Hindawi
Complexity
Volume 2021, Article ID 4020784, 15 pages
https://doi.org/10.1155/2021/4020784

Research Article

Users' Payment Intention considering Privacy Protection in Cloud Storage: An Evolutionary Game-Theoretic Approach

Jianguo Zheng and Jinming Chen

Glorious Sun School of Business and Management, Donghua University, Shanghai, China

Correspondence should be addressed to Jinming Chen; 2191065@mail.dhu.edu.cn

Received 5 July 2021; Revised 1 November 2021; Accepted 27 November 2021; Published 15 December 2021

Academic Editor: Hassan Zargarzadeh

To solve the current privacy leakage problems of cloud storage services, research on users' payment intention for cloud storage services with privacy protection is extremely important for improving the sustainable development of cloud storage services. An evolutionary game model between cloud storage users and providers that considers privacy is constructed. Then, the model's evolutionary stability strategies via solving the replication dynamic equations are analyzed. Finally, simulation experiments are carried out for verifying and demonstrating the influence of model parameters. The results show that the evolutionary stable strategies are mainly affected by the privacy protection profit growth coefficient of both parties, input costs, free-riding gains, and other factors. If the profit growth coefficient is very small, users will not choose to pay and providers will not choose to actively protect user information. As the profit growth coefficient increases, both parties will promote the development of privacy protection with a higher probability. The results are beneficial for cloud storage providers to increase the number of paid users and thus to achieve the sustainable development of cloud storage service.

1. Introduction

With the gradual maturation of cloud computing, massive user data has brought huge demands for file storage, synchronization, and sharing. The development of cloud storage services is also in full swing. The convenience of accessing and using cloud storage services anytime and anywhere makes cloud storage an inevitable tendency. According to iiMedia Consulting's statistics, China's personal cloud storage users have exceeded 374 million in 2019 and reached 404 million in 2020 [1]. However, cloud storage service can not only bring convenience, but also bring some risks such as data security risk and privacy leakage risk.

A greater focus on privacy protection and data security will not only protect cloud storage services from hackers, but also reduce the impact and severity of these types of risks. In addition, the collected user information can be used for personalized recommendation services to users while complying with the privacy policies. However, both parties involved in cloud storage are reluctant to provide such input due to the following reasons: First, despite the fact that hundreds of millions of people are using cloud storage, only 10% of them are paying customers. The cost of maintaining the normal operation of cloud storage is high. In addition, data security and privacy investments do not necessarily bring additional revenue, and service providers do not have unlimited budgets to support such investments. Moreover, cloud storage providers are also concerned with the weak impact of increasing investments in privacy protection and data security on users' willingness to pay. Second, from the perspective of cloud users, there is a deep-rooted sense among users that cloud storage services are free. However, their A cloud storage service provider's level of privacy protection will be one factor that users consider when deciding whether to pay for continuous use. As a result, we observe that economic considerations influence users' and service providers' strategic choices. The fundamental motive for preserving privacy protection and data security for cloud storage services is long-term profits. As a result, determining the long-term viability of maintaining privacy protection

efforts is critical. Game theory [2] has been widely applied into data privacy game to balance the cost and profit of preserving privacy and data protection investment because of its great analysis ability.

Each participant in game theory is rational and will make the best strategic decision in terms of profit maximization, which is the most important aim [3, 4]. Many game theory strategies have become popular in recent years for solving information security issues. Traditional game strategy, on the other hand, assume that both players are rational. This assumption, however, does not match reality. Players are believed to have limited reasoning and to work with inadequate information in reality. Long-term earnings change at each stage, and high-margin strategies tend to supplant low-margin strategies over time; past studies have not looked at the long-term viability of portfolio investments. It is crucial to look into the incentives that encourage people to keep their money in cloud storage service. Evolutionary game theory has a number of advantages over standard game theory. First, the evolutionary game extends the complete rationality of traditional game theory to bounded rationality, believing that participants' choice behavior is limited by their limited cognitive ability and that they typically make decisions based on habits and conventional rules of thumb, which is more practical. Second, traditional game theory places too much emphasis on the solution of game equilibrium and ignores the strategy evolution of each game participant. By introducing various dynamic mechanisms, evolutionary game theory investigates the relationship between the stable structure of the game system and the evolutionary process.

The sustainable and secure development of personal cloud storage is the result of the participants' strategic choices, and there are conflicts and contradictions among the participants to participate in the sustainable and secure development of personal cloud storage service to maximize their own interests. At the same time, due to the limitations of information asymmetry, environmental uncertainty, and their judgment, the participants have the personal characteristics of limited rationality, and the game system cannot reach the Nash equilibrium state at once. Thus, the formation of sustainable and secure development of personal cloud storage services is actually a specific result of the participants in a finite rational game, and the strategic choice of the participants not only depends on their profit and loss coefficients, but also is influenced by the strategy choices of other stakeholders. In addition, there are multiple individuals with different strategy choices in the same participant group, and participants will repeatedly learn and adjust to imitate the strategy with higher gains in the game process. Thus, the strategic interaction of participants in the sustainable security development of personal cloud storage services meets the prerequisites of evolutionary game modeling, and the privacy protection and information security investment are essentially a dynamic evolutionary game process of each participant's strategy, and the whole game is always in motion, and it takes a long time to reach the evolutionary stable state of the game system.

In this paper, we combine the characteristics of cloud storage services, use evolutionary game theory, regard cloud storage service providers and cloud storage users as bounded rational game parties with certain learning capabilities, and regard the behaviors and decisions of both parties regarding cloud storage services as gradual progress. During the learning process, an evolutionary game model of cloud storage service participants in consideration of privacy protection is constructed. By analyzing the evolutionary stability strategy of the evolutionary game model, the key factors affecting the evolution of cloud storage service providers and cloud storage users' payment behavior are studied, and simulation experiments are used to simulate the model to obtain a more intuitive strategy evolution trend.

The remainder of this paper is organized as follows: Section 2 reviews the literature about cloud storage. Section 3 establishes an evolutionary game model of the interaction relationship between cloud storage providers and users and assesses the local stability of each equilibrium point in model. Section 4 vividly describes the results of evolutionary game simulation, which properly verifies the model we presented. Section 5 proposes the conclusion, limitation, and future work of our work. To more comprehensively understand the paper, a paper structure framework is provided in Figure 1.

2. Literature Review

In recent years, existing research on cloud storage privacy protection has mainly focused on cloud storage privacy protection technology and user adoption intention.

2.1. Cloud Storage Privacy Protection Technology. Governments, businesses, and individual users are all actively transferring their data to the cloud at the moment. However, there is a higher danger of illegal access, data leakage, sensitive information revelation, and privacy breach as a result of this. [5]. To protect the data privacy stored in the cloud, many scholars proposed protection schemes that are widely applied in cloud storage system, such as such as access control, attribute-based encryption, trust, and encryption. Yang et al. [6] proposed a blockchain-based access control framework with privacy protection in cloud to overcome the problems that sensitive data in the cloud is easily tampered with or disclosed by hackers or cloud internal managers. Wang et al. [7] combined Ethereum blockchain technology with a ciphertext-policy attribute-based encryption method and used Ethereum smart contract technology to store publicly available data on the blockchain network. Zhang et al. [8] developed an anonymous attribute-based access control system architecture for mobile cloud computing and demonstrated how to design an anonymous attribute-based access control system using the anonymous CP-ABE method as the core building block. Maheswari and Cheelu [9] proposed a novel anonymous attribute-based broadcast encryption that has the property of hidden access policy and allows the data owner to share his or her data with numerous participants who are inside a preset receiver

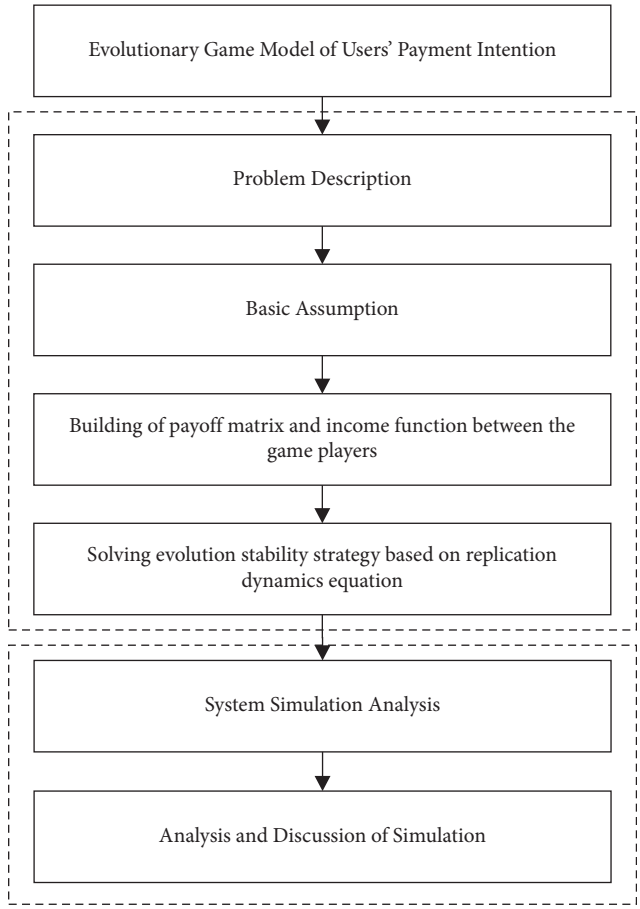

Figure 1: The architecture of the evolutionary game model and system simulation.

group and meet the access policy. Using Exact Regenerating code, Pasupuleti [10] suggested a private public auditing and data dynamics for safe cloud storage. For dynamic shared data in cloud storage, Pasupuleti et al. [11] suggested a certificateless privacy-preserving public auditing approach with group user revocation. Zhang et al. [12] proposed CIPPPA, a cloud-based WBAN-compatible conditional identity privacy-preserving public auditing system. Cloud computing's privacy and data security concerns, on the other hand, are more than just technological ones; they also involve standardization, legislation, and regulations.

