Dynamic Evaluation Model of Cloud Platform User Trust Value Based on Game Theory

Jiangfeng Xu, Kaili Guo and Yonglin Li

ABSTRACT

Trust value mode is becoming more and more significant in computer access control systems. In this paper, we present a dynamic evaluation model of cloud platform user trust value based on game theory in order to resolve the problem of illegitimate access by user. The reward and punishment factors are set in the model, and the legal access behavior will be rewarded, the illegitimate access behavior will be punished. It will make users to choose legal access under their own interests, which will protect the system. We make an experiment in cloud platform using this model, and the result shows that the model has a good effect on the user trust value adjustment.

KEYWORDS

Cloud Platform, Trust Mode, Game Theory, Access Control.

INTRODUCTION

With the development of Internet technology, increasing number of cloud computing is widely used in daily life. But the information security issues have emerged. The security of Internet information has become a serious issue. To solve this problem, Scholars have proposed various access control models. Access control[1] is an important module in computer systems, it is used to protect the security of computer system resource. Scholars at home and abroad studies the access control in the cloud computing environment and proposes some reasonable access control models[2].The traditional access control model is unable to meet the access control requirements of the cloud platform due to its coarse-grained and complex management capabilities[3]. Experts propose an access control model based on trust value[4]. Combined the advantages of traditional model and the user trust value can meet the needs of the modern computer system for the access control model. An important criterion for model performance is the accurate calculation of the user's trust value, which determines the accuracy and personalized access requirements of the access control model[5].

The structure of this paper is as follows. The next section, we review some related work in trust value mode and access control. In section 3, we propose a model for the cloud platform users to evaluation trust value dynamically by using
game theory. In section 4, we describe this model in detail. In section 5, we built a cloud platform by using Hadoop and do some experiments to verify this model. The result shows that this model can protect resources very well in cloud platform. In section 6, we conclude this paper and discuss some work in the future.

RELATED WORK

Trust is a part of our daily life and also be used as a significant security policy for the internet security. The trust value of user's is a standard to reflect whether the user's behavior reaches the standard. A trust relationship between the user and the system is established through the compare of the threshold and the system resource. Alfarze[6] analysis the shortcomings of the trust model, and also propose a new trust model. It will calculate the trust value of each node. And then a trust matrix is formed. Finally, the global trust value is calculated. At present, most people have done quite a number of research on the evaluation of trust value. There are mainly the following measurement methods: virtual arc iteration method, discrete trust value representation method and method based on fuzzy theory.

With the development of game theory[7], many researchers have introduce the idea of game theory into the Internet, especially the emergence of open networks[8-9]. The reward and punishment constraint mechanism of interactive entity behavior in different networks is given in literature[10-12]. But the selection strategy of entity behavior is not optimized and the effect of curbing entity selection of illegitimate access is not very good.

Based on the above research, this paper establishes a dynamic adjustment model of user trust value based on game theory. In the process of the game between two parties, the user's trust value is directly related to the access policy selected by the user. When the user chooses to access the law, the system will give a certain reward to the user's trust value. The system will impose a certain penalty on the user's trust value when the user illegitimately accesses. This process is the dynamic changes in user trust values.

USER TRUST VALUE DYNAMIC EVALUATION MODEL

Game Theory in Access Control

It can solve some security problems in cloud platforms by combining game theory with access control. Through the game theory to analyze the access control, the subject sends an access request to the object, and the object return the request result. We can regard it as a process of two-player game. They all have their own selection strategies and there are no external constraints, it is a noncooperative game. The subject has both legal and illegitimate access policies, at the same time the object also has two strategies to allow and reject access to the subject. On account of the game theory, the system will make corresponding judgments according to the behavior of the subject, and then decide whether to reward or punish the user's trust value. For the user, the income is reward or punishment of user's trust value. And for the cloud platform the system protects its own resources.
by rejecting the user’s illegitimate access, or allows the user's legitimate access for the cloud platform. Expanding its influence can be seen as a benefit of the cloud computing platform. The cloud platform access control based on game theory can be described as follows:

- Both parties involved in game: The user who initiate access request and the cloud platform.
- Game strategy: A complete access control constraint. The user’s policy is to access the cloud platform legitimate and illegitimate. The cloud platform’s policy is to allow or reject access requests from users.
- Game revenue: Under the respective strategies, increase or lost benefits for both users and cloud platforms.

