Hindawi
Security and Communication Networks
Volume 2020, Article ID 6515328, 18 pages
https://doi.org/10.1155/2020/6515328

Research Article

Research on the Optimization Management of Cloud Privacy Strategy Based on Evolution Game

Pan Jun Sun

School of Electronic Information and Electrical Engineering, Shanghai Jiao Tong University, 800 Dongchuan Rd, Minhang District, Shanghai, China

Correspondence should be addressed to Pan Jun Sun; sunpanjun2008@163.com

Received 5 December 2019; Revised 19 February 2020; Accepted 20 June 2020; Published 11 August 2020

Academic Editor: Leandros Maglaras

Cloud computing services have great convenience, but privacy security is a big obstacle of popularity. In the process result of privacy protection of cloud computing, it is difficult to choose the optimal strategy. In order to solve this problem, we propose a quantitative weight model of privacy information, use evolutionary game theory to establish a game model of attack protection, design the optimal protection strategy selection algorithm, and make the evolutionary stable equilibrium solution method from the limited rational constraint. In order to study the strategic dependence of the same game group, the classical dynamic replication equation is improved by using the incentive coefficient, an improved evolutionary game model of attack protection is constructed, the stability of equilibrium point is further analyzed by Jacobian matrix method, and the optimal selection strategy is obtained under different conditions. Finally, the correctness and validity of the model are verified by experiments, different strategies of the same group have the dual effects of promotion and inhibition, and the advantages of this paper are shown by comparing with other articles.

1. Introduction

With the development of information technology, the scale of the network is becoming more and more complex, and the serious privacy leak events cause tremendous harm to cloud computing [1]. To protect privacy of network service, firewalls, intrusion detection, and antivirus software technologies have been widely used. However, invaders can only be detected after the event, which often causes serious losses.

Advanced persistent threat attackers use a variety of complex methods to steal information continuously and secretly from the cloud storage system, such as spear phishing and waterhole attack. They can even induce the cloud storage system to apply specific defense strategies and attack them, which is a great threat to cloud computing. Therefore, it is necessary to research the new privacy protection technologies [2].

An ideal protection system should protect all weak points or attacks. However, considering the limitation of organizational resources, we must consider the concept of "moderate security" to find a balance between information privacy security risk and investment and make the most reasonable decision with limited resources. Whether the strategy of protector is effective should depend not only on its own behavior, but also on the strategies of the attacker and the system. Therefore, the game theory can be used to study the information security problems such as the conflict of attack and protect and the optimal protection decision.

The basic characteristics of game theory are the opposition of objectives; both the dependence of strategies and the noncooperation of relationships are in the process of privacy protection. In the process of the game, because of the learning mechanism, low-payoff participants constantly learn the strategies of high-payoff participants and improve their behaviors [3].

Based on bounded rationality, the evolutionary game continuously improves the intrinsic driving force of behavior strategy through learning mechanism, which can effectively enhance the accuracy and reliability of the game model [3, 4]. This paper constructs an evolutionary game model of attack and protect and analyzes the rules of stability and equilibrium evolution. So, the main contributions of our paper are as follows:

(i) We propose a quantitative weight model of privacy information, construct an evolutionary game model of attack-protect, make an evolutionary stable strategy solution method, achieve the optimal privacy strategy selection, and analyze the different evolutionary stable equilibrium

(ii) To express the strategic dependence, we propose improving the accuracy of the replication dynamic equation by incentive coefficients, construct an improved evolutionary game model of cloud computing privacy protection, and give the detailed process of equilibrium solution

(iii) We use the Jacobian matrix method to analyze the stability of the game equilibrium point and the evolutionary trend of the game and obtain the optimal protect strategy

The structure of this paper is as follows. In Section 2, the related research work is introduced. In Section 3, this paper constructs an evolutionary game model of attack and protect and analyzes the different evolutionary equilibrium. In Section 4, this paper proposes an improved evolutionary game model by incentive coefficients and analyzes the stability of the evolutionary game. In Section 5, this paper designs relevant experiments. In Section 6, this paper summarizes the work and future research directions. To understand this article, a framework is given in Figure 1.

2. Related Work

The main security privacy strategy technologies for cloud system can be classified into three categories: attack defense game, evolution game, and strategy selection.

2.1. Attack Defense Game Approach. Neupane et al. [5] proposed a new defense system based on the camouflage theory, which can prevent the attackers from the analysis of attack characteristics and can reduce the impact of the target attack on the high-value services hosted in the cloud platform by "isolating virtual machine" and strategy coordination. Xiao et al. [6, 7] described the interaction between defenders and attackers in the cloud storage system, studied a mixed strategy in storage defense game, and proved that the view of the attackers can improve the effectiveness of defenders. Li et al. [8] proposed an attack-defend game model, which was a two-person zero-sum static game with complete information. When the price parameter exceeded the threshold, the defender will switch to the protection mode. Lv et al. [9] proposed a dynamic defense model based on the mixed strategy game, which optimized the allocation of the limited security resources of the target network, and allocated the dynamic optimal defense strategy for each node at different times. Based on the game between the data owner and data requester, Sfar et al. [10] proposed a solution to protect privacy in the context, which used incentives for privacy concessions or active attacks to describe game elements and found a balance between privacy concessions and incentives. Min et al. [11] derived the Nash equilibrium of symmetric and asymmetric allocation game between the attacker and the defender, initialized the quality value by using the experience in similar scenarios, and obtained the optimal defense performance. Hota and Sundaram [12] studied the influence of node's behavior probability weight and the distribution of security risk and described the graph topology of the average attack probability under the Nash equilibrium in the weakest game.

Stackelberg games are very useful for decision making in attack and defense scenario. Xiao et al. [6] deduced the Nash equilibrium of detection game and proposed a detection scheme based on strategy hill-climbing, which increased the uncertainty of strategy to deceive attacker in dynamic game. So Jakóbik et al. [13] defined a Stackelberg game model, which allowed the automatic selection of provider level security decisions and maximized the benefits of defenders. Wahab et al. [14] proposed a repeated Bayesian Stackelberg game, which provided the optimal distribution of detection for virtual machines, increased the detection ability of attack, and greatly reduced the number of attacks.

2.2. Evolutionary Game Approach. Khalifa et al. [15] proposed a new tool to simulate the evolution of several populations, defined three different stable levels, strong, weak, and medium, which improved the accuracy and adaptability of the evolutionary game. Jiang et al. [16] studied the information reliability of a series of cooperative networks and proposed an evolutionary game model based on closed expression and reinforcement assistant method. Tan et al. [17] studied the strategy selection problem of evolutionary game dynamics with group interaction and obtained the cooperative conditions of public goods game and volunteer dilemma game. Based on the bounded rationality of the players, Hu et al. [18] established a game model of attack and defense under incomplete information, which extended the game strategy in the game structure. Du et al. [19] used the evolutionary game theory framework of community to analyze the privacy protection behavior of the social network and designed incentives based on cost performance. Based on the analytic hierarchy process, Zhang et al. [20] comprehensively analyzed the impact of mobile target defense technology, proposed an effective strategy selection algorithm based on joint defense, and selected many variation elements to defend different attack.

2.3. Game Strategy Selection Approach. Various game methods have been developed to study the privacy strategy selection between proctors and adversaries. Kamhoua et al. [21] studied the security of cloud computing participants and internal interdependence, analyzed many possible Nash equilibria, and described the adversary's motivation more accurately. In order to study heterogeneous network system and provide the optimal security detection strategy, Wu et al. [22] gave the analysis of Bayesian equilibrium and robust Nash equilibrium with incomplete information and proposed a verification and calculation method for continuous kernels.

Tan et al. [17] studied the strategy selection problem of evolutionary game dynamics with group interaction and obtained the cooperative conditions of public goods game

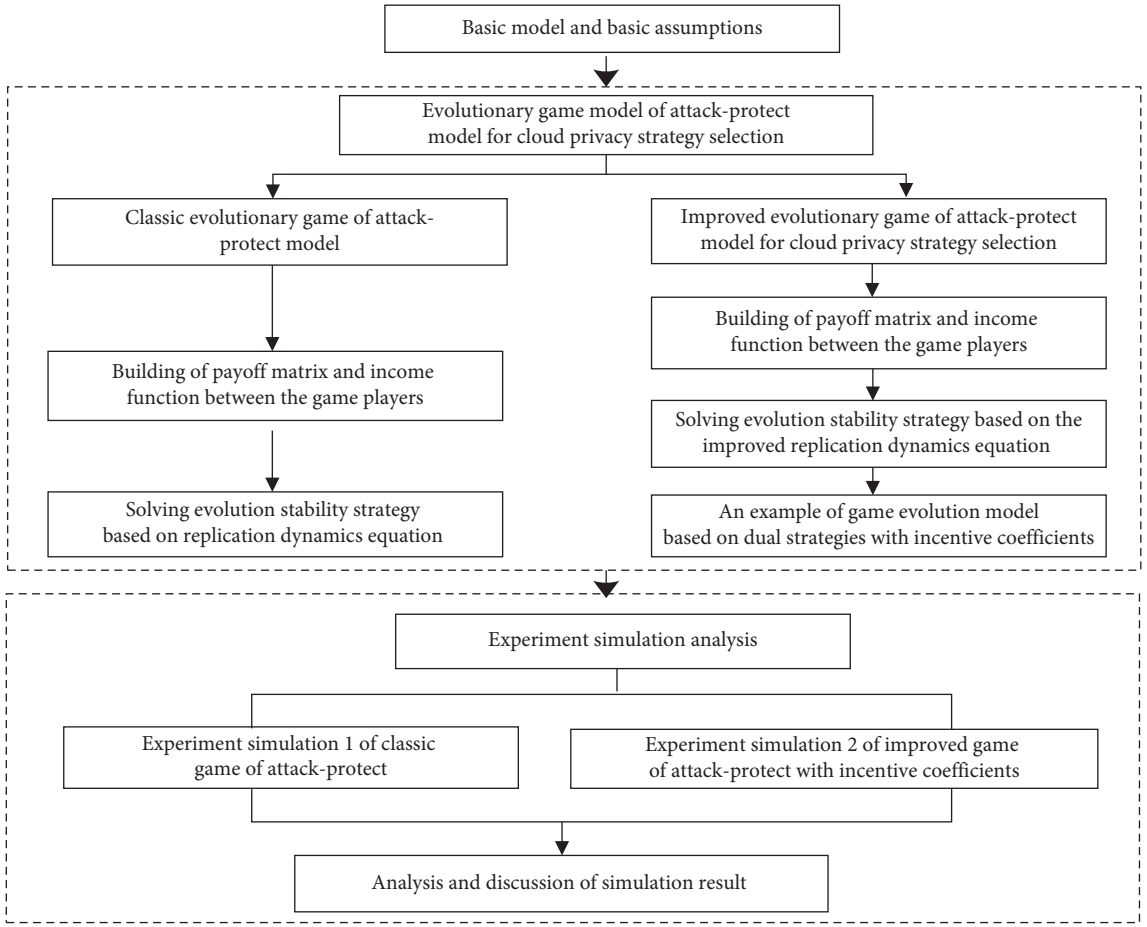

Figure 1: The architecture of the evaluation game model and simulation experiments.

and volunteer dilemma game. Cheng et al. [23] established a mobile target defense game model based on incomplete information and designed an optimal strategy algorithm to prevent the selection strategy from deviating from the actual network conditions.

After synthetically analyzing the influence of defense cost and benefit on strategy selection, Cheng et al. [24] designed an optimal strategy selection algorithm, which corrected the deviation between the selected strategy and the actual network conditions, thus ensuring the correctness of the optimal strategy selection. Zhang et al. [25] emphasized the applicability and advantages of multiobjective in network security, proposed a multiobjective game model, and introduced and demonstrated the set strategy selection technology. Armstrong et al. [26] proposed a threat specific risk assessment method, which allowed administrators to make fine-grained decisions for the selection of mitigation strategies.

2.4. Discussion and Features of Our Research. In the attack defense game approach, the existing research is mainly to explore deterministic strategies, so we need to study the application of stochastic strategies in practice. In the evolutionary game behavior, the current research is mainly to calculate the equilibrium through the income matrix and focuses on the optimization of the calculation process, rarely summarizing the dynamic process of strategic evolution. In terms of application scenarios, both the behavior analysis of cloud computing networks and the dynamic research of privacy security are based on strategy selection, which makes the research on strategy selection more universal. The game is a continuous process, different strategies in the same group have a great impact on the game results, but there are few researches in these above articles.

Our research is more general in network security protection, because the strategy set of our model can be extended to N, and both attackers and defenders can choose any strategy, which can be applied to general protection strategy choice. On the basis of bounded rationality, we consider and quantitatively describe the influence of similar strategies, introduce the influence factors, establish the evolutionary game model of attack and protect based on the improved dynamic replication equation, provide the detailed stability analysis, and improve the accuracy of the model.

3. A Game Model of Attack-Protect

In this section, we propose a quantitative weight model of privacy information, construct a game model of privacy protection, and analyze the evolution of the strategy selection mechanism to realize the optimal protect strategy. To read this article, some parameters are given in Table 1.

Table 1: Parameters and meanings.

