Lv, Yali; Yang, Jian; Sun, Xiaoning; Wu, Huafei

Article

Evolutionary game analysis of stakeholder privacy management in the AIGC model

Operations Research Perspectives

Provided in Cooperation with:
Elsevier

Suggested Citation: Lv, Yali; Yang, Jian; Sun, Xiaoning; Wu, Huafei (2025) : Evolutionary game analysis of stakeholder privacy management in the AIGC model, Operations Research Perspectives, ISSN 2214-7160, Elsevier, Amsterdam, Vol. 14, pp. 1-14, https://doi.org/10.1016/j.orp.2025.100327

This Version is available at:
https://hdl.handle.net/10419/325804

Operations Research Perspectives 14 (2025) 100327

Contents lists available at ScienceDirect

Operations Research Perspectives

journal homepage: www.elsevier.com/locate/orp

Evolutionary game analysis of stakeholder privacy management in the AIGC model

Yali Lv, Jian Yang *, Xiaoning Sun, Huafei Wu

School of Information, Shanxi University of Finance and Economics, Taiyuan, 030006, Shanxi, China

ARTICLE INFO

Keywords:
AIGC
Data privacy
Evolutionary game
Replicator dynamic equations

ABSTRACT

The technological development powered by Artificial Intelligence Generated Content (AIGC) models, exemplified by Generative Pre-trained Transformer 4 (GPT-4) and Bidirectional Encoder Representations from Transformers (BERT), has completely transformed machine language processing and fostered substantial technological advancements. However, their extensive deployment has amplified concerns regarding data privacy risks, which are attributed not only to technological vulnerabilities but also to the intricate conflicts of interest among model providers, application service providers, and privacy regulators. To tackle this challenge, this research develops a tripartite evolutionary game model that examines the strategic interactions and dynamic relationships among large language model providers, application service providers, and privacy regulatory agencies. By employing replicator dynamic equations and Jacobian matrices, the research investigates the stability of strategic equilibria and simulates optimal adjustment paths across diverse policy scenarios. Drawing on the research findings, this paper offers practical recommendations to strengthen data privacy protection in large language models, delivering a solid theoretical foundation for policymakers and industry practitioners.

1. Introduction

Large language models as a significant breakthrough in artificial intelligence (AI) technology, are reshaping service modes across multiple domains. Artificial Intelligence Generated Content (AIGC) models represented by Generative Pre-trained Transformer 4 (GPT-4) and Bidirectional Encoder Representations from Transformers (BERT) [1] demonstrate exceptional capabilities in semantic understanding [2] and content generation [3], particularly in highly specialized fields such as medical diagnostic assistance [4] and financial analysis, significantly enhancing service efficiency and decision support capabilities through accurate comprehension of professional texts and contextual relationships [5]. These models not only handle routine language tasks but also deeply understand domain-specific requirements, bringing innovative solutions to various industries.

With the extensive application of large language models in sensitive fields such as therapy [6], education [7], and healthcare [8–10], their data security risks have become increasingly prominent. Research indicates these risks manifest in three aspects: first, potential leakage of users' personal information due to model memory mechanisms [11]; second, malicious attacks against models, including inference reconstruction [12] and exploitation of personalized configuration vulnerabilities [13]; and third, data leakage risks at the technical interface level [14]. These multi-dimensional security challenges require not only technical protection measures but also the establishment of comprehensive regulatory frameworks and industry standards.

Privacy protection for large language models is a complex systems engineering challenge involving collaboration among multiple stakeholders [15]. This system encompasses various entities including data providers, technology developers, service users, and regulatory agencies, with complex interactions and trade-offs among them [16]. Each participant's decisions and behaviors affect the overall effectiveness of privacy protection: from data providers' privacy awareness to the security design of technical solutions to the formulation and implementation of regulatory policies, all require coordination and optimization within a unified framework. This study focuses on these complex systemic characteristics, attempting to construct an analytical model that reflects the interaction mechanisms among all parties.

This study adopts evolutionary game theory (EGT) as its theoretical framework, leveraging its unique advantages in analyzing multi-agent dynamic decision processes [17–19]. By constructing a tripartite evolutionary game model, this study dynamically tracks the strategy evolution processes among large language model providers, application service providers, and regulatory agencies, while identifying the Nash equilibrium—a stable state where no party can improve its payoff by unilaterally changing its strategy [20]. The model examines several key

* Corresponding author.
E-mail address: yangj@sxufe.edu.cn (J. Yang).

https://doi.org/10.1016/j.orp.2025.100327
Received 13 September 2024; Received in revised form 13 January 2025; Accepted 5 February 2025
Available online 13 February 2025

variables, including the economic benefits of all parties, violation costs, regulatory efficiency, and the social reputation impacts. This analytical framework not only uncovers the optimal strategies for different parties under varying conditions but also predicts the long-term evolutionary trends of the system, thereby providing robust theoretical support for developing privacy protection policies that balance efficiency and security.

This study establishes a novel tripartite evolutionary game model to analyze the interaction mechanisms among large language model providers, application service providers, and privacy regulatory agencies, demonstrating significant value in both theoretical contributions and practical implications:

(a) From a theoretical perspective, the model thoroughly examines key factors such as provider profit growth rates, penalty amounts, social reputation of regulatory agencies, and regulatory costs, offering a novel analytical perspective for large-scale artificial intelligence (AI) privacy governance.
(b) From a practical standpoint, the research findings provide actionable policy recommendations for balancing compliance requirements and stakeholder incentives.

