CLOUD COMPUTING RISK ASSESSMENT METHOD BASED ON GAME THEORY

Yuxia Sun¹, Zhi Li¹, Wu Chaoxia²

¹School of Computer and Communication Engineering, University of Science and Technology Beijing (USTB), Beijing, 100083, China
²School of Applied Mathematics, Xinjiang University of Finance and Economics, Xinjiang, P.R.China
goodluck_syx@163.com

Abstract

As a product of the development of the Internet, security issues of cloud computing has attracted much attention whether it is from the cloud providers' point of view or from the perspective of cloud users. From the view of information security, risk assessment model is established in this paper using game theory, which involves the damage and the restore of the cloud system. Using the framework, the interaction between attacker and defender has been analysed and risk assessment of vulnerable points in cloud environment is conducted.

Keywords: cloud computing, security risk assessment, game theory

1 Introduction

Cloud computing is a business model. It distributes computing task to resource pool which consists of a large number of computers, and it makes all kinds of application systems can obtain the computing power, storage space and information services according to the need. Google, Amazon, IBM, Microsoft, Salesforce and other large companies have a set of their own cloud computing platform.

Libo Yin, the Chief engineer of Institute of Electronic Science and technology information, industry and information technology, once said: cloud computing has become a priority to promote for the development of the national government, due to its advantages of saving cost, ease of maintenance, flexible configuration, etc.. America, Britain, Australia and other countries have introduced the relevant development policies and promoted the transfer of information system of government departments to the cloud computing plat. However, at the same time, using cloud computing services has also brought with challenges to its sensitive data and important business for government departments. The United States, as an advocate of cloud computing services, launched "cloud priority strategy" on the one hand, and argued that the cloud computing services, provided to the federal government, must pass through the security review on the other hand. Thus the importance of cloud computing network security is evident.

Research firm Gartner released a report [1] in 2008 in which 7 major risks of cloud computing technology are listed. International Data Corporation (IDC) has also made corresponding surveys of cloud computing security, a survey in 2009 found that the top three threats, facing by cloud computing services, were service security, stability and performance [2]. Cloud Computing Security Alliance (CSA) listed 9 security threats in the field of cloud computing in the report named "9 major scourge: 2013 cloud computing threat ranking" [3], which reflected the view of industry experts for cloud computing security, and listed the various threats associated with cloud computing emphatically. It is urgent to solve security problems of cloud computing. As a basic part, cloud computing security risk assessment plays an important role in resolving the security problem in cloud system. In this article, we will discuss the details in risk assessment.

2 Related Work

With the promotion of cloud computing, cloud computing security gets more and more attention, cloud computing security risk assessment plays an important role in the process of solving cloud computing security issues. For this reason, many people have been making unremitting efforts. At home, Jiang Rong et al. discussed the impact of security risk on the development of cloud computing, and analysed the research status of cloud computing security risk theory [4]. Zhang Jing et al. presented rough network security analysis model combining attack rough graph and dynamic game theory [5]. Liu Peryu et al. summarized 8 kinds of security threats and raised an information security risk assessment model in cloud computing environment based on analytic hierarchy process [6].

Abroad, Saripalli Ben and Walters Prasad proposed a quantitative risk assessment framework for Cloud Security and evaluated the security risk of cloud computing platform [7]. Djemame Karim et al. designed an effective risk assessment model for cloud service providers, which included risk identification, risk assessment and corresponding countermeasures [8]. Shameli-Sendi Mohamed and Cheriet Alireza proposed a security risk assessment framework related to cloud computing platform, and realized the quantitative security risk assessment of cloud computing platform using the methods of iterative and incremental [9]. Furuncu Evrim and Sogukpinar Ibrahim had established a
scalable security risk assessment model based on game theory and used this model to evaluate whether the cloud computing network need to be repaired [10].

Cloud computing security has become a research hotspot in recent years, and cloud computing security risk assessment is an essential part of the basic link. As an important analytical method and tool, game theory has been widely used in the fields of economics, political science, military strategy, chemical and contemporary computer science. From the view of information security and considering the confidentiality, integrity and availability of information, a game model will be built between the attacker and defender of the cloud computing network in this paper and using this model, assessment of the security risks of cloud computing network will be done.

