribute. Among four approaches, BPP* generally provided the minimum $WMSE$, and conventional approaches did not provide lower values of $WMSE$ than BPP*. Consequently, BPP* results are selected for further implementation of risk evaluation.

Table 9 reflects the final value of all risk incidents $\left(R_{ijk} = \left(a_i \times \sqrt{t_{ij} \times v_{ik}}\right)\right)^{1/2}$, the danger degree of threats for each asset $\left(R_{ij} = \Sigma_{k=1}^{h} R_{ijk}/h\right)$, and the danger degree order of all assets (R_i) which could be determined by maximum, minimum or average value of R_{ij} for each asset. Here we used the equations of [14]. According to Table 9, the risk incidents can be ordered as: $R_{254} > R_{244} > R_{255} > \ldots > R_{445} > R_{434} > R_{444}$, with the highest value, 0.392 and the lowest, 0.051. It can be concluded that risk incidents associated with A_2 and A_1 have higher values, where the ones associated with A_4 have lower values. For A_2, the danger degree of T_j in descending order is $T_5 > T_4 > T_3 > T_2 > T_6 > T_1$, which means that the "cyber attacks" and "ultra vires" are the most dangerous threat for "data". For A_3, the order is $T_2 > T_3 > T_5 > T_4 > T_6 > T_1$, which means that the "hardware and software breakdowns" and "malicious code" are the most dangerous threats for "software". Similar conclusions can be drawn from Table 9 for the remaining cases.

For the whole system, the danger degree order of assets can also derived by comparing the maximum, minimum or average value of R_{ij} for each asset. Consequently, the danger degree order of A_i is $A_2 > A_1 > A_5 > A_3 > A_4$, which means that the assets for which precautionary measures should be taken could be ranked in this order. The outputs given in this table could support the company efficiently when making the information security management decisions.

4. **Conclusions.**

Risk management requires the use of more flexible approaches to measure information security risk. The AHP-GDM offers a technical support for risk analysis by obtaining the judgements of managers and systematically calculating the relative risk values.

The AHP-GDM is a powerful technique that is easy to understand and simple to operate. It is a flexible and practical tool for any organization to prioritize the risk incidents

TABLE 9. Risk values of R_{ijk}, R_{ij} and R_i calculated by BPP*

		V_1	V_2	V_3	V_4	V_5	V_6	R_{ij}	R_i
A_1	T_1	0.125	0.154	0.220	0.215	0.175	0.162	0.175	
	T_2	0.173	0.214	0.305	0.299	0.242	0.225	0.243	0.243(max)
	T_3	0.147	0.181	0.258	0.253	0.205	0.190	0.206	0.166(min)
	T_4	0.156	0.193	0.275	0.269	0.219	0.203	0.219	0.208(aver)
	T_5	0.172	0.212	0.303	0.297	0.241	0.223	0.241	
	T_6	0.118	0.146	0.208	0.204	0.165	0.153	0.166	
A_2	T_1	0.139	0.164	0.178	0.228	0.203	0.168	0.180	
	T_2	0.175	0.206	0.225	0.287	0.256	0.211	0.227	0.310
	T_3	0.209	0.246	0.268	0.342	0.305	0.252	0.270	0.180
	T_4	0.237	0.278	0.304	0.388	0.346	0.285	0.306	0.250
	T_5	0.240	0.282	0.307	**0.392**	0.350	0.288	0.310	
	T_6	0.160	0.188	0.205	0.262	0.234	0.193	0.207	
A_3	T_1	0.063	0.078	0.079	0.107	0.082	0.062	0.078	
	T_2	0.111	0.138	0.140	0.189	0.145	0.109	0.139	0.139
	T_3	0.093	0.116	0.117	0.159	0.122	0.091	0.116	0.078
	T_4	0.073	0.091	0.092	0.124	0.095	0.072	0.091	0.101
	T_5	0.079	0.098	0.099	0.134	0.103	0.077	0.098	
	T_6	0.069	0.086	0.087	0.118	0.090	0.068	0.086	
A_4	T_1	0.111	0.086	0.091	0.074	0.079	0.121	0.093	
	T_2	0.142	0.110	0.116	0.094	0.101	0.154	0.120	0.120
	T_3	0.080	0.062	0.066	0.053	0.057	0.087	0.067	0.065
	T_4	0.077	0.060	0.063	**0.051**	0.055	0.084	0.065	0.090
	T_5	0.102	0.080	0.084	0.068	0.073	0.111	0.086	
	T_6	0.129	0.101	0.106	0.086	0.092	0.140	0.109	
A_5	T_1	0.125	0.110	0.150	0.127	0.117	0.176	0.134	
	T_2	0.086	0.076	0.103	0.087	0.081	0.121	0.092	0.164
	T_3	0.094	0.083	0.113	0.096	0.088	0.133	0.101	0.092
	T_4	0.127	0.112	0.153	0.129	0.119	0.179	0.137	0.120
	T_5	0.087	0.077	0.105	0.088	0.082	0.123	0.093	
	T_6	0.152	0.134	0.183	0.155	0.143	0.215	0.164	