**Game Model**

In order to motivate users to access resources legally, some constraints are set here. When a user use illegitimately policy access a resource, the system will impose a penalty according to the situation until the trust value is reduced to 0. If the user use legally policy access a resource, using $\sigma (\sigma \in (0,1))$ to represent the reward factor, the user's trust value will increase by $\sigma$. The game tree form thus obtained is shown in Figure 1. In the above figure, the specific meanings of the parameters of the game process are as follows:

- **U.legal.al**: The user's income is that the user adopts a legitimate access policy, the cloud platform allows the user's access request.
- **O.legal.al**: The cloud platform’s income is that the user adopts a legitimate, the cloud platform allows the user’s access request.
- **U.legal.de**: The user’s income is that the user adopts a legitimate access policy, the cloud platform rejects the user’s access requests, the user does not get access permission to the resources.
- **O.legal.de**: The cloud platform’s income is that reject the legitimate access requests of the user, leading to their own interests were at loss.
• U.illegal.al: The user’s income is that the user adopt the illegitimate access policy, the cloud platform allows the user’s access request.

• O.illegal.al: The cloud platform’s income is that the user adopt the illegitimate access policy, and the cloud platform suffers losses due to allow the user's request.

• U.illegal.de: The users adopts the illegitimate access policy, and the user suffers losses when the cloud platform rejects the user to initiate a request for access to the resource.

• O.illegal.de: The cloud platform’s income is that the users adopt the illegitimate access policy, the cloud platform protection its resource by rejects the users requests.

Thus, we can get the income matrix of users and cloud platform, as shown in Table I.

### TABLE I. GAME INCOME MATRIX.

| Participants | Cloud platform |
|--------------|----------------|
| User         |                |
| Legitimate   | Access         |
|              | (U.legal.alO.legal.al) |
|              | Reject         |
|              | (U.legal.deO.legal.de) |
| Illegitimate | Access         |
|              | (U.illegal.alO.illegal.al) |
|              | Reject         |
|              | (U.illegal.deO.illegal.de) |

### REWARD AND PUNISHMENT MECHANISM

When a resource is illegitimate accessed by a user, the system reduces it's trust value. The user's income from illegitimate access to the resource is:

\[ X = U.illegal.al + U.illegal.de \]  
(1)

When users continue to choose to use legitimate access resources, the trust value will continue to increase. The specific benefits are:

\[ Y = U.illegal.al + \sigma U.illegal.de + \sigma^2 U.legal.al + \cdots \]  
(2)

\[ Y = U.legal.al / (1 - \sigma) \]  
(3)

Among them, \( \sigma \) is a reward factor. Use \( F \) to represent the user’s access control policy, based on the above can be obtained:

- If \( X > Y \), \( F = \) legitimate
- If \( X = Y \), \( F = \) legitimate or illegitimate
- If \( X < Y \), \( F = \) legitimate

Therefore, when the user selects that the expect benefit of the illegitimate access is greater than the expect benefit of the legitimate access, the user will select the illegitimate access. When the user selects the expected return to the illegitimate access equal to the expected return to the legitimate access, the user may select the legitimate access or illegitimate access. When the user chooses that the expected
benefit of illegitimate access is less than the expected return to legitimate access, the user will always choose legitimate access.

If \( X<Y \), this means that users' legitimate access to resources will get more payoffs in the future, so it will select the legitimate access strategy, namely

\[
\sigma > \frac{U.\text{illegal.al}+U.\text{illegal.de}-U.\text{legal.al}}{U.\text{illegal.al}+U.\text{illegal.de}}
\]  \hspace{1cm} (4)

The system will punish the user for the following situations according to the severity of the user's illegitimate access:

1) Increasing the threshold of user’s access to resources, making it more difficult to access.
2) The trust value is dynamically adjust by setting a penalty factor \( \beta (\beta \in (0,1)) \)
3) When the number of times the user illegitimately access the resource is greater than (equal to) the number of times the system can be tolerated, the user will be forbidden to access the resource forever.

