Research on Security Investment Strategy of Cloud Service Providers and Users Based on Differential Game

Xuan Guo[1], Lingfei Ma[2], Jie Leng[1,*]

[1]School of Management Science and Engineering, Dongbei University of Finance & Economics, Dalian, 116025, China
[2]School of Accounting, Dongbei University of Finance & Economics, Dalian, 116025, China

Xuan Guo:377622305@qq.com
Lingfei Ma:1422003406@qq.com
*Jie Leng,E-mail:lengjie2022@163.com

Abstract. This study uses the principle of differential game theory to explore the security investment decision and coordination strategy between cloud service providers and users. The Hamilton-Jacobi-Bellman equation is used to determine the equilibrium solution for non-cooperative decision making and cooperative decision making. These solutions are then compared, analyzed, and simulated. The results show that under collaborative decision-making, cloud service providers and users reach the highest level in terms of optimal security investment, system security and total system revenue, reaching Pareto optimality. These findings provide valuable theoretical insights to guide security investment decisions for cloud service providers and users.

Keywords: Cloud security; Safe investment decisions; Cooperation mode; Differential game.

1 Introduction

With the advancement of information technology, cloud computing has emerged as the cornerstone of the digital economy and a pivotal infrastructure for enterprise digital transformation. The onset of the COVID-19 pandemic has further expedited the transition of enterprises towards cloud services, intensifying the spotlight on cloud security. Particularly amidst the backdrop of frequent cloud security incidents, security concerns have emerged as a significant obstacle impeding the broader advancement and adoption of cloud computing applications. These security risks leading to cloud security incidents can be categorized into those originating from cloud service providers and those from cloud users [1]. Consequently, unlike traditional information security paradigms, cloud security necessitates the collective involvement of both cloud service providers and users, with shared responsibility for upholding cloud security. Effectively addressing the security challenges posed by cloud computing represents a pressing issue that demands collaborative attention from both parties. However, constrained by the coordination dynamics between them, prevalent issues persist in cloud

B. Siuta-Tokarska et al. (eds.), *Proceedings of the 2024 2nd International Conference on Management Innovation and Economy Development (MIED 2024)*, Advances in Economics, Business and Management Research 300,
https://doi.org/10.2991/978-94-6463-542-3_19

security maintenance. These include fragmented investments, redundant constructions, disparate resource integration, and the absence of cohesive security measures coordination. Hence, analyzing the behavioral dynamics between cloud service providers and users as the primary stakeholders in cloud security maintenance, and exploring coordination strategies for security investment decisions, holds significant practical significance in fostering cloud security and advancing cloud computing innovation and development.

Although various studies have been conducted on cloud security from different perspectives [2], there are still obvious shortcomings. First of all, in cloud computing application scenarios, the lack of dynamic game dynamics between cloud service providers and users in continuous time directly affects the security investment decisions of both sides. Second, the failure to take into account the dynamic evolution of cloud security levels is not conducive to the development of effective coordination strategies and the outcome of the game between them. The interaction between cloud service providers and users in cloud security maintenance is a continuous dynamic game process [3]. Differential game theory is a dynamic model that analyzes the competition and cooperation of multiple parties in continuous time. Therefore, this paper attempts to establish a differential game model to investigate the dynamic game dynamics between cloud service providers and users as the main stakeholders of cloud security maintenance [4]. By solving the game equilibrium in non-cooperative decision making and cooperative decision making mode, the equilibrium results are compared and analyzed. The findings are designed to provide valuable insights into security investment strategies for cloud service providers and users.