recurrently. However, there might be some complexities to use the AHP-GDM in risk evaluation. Decision makers participated in the analysis may have limited expertise about the problem domain or the AHP analysis. Also, they may have difficulties to make pairwise comparisons efficiently because of the large number of assets, threats and vulnerabilities which could result in incomplete or inconsistent judgements.

Considering the problems mentioned above, we propose using BPP based AHP for information security risk assessment. It is assumed that consensus exists among the decision makers with regard to the priorities for each element in this decision system. The multiplicative model with log-normal errors is applied to the problem and the Bayesian analysis is used. This is a process of weighted aggregation of individual priorities and the weights are inversely proportional to the decision makers' levels of inconsistency. We compared the method with the conventional approaches used in the AHP-GDM.

The results show that the proposed methodology performs more robust manner and calculates the final priorities with smaller MSE than the conventional approach. So, it can be concluded that the proposed methodology aggregate the individuals' judgements more effectively than the conventional method, especially after omitting the inconsistent judgements in the pairwise comparison matrices. This method provides managers a flexible way to express their judgements, without forcing them to give complete and consistent judgements and letting them completely focus on the risk management itself. Moreover, it serves the practitioner since the judgements of decision makers directly enter the analysis without any reducing or filtering process.

Any organization can easily adapt this method to their information security system by updating all the elements in the illustrative model, i.e., list of most valuable information assets, threats and vulnerabilities. This technique could be used alone or with any other information security risk analysis methods as a support; and can easily be adapted to any information security standard.

In this study, we applied BPP based AHP to prioritize and order risk incidents which could satisfy the aim of risk management. This approach can also be used for many multiple criteria group decision making problems such as project selection, facility location selection, supplier selection or evaluation, diagnosis and treatment selection for disease management, financial decision making and crisis forecasting, and evacuation selection for emergency management.

Our study is based on the model from a non-informative Bayesian standpoint, where the variances of error terms represented by the inconsistency levels of decision makers are assumed to be known. In the future, this approach can be extended by taking the variances of error terms as additional parameters, or by implementing an informative Bayesian model in which a good estimate of prior distribution for the vector of log-priorities is used.

This study is based on two assumptions. The first assumption is that there is a consensus among the decision makers. Gargallo et al. [28] proposed a Bayesian estimation procedure to determine the priorities where a prior consensus among them is not required. The second assumption is that there is no interaction or dependence between the elements in the decision system. We are currently working on the situations where this assumption is not satisfied.

REFERENCES

[1] T. Sommestad, M. Ekstedt and P. Johnson, A probabilistic relational model for security risk analysis, *Computers & Security*, vol.29, no.6, pp.659-679, 2010.

[2] L. D. Bodin, L. A. Gordon and M. P. Loeb, Information security and risk management, *Communications of the ACM*, vol.51, no.4, pp.64-68, 2008.

[3] N. Feng and M. Li, An information systems security risk assessment model under uncertain environment, *Applied Soft Computing*, vol.11, no.7, pp.4332-4340, 2011.

[4] B. Karabacak and I. Sogukpinar, ISRAM: Information security risk analysis method, *Computers & Security*, vol.24, no.2, pp.147-159, 2005.

[5] D. Zhao, J. Liu and Z. Zhang, Method of risk evaluation of information security based on neural networks, *Proc. of IEEE 2009 International Conference on Machine Learning and Cybernetics*, vol.1, no.6, pp.1127-1132, 2009.

[6] T. L. Saaty, *Multicriteria Decision Making: The Analytic Hierarchy Process*, 2nd Edition, RSW Pub., Pittsburgh, 1990.

[7] H. J. Hwang and H. S. Hwang, Computer-aided fuzzy-AHP decision model and its application to school food service problem, *International Journal of Innovative Computing, Information and Control*, vol.2, no.1, pp.125-137, 2006.