However, the study is limited by its simplified assumptions in the evolutionary game framework and reliance on simulation data, which may restrict the applicability of its findings to real-world scenarios. Further empirical research is required to enhance its generalizability and practical impact.

2. Related work

2.1. Large language models

Large language models, epitomized by ChatGPT, have showcased their astonishing emergent capabilities, further propelling technological breakthroughs in the direction of General Artificial Intelligence (AGI). In this revolutionary shift within the AI paradigm, the academic, industrial, and research communities are actively exploring and studying the potential of large language models, embarking on a series of experiments and applied research.

Vaswani, A et al. [21] introduced the self-attention mechanism in their proposed Transformer architecture, a significant innovation that enhanced the capabilities of NLP and laid the foundation for the training of large language models. Ouyang [22] built upon the GPT-3 architecture, incorporating instruction based learning and reinforcement learning from human feedback to guide the model's training utilizing fine tuning and policy alignment and successfully developed InstructGPT and ChatGPT. Zeng et al. [23] have trained the PanGu-alpha large-scale autoregressive language model, which shows remarkable capabilities in various scenarios based on massive high-quality Chinese industry data within the MindSpore framework.

In the research and development of large language models, studies on data privacy protection and corresponding AI governance are of paramount importance. Xu et al. [24] reviewed key privacy-preserving machine learning (PPML) techniques, such as differential privacy, homomorphic encryption, and secure multi-party computation. They identified significant challenges, including high computational costs, scalability limitations, and trade-offs between privacy and utility, while proposing strategies to integrate these techniques into large-scale AI systems. Li et al. [25] conducted a comprehensive analysis of privacy attacks and defense strategies for large language models, categorizing the types of attacks based on the capabilities of potential attackers and revealing critical vulnerabilities within LLMs. Previous studies have demonstrated that attackers can extract or reconstruct precise training samples from LLMs, potentially leading to the leakage of personal identity information. To mitigate this risk, Rehnia et al. [26] proposed a novel framework known as EW-Tune. This framework employs advanced gradient perturbation techniques to safeguard a limited number of samples while introducing minimal noise. Kandpal N et al. [27] discovered that reducing duplicate data in the training sets of large language models significantly decreases the likelihood of privacy breaches when handling sensitive information, thereby enhancing the overall security of the models regarding data privacy. Recent advancements in privacy-preserving computation technologies have further expanded this field. For instance, Xu et al. [28] proposed a federated learning framework that incorporates privacy-preserving data pricing, ensuring sensitive data remains protected while enabling equitable valuation across stakeholders. This approach underscores the potential of integrating advanced privacy-preserving mechanisms into large language model ecosystems to balance data utility and privacy in multi-stakeholder scenarios. Rajagopal M et al. [29] introduced a conceptual framework for AI governance in public administration, combining regulatory theory and ethical principles. The framework emphasizes transparency, accountability, and stakeholder collaboration while addressing challenges such as bias, privacy concerns, and the complexity of AI systems.

2.2. Game theory

Game theory has become a widely used tool [30,31]. Scholars in academia have analyzed the game behavior of various stakeholders in different scenarios, providing solid theoretical support for logical decision-making processes within these fields. Zhang et al. [32] proposed a game-theoretic framework for privacy-preserving federated learning, referred to as the Federated Learning Privacy Game. This framework considers the strategic interactions between defenders and attackers, accounting for computational costs, model utility, and privacy leakage risks. By addressing incomplete information scenarios, the study provides a structured approach to balancing privacy protection and performance in federated learning environments. Shah H et al. [33] reviewed the applications of game theory models in privacy protection, cybersecurity, intrusion detection, and resource optimization. Xu et al. [34] transformed the privacy issues arising from data collection, anonymization, and release into a game problem. Within this framework, they explored the interactive behaviors amongst data providers, collectors, and users, utilizing a game model based on k-anonymity to propose a general method for finding Nash equilibria.

"Free-riding" is a common behavior studied in game theory, often observed among stakeholders in supply chains where some participants benefit from shared resources or cooperative efforts without contributing proportionally to the associated costs. For example, Ju et al. [35] highlighted that in the adoption of blockchain technology within shipping supply chains, certain stakeholders may strategically avoid investing in the technology while still reaping its benefits. Sagduyu Y E et al. [36] introduces a game-theoretic framework to analyze free-riding behavior in federated learning (FL) over wireless networks. The study highlights how selfish clients, seeking to avoid computational and communication costs, engage in free-riding by not participating in model updates while still benefiting from the global model. This behavior adversely impacts the accuracy of the global model and reduces overall system utility. By formulating a non-cooperative game, the research derives Nash equilibrium strategies for free-riding probabilities and quantifies the trade-offs between participation costs and global accuracy. The results emphasize the need for incentive mechanisms to mitigate free-riding and enhance FL's resilience while preserving privacy through decentralized data sharing.

