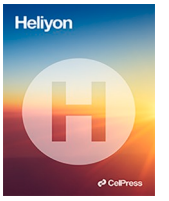
Heliyon 10 (2024) e36391

Contents lists available at ScienceDirect

Heliyon

journal homepage: www.cell.com/heliyon



Research article

# Research on platform data security governance strategy based on three-party evolutionary game

Zhen Tian, Meng Han, Chuchu Jiang *

*Zhengzhou University of Light Industry, School of Economics and Management, China*

ARTICLE INFO

*Keywords:*
Digital security governance
Digital ecology
Evolutionary game model
Simulation analysis

ABSTRACT

With the implementation of the overall national security concept, data security governance rises to a new strategic height. In this paper, for the incomplete status quo of digital service platforms, third-party testing organizations and government regulators in the construction of digital security, an evolutionary game model based on the above three parties is constructed. The model examines the strategic decision-making process, behavioral influences, and evolutionary stability of the three players, and is simulated and analyzed using MATLAB. The results show that the evolutionary system will reach the ideal stable state $E(1,1,1)$, which corresponds to the combination of strategies: providing high-quality products, refusing to rent-seeking, and strict regulation. In order to guide the evolving system to reach the ideal stable state, this study puts forward some policy recommendations in terms of establishing a data security assessment mechanism, collaborative technology governance, and optimizing the governance architecture.

## 1. Introduction

On June 10, 2021, the Twenty-ninth Meeting of the Standing Committee of the Thirteenth National People's Congress passed the Data Security Law of the People's Republic of China, which came into effect on September 1, 2021. According to the definition of Article 3 of the Data Security Law, data security refers to the adoption of necessary measures to ensure that data are in a state of effective protection and lawful utilization, as well as having the ability to guarantee a continuous state of security [1]. With the accelerated advancement of the digital reform process of platform enterprises, it is required that platform enterprises need to pay attention to the construction of data security [2]. Data security governance is an effective guarantee for the construction of data security, and is an important means to ensure that data are effectively protected, legally utilized, and continuously secure [3].

The twenty-sixth meeting of the Central Deep Reform Commission on June 22, 2022 clearly pointed out that "it is necessary to improve the mechanism of market-oriented allocation of data elements, and promote the classification and grading of public data, enterprise data, and personal data to confirm the right to authorize the use of public data" [4]. This indicates that enterprise data is one of the important sources of the data factor market. Enterprise data is business data generated and controlled by enterprises in the process of production, operation, and management that does not involve personal information and public interest. Enterprises can utilize internal data while integrating external data for calculation and analysis to support intelligent decision-making and promote innovation, which has obvious economic value [5]. Usually, the third-party data security assessment and certification is considered as the main hand to improve the data security governance ability, and this technical function is entrusted to the third-party testing

* Corresponding author.
*E-mail address:* chuu313@163.com (C. Jiang).

https://doi.org/10.1016/j.heliyon.2024.e36391
Received 6 October 2023; Received in revised form 14 August 2024; Accepted 14 August 2024
Available online 16 August 2024

organization, however, the testing organization, as a private enterprise, is susceptible to "rent-seeking" behaviors under the pursuit of economic interests, which can easily lead to enterprise data leakage, misuse and modification and other security problems [6,7]. Visible, data security governance is particularly important in maintaining enterprise data security, which is an important part of promoting the healthy development of digital ecology.

Digital security governance refers to the strategic consideration of enterprise security throughout the enterprise and digital environment [8,9]. In the digital era, enterprises need to consider security at the strategic level to achieve corporate sustainability and protection [10,11]. Qingling Qin et al. [12] further extend the concept of data security governance in the new social form of "human-machine-object" ternary integration. Qin et al. further expand the connotation of data security governance in the new social form of "human-machine-object" ternary integration. Some scholars consider the strategic consideration of security in the digital environment as digital security governance [13–15], and propose that digital security governance (DSG) aims to maintain the confidentiality, integrity, and availability of data assets [16], and to ensure that the goals are achieved and security risks are managed appropriately to cope with increasing cyber-attacks [15,17]. The implementation of data security governance and the establishment of strong safeguards as well as dynamic and constant security protection mechanisms can achieve the proper protection and secure use of sensitive data as well as the ability to have a continuous state of security and protection of organizational assets [18].

In terms of the application of data security governance, some scholars have explored the transformative impact of data security governance on a variety of aspects such as public health, higher education [19], government information assets [20,21], and supply chain finance [22], which can enhance their risk management capabilities, protect privacy, and promote open information sharing and service improvement. Some scholars have also conducted theoretical or empirical studies on cross-border data flow regulation, personal privacy protection, and data openness and sharing [23–25], which are closely interconnected with each other. Both cross-border and open sharing of data involve privacy protection issues, and a healthy and effective data security governance framework needs to strike a balance between these aspects to ensure the secure flow of data and protect individual privacy, while promoting openness and sharing of data to promote innovation and sustainable development of society.

At the same time, private (often non-European) companies are playing an increasingly important role in the collaborative governance of digital security, as the corporate perspective focused on in this paper suggests [26]. In turn, whether public actors rely on private firms in the provision of digital security depends on how they make capacity control trade-offs [27]. Given their technical expertise and control over digital infrastructure, public actors often need the capabilities of private intermediaries to address digital security challenges [28]. In recent years, third-party testing as a complement to government regulation has frequently been the subject of misbehavior [29,30]. Private players have strong economic incentives to try to influence these beliefs, which we conceptualize as "desirable business forces" [31]. In practical implementation, limited government regulation, information asymmetry, and economic interests may induce manufacturers and third-party verifiers to manipulate data and jeopardize data security [32,33].

However, on the whole, existing studies pay less attention to the exploration of how the governance subject can play the governance utility issue, which leads to insufficient systematicity and depth of research and weakens the effectiveness and sustainability of data security assurance [7]. Therefore, in order to explore the evolution of the behavioral and strategic choices of each participating subject in data security governance, this paper constructs a tripartite evolutionary game model based on the evolutionary game theory, analyzes the stability points of the model and applies MATLAB numerical simulation simulation to validate the gaming behaviors and final strategic choices of the tripartite gaming subjects in order to provide some theoretical and practical insights into the mechanism of promoting the multifarious collaborative data security governance and to provide some theoretical and practical insights into the mechanism of promoting the multifarious collaborative data security governance and its effectiveness. In order to provide some theoretical and empirical references for exploring the mechanism of multivariate collaborative data security governance.

## 2. Construction of evolutionary game model of DSG

### *2.1. Theoretical framework*

#### *2.1.1. Evolutionary game agents*

In this study, the data security governance strategy based on the tripartite evolutionary game involves three core subjects: digital service platforms, third-party testing organizations, and government regulators. These subjects play different roles in the process of data security governance, and the game and cooperation among them have a crucial impact on enhancing the effectiveness of data security governance.

(1) Digital service platforms

Digital service platforms are directly responsible for data security governance. They are responsible for designing, developing, providing and selling digital products, and their level of data security directly affects users' data security and privacy protection. Digital service platforms need to assume social responsibility for data security governance while pursuing economic benefits. When the market encounters security threats such as privacy leakage and data theft, these behaviors may not only disrupt the market order, but also lead to the loss of platform users and the reduction of transaction volume, thus further affecting the profitability of the platform. Therefore, from the perspective of commercial interests, platform companies have an incentive to maintain the health and security of the online environment to ensure the vitality of the market and enhance the ability to transform the commercial value of data. In short, safeguarding data security is both a responsibility and a strategy to enhance competitiveness for platform enterprises [34]. They need to improve the level of data security through technological innovation, process optimization, etc., and at the same time, they also need

to play a synergistic effect with other subjects to jointly build a data security governance system.

(2) Third-party testing organizations

The third-party testing organizations refer to the third-party supervision and inspection organization that is outside the interests of buying and selling, follows the principle of fairness and impartiality, and carries out commodity inspection activities in accordance with the relevant laws and regulations, industry standards or contracts [30]. As an independent testing and evaluation organization, third-party testing organizations are responsible for testing and evaluating the data security level of digital service platforms. They provide objective and accurate evaluation bases for data security governance by virtue of their specialized technical capabilities and impartial stance. The existence of third-party testing organizations helps promote the self-discipline and enhancement of digital service platforms in terms of data security, and at the same time provides government regulators with an effective means of supervision.

(3) Government regulators

Government regulators play a guiding and regulatory role in data security governance. The main factors affecting the choice of strategy of the game subjects are the level of penalties imposed by government regulators on third-party testing organizations and the cost of regulation by government regulators [35]. Government regulators are responsible for formulating data security-related policies, regulations, and standards and norms to provide legal protection and policy support for data security governance. Government regulators also need to supervise and guide third-party testing organizations and digital service platforms to ensure that they fulfill their responsibilities and obligations for data security governance. At the same time, government regulators also need to strengthen cooperation and communication with other countries and regions to jointly address global challenges in data security governance.

In summary, digital service platforms, third-party testing organizations and government regulators each play an important role in data security governance. The game and cooperation among them is an important part of data security governance strategy research. Through in-depth analysis of the behavioral characteristics and interactive relationships of these subjects, it can provide strong theoretical support and practical guidance for the construction of effective data security governance strategies.

### *2.1.2. Analysis of game relationships*

In this study, the data security governance strategy based on the tripartite evolutionary game involves three main game subjects: digital service platforms, third-party testing organizations, and government regulators. These three subjects play different roles in the process of data security governance, and jointly influence the effect of data security governance through the game relationship between them.

The digital service platform, as the directly responsible body of data security governance, aims to maximize economic benefits while ensuring that data security complies with relevant regulations and standards. In the process of production and operation, enterprises need to weigh the relationship between data security investment and economic benefits, and formulate a reasonable data security governance strategy. In the game with third-party testing organizations, enterprises need to accept testing and make improvements based on the test results to improve their data security level. In the game with government regulators, enterprises need to comply with relevant regulations and accept government supervision and penalties, but also through communication and cooperation with the government for more policy support and market opportunities.

As an independent testing and certification organization, the main responsibility of the third-party testing organization is to objectively and impartially assess and supervise the data security measures of digital service platforms. Between digital service platforms and government regulators, the third-party testing organization plays the role of a bridge and a link. On the one hand, it needs to report the testing results to the government regulator to provide a scientific basis for government decision-making; on the other hand, it also needs to provide improvement suggestions to the digital service platform to help it improve its data security level.

The government regulator plays the role of supervision and guidance in data security governance. It is responsible for formulating data security regulations and standards, regulating and penalizing digital service platforms, and also can guide enterprises to strengthen data security construction through policy incentives. In the game with third-party testing organizations, the government needs to rely on their test results to assess the industry's data security status and formulate targeted regulatory measures. In the game with digital service platforms, the government needs to ensure that enterprises comply with regulations through law enforcement and supervision, and at the same time pay attention to the reasonable demands of enterprises to promote the benign development of data security governance.

