# Research on Cloud Computing Security Risk Assessment Based on Information Entropy and Markov Chain

Ming Yang[1], Rong Jiang[1], Tilei Gao[1], Wanyu Xie[2] and Jia Wang[1]
*(Corresponding author: Rong Jiang)*
School of Information, Yunnan University of Finance and Economics, Kunming 650221, China[1]
2502 Gaodeng St, Chenggong Qu, Kunming Shi, Yunnan Sheng, China
Personnel Department, KunMing Metallurgy College, Kunming 650033, China[2]
(Email: jiangrong@ynu.edu.cn)
*(Received Mar. 31, 2017; revised and accepted July 13, 2017)*

## Abstract

The measurement and assessment of risk is an important basis for the research of cloud computing security risk, it can provide important data for risk management decisions. However, due to the uncertainties of risk occurrences and losses, actual risk have multiple stochastic states, make the research of cloud computing risk become more difficult. In order to measure the risk and avoid the influence of subjective factors, a measurement and assessment model of cloud computing risk is established in this paper. The established model used Markov chain to describe random risk environment, and used information entropy to measure risk, effectively reduced the existing subjective factors in the assessment process, provided a practical and reliable method for risk management decisions.

*Keywords: Cloud Computing Security; Information Entropy; Markov Chain; Risk Assessment; Risk Measurement*

## 1 Introduction

While providing users with strong computing power and huge application resource, cloud computing also brought potential security threats to users. According to the Global survey results of Gartner, IDC and Unisys [1, 18, 23, 24], security problems have become an important factor for users while selecting cloud computing services.

Cloud computing security is threatened by many factors. These factors are not only technical defects, but also include non-technical factors, such as the lack of management, limitations of laws and the problem of geographically distribution, which bring challenges to cloud computing risk management decisions [19]. In risk management decisions, due to uncertainties the occurrences of cloud computing risk have a variety of random state. Therefore, how to effectively measure and assess the actual risk has become the key to risk management decisions.

Based on the viewpoints proposed in the report "Assessing the security risks of cloud computing" [11], this paper stands on the perspective of cloud computing service providers, and refers to the cloud computing security risk factors proposed in related literature, establishes a cloud computing security risk attribute hierarchies. And on the basis of the attribute hierarchies, this paper conducts quantitative researches on risk uncertainty with the theory of information entropy and Markov chain, and puts forward a measurement and assessment model for cloud computing security risks. This model proposes a risk measurement method, and establishes a risk assessment hierarchy, which solves the problem in measuring abstract risk. Finally, a case was conducted, which shows that the established model can be used to measure objectively the existing risks in a real process and has an important reference value for the future development of cloud computing.

The organization of this paper is as follows: Section 1: Introduction. Introduce the research contents and significance of this paper. Section 2: Related researches. This chapter discusses current research situation about risk factors, risk measurement and risk assessment, and put forward the problems that need to be solved. Section 3: Cloud computing risk and information entropy. This chapter proposes a concept of cloud computing risk entropy, establishes an attribute hierarchy of cloud computing security risk, and describes the cloud computing risk environment with Markov chain. Section 4: The measurement and assessment model of cloud computing risk. On the basis of above research results, this chapter proposes a measurement and assessment model of cloud computing risk, and gives the calculation steps. Section 5: Case analysis. This chapter makes a case research on the

cloud computing security risk of a firm's e-commerce platform with the established model in Section 4. Section 6: Conclusion. Summarize the related research in this paper and point out the future research directions.

# 2 Related Researches

Cloud service involves many characters, and contains complex information. So while researching cloud computing security risks, it firstly requires organizing the risk factors, and sorting out the logical relationship between them.

## 2.1 Risk Factors

The report [11] published in Gartner refers to that the risk assessment of cloud computing should be carried out from the data safety, legal risk, investigation support and the survival ability of service providers *etc.* ENISA [3] emphasizes the cloud computing security weakness lies in the defect of management and the lack of laws compliance. Deng [5] analyzes the security problem of cloud computing from different service level based on hadoop, and finds that these security problem mainly include physical infrastructure security, data security, application security, interface security, user rights management security and legal risk *etc.* Cheng [4] takes the information security risks as evaluation target, and establishes an assessment index system which has 35 risk factors, and proposed an new assessment method for the cloud service information security based on AHP (analytic hierarchy process) method; Jiang [13] on the basis of the risk security protection requirements in China, divides the cloud computing security into five aspects as physical security, network security, host system security, application security and data security respectively, and uses AHP method to assign weight for each index, finally puts forward the cloud computing security evaluation model based on the risk security protection. Feng [9] mentioned that the focus of cloud computing security are laws and regulations, business risk management, authentication and access control, application security and physical security.

The above literatures discuss the risk factors of cloud computing security from different aspects, and make a quantitative analysis, provide an important reference value for this paper research. However, when researching the relationship between each risk, these literatures usually divide the risks into several independent categories which do not overlap, and neglect the uncertainty between each risk, which leads to differences between the research results and the real situation.

## 2.2 Risk Measurement

To assess the risk, and identify the risk factors, the risk measurement is essential. Such as risk value model VaR (Value at Risk) [27,28], actuarial model [8], coherent risk measurement [10,17], risk matrix analysis method [7] and so on. These models provide important reference value for the current research of risk measurement, but inevitably be influenced by subjective bias.

## 2.3 The Random State of Risk

As known the cloud computing security risk is independent of each other, when a risk is occurring, it may make other risks appearing together, or it may occur alone, there are a variety of possible states about risk occurrences. So when assessing the risk, all possible states about these risk occurrences are required to consider seriously. But the traditional researches mainly carry on a research on a single risk or similar risks [12, 16, 25], and lack of the comparative analysis about different categories of risk.