In addition to evolutionary game theory (EGT), several foundational approaches have been explored in the context of privacy protection within multi-stakeholder AI governance. Static game theory is effective for analyzing single-shot interactions with fully rational participants; however, it lacks the capacity to model the long-term evolution of strategies, rendering it unsuitable for capturing the iterative adjustments observed in dynamic multi-party scenarios like privacy investments and regulatory actions [37,38]. Agent-based modeling offers

detailed simulations of micro-level interactions and accounts for stakeholder heterogeneity, making it valuable for studying decentralized systems and emergent behaviors; yet, it lacks the theoretical generalizability and analytical precision of equilibrium-based methods like EGT, which are more adept at deriving global strategic insights. System dynamics excels at analyzing macro-level trends and modeling feedback loops and long-term system behaviors but struggles to represent the nuanced and strategic interactions among individual stakeholders essential in privacy protection and investment decisions [39,40]. In contrast, EGT addresses these limitations by modeling bounded rationality and the dynamic evolution of strategies over time, effectively capturing the interplay of competition and cooperation among stakeholders under conditions of uncertainty, thereby making it well-suited for analyzing privacy governance in AI ecosystems.

Building upon the strengths of EGT, this study explores its application to the domain of user privacy protection in the context of large language models, where dynamic and iterative interactions among stakeholders are particularly prominent. To achieve this, a tripartite evolutionary game model is developed, offering an in-depth analysis of privacy protection strategies and their evolution among key participants. Unlike traditional game theory, which assumes fully rational behavior, this study adopts the more realistic framework of bounded rationality, enabling a nuanced understanding of strategic decision-making under uncertainty. Through numerical simulations, the study further investigates how vested interests drive strategic adjustments during ongoing interactions, providing valuable insights into the challenges and opportunities of privacy governance in large language model ecosystems.

3. Basic assumptions and model construction

3.1. Model assumptions

To ensure the realism and validity of the constructed model, this study grounds its assumptions in empirical evidence and industry practices observed in the AI supply chain. Specifically, the roles of large language model providers (Participant 1), application service providers (Participant 2), and privacy regulatory authorities (Participant 3) are consistent with the stakeholder interactions described in existing literature. For instance, [41] highlights the complex dynamics among stakeholders in the large language model supply chain, including the need for coordinated investment in privacy and security measures. Similarly, [42] emphasizes the bounded rationality of stakeholders and the importance of balancing costs, benefits, and regulatory pressures. In this context, the strategic choices of these participants are modeled as evolving over time and stabilizing at optimal strategies, as summarized in Table 1.

Assumption 1. There are three key game participants in the data privacy game and investment decision-making. Firstly, large language model providers (S) possess the technology frameworks of deep learning and machine learning, large language model interfaces, as well as related storage and computational capabilities. They choose to invest in data privacy protection with a probability of x, and choose not to with a probability of $1 - x$. Secondly, application service providers (H) utilize the basic technology offered by large language model providers to provide sector-specific software solutions, support, and maintenance. They choose to invest in data privacy protection with a probability of y, and not to with a probability of $1 - y$. The third entity is privacy regulatory authorities (G). Their responsibilities include issuing privacy protection guidelines and conducting technical audits and certifications. They also have the power to investigate and penalize non-compliant behaviors, with the assumption that the probability of them enforcing strict regulation is z, and lax regulation is $1 - z$. x, y, and z are all defined within the interval $[0, 1]$.

Assumption 2. From the perspective of large language model providers, when neither they nor the application service providers invest in privacy protection, their profit is P_S. However, under the supervision of regulatory authorities, large language model providers will face a fine of F. Even if large language model providers choose to invest in privacy protection (at a cost of C_S), they cannot ensure that the privacy protection measures are 100% effective, and there is a risk of failure. This means they may still face fines of F due to privacy breaches. Nevertheless, investing in privacy protection can generally be expected to increase their profit to $(1 + \alpha_0)P_S$, where α_0 is the profit growth rate when large language model providers invest in privacy protection alone. Additionally, under strict regulation by regulatory authorities, large language model providers who invest in privacy protection may receive an additional reward subsidy of F. When large language model providers do not invest while application service providers do, they can free-ride and obtain an additional benefit of ξ_S. However, due to not investing in privacy protection themselves, there is a higher risk of privacy breaches, which may lead to fines of F.

Assumption 3. From the perspective of application service providers, when neither they nor the large language model providers invest in privacy protection, their profit is P_H. However, under strict regulation, they will face a fine of F. Even if application service providers choose to invest in privacy protection (at a cost of C_H), the privacy protection measures may not be completely effective, and there is a risk of failure, leading to the possibility that they may still face fines of F due to privacy breaches. Nevertheless, investing in privacy protection can generally be expected to increase their profit to $(1 + \beta_0)P_H$, where β_0 is the profit growth rate when application service providers invest in privacy protection alone. Furthermore, under strict regulation, application service providers who invest in privacy protection may receive an additional reward subsidy of F. When application service providers do not invest while large language model providers do, they can free-ride and obtain an additional benefit of ξ_H. However, due to not investing in privacy protection themselves, there is a higher risk of privacy breaches, which may lead to fines of F.

Assumption 4. The motivations for regulatory authorities to enforce strict regulations arise from fiscal, reputational, and ethical considerations. Strict regulation incurs a cost of C_G. Non-investing providers are penalized with a fine F, while investing providers receive an equivalent subsidy of F. Strict regulation enhances the social reputation of regulatory authorities, with an increase of R_0. In contrast, lax regulation results in no reputation gain, and ineffective regulation leads to a reputation loss of L. When all providers choose to invest, regulatory authorities achieve the maximum reputation gain, R_1, where $R_1 > R_0$.