2.2. Cloud Storage User Adoption Intention. Few studies have looked into consumers' perceptions of cloud service use, and little is known about the psychological elements that influence user acceptance and adoption. However, there is a considerable disconnect between academic research findings and cloud computing business statements about consumers' security and privacy concerns as they relate to their usage behavior. [13]. From the perspective of the privacy perception of the participants in cloud services, Abdulaziz and Yasin [14] constructed a behavioral model for the continuous use of cloud storage services by researchers from the perspective of perceived risk and explored the perception of specific risk factors by researchers in the process of using cloud storage. Fan et al. [15] combined the characteristics of personal cloud storage services to build a personal cloud storage service quality evaluation system from the perspective of user experience. Gashami et al. [16] constructed a research paradigm based on the Theory of Reasoned Action, the Privacy-Trust-Intention model, and cost-benefit theories to capture the trade-off between advantages and privacy from SaaS customers. Mariani et al. [17] suggested a more complete version of the Technology Acceptance Model for Digital Personal Data Stores, taking into account perceived privacy threats, and trust. Li et al. [18] studied the influence of three basic psychological needs of perception autonomy, perception ability, and perception association on the relationship between cloud storage user information assurance and perception information control. To study the willingness of cloud storage users, Widjaja et al. [19] built a privacy-trust-behavior willingness model. Park and Oh [20] investigated the effects of security breach risk on trust and the intention of a continuous usage of mobile cloud services to determine the components that affect the intention of a continuous use.

2.3. Application of Evolutionary Game in Cloud Storage and Privacy Protection. Game-theoretic techniques give a quantitative decision framework for modeling, analyzing, and forecasting the activities of several participants [21]. Evolutionary Game Theory is a branch of game theory that

integrates Lamarck's genetic theory with Darwin's biological evolution theory [22], and it is also a useful tool for studying how different participants interact. Because its bounded rationality hypothesis is more realistic than classical game theory, it offers a broader set of practical applications. When game participants face a complex situation, due to bounded rationality and information asymmetry at the beginning of the game, they cannot determine the best behavior strategy at the beginning of the game. They continue to optimize their strategies by imitating and learning in the long-term process and improve the realization of game equilibrium. The game theory emphasizes dynamic equilibrium and the analysis of the dynamic evolution process of group behavior, which effectively explains the evolution path and reasons for the group to reach equilibrium. As a research method to describe and solve behavioral decision-making problems, relevant scholars are involved in e-commerce [23], environment protection [24, 25], medical [21], and information security [26–28], and other fields use game theory to analyze the benefits, costs, and losses of different privacy behaviors such as privacy disclosure, investment, and supervision. Wu et al. [23] constructed an evolutionary game model based on Prospect Theory and Mental Account from the standpoint of cooperative supervision between the government and customers to defend consumer rights and support the long-term development of the e-commerce market. It is suggested that the evolution game of participants' strategy does not have a stable equilibrium point based on theoretical derivation and simulation study. Based on game theory, Su [24] examined the evolutionary decision-making process and stable strategies among three parties participating in the CW recycling business, including the government agency, waste recycler, and waste producer. Zhu et al. [25] constructed an evolutionary game to model three types of organizations (including system providers, hospitals, and governments) under the limitations of incomplete knowledge and restricted rationality, using the mHealth system as the environment. In the sphere of cloud storage services, however, fewer scientists have used evolutionary games [29–31]).

2.4. Discussion. Scholars have undertaken many valuable research studies on privacy protection technology, user privacy perception, and evolutionary games in general; however, there are still some gaps that need to be addressed in future research:

(a) The main privacy protection technology of cloud storage service privacy protection research has been improved, ignoring the privacy perception of participants in cloud storage services. It is far from enough to solve the cloud storage privacy problem from the technical level. In real life, the participants of cloud storage services often measure their own benefits and costs from an economic perspective and make decisions.

(b) The research on the willingness to use cloud services mostly uses questionnaires and statistical analysis to solve the problem. The research objects are only users, and the behavior analysis of cloud service providers is ignored.

(c) The willingness to use cloud storage services is often closely related to the perceived benefits of the actors. To date, there are few studies that have investigated how cloud storage providers and users act under the different attitude of privacy protection investment from the perspective of cost-benefit.

Above all, our contributions are as follows:

(a) First, different from the privacy protection technology researches, their perspective focuses on the promotion of privacy protection and data security technology for data storage. Our paper focuses on the cloud storage participants behavior strategy choice of cloud storage service privacy protection, because, in real life, the participants of cloud storage services often measure their own benefits and costs from an economic perspective and make decisions.

(b) Second, different from the research on the willingness to use cloud services, most researches use questionnaires and other statistical analyses to explore the users' subjective feelings about cloud storage service adoption. Our paper aims to explore how participants choose their strategies from the perspective of the cost and benefit of privacy protection.

3. Evolutionary Game Model of Users' Payment Intention

3.1. Problem Description. In the privacy protection game of cloud storage services, stakeholders include cloud storage service providers and cloud storage users. Cloud storage service providers provide services for storing and managing user information. There are two strategies to choose from: actively protecting user information and passively protecting user information. Actively protecting information means that cloud storage service providers have to invest a lot of manpower, material, and financial resources, formulate a strong information security management system, develop information security technology, and resist hacker attacks; passive protection of information means that cloud storage service providers have to deal with user information. The degree of privacy protection is not enough, there is a risk of user information privacy leakage, and cloud storage service providers also actively leak user information to obtain improper benefits. Users are the owners of personal information. Users have two strategies in the game: free use of cloud storage services and paid use of cloud storage services.

3.2. Basic Assumptions

Hypothesis 1: participants are all aimed at maximizing their interests.

Hypothesis 2: due to the differences and evolution of privacy perceptions of different subjects and the hidden benefits of privacy protection investment, cloud storage

service providers and users cannot make the optimal decision to "maximize revenue" in the initial stage, but they are subjects with bounded rationality that have a certain ability to imitate and can adjust their strategies based on experience. Therefore, assuming that the subject of the game is bounded rationality, it is more in line with the actual application context of cloud storage services.

Hypothesis 3: the user uploads data (texts, pictures, videos, etc.) containing their private information to the cloud storage space. If users feel that their information privacy is threatened, then they may give up paying for cloud storage services.

Hypothesis 4: the user's personal information is leaked by the cloud storage service provider or traded to other institutions or organizations to obtain additional benefits. Cloud storage service providers to actively protect user information will increase the cost of information protection. And cloud storage service providers passively protect user information without paying additional information protection costs.

3.3. Evolutionary Game Model Establishment. Based on the above assumptions, considering the main factors that users and cloud storage service providers consider when choosing a game strategy, the model parameters are defined. The symbols and their meanings of each parameter are shown in Table 1.

The payoff matrix between users and cloud storage service providers is shown in Table 2:

3.4. Evolutionary Game Analysis

3.4.1. Equilibrium Point of the Evolution Process. In the initial stage of the evolutionary game, $x\,(0 < x < 1)$ represents the population of users choosing "paid use", and $1 - x$ represents the population choosing "free use." As the same, the population of providers choosing" positive protection" is $y\,(0 < y < 1)$, and the population choosing "negative protection" is $1 - y$. In the evolutionary game, these possibilities evolve and present dynamics.

Based on the payoff matrix, the expected profit obtained by users when the "paid use" strategy (P_{11}) is computed as (1). As the same, the expected profit of users when the "free use" strategy is adopted (P_{12}) is formulated by (2). Combining (1) and (2), the average profit obtained by users $(\overline{P_1})$ is formulated by (3)

$$P_{11} = y\left[(1+\alpha_1)P_u - C_u\right] + (1-y)\left[(1+\alpha_0)P_u - C_u\right], \tag{1}$$

$$P_{12} = y\varepsilon_u + (1-y)P_u, \tag{2}$$

$$\overline{P_1} = xP_{11} + (1-x)P_{12}. \tag{3}$$

According to the Malthusian equation, the users choose the "paid use" strategy growth rate to be described by the difference between P_{11} and P_{12}. Let t be the evolution time; the users' replication dynamic equation for the "paid use" strategy is given in

$$F(x) = \frac{\mathrm{d}x}{\mathrm{d}t} = x\left(P_{11} - \overline{P_1}\right) = x(1-x)\left[yP_u(\alpha_1 - \alpha_0) + y\left(P_u - \varepsilon_u\right) + \alpha_0 P_u - C_u\right]. \tag{4}$$

Similarly, the providers' expected profits when it adopts "positive protection" and "negative" strategies (P_{21} and P_{22}) are formulated by (5) and (6). So, the overall average profit $(\overline{P_2})$ is computed by (7).

$$P_{21} = x\left[(1+\beta_1)P_p - C_p\right] + (1-x)\left[(1+\beta_0)P_p - C_p\right], \tag{5}$$

$$P_{22} = x\varepsilon_p + (1-x)P_p, \tag{6}$$

$$\overline{P_2} = yP_{21} + (1-y)P_{22}. \tag{7}$$

Then, the replication dynamic equation $(F(y))$ is provided in

$$F(y) = \frac{\mathrm{d}y}{\mathrm{d}t} = y\left(P_{21} - \overline{P_2}\right) = y(1-y)\left[xP_p(\beta_1 - \beta_0) + x\left(P_p - \varepsilon_p\right) + \beta_0 P_p - C_p\right]. \tag{8}$$

Table 1: Parameter definition.