Different from traditional game theory, evolutionary game theory assumes that human beings are limitedly rational and usually reach game equilibrium through trial and error. Due to the asymmetry or incompleteness of information, in order to obtain the maximum benefit, the subject will waver in different strategies, and its strategy selection is very easy to be influenced by the surrounding subjects or game parties, and there is a dynamic adjustment and imitation of the process of others. These three parties are driven by interests, and will eventually make a scientific evolutionary game strategy that is fit for purpose and operability [36]. Combined with practical research, the evolution of data security governance process requires the participation of digital service platforms, third-party testing organizations, government regulators, the main body of the interests of the impossibility of complete rationality, the choice of its strategy affects each other, is the behavior of all parties to adjust each other's dynamic evolution under certain rules [37]. Therefore, this paper analyzes the dynamic game process of data security governance using evolutionary game theory and numerical simulation. By constructing a tripartite evolutionary game model of digital service platforms, third-party testing organizations, and government regulators, it determines the evolutionary and stabilization strategies of the three parties to reach the

ideal state in different contexts, and provides decision-making references for creating a good digital ecology.

The game relationship between the three parties of data security governance constructed in this paper is shown in Fig. 1.

### 2.2. Model construction

#### 2.2.1. Behavioral strategies

From the perspective of digital service platforms, digital service platforms, as a party to the game, are faced with the choice of two behavioral strategies: "providing high-quality digital products" or "providing low-quality digital products". "Providing high-quality digital products" means that enterprises will follow the standards and regulations of data security governance, invest the necessary resources to ensure the quality and safety of digital products, and invest higher costs in product provision. "Providing low-quality digital products" may bring short-term economic benefits, but in the long run may face legal risks and reputational damage. The strategic choices of digital service platforms are affected by a variety of factors, such as the strength of government regulation, the cost of non-compliance, and the state of competition in the market [38].

Considering from the perspective of third-party testing organizations, testing organizations, as a party to the game, are faced with two behavioral strategy choices: "refusing to rent-seeking" or "intending to rent-seeking". "Refuse to rent-seeking" means that the organization will strictly follow the standards to ensure the accuracy and reliability of the data. It provides government regulators with a strong basis for supervision, thus effectively curbing irregularities in digital service platforms and promoting fair competition in the market. At the same time, this will help reduce data security risks and minimize legal disputes and economic losses caused by data leakage or tampering. "Intending to rent-seeking" means that the results of third-party testing may be tempted by the rent-seeking of digital service platforms and deviate from an impartial stance. This behavior will undermine the impartiality and effectiveness of data security governance, making the test results lose objectivity and accuracy. This will lead to the government regulatory authorities not being able to accurately grasp the security status of digital product data, which in turn makes it difficult to effectively supervise and penalize violations, thus weakening the effectiveness of the entire regulatory system.

From the perspective of government regulators, as the other side of the game, their strategy choices include "strict regulation" and "loose regulation". "Strict regulation" means that the government will increase penalties for non-compliance and improve data security standards, while "loose regulation" may lead to regulatory gaps, allowing unscrupulous companies and organizations to take advantage of the situation.

In the three-party game model, the strategic choices of each participant are influenced by each other. The strategic choices of digital service platforms will affect the business volume and impartiality of third-party testing organizations; the strategic choices of third-party testing organizations will affect the effect of government regulation and public confidence in data security; and the strategic choices of government regulators will directly affect the series of behaviors of digital service platforms and third-party testing organizations in the process of data security governance.

#### 2.2.2. Model hypothesis

**Assumption 1**. All subjects of interest are finitely rational and their strategy choices evolve over time, eventually converging to a steady state of optimal strategies.

**Assumption 2**. Probability assumption. The probability that a digital service platform provides high-quality digital products is $x$, and the probability that it provides low-quality digital products is $1-x$; the probability that a third-party testing organization refuses to rent-seeking is $y$, and the probability that it intends to rent-seeking is $1-y$; and the probability that a government regulator strictly regulates is $z$, and the probability that it loosely regulates is $1-z$, where $0 \leq x,y,z \leq 1$.

**Assumption 3**. The daily revenue and cost of normal operation of the digital service platform are *RM* and *CM* respectively. If the digital service platform consciously fulfills its governance responsibilities, assumes social responsibility, and actively provides "high-

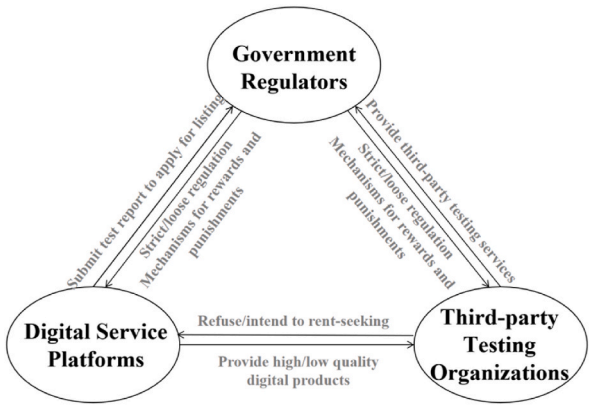



**Fig. 1.** Structure of the tripartite game of DSG.

quality digital products", it needs to invest additional technology, management, operation, and maintenance costs *CE*. At the same time, along with the authenticity and reliability, reputation, political resources, etc., digital service platforms will gain implicit benefits *RH*, and this benefit will produce positive externalities, which will lead to the third-party testing organizations to improve the credibility of the test *W* as well as the social benefits for the government *T*. Third-party testing organizations need to invest human, material and financial costs *CI* and receive subsidies *S* from government regulators when auditing the qualifications of digital service platforms. In the event of a data security incident, the scope of impact and level of importance may be relatively ordinary, or the government regulator, after considering the image of the government, economic interests, and social stability, does not need to deal with the incident urgently, and adopts the strategy of "loose regulation" to deal with the incident according to the daily plan. If the government regulator does not choose "strict regulation" from a holistic perspective, it may cause misunderstanding and disapproval among other stakeholders, leading to the generation of discordant voices, which in turn affects the stability and order of the society as well as causing corresponding reputational loss, which is partly recorded as negative environmental externality loss *L*.In the event of damage, loss or leakage of important data that jeopardizes the public interest or the national interest, government regulators need to adopt "strict regulation". "Strict regulation" may also require additional investment in specialized data recovery and restoration work compared to ordinary "loose regulation". This includes the cost of data recovery software, data recovery services, etc., as well as the cost of hiring external consultants and experts to provide technical support and consulting services, which is recorded as *CG*. At the same time, this will also recover certain losses for the digital service platform, third-party testing organizations, and governmental authorities, which are recorded as $R1$、$R2$ and $R3$ respectively.

**Assumption 4**. Impact of a data security incident. Assume that the probability of a data security event is $p$, which means that there is a certain amount of risk that makes it possible for a data security problem to occur. When a data security event occurs, it will bring different degrees of loss to each subject of interest. The digital service platform will face a direct revenue loss $m$ (including the direct revenue loss of the digital service platform, the compensation payment that may need to be paid), while the third-party testing organization usually decides whether to charge the digital service platform more testing fees due to the testing costs based on the severity and impact of the data security incidents of the digital service platform. The above additional fees levied by the third-party testing organization on the digital service platform are denoted as $i$. At the same time, if the data security incident affects the whole society due to the rent-seeking behavior of the third-party testing organization, and may even pose a serious threat to the national security and public interests, the government regulator will hold the third-party testing organization accountable, which may involve the accountability of the relevant responsible personnel, financial penalties and other measures. Third-party testing organizations are penalized by government regulators, recorded as a loss of third-party testing organizations in the event of a data security incident $g$.

Table 1 illustrates the parameters of the above assumptions, and Table 2 illustrates the game benefit matrix of digital service platforms, third-party testing organizations and government regulators in the DSG process.

## 3. Analysis of evolutionary game models

### 3.1. Strategic stability analysis of digital service platforms

The expected returns and average expected returns ($E_{11}$、$E_{12}$、$\overline{E_1}$) of digital service platforms "providing high-quality digital products" or "providing low-quality digital products" are respectively:

**Table 1**
Parameter settings of the three-party game model.

| Stakeholders | Symbols | Descriptions |
|---|---|---|
| Digital | *RM* | Ordinary income in the ordinary course of business |
| Service | *CM* | Ordinary costs in the ordinary course of business |
| Platforms | *CE* | Costs of additional inputs in fulfilling governance responsibilities |
| | *RH* | Hidden gains made in the performance of governance duties |
| | *R*1 | Losses recovered for digital service platforms under a strict regulatory model |
| | *m* | Loss of direct revenue in the event of a data security incident |
| | *i* | Additional fees levied on digital service platforms by third-party testing organizations |
| Third-party testing | *W* | Increased detection credibility due to positive externalities generated by digital service platforms |
| organizations | *CI* | Costs involved in qualifying digital service platforms |
| | *R*2 | Losses recovered for third-party testing organizations under a strict regulatory model |
| Government regulators | *T* | Increased social gains from positive externalities generated by digital service platforms |
| | *S* | Subsidies to third-party testing organizations |
| | *L* | Losses from negative environmental externalities in case of loose regulation |
| | *CG* | Technical and human costs invested in strict regulation |
| | *R*3 | Losses recovered for government regulators under the strict regulatory model |
| | *g* | Penalties for rent-seeking by third-party testing organizations |

**Table 2**
Benefit matrix for the three-party game.

| Third-party testing organizations | | | Government regulators | |
|---|---|---|---|---|
| | | | Strict regulation $z$ | loose regulation $1-z$ |
| **Digital service platforms** | Provide high quality digital products $x$ | Refuse to rent-seeking $y$ | $RM+RH-CM-CE-p(m+i-R1)$<br>$p(i+R2)-CI+S+W$<br>$T-S+pR3-CG$ | $RM+RH-CM-CE-p(m+i)$<br>$pi-CI+S+W$<br>$T-S-pL$ |
| | Provide low quality digital products $1-x$ | | $RM-CM-p(m+i-R1)$<br>$p(i+R2)+S-CI$<br>$-S+pR3-CG$ | $RM-CM-p(m+i)$<br>$pi+S-CI$<br>$-S-pL$ |
| | Provide high quality digital products $x$ | Intend to rent-seeking | $RM+RH-CM-CE-p(m-R1)$<br>$p(-g+R2)+W$<br>$T+p(g+R3)$ | $RM+RH-CM-CE-pm$<br>$W$<br>$T-pL$ |
| | Provide low quality digital products $1-x$ | $1-y$ | $RM-CM-p(m-R1)$<br>$p(-g+R2)$<br>$p(g+R3)$ | $RM-CM-pm$<br>$0$<br>$-pL$ |

$$\begin{cases} E_{11}=yz(RM+RH-CM-CE-p(m+i-R1)) \\ \quad +y(1-z)(RM+RH-CM-CE-p(m+i)) \\ +z(1-y)(RM+RH-CM-CE-Pp(Mm-R1)) \\ \quad +(1-y)(1-z)(RM+RH-CM-CE-pm) \\ \quad =RH-CE-CM+RM-pm-ipy+zpR1 \\ E_{12}=yz(RM-CM-p(m+i-R1)) \\ \quad +y(1-z)(RM-CM-p(m+i)) \\ \quad +(1-y)z(RM-CM-p(m-R1)) \\ \quad +(1-y)(1-z)(RM-CM-pm) \\ \quad =RM-CM-pm-ipy+zpR1 \\ \overline{E_1}=xE_{11}+(1-x)E_{12} \\ =RM-CM-CEx+RHx-pm-ipy+zpR1 \end{cases} \tag{3–1}$$

The replication dynamics equation for the digital service platform is:

$$F(x)=\frac{dx}{dt}=x(E_{11}-\overline{E_1})=x(1-x)(E_{11}-E_{12})=x(CE-RH)(x-1) \tag{3–2}$$

According to the stability theorem of the differential equation, the conditions that make the probability of the digital service platform choosing to "provide high-quality digital products" in a stable state are $F(x)=0$ and $\frac{dF(x)}{dx}<0$.