## 2.4 Risk Assessment

In addition, in the risk weighting process, most of the literatures haven't make quantitative analysis on the uncertainty and loss degree of each risk, and haven't established the risk assessment system. These research [2, 14, 15, 20, 21, 26] results often focus on the technical risk, not to the other risk factors, and therefore can't give a comprehensive comparison for all kinds of risks from different levels and dimensions.

The above problems all need to be solved in the process of cloud computing risk assessment, and are also the main research content of this paper. Therefore, the first for this article to do is sorting out the risk factors. On the basis of the risk factors, this paper will establish a risk attribute hierarchies with cross relation by using Markov chain to simulate the actual cloud computing risk environment, and carry on a quantitative analysis around the uncertainties of risk occurrences and losses, so that to realizes the quantitative risk analysis from different levels and angles.

# 3 Cloud Computing Risk and Information Entropy

## 3.1 Cloud Computing Risk Entropy

Due to the characteristics of cloud computing service itself, the probability of risk occurrence P(x), the risk loss C(x), and the possible occurrence states of risk environments are all uncertain. Therefore, considering the uncertainty of risks, this paper wants to use information entropy method to measure the size of cloud computing risk.

Information refers to the reduction of uncertainty in course of people cognition, in order to quantitatively describe the degree of information uncertainty, the theory founder Shannon proposed the concept of information entropy, and used it to describe the size of information contained in system.

Suppose that a research object $X$ contains $n$ possible result $X_i$, $X = \{X_1 X_2, \ldots, X_n\}$, in which the occurrence probability of each result is $P(X_i) \sum P(X_i) = 1$, thus the information entropy of this object is $H(X) = -\sum_{i=1}^{n} P(X_i) \log_2 P(X_i)$. Its value is bigger, means that more information of the object contains, more complex the object is, and more high the uncertainty degree is.

When the object has only one possible outcome, now $P(X_1) = 1$, its information entropy $H(X) = 0$, means that the object does not exist any uncertain information; On the contrary, when the object contains N possible outcome, and the occurrence probability of each result is equal as $P(X_1) = P(X_2) =, \ldots, = P(X_n)$, its information entropy will reached a maximum value as $H(X) = \log_2 n$, means that the object reaches the highest uncertainty degree.

However, in the actual situation, information entropy is almost impossible to reach maximum or minimum, and it usually located a value between maximum and minimum.

According to the above theorem, when there is only one possible risk in process of cloud computing, the goal of risk management and maintenance is clear, the risk will be easier to maintain. Conversely, when there is a variety of possible risk, the risk maintenance will be more uncertain. Therefore, it can use the information entropy to describe the uncertainty degree of cloud computing risk. The higher risk uncertainty degree is, the greater risk entropy is, means the risk will be more difficult to control; on the other hand, the lower risk uncertainty degree is, the clearer that the goal of risk maintain is, and the easier risk will be controlled.

### 3.2 Cloud Computing Security Risk Attribute Hierarchies

Different from the traditional analysis of cloud computing risk, in order to realize the calculation and analysis on cloud computing security from different levels and angles, this paper divides the cloud computing security risk attribute into three levels, as shown in Figure 1 (Cross analysis of cloud computing risk).

The three layers' meanings are:

**Target layer:** The goal of this paper research;

**Risk class layer:** The different classes of cloud computing risk, uses $\beta_i, i = 1, 2, \ldots, n$ to express each risk class;

**Risk factor layer:** The risk factors influencing the cloud computing security, uses $\alpha_j, i = 1, 2, \ldots, m$ to express each risk factor;

This risk attributes hierarchies is different from the traditional research hierarchies, there is complex cross relationships between risk class layer and risk factor layer, which can better reflect the random environment of cloud computing risk.

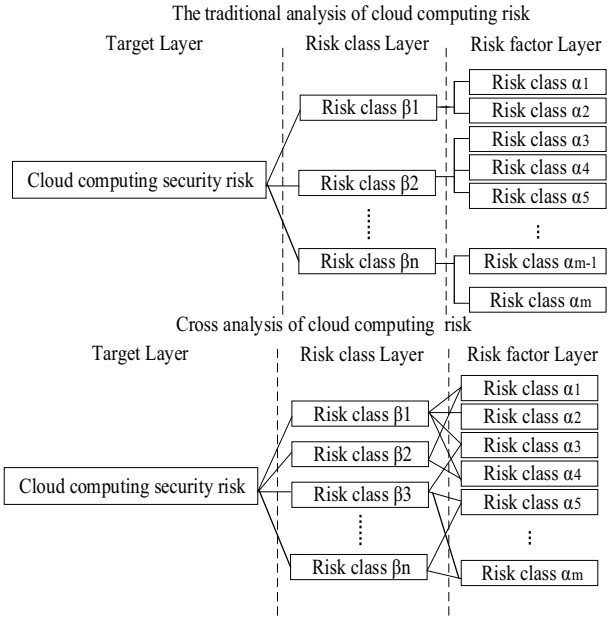


Figure 1: The attribute hierarchies of cloud computing risks

1) The degree of risk uncertainty.
Uses $P(\alpha_j)$ to express the threat frequency of risk factor $\alpha_j$ to cloud security, and uses $P(\beta_i \alpha_j)$ to express the entropy weight of risk factor $\alpha_j$ relative to risk class $\beta_i$; Assuming that the class $\beta_i$ contains $K$ risk factors, thus the calculation formula of $P(\beta_i \alpha_j)$ is as follow:

$$p(\beta_i, \alpha_j) = \frac{1}{\sum_{j=1}^{k} p(\alpha_j)} p(\alpha_j) \tag{1}$$

Then take it into the information entropy formula, as shown below:

$$C(\beta_i) = \sum_{j=1}^{m} p(\beta_i, \alpha_j) C(\alpha_j) \tag{2}$$

$H(\beta_i)(0 \leq H_i \leq 1)$ is risk entropy,it expresses the uncertainty degree of risk class $\beta_i$, the higher its value is, the harder the factors causing the risk could be determined, and the harder risk management decisions will be.