Symbol	Description
P_u	Basic storage profits of users if users choose "free use" strategy and providers choose "negative protecting" strategy, $P_u > 0$
P_p	Basic storage service profits of providers if users choose "free use" strategy and providers choose "negative protecting" strategy, $P_p > 0$
C_u	Users' costs of privacy protection service if users choose "paid use" strategy and providers choose "positive protecting" strategy, $C_u > 0$
C_p	Providers' investment costs for improving privacy protection service if users choose "paid use" strategy and providers choose "positive protecting" strategy, $C_p > 0$
ε_u	Profits of users from free riding if users choose "free use" strategy and providers choose "positive protecting" strategy, $\varepsilon_u > P_u > 0$
ε_p	Profits of providers from free riding if users choose "paid use" strategy and providers choose "negative protecting" strategy, $\varepsilon_p > P_p > 0$
α_1	Privacy protection profit growth coefficient of users if users choose "paid use" strategy and providers choose "positive protecting" strategy, $\alpha_1 > 0$
α_0	Privacy protection profit growth coefficient of users if users choose "paid use" strategy and providers choose "negative protecting" strategy, $\alpha_1 > \alpha_0 > 0$
β_1	Privacy protection profit growth coefficient of providers if users choose "paid use" strategy and providers choose "positive protecting" strategy, $\beta_1 > 0$
β_0	Privacy protection profit growth coefficient of providers if users choose "free use" strategy and providers choose "positive protecting" strategy, $\beta_1 > \beta_0 > 0$

Table 2: The payoff matrix.

Cloud storage users	Cloud storage providers	
	Positive protection (y)	Negative protection $(1-y)$
Paid use (x)	$((1+\alpha_1)P_u - C_u, (1+\beta_1)P_p - C_p)$	$((1+\alpha_0)P_u - C_u, \varepsilon_p)$
Free use $(1-x)$	$(\varepsilon_u, (1+\beta_0)P_p - C_p)$	(P_u, P_p)

Based on the solution of (5) and (8), five local equilibrium points from the nonlinear dynamic system are obtained: (0, 0), (0, 1), (1, 0), (1, 1), (x_0, y_0), wherein

$$x_0 = \frac{C_p - \beta_0 P_p}{P_p(\beta_1 - \beta_0 + 1) - \varepsilon_p},$$
$$y_0 = \frac{C_u - \alpha_0 P_u}{P_u(\alpha_1 - \alpha_0 + 1) - \varepsilon_u}. \tag{9}$$

3.4.2. Stable Analysis of Equilibrium Points. The stability of equilibrium points can be analyzed using a Jacobian matrix [32]. The Jacobian matrix can be defined in

$$J = \begin{bmatrix} \dfrac{\partial F(x)}{\partial x} & \dfrac{\partial F(x)}{\partial y} \\ \dfrac{\partial F(y)}{\partial x} & \dfrac{\partial F(y)}{\partial y} \end{bmatrix} = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}. \tag{10}$$

The stability of equilibrium points can be examined using the following conditions:

$$\mathrm{tr}J = a_{11} + a_{22} < 0,$$
$$\det J = a_{11}a_{22} - a_{12}a_{21} > 0. \tag{11}$$

The values of the equilibrium points are shown in Table 3. tr$J$ calculation formulas for each equilibrium point are shown in Table 4, and det$J$ calculation formulas for each equilibrium point are shown in Table 5.

Various equilibrium propositions are analyzed as follows:

Scenario 1. When $0 < \alpha_0 < C_u/P_u, \alpha_0 < \alpha_1 < C_u + \varepsilon_u - P_u/P_u$ and $0 < \beta_0 < C_p/P_p, \beta_0 < \beta_1 < C_p + \varepsilon_p - P_p/P_p$, (0, 0) is ESS point. That is, the cloud storage users and providers are more inclined to "free use, negative protection" strategy.

In this scenario, the users and providers all get less benefit because of the low privacy protection profit growth coefficient ($\alpha_0, \alpha_1, \beta_0$ and β_1). Therefore, (0, 0) is an ESS point, (0, 1) and (1, 0) are saddle points, and (1, 1) is an unstable point.

Scenario 2. When $0 < \alpha_0 < C_u/P_u, \alpha_0 < \alpha_1 < C_u + \varepsilon_u - P_u/P_u$ and $0 < \beta_0 < C_p/P_p, \beta_0 < \beta_1 < C_p + \varepsilon_p - P_p/P_p$, (0, 1) is ESS point. That is, the cloud storage users and providers are more inclined to "free use, positive protection" strategy.

In this scenario, cloud providers' privacy protection profit growth benefit is greater than the cost, but less than the free-riding benefit. Cloud users' protection profit growth benefit is less than the cost, so that they will not choose to pay for usage. Thus, (0, 1) is an ESS point, (0, 0) and (1, 0) are saddle points, and (1, 1) is an unstable point.

Scenario 3. When $0 < \beta_0 < C_p/P_p, \beta_0 < \beta_1 < C_p + \varepsilon_p - P_p/P_p$ and $0 < \beta_0 < C_p/P_p, \beta_0 < \beta_1 < C_p + \varepsilon_p - P_p/P_p$, (1, 0) is ESS point. That is, the cloud storage users and providers are more inclined to "paid use, negative protection" strategy.

Table 3: Values of equilibrium points.

Equilibrium point	α_{11}	α_{12}	α_{21}	α_{22}
$(0,0)$	$\alpha_0 P_u - C_u$	0	0	$\beta_0 P_p - C_p$
$(0,1)$	$P_u 0\alpha_1 + P_u - \varepsilon_u - C_u$	0	0	$-(\beta_0 P_p - C_p)$
$(1,0)$	$-(\alpha_0 P_u - C_u)$	0	0	$P_p\beta_1 + P_p - \varepsilon_p - C_p$
$(1,1)$	$-(P_u\alpha_1 + P_u - \varepsilon_u - C_u)$	0	0	$-(P_p\beta_1 + P_p - \varepsilon_p - C_p)$
(x_0, y_0)	0	$a_{12}(x_0, y_0)$	$a_{21}(x_0, y_0)$	0

Table 4: tr$J$ values of equilibrium points.

Equilibrium point	tr$J$
$(0,0)$	$\alpha_0 P_u - C_u + \beta_0 P_p - C_p$
$(0,1)$	$P_u\alpha_1 + P_u - \varepsilon_u - C_u - (\beta_0 P_p - C_p)$
$(1,0)$	$-(\alpha_0 P_u - C_u) + P_p\beta_1 + P_p - \varepsilon_p - C_p$
$(1,1)$	$-(P_u\alpha_1 + P_u - \varepsilon_u - C_u) - (P_p\beta_1 + P_p - \varepsilon_p - C_p)$
(x_0, y_0)	0

Table 5: det$J$ values of equilibrium points.

Equilibrium point	det$J$
$(0,0)$	$(\alpha_0 P_u - C_u)(\beta_0 P_p - C_p)$
$(0,1)$	$-(\beta_0 P_p - C_p)(P_u\alpha_1 + P_u - \varepsilon_u - C_u)$
$(1,0)$	$-(\alpha_0 P_u - C_u)(P_p\beta_1 + P_p - \varepsilon_p - C_p)$
$(1,1)$	$(P_u\alpha_1 + P_u - \varepsilon_u - C_u)(P_p\beta_1 + P_p - \varepsilon_p - C_p)$
(x_0, y_0)	$-a_{21}(x_0, y_0) * a_{12}(x_0, y_0)$

In this scenario, cloud users' privacy protection profit growth benefit is greater than the cost, but less than the free-riding benefit. Cloud providers' protection profit growth benefit is less than the cost, so that they will not choose to positively protect. Thus, (1, 0) is an ESS point, (0, 0) and (0, 1) are saddle points, and (1, 1) is an unstable point.

Scenario 4. When $0 < \beta_0 < C_p/P_p, \beta_0 < \beta_1 < C_p + \varepsilon_p - P_p/P_p$ and $0 < \beta_0 < C_p/P_p, \beta_0 < \beta_1 < C_p + \varepsilon_p - P_p/P_p$, (0, 1) and (1, 0) are ESS points. That is, the cloud storage users and providers are more inclined to "paid use, positive protection" strategy. The equilibrium state depends on the initial state of system. (1) When the initial state is on area A or D, (0, 1) is ESS point. (2) When the initial state is on area B or C, (1, 0) is ESS point. Then, (0, 0) and (1, 1) are unstable points.