In the process of user transition strategy from legal to illegitimate, the user's loss \( U.\text{loss} \) can be calculated through the reward and punishment mechanism. The loss at the kth is the sum of all previous losses. The \( U.\text{loss} \) is defined as

\[
U.\text{loss} = \sum_{0}^{k-1} \frac{1}{\beta^{k-1}} U.\text{illegal.de}
\]  \hspace{1cm} (5)

During the transition strategy from legal to illegitimate, the user can analyze his biggest loss through the game theory, and obtain the comprehensive trust value \( TV(t+1)=TV(t)-U.\text{loss} \) after the user illegitimately accesses. In turn, it is determined whether the user's trust value is less than the current threshold. This mechanism greatly protects the security of the system and prevents users from converting from legitimate access to illegitimate access, which has a certain deterrent effect on users who have illegitimate access.

In general, the reward and punishment mechanism can be described using Figure 2.
EXPERIMENT AND ANALYSIS

In order to verify the effect of the reward and punishment mechanism, we built a cloud platform by using Hadoop. It’s a single node cluster in Linux operate system. We assumed that the game income matrix of the two parties is shown in Table II. Before the time t, the interaction strategy between the user and the cloud platform is (legal, allowed), then the revenue is (8, 8). Now if the user chooses to access illegitimately, the cloud platform allows, the user will get 20 benefits, but from time t+1, the cloud platform will punish users.

| Participants | Cloud platform |
|--------------|----------------|
| User         |                |
| User         | Behavior       | Access       | Reject       |
| User         | Legitimate     | (8,8)        | (0,-5)       |
| User         | Illegitimate   | (20,-10)     | (-10,10)     |

Set the initial trusts value of 0.5. Adjust the values of σ bonus factor and β penalty factor respectively when the initial value is unchanged, and use the legally
allowed and illegitimate rejection strategies to calculate the values of $\sigma$ and $\beta$. We can get the following evaluation results as shown in Figure 4 and 5.

From the above two figures, we can see that when $\sigma = 0.5$, the trust value of the entity convergence speedily obviously faster than the others, and when $\sigma = 0.3$, the trust value of the entity converges the slowest, we can take the value of $\sigma = 0.4$ as a reward factor for legitimate access. When $\beta=0.1$, the trust value of the entity decreases the fastest, $\beta=0.2$, and $\beta=0.3$, the slowest decline rate, which can take the intermediate value as the penalty factor for the illegitimate access of the subject.

The experimental parameters are set as follows: set $\sigma=0.4$, $\beta=0.2$ respectively, as a factor of reward and punishment mechanism, the initial trust value is 0.5. Seven users are randomly selected, namely U1, U2, U3, U4, U5, U6 and U7, among them U1, U3, U5, and U6 are legitimate access subjects, and U2, U4, and U7 are random number illegitimate access subjects. In order to better reflect the effect of the reward and punishment mechanism, using the reward and punishment mechanism in this paper and article[13] and the unused reward and punishment mechanism[14] to compare, set the system to tolerate the minimum number of illegitimate accesses to 3, the number of interactions is 5. The access behavior matrix is as in Figure 3:

\[
\begin{array}{cccc}
1 & 1 & 1 & 1 \\
1 & 0 & 1 & 1 \\
1 & 1 & 1 & 1 \\
0 & 1 & 0 & 0 \\
1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 \\
1 & 0 & 0 & 1 \\
\end{array}
\]

Figure 3. The access behavior matrix.

0 represents illegitimate access and 1 represents legal access. According to the above access behavior matrix, the income of the subject under the adoption and lack of reward and punishment mechanism can be obtained. Figure 6 shows the comparison of the returns of each entity in three cases, and

Figure 4. The relationship between the reward factor $\sigma$ and the trust value.
Figure 5. The relationship between the penalty factor $\beta$ and the trust value.

Figure 6. Expected trust value in different reward and punishment mechanisms.