2) The degree of risk loss.
In addition to the uncertainties of risk occurrences, in the risk assessment process it also need to consider the degree of risk loss. The calculation formula of risk loss degree is as follow:

$$\begin{aligned} L(\beta_i) &= (L(\beta_1), L(\beta_2), ..., L(\beta_6)) \\ &= (0.392, 0.482, 0.439, 0.476, 0.377, 0.500) \\ L &= 0.451 \end{aligned} \tag{3}$$

In which, $C(\alpha_j)$ expresses risk loss degree of factor $\alpha_j$, $P(\beta_i, \alpha_j)$ is the entropy weight of factor $\alpha_j$ relative to risk class $\beta_i$. As shown in Equation (3),

$C(\beta_i)$expresses risk loss degree of risk class $\beta_{\mathrm{i}}$. The higher its value is, the greater its impact on cloud security is.

### 3.3 Markov Chain and Cloud Computing Risk

As shown in Figure 1, in a cloud computing environment there are n risk classes as $\beta_i = 1, 2, \cdots, n$, and each risk class contains a number of risk factors as $\alpha_j, i = 1, 2, \cdots, m$, so the risk occurrence has a variety of random possible states in actual operation process of cloud computing service.

Markov chain has the mathematical definition, it can describe the state of things' random process, with the transfer matrix Q it can calculate the probability of things' random state [6]. Therefore, this paper prepares to use Markov chain to calculate the steady state probability of each risk class during the long operation process of cloud computing service. The first thing is to define the all possible state sets of cloud computing risks, then establish the transfer matrix between them, as shown below:

$$Q = \begin{bmatrix} P(\beta_{11}) & P(\beta_{12}) & P(\beta_{13}) & \ldots & P(\beta_{1n}) \\ P(\beta_{21}) & P(\beta_{22}) & P(\beta_{23}) & \ldots & P(\beta_{2n}) \\ P(\beta_{31}) & P(\beta_{32}) & P(\beta_{33}) & \ldots & P(\beta_{3n}) \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ P(\beta_{n1}) & P(\beta_{n2}) & P(\beta_{n3}) & \ldots & P(\beta_{nn}) \end{bmatrix} \quad (4)$$

The matrix Q expresses the all possible states of each risk class in cloud computing environment. Among them, diagonal elements $\mathrm{P}(\beta_{\mathrm{ij}})(\mathrm{i} = \mathrm{j})$ represent the probability of each risk class happen alone. Thus $\mathrm{P}(\beta_{\mathrm{ij}})(\mathrm{i} \neq \mathrm{j})$ represent the probability of risk class $\beta_{\mathrm{i}}$ and $\beta_{\mathrm{j}}$ happen at the same time, $\sum_{\mathrm{j}=1}^{\mathrm{n}} \mathrm{P}(\beta_{\mathrm{ij}}) = 1$.

Assuming that the probability of each risk class in the steady state is $\mathrm{P}(\beta_{\mathrm{i}}) = (\mathrm{P}(\beta_1), \mathrm{P}(\beta_2), \ldots, \mathrm{P}(\beta_{\mathrm{n}}))$ $\sum \mathrm{P}(\beta_{\mathrm{i}}) = 1$, it satisfying the following equations:

$$\begin{cases} P(\beta_1) = P(\beta_{11})P(\beta_1) + P(\beta_{12})P(\beta_2) + \cdots \\ \qquad + P(\beta_{1n})P(\beta_n) \\ P(\beta_2) = P(\beta_{21})P(\beta_1) + P(\beta_{22})P(\beta_2) + \cdots \\ \qquad + P(\beta_{2n})P(\beta_n) \\ \qquad \cdots . \\ P(\beta_n) = P(\beta_{n1})P(\beta_1) + P(\beta_{n2})P(\beta_2) + \cdots \\ \qquad + P(\beta_{nn})P(\beta_n) \end{cases} \quad (5)$$

Through solving the equations, it can be obtained the steady-state probability $\mathrm{P}(\beta_{\mathrm{i}}), \mathrm{i} = 1, 2, \ldots, \mathrm{n}$. The higher its value is, the easier this risk class will occur in the steady-state, the greater its threat frequency to cloud security is.

## 4 The Measurement and Assessment Model of Cloud Computing Risk

### 4.1 The Assessment System of Cloud Computing Risk

This paper on the basis of the index system proposed by GB/T 22239-2008 [22], refers to the risk factors listed in the report "Assessing the security risks of cloud computing" [11] and the risk assessment index proposed by Cheng [27] and Zhu [29], from 6 aspects to establish a hierarchy of cloud computing risk assessment, as shown in Figure 2.

### 4.2 The Process of Measurement and Assessment Based on Information Entropy

After establishing the risk assessment system, this paper will make detailed measurement and assessment from three aspects: the degree of risk uncertainty, the degree of risk loss and the threat frequency of risk. Its process is as follows:

**Step 1:** Establish the assessment table as Table 1 and Table 2, and assign weight to the $\mathrm{P}(\alpha_{\mathrm{j}})$ and $\mathrm{C}(\alpha_{\mathrm{j}})$ of risk factors in third layer according to the assessments of 15 domain experts.