Parameters	Meanings
$PI(s) = \{PI_1, PI_2, \ldots, PI_n\}$	Privacy information set
(G, S, T, U)	Evolutionary game model
GP and GA	Protector and adversary
$\{PS_1, PS_2, \ldots, PS_n\}$	Strategy set for protector
$\{AS_1, AS_2, \ldots, AS_m\}$	Strategy set for adversary
$T = (p, q)$	Game beliefs
q_i	Probability of strategy PS_i
p_i	Probability of strategy AS_i
a_{ij}	Payoff of adversary adopt AS_i
b_{ij}	Payoff of protector adopt PS_i
UP	Expected payoff of protector
UA	Expected payoff of adversary
$\overline{UP}$	Average payoff of protector
$\overline{UA}$	An attack-protect payoff of adversary
$x_i(t)$	Number of players choosing PS_i
$\alpha_i(\alpha_i > 0)$	Protect strategy influence factor
$y_i(t)$	Number of players choosing AS_i
$\beta_i(\beta_i > 0)$	Attack strategy influence factor
θ_{ij}	Protect strategy incentive coefficient
Δ_{ij}	Attack strategy incentive coefficient

3.1. Privacy Metric Space. To make the expression of privacy information, this paper proposes a measurement model and proposes the distance between any elements in the metric space.

Definition 1. Suppose that $\mathfrak{R}$ is a nonempty set metric space; for two elements x, y in the $\mathfrak{R}$, $\Phi(x, y)$ represents the distance between two elements, which has two characters:

(1) $\Phi(x, y) \geq 0$, $\Phi(x, y) = 0$, and $x = y$

(2) If $z \in \mathfrak{R}$, $\Phi(x, y) < \Phi(x, z) + \Phi(y, z)$

$\Phi(x, y)$ is the distance between two points x, y. $(\mathfrak{R}, \Phi)$ is called as metric space according to the distance.

According to the definition of metric space, the following properties can be obtained:

$$\Phi(x, y) = \Phi(y, x), \quad x, y, z \in \mathfrak{R}, |\Phi(x, z) - \Phi(y, z)| < \Phi(x, y). \tag{1}$$

Norm is a basic concept in performance analysis, which is often used to measure the length or size of each element in the metric space.

Let $n(n_1, n_2, \ldots, n_k)$ be a vector, and $H = (h_{i,j})_{m \times n}$ is a matrix.

Vector 1-norm is

$$\|n\|_1 = \sum_{i=1}^{k} |n_i|. \tag{2}$$

Vector 2-norm is

$$\|n\|_2 = \left(\sum_{i=1}^{k} n_i^2 \right)^{(1/2)}. \tag{3}$$

Matrix F-norm is

$$\|H\|_F = \left(\sum_{i=1}^{m} \sum_{j=1}^{n} h_{i,j}^2 \right)^{(1/2)}. \tag{4}$$

In this paper, the privacy vector is considered as an index in the measurement space, 2-norm is used to represent the size of the privacy value.

Assuming that a piece of privacy information is $PI_i = (g_1, g_2, \ldots, g_i, \ldots, g_n)$, w_i represents the privacy factor related to the user's privacy; then the privacy value $|PI_i|$ of PI_i can be expressed as

$$\begin{aligned} |PI_i| &= \sqrt[2]{(w_1 g_1)^2 + (w_2 g_2)^2 + \cdots + (w_n g_n)^2} \\ &= \sqrt[2]{\sum_{i=1}^{n} (w_i \times g_i)^2}, \quad i = 1, 2, \ldots, n. \end{aligned} \tag{5}$$

w_i is the weight coefficient of the influence factor g_i.

The correlation coefficient is an objective weight method to eliminate the influence of duplicate information on the comprehensive evaluation results. Calculate the correlation coefficient matrix; the original data contains n factors. Then the correlation coefficient matrix is

$$E = \begin{bmatrix} e_{11} & e_{12} & \cdots & e_{1n} \\ e_{21} & e_{22} & \cdots & e_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ e_{n1} & e_{n2} & \cdots & e_{nn} \end{bmatrix}. \tag{6}$$

After standardization, it can be simplified as

$$E = \left(e_{ij}\right)_{nn}. \tag{7}$$

Calculate the sum value of $(1 - r_{ij})$ in the jth column as follows:

$$\sum(1 - e_{i1}), \sum(1 - e_{i2}), \ldots, \sum\left(1 - e_{ij}\right). \tag{8}$$

The result of $\sum(1 - e_{ij})$ row vector is larger, the influence in the comprehensive evaluation system is greater, and the weight is more. Both privacy variability and conflict factor need to be considered in weight. In the paper, the objective weight method is adopted, and factor variability is represented by the standard deviation to show the difference between evaluation schemes of a factor. The larger the standard deviation is, the larger the value is.

Assume that I_i is the information quantity of ith factor; the various results of indicators can be considered by selecting the standard deviation σ_i. The conflict characteristics between the ith standard and other standards are measured by $\sum(1 - e_{ij})$. e_{ij} represents the correlation coefficient between the ith and the jth factors, and I_i can be expressed as follows:

$$I_i = \sigma_i \sum_{i=1}^{n} \left(1 - e_{ij}\right). \tag{9}$$

The result of I_i is larger, the amount of data in the ith criterion is larger, and the importance is more. Therefore, the weight w_i of the ith factor is as follows:

$$w_i = \frac{I_i}{\sum_{i=1'}^{n} I_i}. \tag{10}$$

3.2. Attack-Protect Evolutionary Game Model. In order to protect privacy information $PI(s) = \{PI_1, PI_2, \ldots, PI_n\}$, we propose an attack-protect game model (Figure 2).

Definition 2. An attack-protect evolutionary game model can be defined as a 4-tuple $APEGM = (G, S, T, U)$.

$G = (GP, GA)$ is the participant space of evolutionary game, GP is the protector, and GA is the adversary.

$S = (PS, AS)$ is game action strategy space, $PS = \{PS_1, PS_2, \ldots, PS_n\}$ represents an optional strategy set for the protector, and $AS = \{AS_1, AS_2, \ldots, AS_m\}$ represents an optional strategy set for the adversary. Both adversary and protector have multiple strategies.

$T = (p_i, q_i)$ is a set of game beliefs, q_i represents the probability set that the protector chooses a strategy PS_i, and p_i represents the probability set that the adversaries choose a strategy AS_i.

$U = (UP, UA)$ is a set of game payoff functions, UP represents the game payoffs of protectors, and UA expresses the game payoffs of adversaries.

In the game, both protector and adversary have $PS = \{PS_1, PS_2, \ldots, PS_n\}$ and $AS = \{AS_1, AS_2, \ldots, AS_m\}$, respectively, $m, n \in N$, $m, n \geq 2$. When different strategies are used in the attack-protect game, both a_{ij} and b_{ij} represent the payoffs of adversary and protector when they adopt AS_i and PS_i. We can get the following formula:

$$\begin{bmatrix} a_{11}, b_{11} & a_{12}, b_{12} & \cdots & a_{1n}, b_{1n} \\ a_{21}, b_{21} & a_{22}, b_{22} & \cdots & a_{2n}, b_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1}, b_{m1} & a_{m2}, b_{m1} & \cdots & a_{mn}, b_{mn} \end{bmatrix}. \tag{11}$$

In the $PS = \{PS_1, PS_2, \ldots, PS_n\}$, the player chooses PS_i with q_i, and $q_1 + q_2 + \cdots + q_n = 1$. Similarly, in the $AS = \{AS_1, AS_2, \ldots, AS_m\}$, adversary selects AS_i with p_i, $p_1 + p_2 + \cdots + p_m = 1$. Further, we can get the expected payoff UPS_i and average payoff $\overline{UP}$ of different protection strategies:

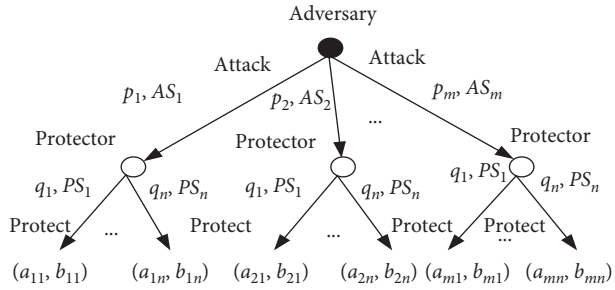

Figure 2: Basic game tree of adversary-protector.

$$\begin{cases} UPS_1 = p_1 b_{11} + p_2 b_{21} + \cdots + p_m b_{m1}, \\ UPS_2 = p_1 b_{12} + p_2 b_{22} + \cdots + p_m b_{m2}, \\ \vdots \\ UPS_n = p_1 b_{1n} + p_2 b_{2n} + \cdots + p_m b_{mn}, \end{cases} \tag{12}$$

$$\overline{UP} = q_1 UPS_1 + q_2 UPS_2 + \cdots + q_n UPS_n. \tag{13}$$

In strategy set $PS = \{PS_1, PS_2, \ldots, PS_n\}$, because of the learning mechanism, we use $q_i(t)$ to show the proportion of people who choose a strategy PS_i with time, and $\sum_{i=1}^{n} q_i(t) = 1$.

$q_i(t)$ is a time constant, for the first derivation, and the dynamic replication rate can be expressed as the following formula:

$$UP(q) = \frac{\mathrm{d}q_i(t)}{\mathrm{d}t} = q\left(UPS_i - \overline{UP}\right). \tag{14}$$

Similarly, the expected payoff UAS_i and average payoff $\overline{UA}$ of different protect strategy are calculated:

$$\begin{cases} UAS_1 = q_1 a_{11} + q_2 a_{21} + \cdots + q_n a_{n1}, \\ UAS_2 = q_1 a_{12} + q_2 a_{22} + \cdots + q_n a_{n2}, \\ \vdots \\ UAS_m = q_1 a_{1m} + q_2 a_{2m} + \cdots + q_n a_{nm}, \end{cases} \tag{15}$$

$$\overline{UA} = p_1 UAS_1 + p_2 UAS_2 + \cdots + p_n UAS_m. \tag{16}$$

In the strategy set $\{AS_1, AS_2, \ldots, AS_m\}$, $p_i(t)$ is the proportion of people who choose the attack strategy AS_i, and $\sum_{i=1}^{m} p_i(t) = 1$.

For a strategy AS_i, $p_i(t)$ is a time constant, according to the expected payoff UAS_i and average payoff $\overline{UA}$, and we can get the dynamic replication equation of attack strategy:

$$UA(p) = \frac{\mathrm{d}p_i(t)}{\mathrm{d}t} = p\left(UAS_i - \overline{UA}\right). \tag{17}$$

By combining formulas (14) and (17), we can get the following formula:

$$\begin{cases} UP(q) = \dfrac{\mathrm{d}q_i(t)}{\mathrm{d}t} = q\left(UPS_i - \overline{UP}\right), \\ UA(p) = \dfrac{\mathrm{d}p_i(t)}{\mathrm{d}t} = p\left(UAS_i - \overline{UA}\right). \end{cases} \tag{18}$$

When $\begin{cases} UP(q) = 0 \\ UA(p) = 0 \end{cases}$, we can get the equilibrium point of evolutionary game and thus realize the analysis and prediction of strategy selection.

According to the basic theory of game theory, pure strategy can be regarded as the mixed strategy with the choice probability 1 and the choice probability 0 of other strategies. Because the attack and protect game of cloud network system is a limited game, there must be a mixed strategy (p_i^*, q_j^*) to form the Nash equilibrium, and (p_i^*, q_j^*) meets the following conditions:

$$\begin{cases} \forall p_i, \quad \sum_{i=1}^{m}\sum_{j=1}^{n} p_i^* q_j^* a_{ij} \geq \sum_{i=1}^{m}\sum_{j=1}^{n} p_i q_j^* a_{ij}, \\ \forall q_j, \quad \sum_{i=1}^{m}\sum_{j=1}^{n} p_i^* q_j^* b_{ij} \geq \sum_{i=1}^{m}\sum_{j=1}^{n} p_i^* q_j b_{ij}, \\ \sum_{i=1}^{m} p_i = 1, \quad p_i \geq 0, \\ \sum_{j=1}^{n} q_i = 1, \quad q_j \geq 0. \end{cases} \tag{19}$$

3.3. Protect Strategy Selection Algorithm. Both adversary and protector choose different strategy with different probabilities. We design an optimal privacy strategy selection algorithm (Algorithm 1).

From the analysis of Section 3, the time complexity of the algorithm is $O(m+n)^2$, and the storage space complexity is $O(mn)$. According to this algorithm, not only the payoff value of each strategy can be obtained, but also the state change rate of strategy selection can be obtained.

4. Improvement of the Game Model

The evolutionary game originates from the idea of biological evolution, and replication dynamic application is the most widely used in many ways. However, in the actual process of network attack and protection, not only the strategy groups of the attacker and the protector are dependent on each other, but also the protect strategy and the attack strategy are dependent on each other. Therefore, it is necessary to study the interaction among the same strategy group. In this section, we introduce the relation function to express the strategy dependence to improve the traditional replication dynamic equation and the accuracy of the replication dynamic rate.