3 Cloud Computing Risk Assessment Model

The cloud computing risk assessment model in this paper consists of three parts, the participants, the action set, and the utility function.

The participants include the attackers and defenders of cloud computing networks. An attacker will try the best to use the minimum cost to obtain the largest damage of cloud computing network. In contrast, the defender will minimize the loss of the cloud computing network to the greatest extent. In the cloud computing network, the attacker and the defender will make the appropriate adjustments to the strategies they take according to the other side's measures. In the course of a game between an attacker and a defender, the attacker could select to attack or not to attack, expressed as \( SA = \{ \text{Attack}, \text{No Attack} \} \). Correspondingly, defender may choose to defend or not, referred to as \( SD = \{ \text{Defence}, \text{No Defence} \} \). Thus, four kinds of states are formed by attacker and defender, these are (Attack, Defence), (No Attack, Defence), (No Attack, Defence) and (No Attack, No Defence).

The attacker's utility function is defined as \( U_A = A_B - A_C \), in which \( A_B \) and \( A_C \) are the benefit and cost of attacker, accordingly, the utility function of defender is \( U_D = D_B - D_C \), \( D_B \) and \( D_C \) are the benefit and cost of defender. The benefit of attacker, \( A_B \), is considered to be that the damage of the network minus the restore and the punish by the defender when the defender detect the attacker, while the benefit of defender, \( D_B \), is the damage of the network minus the restore. The cost of attack, \( A_C \), consists of resource consumption (\( A_{CE} \)) and time consumption (\( A_{CT} \)). Apart from resource consumption and time consumption, the cost of defender also includes the consumption of recovery system (\( D_{CR} \)).

Defining that the damage of cloud computing system \( \text{Damage} = L_C \times V_C + L_I \times V_I + L_A \times V_A \), in which \( V_C \), \( V_I \), and \( V_A \) are the values of confidentiality, integrity, availability of the information in cloud network respectively, while \( L_C, L_I, L_A \) indicate the damage coefficients in C, I, A three parts when the cloud network is under attack and different attack types have different damage coefficients in different aspects of the system.

### Table 1 the damage coefficient of different attack types

<table>
<thead>
<tr>
<th>Attack Type</th>
<th>Damage Coefficients</th>
</tr>
</thead>
<tbody>
<tr>
<td>DoS</td>
<td>( L_C ) ( L_I ) ( L_A )</td>
</tr>
<tr>
<td>User</td>
<td>0.5 0.8 0.1</td>
</tr>
<tr>
<td>Root</td>
<td>1 1 0.4</td>
</tr>
</tbody>
</table>

### Table 2 Recovery coefficient of different attack types

<table>
<thead>
<tr>
<th>Attack Type</th>
<th>Recovery Coefficients</th>
</tr>
</thead>
<tbody>
<tr>
<td>DoS</td>
<td>( R_C ) ( R_I ) ( R_A )</td>
</tr>
<tr>
<td>User</td>
<td>0.8 0.9 0.5</td>
</tr>
<tr>
<td>Root</td>
<td>0.95 0.95 0.2</td>
</tr>
</tbody>
</table>

We assume that defender detect the attacker with the probability of \( p_D \) and the detect results include correct detection, false detection and missed detection.

The participants include the attackers and defenders of cloud computing networks. An attacker will try the best to use the minimum cost to obtain the largest damage of cloud computing network. In contrast, the defender will minimize the loss of the cloud computing network to the greatest extent. In the cloud computing network, the attacker and the defender will make the appropriate adjustments to the strategies they take according to the other side's measures. In the course of a game between an attacker and a defender, the attacker could select to attack or not to attack, expressed as \( SA = \{ \text{Attack}, \text{No Attack} \} \). Correspondingly, defender may choose to defend or not, referred to as \( SD = \{ \text{Defence}, \text{No Defence} \} \). Thus, four kinds of states are formed by attacker and defender, these are (Attack, Defence), (No Attack, Defence), (No Attack, Defence) and (No Attack, No Defence).
Below is the analysis of four states of attack and defence:

1. (Attack, Defence)
   When a defender correctly detects an attack with the probability of \( p \), the attacker will be punished by the system, its benefit \( A_{\text{Benefit}} = \text{damage} - \text{restore} - A_{\text{Punish}} \), and the benefit of defender \( D_{\text{Benefit}} = -\text{damage} + \text{restore} \), while the costs of attack and defender are \( A_{\text{Cost}} = A_{\text{CE}} + A_{\text{CT}} \), and \( D_{\text{Cost}} = D_{\text{CE}} + D_{\text{CT}} + D_{\text{CR}} \) respectively.