Table 1: The assessment table of risk frequency$\mathrm{P}(\alpha_{\mathrm{j}})$

| Weight | Level | Specific definitions |
|---|---|---|
| 1 | Very high | The frequencies of risk factors are very high, almost inevitable in actual situation |
| 0.8 | high | The frequencies of risk factors are high, often occur in most cases |
| 0.6 | Medium | The frequencies of risk factors are normal, may occur in some cases |
| 0.4 | low | The frequencies of risk factors are low, it will occur in a minority of cases |
| 0.2 | Very low | The frequencies of risk factors are very low, almost never happen in a minority of cases |

Assuming that experts' assessment distributions of risk frequencies and risk losses are$\mathrm{P}(\mathrm{x}, \mathrm{y})$ and $\mathrm{C}(\mathrm{x}, \mathrm{y})$, in which $x$ expresses risk factors and $y$ expresses the weight level. Thus calculations of $\mathrm{P}(\alpha_{\mathrm{j}})$ and $\mathrm{C}(\alpha_{\mathrm{j}})$

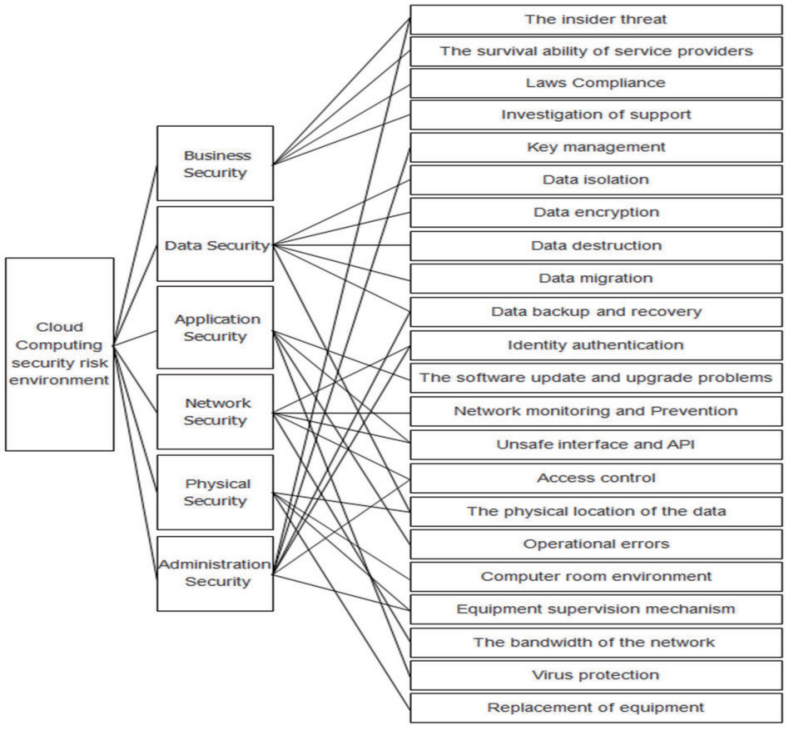


Figure 2: The assessment hierarchy of cloud computing security risk

are shown as the following formula:

$$P(\alpha_j) = (0.2, 0.4, 0.6, 0.8, 1)(p(x,1), p(x,2), \cdots, p(x,5))$$
$$C(\alpha_j) = (0.2, 0.4, 0.6, 0.8, 1)(c(x,1), c(x,2), \cdots, c(x,5)) \quad (6)$$

The $P(\alpha_j)$ and $C(\alpha_j)$ depend on *experts'* assessment distribution, the more dispersed expert assessments are, the higher assessment results' uncertainties are. Conversely, the more concentrated expert assessments are, the higher assessment results' certainties are, so the assessment weight of each risk factor can be defined as the following formula:

$$V(\alpha_j) = \sqrt[2]{(1 - \sum_{j=1}^{5} p_{ij} \log_5 p_{ij})(1 - \sum_{j=1}^{5} c_{ij} \log_5 c_{ij})} \quad (7)$$

The value of $V(\alpha_j)$ expresses its contribution on risk assessment, the higher its value is, the greater its contribution is.

**Step 2:** According to the classification in Figure 2, use Equation (1) to calculate the entropy weight coefficient $P(\beta_i, \alpha_j)$;

**Step 3:** Put the $P(\beta_i, \alpha_j)$into Equations (2) and (3), and calculate the degree of risk uncertainty $H(\beta_i)$ and the degree of risk losses $C(\beta_i)$.

**Step 4:** According to Markov chain principle, calculate the steady-state probability of each risk class $P(\beta_i) = (P(\beta_1), P(\beta_2), \ldots, P(\beta_6))$.

Firstly, according to the assessment system of cloud computing security risk shown in Fig.2, and combined with the frequency $P(\alpha_j)$ of each risk factor to establish the transfer matrix between each risk class, as follows:

$$Q = \begin{bmatrix} P(\beta_{11}) & P(\beta_{12}) & P(\beta_{13}) & \cdots & P(\beta_{16}) \\ P(\beta_{21}) & P(\beta_{22}) & P(\beta_{23}) & \cdots & P(\beta_{26}) \\ P(\beta_{31}) & P(\beta_{32}) & P(\beta_{33}) & \cdots & P(\beta_{36}) \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ P(\beta_{61}) & P(\beta_{62}) & P(\beta_{63}) & \cdots & P(\beta_{66}) \end{bmatrix} \quad (8)$$

In the matrix, the diagonal elements $P(\beta_{ii})$ represent the probability of the risk class $\beta_i$ occurred alone, and the elements $P(\beta_{ij})$ represent the probabilities of risk class $\beta_i$ and $\beta_j$ happen at the same time, its value depends on the factors contained in each risk class.