4.1. Improvement of the Replication Dynamic Model. Based on Section 3, in the strategy $PS = \{PS_1, PS_2, \ldots, PS_n\}$, assume that the number of strategy PS_i is $x_i(t)$ at t; the proportion of the number of protect strategy is $q_i(t)$, and we can get the following formula:

$$q_i(t) = \frac{x_i(t)}{\sum_{i=1}^{n} x_i(t)}. \tag{20}$$

With the advance of the game process, the number $x_i(t)$ of players selecting strategy PS_i changes with time, and the replication dynamic rate is proportional to the number of selection strategy PS_i, which is related to the adaptability of strategy PS_i. The expected payoff of protect strategy PS_i is UPS_i, and the average payoff of protect strategy is $\overline{UP}$. We can construct the following formula:

$$x_i'(t) = a_i x_i(t) UPS_i, \tag{21}$$

$\alpha_i\,(\alpha_i > 0)$ is the influence factor, which indicates the impact of protect strategy PS_i. The greater the value of α_i, the stronger the influence of PS_i on the other protect strategy. Based on formula (21), we can obtain formula (22) of PS_i:

$$\begin{aligned} q_i'(t) &= \frac{x_i'(t)\sum_{i=1}^{n} x_i(t) - x_i(t)\sum_{i=1}^{n} x_i'(t)}{\left[\sum_{i=1}^{n} x_i(t)\right]^2} \\ &= a_i q_i(t)\left[UPS_i(t) - \overline{UP}(t) + \sum_{j=1}^{n}\left(1 - \frac{a_j}{a_i}\right) x_j(t) UPS_j(t)\right]. \end{aligned} \tag{22}$$

Similarly, assume that the number of AS_i is $y_i(t)$ at time t. The proportion of the number of adversary is $p_i(t)$, the expected payoff is UAS_i, and the average payoff is $\overline{UA}$. We can get the following formula to express the $p_i(t)$:

$$p_i(t) = \frac{y_i(t)}{\sum_{i=1}^{m} y_i(t)}. \tag{23}$$

With the advance of the attack-protect game, the number of adversary who chooses the strategy AS_i changes with time, and the dynamic replication rate is proportional to the number of players, so we can get the following formula:

$$y_i'(t) = \beta_i y_i(t) UAS_i. \tag{24}$$

$\beta_i\,(\beta_i > 0)$ is the strategy influence factor, which is determined by the strategy AS_i. The larger the value of β_i, the stronger the influence of AS_i on other attack strategies.

Furthermore, we can get the replication dynamics of AS_i:

Input: cloud computing attack-protect game tree.
Output: optimal privacy protect strategy.
(1) Initialization $APEGM = (G, S, T, U)$
(2) Constructing protector's space set $UP = \{PS_i, i \geq 1\}$
(3) Constructing an optional strategy space set for protectors $PS = \{PS_1, PS_2, \ldots, PS_n\}$
(4) According to the strategy selection of the adversary, a reasonable protect strategy PS_i is selected by probability $q_i\,(1 \leq i \leq m)$, and $\sum_{i=1}^{m} q_i(t) = 1$
(5) For attack –protect strategy $\{AS_i, PS_j\}$, we get the payoff value b_{ij} of protect strategy.
(6) Calculating $UPS_i = p_1 b_{1i} + p_2 b_{2i} + \cdots + p_n b_{ni}$ of the protect strategy.
(7) Calculating the average payoffs of the protector $\overline{UP} = \sum_{i=1}^{n} q_i UPS_i$.
(8) Establishing protector's dynamic replication equation $UP(q) = (\mathrm{d}q_i(t)/\mathrm{d}t) = q(UPS_i - \overline{UP})$.
(9) Computing equilibrium solution of $UP(q) = 0$.
(10) Output privacy protect strategy.

Algorithm 1: Optimal privacy strategy selection.

$$\begin{aligned} p_i'(t) &= \frac{y_i'(t)\sum_{i=1}^{m} y_i(t) - y_i(t)\sum_{i=1}^{m} y_i'(t)}{\left[\sum_{i=1}^{m} y_i(t)\right]^2} \\ &= \beta_i p_i(t)\left[UAS_i(t) - \overline{UA}(t) + \sum_{j=1}^{n}\left(1 - \frac{\beta_j}{\beta_i}\right) y_j(t) UAS_j(t)\right]. \end{aligned} \tag{25}$$

By combining formulas (22) and (25), we obtain an improved replicated dynamic differential equation:

$$\begin{cases} q_i'(t) = \alpha_i q_i(t)\left[UPS_i(t) - \overline{UP}(t) + \sum_{j=1}^{n}\left(1 - \frac{\alpha_j}{\alpha_i}\right) x_j(t) UPS_j(t)\right], \\ p_i'(t) == \beta_i p_i(t)\left[UAS_i(t) - \overline{UA}(t) + \sum_{j=1}^{n}\left(1 - \frac{\beta_j}{\beta_i}\right) y_j(t) UAS_j(t)\right]. \end{cases} \tag{26}$$

When $a_i = a_j = 1$ and $\beta_i = \beta_j = 1$, we can obtain the following dynamic replication equations:

$$\begin{cases} q_i'(t) = q_i(t)\left[UPS_i(t) - \overline{UP}(t)\right], \\ p_i'(t) = p_i(t)\left[UAS_i(t) - \overline{UA}(t)\right]. \end{cases} \tag{27}$$

We define an incentive coefficient $\theta_{ij} = (a_i/a_j)$ to represent incentive relationship between PS_i and PS_j, $\theta_{ij} < 1$ indicates that protect strategy PS_i can promote PS_j, and $\theta_{ij} > 1$ indicates that protect strategy PS_i can suppress PS_i.

Similarly, we define an incentive coefficient $\Delta_{ij} = (\beta_i/\beta_j)$ to represent incentive relationship between AS_i and AS_i. Through further deduction, we can get the following formula:

$$\begin{cases} q_i'(t) = \alpha_i q_i(t)\left[UPS_i(t) - \overline{UP}(t) + \sum_{j=1}^{n}\left(1 - \theta_{ji}\right) x_j(t) UPS_j(t)\right], \\ p_i'(t) == \beta_i p_i(t)\left[UAS_j(t) - \overline{UA}(t) + \sum_{j=1}^{n}\left(1 - \Delta_{ji}\right) y_j(t) UAS_j(t)\right]. \end{cases} \tag{28}$$

When $\begin{cases} q_i'(t) = 0 \\ p_i'(t) = 0 \end{cases}$, we can get the equilibrium solution of attack-protect evolutionary game to realize the analysis and prediction of strategy selection.

4.2. Evolutionary Game Description. Assume that the protector has an optional strategy set $\{PS_1, PS_2\}$, where PS_1 represents investment privacy protection and PS_2 represents noninvestment privacy protection. Similarly,

an adversary has an optional strategy set $\{AS_1, AS_2\}$, where AS_1 represents that the adversary implements attack and AS_2 represents the idea that the adversary does not implement an attack. p_1 denotes the selection probability of attack strategy AS_1, p_2 denotes the selection probability of attack strategy AS_2, and $p_1 + p_2 = 1$; q_1 denotes the selection probability of strategy AS_1 and q_2 denotes the selection probability of strategy AS_2, and $q_1 + q_2 = 1$.

4.3. Evolutionary Game Solution of Attack-Protect. Based on the attack-protect model of Section 3, similarly, we can construct the following formula:

$$\begin{cases} UPS_1(t) = q_1(t)b_{11} + q_2(t)b_{21}, \\ UPS_2(t) = q_1(t)b_{12} + q_2(t)b_{22}, \\ \overline{UP}(t) = q_1(t)UPS_1(t) + q_2(t)UPS_2(t), \\ UAS_1(t) = p_1(t)b_{11} + p_2(t)b_{21}, \\ UAS_2(t) = p_1(t)b_{12} + p_2(t)b_{22}, \\ \overline{UA}(t) = q_1(t)UAS_1(t) + q_2(t)UAS_2(t). \end{cases} \tag{29}$$

According to $q_1(t) + q_2(t) = 1$, $p_1(t) + p_2(t) = 1$, by first derivative of time t, we can get the following formula:

$$\begin{aligned} q_1'(t) &= -q_2'(t), \\ p_1'(t) &= -p_2'(t). \end{aligned} \tag{30}$$

According to formulas (28) and (30), we can further obtain the dynamic replication equation of PS_1 and AS_2:

$$\begin{cases} \dfrac{dq_1(t)}{dt} = a_1 q_1(1 - q_1)[b_{21} - \theta_{21}b_{22} + (b_{11} - b_{21} - \theta_{21}b_{21} \\ \quad +\theta_{21}b_{22})p_1], \\ \dfrac{dp_1(t)}{dt} = \beta_1 p_1(1 - p_1)[a_{12} - \Delta_{21}a_{22} + (a_{11} - a_{12} \\ \quad -\Delta_{21}a_{21} + \Delta_{21}a_{22})q_1]. \end{cases} \tag{31}$$

When $\begin{cases} q_1'(t) = 0 \\ p_1'(t) = 0 \end{cases}$, we can get five solutions: $\begin{cases} q_1 = 0 \\ p_1 = 0 \end{cases}$, $\begin{cases} q_1 = 0 \\ p_1 = 1 \end{cases}$, $\begin{cases} q_1 = 1 \\ p_1 = 0 \end{cases}$, $\begin{cases} q_1 = 1 \\ p_1 = 1 \end{cases}$, and $\begin{cases} q^* = (-b_{21} + \theta_{21}b_{22})/(b_{11} - b_{21} - \theta_{21}b_{12} + \theta_{21}b_{22}) \\ p^* = (-a_{12} + \Delta_{21}a_{22})/(a_{11} - a_{12} - \theta_{21}a_{21} + \Delta_{21}a_{22}) \end{cases}$.

4.4. Dynamic Analysis of Attack-Protect Evolution. According to the above improved evolutionary game model, we use the Jacobian matrix method to analyze the evolutionary stability of these above five equilibrium points, and get formula (32). Both determinant det and trace tr of the Jacobian matrix can be expressed as in formulas (33) and (34):

$$J = \begin{bmatrix} a_1(1 - 2q_1)[b_{21} - \theta_{21}b_{22} + (b_{11} - b_{21} - \theta_{21}b_{21} + \theta_{21}b_{22})p_1] & a_1 q_1(1 - q_1)(b_{11} - b_{21} - \theta_{21}a_{12} + \theta_{21}b_{22}) \\ \beta_1 p_1(1 - p_1)(a_{11} - a_{12} - \Delta_{21}a_{21} + \Delta_{21}a_{22}) & \beta_1(1 - 2p_1)[a_{12} - \gamma_{21}a_{22} + (a_{11} - a_{12} - \Delta_{21}a_{21} + \Delta_{21}a_{22})q_1] \end{bmatrix}, \tag{32}$$

$$\begin{aligned} \det J = {} & a_1(1 - 2q_1)[b_{21} - \theta_{21}b_{22} + (b_{11} - b_{21} - \theta_{21}b_{12} + \theta_{21}b_{22})p_1]\beta_1(1 - 2p_1)[a_{12} - \Delta_{21}a_{22} + (a_{11} - a_{12} - \Delta_{21}a_{21} + \Delta_{21}a_{22})q_1] \\ & - a_1 q_1(1 - q_1)(b_{11} - b_{21} - \theta_{21}b_{12} + \theta_{21}b_{22})\beta_1 p_1(1 - p_1)(a_{11} - a_{12} - \Delta_{21}a_{21} + \Delta_{21}a_{22}), \end{aligned} \tag{33}$$

$$\mathrm{tr}J = a_1(1 - 2q_1)[b_{21} - \theta_{21}b_{22} + (b_{11} - b_{21} - \theta_{21}b_{22} + \theta_{21}b_{22})p_1] + \beta_1(1 - 2p_1)[a_{12} - \Delta_{21}a_{22} + (a_{11} - a_{12} - \Delta_{21}a_{11} + \Delta_{21}a_{22})q_1]. \tag{34}$$

When $\det J > 0$ and $\mathrm{tr}J > 0$, the equilibrium point is unstable; when $\det J < 0$ and $\mathrm{tr}J$ is an arbitrary value, the equilibrium point is a saddle point.

Condition 1. $b_{11} - b_{21} - \theta_{21}b_{21} + \theta_{21}b_{22} = 0, a_{11} - a_{12} - \Delta_{21}a_{21} + \Delta_{21}a_{22} \neq 0$; the game system has four equilibrium points: $O(0,0)$, $A(1,0)$, $B(1,1)$, $C(0,1)$. By the four points of formulas (32) and (33), we get the expressions of Table 2, and discuss several cases by determinant and trace of the Jacobian matrix:

Case 1: when $b_{11} - \theta_{21}b_{12} < 0$, $a_{11} - \Delta_{21}a_{21} < 0$, $O(0,0)$ is a stable point, both $C(0,1)$ and $A(1,0)$ are saddle points, $B(1,1)$ is an unstable point, and (no protect, no attack) is the stable strategy

Case 2: when $b_{11} - \theta_{21}b_{12} < 0$, $a_{11} - \Delta_{21}a_{21} > 0$, $C(0,1)$ is a stable point, both $O(0,0)$ and $B(1,1)$ are saddle points, $A(1,0)$ is an unstable point, and (no protect, no attack) is the stable strategy

Case 3: when $b_{11} - \theta_{21}b_{12} > 0$, $a_{11} - \Delta_{21}a_{21} < 0$, $A(1,0)$ is a stable point, both $O(0,0)$ and $B(1,1)$ are saddle

Table 2: Determinant and trace of the equilibrium point in the game system.