Figure 7. The change of U4 trust value.

Figure 7 shows the change of the trust value of U4 in the case of the reward and punishment mechanism.

As can be seen from the above figure, the expected returns of the entities U1, U3, U5, U6 under the incentive mechanism are always higher than those without incentive mechanism. The expected benefits of U2, U4 and U7 can be divided into two cases. One is that the number of U4 illegitimate accesses reaches the minimum number of illegitimate accesses that the system tolerates, the return is 0. The other is U2, U7, the number of illegitimate visits does not reach the minimum number of illegitimate visits tolerated by the system, and under the effect of the reward and punishment mechanism, the expected return is less than the case without the reward.
mechanism. This dynamic trust value change strategy protects the security of the system.

CONCLUSION

In this paper, the user's access control model is transformed into a double game problem. In order to enable users to access resources legally, a dynamic evaluation model of user trust value based on game theory is proposed. The user's access behavior is monitored in real time, and the user's trust value is dynamically adjusted according to the user's access behavior. It can be obtained through experiments and the model proposed in this paper has a good performance in power consumption, and it has a certain inhibitory effect on the illegitimate access behavior of users. However, in the cloud platform, the actual number of users will be more than the number of users in the experiment. When the number of users reaches a certain level, the impact of the model on system performance should be considered. In the future, we can optimize the structure and algorithm of the model to reduce the impact of the model on the system.

REFERENCES

1. Butler W, Lampson. Protection[J].Proc.5th Princeton Symposium on Information Sciences and Systems,1971:437-443.
2. Mingbin Zhao, Zhiqiang Yao. Access control model based on RBAC in cloud computing[J]. Computer application, 2012, 32(S2):267-270.
3. Wang YD, Yang JH, Xu C, Ling X, Yang Y. Survey on access control technologies for cloud computing. Ruan Jian Xue Bao/Journal of Software, 2015,26(5):1129-1150 (in Chinese). http://www.jos.org.cn/1000-9825/4820.htm.
4. Li Feng-hua, Su Mang, Shi Guo-zhen, Ma Jian-feng. Research Status and Development Trends of Access Control Model[J]. ACTA Electronicasinica, 2012, 40(04):805-813.
5. Xu Hao-Hai, Yu Jiong, Bian Chen, Lu Liang, Jin Liang. Structure data access control model based on credit value[J]. Computer Engineering and Desing, 2018, 39(08):2407-2411.
6. Abdul-Rahman, Alfarez, Stephen Hailes. A distributed trust model[C]. Mics, 1997.
7. Fudenberg D and Tirole J. Game Theory[M].Cambridge, Massachusetts, US, MIT Press, 1991: 275–277.
8. Xing Gao, Weijun Zhong, Shue Mei. A game-theory approach to configuration of detection software with decision errors [J]. Reliability Engineering & System Safety, 2013, 119: 35-43.
9. Tarek Alskaif, Manel Guerrero Zapata, Boris Bellalta. Game theory for energy efficiency in wireless sensor networks: Latest trends [J]. Journal of Network and Computer Applications, 2015, 54: 33-61.
10. Iosifidis G, Gao Lin, and Huang Jianwei. Incentive mechanisms for user-provided networks[J]. Communications Magazine IEEE, 2014, 52(9): 20–27.
11. Wu Tinyu, Lee Weitsong, Guizani N, et al. Incentive mechanism for P2P file sharing based on social network and game theory[J]. Journal of Network and Computer Applications, 2014, 41(5): 47–55.
12. Ciobanu R, Dobre C, Dascalu M, et al. SENSE: A collaborative selfish node detection and incentive mechanism for opportunistic networks[J]. Journal of Network and Computer Applications, 2014, 41(5): 240–249.
13. Wang Y, Cui Z, Yin G, et al. A game theory-based trust measurement model for social networks[J]. Computational Social Networks, 2016, 3(1):2.
14. Z. Tan, Z. Tang, R. Li, et al. Research on trust-based access control model in cloud computing[C]. 2011 6th IEEE Joint International Information Technology and Artificial Intelligence Conference, Chongqing: IEEE, 2011:339-344.