2 Problem Description and Basic Assumptions

This paper focuses on the cloud security system, comprising cloud service providers (G) and cloud users (E), as its research subject. It delves into the security investment decisions of both cloud service providers and users within the realm of cloud security maintenance. Cloud users, whether enterprises or individuals, who utilize cloud services and share security responsibilities with cloud service providers are considered integral components of this system. Conversely, organizations that furnish public cloud services and shoulder the responsibility of maintaining cloud security for users, such as Alibaba Cloud and Huawei Cloud, are categorized as cloud service providers. In this context, both cloud service providers and users have the agency to invest in security measures aimed at fortifying the security of the cloud service system. These investments encompass bolstering protection resource configurations (e.g., implementing firewalls, deploying antivirus systems) and enhancing staff training and management. Both entities are rational actors in this scenario. The fundamental assumptions of the model are as follows:

The security investment cost of cloud service providers and cloud users is positively correlated with their security investment level, and increases with the increase of security investment, and the increase rate is on the rise. Therefore, the security cost function of both parties is constructed as follows:

$$C_G(t) = \xi_G E_G^2(t)/2 \quad C_E(t) = \xi_E E_E^2(t)/2 \tag{1}$$

Where, $E_G(t)$ and $E_E(t)$ respectively represent the security investment level of cloud service providers and cloud users, and ξ_G and ξ_E respectively represent the cost coefficient of cloud service providers and cloud users in the maintenance process of cloud security level. Cloud security level is jointly determined by cloud service providers and cloud users, and there is a natural decay of cloud security level. In addition, this article does not consider scenarios where the level of cloud security, such as on-premises private clouds, is entirely determined by a single stakeholder. Therefore, the change of cloud security level over time is described as a differential equation [5]:

$$\begin{cases} \tau(t) = d\tau(t)/dt = \zeta_G E_G(t) + \zeta_E E_E(t) - \delta\tau(t) \\ \tau(0) = \tau_0 \geq 0 \end{cases} \tag{2}$$

Where, ζ_G and ζ_E represent the influence coefficient of security investment level of cloud service providers and cloud users on cloud security level respectively. With the increase of time, the cloud security level gradually decreases due to outdated security policies, lagging technical solutions, aging hardware facilities and other factors. δ is defined as the cloud security level attenuation coefficient. $\tau(0)$ is the cloud security level at the initial moment. The total revenue of the cloud security system is determined by the level of security investment of the cloud service provider and cloud users and the cloud security level of the system. On the one hand, the security investment behavior of cloud service providers and cloud users will generate advertising effect, enhance the corporate image, and bring reputation benefits to the cloud security system. On the other hand, when the cloud security level is guaranteed and cloud-related businesses run smoothly, cloud service providers can attract more users and expand profits. Cloud users can improve management efficiency, reduce the difficulty of development, operation and maintenance, and reduce the overall business cost. The above reputation and economic benefits brought by the improvement of cloud security level to both sides of the game are regarded as the benefits of all parties. Reference [6] describes the total benefits of cloud security system as follows:

$$\pi(t) = \alpha_G E_G(t) + \alpha_E E_E(t) + \beta\tau(t) \tag{3}$$

Where, α_G and α_E respectively represent the impact coefficient of cloud service providers and cloud users' maintenance of cloud security on the total system revenue, and β represents the impact coefficient of cloud security level on the total system revenue. Assume that the total revenue of the cloud security system is divided between the two, and the distribution ratio is γ and $1-\gamma$, respectively. Since this income distribution is related to existing factors such as the nature of cloud users, the

type of cloud services and the management mode of cloud services, the model treats this income distribution coefficient as an exogenous variable. In the infinite time range, both cloud service providers and cloud users seek to maximize their own benefits in the infinite time range, and the discount factor is ρ.

3 Model Construction

According to the coordination relationship between the two sides of the game, it can be divided into two decision-making modes :(1) non-cooperative decision-making mode, in which the cloud service provider and the cloud user do not take any cooperation measures and make independent decisions based on the principle of maximizing their own interests; (2) Collaborative cooperation mode. Both cloud service providers and cloud users are aware of the positive impact of maintaining cloud security on their own interests, and both parties actively cooperate on security and make centralized decisions based on the principle of optimal cloud security system revenue.