Firstly, by making $F(x)=0$, two zero points of $x=0$ and $x=1$ can be obtained. According to the stability theory of dynamical system, the point which only satisfies the condition $F(x)=0$ is the general stable state point, and it is also necessary to satisfy the condition $F(x)^{'}<0$ at the same time is the evolutionary stable equilibrium point. Therefore, the derivation of $F(x)$ is obtained according to equations (3)–(2):

$$dF(x)/dx=(1-2x)(RH-CE) \tag{3-3}$$

We find that the positive or negative form of the derived equation is determined by $x$、$RH$ and $CE$ only.

**Corollary 1**. *The probability of delivering high-quality digital products while fulfilling governance responsibilities during evolution is positively correlated with the implicit benefits it brings, and negatively correlated with the additional costs invested in delivering high-quality digital products (costs of technology, management, operation, maintenance, etc.).*

**Proof**. *When $CE<RH$, $dF(x)/dx|_{x=0}>0$, $dF(x)/dx|_{x=1}<0$, so $x=1$ is the evolutionary equilibrium strategy, and the digital service platform, as a finite and rational economist, will adopt the strategy of "providing high-quality digital products". When $CE>RH$, then $dF(x)/dx|_{x=1}>0$, $dF(x)/dx|_{x=0}<0$, so $x=0$ is the evolutionary equilibrium strategy, and the optimal strategy of the digital service platform is to "provide low-quality digital products".*

Corollary 1 suggests that safeguarding the implicit benefits that digital service platforms can derive from fulfilling their governance role can prevent enterprises from providing low-quality digital products. Increasing the implicit benefits that digital service platforms can obtain when they fulfill their governance responsibilities will help digital service platforms to choose "providing high-quality digital products" as their stabilization strategy. Increased input costs will encourage digital service platforms to choose "providing low-quality digital products" as a stabilizing strategy. Government regulators can not only ensure the smooth fulfillment of the

governance of digital service platforms by increasing the probability of strict government supervision, but also by developing the impartiality of third-party testing organizations. For example, it can take measures to improve the reputation value and social responsibility of third-party testing organizations, give full play to the effectiveness of social forces in regulating the safety of digital products, and build a quality supervision system of social co-governance for the safety of digital products.

### 3.2. Strategic stability analysis of third-party testing organizations

The expected returns and average expected returns ($E_{21}$、$E_{22}$、$\overline{E_2}$) of the third-party testing organizations for " refusing to rent-seeking" or "intending to rent-seeking" are respectively:

$$\begin{cases} E_{21} = xz(p(i+R2) - CI + S + W) \\ \quad +x(1-z)(pi - CI + S + W) \\ \quad +(1-x)z(p(i+R2) + S - CI) \\ \quad +(1-x)(1-z)(pi + S - CI) \\ \quad = S - CI + ip + Wx + pR\,2z \\ E_{22} = xz(p(-g+R2) + W) + x(1-z)W \\ +(1-x)z(p(-g+R2)) = Wx - gpz + pR\,2z \\ \overline{E_2} = yE_{21} + (1-y)E_{22} \\ = Sy - CIy + Wx - gpz + ipy + pR\,2z + gpyz \end{cases} \tag{3–4}$$

The replication dynamic equation for the third-party testing organization is:

$$F(y) = \frac{dy}{dt} = y(E_{21} - \overline{E_2}) = y(1-y)(E_{21} - E_{22}) = y(1-y)(S - CI + ip + gpz) \tag{3–5}$$

Based on equations (3)–(5), solve the replication dynamic equation for the tendency of third-party testing organizations to "refuse to rent-seeking", so that

$$z_0 = \frac{CI - S - ip}{gp} \tag{3–6}$$

(1) When $z = z_0$, then $F(y) \equiv 0$ and is in a stable state no matter what value $y$ takes. That is, at this time, regardless of whether the third-party testing organization is actively managed, for the third-party testing organization is the optimal choice of strategy, and the third-party testing organization will not adjust its own strategy with the change of time. At this time, the third-party testing organization can not determine the stabilization strategy.

(2) When $z \neq z_0$, making $F(y) = 0$, two zero points of $y = 0$ and $y = 1$ can be obtained. According to the stability theory of dynamical system, the point which only satisfies the condition $F(y) = 0$ is the general stable state point, and the point which satisfies both the condition $F(y) = 0$ and the condition $F(y)' < 0$ is the evolutionary stable equilibrium point. Therefore, derivation of $F(y)$ leads to Eq:

$$\frac{dF(y)}{dy} = (1-2y)(S - CI + ip + gpz) \tag{3–7}$$

**Corollary 2.** The probability of a third-party testing organization rejecting rent-seeking in the evolutionary process is affected by a number of factors, including government subsidies, costs invested in testing, losses incurred in digital governance, and losses incurred in intentional rent-seeking. It is positively correlated with government subsidies, losses at the time of digital governance, and losses at the time of intentional rent-seeking, and negatively correlated with the costs invested in testing.

**Proof.**

(1) When $z_0 < 0$, $z > z_0$ holds, i.e., $S - CI + ip + gpz > 0$, at this time, $\frac{dF(y)}{dy}|_{y=0} > 0$, $\frac{dF(y)}{dy}|_{y=1} < 0$, then $y = 1$ is an evolutionary equilibrium strategy, i.e., the third-party testing organization as a finite and rational economic agent will choose the decision of "refusing to rent-seeking ".

(2) When $z_0 > 1$, $z < z_0$ constant, that is, $S - CI + ip + gpz < 0$, at this time $\frac{dF(y)}{dy}|_{y=0} < 0$, $\frac{dF(y)}{dy}|_{y=1} > 0$, then $y = 0$ is the evolutionary equilibrium strategy, that is, the third-party testing organization as a finite rational economic man will choose the decision of "intention to rent-seeking ".

(3) *When* $0 < z_0 < 1$, it is divided into two cases: when $0 < z < z_0 < 1$, at this time $\frac{dF(y)}{dy}|_{y=0} < 0$, $\frac{dF(y)}{dy}|_{y=1} > 0$, then $y = 0$ is the evolutionary equilibrium strategy, that is, the third-party testing organization as a limited rational economic man will choose the decision of "intention to rent-seeking". When $0 < z_0 < z < 1$, at the same time, $\frac{dF(y)}{dy}|_{y=0} > 0$, $\frac{dF(y)}{dy}|_{y=1} < 0$, then $y = 1$ is the evolutionary equilibrium strategy, i.e., the third-party testing organization as a finite rational economic agent will choose "refusing to rent-seeking".

Corollary 2 suggests that when the government subsidizes third-party testing organizations, these organizations may become less dependent on rent-seeking practices because of the additional financial support they receive. This is because the subsidy reduces their operating costs and increases their profitability, allowing them to make profits through normal market competition without having to resort to improper means such as rent-seeking. High testing costs may lead to greater financial pressure on third-party testing organizations in their operations. In order to maintain their operations and profitability, some organizations may consider accepting rent-seeking behavior in order to obtain additional financial gains, thereby relieving operational pressure. Losses suffered during digital governance include reputational losses, legal risks, and financial losses. These costs and losses can make third-party testing organizations more cautious when faced with the temptation of rent-seeking, thus increasing their probability of rejecting rent-seeking. Losses suffered when intending to engage in rent-seeking include potential legal risks, reputational damage, and ethical pressures. If the third-party testing organization has the intention to participate in rent-seeking behavior, these risks will bring serious consequences to the organization, which will make the third-party testing organization more cautious when it has the intention to rent-seeking, thus increasing its probability of refusing rent-seeking. By enhancing the professionalism of testing personnel, expanding media disclosure, and other such means, it will also increase the speculative costs of third-party testing organizations intent on rent-seeking, which will help reduce their speculative behavior. Penalties and losses can effectively ensure digital security, and rewards and subsidies can also promote the level of digital governance participation of third-party testing organizations.

### 3.3. Strategic stability analysis of government regulators

The expected returns and average expected returns ($E_{31}$、$E_{32}$、$\overline{E_3}$) for "strict regulation" or "loose regulation" by the government regulator are respectively:

$$\begin{cases} E_{31} = xy(T - S + pR\,3 - CG) + x(1-y)(T + p(g + R3)) \\ \qquad +(1-x)y(-S + pR\,3 - CG) \\ \qquad +(1-x)(1-y)(p(g + R3)) \\ \qquad = Tx - CGy + gp + pR3 - Sy - gpy \\ E_{32} = xy(T - S - pL) + x(1-y)(T - pL) \\ +(1-x)y(-S - pL) + (1-x)(1-y)(-pL) = Tx - Lp - Sy \\ \overline{E_3} = zE_{31} + (1-z)E_{32} \\ \qquad = (z-1)(x(T - Lp)(y-1) - y(x-1)(S + Lp) \\ \qquad +xy(S - T + Lp) + (x-1)((y-1)Lp) \\ +z\begin{pmatrix} y(x-1)(CG + S - pR\,3) \\ -x(T + p(g + R3))(y-1) + xy(T - CG - S + pR\,3) \\ +p(g + R3)(x-1)(y-1) \end{pmatrix} \end{cases} \tag{3–8}$$

The equation for the replication dynamics of the government regulator is:

$$F(z) = \frac{dz}{dt} = z(E_{31} - \overline{E_3}) = z(1-z)(Lp - CGy + gp + pR\,3 - gpy) \tag{3–9}$$

Based on equations (3)–(9), solve the equation for the replication dynamics of the government regulator's preference for "strict regulation," so that

$$y_0 = \frac{Lp + gp + pR\,3}{CG + gp} \tag{3 -10}$$

(1) When $y = y_0$, then $F(z) \equiv 0$, regardless of the value of $z$, are in a stable state. That is, at this time, whether the government regulator adopts the "strict regulation" strategy or "loose regulation" strategy, is the optimal choice of strategy, and the government regulator will not adjust its own strategy over time. At this time, the government regulator cannot determine the stabilization strategy.