In scenarios where regulatory authorities act as government entities, their decisions are not solely driven by fiscal or reputational factors. Ethical responsibilities, such as protecting public interests and ensuring privacy standards, may also influence their choices. While the current model simplifies this complexity by focusing primarily on reputational considerations, future extensions could incorporate additional factors (*e.g.*, ethical responsibilities or public expectations) into the decision-making framework to better reflect the multifaceted motivations of government regulators.

Assumption 5. In industrial practice, due to constraints of funding, technical challenges, and difficulties in the evaluation process, regulatory authorities are unable to comprehensively monitor strategies like privacy investment or free-riding. Therefore, the actual fines may be lower than the reputation gains due to regulation, *i.e.*, $2F < R_0$.

Assumption 6. When both large language model providers and application service providers choose to invest in privacy protection, both parties achieve a win–win situation. At this time, the profit growth rate

Table 1
Main symbols used in the paper.

Symbol	Description	Unit
x	The probability that large language model providers (S) invest in data privacy protection, with $x \in [0, 1]$	–
y	The probability that application service providers (H) invest in data privacy protection, with $y \in [0, 1]$	–
z	The probability that privacy regulatory authorities (G) enforce strict regulation, with $z \in [0, 1]$	–
P_S	The profit of large language model providers when not investing in privacy protection	Monetary Unit (*e.g.*, $)
P_H	The profit of application service providers when not investing in privacy protection	Monetary Unit (*e.g.*, $)
C_S	The investment cost of privacy protection for large language model providers	Monetary Unit (*e.g.*, $)
C_H	The investment cost of privacy protection for application service providers	Monetary Unit (*e.g.*, $)
C_G	The fiscal expenditure produced by regulatory authorities for enforcing strict regulation	Monetary Unit (*e.g.*, $)
F	The fine imposed by regulatory authorities for non-compliance	Monetary Unit (*e.g.*, $)
α_0	The profit growth rate of large language model providers when investing alone in privacy protection	Fraction (*e.g.*, 0.1)
α_1	The profit growth rate when both large language model providers and application service providers invest, $\alpha_1 > \alpha_0 > 0$	Fraction (*e.g.*, 0.1)
β_0	The profit growth rate of application service providers when investing alone in privacy protection	Fraction (*e.g.*, 0.1)
β_1	The profit growth rate when both application service providers and large language model providers invest, $\beta_1 > \beta_0 > 0$	Fraction (*e.g.*, 0.1)
ξ_S	The additional benefit that large language model providers obtain from free-riding on the investments of application service providers	Monetary Unit (*e.g.*, $)
ξ_H	The additional benefit that application service providers obtain from free-riding on the investments of large language model providers	Monetary Unit (*e.g.*, $)
R_0	The social reputation gained by regulatory authorities from enforcing strict regulation	–
R_1	The more significant social reputation gained when both providers invest, $R_1 > R_0$	–
L	The reputation loss faced by regulatory authorities due to lax regulation	–

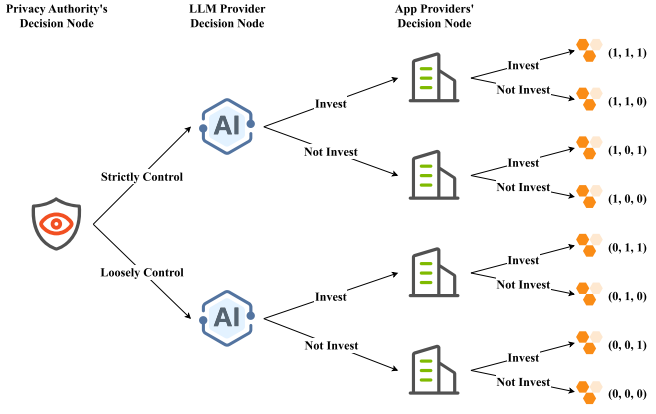


Fig. 1. Tripartite Evolutionary Game Decision Tree.

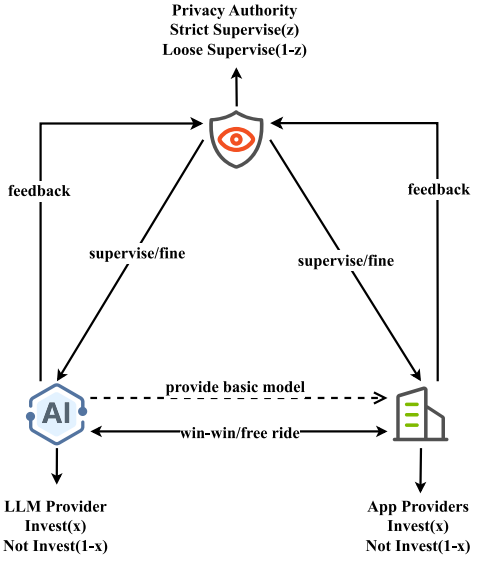


Fig. 2. Tripartite Evolutionary Game Framework.

of large language model providers increases to α_1, *i.e.*, $\alpha_1 > \alpha_0 > 0$; the profit growth rate of application service providers increases to β_1, *i.e.*, $\beta_1 > \beta_0 > 0$. Although privacy protection measures may still fail, the collaborative investment of both parties can reduce the risk of failure, enhance the overall effectiveness of privacy protection, and thereby reduce the likelihood of fines and reputational losses.