Equilibrium	Det	Tr
$O(0,0)$	$\det J = \alpha_1\beta_1(b_{21}-\theta_{21}b_{22})(a_{12}-\Delta_{21}a_{22})$	$\mathrm{tr}J = a_1(b_{21}-\theta_{21}b_{22})+\beta_1(a_{12}-\Delta_{21}a_{22})$
$A(1,0)$	$\det J = -\alpha_1\beta_1(b_{21}-\theta_{21}b_{22})(a_{11}-\Delta_{21}a_{21})$	$\mathrm{tr}J = -a_1(b_{21}-\theta_{21}b_{22})+\beta_1(a_{11}-\Delta_{21}a_{21})$
$B(1,1)$	$\det J = \alpha_1\beta_1(b_{21}-\theta_{21}b_{12})(a_{11}-\Delta_{21}a_{21})$	$\mathrm{tr}J = -a_1(b_{11}-\theta_{21}b_{12})-\beta_1(a_{11}-\Delta_{21}a_{22})$
$C(0,1)$	$\det J = \alpha_1\beta_1(b_{21}-\theta_{21}b_{12})(a_{12}-\Delta_{21}a_{22})$	$\mathrm{tr}J = a_1(b_{11}-\theta_{21}b_{12})-\beta_1(a_{12}-\Delta_{21}a_{22})$

points, $C(0,1)$ is an unstable point, at this time, and (protect, no attack) is the stable strategy

Case 4: when $b_{11}-\theta_{21}b_{12}>0, a_{11}-\Delta_{21}a_{21}>0, B(1,1)$ is a stable point, both $C(0,1)$ and $A(1,0)$ are saddle points, $O(0,0)$ is an unstable point, (protect, attack) is the stable strategy, and privacy protect is the optimal selection of protector

Condition 2. When $b_{11}-b_{21}-\theta_{21}b_{21}+\theta_{21}b_{22}=0, a_{11}-a_{12}-\Delta_{21}a_{21}+\Delta_{21}a_{22}\neq 0$, there are four equilibrium points: $O(0,0)$, $A(1,0)$, $B(1,1)$, and $C(0,1)$; there are eight cases as follows:

Case 1: $b_{11}-\theta_{21}b_{12}<0$, $a_{11}-\Delta_{21}a_{21}<0$, $a_{12}-\Delta_{21}a_{22}<0$, $O(0,0)$ is a stable point, both $C(0,1)$ and $A(1,0)$ are saddle points, and $B(1,1)$ is an unstable point

Case 2: $b_{11}-\theta_{21}b_{12}<0$, $a_{11}-\Delta_{21}a_{21}<0$, $a_{12}-\Delta_{21}a_{22}>0$, $A(1,0)$ is a stable point, both $O(0,0)$ and $C(0,1)$ are saddle points, and $B(1,1)$ is an unstable point

Case 3: $b_{11}-\theta_{21}b_{12}<0$, $a_{11}-\Delta_{21}a_{21}>0$, $a_{12}-\Delta_{21}a_{22}<0$, $C(0,1)$ is a stable point, and $O(0,0)$,$A(1,0)$, and $B(1,1)$ are saddle points

Case 4: $b_{11}-\theta_{21}b_{12}<0$, $a_{11}-\Delta_{21}a_{21}>0$, $a_{12}-\Delta_{21}a_{22}>0$, $O(0,0)$ is an unstable point, both $B(1,1)$ and $A(1,0)$ are saddle points, and $C(0,1)$ is a stable point

Case 5: $b_{11}-\theta_{21}b_{12}>0$, $a_{11}-\Delta_{21}a_{21}<0$, $a_{12}-\Delta_{21}a_{22}<0$, $O(0,0)$, $C(0,1)$, and $B(1,1)$ are saddle points, and $A(1,0)$ is an unstable point

Case 6: $b_{11}-\theta_{21}b_{12}>0$, $a_{11}-\Delta_{21}a_{21}<0$, $a_{12}-\Delta_{21}a_{22}>0$, $A(1,0)$ is a stable point, both $O(0,0)$ and $B(1,1)$ are saddle points, and $C(0,1)$ is an unstable point

Case 7: $b_{11}-\theta_{21}b_{12}>0$, $a_{11}-\Delta_{21}a_{21}>0$, $a_{12}-\Delta_{21}a_{22}<0$, $B(1,1)$ is a stable point, both $O(0,0)$ and $C(0,1)$ are saddle points, and $A(1,0)$ is an unstable point

Case 8: $b_{11}-\theta_{21}b_{12}>0$, $a_{11}-\Delta_{21}a_{21}<0$, $a_{12}-\Delta_{21}a_{22}>0$, $B(1,1)$ is a stable point, both $C(0,1)$ and $A(1,0)$ are saddle points, and $O(0,0)$ is an unstable point

Condition 3. When $b_{11}-b_{21}-\theta_{21}b_{21}+\theta_{21}b_{22}\neq 0, a_{11}-a_{12}-\Delta_{21}a_{21}+\Delta_{21}a_{22}=0$, there are four equilibrium points; $O(0,0)$, $A(1,0)$, $B(1,1)$, $C(0,1)$, which can be divided into the following eight cases.

Case 1: $b_{11}-\theta_{21}b_{12}<0$, $a_{11}-\Delta_{21}a_{21}<0$, $b_{21}-\theta_{21}b_{22}<0$, $O(0,0)$ is a stable point, both $C(0,1)$ and $A(1,0)$ are saddle points, and $B(1,1)$ is an unstable point

Case 2: $b_{11}-\theta_{21}b_{12}<0$, $a_{11}-\Delta_{21}a_{21}<0$, $b_{21}-\theta_{21}b_{22}>0$, $C(0,1)$ is a stable point, both $B(1,1)$ and $A(1,0)$ are saddle points, and $O(0,0)$ is an unstable point

Case 3: $b_{11}-\theta_{21}b_{12}<0$, $a_{11}-\Delta_{21}a_{21}>0$, $b_{21}-\theta_{21}b_{22}<0$, $O(0,0)$ is a stable point, and $C(0,1)$, $B(1,1)$, and $A(1,0)$ are saddle points

Case 4: $b_{11}-\theta_{21}b_{12}<0$, $a_{11}-\Delta_{21}a_{21}>0$, $b_{21}-\theta_{21}b_{22}>0$, $O(0,0)$ is a stable point, $A(1,0)$ is a saddle point, and both $A(1,0)$ and $B(1,1)$ are unstable points

Case 5: $b_{11}-\theta_{21}b_{12}>0$, $a_{11}-\Delta_{21}a_{21}<0$, $b_{21}-\theta_{21}b_{22}<0$, $A(1,0)$ is a stable point, both $O(0,0)$ and $B(1,1)$ are saddle points, $C(0,1)$ is an unstable point

Case 6: $b_{11}-\theta_{21}b_{12}>0$, $a_{11}-\Delta_{21}a_{21}<0$, $b_{21}-\theta_{21}b_{22}>0$, $O(0,0)$ is an unstable point, both $C(0,1)$ and $B(1,1)$ are saddle points, and $A(1,0)$ is a unstable point

Case 7: $b_{11}-\theta_{21}b_{12}>0$, $a_{11}-\Delta_{21}a_{21}>0$, $b_{21}-\theta_{21}b_{22}<0$, $B(1,1)$ is a stable point, both $O(0,0)$ and $A(1,0)$ are saddle points, $C(0,1)$ is an unstable point

Case 8: $b_{11}-\theta_{21}b_{12}>0$, $a_{11}-\Delta_{21}a_{21}>0$, $b_{21}-\theta_{21}b_{22}>0$, $B(1,1)$ is a stable point, both $A(1,0)$ and $C(0,1)$ are saddle points, and $O(0,0)$ is an unstable point

Condition 4. When $b_{11}-b_{21}-\theta_{21}b_{12}+\theta_{21}b_{22}\neq 0, a_{11}-a_{12}-\Delta_{21}a_{21}+\Delta_{21}a_{22}\neq 0$, there are five equilibrium points; $O(0,0)$, $A(1,0)$, $B(1,1)$, $C(0,1)$, $(q^*=(-a_{12}+\Delta_{21}a_{22})/(a_{11}-a_{12}-\Delta_{21}a_{21}+\Delta_{21}a_{22}), p^*=(-b_{21}+\theta_{21}b_{22})/(b_{11}-b_{21}-\theta_{21}b_{12}+\theta_{21}b_{22}))$.

Because the value of $D(p^*,q^*)$ cannot be determined, we give several discussion of different values of q^* and p^*:

(1) $(b_{21}-\theta_{21}b_{22})/((b_{21}-\theta_{21}b_{22})-(b_{11}-\theta_{21}b_{12}))<0$, $(a_{12}-\Delta_{21}a_{22})/((a_{12}-\Delta_{21}a_{22})-(a_{11}-\Delta_{21}a_{21}))<0$; there are four cases:

Case 1: $a_{11}-\Delta_{21}a_{21}<a_{12}-\Delta_{21}a_{22}<0, b_{11}-\theta_{21}b_{12}<b_{21}-\theta_{21}b_{22}<0$, $O(0,0)$ is a stable point, $C(0,1)$, $A(1,0)$, and $D(p^*,q^*)$ are saddle points, and $B(1,1)$ is an unstable point

Case 2: $0<a_{12}-\Delta_{21}a_{22}<a_{11}-\Delta_{21}a_{21}, 0<b_{21}-\theta_{21}b_{22}<b_{11}-\theta_{21}b_{12}$, $O(0,0)$ is an unstable point, $C(0,1)$, $A(1,0)$, and $D(p^*,q^*)$ are saddle points, and $B(1,1)$ is a stable point

Case 3: $0<a_{12}-\Delta_{21}a_{22}<a_{11}-\Delta_{21}a_{21}, b_{11}-\theta_{21}b_{12}<b_{21}-\theta_{21}b_{22}<0$, $C(0,1)$ is an unstable point, both

$P1(0,0)$ and $B(1,1)$ are saddle points, $A(1,0)$ is a stable point, and $D(p^*,q^*)$ is a center point
Case 4: $a_{11}-\Delta_{21}a_{21}<a_{12}-\Delta_{21}a_{22}<0, 0<b_{21}-\theta_{21}b_{22}<b_{11}-\theta_{21}b_{12}$, $C(0,1)$ is a stable point, both $O(0,0)$ and $B(1,1)$ are saddle points, $A(1,0)$ is an unstable point, and $D(p^*,q^*)$ is a center point

(2) $0<(b_{21}-\theta_{21}b_{22})/((b_{21}-\theta_{21}b_{22})-(b_{11}-\theta_{21}b_{12}))<1$, $(a_{12}-\Delta_{21}a_{22})/((a_{12}-\Delta_{21}a_{22})-(a_{11}-\Delta_{21}a_{21}))<0$; there are four cases:

Case 1: $0<a_{12}-\Delta_{21}a_{22}<a_{11}-\Delta_{21}a_{21}, b_{11}-\theta_{21}b_{12}<0<b_{21}-\theta_{21}b_{22}$, $O(0,0)$ is an unstable point, $C(0,1)$, $B(1,1)$, and $D(p^*,q^*)$ are saddle points, and $A(1,0)$ is a stable point
Case 2: $a_{11}-\Delta_{21}a_{21}<a_{12}-\Delta_{21}a_{22}<0, b_{21}-\theta_{21}b_{22}<0<b_{11}-\theta_{21}b_{12}$, $O(0,0)$ is a stable point, $C(0,1)$, $B(1,1)$, and $D(p^*,q^*)$ are saddle points, and $A(1,0)$ is an unstable point
Case 3: $a_{11}-\Delta_{21}a_{21}<a_{12}-\Delta_{21}a_{22}<0, b_{11}-\theta_{21}b_{12}<0<b_{21}-\theta_{21}b_{22}$, $B(1,1)$ is an unstable point, both $O(0,0)$ and $A(1,0)$ are saddle points, $C(0,1)$ is a stable point, and $D(p^*,q^*)$ is a center point
Case 4: $0<a_{12}-\Delta_{21}a_{22}<a_{11}-\Delta_{21}a_{21}, b_{21}-\theta_{21}b_{22}<0<b_{11}-\theta_{21}b_{12}$, $B(1,1)$ is a stable point, both $O(0,0)$ and $A(1,0)$ are saddle points, $C(0,1)$ is an unstable point, and $D(p^*,q^*)$ is a center point

(3) $(b_{21}-\theta_{21}b_{22})/((b_{21}-\theta_{21}b_{22})-(b_{11}-\theta_{21}b_{12}))>1$, $(a_{12}-\Delta_{21}a_{22})/((a_{12}-\Delta_{21}a_{22})-(a_{11}-\Delta_{21}a_{21}))<0$; there are four cases:

Case 1: $0<a_{12}-\Delta_{21}a_{22}<a_{11}-\Delta_{21}a_{21}, 0<b_{11}-\theta_{21}b_{12}<b_{21}-\theta_{21}b_{22}$, $O(0,0)$ is an unstable point, both $C(0,1)$ and $A(1,0)$ are saddle points, $B(1,1)$ is a stable point, and $D(p^*,q^*)$ is a center point
Case 2: $a_{11}-\Delta_{21}a_{21}<a_{12}-\Delta_{21}a_{22}<0, 0<b_{11}-\theta_{21}b_{12}<b_{21}-\theta_{21}b_{22}$, $C(0,1)$ is a stable point, $O(0,0)$, $B(1,1)$, and $D(p^*,q^*)$ are saddle points, and $A(1,0)$ is an unstable point
Case 3: $0<a_{12}-\Delta_{21}a_{22}<a_{11}-\Delta_{21}a_{21}, b_{21}-\theta_{21}b_{22}<b_{11}-\theta_{21}b_{12}<0$, $A(1,0)$ is an unstable point, $O(0,0)$, $B(1,1)$, and $D(p^*,q^*)$ are saddle points, and $C(0,1)$ is a stable point
Case 4: $0>a_{12}-\Delta_{21}a_{22}>a_{11}-\Delta_{21}a_{21}, b_{21}-\theta_{21}b_{22}<b_{11}-\theta_{21}b_{12}<0$, $O(0,0)$ is a stable point, both $C(0,1)$ and $A(1,0)$ are saddle points, $B(1,1)$ is an unstable point, and $D(p^*,q^*)$ is a center point