3.1 Non-Cooperative Decision-Making Model

First, the non-cooperative decision-making mode (represented by superscript N) is analyzed. In the case that both parties have no cost sharing contract restrictions, make independent decisions and pursue the maximization of their own benefits, the objective functions of cloud service providers and cloud users are as follows:

$$\max_{E_G} J_G^N = \int_0^\infty e^{-\rho t}(\gamma(\alpha_G E_G^N + \alpha_E E_E^N + \beta\tau - \frac{1}{2}\xi_G E_G^{N2})dt \tag{4}$$

$$\max_{E_E} J_E^N = \int_0^\infty e^{-\rho t}((1-\gamma)(\alpha_G E_G^N + \alpha_E E_E^N + \beta\tau) - \frac{1}{2}\xi_G E_E^{N2})dt \tag{5}$$

In order to obtain the feedback balancing strategy of cloud service providers and cloud users, the Hamilton-Jacobi-Bellman equation is used to solve the objective function in non-cooperative decision-making mode, and the solution result is shown in proposition 1.

Proposition 1. The optimal security investment between cloud service providers and cloud users in non-cooperative decision-making mode is as follows:

$$E_G^{N*} = \frac{\gamma(\alpha_G(\rho+\delta) + \beta\zeta_G)}{\xi_G(\rho+\delta)}, E_E^{N*} = \frac{(1-\gamma)(\alpha_E(\rho+\delta) + \beta\zeta_E)}{\xi_E(\rho+\delta)} \tag{6}$$

The optimal trajectory of cloud security level can be obtained from proposition 1 as follows:

$$\tau^{N*}(t) = (\tau_0 - \frac{L^N}{\delta})e^{-\delta t} + \frac{L^N}{\delta} \tag{7}$$

Among them, $L^N = \frac{\zeta_G \gamma(\alpha_G(\rho+\delta)+\beta\zeta_G)}{\xi_G(\rho+\delta)} + \frac{\zeta_E(1-\gamma)(\alpha_E(\rho+\delta)+\beta\zeta_E)}{\xi_E(\rho+\delta)}$.

On this basis, the total revenue of the system under the non-cooperative decision-making mode can be further obtained as follows:

$$V^{N*}(\tau) = \frac{\beta}{\rho+\delta}\tau + \frac{\gamma(2-\gamma)(\alpha_G(\rho+\delta)+\beta\zeta_G)^2}{2\rho\xi_G(\rho+\delta)^2} + \frac{(1-\gamma)^2(\alpha_E(\rho+\delta)+\beta\zeta_E)^2}{2\rho\xi_E(\rho+\delta)^2} \tag{8}$$

Proposition 1 shows that in the non-cooperative decision-making mode, both cloud service providers and cloud users take maximizing their own interests as the decision-making goal, and the security investment decisions of both parties in this case do not consider the overall benefits of the system.

3.2 Cooperative Mode

In order to assume the security responsibility of ensuring the smooth and reliable operation of cloud services, cloud security service providers and cloud users want to ensure the security of cloud services as much as possible in order to improve their reputation and revenue, and cloud users want to ensure the security of cloud services from any perspective. Therefore, both parties are willing to strengthen cooperation and determine their respective optimal strategies based on the consideration of maximizing the overall benefits of the system, namely the cooperative cooperation mode (represented by superscript C). The objective function of the cooperative system is as follows:

$$\max_{E_G, E_E} J_G^C = \int_0^\infty e^{-\rho t}(\alpha_G E_G^C + \alpha_E E_E^C + \beta\tau - \frac{1}{2}\xi_G E_G^{C2} - \frac{1}{2}\xi_E E_E^{C2})dt \tag{9}$$

Proposition 2. The optimal security investment of cloud service providers and cloud users in non-cooperative decision-making mode is as follows:

$$E_G^{C*} = \frac{\alpha_G(\rho+\delta)+\beta\zeta_G}{\xi_G(\rho+\delta)}, E_E^{C*} = \frac{\alpha_E(\rho+\delta)+\beta\zeta_E}{\xi_E(\rho+\delta)} \tag{10}$$

The optimal trajectory of cloud security level can be obtained from proposition 2 as follows:

$$\tau^{C*}(t) = (\tau_0 - \frac{L^C}{\delta})e^{-\delta t} + \frac{L^C}{\delta} \tag{11}$$

Among them, $L^C = \frac{\zeta_G(\alpha_G(\rho+\delta)+\beta\zeta_G)}{\xi_G(\rho+\delta)} + \frac{\zeta_E(\alpha_E(\rho+\delta)+\beta\zeta_E)}{\xi_E(\rho+\delta)}$.