   When the defender misses the attack with the probability of \( (1-p) \), at this time, \( A_{\text{Benefit}} = \text{damage} \) and \( D_{\text{Benefit}} = -\text{damage} \), \( A_{\text{Cost}} = A_{\text{CE}} + A_{\text{CT}} \) and \( D_{\text{Cost}} = D_{\text{CE}} + D_{\text{CT}} \).

   In conclusion, in the first state, the attacker's expectation of benefit is
   \[
   (\text{damage} - \text{restore} - A_{\text{Punish}}) \times p + \text{damage}(1-p)
   \]
   the defender's expectations for benefit is
   \[
   (\text{damage} + \text{restore}) \times p + (-\text{damage})(1-p)
   \]

   Cost expectations of the attacker and defender are \( A_{\text{Cost}} = A_{\text{CE}} + A_{\text{CT}} \) and \( D_{\text{Cost}} = D_{\text{CE}} + D_{\text{CT}} \).

2. (Attack, No Defence)
   In this case, the benefits of attacker and defender are \( A_{\text{Benefit}} = \text{damage} \) and \( D_{\text{Benefit}} = -\text{damage} \) while the costs of attacker and defender are \( A_{\text{Cost}} = A_{\text{CE}} + A_{\text{CT}} \) and \( D_{\text{Cost}} = 0 \) correspondingly.

3. (No Attack, Defence)
   When the defender is correctly detected, where the attack is not detected, \( A_{\text{Benefit}} = 0 \), \( D_{\text{Benefit}} = 0 \) and \( A_{\text{Cost}} = 0 \), \( D_{\text{Cost}} = D_{\text{CE}} + D_{\text{CT}} \).

   When the defence appears error measurement, where the attack does not exist in fact, but the result of detection is that there exists attack, the detection results will cause a series of responses of the system including restoring the system, and resulting in the waste of resources. Thus, \( A_{\text{Benefit}} = 0 \), \( D_{\text{Benefit}} = 0 \) and \( A_{\text{Cost}} = 0 \), \( D_{\text{Cost}} = D_{\text{CE}} + D_{\text{CT}} + D_{\text{CR}} \).

4. (No Attack, No Defence)
   Under this circumstance, both attacker and defender have no corresponding action, so, \( A_{\text{Benefit}} = 0 \), \( D_{\text{Benefit}} = 0 \) and \( A_{\text{Cost}} = 0 \), \( D_{\text{Cost}} = 0 \).

Here are the benefit matrix, cost matrix and payoff matrix of attacker and defender:

### Table 3 Benefit Matrix of Attack and Defence

<table>
<thead>
<tr>
<th></th>
<th>Defence</th>
<th>No Defence</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attack</td>
<td>[((\text{damage} - \text{restore} - A_{\text{Punish}}) \times p + \text{damage}(1-p))]</td>
<td></td>
</tr>
<tr>
<td>No</td>
<td>[0,0]</td>
<td>[0,0]</td>
</tr>
</tbody>
</table>

### Table 4 Cost Matrix of Attack and Defence

<table>
<thead>
<tr>
<th></th>
<th>Defence</th>
<th>No Defence</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attack</td>
<td>[((\text{damage} - \text{restore} - A_{\text{Punish}}) \times p + \text{damage}(1-p))] - ((A_{\text{CE}} + A_{\text{CT}}))</td>
<td></td>
</tr>
<tr>
<td>No</td>
<td>[0, -(D_{\text{CE}} + D_{\text{CT}}) - D_{\text{CR}} \times (1-p)]</td>
<td>[0,0]</td>
</tr>
</tbody>
</table>