(4) $(b_{21}-\theta_{21}b_{22})/((b_{21}-\theta_{21}b_{22})-(b_{11}-\theta_{21}b_{12}))<0, 0<(a_{12}-\Delta_{21}a_{22})/((a_{12}-\Delta_{21}a_{22})-(a_{11}-\Delta_{21}a_{21}))<1$; there are four cases:

Case 1: $a_{11}-\Delta_{21}a_{21}<0<a_{12}-\Delta_{21}a_{22}<, 0<b_{21}-\theta_{21}b_{22}<b_{11}-\theta_{21}b_{12}$, $O(0,0)$ is an unstable point, $C(0,1)$ is a stable point, $A(1,0)$, $B(1,1)$, and $D(p^*,q^*)$ are saddle points
Case 2: $a_{12}-\Delta_{21}a_{22}<0<a_{11}-\Delta_{21}a_{21}, 0<b_{21}-\theta_{21}b_{22}<b_{11}-\theta_{21}b_{12}$, both $O(0,0)$ and $C(0,1)$ are saddle points, $A(1,0)$ is an unstable point, $B(1,1)$ is a stable point, and $D(p^*,q^*)$ is a center point
Case 3: $a_{12}-\Delta_{21}a_{22}<0<a_{11}-\Delta_{21}a_{21}, 0>b_{21}-\theta_{21}b_{22}>b_{11}-\theta_{21}b_{12}$, $C(0,1)$ is an unstable point, $D(p^*,q^*)$ and both $B(1,1)$ and $A(1,0)$ are saddle points, and $O(0,0)$ is a stable point
Case 4: $a_{11}-\Delta_{21}a_{21}<0<a_{12}-\Delta_{21}a_{22}, b_{11}-\theta_{21}b_{12}<b_{21}-\theta_{21}b_{22}<0$, $A(1,0)$ is a stable point, both $O(0,0)$ and $C(0,1)$ are saddle points, $B(1,1)$ is an unstable point, and $D(p^*,q^*)$ is a center point

(5) $0<(b_{21}-\theta_{21}b_{22})/((b_{21}-\theta_{21}b_{22})-(b_{11}-\theta_{21}b_{12}))<1, 0<(a_{12}-\Delta_{21}a_{22})/((a_{12}-\Delta_{21}a_{22})-(a_{11}-\Delta_{21}a_{21}))<1$; there are four cases:

Case 1: $a_{11}-\Delta_{21}a_{21}<0<a_{12}-\Delta_{21}a_{22}, b_{21}-\theta_{21}b_{22}<b_{11}-\theta_{21}b_{12}$, both $O(0,0)$ and $B(1,1)$ are unstable points, both $C(0,1)$ and $A(1,0)$ are stable points, and $D(p^*,q^*)$ is a saddle point
Case 2: $a_{12}-\Delta_{21}a_{22}<0<a_{11}-\Delta_{21}a_{21}, b_{11}-\theta_{21}b_{12}<b_{21}-\theta_{21}b_{22}$, both $O(0,0)$ and $B(1,1)$ are stable points, $D(p^*,q^*)$ is a saddle point, and both $C(0,1)$ and $A(1,0)$ are unstable points
Case 3: $a_{12}-\Delta_{21}a_{22}<0<a_{11}-\Delta_{21}a_{21}, b_{21}-\theta_{21}b_{22}<0<b_{11}-\theta_{21}b_{12}$, $O(0,0)$, $C(0,1)$, $A(1,0)$, and $B(1,1)$ are saddle points, and $D(p^*,q^*)$ is a center point
Case 4: $a_{11}-\Delta_{21}a_{21}<0<a_{12}-\Delta_{21}a_{22}, b_{11}-\theta_{21}b_{12}<0<b_{21}-\theta_{21}b_{22}$, $O(0,0)$, $C(0,1)$, $A(1,0)$, and $B(1,1)$ are saddle points, and $D(p^*,q^*)$ is a center point

(6) $(b_{21}-\theta_{21}b_{22})/((b_{21}-\theta_{21}b_{22})-(b_{11}-\theta_{21}b_{12}))>1, 0<(a_{12}-\Delta_{21}a_{22})/((a_{12}-\Delta_{21}a_{22})-(a_{11}-\Delta_{21}a_{21}))<1$; there are four cases:

Case 1: $a_{11}-\Delta_{21}a_{21}<0<a_{12}-\Delta_{21}a_{22}, 0<b_{11}-\theta_{21}b_{12}<b_{21}-\theta_{21}b_{22}$, $O(0,0)$ is an unstable point, both $A(1,0)$ and $B(1,1)$ are saddle points, $C(0,1)$ is a stable point, and $D(p^*,q^*)$ is a center point
Case 2: $a_{12}-\Delta_{21}a_{22}<0<a_{11}-\Delta_{21}a_{21}, b_{21}-\theta_{21}b_{22}<b_{11}-\theta_{21}b_{12}<0$, $O(0,0)$ is a stable point, both $A(1,0)$ and $B(1,1)$ are saddle points, $C(0,1)$ is an unstable point, and $D(p^*,q^*)$ is a center point

Case 3: $a_{12}-\Delta_{21}a_{22}<0<a_{11}-\Delta_{21}a_{21}, b_{21}-\theta_{21}b_{22}<b_{11}-\theta_{21}b_{12}<0$, $B(1,1)$ is a stable point, $O(0,0)$, $C(0,1)$, and $D(p^*,q^*)$ are saddle points, and $A(1,0)$ is an unstable point
Case 4: $a_{11}-\Delta_{21}a_{21}<0<a_{12}-\Delta_{21}a_{22}>, b_{21}-\theta_{21}b_{22}<b_{11}-\theta_{21}b_{12}<0$, $A(1,0)$ is a stable point, $O(0,0)$, $C(0,1)$, and $D(p^*,q^*)$ are saddle points, and $B(1,1)$ is an unstable point

(7) $(b_{21}-\theta_{21}b_{22})/((b_{21}-\theta_{21}b_{22})-(b_{11}-\theta_{21}b_{12}))<0$, $(a_{12}-\Delta_{21}a_{22})/((a_{12}-\Delta_{21}a_{22})-(a_{11}-\Delta_{21}a_{21}))>1$; there are four cases:

Case 1: $0<a_{11}-\Delta_{21}a_{21}<a_{12}-\Delta_{21}a_{22}, 0<b_{21}-\theta_{21}b_{22}<b_{11}-\theta_{21}b_{12}$, $O(0,0)$ is an unstable point, both $C(0,1)$ and $A(1,0)$ are saddle points, $B(1,1)$ is a stable point, and $D(p^*,q^*)$ is a center point
Case 2: $a_{12}-\Delta_{21}a_{22}<a_{11}-\Delta_{21}a_{21}<0, b_{11}-\theta_{21}b_{12}<b_{21}-\theta_{21}b_{22}<0$, $O(0,0)$ is a stable point,

$C(0,1)$ and $A(1,0)$ are saddle points, $B(1,1)$ is an unstable point, and $D(p^*,q^*)$ is a center point

Case 3: $a_{12}-\Delta_{21}a_{22}<a_{11}-\Delta_{21}a_{21}<0, 0<b_{21}-\theta_{21}b_{22}<b_{11}-\theta_{21}b_{12}$, $C(0,1)$ is a stable point, $O(0,0)$, $B(1,1)$, and $D(p^*,q^*)$ are saddle points, and $A(1,0)$ is an unstable point

Case 4: $a_{12}-\Delta_{21}a_{22}>a_{11}-\Delta_{21}a_{21}>0, b_{11}-\theta_{21}b_{12}<b_{21}-\theta_{21}b_{22}<0$, $C(0,1)$ is a stable point, $O(0,0)$, $B(1,1)$, and $D(p^*,q^*)$ are saddle points, and $A(1,0)$ is an unstable point

(8) $0<(b_{21}-\theta_{21}b_{22})/((b_{21}-\theta_{21}b_{22})-(b_{11}-\theta_{21}b_{12}))<1$, $(a_{12}-\Delta_{21}a_{22})/((a_{12}-\Delta_{21}a_{22})-(a_{11}-\Delta_{21}a_{21}))>1$; there are four cases:

Case 1: $0<a_{11}-\Delta_{21}a_{21}<a_{12}-\Delta_{21}a_{22}, b_{11}-\theta_{21}b_{12}<0<b_{21}-\theta_{21}b_{22}$, $O(0,0)$ is an unstable point, both $C(0,1)$ and $B(1,1)$ are saddle points, $A(1,0)$ is a stable point, and $D(p^*,q^*)$ is a center point

Case 2: $a_{11}-\Delta_{21}a_{21}<a_{12}-\Delta_{21}a_{22}<0, 0<b_{11}-\theta_{21}b_{12}<b_{21}-\theta_{21}b_{22}$, $O(0,0)$ is a stable point, both $C(0,1)$ and $B(1,1)$ are saddle points, $A(1,0)$ is an unstable point, and $D(p^*,q^*)$ is a center point

Case 3: $a_{12}-\Delta_{21}a_{22}<a_{11}-\Delta_{21}a_{21}<0, b_{11}-\theta_{21}b_{12}<0<b_{21}-\theta_{21}b_{22}$, $B(1,1)$ is an unstable point, $O(0,0)$, $A(1,0)$, and $D(p^*,q^*)$ are saddle points, and $C(0,1)$ is a stable point

Case 4: $0<a_{11}-\Delta_{21}a_{21}<a_{12}-\Delta_{21}a_{22}, b_{21}-\theta_{21}b_{22}<0<b_{11}-\theta_{21}b_{12}$, $B(1,1)$ is a stable point, $O(0,0)$, $A(1,0)$, and $D(p^*,q^*)$ are saddle points, and $C(0,1)$ is an unstable point

(9) $(b_{21}-\theta_{21}b_{22})/((b_{21}-\theta_{21}b_{22})-(b_{11}-\theta_{21}b_{12}))>1$, $(a_{12}-\Delta_{21}a_{22})/((a_{12}-\Delta_{21}a_{22})-(a_{11}-\Delta_{21}a_{21}))>1$; there are four cases:

Case 1: $0<a_{11}-\Delta_{21}a_{21}<a_{12}-\Delta_{21}a_{22}, 0<b_{11}-\theta_{21}b_{12}<b_{21}-\theta_{21}b_{22}$, $O(0,0)$ is an unstable point, $C(0,1)$, $A(1,0)$, and $D(p^*,q^*)$ are saddle points, and $B(1,1)$ is a stable point

Case 2: $a_{12}-\Delta_{21}a_{22}<a_{11}-\Delta_{21}a_{21}<0, 0>b_{11}-\theta_{21}b_{12}>b_{21}-\theta_{21}b_{22}$, $O(0,0)$ is a stable point, $C(0,1)$, $A(1,0)$, and $D(p^*,q^*)$ are saddle points, and $B(1,1)$ is an unstable point

Case 3: $a_{12}-\Delta_{21}a_{22}<a_{11}-\Delta_{21}a_{21}<0, 0<b_{21}-\theta_{21}b_{22}<b_{11}-\theta_{21}b_{12}$, $A(1,0)$ is an unstable point, both $O(0,0)$ and $B(1,1)$ are saddle points, $C(0,1)$ is a stable point, and $D(p^*,q^*)$ is a center point

Case 4: $0<a_{11}-\Delta_{21}a_{21}<a_{12}-\Delta_{21}a_{22}, b_{21}-\theta_{21}b_{22}<b_{11}-\theta_{21}b_{12}<0$, $A(1,0)$ is a stable point, both $O(0,0)$ and $B(1,1)$ are saddle points, $C(0,1)$ is an unstable point, and $D(p^*,q^*)$ is a center point

4.5. Further Discussion and Analysis. According to the above analysis, when the parameters in the income matrix satisfy Conditions 1–3, the system has four equilibrium points, $O(0,0)$, $C(0,1)$ $A(1,0)$, and $B(1,1)$. Under these conditions, the game system has a unique evolutionary stable state, which is related to the incentive coefficients θ_{ij} and Δ_{ij}. When the payoff function of attack-protect satisfies Condition 4, there are five equilibrium points: $O(0,0)$, $A(1,0)$, $B(1,1)$, $C(0,1)$, and $D(p^*,q^*)$. Next, we analyze Case 1 of situation 5 in Condition 4, and other cases are similar.

Based on the above analysis, we know that, in this situation, $0>a_{12}-\Delta_{21}a_{22}>a_{11}-\Delta_{21}a_{21}, b_{21}-\theta_{21}b_{22}<b_{11}-\theta_{21}b_{12}<0$, $C(0,1)$ and $A(1,0)$ are stable points, both $O(0,0)$ and $B(1,1)$ are unstable point, and $D(p^*,q^*)$ is a saddle point. At this time, the dynamic evolution of the system is shown in Figure 3.

In this situation, $D(p^*,q^*)$ is an internal point in the quadrilateral of vertexes between $O(0,0)$, $C(0,1)$, $A(1,0)$, and $B(1,1)$.

Based on geometry knowledge, the area S of the quadrilateral region by $O(0,0)$, $A(1,0)$, $B(1,1)$, and $D(p^*,q^*)$ is shown as follows:

$$S=\frac{q^*}{2}+\frac{1-p^*}{2}=\frac{1}{2}\left(\frac{a_{12}-\Delta_{21}a_{22}}{a_{12}-\Delta_{21}a_{22}+\Delta_{21}a_{21}-a_{11}}+\frac{\theta_{21}b_{12}-b_{11}}{b_{21}-\theta_{21}b_{22}+\theta_{21}b_{12}-b_{11}}\right). \tag{35}$$

Because of $(\partial S/\partial\Delta_{21})=(a_{11}a_{22}-a_{12}a_{21})/(2(a_{12}-\Delta_{21}a_{22}+\Delta_{21}a_{21}-a_{11})^2)>0$, when Δ_{21} increases, S will increase and the equilibrium strategy is $p_1(t)=1$; similarly, because of $\partial S/\partial\theta_{21}=(b_{12}b_{21}-b_{11}b_{22})/(2(b_{21}-\theta_{21}b_{22}+\theta_{21}b_{12}-b_{11})^2)<0$, when θ_{21} increases, S will decrease and the equilibrium strategy is $q_1(t)=0$. So the stable state of the system tends to the equilibrium point $A(1,0)$; on the contrary, the stable state of the system tends to the equilibrium point $C(0,1)$.