(2) When $y = y_0$, make $F(z) = 0$, can get $z = 0$ and $z = 1$ two zeros. According to the stability theory of dynamical systems, the point that only satisfies the condition $F(z) = 0$ is the general stable state point, and the point that satisfies both the condition $F(z) = 0$ and the condition $F(z)' < 0$ is the evolutionary stable equilibrium point. Therefore, derivation of F(z) leads to Eq:

$$\frac{dF(z)}{dz} = (1-2z)(Lp - CGy + gp + pR\,3 - gpy) \quad (3\text{-}11)$$

**Corollary 3**. In the process of evolution, the probability of strict regulation by government regulators is affected by a number of factors, such as the negative environmental externality loss generated by lax regulation, the technological and labor costs invested in strict regulation, the punishment for the third-party enterprises that intend to rent-seeking, and the loss recovered for the government regulators by strict regulation, and so on. Among them, the probability of strict regulation by government regulators is positively correlated with the negative environmental externality loss generated by loose regulation, the penalty for the third-party enterprise intending to seek rent, and the loss recovered for the government regulators by strict regulation; and it is negatively correlated with the technological and human cost invested in strict regulation.

**Proof**. (1) When $y_0 < 0$, $y > y_0$ holds, i.e., $Lp - CGy + gp + pR\,3 - gpy < 0$, at this time, $\frac{dF(z)}{dz}|_{z=1} > 0$, and $\frac{dF(z)}{dz}|_{z=0} < 0$, $z = 0$ is the point of stability of decision-making, i.e., the government regulator, as a finite and rational economic man, will choose "loose regulation".

(2) When $y_0 > 1$, $y < y_0$ constant, that is, $Lp - CGy + gp + pR\,3 - gpy > 0$, at this time $\frac{dF(z)}{dz}|_{z=1} < 0$, $\frac{dF(z)}{dz}|_{z=0} > 0$, then $z = 1$ is the decision-making point of stability, i.e., the government regulator as a finite rational economic man will choose "strict regulation ".

(3) When $0 < y_0 < 1$, there are two cases: when $0 < y < y_0 < 1$, when $\frac{dF(z)}{dz}|_{z=1} < 0$, $\frac{dF(z)}{dz}|_{z=0} > 0$, then $z = 1$ is the decision-making point of stability, i.e., the government regulator as a finite rational economic man will choose " strict regulation"; when $0 < y_0 < y < 1$, when $\frac{dF(z)}{dz}|_{z=1} > 0$, $\frac{dF(z)}{dz}|_{z=0} < 0$ is the decision-making point of stability, that is, the government regulator as a limited rationality of the economic man will choose "loose regulation".

Corollary 3 suggests that government regulators will have an increased incentive to adopt a strict regulatory strategy when they face negative externality losses from adopting a loose regulatory strategy. Strict regulation can effectively curb market participants' misbehavior and reduce the occurrence of negative externality loss. Meanwhile, the probability of strict regulation by government regulators is affected by the strategic choice of third-party testing organizations; when third-party testing organizations intend to seek rents, government regulators levy penalties on the third party through strict regulation, which promotes the probability of regulators choosing strict regulation. The government invests significant technical and human costs in strict regulation, and while these costs are critical to ensuring the effectiveness and fairness of regulation, government regulators may reduce the probability of strict regulation after weighing the pros and cons due to resource constraints, cost-benefit considerations, regulatory fatigue, and market changes.

### *3.4. Stability analysis of the system*

In evolutionary games, replicated dynamic equations are usually used to study the strategy evolution within a single group. However, equilibrium analysis of the whole game system is used to understand the stability and evolutionary trend of the game more comprehensively. In replication dynamics, the strategy evolution of each individual is influenced by other individuals in the group, and the stability of the whole system depends not only on the strategy choices within a single group, but also on the strategy competition and evolution process among different groups. So an equilibrium analysis of the whole game system is also needed to study the propagation and competition process of different strategies among groups and the stable state that may be reached in the end. Organizing Eqs. (3)–(2), Eqs. (3)–(5) and Eqs. (3)–(9) so that $F(x) = 0, F(y) = 0, F(z) = 0$, several special equilibrium solutions existed in this research problem can be obtained, including eight pure strategy Nash equilibrium solutions. These solutions are $E(1,1,1)$, $E(1,1,0)$, $E(1,0,1)$, $E(1,0,0)$, $E(0,1,1)$, $E(0,1,0)$, $E(0,0,1)$, $E(0,0,0)$, respectively. All individuals at these equilibrium points have no incentive to change their strategy when adopting a particular strategy, unless a mutant emerges that can make him change his strategy. This means that the replication dynamics of the strategies are in equilibrium and the strategy frequency is stable. There are also 2 mixed-strategy equilibrium points, $E(x_1, y_0, z_0)$ and $E(x_2, y_0, z_0)$, in which

$$x_1 = 0; x_2 = 1; y_0 = \frac{Lp + gp + pR\,3}{CG + gp}; z_0 = \frac{CI - S - ip}{gp}$$

This equilibrium exists if and only if $x_1$, $x_2$, $y_0$, $z_0 \in (0,1)$.

The stable solution in multiple group evolutionary games is a strict Nash equilibrium, and a strict Nash equilibrium must be a pure strategy. Therefore, in order to explore the evolutionary stability of the digital service platform - the third-party testing agency - the government regulatory department of the three parties, this paper carries out stability research on the eight pure strategy equilibrium points in the three-party evolutionary game. According to the method proposed by Friedman to test the stability of equilibrium points, the local stability of equilibrium points is judged by the Jacobi matrix. The Jacobi matrix of this evolutionary system is obtained from the above replicated dynamic differential equation, and the partial derivatives of $F(x)$, $F(y)$, and $F(z)$ with respect to $x$, $y$, and $z$ are obtained respectively, then the Jacobi matrix of the three-party game is:

$$J=\begin{bmatrix} j_{11} & j_{12} & j_{13} \\ j_{21} & j_{22} & j_{23} \\ j_{31} & j_{32} & j_{33} \end{bmatrix}=\begin{bmatrix} \frac{\partial F(x)}{\partial x} & \frac{\partial F(x)}{\partial y} & \frac{\partial F(x)}{\partial z} \\ \frac{\partial F(y)}{\partial y} & \frac{\partial F(y)}{\partial y} & \frac{\partial F(y)}{\partial z} \\ \frac{\partial F(z)}{\partial x} & \frac{\partial F(z)}{\partial y} & \frac{\partial F(z)}{\partial z} \end{bmatrix}= \tag{3 -12}$$

$$\begin{bmatrix} (CE-RH)(2x-1) & 0 & 0 \\ 0 & (1-2y)(S-CI+ip+gpz) & gpy(1-y) \\ 0 & z(z-1)(CG+gp) & (1-2z)(Lp-CGy+Gp+pR\,3-gpy) \end{bmatrix}$$

The equilibrium point stability determination is made according to the Lyapunov stability condition, i.e., by analyzing the positive and negative cases of the eigenvalues. If the real part of all the eigenvalues of the Jacobi matrix is less than zero, the equilibrium point is locally asymptotically stable, and the equilibrium point is evolutionarily stable strategy. If at least one of the eigenvalues has a real part greater than zero, the equilibrium point is unstable. If there are positive and negative eigenvalues, the equilibrium point is a saddle point where the system converges to the equilibrium point in some directions and deviates from the equilibrium point in other directions.

Taking the equilibrium point $E(1,1,1)$ as an example, the conditions for the system to satisfy the evolutionary stabilization strategy are discussed by substituting it into the following equation:

$$J=\begin{bmatrix} CE-RH & 0 & 0 \\ 0 & CI-S-ip-gp & 0 \\ 0 & 0 & CG-pR\,3-Lp \end{bmatrix} \tag{3 -13}$$

It is known that the three eigenvalues of the Jacobi matrix corresponding to the equilibrium point $E(1,1,1)$ are $\lambda 1=CE-RH$,$\lambda 2=CI-S-ip-gp$,and $\lambda 3=CG-pR\,3-Lp$. Assuming that $\lambda 1$, $\lambda 2$, and $\lambda 3$ satisfy the condition less than 0, the equilibrium point $E(1,1,1)$ is asymptotically stable. Similarly substituting the remaining equilibrium points into Eqs. 3–13 respectively, the corresponding Jacobi matrix eigenvalues of each strategy equilibrium point can be obtained, as shown in Table 3.

Since $Lp+CG+pR\,3>0$ and $e>0$, neither $E(1,0,0)$, nor $E(0,0,0)$ satisfies the condition of ESS. In summary, in the three-party evolutionary game model of digital service platform, third-party testing organization, and government regulator, only $E(0,1,1)$, $E(0,1,0)$, $E(0,0,1)$, $E(1,1,0)$, $E(1,0,1)$, and $E(1,1,1)$ can be transformed into a stabilization strategy under certain conditions. And the decision-making behaviors of digital service platforms, third-party testing organizations and government regulators are determined by $RH-CE, S+ip-CI$ and $Lp-CG+pR\,3$. Among them, $RH-CE$ denotes the excess profit between the invisible revenue and the cost paid by the digital service platform when it provides high-quality digital products. $S+ip-CI$ denotes the excess profit between the subsidies received by the third-party testing organization when it rejects rent-seeking, the penalties collected and its input costs. $Lp-CG+pR\,3$ denotes the difference between the losses recovered and the costs incurred when government regulators strictly supervise the response to data security incidents. Based on the analysis of Table 3, the values of $CI-S-ip$ may fall within the intervals $(-\infty,0)$, $(0,ep)$, and $(ep,\ +\infty)$, while the intervals of $RH-CE$ and $Lp-CG+pR\,3$ are $(-\infty,0)(0,\ +\infty)$.

**Corollary 4.** The probability that a digital service platform chooses the strategy of " providing high-quality digital products" is

**Table 3**
Equilibrium point and eigenvalue of the system.

| Equilibrium point | $\lambda_1$ | $\lambda_2$ | $\lambda_3$ | State |
|---|---|---|---|---|
| $E(0,0,0)$ | $\alpha$ | $-\beta$ | $\gamma+CG+gp$ | Unstable $(\lambda_3>0)$ |
| $E(0,1,0)$ | $\alpha$ | $\beta$ | $\gamma$ | $\alpha,\beta,\gamma<0$ |
| $E(0,0,1)$ | $\alpha$ | $gp-\beta$ | $-\gamma-CG-gp$ | $\alpha<0,\ g\,p-\beta<0$ |
| $E(0,1,1)$ | $\alpha$ | $\beta-gp$ | $-\gamma$ | $\alpha,-\gamma,\beta-gp<0$ |
| $E\left(0,\frac{Lp+gp+pR\,3}{CG+gp},\frac{CI-S-ip}{gp}\right)$ | $\alpha$ | $e$ | $-e$ | Unstable $(\lambda_2>0)$ |
| $E(1,0,0)$ | $-\alpha$ | $-\beta$ | $\gamma+CG+gp$ | Unstable $(\lambda_3>0)$ |
| $E(1,1,0)$ | $-\alpha$ | $\beta$ | $\gamma$ | $-\alpha,\beta,\gamma<0$ |
| $E(1,0,1)$ | $-\alpha$ | $gp-\beta$ | $-\gamma-CG-gp$ | $-\alpha,gp-\beta<0$ |
| $E(1,1,1)$ | $-\alpha$ | $\beta-gp$ | $-\gamma$ | $\beta-gp,-\alpha,-\gamma<0$ |
| $E\left(1,\frac{Lp+gp+pR\,3}{CG+gp},\frac{CI-S-ip}{gp}\right)$ | $-\alpha$ | $e$ | $-e$ | $Unstable(\lambda_2>0)$ |

Notes: $\alpha=RH-CE$, $\beta=CI-S-ip$, $\gamma=Lp-CG+pR\,3$ and $e=(-g(CG+gp)(Lp-CG+pR\,3)(L+g+R3)(S-CI+ip)(S-CI+gp+ip))^{\left(\frac{1}{2}\right)}/(pg^2+CGg)$.

positively correlated with the amount of excess profit that it earns from carrying out this strategy. This implies that the higher the excess profit earned from providing high-quality digital products, the more the digital service platform, as a rational economic agent, tends to provide such products.