As shown in the following example. The Markov transition matrix of them is as follows:

$$\begin{bmatrix} P(\beta_{11}) & P(\beta_{12}) \\ P(\beta_{21}) & P(\beta_{22}) \end{bmatrix}$$
$$= \begin{bmatrix} \frac{1}{\sum_{i=1}^{3} P(\alpha_i)} P(\alpha_1) + P(\alpha_2) & \frac{1}{\sum_{i=3}^{5} P(\alpha_i)} P(\alpha_3) \\ \frac{1}{\sum_{i=1}^{3} P(\alpha_i)} P(\alpha_3) & \frac{1}{\sum_{i=3}^{5} P(\alpha_i)} P(\alpha_4) + P(\alpha_5) \end{bmatrix}$$

After establishing the Markov transition matrix, suppose that the steady-state probability of each risk class in second layer is $P(\beta_i) = (P(\beta_1), P(\beta_2), \ldots,$

Table 2: The assessment table of risk loss degree C($\alpha_j$)

| Weight | Level | Specific definitions |
|---|---|---|
| 1 | Very high | Once the risk occurs will cause devastating losses |
| 0.8 | high | The impact of risk is larger, maintenance needs higher funds |
| 0.6 | Medium | The impact and economic loss caused by risk is normal |
| 0.4 | low | The impact caused by risk is lower, and the maintenance funds required lower |
| 0.2 | Very low | The impact caused by risk can be ignored, and hardly need maintenance |

Table 3: Two different risk classes

| | **risk class $\beta_1$** | **risk class $\beta_2$** |
|---|---|---|
| **risk factors** | $\alpha_1$,$\alpha_2$,$\alpha_3$ | $\alpha_3$,$\alpha_4$,$\alpha_5$ |

$P(\beta_6))\sum \mathrm{P}(\beta_i)=1$, then put it into Equation (5) to calculate the steady-state probability.

**Step 5:** Define the grade of cloud computing security risk, and make integrated risk assessment.

The definition of cloud computing security risk grade contains three factors: the degree of risk uncertainty H($\beta_i$), the degree of risk loss C($\beta_i$) and the frequency of risk occurrence P($\beta_i$). The specific definitions are as shown in Table 4.

The calculation formula of the grade of each risk class is as follows:

$$L(\beta_i) = \sqrt[3]{H(\beta_i)C(\beta_i)P(\beta_i)} \tag{9}$$

According to the definition in the Table 4, the greater value of L($\beta_i$) is, the higher occurrence frequency of this risk class is, the harder risk maintenance is, and the greater risk loss is.

Next, on the basis of L($\beta_i$), this paper will further assess the whole cloud computing security risk grade, its calculation formula is as follows:

$$L = (L(\beta_1), L(\beta_2), \cdots, L(\beta_6))(V(\beta_1), V(\beta_2), \cdots, V(\beta_6))^T \tag{10}$$

Among them,V $(\beta_i)$ , i = 1, 2, . . . , 6 expresses the assessment weight of each risk class $\beta_i$, its calculation formula is as follows:

$$V(\beta_i) = \frac{1}{\sum_{i=1}^{6}\sum_{j=1}^{m} V(\alpha_j)} \sum_{j=1}^{m} V(\alpha_j) \tag{11}$$

Among them, $m$ is the counts of risk factors contained in risk class $\beta_i$. The value of V $(\beta_i)$ expresses its impact on the entire cloud security.

Table 4: The grade of cloud computing security risk

| Grade | Specific definitions |
|---|---|
| $0.8 < L < 1$ | The factors causing risk can't be determined. Once risks occur, cloud service will be almost impossible to maintain success. Its cloud security belongs the catastrophic risk |
| $0.6 < L \leq 0.8$ | The factors causing risk are many and be difficult to determine. Once risks occur, they will directly affect the normal operation process of cloud services |
| $0.4 < L \leq 0.6$ | There will be some impact on the operation process of cloud services. The cloud security belongs the general risk level, its service need maintenance routine, |
| $0.2 < L \leq 0.4$ | Risk maintenance goals is clear, its cloud computing services are well-managed |
| $0 < L \leq 0.2$ | Risk maintenance goal was very clear, there is almost not any impact on cloud computing services,the risk impact often can be ignored |

# 5 Case Analysis

## 5.1 The Process of Calculation

According to the risk assessment system established in this paper, this article makes a case research on the cloud computing security risk of a firm's e-commerce platform.

**Step 1:** Trough the experts scoring, the assessment distribution results are shown in Table 5.

**Step 2:** Make normalization processing, get the entropy weight coefficient of $P(\beta_i, \alpha_j)$,as shown in Table 6.

**Step 3:** According to Formula (2) and (3), calculate the degree of risk uncertainty $H(\beta_i)$ and the degree of risk loss $(\beta_i)$, get the results as follows:

$$\begin{aligned} H(\beta_i) &= (H(\beta_1), H(\beta_2), \cdots, H(\beta_6)) \\ &= (0.941, 0.978, 0.992, 0.993, 0.992, 0.987) \\ C(\beta_i) &= (C(\beta_1), C(\beta_2), \cdots, C(\beta_6)) \\ &= (0.622, 0.594, 0.474, 0.500, 0.562, 0.592) \end{aligned}$$

**Step 4:** According to the principle of Markov chain, establish the Markov transfer matrix of each risk class.

$$\begin{vmatrix} 0.574 & 0.000 & 0.000 & 0.000 & 0.000 & 0.426 \\ 0.000 & 0.758 & 0.000 & 0.000 & 0.116 & 0.126 \\ 0.000 & 0.000 & 0.761 & 0.239 & 0.000 & 0.000 \\ 0.000 & 0.000 & 0.198 & 0.436 & 0.000 & 0.366 \\ 0.000 & 0.234 & 0.000 & 0.000 & 0.486 & 0.280 \end{vmatrix}$$