This paper extends the framework of evolutionary game theory by incentive coefficient, analyzes the evolutionary stability of two players when they adopt different strategies, and reflects the influence of incentive coefficient on game decision making. Further analysis shows that the incentive coefficient can affect the optimal behavior of the players in multiple stable states and affect the evolution trend of the stable state of the dynamic system.

5. Experiment Simulation and Analysis

Based on the evolution of dynamic privacy protection game in this paper, a simple network system is deployed for simulation experiments to verify the validity of our research. The system's topology environment is shown in Figure 4, which is mainly composed of cloud computing protection device, web server, file server, data server, and client. The access control rules are that the remote host can only access the web server in the system, and the local host can access the data server.

We set the duration time of the game of attack and protect for 35 minutes, $t\in[0,35]$, and we can realize the optimal protect strategy selection algorithm and obtain the optimal game strategy.

5.1. Experiment 1. Aiming at the above conventional attack-protect model, system dynamics is used to simulate and analyze the selection of the optimal protect strategy in the

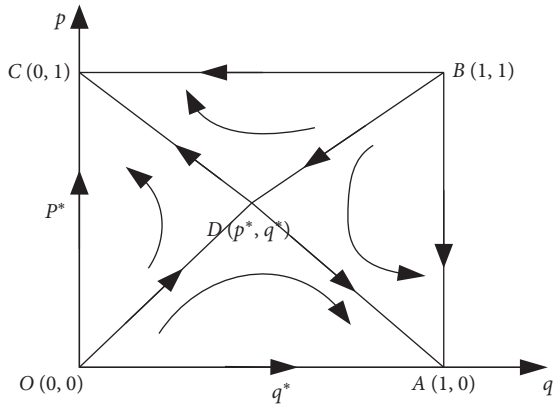

FIGURE 3: The dynamic attack-protect evolutionary replication relationship of $a_{11} - \Delta_{21}a_{21} < 0 < a_{12} - \Delta_{21}a_{22}, b_{21} - \theta_{21}b_{22} < 0 < b_{11} - \theta_{21}b_{12}$.

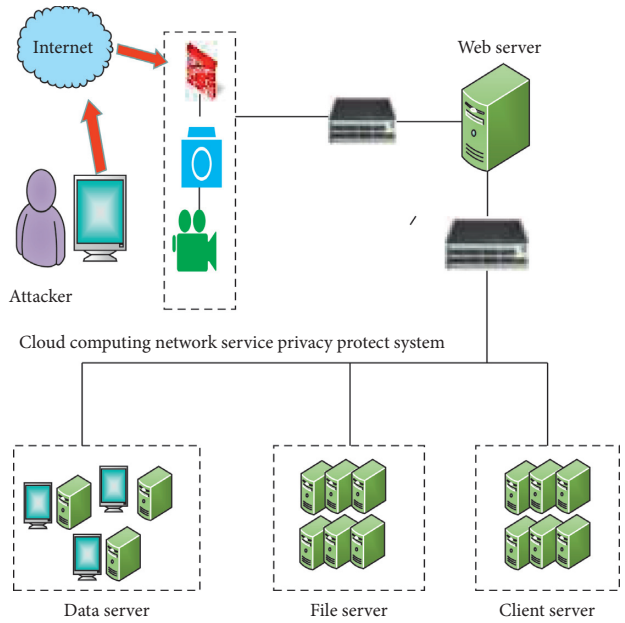

FIGURE 4: Experiment structural topology.

evolutionary game model. Section 3 shows that the evolutionary stable states analyses of this attack-protect game model are $Y_1 = \begin{bmatrix} 0 \\ 0 \end{bmatrix}$, $Y_2 = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$, $Y_3 = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$, and $Y_4 = \begin{bmatrix} 1 \\ 1 \end{bmatrix}$ in four kinds of situations. Next, we will simulate the different states of p and q. By observing their evolution trend, we can get the final stable state of evolution, and we can realize the prediction of attack strategy and select the optimal protect strategy:

(1) When the initial states are $p = 0$ and $q = 0$, the adversary chooses a strategy AS_2, and the protector chooses a strategy PS_2. From the evolution of the system, the choice of strategies between the adversary and the protector will be consistent. PS_2 is the optimal protect strategy in Figure 5.

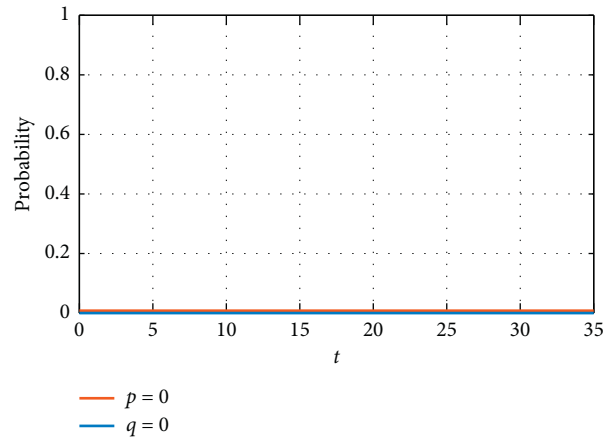

FIGURE 5: Evolution curve of $p = 0$ and $q = 0$.

(2) When the initial states are $p = 1$ and $q = 1$, the adversary chooses a strategy AS_2, and the protector chooses a strategy PS_2. From the evolution of the system, it can be seen that the choice of strategies between the adversary and the protector will be consistent. PS_1 is the optimal protect strategy in Figure 6.

(3) When the initial state is $p = 0.3$ and $q = 0.4$, the adversary chooses $\{AS_1, AS_2\}$ with the probability $(0.3, 0.7)$ and the protector chooses $\{PS_1, PS_2\}$ with the probability $(0.4, 0.6)$. After continuous evolution, the protector finally does not choose strategy PS_1 and chooses PS_2 to reach equilibrium state. $Y_1 = \begin{bmatrix} 0 \\ 0 \end{bmatrix}$ is one of the evolutionary equilibrium points, and PS_2 is the optimal protect strategy in Figure 7.

(4) When the initial state is $p = 0.6$ and $q = 0.4$, the adversary chooses $\{AS_1, AS_2\}$ with the probability $(0.6, 0.4)$, and the protector chooses $\{PS_1, PS_2\}$ with the probability $(0.4, 0.6)$. After continuous evolution, the protector finally chooses PS_2 instead of PS_1. $Y_1 = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$ is the equilibrium point, PS_2 is the optimal protect strategy in Figure 8 at this time, (investment protection, no attack) is the evolution stable strategy of attack protect, and investment protection is the optimal selection of the protector.

(5) When the initial state is $p = 0.3$ and $q = 0.7$, the adversary chooses AS_2, and the protector chooses a strategy PS_1. After continuous evolution, the protector finally chooses PS_1 to reach an equilibrium state, the value of q tends to be 1, and the value of p tends to be 0. $Y_3 = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$ is the equilibrium point, and PS_1 is the optimal protect strategy in Figure 9.

(6) When the initial states are $p = 0.8$ and $q = 0.7$, after continuous evolution, the adversary chooses AS_2, and the protector chooses strategy PS_1. The values of

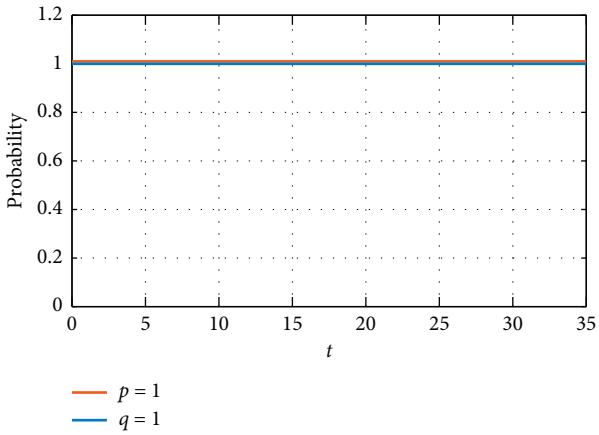

Figure 6: Evolution curve of $p = 1$ and $q = 1$.

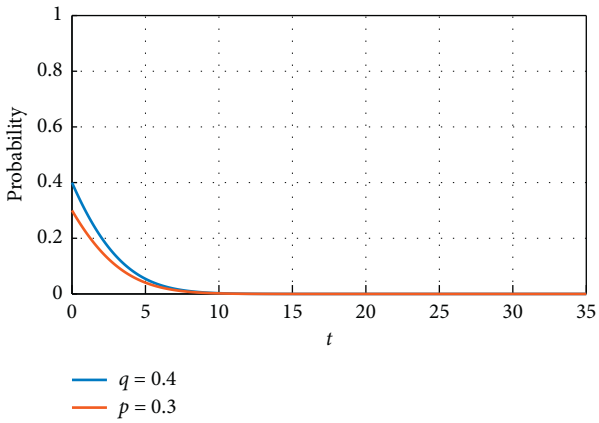

Figure 7: Evolution curve of $p = 0.3$ and $q = 0.4$.

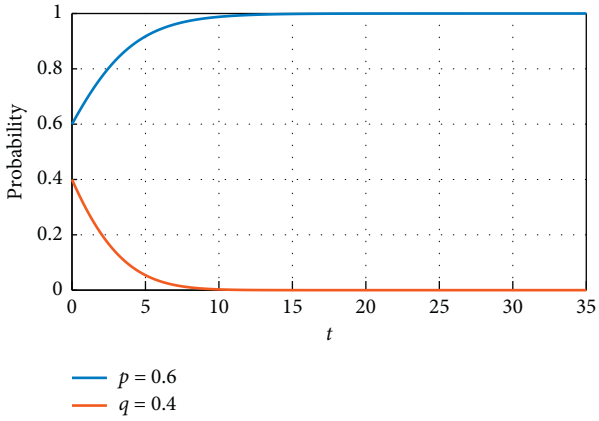

Figure 8: Evolution curve of $p = 0.6$ and $q = 0.4$.

p and q tend to be 1, $Y_4 = \begin{bmatrix} 1 \\ 1 \end{bmatrix}$ is the evolutionary equilibrium point, and PS_1 is the optimal protect strategy in Figure 10.

When q is adjusted from 0.91 to 0.86 and p is adjusted from 0.44 to 0.38, the simulation evolution trend of the game has no obvious change in Figure 11, which indicates that the game has good robustness. Therefore, the game model has good adaptability and can be applied to complex and changeable network environment.

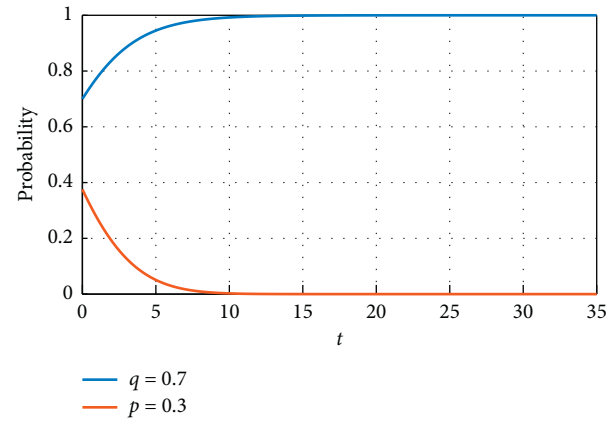

Figure 9: Evolution curve of $p = 0.3$ and $q = 0.7$.

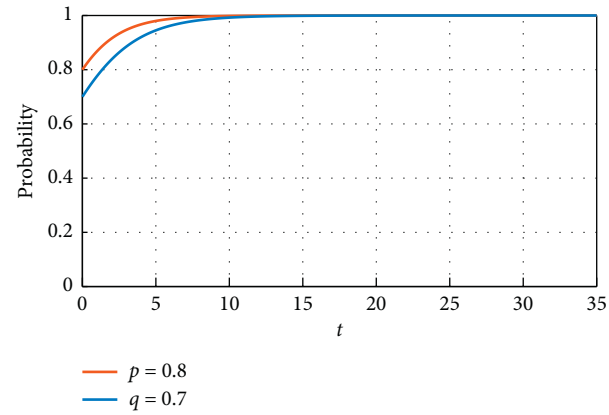

Figure 10: Evolution curve of $p = 0.8$ and $q = 0.7$.

From the above simulation results, we can see that the evolutionary system will eventually evolve to a stable state under the initial state of different strategies. By observation and comparison, we can find that the simulation results of the system are consistent with the theoretical analysis of the model, which shows that the evolutionary game model is consistent with the evolutionary law of the real system.

The influence of parameter variation on system behavior is studied by parameter sensitivity test. If the parameters change slightly, the evolutionary behavior curve changes greatly, which indicates that the game model is sensitive, and it is difficult to maintain stability and robustness in the the network environment, and vice versa.