**Proof**. When $RH - CE \in (-\infty, 0)$, for the digital service platform, the additional revenue brought by "providing high-quality digital products" is smaller than the initial investment in technology, management, operation and other costs. In this case, "providing low-quality digital products" becomes the preferred choice of the digital service platform. When $RH - CE \in (0, +\infty)$, the invisible benefit obtained from "providing high-quality digital products" is higher than the cost consumed, then the platform prefers this behavioral choice.

Corollary 4 shows that safeguarding the governance revenue of digital service platforms can effectively prevent platforms from treating data security negatively, and instead consciously take precautionary measures to strengthen the management and governance of data security, so that the platform's stable decision-making level will evolve from $x = 0$ to $x = 1$. Government regulators can increase the net benefit of platform governance by giving subsidies, or expand the reputation of platforms by publicizing and awarding them with the help of official websites or media reports. Increasing the platform's willingness to provide high-quality digital products will effectively prevent improper data processing behavior, better protect the security of national digital assets, further improve the quality and efficiency of digital service, and promote the construction of digital ecological security.

**Corollary 5**. The probability of a third-party testing organization choosing the "refusing to rent-seeking" strategy is positively related to the amount of excess profit earned when engaging in this strategy. This means that the higher the excess profit earned from refusing rent-seeking, the more likely that the third-party inspection organization, as a rational economic agent, will choose this strategy.

**Proof**. When , the subsidies and penalties received by the third-party testing organization for choosing the "refusing to rent-seeking" strategy are higher than the costs incurred by the third-party testing organization. "Refusing to rent-seeking" is the optimal strategy for the third-party testing organization. When , the expected penalties imposed on the third-party testing organization by the government regulator after the data leakage are higher than the cost of "refusing to rent-seeking" by the third-party testing organization. In this case, in order to avoid being penalized by the government regulator, "refusing to rent-seeking" will become its optimal choice. When , the cost paid by the third-party testing organization in "refusing to rent-seeking" is higher than the possible penalties, and its stabilization strategy will become "intentional rent-seeking". This is not conducive to the stable development of the digital ecosystem.

Corollary 5 suggests that when third-party testing organizations choose "intending to rent-seeking" to gain more benefits, government regulators should strengthen the penalty for rent-seeking behavior of third-party testing organizations. Heavier penalties for third-party testing organizations can encourage them to strictly fulfill their data governance responsibilities and improve their fairness, effectiveness and governance capacity. In addition, through the appropriate use of financial subsidies, third-party testing organizations can alleviate the rent-seeking behavior brought about by the profit-seeking mentality that disrupts the market. Improving the enthusiasm of third-party testing organizations in data security governance makes the stable decision-making of third-party testing organizations evolve from $y = 0$ to $y = 1$, which effectively ensures the availability and security of local data resources, and thus maintains the stable operation of the digital ecology and public security.

**Corollary 6**. The probability of a government regulator choosing the "strict regulation" strategy is negatively correlated with the cost of responding to a data security incident while pursuing that strategy. This means that the lower the cost of strict regulation, the more likely the government regulator, as a rational economic agent, will choose this strategy.

**Proof**. When $Lp - CG + pR\ 3 \in (-\infty, 0)$, the cost of the government regulator to deal with the data security problem by adopting the "strict regulation" strategy is much higher than the negative externality loss. At this point, the government regulator will tend to adopt "loose regulation". When $Lp - CG + pR\ 3 \in (0, +\infty)$, the severity of the consequences of the data security problem far exceeds the cost of the government regulator choosing the "strict regulation" strategy. In this case, the government regulator will pay more attention to the strict regulation of data security incidents, and will choose a rapid response strategy to prevent and control cyber-attacks, disinformation, and other digital risks, so as to minimize the damage to the digital ecosystem.

Corollary 6 suggests that government regulators, as rational economic agents, will tend to choose the " loose regulation" strategy when the cost of choosing the " strict regulation" strategy is high. Strict regulation can ensure that data service platforms provide high-quality digital products, which includes the accuracy, integrity and reliability of data. High-quality data is the basis for data analysis, decision-making and policy implementation, and is crucial for socio-economic development and national security. It will also help prevent rent-seeking behavior between third-party testing organizations and data service platforms, i.e., obtaining benefits through improper means, such as data forgery and collusive testing. At the same time, strict regulation will also help enhance the reputation and credibility of the entire data services industry. When consumers and investors see that government regulators are working hard to maintain market order and safeguard data quality, they are more willing to trust companies and products in the industry. This means that there will be a push to enhance the proactivity of government regulators in data security governance, so that the stable decision-making of government regulators will evolve from $z = 0$ to $z = 1$, thus effectively ensuring the availability and security of local data resources, maintaining the stable operation of the digital ecosystem and public safety, and providing strong data support for economic development.

In summary, there are six possible stabilization points in the data security governance game system, among which $E(1, 1, 1)$ is the ideal stabilization point, which corresponds to the ideal strategy combination of "providing high-quality digital products, refusing to rent-seeking, and strict regulation". Different conditions correspond to different strategy combinations. Obviously, in order to make

$E(1,1,1)$ a stabilization point, the three conditions of $CE - RH < 0$, $CI - S - ip - gp < 0$ and $CG - pR\,3 - Lp < 0$ must be satisfied at the same time. That is, the cost of digital service platforms to maintain data security is less than the hidden gains they receive, the cost of third-party testing organizations to refuse rent-seeking is less than the subsidies and penalties they receive, and the cost of strict supervision by government regulators is less than the negative externality loss brought about by the continued fermentation of the incident.

## 4. Numerical simulation analysis and recommendations

In order to verify the validity of the evolutionary stability analysis, this paper uses Matlab2023b to assign the model to numerical values for numerical simulation.

Considering the research assumptions of this paper, by drawing on the research of scholars such as Qu Xinchi et al. [39], Lv Peng et al. [40], and Xu Hui [36], on the basis of the evolutionary stabilization strategy (providing high-quality digital products, rejecting rent-seeking, and strictly regulating), we make the values of the initial parameters to be $RH = 9, CE = 8, p = 0.4, CI = 5, S = 4, i = 2, L = 20, CG = 8, R3 = 4, g = 6$. It has been analyzed in the previous section that the decision-making behaviors of digital service platforms, third-party testing organizations and government regulators are determined by $RH - CE$, $S + ip - CI$ and $Lp - CG + pR\,3$. And it is obvious that $RH$, $CE$, $S$, and $i$ are mutually antagonistic interest factors, because the increase of $RH$ and the decrease of $CE$ imply the increase of interest, which are of the same nature, and the evolution state of the simulation image is just the opposite.

Therefore, excluding the factors of the same nature, the next main analysis is the impact of $RH$, $S$, $p$, $L$, and $CG$ on the evolutionary trajectory of the data security governance system.

### 4.1. Implicit benefits

Based on the initial parameter values, the $RH$ is 1, 9, 15, respectively, and the simulation results of its evolution from the initial time 0 to 50 are observed. As shown in Fig. 2, when $RH < 9$, the behavior of digital service platforms to provide high-quality digital products obtains small benefits, and their final strategy choice is to "provide low-quality digital products", $x$ converges to 0, and the data security governance system degrades to the bad state of $E(0,1,1)$. With the growth of $RH$, the willingness of the digital service platform to provide high-quality digital products gradually rises from providing low-quality products to providing high-quality products, and the system evolves to the ideal state of $E(1,1,1)$. This is because if the platform can effectively protect the information security of business secrets, personal privacy, etc. when providing high-quality digital products, it can not only reduce legal risks, but also significantly improve user experience, enhance user stickiness, and thus expand market share. These advantages can win the trust and reputation of users, attract more potential users for the data service platform, and promote continuous business growth. At the same time, high-quality products also help to enhance brand image and win more competitive advantages and market share for the company. Therefore, the invisible benefits positively affect the platform's behavioral choices, and the more cost-effective the platform's strategy of providing high-quality digital products is, the higher the probability of producing high-quality products.

### 4.2. Government subsidies

Based on the initial parameter values, so that $S = 1, 4, 6$, view its replication of the dynamic equation over time evolution of the simulation results of 50 times can be obtained in Fig. 3. As can be seen from Fig. 3, when $S < 4$, that is, the government regulators to establish a low subsidy, the third-party testing organizations to choose "refusal to rent-seeking" strategy of the probability of convergence to 0, when the third-party testing organization's strategy choice for the "intending to rent-seeking". When $S > 4$, the third-party testing organization's strategy choice from "intending to rent-seeking" to " refuse to rent-seeking ", the probability of