On this basis, the total revenue of the system under the cooperative cooperation model can be further obtained as follows:

$$V^{C*}(\tau) = \frac{\beta}{\rho+\delta}\tau + \frac{(\alpha_G(\rho+\delta)+\beta\zeta_G)^2}{2\rho\xi_G(\rho+\delta)^2} + \frac{(\alpha_E(\rho+\delta)+\beta\zeta_E)^2}{2\rho\xi_E(\rho+\delta)^2} \tag{12}$$

3.3 Comparative Analysis of Equilibrium Results

Through comparative analysis of the equilibrium solution under the two modes, the following conclusions can be drawn: Compared with the non-cooperative mode, the collaborative cooperation between cloud service providers and cloud users can maximize the enthusiasm of both parties to participate in cloud security maintenance work, and thus promote the increase of optimal security investment of both parties. The system cloud security level in non-cooperative decision-making mode is the lowest, while the system cloud security level in cooperative decision-making mode is the highest. From the perspective of total system revenue, cooperative mode is the highest.

4 Conclusion

This paper takes the cloud security system composed of cloud service providers and cloud users as the research object, and analyzes the security investment decisions and coordination problems of cloud service providers and cloud users as the main body of cloud security maintenance through the construction of differential game model. The results show that in the non-cooperative decision-making mode, the cloud service provider and the cloud user make decisions independently, and the optimal security investment, system cloud security level and total revenue of the two modes are the lowest. In the collaborative cooperation mode, the security investment, cloud security level and total system revenue of cloud service providers and cloud users are the highest, reaching the Pareto optimal. In addition, due to the limitations of model assumptions and other factors, this paper still has many shortcomings, such as network threats and other random factors interfere with the change of cloud security level, and how to affect the cost sharing between the two sides of the game under the condition that the revenue distribution ratio of the cloud security system can be coordinated is not discussed in this paper, and further research is still needed.

Reference

1. Demirezen, E.M., Kumar, S. and Shetty, B. (2020). Two Is Better Than One: A Dynamic Analysis of Value Co-Creation. Production and Operations Management 29(9), 2057-2076.https://doi.org/10.1111/poms.12862.
2. Gill, K.S., Saxena, S. and Sharma, A. (2020). GTM-CSec: Game theoretic model for cloud security based on IDS and honeypot. Computers & Security 92, 101732. https://doi.org/10.1016/j.cose.2020.101732.
3. Hasimi, L., Zavantis, D., Shakshuki, E. and Yasar, A. (2024). Cloud Computing Security and Deep Learning: An ANN approach. Procedia Computer Science 231, 40-47. https://doi.org/10.1016/j.procs.2023.12.155.
4. Jakóbik, A. (2020). Stackelberg game modeling of cloud security defending strategy in the case of information leaks and corruption. Simulation Modelling Practice and Theory 103, 102071.https://doi.org/10.1016/j.simpat.2020.102071.
5. Kakkad, V., Shah, H., Patel, R. and Doshi, N. (2019). A Comparative study of applications of Game Theory in Cyber Security and Cloud Computing. Procedia Computer Science 155, 680-685.https://doi.org/10.1016/j.procs.2019.08.097.
6. Liu, S., Han, W., Zhang, Z. and Chan, F.T.S. (2024). An analysis of performance, pricing, and coordination in a supply chain with cloud services: The impact of data security. Computers & Industrial Engineering 192, 110237. https: //doi. org/ 10. 1016/ j.cie.2024.110237.