In this scenario, both game players' privacy protection profit growth benefit is greater than the cost, but less than the free-riding benefit. Both game players will choose paid use and positive protect strategy at first because of the high benefit of privacy protection. However, cloud users can get higher profits if they free ride off providers; then they will change their strategy to pay for free; similarly, cloud providers can get higher profits; if they cheat users to negative protect, then they will change their strategy to negative protect.

Scenario 5. When $C_u + \varepsilon_u - P_u/P_u < \alpha_0 < \alpha_1$ and $C_p + \varepsilon_p - P_p/P_p < \beta_0 < \beta_1$, (1, 1) is ESS point. That is, the cloud storage users and providers are more inclined to "paid use, positive protection" strategy.

In this scenario, both game players' privacy protection profit growth benefit is greater than the free-riding benefit. Thus, cloud users and providers are willing to invest for the privacy protection environment of cloud storage. Therefore, (1, 1) is an ESS point, (0, 1) and (1, 0) are two saddle points, and (0, 0) is an unstable point.

Finally, the phase diagrams of the evolutionary game of above five scenarios are shown in Figures 2(a)–2(e). The stability analysis of equilibrium point is shown in Table 6.

4. System Simulation Analysis

To more intuitively show the evolution trend of the game strategy between users and cloud storage service providers in the process of user payment intention with privacy protection and verify the correctness of the constructed model, Matlab R2016a is used to numerically simulate different parameters and the game, and both sides' evolutionary stability strategies are analyzed.

First, the model parameters we assumed are shown in Table 7. Please note that the values we used in this MATLAB simulation are just for illustration, which do not represent the real benefits of stakeholders in cloud storage service.

Then, according to the parameters, these four variables $(\alpha_0, \alpha_1, \beta_0, \beta_1)$ can be calculated as follows. the value range of the four variables is shown as follows: $C_u/P_u = 0.43, C_p/P_p = 0.4, C_u + \varepsilon_u - P_u/P_u = 0.71, C_p + \varepsilon_p - P_p/P_p = 0.6$.

4.1. Simulation of the Evolutionary Process. The numerical simulation of different ESSs can be analyzed under different values of $\alpha_0, \alpha_1, \beta_0, \beta_1$ as shown in Table 8. The simulation results are depicted in Figures 3(a)–3(e), and these results are consistent with Scenario 1 to Scenario 5:

(1) The parameters are set in Table 8 line 1, which satisfy the conditions in Scenario 1. The simulation result is shown in Figure 3(a), which is consistent with Scenario 1. That is to say, both cloud storage users and providers will converge to 0 no matter what the initial state is. It means that the privacy protection profits of cloud storage users and providers are relatively lower than the costs, so that no one is willing to pay for privacy protection or positive protection. Finally, after a long-term repeated games, the proportion of cloud users that choose paid use gradually decreases until all of them choose to free use and not try to put their privacy information on the cloud. Similarly, the proportion of cloud storage providers that choose positive protection gradually decreases until all of them choose negative

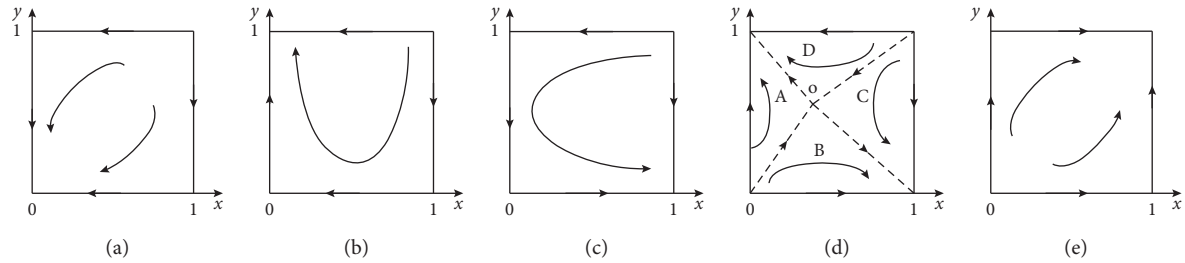

Figure 2: The phase diagrams of the evolutionary game of five scenarios. (a) Scenario 1 (0, 0). (b) Scenario 2 (0, 1). (c) Scenario 3 (1, 0). (d) Scenario 4 (0, 1) and (1, 0). (e) Scenario 5 (1, 1).

Table 6: Stability analysis of the equilibrium point.

Scenarios	Range of values	Equilibrium point	tr$J$	det$J$	State
Scenario 1	$0 < \alpha_0 < C_u/P_u, \alpha_0 < \alpha_1 < C_u + \varepsilon_u - P_u/P_u$ $P_p 0 < \beta_0 < C_p/P_p, \beta_0 < \beta_1 < C_p + \varepsilon_p - P_p/P_p$	(0,0)	−	+	ESS point
		(0,1)	Uncertain	−	Saddle point
		(1,0)	Uncertain	−	Saddle point
		(1,1)	+	+	Unstable point
Scenario 2	$0 < \alpha_0 < C_u/P_u, \alpha_0 < \alpha_1 < C_u + \varepsilon_u - P_u/P_u$ $C_p/P_p < \beta_0 < \beta_1 < C_p + \varepsilon_p - P_p/P_p$	(0,0)	Uncertain	−-	Saddle point
		(0,1)	−-	+	ESS point
		(1,0)	Uncertain	−	Saddle point
		(1,1)	+	+	Unstable point
Scenario 3	$C_u/P_u < \alpha_0 < \alpha_1 < C_u + \varepsilon_u - P_u/P_u$ $0 < \beta_0 < C_p/P_p, \beta_0 < \beta_1 < C_p + \varepsilon_p - P_p/P_p$	(0,0)	Uncertain	−	Saddle point
		(0,1)	Uncertain	−	Saddle point
		(1,0)	−	+	ESS point
		(1,1)	+	+	Unstable point
Scenario 4	$C_u/P_u < \alpha_0 < \alpha_1 < C_u + \varepsilon_u - P_u/P_u$ $C_p/P_p < \beta_0 < \beta_1 < C_p + \varepsilon_p - P_p/P_p$	(0,0)	+	+	Unstable point
		(0,1)	−	+	ESS point
		(1,0)	−	+	ESS point
		(1,1)	+	+	Unstable point
		(x_0, y_0)	Uncertain	−	Saddle point
Scenario 5	$C_u + \varepsilon_u - P_u/P_u < \alpha_0 < \alpha_1$ $C_p + \varepsilon_p - P_p/P_p < \beta_0 < \beta_1$	(0,0)	+	+	Unstable point
		(0,1)	Uncertain	−	Saddle point
		(1,0)	Uncertain	−	Saddle point
		(1,1)	−	+	ESS point

Table 7: Initial model parameters.

Parameter	C_u	C_p	P_u	P_p	ε_u	ε_p
Value	3	2	7	5	9	6

Table 8: Different values of $\alpha_0, \alpha_1, \beta_0, \beta_1$, and ESSs.

	α_1	α_0	β_1	β_0	ESS
Scenario 1	0.3	0.2	0.35	0.3	(0,0)
Scenario 2	0.3	0.2	0.55	0.45	(0,1)
Scenario 3	0.6	0.5	0.55	0.35	(1,0)
Scenario 4	0.6	0.5	0.55	0.45	(0,1) & (1,0)
Scenario 5	0.8	0.75	0.8	0.75	(1,1)

protection. The ESS profile thus becomes "free use, negative protection."

(2) The parameters are set in Table 8 line 2, which satisfy the conditions in Scenario 2. The simulation result is shown in Figure 3(b), which is consistent with scenario 2. That is to say, cloud storage users will converge to 0, and providers will converge to 1 no matter what the initial state is. It means that cloud providers' privacy protection profit growth benefit is greater than the cost, but less than the free-riding