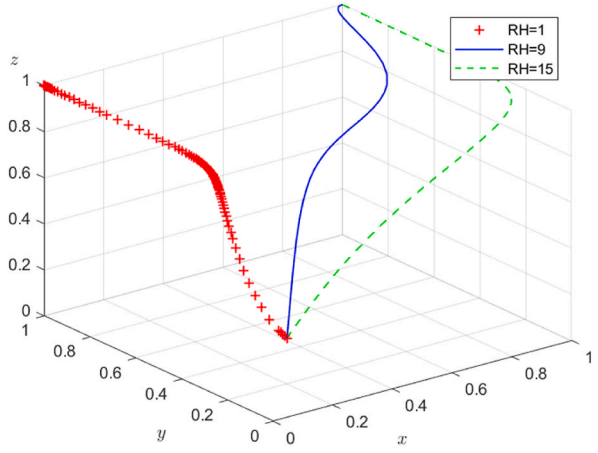



**Fig. 2.** Impact of invisible benefits.

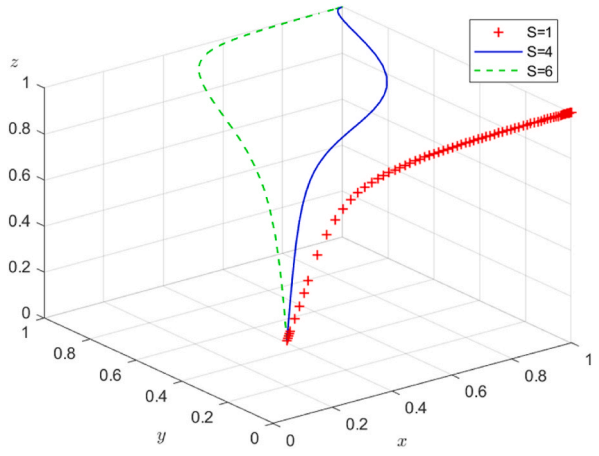



**Fig. 3.** Impact of government subsidies.

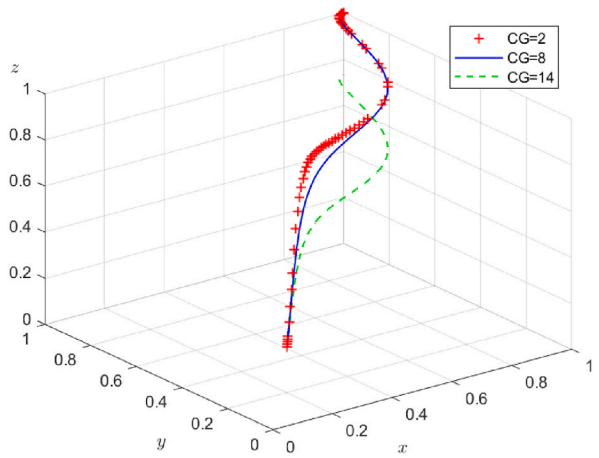



**Fig. 4.** Impact of regulatory costs.

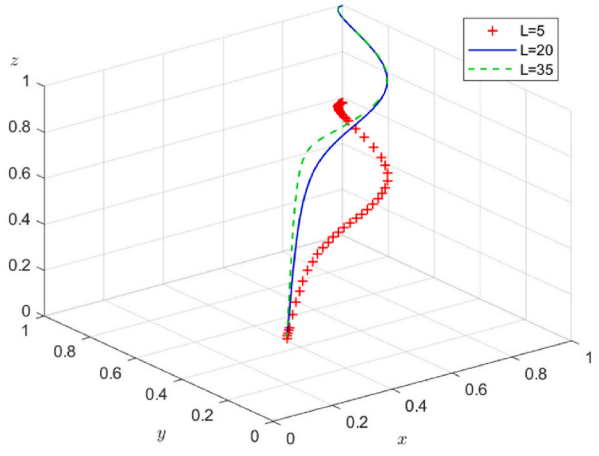



**Fig. 5.** Impact of negative externality losses.

refusing to rent-seeking will converge more and more on 1. This indicates that increasing the subsidy amount of third-party testing organizations has a significant effect on increasing their willingness to refuse to rent-seeking, and can positively affect the development of the data ecosystem. This is because third-party testing organizations, as rational economic agents, may face economic pressures and resource constraints when digital governance is costly, leading to their reluctance to actively govern. High costs may involve multiple aspects of data collection, analysis, processing and storage, as well as investments in compliance audits, technology updates and staff training. With limited resources, third-party testing organizations may weigh the costs and benefits, and may lack sufficient motivation and resources to invest in higher-cost governance projects, which reduces the motivation and effectiveness of governance, at which point the system degrades to a poorly stabilized state of $E(1,0,1)$. When government regulators vigorously support third-party testing organizations to protect data information security, and the support is in the medium-high range, the third-party testing organizations will take the initiative to participate in the data governance process.

### 4.3. Regulatory costs and negative externality losses

Based on the initial parameter values, in the case of other parameter values remain unchanged, respectively, so that $CG = 2, 8, 14$, view its replicated dynamic equations with time evolution of 50 times the simulation results can be obtained in Fig. 4; so that $L = 5$, 20, 35, and the same evolution 50 times can be obtained in Fig. 5.

When $CG \leq 8$, or when $L > 20$, the probability of strict regulation by the government regulator tends to 1, the government regulator has been inclined to adopt the "strict regulation" strategy, $z$ converges to 1, the system is in the optimal and stable state of $E(1, 1,1)$, which can continue to promote the healthy development of digital ecology. When $CG$ is higher or when $L$ is lower, the probability of adopting the strict regulation strategy gradually decreases, but it will not be lower than the initial probability of willingness, unless the coping cost is much higher than the loss of negative externality, and the amount tends to infinity, the system will degrade to the bad stability of $E(1,1,0)$. This is because when the cost of strict regulation is low, the government regulator has enough financial ability to afford this part of the cost, and the government regulator based on the overall welfare of the society, will not let the data problem exist because of the cost of loss of its own interests, so even if the cost of coping is still growing will choose to respond in time. However, when the growth of response costs is too high, much lower than the negative externality impact of the data breach risk, which seriously affects the country's financial resources allocation, the stabilization strategy of government regulators will tend to lax regulation.

### 4.4. Probability of data security incidents

Based on the initial parameter values, let $p = 0.1$, 0.2, 0.4, 0.6, and observe its influence on the strategy selection of the three-party subject, and the relevant situation can be obtained in Fig. 6. Where the horizontal axis indicates the growth of time, and the vertical

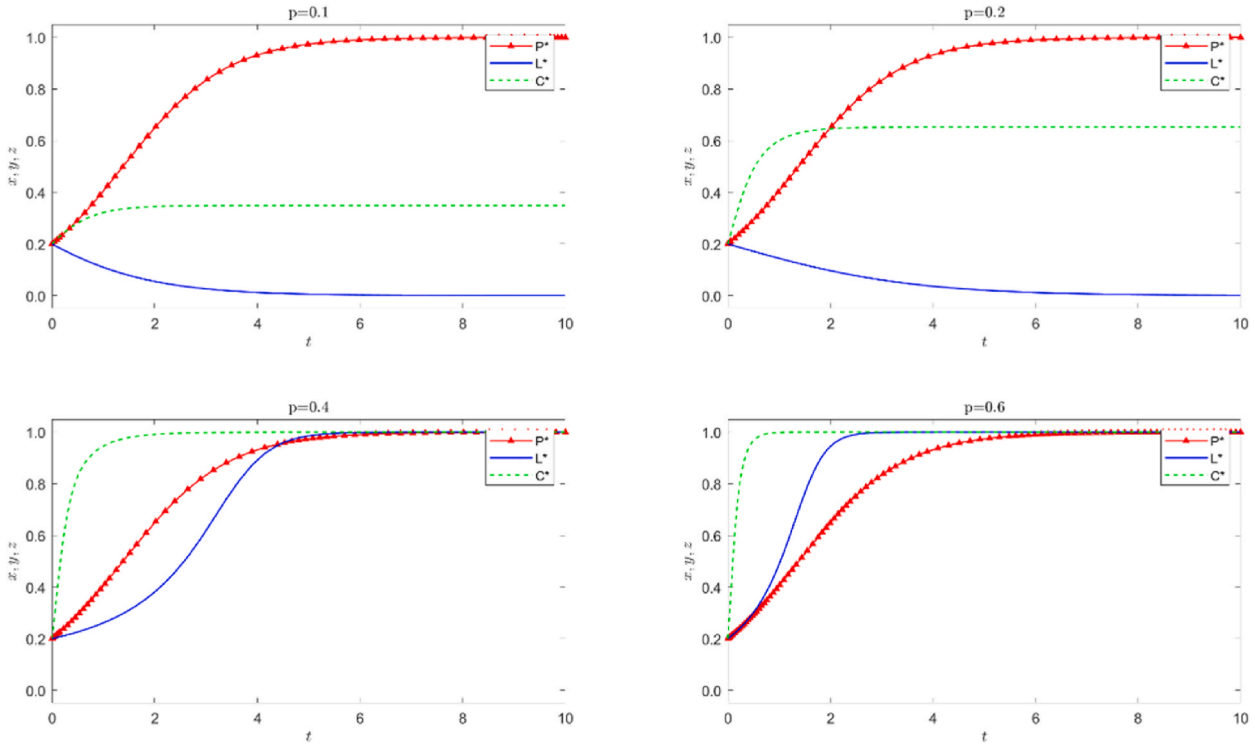



**Fig. 6.** Impact of probability of data security incidents.

axis indicates the probability that the digital service platform, the third-party testing organization and the government regulator choose to adopt the corresponding strategy. As can be seen in Fig. 6, the probability of data security events has significantly different degrees of influence on digital service platforms, third-party testing organizations, and government regulators. Overall, when $p = 0.1$, 0.2 in the low range, the probability of data security events negatively affects the governance behavior of the third-party testing agency, and positively affects the behavior of digital service platforms and government regulators, but the latter has not reached a stable state. When the middle and high intervals of $p = 0.4$ and 0.6, all three subjects reach a positive stabilization state, which indicates that higher data crises motivate all parties to take active actions to block the occurrence of threatening events. Looking apart, as the probability of data security events increases, the evolution of the strategy of digital service platforms does not change, the probability of government regulators adopting the strategy of "strict regulation" continues to rise, and the speed of convergence continues to accelerate, while the strategy of third-party testing organizations is to reject rent-seeking. This shows that after the digital service platform can obtain satisfactory benefits through active governance, regardless of the size of the probability of crisis, will take the initiative to assume the main responsibility for data security governance, to build a solid foundation for a good data ecosystem. At this time, the third-party testing organization to choose "intending to seek rent" will get more self-serving benefits. However, with the further increase in the probability of data security problems, relying on the platform can not guarantee the security of data assets in the field. Therefore, when the third-party testing organizations get the required testing data, they will tend to "refuse to rent-seeking" for their own interests and reputation, and the time to reach the steady state will be shortened gradually. Therefore, at the stage of low crisis probability, government regulators can make third-party testing organizations participate in the governance process through standard control, official media reports and punitive interventions or coercive measures to enhance the enthusiasm and effectiveness of the subject's governance.

### 4.5. Suggestions

#### 4.5.1. Building a credit assessment mechanism

Theoretical and practical studies have shown that reputation is a resource leading to competitive advantage [41]. In the increasingly competitive market, various types of platforms have focused on their reputation and word-of-mouth, and these factors are decisive for their market position. At the same time, trust and reputation systems are becoming an important trend in the provision of decision support for Internet intermediary services [42]. Such systems not only can effectively record and feedback the results of data security governance efforts, but also can effectively prevent the occurrence of moral hazard [43]. In order to strengthen this trend, the government should improve the data security governance guarantee system, for example, in terms of improving the legal and institutional construction, it should improve the regulations on data ownership issues, improve the data security management system, and build a legal and institutional framework system integrating civil, criminal and administrative [2].

(1) Improving data security assessment procedures. The Government can promote the construction of a comprehensive, scientific and operational data security credit assessment indicator system based on the full life cycle of data. The indicator system should cover all aspects of the full life cycle, including data collection, storage, transmission, use and destruction, while taking into account the confidentiality, integrity and availability of data. In addition, factors such as the enterprise's historical data security incidents, violation records, and compliance inputs should be included in the assessment.
(2) Implement dynamic governance of digital security. Data security credit assessment should not be a one-time event, but a dynamic process. As an enterprise's data security situation changes, its credit assessment results should be adjusted accordingly. This requires the assessment organization to review the enterprise's data security status on a regular or irregular basis to ensure the accuracy and timeliness of the assessment results.
(3) Strengthen the publicity and promotion of data security credit assessment. In order to make more enterprises realize the importance of data security credit assessment, the government and the community should strengthen the publicity and promotion of data security credit assessment. By organizing training, seminars and other activities, it can raise enterprises' awareness of and attention to data security credit assessment. At the same time, advanced experience and typical cases of data security credit assessment can be widely publicized through the media and other channels to form a favorable social atmosphere.