### Table 5 Payoff Matrix of Attack and Defence

4 Numerical Calculation and Analysis

Calculation of \( P_D \) and \( P_A \) by Nash equilibrium:

\[
[\text{damage} - \text{restore}(1-p)] 
\]

\[
[(\text{damage} + \text{restore}) \times p + (-\text{damage}) \times (1-p)]
\]

Obtaining that:

\[
P_D = \frac{\text{damage} - (A_{\text{CE}} - A_{\text{CT}})}{(\text{restore} - A_{\text{Punish}}) \times p}
\]

\[
P_A = \frac{D_{\text{CE}} + D_{\text{CT}} + D_{\text{CR}} \times (1-p)}{D_{\text{CR}} \times (1-2p) + \text{restore} \times p}
\]
As shown in Figure 4, when the value of restore is constant, the probability of defender increases with the increase of the damage of the system. While in the same way, the probability of defender decreases due to the increase of restore value.

From Figure 5, the probability of attacker decrease as the increase of correct detecting rate $p$ under the premise of the restore value is constant.

Because the defence consumption is far less than the node's total assets in the cloud network, so we assume that, the cost of resource and time in the process of detecting is 5, expressed as $D_{CE} + D_{CT} = 5$. Supposing that the cost of defender in resource and time is equal to the cost of attacker, so $A_{CE} + A_{CT} = 5$.

Defining that the system cost $D_{CR}$ is a linear function of the recovery value when the defender repair the system, which is expressed that $D_{CR} = \varepsilon \times restore$, in this paper, we set the value of $\varepsilon$ is 0.5.

Similarly, we premise that the penalty for an attacker is the linear function of the system damage: $A_{Punish} = \beta \times damage$, in this paper, $\beta = 1$.

Here is the analysis of three different attack types of a node in cloud computing network, the total asset value of the node $V(V_C, V_I, V_A)$, the probability of correct detection $p$, and the probability of false detection or missed detection $(1-p)$ are shown in the following table:

Table 6 Node information

<table>
<thead>
<tr>
<th>Node A</th>
<th>Node asset</th>
<th>Attack type</th>
<th>p</th>
<th>1-p</th>
</tr>
</thead>
<tbody>
<tr>
<td>(80,100,50)</td>
<td>DoS</td>
<td>0.6</td>
<td>0.4</td>
<td></td>
</tr>
<tr>
<td></td>
<td>User</td>
<td>0.75</td>
<td>0.25</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Root</td>
<td>0.85</td>
<td>0.15</td>
<td></td>
</tr>
</tbody>
</table>

Table 7 Damage value and Recovery value

According to table 1, table 2 and table 6, we calculate the damage and recovery values of the cloud computing network under different attack types:

<table>
<thead>
<tr>
<th>Node A (80,100,50)</th>
<th>Damage</th>
<th>Restore</th>
<th>Punish</th>
<th>$D_{CR}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>DoS</td>
<td>0</td>
<td>40</td>
<td>0</td>
<td>36</td>
</tr>
<tr>
<td>User</td>
<td>40</td>
<td>5</td>
<td>32</td>
<td>2.5</td>
</tr>
<tr>
<td>Root</td>
<td>80</td>
<td>20</td>
<td>76</td>
<td>4</td>
</tr>
</tbody>
</table>

Table 8 The probabilities of attacker and defender

In table 8, under DOS circumstances, if the attacker selects to attack in the probability of 70% and the defender selects to defend in the probability of 80%, the game between attacker and defender will be in Nash equilibrium state. Analyse the other two circumstances with the same theory.

5 Conclusion

In this paper, a cloud computing risk assessment framework has been proposed. Using this framework, analyse three different types attack including the damage value and the restore value of the cloud system, and then, get a payoff matrix. Based on the payoff matrix, the probabilities of attacker and defender have been computed. In the specific calculation process, assume that the system cost $D_{CR}$ and the penalty for an attacker when the defender repair the system are the liner function of the recovery value and the system damage value correspondingly. In the last of the article, specific numerical calculation and analysis were completed.
Acknowledgements

We gratefully acknowledge anonymous reviewers who read drafts and made many helpful suggestions. This work is supported by the National Science and Technology Major Project No. 2015ZX03001041, the National Natural Science Foundation of China under Grant No. 61572072, and the Fundamental Research Funds for the Central Universities "Research on the System of Personalized Education using Big Data".

References