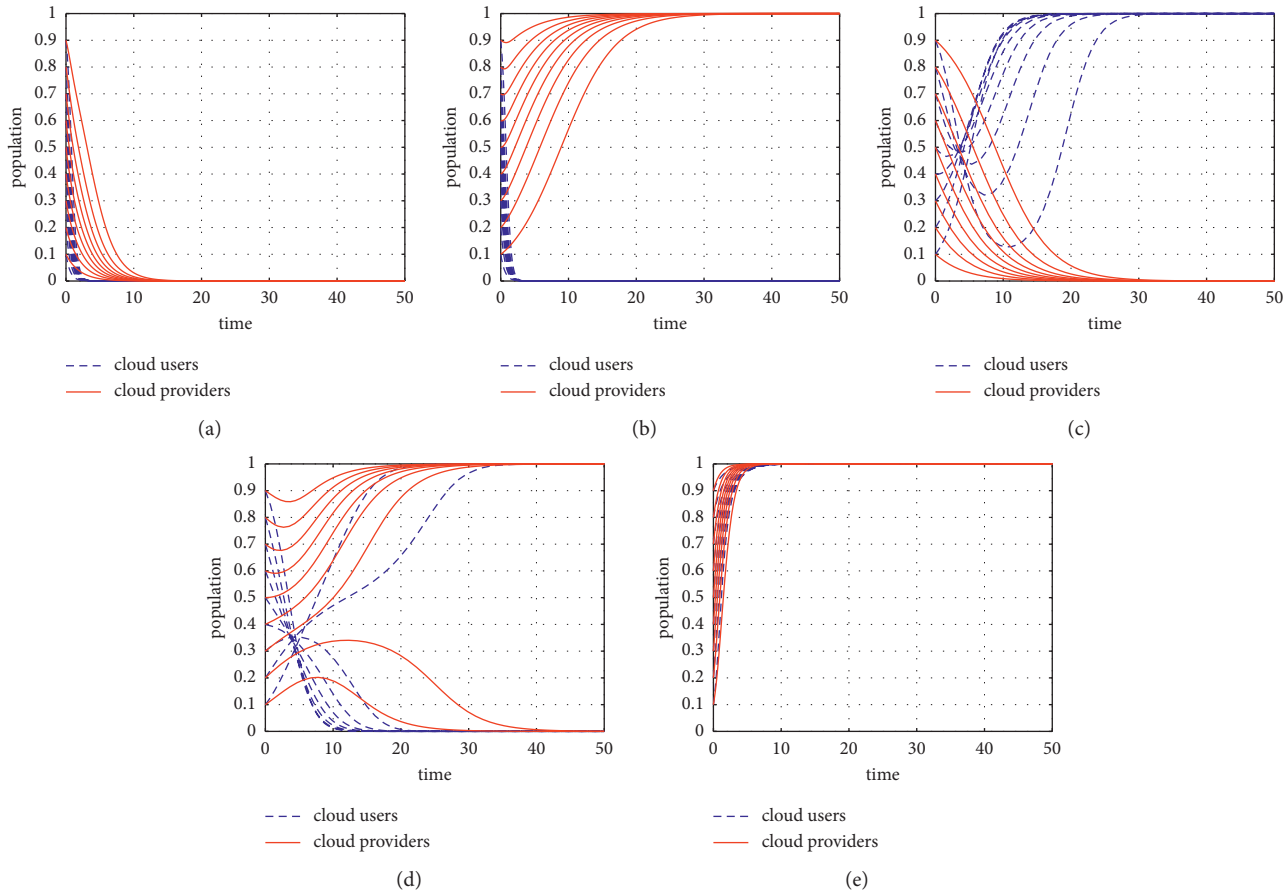

FIGURE 3: The simulation results of evolutionary game. (a) Scenario 1 (0, 0). (b) Scenario 2 (0, 1). (c) Scenario 3 (1, 0). (d) Scenario 4 (0, 1) and (1, 0). (e) Scenario 5 (1, 1).

benefit. Cloud users' privacy protection profit growth benefit is less than the cost, so that they will not choose to pay for usage. Finally, after long-term repeated games, the proportion of cloud users that choose paid use gradually decreases until all of them choose to free use and not try to put their privacy information on the cloud. And the proportion of cloud storage providers that choose positive protection gradually increases until all of them choose positive protection. The ESS profile thus becomes "free use, positive protection."

(3) The parameters are set in Table 8 line 3, which satisfy the conditions in Scenario 3. The simulation result is shown in Figure 3(c), which is consistent with scenario 3. That is to say, the system will converge to (1, 0) no matter what the initial state is. It means that cloud users' privacy protection profit growth benefit is greater than the cost, but less than the free-riding benefit. Thus, cloud providers' privacy protection profit growth benefit is less than the cost, so that they will not choose to pay for usage. Finally, after several times repeated games, the proportion of cloud users that choose paid use gradually increases until all of them choose to pay for use. And the proportion of cloud storage providers that choose positive protection gradually decreases until all of them choose negative protection. The ESS profile thus becomes "paid use, negative protection."

(4) The parameters are set in Table 8 line 4, which satisfy the conditions in Scenario 4. The simulation result is shown in Figure 3(d), which is consistent with scenario 4. the proportion of the system will not converge to a fixed value, but either (0, 1) or (1, 0) relying on the initial state of the system and values of the related variables. It means that the game players aim to obtain extra profits by free riding off other players under this scenario.

(5) The parameters are set in Table 8 line 5, which satisfy the conditions in Scenario 5. The simulation result is shown in Figure 3(e), which is consistent with scenario 5. That is to say, both cloud storage users and providers will converge to 1 no matter what the initial state is. It means that the privacy protection profit growth benefits of cloud storage users and providers are relatively higher than the free-riding benefit, so that they are willing to pay for privacy protection or positive protection. Finally, the proportion of cloud users that choose paid use gradually increases until all of them choose to paid use and believe the safety of the cloud. Similarly, the

proportion of cloud storage providers that choose positive protection gradually increases until all of them choose positive protection. The ESS profile thus becomes "paid use, positive protection."

4.2. Influence of Initial States x_0 and y_0. No matter what the initial state is, the final strategies will not change in Scenarios 1, 2, 3, and 4, because there is only one equilibrium point for each scenario. However, there are two equilibrium points in scenario 4. The simulation result is shown in Figure 3(d). Therefore, in this section, the influence of different initial states was analyzed. First, assume that the parameters and variables $(C_u, C_p, P_u, P_p, \varepsilon_u, \varepsilon_p, \alpha_0, \alpha_1, \beta_0, \beta_1)$ in the section are constant. Second, we set $x_0 = 0.3$, and y_0 sets from 0.1 to 0.9 with a step length of 0.1, wherein, when $y0 = 0.1$ and 0.2, the system will be inclined to (1, 0). When $y_0 = 0.3$, 0.4, 0.5, 0.6, 0.7, 0.8, and 0.9, the system will be inclined to (0, 1). The simulation result can be seen in Figure 4(a). Third, we set $y_0 = 0.3$, and x_0 sets from 0.1 to 0.9 with a step length of 0.1, wherein when $x_0 = 0.1$, 0.2 and 0.3, the system will be inclined to (0, 1). When $x_0 = 0.4$, 0.5, 0.6, 0.7, 0.8, and 0.9, the system will be inclined to (1, 0). The simulation result can be seen in Figure 5(a).

Based on the above analysis, It can be seen that whether the system finally converges to (0, 1) or (1, 0) depends on the initial state of the system. The results show that if the proportion of "paid use" of cloud users or the proportion of "positive protection" of cloud storage providers exceeds a certain threshold, the two game players will change to free riding state, which means that the behavior strategies between cloud users and providers influence each other.

4.3. Influence of Model Parameters

4.3.1. Influence of Basic Storage Profits (P_u, P_p). The influence of the basic storage profits (P_u, P_p) on cloud users and providers is analyzed in this section. First, P_u are set as 6, 7, and 8. Second, the other parameters are consistent with the base values in Table 7. The privacy protection profit growth coefficients are set as $\alpha_1 = 0.7, \alpha_0 = 0.2, \beta_1 = 0.8, \beta_0 = 0.3$. Third, the initial state is assumed to be (0.6, 0.4). The simulation result is shown in Figure 6(a). With the increase of P_u, cloud users and providers change the strategy of (0, 0) and gradually evolve to the strategy of (1, 1).

Similarly, when we set P_p as 4, 5, and 6, the same change comes with the increase of P_p, and both players change their strategy from (0, 0) to (1) and (1). The simulation result is shown in Figure 6(b).

4.3.2. Influence of Costs of Privacy Protection Service (C_u, C_p). In this section, the influence of the privacy protection service costs (C_u, C_p) on cloud users and providers is analyzed. First, C_u are set as 2, 3, and 4. Second, the remnant parameters are consistent in Section 4.3.1. The simulation result is shown in Figure 7(a). When the value of C_u increases, cloud users and providers eventually evolve to the strategy of (0, 0). Besides, when C_p are set as 4, 5, and 6, with the increase of P_p, both players change their strategy from (1, 1) to (0, 0). The simulation result is shown in Figure 7(b).

4.3.3. Influence of Profits from Free Riding $(\varepsilon_u, \varepsilon_p)$. Next, the influence of profits from free riding was analyzed. By setting the same values of other parameters in Section 4.3.1, ε_u is assumed as 8, 9, and 10. The simulation result is shown in Figure 8(a). When the profits from free riding are larger, the less the time that cloud users and providers can evolve to (0, 0). Simultaneously, when we set ε_p as 5, .6, and 7, the simulation result is shown in Figure 8(b). It can be found that the larger ε_p is, the much more time the two players spend getting to (1, 1). Moreover, when the value of ε_p reached to a certain value, their strategy will change (1, 1) to (0, 0).

4.3.4. Influence of Privacy Protection Profit Growth Coefficient $(\alpha_1, \alpha_0, \beta_1, \beta_0)$. Finally, the influence of the values of privacy protection profit growth coefficients of both game players was analyzed. By setting the same values of other parameters in Section 4.3.1, the values of α_0 increase from 0.1 to 0.3 with a step length of 0.1, and the values of α_1 increase from 0.6 to 0.8 with a step length of 0.1. From the simulation results, as shown in Figure 9(a), It can be seen that, with the increase of coefficients, the rate of evolution converging to 0 decreases gradually. When it reached to a certain value, they will evolve from 0 to 1. Similarly, assume that the values of β_0 increase from 0.2 to 0.4 with a step length of 0.1, and the values of β_1 increase from 0.7 to 0.9 with a step length of 0.1. The simulation result is shown in Figure 9(b). With the increases of β_0 and β_1, they will evolve from 0 to 1 and even use less time to the final result.