Table 5: The results of assessment distribution

| | assessment distribution of **P**(**xy**) | | | | | | assessment distribution of **C**(**xy**) | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Risk factors** $\alpha_j$ | **0.2** | **0.4** | **0.6** | **0.8** | **1** | **P**($\alpha_j$) | **0.2** | **0.4** | **0.6** | **0.8** | **1** | **C**($\alpha_j$) |
| Identity authentication | 0.00 | 0.27 | 0.60 | 0.13 | 0.00 | 0.573 | 0.00 | 0.07 | 0.73 | 0.20 | 0.00 | 0.627 |
| Access control | 0.00 | 0.07 | 0.80 | 0.13 | 0.00 | 0.613 | 0.00 | 0.07 | 0.87 | 0.07 | 0.00 | 0.600 |
| Laws Compliance | 0.27 | 0.73 | 0.00 | 0.00 | 0.00 | 0.347 | 0.07 | 0.33 | 0.40 | 0.20 | 0.00 | 0.547 |
| Investigation of support | 0.47 | 0.53 | 0.00 | 0.00 | 0.00 | 0.307 | 0.27 | 0.60 | 0.13 | 0.00 | 0.00 | 0.373 |
| Key management | 0.00 | 0.20 | 0.67 | 0.13 | 0.00 | 0.587 | 0.00 | 0.33 | 0.47 | 0.20 | 0.00 | 0.573 |
| Data isolation | 0.00 | 0.13 | 0.53 | 0.33 | 0.00 | 0.640 | 0.00 | 0.27 | 0.60 | 0.13 | 0.00 | 0.573 |
| Data encryption | 0.00 | 0.13 | 0.40 | 0.33 | 0.13 | 0.693 | 0.00 | 0.00 | 0.47 | 0.47 | 0.07 | 0.720 |
| Data destruction | 0.07 | 0.80 | 0.13 | 0.00 | 0.00 | 0.413 | 0.07 | 0.27 | 0.47 | 0.20 | 0.00 | 0.560 |
| Data migration | 0.07 | 0.73 | 0.20 | 0.00 | 0.00 | 0.427 | 0.00 | 0.20 | 0.80 | 0.00 | 0.00 | 0.560 |
| Data backup and recovery | 0.20 | 0.80 | 0.00 | 0.00 | 0.00 | 0.360 | 0.07 | 0.53 | 0.20 | 0.20 | 0.00 | 0.507 |
| The insider threat | 0.00 | 0.13 | 0.53 | 0.27 | 0.07 | 0.653 | 0.00 | 0.07 | 0.47 | 0.33 | 0.13 | 0.707 |
| software update problems | 0.00 | 0.00 | 0.53 | 0.27 | 0.20 | 0.733 | 0.13 | 0.60 | 0.27 | 0.00 | 0.00 | 0.427 |
| Network monitoring and Prevention | 0.00 | 0.20 | 0.73 | 0.07 | 0.00 | 0.573 | 0.20 | 0.40 | 0.40 | 0.00 | 0.00 | 0.440 |
| Unsafe interface and API | 0.00 | 0.07 | 0.67 | 0.27 | 0.00 | 0.640 | 0.00 | 0.07 | 0.60 | 0.33 | 0.00 | 0.653 |
| survival ability of service providers | 0.87 | 0.13 | 0.00 | 0.00 | 0.00 | 0.227 | 0.00 | 0.00 | 0.07 | 0.73 | 0.20 | 0.827 |
| data physical location | 0.33 | 0.67 | 0.00 | 0.00 | 0.00 | 0.333 | 0.13 | 0.13 | 0.53 | 0.20 | 0.00 | 0.560 |
| Operational errors | 0.00 | 0.00 | 0.33 | 0.40 | 0.27 | 0.787 | 0.13 | 0.67 | 0.20 | 0.00 | 0.00 | 0.413 |
| Computer room environment | 0.20 | 0.80 | 0.00 | 0.00 | 0.00 | 0.360 | 0.00 | 0.00 | 0.33 | 0.53 | 0.13 | 0.760 |
| Equipment supervision mechanism | 0.00 | 1.00 | 0.00 | 0.00 | 0.00 | 0.400 | 0.13 | 0.53 | 0.27 | 0.07 | 0.00 | 0.453 |
| bandwidth of network | 0.00 | 0.00 | 0.13 | 0.53 | 0.33 | 0.840 | 0.73 | 0.20 | 0.07 | 0.00 | 0.00 | 0.267 |
| Virus protection | 0.00 | 0.40 | 0.60 | 0.00 | 0.00 | 0.520 | 0.07 | 0.80 | 0.13 | 0.00 | 0.00 | 0.413 |
| Replacement of equipment | 0.33 | 0.67 | 0.00 | 0.00 | 0.00 | 0.333 | 0.00 | 0.40 | 0.53 | 0.07 | 0.00 | 0.533 |

Table 6: The entropy weight coefficient P($\beta_i\alpha_j$) of each risk class

| **Business Security** $\beta_1$ | **P**($\alpha_j$) | **P**($\beta_1\alpha_j$) | **Data Security** $\beta_2$ | **P**($\alpha_j$) | **P**($\beta_2\alpha_j$) |
|---|---|---|---|---|---|
| The insider threat | 0.653 | 0.426 | data physical location | 0.333 | 0.116 |
| survival ability | 0.227 | 0.148 | Data encryption | 0.693 | 0.242 |
| Laws Compliance | 0.347 | 0.226 | Data backup and data recovery | 0.360 | 0.126 |
| investigation support | 0.307 | 0.200 | Data isolation | 0.640 | 0.223 |
| | | | Data destruction | 0.413 | 0.144 |
| | | | Data migration | 0.427 | 0.149 |
| **Application Security** $\beta_3$ | **P**($\alpha_j$) | **P**($\beta_3\alpha_j$) | **Network Security** $\beta_4$ | **P**($\alpha_j$) | **P**($\beta_4\alpha_j$) |
| Virus protection | 0.520 | 0.194 | bandwidth of the network | 0.840 | 0.259 |
| Operational errors | 0.787 | 0.294 | Network monitoring and Prevention | 0.573 | 0.177 |
| Unsafe interface | 0.640 | 0.239 | Unsafe interface | 0.640 | 0.198 |
| problems of software update | 0.733 | 0.274 | Identity authentication | 0.573 | 0.177 |
| | | | Access control | 0.613 | 0.189 |
| **Physical Security** $\beta_5$ | **P**($\alpha_j$) | **P**($\beta_5\alpha_j$) | **Administration Security** $\beta_6$ | **P**($\alpha_j$) | **P**($\beta_6\alpha_j$) |
| data physical location | 0.333 | 0.217 | Data backup and recovery | 0.360 | 0.113 |
| Equipment supervision mechanism | 0.400 | 0.280 | Equipment supervision mechanism | 0.400 | 0.126 |
| Computer room environment | 0.360 | 0.252 | Identity authentication | 0.573 | 0.180 |
| Replacement of equipment | 0.333 | 0.234 | Access control | 0.613 | 0.192 |
| | | | The insider threat | 0.653 | 0.205 |
| | | | Key management | 0.587 | 0.184 |