#### 4.5.2. Promoting technological collaboration

In the practice of data security governance, technology collaboration plays a crucial role. Technical collaboration can not only effectively improve the efficiency of data security protection, but also significantly reduce the cost of data security governance. In view of the trilateral evolutionary game model constructed in this paper and its analytical results, the following suggestions are put forward, aiming at reducing the cost of data security governance through technological synergy.

(1) Establish unified technical standards and frameworks. In the field of data security governance, the establishment of unified technical standards and frameworks is the foundation of technical synergy. Government administrations should take the lead in formulating and improving relevant standards to ensure that digital service platforms and third-party testing organizations follow unified technical specifications in the process of data security testing, assessment and management. This will help reduce additional costs due to technical differences and improve the overall efficiency of data security governance.
(2) Implement a risk-sharing mechanism. In order to motivate the private sector in the area of data security R&D, an effective risk-sharing mechanism needs to be constructed. The government can adopt a series of measures, such as providing R&D insurance

to reduce the economic risks faced by enterprises due to R&D failures, or setting up a special venture capital fund for supporting high-risk but potentially high-return data security technology R&D projects. In addition, the government should also actively lead or participate in the formulation of technical standards in the field of data security, provide clear guidance and direction for private sector R&D activities, and ensure that R&D results are in line with market demand and industry norms. In this way, not only can the private sector's confidence in data security R&D be enhanced, but also the success rate and economic benefits of R&D projects can be improved, thus realizing a risk-sharing and mutually beneficial situation.

(3) Explore cross-border data flow security paradigm. Strengthening international technical cooperation and exchanges is of great significance in reducing the cost of data security governance. China can actively participate in the formulation and revision of international data security standards, strengthen data flows with other economies, and promote the convergence of domestic standards with international standards. For example, China has actively applied to join the Comprehensive and Progressive Trans-Pacific Partnership Agreement and the Digital Economy Partnership Agreement, which are high-standard regional trade agreements.

#### *4.5.3. Optimizing the governance structure*

By establishing a national data security governance center that covers a wide range of regions and a variety of information types, it is possible to promote information sharing and exchange among provinces, thereby deepening inter-provincial coordination and cooperation. Such a platform will help regions share successful experiences and advanced technologies in the field of data security management and provide guidance and support for field activities. The National Governance Center will compile best practices distilled from successful cases by professional scholars and institutions and promote them to provinces, helping third-party testing organizations gain a deeper understanding of data security governance strategies and actively participate in and work together to enhance the security level of the cyber environment. While promoting national data security governance, such a center will also work to promote a harmonious balance between development and security, ensuring that the two go hand in hand and move forward together.

(1) Clarify the responsibilities and rights of each participating entity. Ensure that their roles in the data security governance process are clearly defined. Digital service platforms, as the main collectors and users of data, should assume the main responsibility of protecting user data security, strengthening data security management, and ensuring the legal and compliant use of data. As an independent third party, the third-party testing organization should provide objective and impartial data security testing services to provide a basis for decision-making by the government management. For its part, the government administration should formulate and implement data security policies, supervise and manage the behavior of digital service platforms and third-party testing agencies, and ensure the overall advancement of data security governance.

(2) Establish synergistic governance channels. Two-way communication should be strengthened between governance subjects, communication channels should be opened up, the cognition of each subject to the data governance system should be improved, and governance subjects should be incentivized to identify with and participate in digital security governance. At the same time, cross-functional coordination and collaboration between different departments should be strengthened, which can be done by setting up a joint working group and establishing an information sharing platform.

(3) Improve legal and institutional construction. Government management should improve data security governance procedures based on the full life cycle of data, improve regulations on data ownership, improve the data security management system, and build a legal and institutional framework system integrating civil, criminal and administrative aspects. At the same time, digital service platforms and third-party testing organizations should be regularly inspected and evaluated, and problems should be dealt with and corrected in a timely manner, so as to ensure the implementation and enforcement of data security governance policies.

## 5. Conclusions

### *5.1. Conclusions of the research*

The importance of data security in the digital ecosystem cannot be overstated, as it constitutes the cornerstone of the digital world and provides a solid guarantee for various information technology applications and business processes. Data security governance can provide a set of comprehensive and systematic methods for subjects to manage and protect their data assets, ensure data confidentiality, integrity, and availability, and prevent data leakage, misuse, or damage, so as to maintain an organization's business continuity, customer trust, and legal compliance, and thus promote the long-term and stable development of each subject. This study explores the interactions among third-party testing organizations, digital service platforms, and government administrations and their strategic choices by analyzing the evolutionary game in the field of data security governance. On the basis of theoretical analysis and empirical research, the heterogeneous influence of different factors on data security governance is scrutinized.

The study points out that in the game process of data security governance, key elements, such as hidden gains, government subsidies and negative externality losses, have a significant and positive role in promoting the robust development of digital ecology. Within a reasonable range, these parameters can positively incentivize the participants to adopt desirable action strategies and gradually lead the system to a stable state. Specifically, increasing implicit revenue can strengthen the self-discipline and sense of responsibility of digital service platforms, motivate them to provide more high-quality digital products, and further improve data encryption and access control mechanisms. Therefore, increasing the revenue that digital service platforms receive by providing high-

quality products and reducing their production costs are effective means to prevent digital service platforms from slacking off in their data security governance. At the same time, the government regulator's strategy of subsidizing third-party testing organizations can also significantly enhance the latter's willingness to reject improper practices and ensure the reliability of testing results. However, this subsidy needs to be more than the sum of the costs and fine revenues invested by the testing organizations in data security governance to play a significant role in ensuring that data security is safeguarded in an evolutionarily stable market environment. In addition, low negative externality losses and high contingency costs reduce the probability that government regulators will choose a strict regulatory strategy to address data security threats. However, given that the core responsibility of government regulators is to protect the public interest and national security, as long as the cost of strict regulation is affordable, government regulators are still inclined to adopt a "strict regulation" strategy.

The probability of data security incidents has a significant impact on the operation of the digital ecosystem. Depending on the situation, we can categorize them into two main scenarios. First, when the probability of data security incidents is in the low range, it means that the data security risk is relatively low and the market environment is relatively robust. In this scenario, digital service platforms tend to choose to provide high-quality digital products as their main behavioral strategy, while third-party testing organizations tend to reject any form of rent-seeking behavior in order to maintain the fairness and transparency of the market. However, at this time, the behavioral strategies of government regulators have not yet reached a stable state, with no obvious strategic tendency, and may be flexibly adjusted according to the specific situation. On the other hand, when the probability of a data security event is in the mid-to-high range, it indicates a high data security risk and a relatively volatile market environment. In this scenario, all three participants adopted active and positive behavioral strategies to cope with the challenges. Digital service platforms continue to provide high-quality digital products, third-party testing organizations firmly reject rent-seeking, and government regulators opt for strict supervision to ensure data security. This common positive behavioral strategy helps stabilize the digital ecosystem in a volatile market environment and reduces potential security risks. This leads to different governance models in different environments as follows:

(1) In a robust market environment, strengthening the regulation of third-party testing organizations is particularly critical due to the low risk of data crises. Government regulators vary in their regulatory costs in response to different data crisis events. Typically, as the cost of regulation rises, the likelihood of regulators adopting a strict regulatory strategy decreases. However, government regulators are still willing to incur these costs to a certain extent in the interest of maintaining the overall well-being of society. A secure data environment can bring about many positive externality benefits, but at the same time, it may also induce third-party testing organizations to exploit the testing data of other people or other organizations, thereby potentially disrupting the market. To prevent this potential market disruption, government regulators can incentivize and guide third-party testing organizations to actively participate in the data security governance process by setting clear industry guidelines, using official media to report on the issue, and taking punitive interventions or coercive measures when necessary.
(2) Enhancing the self-regulation of digital service platforms and third-party testing organizations is particularly urgent in the turbulent and volatile market environment. In order to enhance the willingness of digital service platforms to self-regulate, emphasis should be placed on increasing their hidden benefits, such as security, word-of-mouth reputation and political resources. The subsidy mechanism established should be sufficient to cover the costs incurred by third-party testing organizations in the process of self-regulation, thus stimulating their self-regulatory motivation. The governance strategies of digital service platforms are closely related to the implicit benefits of their self-regulation, and this correlation is particularly significant in a dynamically changing data environment. When the implicit gains increase, the platform's willingness to govern will also increase. At the same time, government regulators' implementation of a reasonable subsidy incentive mechanism is of inestimable value in enhancing the willingness of third-party testing organizations to reject rent-seeking and maintain data security. The strategic choice of third-party testing organizations is deeply influenced by the reward and punishment policies of government regulators. When policy subsidies can balance the benefits and costs of governance, third-party testing organizations are more likely to choose to reject rent-seeking, which will have a positive and far-reaching impact on the healthy development of the digital ecosystem.

### *5.2. Research shortcomings and prospects*

Data security governance is an evolving process, profoundly influenced by multiple factors such as technological innovations, regulatory changes, and market trends. Under this dynamic background, the interest patterns and strategy choices of all parties are also transformed. In order to gain a deep insight into these changes, the construction of an evolutionary game model has become an effective tool. The model not only helps to theoretically analyze the behavioral patterns and strategic choices of digital service platforms, third-party testing organizations, and government regulators in data security governance, but also systematically reveals the interests, potential conflicts, and opportunities for cooperation among them. Considering the intricate interactions among these three, an evolutionary game model can be used for better simulation demonstration. The research model enables us to predict the potential impact of different interests on data security governance by evaluating their behaviors and strategies in specific contexts, thus providing valuable references and strategy suggestions for decision makers.