4.4. Suggestions. According to the above analysis, the following suggestions for long-term cloud storage management are meant to help both parties progress toward sustainability:

(a) Increase the profit growth coefficients for inputs that protect privacy. The sooner customers and cloud storage service providers evolve toward privacy protection sustainability, the better the income growth coefficient from privacy protection for both sides. The following are some examples of particular measures that could be taken: first, improving the privacy protection's technological strength: government incentives for cloud storage privacy protection technology development can be used to boost profits and cut costs. Through policy assistance and financial incentives, the government can encourage cloud storage service providers to pursue privacy protection technology research and development. Second, raising awareness of the need of protecting user privacy: to improve users' attention to personal privacy, increase the promotion of public awareness about personal privacy protection across numerous channels.

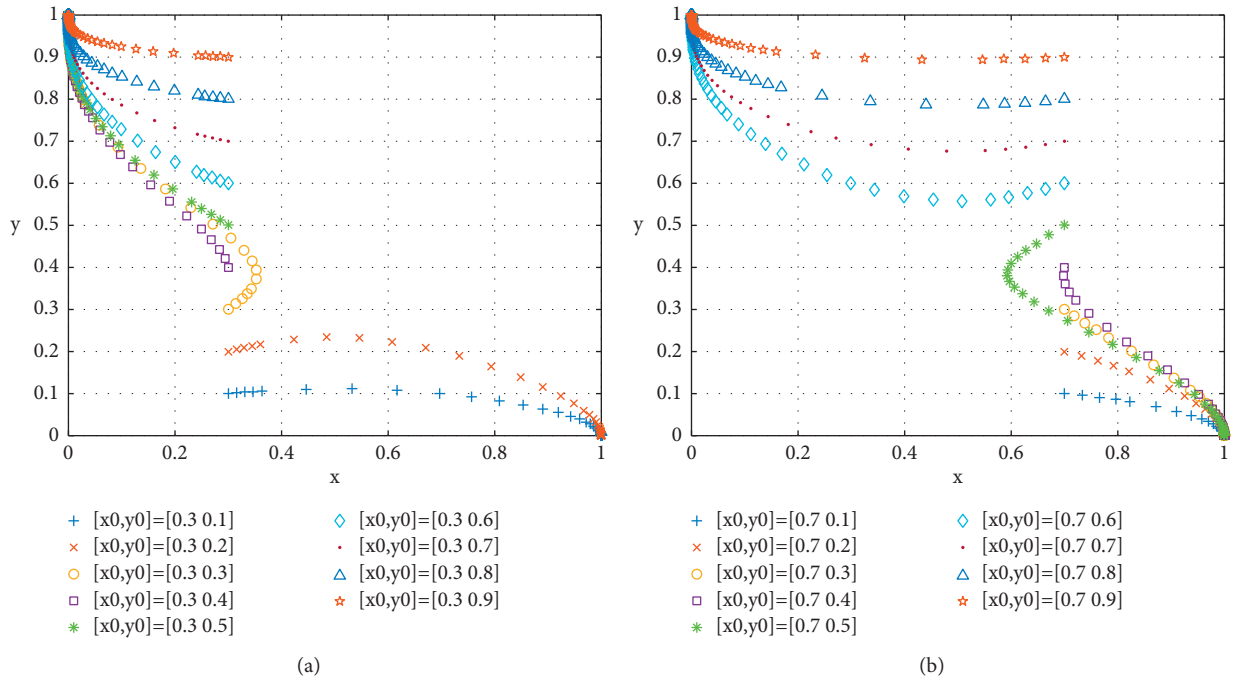

FIGURE 4: Influences of the changes in the initial value y_0 on the evolutionary result, where (a) $x_0 = 0.3$ and (b) $x_0 = 0.5$.

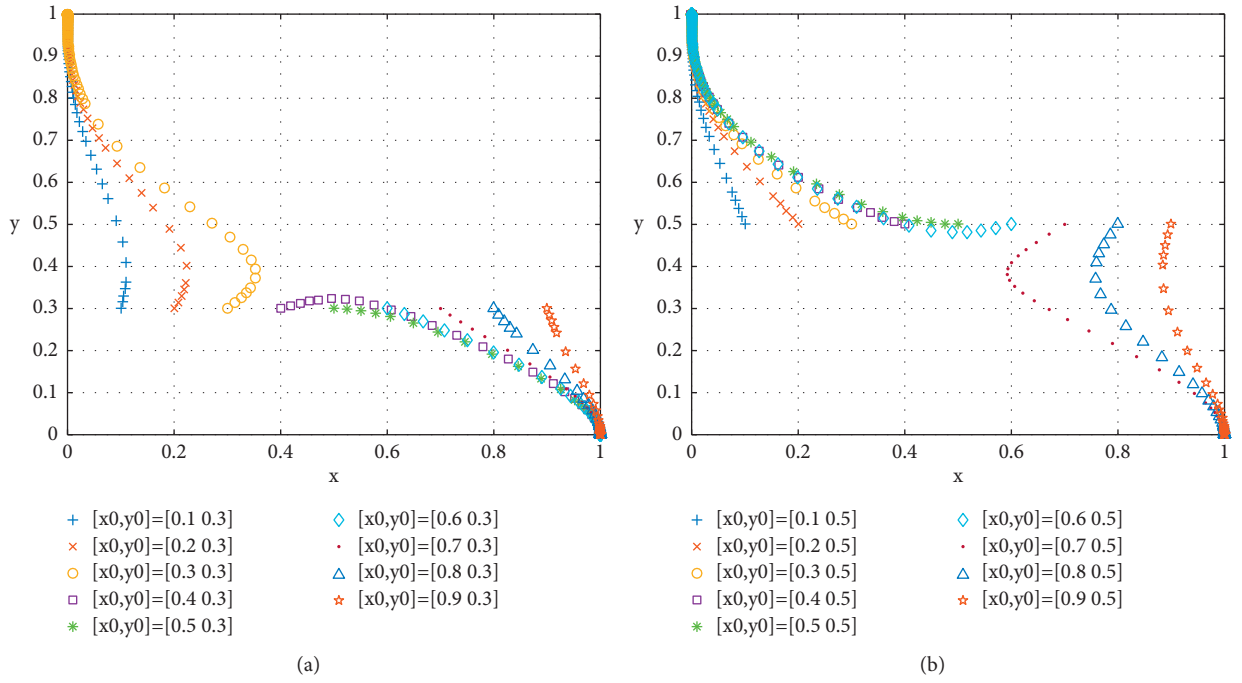

FIGURE 5: Influences of the changes in the initial value x_0 on the evolutionary result, where (a) $y_0 = 0.3$ and (b) $y_0 = 0.7$.

(b) Cut down privacy protection investments of users and cloud storage service providers. The likelihood that both parties will choose to treat privacy investment positively decreases as the cost rises. When the investment costs are too high, both parties are more likely to opt out (free use, negative protection). Reducing the investment cost of privacy protection can also eliminate speculation on both sides and maintain the sustainability of personal cloud storage.

(c) Increase penalties and provide incentives. An important reason for both parties to choose between free use or negative protection is that both parties do

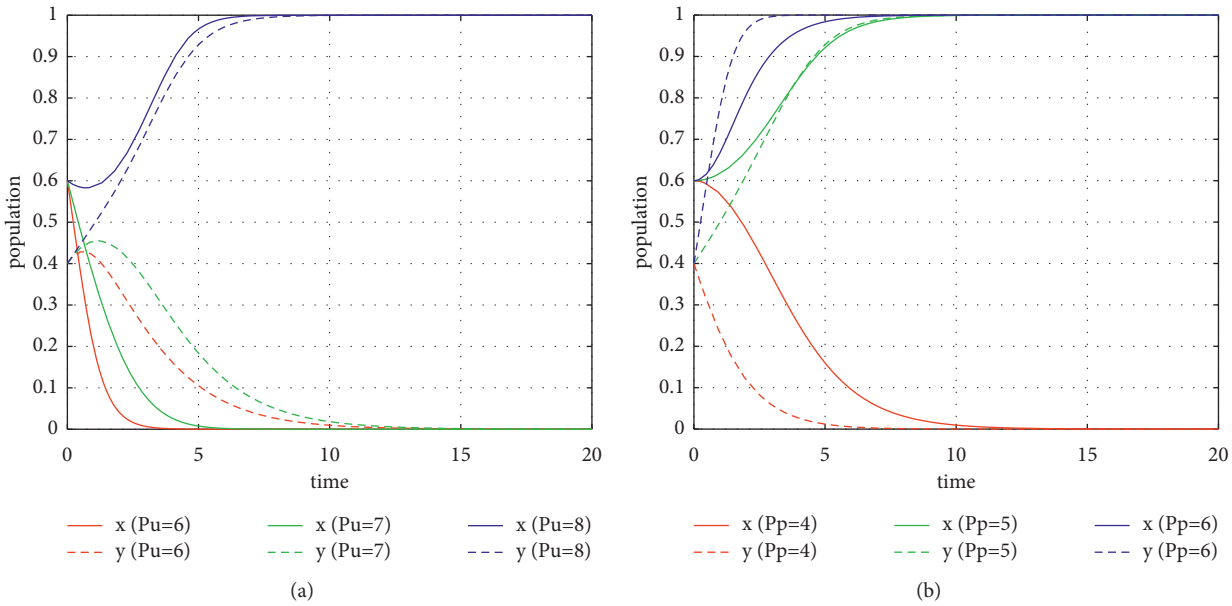

Figure 6: Influences of the basic profit when using cloud storage. (a) Influence different values of P_u. (b) Influence different values of P_p.