Put the above data into Equation (5) to calculate, it can get the steady-state probability of each risk class in the long-term operation process of cloud computing service, as shown below:

$$p(\beta_i) = (p(\beta_1), p(\beta_2), \cdots, p(\beta_6)) = (0.103, 0.192, 0.179, 0.217, 0.096, 0.213)$$

**Step 5:** According to Equations (9) and (10), calculate the risk grade of each class and the risk grade of the whole environments, get the results shown below:

$$L(\beta_i) = (L(\beta_1), L(\beta_2), \cdots, L(\beta_6)) = (0.392, 0.482, 0.439, 0.476, 0.377, 0.500)$$
$$L = 0.451$$

### 5.2 Analysis of Research Results

The model presented in this paper realizes measurement and assessment of cloud computing security from different layers, different angles and different classes. The above research results are summarized, as shown in Table 7.

Table 7: The research results of risk measurement and assessment

| | $\beta_1$ | $\beta_2$ | $\beta_3$ | $\beta_4$ | $\beta_5$ | $\beta_6$ |
|---|---|---|---|---|---|---|
| $\mathbf{H}(\beta_i)$ | 0.941 | 0.978 | 0.992 | 0.993 | 0.992 | 0.987 |
| $\mathbf{C}(\beta_i)$ | 0.622 | 0.594 | 0.474 | 0.500 | 0.562 | 0.592 |
| $\mathbf{P}(\beta_i)$ | 0.103 | 0.192 | 0.179 | 0.217 | 0.096 | 0.213 |
| $\mathbf{L}(\beta_i)$ | 0.392 | 0.482 | 0.439 | 0.476 | 0.377 | 0.500 |
| | the risk grade of entire cloud computing security | | | | | |
| $\boldsymbol{L}$ | 0.451 | | | | | |

Through the analysis of the research results, it can be found:

1) $L = 0.451$, it expresses the grade of whole cloud computing security risk. This value illustrates that this firm's cloud computing security belongs the general risk level, its cloud computing service exists some risk, need maintenance routine, and its service is in the acceptable level.

2) $L(\beta_6) = 0.5, L(\beta_2) = 0.482$ and $L(\beta_4) = 0.476$, these values are more higher than other risk grade of the whole system. These data illustrate that the administration Security, data security and network security are the most threats to this firm's cloud security, which are the key to decide the security of this e-commerce platform and should be paid more attention in the risk management decisions. Conversely, $L(\beta_1) = 0.392$ and $L(\beta_5) = 0.377$ means that this firm's physical Security and business Security is well-managed.

In addition, according to the data of $P(\beta_i)$, $C(\beta_i)$ and $H(\beta_i)$, it can be found:

1) $P(\beta_4)$=*0.217*, it means that the occurrence frequency of network risk is the highest in long-term operation process. If this firm want to improve its cloud security, it should strengthen the protection of network.

2) $C(\beta_1)$=*0.622*, $C(\beta_2)$=*0.594* and $C(\beta_1)$=*0.592*, these data mean that the business risk, data risk and administration risk are the greatest potential threat to this firm's cloud security, once the risks occur they will cause huge losses to the company.

3) Comparing the risk uncertainty, it can be found that only business risk and data risk are lower. It illustrates that only these two risk classes are easier to control compared with the other risk.

On the basis of the above analysis, through the model presented in this paper, it can also make further in-depth analysis around the risk factors in the third layer, so that to provide detailed information for the firm's cloud computing security risk management.

## 6 Conclusion

This paper, bases on the information entropy theory, makes quantitative research on risk uncertainty, has reduced the influence of subjective factors on the quantitative results, and finally provides a reference standard for risk management decision.

Compared with the past research methods, this paper divides the cloud computing risk into 6 classes and establishes a risk assessment hierarchy with cross relations.

Combined with the Markov chain, this paper, calculates the steady-state probability of each risk class in the stable cloud computing process, makes up the lack of research on the uncertainty between each risk, and gives the definition of risk grade based on information entropy.

In the following work, author will still continue to identify and add new security risk factors of cloud computing, and avoid redundant factors, so that to provide more detailed risk assessment system.

## Acknowledgments

This work was supported by National Natural Science Foundation of China (Nos. 61763048, 61263022 and 61303234), National Social Science Foundation of China (No. 12XTQ012), Science and Technology Foundation of Yunan Province (No. 2017FB095), the 18th Yunnan Young and Middle-aged Academic and Technical Leaders Reserve Personnel Training Program (No.2015HB038), Yunnan Province Applied Basic Research Project (No.2016FD060) and Science Research Foundation of Yunnan Provincial Department of Education (No. 2017ZZX001).

The authors would like to thank the anonymous reviewers and the editors for their suggestions.

## References


[1] M. Ahmad, *Security Risks of Cloud Computing and Its Emergence as 5th Utility Service*. Springer Berlin Heidelberg, 2010.

[2] Y. Cai, "Security risk assessment model of information system based on cloud computing," *China Management Informationization*, vol. 12, pp. 75–77, 2010.

[3] D. Catteddu, "Cloud computing: benefits, risks and recommendations for information security," in *Web application security*. Springer, 2010, pp. 17–17.

[4] Y. Cheng, "The evaluation index of cloud service information security and its method study," *Beijing Jiaotong University*, 2013.

[5] Q. Deng, "Research on the security mechanism of cloud computing based on hadoop," *Nanjing: Nanjing University of Posts and Telecommunications*, 2013.