To delve deeper into strategic interactions in large language model data privacy protection, we have constructed a decision tree for evolutionary game involving three participants. As shown in Fig. 1, this decision tree illustrates the potential strategies and evolutionary paths of large language model providers, application service providers, and privacy regulatory authorities in the data privacy game. Each game participant has two choices at every decision node; these decisions unfold throughout the decision tree, eventually forming eight end-states representing the evolutionary results of the tripartite bodies under different strategy combinations. This model highlights the uncertainty of strategic choices and the complexity of strategy evolution, providing a theoretical framework for understanding and predicting the behavior patterns of each participant in data privacy protection.

3.2. Game participant relations

Fig. 2 depicts a tripartite evolutionary game model for data privacy protection, involving large language model providers, application service providers, and privacy regulatory authorities as principal players. In this framework, users and hackers play pivotal roles. Users, as data generators, supply information to both service provider categories. Conversely, hackers aim to breach these systems to pilfer critical user data, directly jeopardizing system data privacy. Large language model providers possess key technologies and computational resources, which application service providers leverage to offer tailored solutions. Their investment decisions in privacy protection are mutually dependent: if one invests and the other does not, the non-investor may indirectly benefit from the investor's commitment. However, mutual investment in privacy protection enables both to achieve a symbiotic gain, enhancing their profitability.

Privacy regulatory authorities play a critical role in this game by influencing the investment behavior of service providers through the formulation and enforcement of privacy protection policies. The strictness of their regulatory strategy is directly linked to the net benefits and investment motivations of service providers: too strict regulation may lead to fines for non-compliant providers, while reward mechanisms may encourage providers to comply with regulations. The effectiveness of the regulatory institutions not only affects the economic benefits of

Table 2
The profit and loss matrix of the three game participants.

LLM provider	App provider	Privacy authority	
		Strict regulation(z)	Lax regulation(1-z)
Invest(x)	Invest(y)	$(1+\alpha_1)P_S - C_S$ $(1+\beta_1)P_H - C_H$ $R_1 - C_G$	$(1+\alpha_1)P_S - C_S$ $(1+\beta_1)P_H - C_H$ R_1
	Not Invest(1-y)	$(1+\alpha_0)P_S - C_S + F$ $\xi_H - F$ $R_0 - C_G$	$(1+\alpha_0)P_S - C_S$ ξ_H $-L$
Not Invest(1-x)	Invest(y)	$\xi_S - F$ $(1+\beta_0)P_H - C_H + F$ $R_0 - C_G$	ξ_S $(1+\beta_0)P_H - C_H$ $-L$
	Not Invest(1-y)	$P_S - F$ $P_H - F$ $2F - C_G$	P_S P_H $-L$

the service providers but is also related to their own social credibility and authority. Effective regulation cannot only improve their reputation among the public but can also enhance social welfare; conversely, it may lead to damage to their reputation.

3.3. Model establishment

After synthesizing the assumptions and analyses proposed in Sections 3.1 and 3.2, we have constructed a detailed payoff matrix to quantitatively describe the interactions and expected payoffs of the game entities — large language model providers, application service providers, and privacy regulatory authorities — under different strategy combinations. Detailed information is outlined in Table 2.

3.3.1. Replicator dynamics equation and phase diagram for large language model providers

Based on Table 2, it is known that large language model providers face two strategic choices: to invest or not invest in privacy protection.

When they choose the former, the expected payoff is E_{S1}; for the latter, it is E_{S2}. We define the specific calculation formulas for E_{S1} and E_{S2} as follows:

If choosing to invest in privacy protection, the expected payoff E_{S1} is calculated via the formula:

$$\begin{aligned} E_{S1} &= yz[(1+\alpha_1)P_S - C_S] \\ &\quad + y(1-z)[(1+\alpha_1)P_S - C_S] \\ &\quad + (1-y)z[(1+\alpha_0)P_S - C_S + F] \\ &\quad + (1-y)(1-z)[(1+\alpha_0)P_S - C_S] \\ &= P_S - C_S + P_S\,\alpha_0 + F\,z - P_S\,\alpha_0\,y + P_S\,\alpha_1\,y - F\,y\,z \end{aligned} \tag{1}$$

If choosing not to invest in privacy protection, the expected payoff E_{S2} is calculated via the formula:

$$\begin{aligned} E_{S2} &= yz[\xi_S - F] + y(1-z)\xi_S \\ &\quad + (1-y)z[P_S - F] \\ &\quad + (1-y)(1-z)P_S \\ &= P_S - F\,z - P_S\,y + \xi_S\,y \end{aligned} \tag{2}$$

Subsequently, the average expected payoff $\overline{E_S}$ for large model providers can be represented by the formula:

$$\overline{E_S} = xE_{S1} + (1-x)E_{S2} \tag{3}$$

To delve into the pathways and equilibrium points of strategy evolution for the tripartite game participants, we solve the replicator dynamics equation for large model providers:

$$\begin{aligned} F(x) = \frac{\mathrm{d}x}{\mathrm{d}t} &= x(E_{S1} - \overline{E_S}) \\ &= x(x-1)\left(C_S - P_S\alpha_0 - 2Fz - P_S y\right. \\ &\quad \left. + \xi_S y + P_S\alpha_0 y - P_S\alpha_1 y + Fyz\right) \end{aligned} \tag{4}$$