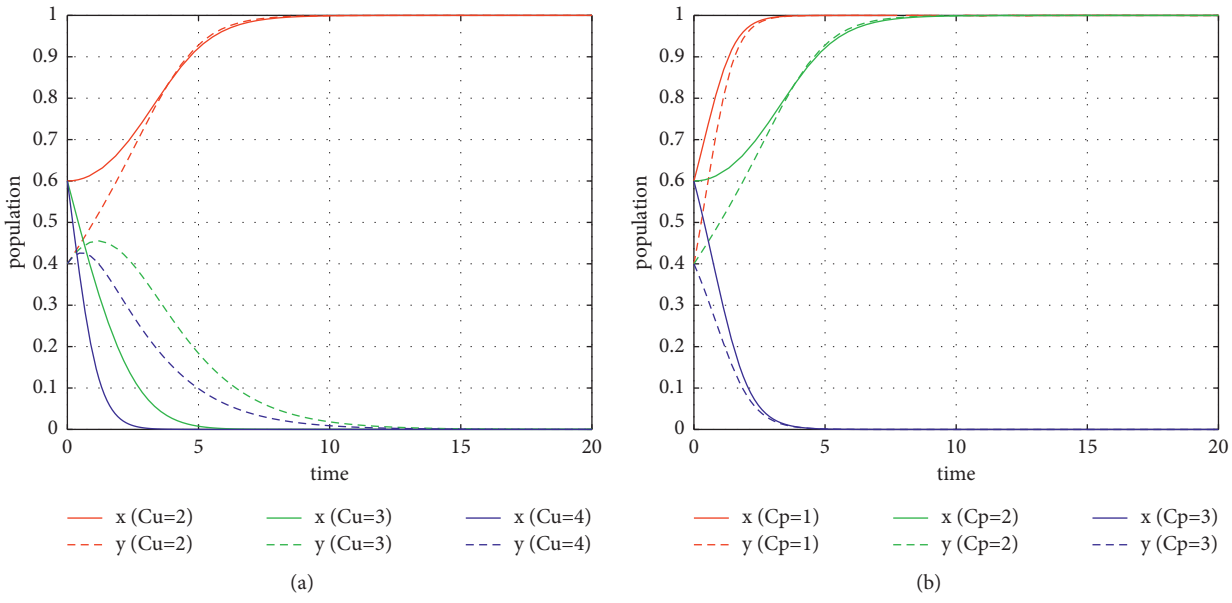

Figure 7: Influences of the privacy protection costs. (a) Influence different values of C_u. (b) Influence different values of C_p.

not have to pay for their own free-rider behavior. As the revenue from free-riding increases, the probability that both parties will choose to be aggressive about their privacy protection investment decreases. Effective incentives can be created through the government to increase subsidies and fines for users and cloud storage providers. The government can reward and support those cloud storage service providers who continuously use privacy protection input to enhance privacy security awareness.

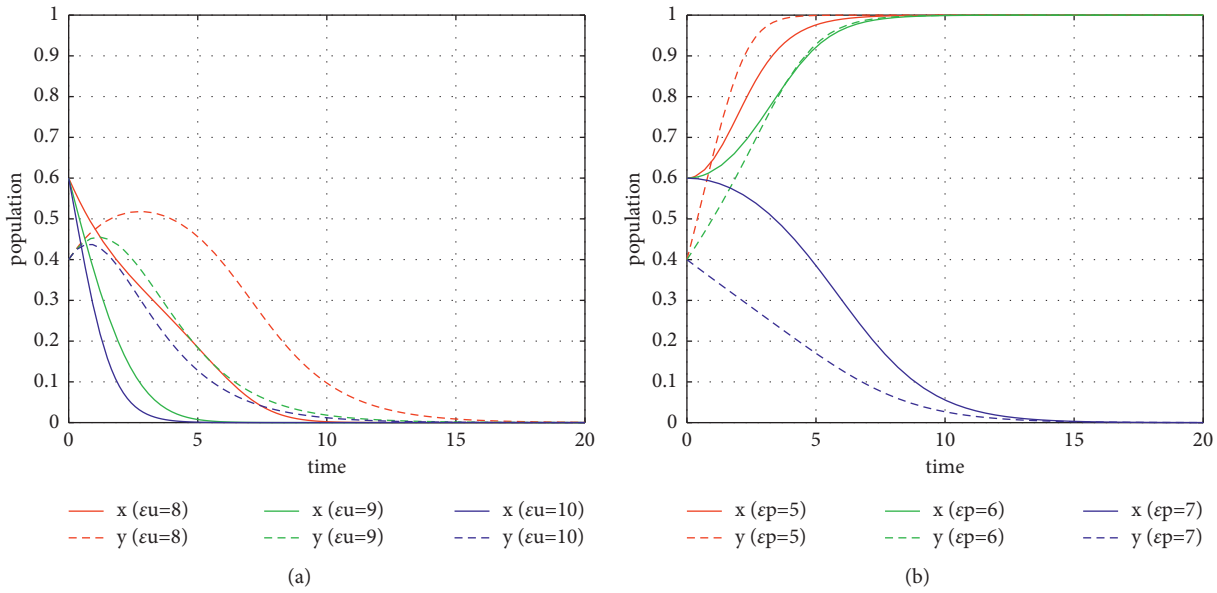

Figure 8: Influences of profits of free riding. (a) Influence different values of ε_u. (b) Influence different values of ε_p.

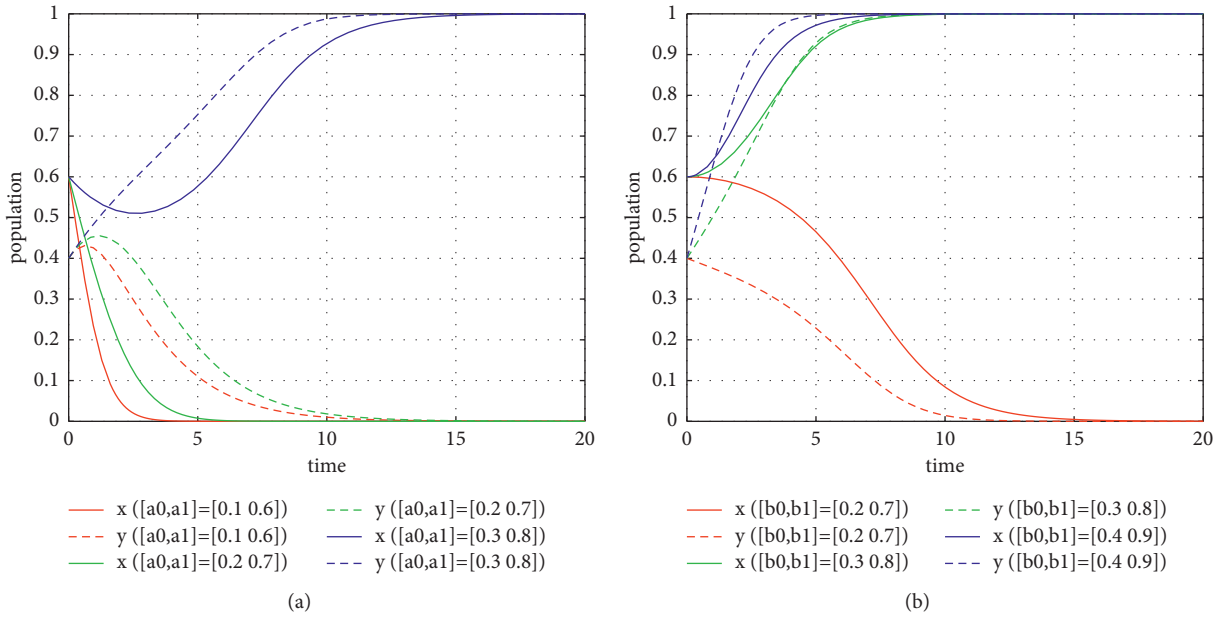

Figure 9: Influences of privacy protection profit growth coefficients. (a) Influence different values of a_0 and a_1. (b) Influence different values of b_0 and b_1.

5. Conclusions

In this paper, the privacy protection investment problem of cloud storage services is regarded as an economic problem, regarding cloud storage service providers and cloud storage users as bounded rational game parties with certain learning capabilities; by introducing the privacy protection profit growth coefficient, an evolutionary game model of cloud storage service participants in consideration of privacy protection is built during the evolution process. By analyzing the evolutionary stability strategy of the evolutionary game model, the key factors affecting the evolution of cloud storage service providers and cloud storage users' payment behavior are investigated. Additionally, simulation experiments are conducted to verify the modeling analyses and demonstrate the effects of game parameters. The study finds the following:

(a) The growth coefficient of privacy protection profit during the sustainable use of cloud storage services, privacy protection investment costs, basic usage profit, and free-riding profits are important influencing factors in the choice of game strategy.