And MATLAB simulation simulates the dynamic evolution process through parameter setting, which makes the simulation results closer to the real situation. Meanwhile, different factors can be controlled and adjusted during the simulation process, such as strengthening preferential policy subsidies, improving governance technology investment, strengthening supervision, etc., to observe the trend of change and evolution law of the behavior of all parties' interests, and improve the controllability and reliability of the simulation. Through simulation, researchers can model the effect of data security governance in various situations, quantify the

advantages and disadvantages of different strategies, and more accurately predict the future development trend. This provides government regulators, platform service enterprises and other interested parties with a scientific basis for decision-making, helping them to formulate more reasonable, effective and forward-looking data security governance strategies and measures. However, it may not be able to fully cover all the pending issues when dealing with data security, which is mainly due to the following limitations and challenges, and the limitations that exist will be the focus of future research:

(1) The strategy setting of the evolutionary game model is simple. It may be reflected in the failure to fully consider the dynamic adjustment of the strategies of the parties and the complex interactions among them, and these complex interactions may be simplified or ignored, resulting in the model failing to accurately reflect the complexity and dynamics of data security governance in the real world, which may be quite different from the actual situation. In addition, the setting may also ignore the impact of external environmental factors (e.g., technological development, changes in laws and regulations, etc.) on the strategic choices of participants, which reduces the predictive power and usefulness of the model. A more in-depth understanding of the governance mechanisms that encompasses more practically possible behaviors and responses could provide a more comprehensive and in-depth analysis.
(2) In the process of data security governance, the human factor often plays a non-negligible role, which is then missing from the paper without consideration. First, due to the subjectivity and behavioral diversity of human beings, the formulation and implementation of data security governance strategies are easily affected by individual bias and experience, resulting in strategies that are not comprehensive enough or deviate from the actual needs. Second, irregularities or mistakes in human operations may lead to data leakage, loss or misuse, posing a threat to the privacy and rights of users of digital service platforms. Furthermore, personnel from third-party testing organizations and government administration may relax their supervision of digital service platforms due to interest entanglements or professional ethics, leaving data security issues undetected and unresolved in a timely manner. In addition, human factors may also lead to poor information communication and inefficient decision-making in the data security governance process, thus affecting the overall effect of data security governance. In this paper, due to the limitations of research resources and time, the complex interactions among factors in data security governance and their specific impact on game dynamics have not yet been analyzed in depth. In order to more precisely reveal the dynamic changes in the process of data security governance, future research can apply the system dynamics approach and combine the theories of behavioral economics and psychology to explore in detail the interactions and feedback mechanisms among different factors, especially how irrational factors substantially affect the decision-making behaviors and outcomes of the participants. Through this approach, it is expected to gain a more profound and comprehensive understanding of data security governance issues.

## Funding statement

This research was funded by the National Social Science Foundation of China (21BGJ037).

## Data availability statement

Data will be made available on request.

## CRediT authorship contribution statement

**Zhen Tian:** Writing – review & editing, Methodology, Conceptualization. **Meng Han:** Writing – original draft, Validation, Software, Methodology. **Chuchu Jiang:** Writing – original draft, Validation, Software.

## Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

## Acknowledgments

The authors thank the editors and reviewers.

## References

[1] China, T.N.P.s.C.o.t.P.s.R.o. Data Security Law of the People's Republic of China. Available online: http://www.npc.gov.cn/npc/c2/c30834/202106/t20210610_311888.html (accessed on 2024-June-18).
[2] Y. Zhou, Research on current situation and governance system of enterprise data security governance, J. Entrepren. Sci. Technol. 37 (2024) 170–173.
[3] Henan Shushuo Safety Research Institute Co, L. *Data Security Market Research Report*, 2022.
[4] Duan, L. Continue to deepen the market-oriented reform of data elements. Available online: https://theory.gmw.cn/2022-09/21/content_36038476.htm (accessed on 2024-June-18).

[5] Gao, F. Building a mechanism for authorization of data classification and hierarchical rights. Available online: https://www.ndrc.gov.cn/xxgk/jd/jd/202212/t20221219_1343664.html (accessed on 2024-June-18).
[6] J. Dai, Analytical framework of the identification and prevention of potential risks in open government data: a process-based research, J. Intell. 38 (2019) 145–151.
[7] W.Y.M. Haiqun, Several problems on public data security guarantee from perspective of data elements, J. Mod. Inf. (2024) 1–13.
[8] M. Nicho, A process model for implementing information systems security governance, Inf. Comput. Secur. 26 (2018) 10–38, https://doi.org/10.1108/ICS-07-2016-0061.
[9] S. Schinagl, A. Shahim, What do we know about information security governance? Inf. Comput. Secur. 28 (2020) 261–292, https://doi.org/10.1108/ICS-02-2019-0033.
[10] E. McFadzean, J.N. Ezingeard, D. Birchall, Perception of risk and the strategic impact of existing IT on information security strategy at board level, Online Inf. Rev. 31 (2007) 622–660, https://doi.org/10.1108/14684520710832333.
[11] T. Kayworth, G. Whitten, Effective information security requires a balance of social and technology factors, MIS Q. Exec. 9 (2010).
[12] Q.Q.P.Z.L. Xiaowei, Date security protection system in the wave of global digital Economy. Information Security and Communications Privacy, 2020, pp. 67–81.
[13] S. AlGhamdi, W. Khin Than, E. Vlahu-Gjorgievska, Information security governance challenges and critical success factors: systematic review, Comput. Secur. 99 (2020), https://doi.org/10.1016/j.cose.2020.102030.
[14] S. Schinagl, A. Shahim, What do we know about information security governance? "From the basement to the boardroom": towards digital security governance, Inf. Comput. Secur. 28 (2020) 261–292, https://doi.org/10.1108/ics-02-2019-0033.
[15] S. Schinagl, S. Khapova, A. Shahim, Tensions that Hinder the Implementation of Digital Security Governance, 2021, pp. 430–445. Cham.
[16] S.X.G. Daosheng, Research on data security governance in open sharing of scientific data, Libr. Inf. Serv. 64 (2020) 25–36, https://doi.org/10.13266/j.issn.0252-3116.2020.22.003.
[17] T.H. Tan, S.B. Maynard, A. Ahmad, T. Ruighaver, Information security governance: a case study of the strategic context of information security, in: Proceedings of the PACIS, 2017, p. 43.
[18] S.H. Kim, J. Kwon, How do EHRs and a meaningful use initiative affect breaches of patient information? Inf. Syst. Res. 30 (2019) 1184–1202, https://doi.org/10.1287/isre.2019.0858.
[19] J. Gabriel, S.M.A. Latheef, V. Jayavardhanavelu, Issues on management and governance of data security in HEIs, J. Trend in Sci. Res. Dev. 1 (2018) 243–247.
[20] P.H.H. Zhen, On the realistic dilemma and coping strategies of government data security governance in the context of artificial intelligence, Soc. Sci. Yunnan (2022) 29–37.
[21] L. Masilela, D. Nel, The role of data and information security governance in protecting public sector data and information assets in national government in South Africa, Afr. Pub. Ser. Deliv. Perform. Stu. Prac.Rev. 9 (2021) 385.
[22] R. Ying, Research on the innovation of public health data security governance, Study and Practice (2020) 72–80, https://doi.org/10.19624/j.cnki.cn42-1005/c.2020.08.010.
[23] W.C.J. Jie, Multi -dimensional Logic of Cross -border Data Security Governance and China's Response, Library & Information, 2022, pp. 26–33.
[24] G.D.J. Yan, Personal information security governance strategies in the era of artificial intelligence, Inf. Sci. 39 (2021) 53–59, https://doi.org/10.13833/j.issn.1007-7634.2021.08.007.
[25] H.W.G.Z.J. Wenjun, Data advantages of platform enterprises and consumer privacy protection———from the perspective of tripartite game between Government,Platform enterprises and consumers under data empowerment, Econ. Rev. J. (2022) 59–69, https://doi.org/10.16528/j.cnki.22-1054/f.202212059.
[26] R. Bellanova, M. Goede, Co-Producing security: platform content moderation and European security integration, J. Commun. Media Stud.: J. Common. Mark. Stud. 60 (2021), https://doi.org/10.1111/jcms.13306.
[27] A.K.W. a.o, 3Competence–Control theory: the challenge of governing through intermediaries, The Governor's Dilemma: Indirect Governance Beyond Principals and Agents (2020), https://doi.org/10.1093/oso/9780198855057.003.0001, 0.
[28] D. Mügge, The securitization of the EU's digital tech regulation, J. Eur. Publ. Pol. 30 (2023) 1431–1446, https://doi.org/10.1080/13501763.2023.2171090.
[29] W.X.W. Weijia, The mechanism and governance path of misconduct of third party testing institutions, Sci. Technol. Econ. 37 (2024) 81–85, https://doi.org/10.14059/j.cnki.cn32-1276n.2024.01.008.
[30] Z.Y.L. Peng, Common agency and the failure in regulatory governance: an empirical study on the third-party testing services entrusted by enterprise, J. Public Adm. 15 (2022) 69–88+198.
[31] N. Selling, The long shadow of lobbying: ideational power of lobbying as illustrated by welfare profits in Sweden, Interest Groups Advocacy 10 (2021) 47–67, https://doi.org/10.1057/s41309-021-00111-6.
[32] Z.Z.W. Lihong, Current situation and trend of private third-party testing service in China, Anal. Test. Technol. Instrum. 29 (2023) 334–338, https://doi.org/10.16495/j.1006-3757.2023.03.014.
[33] Z.L.S. Shuhui, Tripartite evolution game and simulation analysis of food quality and safety supervision under consumer feedback mechanism, J. Chongqing Univ. (Nat. Sci. Ed.) 25 (2019) 94–107.
[34] W.Y.F. Hua, Dual supervision of the platform Economy: private supervision and public supervision, Economist (2017) 73–80, https://doi.org/10.16158/j.cnki.51-1312/f.2017.11.009.
[35] L. Enquan, X. Shuwen, Y. Yanlong, N. Sethi, A stochastic and time-delay evolutionary game of food safety regulation under central government punishment mechanism, Heliyon 10 (2024) e30126, https://doi.org/10.1016/j.heliyon.2024.e30126.
[36] X. Hui, Construction of a tripartite game model for emergency management of public emergencies, Stat. Decis. 36 (2020) 164–168, https://doi.org/10.13546/j.cnki.tjyjc.2020.22.037.
[37] M. Wang, S. Lian, S. Yin, H. Dong, A three-player game model for promoting the diffusion of green technology in manufacturing enterprises from the perspective of supply and demand, Mathematics 8 (2020) 1585.
[38] X.Y. Zhou, Z.Z. Li, Y. Liu, F. Zhao, G.Z. Feng, S.Y. Wanag, Tripartite cooperation evolutionary strategy of industrial Internet platform, developer and enterprise: the role of government subsidies and revenue sharing, Chin. J. Manag. Sci. 32 (2024) 276–287, https://doi.org/10.16381/j.cnki.issn1003-207x.2021.2558.
[39] Q.X.H. Guisheng, Governance of platform information security based on tripartite evolutionary game, J. Mod. Inf. 40 (2020) 114–125.
[40] L.P.F.B.J. Ruitao, Research on strategy of public safety governance: a case study of the generation of violence events and the spread of relevant public opinion, China Soft Sci. (2017) 47–55.
[41] D.L. Deephouse, Media reputation as a strategic resource: an integration of mass communication and resource-based theories, J. Manag. 26 (2000) 1091–1112.
[42] A. Jøsang, R. Ismail, C. Boyd, A survey of trust and reputation systems for online service provision, Decis. Support Syst. 43 (2005) 618–644.
[43] P. Resnick, R. Zeckhauser, Trust among strangers in Internet transactions: empirical analysis of eBay's reputation system, in: The Economics of the Internet and E-Commerce, Emerald Group Publishing Limited, 2002, pp. 127–157.