Designating $y_0 = \frac{P_S\alpha_0 - C_S + 2Fz}{\xi_S - P_S + P_S\alpha_0 - P_S\alpha_1 + Fz}$ and calculating the partial derivative of the replicator dynamics equation $F(x)$ with respect to variable x, we obtain:

$$\begin{aligned} \frac{dF(x)}{dx} &= (2x-1)\left(C_S - P_S\alpha_0 - 2Fz - P_S y + \xi_S y\right. \\ &\quad \left. + P_S\alpha_0 y - P_S\alpha_1 y + Fyz\right) \\ &= (2x-1)\left[\left(\xi_S - P_S + P_S\alpha_0 - P_S\alpha_1 + Fz\right)y\right. \\ &\quad \left. - \left(-C_S + P_S\alpha_0 + 2Fz\right)\right] \end{aligned} \tag{5}$$

If $y = y_0$, we can obtain $F(x) = 0$, where regardless of the value of x, the strategic choice of large language model providers is in a stable state.

If $y < y_0$, we can derive that $\left.\frac{dF(x)}{dx}\right|_{x=0} > 0$ and $\left.\frac{dF(x)}{dx}\right|_{x=1} < 0$, at which point $x = 1$ is an equilibrium point. When the probability of application service providers choosing "invest in privacy protection" is lower than a certain threshold, large language model providers will choose the "invest in privacy protection" strategy.

If $y > y_0$, we can deduce that $\left.\frac{dF(x)}{dx}\right|_{x=0} < 0$ and $\left.\frac{dF(x)}{dx}\right|_{x=1} > 0$, at which point $x = 0$ is an equilibrium point. When the probability of application service providers choosing to "invest in privacy protection" exceeds a certain threshold, large language model providers will opt for the "not invest in privacy protection" strategy.

According to the above analysis, the large language model providers' replication dynamic phase diagram can be obtained, as shown in Fig. 3.

3.3.2. Application service provider's replicator dynamics equation and phase diagram

For application service providers, their decision-making strategies can be divided into "investing in privacy protection" and "not investing in privacy protection". When choosing to "invest in privacy protection", the expected payoff is defined as E_{H1}; when choosing "not investing in privacy protection", the expected payoff is defined as E_{H2}. The specific formulas are:

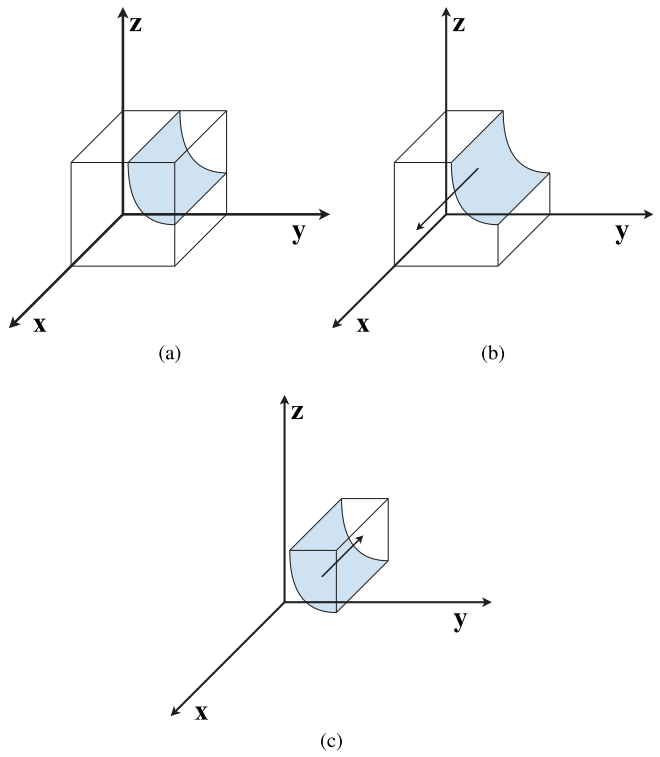


Fig. 3. Replication dynamic phase diagram of large language model providers: (a) $y = y_0$; (b) $y < y_0$; (c) $y > y_0$.

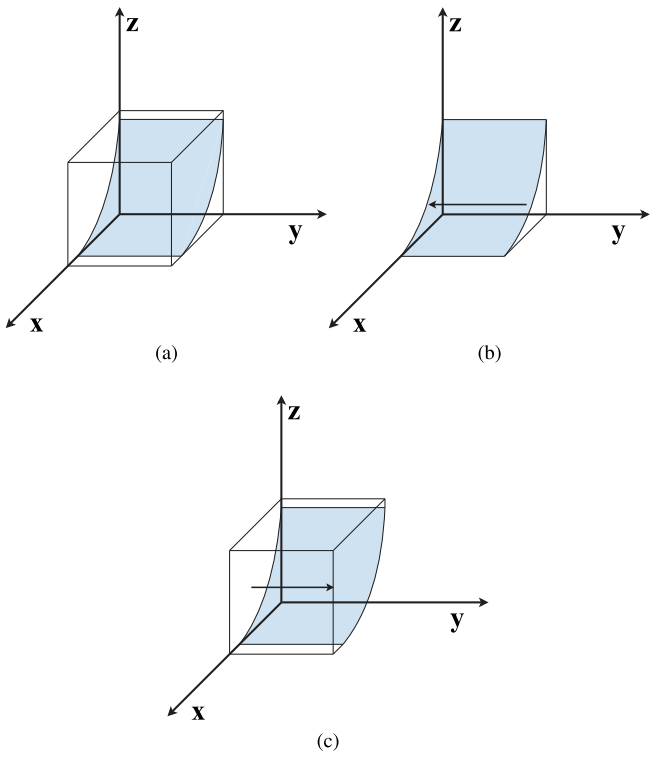


Fig. 4. Replication dynamic phase diagram of application service providers: (a) $z = z_0$; (b) $z < z_0$; (c) $z > z_0$.