[8] I. Nakaoka, M. Matsumura, J. I. Kushida and K. Kamei, A proposal of group decision support system for Kansei commodity purchase using SOM and its applications, *International Journal of Innovative Computing, Information and Control*, vol.5, no.12(B), pp.4915-4926, 2009.

[9] B. Guan, C. Lo, P. Wang and J. Hwang, Evaluation of information security related risks of an organization – The application of the multi-criteria decision-making method, *Proc. of IEEE the 37th Annual International Carnahan Conference on Security*, pp.168-175, 2003.

[10] L. D. Bodin, L. A. Gordon and M. P. Loeb, Evaluating information security investments using the analytic hierarchy process, *Communications of the ACM*, vol.48, no.2, pp.78-83, 2005.

[11] C. Xu and J. Lin, An information system security evaluation model based on AHP and GRAP, *Proc. of IEEE International Conference on Web Information Systems and Mining*, pp.493-496, 2009.

[12] I. Syamsuddin and J. Hwang, The use of AHP in security policy decision making: An open office calc application, *Journal of Software*, vol.5, no.10, 2010.

[13] M. Y. Huang, Research on information security evaluation of internet of things electronic commerce based on AHP, *Advanced Materials Research*, vol.217-218, pp.1355-1360, 2011.

[14] X. Zhang, Z. Huang, G. Wei and X. Zhang, Information security risk assessment methodology research: Group decision making and analytic hierarchy process, *Proc. of IEEE the 2nd World Congress on Software Engineering*, vol.2, pp.157-160, 2010.

[15] A. Altuzarra, J. M. Moreno-Jimnez and M. Salvador, A Bayesian prioritization procedure for AHP-group decision making, *European Journal of Operational Research*, vol.182, no.1, pp.367-382, 2007.

[16] T. L. Saaty, Group decision-making and the AHP, in *The Analytic Hierarchy Process: Applications and Studies*, B. L. Golden, E. A. Wasil and P. T. Harker (eds.), New York, Springer-Verlag, 1989.

[17] R. Ramanathan and L. S. Ganesh, Group preference aggregation methods employed in AHP: An evaluation and an intrinsic process for deriving members' weightages, *European Journal of Operational Research*, vol.79, no.2, pp.249-265, 1994.

[18] E. Forman and K. Peniwati, Aggregating individual judgments and priorities with the analytic hierarchy process, *European Journal of Operational Research*, vol.108, no.1, pp.165-169, 1998.

[19] R. F. Dyer and E. H. Forman, Group decision support with the analytic hierarchy process, *Decision Support Systems*, vol.8, no.2, pp.99-124, 1992.

[20] G. Crawford and C. Williams, A note on the analysis of subjective judgment matrices, *Journal of Mathematical Psychology*, vol.29, no.4, pp.387-405, 1985.

[21] J. Aguarn and J. M. Moreno-Jimnez, Local stability intervals in the analytic hierarchy process, *European Journal of Operational Research*, vol.125, no.1, pp.113-132, 2000.

[22] T. L. Saaty, Procedures for synthesizing ratio judgements, *Journal of Mathematical Psychology*, vol.27, no.1, pp.93-102, 1983.

[23] M. A. Tanner and W. H. Wong, The calculation of posterior distributions by data augmentation, *Journal of the American Statistical Association*, vol.82, no.398, pp.528-540, 1987.

[24] J. M. Alho and J. Kangas, Analyzing uncertainties in experts'opinions of forest plan performance, *Forest Science*, vol.43, pp.521-528, 1997.

[25] I. Basak, Probabilistic judgments specified partially in the analytic hierarchy process, *European Journal of Operational Research*, vol.108, no.1, pp.153-164, 1998.

[26] A. Salo and R. P. Hmlinen, Preference programming multicriteria weighting models under incomplete information, in *Handbook of Multicriteria Analysis*, C. Zopounidis and P. M. Pardalos (eds.), Berlin, Springer, 2010.

[27] S. H. Kim and B. S. Ahn, Group decision making procedure considering preference strength under incomplete information, *Computers & Operations Research*, vol.24, no.12, pp.1101-1112, 1997.

[28] P. Gargallo, J. M. Moreno-Jimnez and M. Salvador, AHP-group decision making: A Bayesian approach based on mixtures for group pattern identification, *Group Decision and Negotiation*, vol.16, no.6, pp.485-506, 2007.