[6] X. Duan, M. X. Huang, B. Wan, and X. Yang, "Research on supply chain partner selection based on markov chain dynamic fuzzy evaluation in cloud computing," *Application Research of Computers*, vol. 31, no. 8, pp. 2403–2406, 2014.

[7] Y. Duan, J. Zhao, J. Chen, and G. Bai, "A risk matrix analysis method based on potential risk influence: A case study on cryogenic liquid hydrogen filling system," *Process Safety & Environmental Protection*, vol. 102, pp. 277–287, 2016.

[8] M. Eling and N. Loperfido, "Data breaches: Goodness of fit, pricing, and risk measurement," *Insurance Mathematics & Economics*, vol. 75, p. 126136, 2017.

[9] D. Feng, M. Zhang, Y. Zhang, and Z. Xu, "Cloud computing security research journal of software," *Journal of software, Computer Science*, vol. 22, no. 1, pp. 71–83, 2011.

[10] H. Föllmer and I. Penner, "Consistent risk measures and a non-linear extension of backwards martingale convergence." *Festschrift Masatoshi Fukushima*, pp. 183–202, 2015.

[11] J. Heiser and M. Nicolett, "Assessing the security risks of cloud computing," 2008.

[12] W. F. Hsien, C. C. Yang, and M. S. Hwang, "A survey of public auditing for secure data storage in cloud computing," *International Journal of Network Security*, vol. 18, no. 1, pp. 133–142, 2016.

[13] Z. W. Jiang, W. R. Zhao, and Y. Liu, "Model for cloud computing security assessment based on classified protection," *Computer Science*, 2013.

[14] C. Joshi and U. K. Singh, "Information security risk management framework for university computing environment," *International Journal of Network Security*, 2017.

[15] M. Jouini and L. B. A. Rabai, "Comparative study of information security risk assessment models for cloud computing systems ," *Procedia Computer Science*, vol. 83, pp. 1084–1089, 2016.

[16] C. W. Liu, W. F. Hsien, C. C. Yang, and M. S. Hwang, "A survey of public auditing for shared data storage with user revocation in cloud computing," *International Journal of Network Security*, vol. 18, no. 4, pp. 650–666, 2016.

[17] S. Mitra, "Efficient option risk measurement with reduced model risk," *Insurance Mathematics & Economics*, 2016.

[18] R. Morrell and A. Chandrashekar, "Cloud computing: new challenges and opportunities," *Network Security*, vol. 2011, no. 10, pp. 18–19, 2011.

[19] A. Mosa, H. M. El-Bakry, S. M. Abd El-Razek, S. Q. Hasan, "A proposed E-government framework based on cloud service architecture," *International Journal of Electronics and Information Engineering*, vol. 5, no. 2, pp. 93–104, 2016.

[20] D. R. D. Santos, R. Marinho, G. R. Schmitt, C. M. Westphall, and C. B. Westphall, "A framework and risk assessment approaches for risk-based access control in the cloud," *Journal of Network & Computer Applications*, vol. 74, pp. 86–97, 2016.

[21] F. U. Sha, Y. Z. Xiao, and M. H. Liao, "An approach for campus information systems security risk assessment based on fuzzy set and entropy weight," *Information Science*, 2013.

[22] Standardization Administration of the People's Republic of China, *Information Security Technology - Baseline for Classified Protection of Information System Security*, GB/T 22239-2008, 2008.

[23] D. Sun, G. Chang, L. Sun, and X. Wang, "Surveying and analyzing security, privacy and trust issues in cloud computing environments," *Procedia Engineering*, vol. 15, no. 1, pp. 2852–2856, 2011.

[24] S. Tanimoto, M. Hiramoto, M. Iwashita, H. Sato, and A. Kanai, "Risk management on the security problem in cloud computing," in *First Acis/jnu International Conference on Computers, Networks, Systems and Industrial Engineering*, 2011, pp. 147–152.

[25] J. Wang, J. Liu, and H. Zhang, "Access control based resource allocation in cloud computing environment," *International Journal of Network Security*, vol. 19, no. 2, pp. 236–243, 2017.

[26] Z. C. Wang, "Research on information security risk assessment based on cloud computing model," *Netinfo Security*, 2011.

[27] Y. C. Xu, "Research status of risk value model in foreign countries," *Foreign Economics & Management*, vol. 27, no. 6, pp. 44–51, 2005.

[28] Z. Zhang, L. Yang, H. Li, and F. Xiang, "A quantitative and qualitative analysis-based security risk assessment for multimedia social networks," *International Journal of Network Security*, vol. 18, no. 1, pp. 43–51, 2016.

[29] S. C. Zhu, X. U. Yu, and M. Y. Jin, "Cloud computing security risk assessment based on level protection strategy," *Computer Security*, 2013.


## Biography

**Ming Yang** is a lecturer at the school of information, Yunnan University of Finance and Economics, China.

He received his Ph.D. in system analysis and integration from the school of software at Yunnan University. His main research interests include information management and data mining.

**Rong Jiang** is a professor and Ph. D. supervisor at the school of information, Yunnan University of Finance and Economics, China. He received his Ph.D. in system analysis and integration from the school of software at Yunnan University. He has published more than 30 papers and ten books, and has gotten more than 40 prizes in recent years. His main research interests include cloud computing, big data, software engineering, information management, etc.

**Tilei Gao** is a lecturer at the school of information, Yunnan University of Finance and Economics. He is also a Ph.D candidate in system analysis and integration at the school of software at Yunnan University. His main research interests include software engineering and information management.

**Wanyu Xie** is a lecturer at Kunming Metallurgy College. She received Her master's degree in computer science and technology from the school of information science and engineering at Yunnan University. Her main research interests is information management.

**Jia Wang** is a lecturer at the Yunnan University of Finance and Economics. He received his master's degree in software engineering from the school of software at Yunnan University. His main research interests include embedded system architecture and information management.