If choosing to invest in privacy protection, the expected payoff E_{H1} is calculated as:

$$\begin{aligned} E_{H1} &= xz[(1+\beta_1)P_H - C_H] + x(1-z)[(1+\beta_1)P_H - C_H] \\ &\quad + (1-x)z[(1+\beta_0)P_H - C_H + F] \\ &\quad + (1-x)(1-z)[(1+\beta_0)P_H - C_H] \\ &= P_H - C_H + P_H\beta_0 + Fz \\ &\quad - P_H\beta_0 x + P_H\beta_1 x - Fxz \end{aligned} \tag{6}$$

If not choosing to invest in privacy protection, the expected payoff E_{H2} is calculated as:

$$\begin{aligned} E_{H2} &= xz[\xi_H - F] + x(1-z)\xi_H \\ &\quad + (1-x)z(P_H - F) \\ &\quad + (1-x)(1-z)P_H \\ &= P_H - F\,z - P_H\,x + x\,\xi_H \end{aligned} \tag{7}$$

The average expected payoff $\overline{E_H}$ for application service providers can be expressed by the following formula:

$$\overline{E_H} = yE_{H1} + (1-y)E_{H2} \tag{8}$$

The replicator dynamics equation for application service providers is:

$$\begin{aligned} F(y) &= \frac{\mathrm{d}y}{\mathrm{d}t} \\ &= y(E_{H1} - \overline{E_H}) \\ &= y(y-1)\left(C_H - P_H\beta_0 - 2Fz - P_H x + x\xi_H\right. \\ &\quad \left. + P_H\beta_0 x - P_H\beta_1 x + Fxz\right) \end{aligned} \tag{9}$$

Setting z_0 to make the growth rate neutral: $z_0 = \frac{C_H - P_H\beta_0 - P_H x + x\xi_H + P_H\beta_0 x - P_H\beta_1 x}{2F - Fx}$, calculating the partial derivative of the replicator dynamics equation $F(y)$ with respect to the variable y, we get:

$$\begin{aligned} \frac{dF(y)}{dy} &= (2y-1)\left(C_H - P_H\beta_0 - 2Fz - P_H x + x\xi_H\right. \\ &\quad \left. + P_H\beta_0 x - P_H\beta_1 x + Fxz\right) \\ &= (2y-1)\left[(Fx - 2F)\,z + C_H - P_H\beta_0\right. \\ &\quad \left. - P_H x + x\xi_H + P_H\beta_0 x - P_H\beta_1 x\right] \end{aligned} \tag{10}$$

If $z = z_0$, we have $F(y) = 0$, so no matter the value of y, the strategic choice of the application service provider is in a stable state.

If $z < z_0$, $\left.\frac{dF(y)}{dy}\right|_{y=0} < 0$ and $\left.\frac{dF(y)}{dy}\right|_{y=1} > 0$, thus at $y = 0$ there is an equilibrium point. When the probability of the regulatory body choosing a "strict regulation" strategy is below a specific threshold, the application service provider will choose the "not investing in privacy protection" strategy.

If $z > z_0$, $\left.\frac{dF(y)}{dy}\right|_{y=0} > 0$ and $\left.\frac{dF(y)}{dy}\right|_{y=1} < 0$, thus at $y = 1$ there is an equilibrium point. When the probability of the regulatory body choosing a "strict regulation" strategy exceeds a certain threshold, the application service provider will choose the "investing in privacy protection" strategy.

According to the above analysis, the application service providers' replication dynamic phase diagram can be obtained, as shown in Fig. 4.

3.3.3. Regulatory authority's replicator dynamics equation and phase diagram

For privacy regulatory authorities, when implementing the strategy of "strict regulation", the expected payoff is defined as E_{G1}; while implementing "lax regulation", the expected payoff is E_{G2}. The formulas are:

$$\begin{aligned} E_{G1} &= xy\left[R_1 - C_G\right] \\ &\quad + x(1-y)\left[R_0 - C_G\right] \\ &\quad + (1-x)y\left[R_0 - C_G\right] \\ &\quad + (1-x)(1-y)\left[2F - C_G\right] \end{aligned} \tag{11}$$

$$\begin{aligned} E_{G2} = {} & xyR_1 \\ & + x(1-y)[-L] \\ & + (1-x)y[-L] \\ & + (1-x)(1-y)[-L] \end{aligned} \tag{12}$$