(b) As the parameters for basic cloud storage service profits and privacy protection profit growth coefficient rise, the likelihood of users paying for use rises, as does the likelihood of cloud storage service providers actively protecting user information, both of which have a positive effect on the system's evolution. The probability of users paying for use will increase as the parameters for privacy protection investment cost and free-riding profit decrease, as will the probability of cloud storage service providers actively protecting user information, both of which have a positive effect on the system's evolution.

(c) Profit growth coefficients are essential elements that determine the game system's development direction. When the profit growth coefficient is very small, users will not choose to pay, and cloud storage service providers will not choose to actively protect user information. The profit growth coefficients influence the profits from privacy protection investment, which further influence their strategy choice of free-riding, paid use, or positive protection. As the profit growth coefficient increases, the two parties of the game will invest in the development of privacy protection with a higher probability.

In addition, this study also has some limitations, which provide directions for future research. First, in terms of simulation data, there is a lack of actual data based on real cases for simulation. The next step will be based on the actual data of the real case simulation to make the research conclusions more reliable. Second, the variable design of this article is based on the scenario assumption. In reality, there are inevitably other variables that are not taken into consideration. More variables will be included in the research in the future. Third, in addition to the participation of both the service provider and the user, the privacy protection issues in the sustainable use of cloud storage services will also involve the supervision and restriction of third-party regulatory authorities. The future studies will address cloud storage services that consider privacy protection. Three-party game analysis is carried out during the continuous use of the cloud storage service, and a more systematic and comprehensive analysis is carried out for the sustainable development of cloud storage services.

Despite these limitations in this study, our research results still have important contributions in both theory and practice. Theoretically, our research enriches the privacy protection behavior theory under the cloud storage service and provides the evolutionary game model of privacy protection investment strategies to analyze the decision and broaden our understanding of relationship between behavior and attitude of the privacy protection investment of users and providers. Practically, according to our research results, proper suggestions to better promote the sustainable development of cloud storage service are provided.

Data Availability

The numerical simulation data used to support the findings of this study are included within the article.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

References

[1] iiMedia, "Research report on the current situation of Chinese individual web disk market and the layout of leading enterprises in the first half of 2020," 2021, http://Report.iimedia.cn/repo1-0/39252.html.

[2] X. Li, "Decision making of optimal investment in information security for complementary enterprises based on game theory," *Technology Analysis & Strategic Management*, vol. 33, no. 7, pp. 755–769, 2020.

[3] E. Kalai, E. Lehrer, and S. Center, *Rational Learning Leads to Nash Equilibrium*, New York University, New York, NY, USA, 1991.

[4] R. Aumann and A. Brandenburger, "Epistemic conditions for Nash equilibrium," *Econometrica*, vol. 63, no. 5, p. 1161, 1995.

[5] P. Yang, N. Xiong, and J. Ren, "Data security and privacy protection for cloud storage: a survey," *IEEE Access*, vol. 8, pp. 131723–131740, 2020.

[6] C. Yang, L. Tan, N. Shi, B. Xu, Y. Cao, and K. Yu, "AuthPrivacyChain: a blockchain-based access control framework with privacy protection in cloud," *IEEE Access*, vol. 8, pp. 70604–70615, 2020.

[7] S. Wang, X. Wang, and Y. Zhang, "A secure cloud storage framework with access control based on blockchain," *IEEE Access*, vol. 7, pp. 112713–112725, 2019.

[8] Y. Zhang, X. Chen, J. Li, D. S. Wong, H. Li, and I. You, "Ensuring attribute privacy protection and fast decryption for outsourced data security in mobile cloud computing," *Information Sciences*, vol. 379, pp. 42–61, 2017.

[9] K. V. U. Maheswari and D. D. Cheelu, "Attribute-based privacy-preserving data sharing for dynamic groups in cloud computing," *International Journal of Scientific Research in*

Computer Science, Engineering and Information Technology, pp. 585–590, 2021.

[10] S. K. Pasupuleti, "Privacy-preserving public auditing and data dynamics for secure cloud storage based on exact regenerated code," *International Journal of Cloud Applications and Computing*, vol. 9, no. 4, pp. 1–20, 2019.

[11] J. R. Gudeme, S. Pasupuleti, and R. Kandukuri, "Certificateless privacy preserving public auditing for dynamic shared data with group user revocation in cloud storage," *Journal of Parallel and Distributed Computing*, vol. 156, pp. 163–175, 2021.

[12] X. Zhang, J. Zhao, C. Xu, H. Li, H. Wang, and Y. Zhang, "CIPPPA: conditional identity privacy-preserving public auditing for cloud-based WBANs against malicious auditors," *IEEE Transactions on Cloud Computing*, vol. 9, no. 4, pp. 1362–1375, 2021.

[13] D. Alsmadi and V. Prybutok, "Sharing and storage behavior via cloud computing: security and privacy in research and practice," *Computers in Human Behavior*, vol. 85, pp. 218–226, 2018.

[14] S. G. Abdulaziz and N. B. M. Yasin, "AN exploratory study to understand the critical factors affecting the decision to adopt cloud computing IN SAUDI hospitals," *PONTE International Scientific Researchs Journal*, vol. 75, no. 6, 2019.

[15] A. Fan, Q. Wu, X. Yan, X. Lu, Y. Ma, and X. Xiao, "Research on influencing factors of personal information disclosure intention of social media in China," *Data and Information Management*, vol. 5, no. 1, pp. 195–207, 2020.

[16] J. P. G. Gashami, Y. Chang, J. J. Rho, and M.-C. Park, "Privacy concerns and benefits in SaaS adoption by individual users," *Information Development*, vol. 32, no. 4, pp. 837–852, 2016.

[17] M. M. Mariani, M. Ek Styven, and F. Teulon, "Explaining the intention to use digital personal data stores: an empirical study," *Technological Forecasting and Social Change*, vol. 166, Article ID 120657, 2021.

[18] Y. Li, K.-C. Chang, and J. Wang, "Self-determination and perceived information control in cloud storage service," *Journal of Computer Information Systems*, vol. 60, no. 2, pp. 113–123, 2020.

[19] A. E. Widjaja, J. V. Chen, B. M. Sukoco, and Q.-A. Ha, "Understanding users' willingness to put their personal information on the personal cloud-based storage applications: an empirical study," *Computers in Human Behavior*, vol. 91, pp. 167–185, 2019.

[20] S.-T. Park and M.-R. Oh, "An empirical study on the influential factors affecting continuous usage of mobile cloud service," *Cluster Computing*, vol. 22, no. S1, pp. 1873–1887, 2017.

[21] G. Zhu, H. Liu, and M. Feng, "Sustainability of information security investment in online social networks: an evolutionary game-theoretic approach," *Mathematics*, vol. 6, no. 10, p. 177, 2018.

[22] R. C. Lewontin, "Evolution and the theory of games," *Journal of Theoretical Biology*, vol. 1, no. 3, pp. 382–403, 1961.

[23] B. Wu, J. Cheng, and Y. Qi, "Tripartite evolutionary game analysis for "Deceive acquaintances" behavior of e-commerce platforms in cooperative supervision," *Physica A: Statistical Mechanics and Its Applications*, vol. 550, Article ID 123892, 2020.

[24] Y. Su, "Multi-agent evolutionary game in the recycling utilization of construction waste," *The Science of the Total Environment*, vol. 738, Article ID 139826, 2020.

[25] G. Zhu, G. Pan, and W. Zhang, "Evolutionary game theoretic analysis of low carbon investment in supply chains under governmental subsidies," *International Journal of Environmental Research and Public Health*, vol. 15, no. 11, p. 2465, 2018.

[26] Y. Sun, F. Lin, and N. Zhang, "A security mechanism based on evolutionary game in fog computing," *Saudi Journal of Biological Sciences*, vol. 25, no. 2, pp. 237–241, 2018.

[27] H. Hu, Y. Liu, C. Chen, H. Zhang, and Y. Liu, "Optimal decision making approach for cyber security defense using evolutionary game," *IEEE Transactions on Network and Service Management*, vol. 17, no. 3, pp. 1683–1700, 2020.

[28] 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.

[29] J. X. Sun, F. C. Liao, L. Q. Tian, and T. G. Ji, "User behavior decision model based on game theory," *Computer Engineering*, vol. 9, pp. 159–161, 2008.

[30] Z. Y. Wang, X. Wang, X. Su, Y. X. Sheng, and S. L. Ge, "Dynamic game of cloud computing adoption for the small and medium-sized enterprises under the influence of data security from the perspective of information asymmetry," *Modern Manufacturing Engineering*, vol. 6, pp. 40–46, 2016.

[31] H. P. Cheng, W. Xiao, and Y. Q. Cheng, "Evolutionary game analysis on user adoption behavior of personal cloud service," *Research on Library Science*, vol. 5, pp. 51–57, 2018.

[32] D. Friedman, "On economic applications of evolutionary game theory," *Journal of Evolutionary Economics*, vol. 8, no. 1, pp. 15–43, 1998.