5.2. Experiment 2. During this experiment, the game strategies consist of attack strategy $AS_i = \{r_1, r_2, \ldots, r_k\}$ and protect strategy $PS_i = \{b_1, b_2, \ldots, b_l\}$. The atomic attack strategies are shown in Table 3 and the atomic protect strategy is shown in Table 4. In the experiment, we design these related attack strategies for $AS_1 = \{r_1, r_2, r_5\}$ and $AS_2 = \{r_3, r_4, r_6\}$ and protect strategy for $PS_1 = \{b_3, b_4, b_6\}$ and $PS_2 = \{b_1, b_2, b_5\}$.

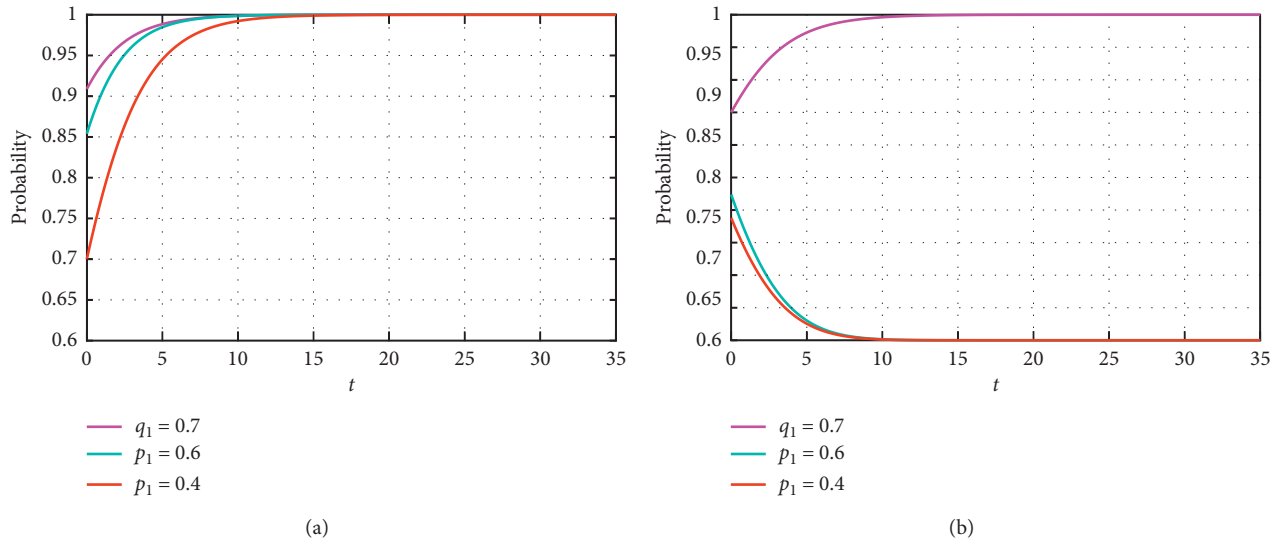

Figure 11: Sensitivity test of game parameter. (a) $q = 0.91$, $q = 0.86$ and $p = 0.7$. (b) $p = 0.44$, $p = 0.38$, $q = 0.7$.

Table 3: Atomic attack strategy description.

Number	Attack action name	Attack strategy	
		AS_1	AS_2
r_1	Weak password	√	
r_2	Node attack	√	
r_3	Trojan horse		√
r_4	Network monitoring		√
r_5	User name enumeration	√	
r_6	Network sniffing		√

Table 4: Description of atomic protect strategy.

Number	Protection action name	Protect strategy	
		PS_1	PS_2
b_1	System update		√
b_2	Behavioral filtering		√
b_3	Abnormal recognition	√	
b_4	Delete suspicious accounts	√	
b_5	Tool detection		√
b_6	Firmware update	√	

By setting different values of incentive coefficients, we verify the influence of the dependence between different strategies on the evolution process of the game, and we highlight the superiority of the improved replicated dynamic evolutionary game model. The greater the incentive coefficient, the greater the influence among the strategies; otherwise, the smaller the influence among the strategies. In the cloud computing system, there are 200 players, according to the different values of the incentive coefficients (Table 5), the initial parameters in the experiment are $(q_1, p_1) = (0.3, 0.4)$ and $(q_1, p_1) = (0.7, 0.6)$, and the role of different incentive coefficients in the evolution process of the game can be obtained.

(1) Under the conditions $\theta_{21} = 1$ and $\Delta_{21} = 1$, there is no dependency between protect strategy and attack strategy. The evolution process belongs to the classical replication dynamics. The state evolution trend of the game system is shown in Figure 12. When the initial state is $(q_1, p_1) = (0.3, 0.4)$, PS_1 achieves stability at the time $t = 7$ and AS_1 achieves stability at time $t = 8$. When the initial state is $(q_1, p_1) = (0.7, 0.6)$, PS_1 achieves stability at time $t = 8$ and AS_1 achieves stability at time $t = 9$.

Table 5: The value of related game parameters.

$a_{11} = 12$	$a_{12} = 10$	$a_{21} = 10$	$a_{22} = 12$	$a_1 = 1$
$b_{11} = 10$	$b_{12} = 12$	$b_{21} = 12$	$b_{22} = 10$	$\beta_1 = 1$

(2) Under the conditions $\theta_{21} = 0.5$ and $\Delta_{21} = 0.5$, the protect strategy PS_2 promotes PS_1 and the attack strategy AS_2 promotes AS_1. The state evolution trend of the game system is shown in Figure 13. When the initial state is $(q_1, p_1) = (0.3, 0.4)$, PS_1 achieves stability at time $t = 2$ and AS_1 achieves stability at time $t = 2$. When the initial state is $(q_1, p_1) = (0.7, 0.6)$, PS_1 achieves stability at time $t = 3$ and AS_1 achieves stability at time $t = 5$.

(3) Under the conditions $\theta_{21} = 1.5$ and $\Delta_{21} = 1.5$, the protect strategy PS_2 promotes PS_1 and the attack strategy AS_2 promotes AS_1. The state evolution trend of the game system is shown in Figure 14. When the initial state is $(q_1, p_1) = (0.3, 0.4)$, strategy PS_1 achieves stability at time $t = 8$ and strategy AS_1 achieves stability at time $t = 10$. When the initial state is $(q_1, p_1) = (0.7, 0.6)$, strategy PS_1 achieves stability at time $t = 10$ and strategy AS_1 achieves stability at time $t = 12$. Compared with Figure 12, when $\theta_{21} = 1.5$ and $\Delta_{21} = 1.5$, different strategies in the same group have a suppression effect, which reduces the convergence speed of the protective strategy. This can lead to better performance.

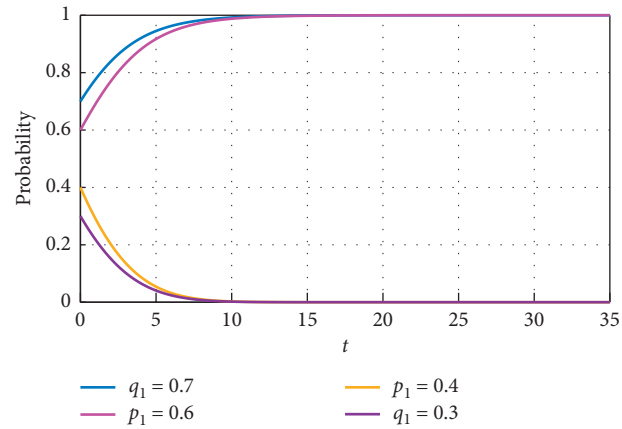

Figure 12: Evolution game of attack-protect under $\theta_{21} = 1$ and $\Delta_{21} = 1$.

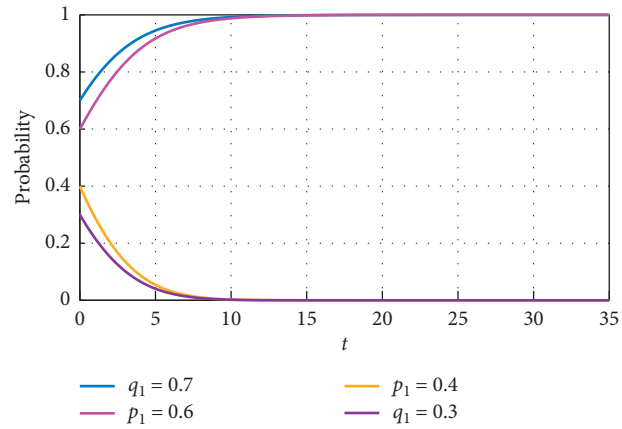

Figure 14: Evolution game of attack-protect under $\theta_{21} = 1.5$ and $\Delta_{21} = 1.5$.

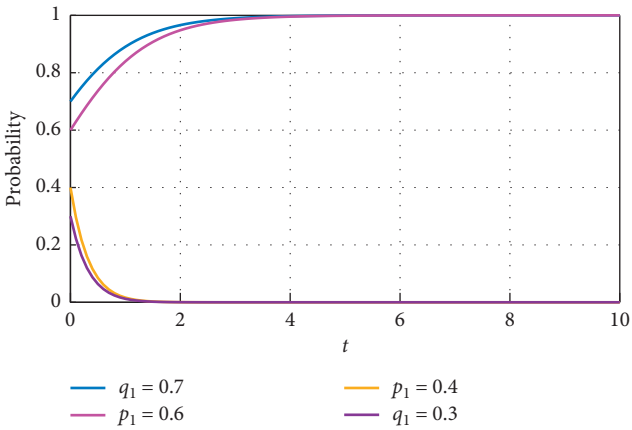

Figure 13: Evolution game of attack-protect under $\theta_{21} = 0.5$ and $\Delta_{21} = 0.5$.

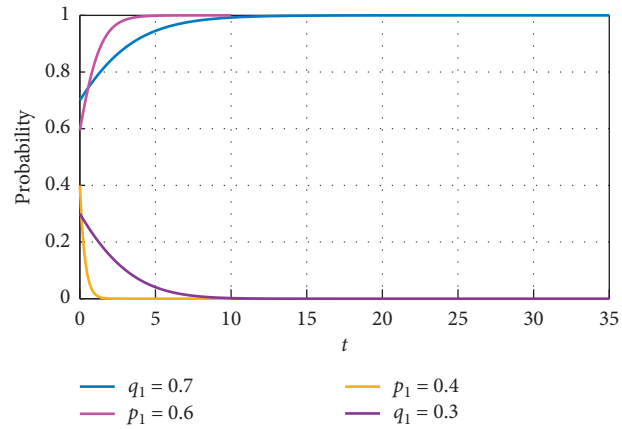

Figure 15: Evolution game of attack-protect under $\theta_{21} = 0.5$ and $\Delta_{21} = 1.5$.

(4) Under the conditions $\theta_{21} = 1.5$ and $\Delta_{21} = 0.5$, the protect strategy PS_2 can suppress PS_1 and the attack strategy AS_2 can promote AS_1. The state evolution trend is shown in Figure 15. When the initial state is $(q_1, p_1) = (0.2, 0.3)$, strategy PS_1 achieves stability at time $t = 10$, strategy AS_1 achieves stability at time $t = 2$. When the initial state is $(q_1, p_1) = (0.6, 0.7)$, strategy PS_1 achieves stability at time $t = 11$ and strategy AS_1 achieves stability at time $t = 4$. Compared with Figure 12, when $\theta_{21} = 1.5$, the strategy PS_2 can suppress PS_1 and reduce the convergence speed. When $\Delta_{21} = 0.5$, the strategy AS_2 can promote AS_1 and accelerate the convergence speed.

(5) Under the conditions $\theta_{21} = 0.5$ and $\Delta_{21} = 1.5$, the strategy PS_2 can promote PS_1 and the strategy AS_2 can suppress AS_1. The state evolution trend is shown in Figure 16. When the initial state is $(q_1, p_1) = (0.3, 0.4)$, PS_1 achieves stability at time $t = 2$ and AS_1 achieves stability at time $t = 10$. When the initial state is $(q_1, p_1) = (0.7, 0.6)$, PS_1 achieves stability at time $t = 3$ and AS_1 achieves stability at time $t = 12$. Compared with Figure 12, when $\Delta_{21} = 1.5$, AS_2 can suppress AS_1 and reduce the convergence speed. When $\theta_{21} = 0.5$, PS_2 can promote PS_1 and accelerate the convergence speed.

5.3. Comparison of Several Models. According to the experimental parameters in Table 5 and formulas (29) and (31), we compare this paper with [11, 14, 18] to enhance credibility, and we show the results with several experimental graphs.

According to Figure 17(a), with the increase of experiments, the average attack rate is stable at 0.141, 0.135, 0.125, and 0.114, respectively. Our scheme is lower than [11, 14, 18], because our scheme can moderately adjust the relationship between attack strategy and protection strategy, and has better adaptability.

According to Figure 17(b), in terms of the average attack detection rate, alarm rate, and survived service rate, our

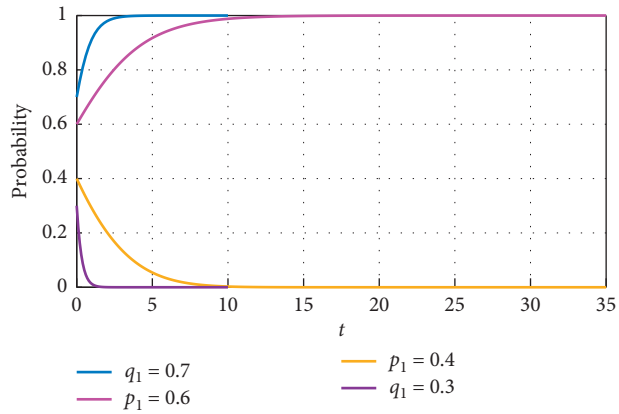

Figure 16: Evolution game of attack-protect under $\theta_{21} = 1.5$ and $\Delta_{21} = 0.5$.

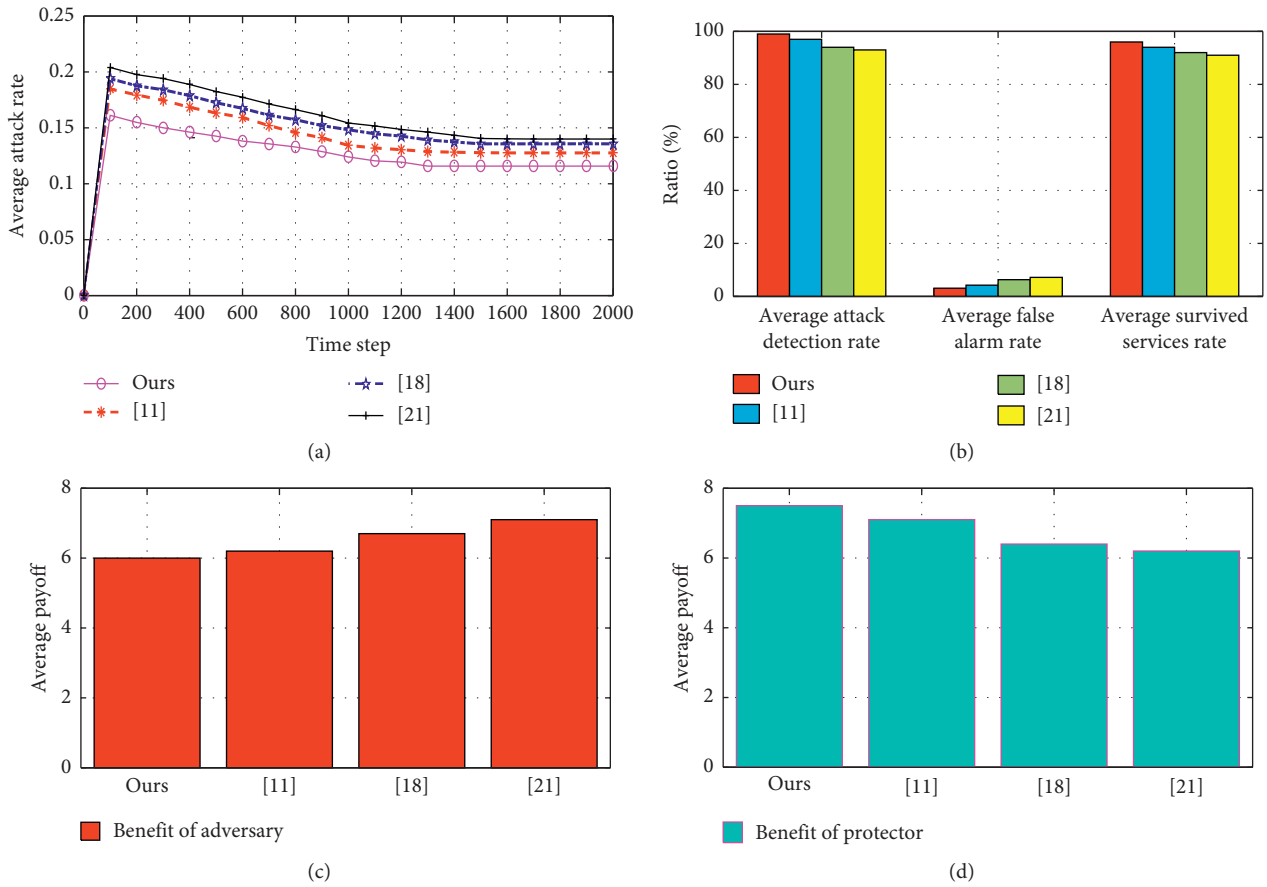

Figure 17: Comparison of several models.

scheme performs better than [11, 14, 18]. According to Figures 17(c) and 17(d), compared with [11, 14, 18], in our scheme, the protector can get more benefits and the attacker can get fewer benefits.

Through observation and comparison, different incentive coefficients have different effects on the convergence speed of game system evolution. This shows that our research improves the evolution process of the game and can be used to guide cloud computing privacy protection.

5.4. Performance Comparison. To further show the characteristics and advantages of our study, the related results of comparison with other works of literature are shown in Table 6.

Table 6: Performance analysis and comparison.

Article	Game type	Rationality	Reproduction rate	Player	Equilibrium	Versatility	Application
[21]	Dynamic game	Complete information	General	2	Simple	Poor	Cloud security
[8]	Dynamic game	Complete information	Poor	2	General	Poor	Mobile environment
[17]	Evolutionary game	Incomplete information	Poor	N	General	Poor	Strategy selection
[18]	Evolutionary game	Incomplete information	Poor	N	General	General	Strategy selection
[27]	Evolutionary game	Incomplete information	Poor	2	General	General	Cloud storage
[Our]	Evolutionary game	Incomplete information	Good	N	Good	Good	Strategy selection

In [8, 21], the participants are completely rational, but because of the participants' incomplete rationality in the implementation, the feasibility of the model is reduced. Literature [17] and literature [18] are evolutionary game models, but the process of solving the model is simple. The universality of a model is mainly reflected in whether the type and strategy set are well extended to n. Paper [27] is only applicable to two game objects, and its universality is poor, which indicates that the model can only be applied to special cases. Moreover, our model has good generality by extending the optional strategy to n and can be applied to the common selection strategy.

6. Conclusion

Privacy protection has always been a hotpot in the field of cloud computing. Based on the assumption of bounded rationality, this paper proposes an attack protection game model for privacy strategy selection. Firstly, the dynamic replication equation is used to analyze the strategy process of the attack-protect and the formation mechanism of the evolution stable state. Secondly, the solution method of the evolution stable strategy is proposed, and the optimal privacy strategy selection algorithm is designed. Thirdly, aiming at the problem of strategy dependence, we construct an improved replication dynamic attack-protect evolutionary game model by incentive coefficients, and we use the Jacobian matrix to analyze the stability of the equilibrium point and get the optimal protect strategies under different conditions. Finally, the effectiveness of our research is validated by simulation experiments under several game parameters.

Our research expands the evolutionary game theory and has important significance for cloud computing privacy protection [25]. Although this paper is limited to analyzing the situation of two players of two strategies, for the stable state of multiple strategies of multiple players, the same theory can be studied; only the amount of calculation is relatively complex. This will play an important role in guiding the use of evolutionary game theory to solve practical problems. Besides, there are still some shortcomings, such as the determination of attack-protect strategy set, lack of credible third-party supervision, and the quantification of incentive coefficient, which will become the future research [28, 29].

Data Availability

The data used to support the findings of the article are included within the article.

Conflicts of Interest

The author declares no conflicts of interest regarding the publication.

References

[1] J. V. Neumann and O. Morgenstern, *Theory of Games and Economic Behavior: 60th Anniversary Commemorative Edition*, Princeton University Press, Princeton, NJ, USA, 2007.

[2] Cloud Security Alliance, *Security Guidance for Critical Areas of Focus in Cloud Computing V4.0*, Cloud Security Alliance, Seattle, WA, USA, 2017, http://www.cloudsecurityalliance.org/.

[3] C. T. Do, N. H. Tran, C. Hong et al., "Game theory for cyber security and privacy," *ACM Computing Surveys*, vol. 50, no. 2, pp. 1–37, 2017.

[4] R. Cressman and J. Apaloo, "Evolutionary game theory," *Handbook of Dynamic Game Theory*, Springer International Publishing AG, part of Springer Nature, Cham, Switzerland, pp. 461–510, 2018.

[5] R. L. Neupane, T. Neely, P. Calyam, N. Chettri, M. Vassell, and R. Durairajan, "Intelligent defense using pretense against targeted attacks in cloud platforms," *Future Generation Computer Systems*, vol. 93, pp. 609–626, 2019.

[6] L. Xiao, D. Xu, N. B. Mandayam, and H. V. Poor, "Attacker-centric view of a detection gameagainst advanced persistent threats," *IEEE Transactions on Mobile Computing*, vol. 17, no. 11, pp. 2512–2523, 2018.

[7] L. Xiao, D. Xu, N. B. Mandayam, and H. V. Poor, "Cloud storage defense against advanced persistent threats: a prospect theoretic study," *IEEE Journal on Selected Areas in Communications*, vol. 35, no. 3, pp. 534–544, 2017.

[8] Y.-P. Li, S.-Y. Tan, Y. Deng, and J. Wu, "Attacker-defender game from a network science perspective," *Chaos:An Interdisciplinary Journal of Nonlinear Science*, vol. 28, no. 5, Article ID 051102, 2018.

[9] K. Lv, Y. Chen, and C. Hu, "Dynamic defense strategy against advanced persistent threat under heterogeneous networks," *Information Fusion*, vol. 49, pp. 216–226, 2019.

[10] A. R. Sfar, Y. Challal, P. Moyal, and E. Natalizio, "A game theoretic approach for privacy preserving model in IoT-based transportation," *IEEE Transactions on Intelligent Transportation Systems*, vol. 20, no. 12, pp. 4405–4414, 2019.

[11] M. Min, L. Xiao, C. Xie, M. Hajimirsadeghi, and N. B. Mandayam, "Defense against advanced persistent threats in dynamic cloud storage: a colonel blotto game approach," *IEEE Internet of Things Journal*, vol. 5, no. 6, pp. 4250–4261, 2018.

[12] A. R. Hota and S. Sundaram, "Interdependent security games on networks under behavioral probability weighting," *IEEE Transactions on Control of Network Systems*, vol. 5, no. 1, pp. 262–273, 2018.

[13] A. Jakóbik, F. Palmieri, and J. Kołodziej, "Stackelberg games for modeling defense scenarios against cloud security threats," *Journal of Network and Computer Applications*, vol. 110, pp. 99–107, 2018.

[14] O. A. Wahab, J. Bentahar, H. Otrok, and A. Mourad, "Resource-aware detection and defense system against multi-type attacks in the cloud: repeated bayesian stackelberg game," *IEEE Transactions On Dependable And Secure Computing*, p. 1, 2019.

[15] N. B. Khalifa, R. El-Azouzi, Y. Hayel, and I. Mabrouki, "Evolutionary games in interacting communities," *Dynamic Games and Applications*, vol. 7, no. 2, pp. 131–156, 2017.

[16] C. Jiang, L. Kuang, Z. Han, Y. Ren, and L. Hanzo, "Information credibility modeling in cooperative networks: equilibrium and mechanism design," *IEEE Journal on Selected Areas in Communications*, vol. 35, no. 2, pp. 432–448, 2017.

[17] S. Tan, S. Feng, P. Wang, and Y. Chen, "Strategy selection in evolutionary game dynamics on group interaction networks," *Bulletin of Mathematical Biology*, vol. 76, no. 11, pp. 2785–2805, 2014.

[18] H. Hu, Y. Liu, H. Zhang, and R. Pan, "Optimal network defense strategy selection based on incomplete information evolutionary game," *IEEE Access*, vol. 6, pp. 29806–29821, 2018.

[19] J. Du, C. Jiang, K.-C. Chen, Y. Ren, and H. V. Poor, "Community-structured evolutionary game for privacy protection in social networks," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 3, pp. 574–589, 2018.

[20] H. Zhang, K. Zheng, X. Wang, S. Luo, and B. Wu, "Efficient strategy selection for moving target defense under multiple attacks," *IEEE Access*, vol. 7, pp. 65982–65995, 2019.

[21] C. A. Kamhoua, L. Kwiat, K. A. Kwiat, J. S. Park, M. Zhao, and M. Rodriguez, "Security and interdependency in a public cloud: a game-theoretic approach," *Game Theory for Security and Risk Management, Static & Dynamic Game Theory: Foundations & Applications*, Springer, Berlin, Germany, 2018.

[22] H. Wu, W. Wang, C. Wen, and Z. Li, "Game theoretical security detection strategy for networked systems," *Information Sciences*, vol. 453, pp. 346–363, 2018.

[23] L. Cheng, H.-Q. Zhang, L.-M. Wan, L. Liu, and D.-H. Ma, "Incomplete information Markov game theoretic approach to strategy generation for moving target defense," *Computer Communications*, vol. 116, pp. 184–199, 2018.

[24] L. Cheng, D.-H. Ma, and H.-Q. Zhang, "Optimal strategy selection for moving target defense based on markov game," *IEEE Access*, vol. 5, pp. 156–169, 2017.

[25] J. Zhang, Y. Zhu, and Z. Chen, "Evolutionary game dynamics of multiagent systems on multiple community networks," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, pp. 1–17, 2018.

[26] N. Armstrong, J. B. Hong, D. D. Kim et al., "Threat-specific security risk evaluation in the cloud," *IEEE Transactions On Cloud Computing*, vol. 99, p. 1, 2018.

[27] A. A. A. Abass, L. Xiao, N. B. Mandayam, and Z. Gajic, "Evolutionary game theoretic analysis of advanced persistent threats against cloud storage," *IEEE Access*, vol. 5, pp. 8482–8491, 2017.

[28] W. Duan, C. Li, P. Zhang, and Q. Chang, "Game modeling and policy research on the system dynamicsbased tripartite evolution for government environmental regulation," *Cluster Computer*, vol. 19, no. 4, pp. 2061–2074, 2016.

[29] H. Ding, Y. Wang, S. Guo, X. Xu, and C. Che, "Game analysis and benefit allocation in international projects among owner, supervisor and contractor," *International Journal of General Systems*, vol. 45, no. 3, pp. 253–270, 2016.