To fully evaluate the impact of these strategies, we calculate the average expected benefit $\overline{E_G}$ for the regulatory authorities using the following formula:

$$\overline{E_G} = zE_{G1} + (1-z)E_{G2} \tag{13}$$

The replicator dynamics equation for the regulatory authority is:

$$F(z) = \frac{dz}{dt} = z(E_{G1} - \overline{E_G}) \tag{14}$$

Setting x_0 to make the growth rate neutral: $x_0 = \frac{2F - C_G + L - 2Fy + R_0 y}{2F - R_0 - 2Fy + Ly + 2R_0 y}$, calculating the partial derivative of the replicator dynamics equation $F(z)$ with respect to the variable z, we obtain:

$$\begin{aligned} \frac{dF(z)}{dz} &= (2z-1)\left(C_G - 2F - L + 2Fx + 2Fy \right. \\ &\quad \left. - R_0 x - R_0 y - 2Fxy + Lxy + 2R_0 xy\right) \\ &= (2z-1)\left[\left(2F - R_0 - 2Fy + Ly + 2R_0 y\right)x \right. \\ &\quad \left. - \left(-C_G + 2F + L - 2Fy + R_0 y\right)\right] \end{aligned} \tag{15}$$

If $x = x_0$, $F(z) = 0$, and no matter the value of z, the strategy choice of the regulatory authority is in a stable state.

If $x < x_0$, $\left.\frac{dF(z)}{dz}\right|_{z=0} > 0$ and $\left.\frac{dF(z)}{dz}\right|_{z=1} < 0$, thus at $z = 1$ there is an equilibrium point. When the probability of the big language model provider choosing to "invest in privacy protection" is below a certain threshold, the regulatory authority will choose the "strict regulation" strategy.

If $x > x_0$, $\left.\frac{dF(z)}{dz}\right|_{z=0} < 0$ and $\left.\frac{dF(z)}{dz}\right|_{z=1} > 0$, thus at $z = 0$ there is an equilibrium point. When the probability of the big language model provider choosing to "invest in privacy protection" exceeds a certain threshold, the regulatory authority will choose the "lax regulation" strategy.

According to the above analysis, the privacy regulatory authorities' replication dynamic phase diagram can be obtained, as shown in Fig. 5.

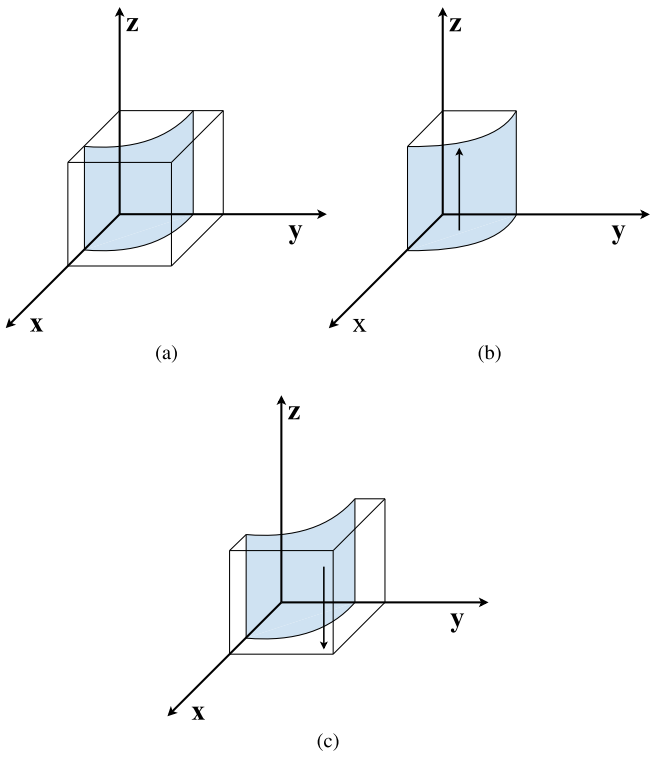


Fig. 5. Replication dynamic phase diagram of regulatory authority: (a) $x = x_0$; (b) $x < x_0$; (c) $x > x_0$.

4. Stability analysis of the model's equilibrium points

4.1. Jacobian matrix

Through Eqs. (4), (9) and (14), we derive the state equations for the tripartite game involving large language model providers, application service providers, and privacy regulatory authorities in the context of data privacy protection:

$$\begin{cases} F(x) = x(x-1)\left(C_S - P_S\alpha_0 - 2Fz - P_S y + \xi_S y + P_S\alpha_0 y - P_S\alpha_1 y + Fyz\right) \\ F(y) = y(y-1)\left(C_H - P_H\beta_0 - 2Fz - P_H x + x\xi_H + P_H\beta_0 x - P_H\beta_1 x + Fxz\right) \\ F(z) = z(z-1)\left(C_G - 2F - L + 2Fx + 2Fy - R_0 x - R_0 y - 2Fxy + Lxy + 2R_0 xy\right) \end{cases} \tag{16}$$

In system dynamics, an analysis of the eigenvalues of the Jacobian matrix is a key step in assessing local stability. The determination of Evolutionarily Stable Strategy (ESS) often relies on a local stability analysis of the Jacobian matrix near the equilibrium point. Specifically, an equilibrium point's ESS is considered stable only if all eigenvalues of its Jacobian matrix are negative; otherwise, the equilibrium point is considered unstable. On this theoretical basis, we first derive the Jacobian matrix based on Formula (16) and further use Lyapunov's method to conduct a comprehensive assessment of the stability of each equilibrium point in the game system, providing a strict mathematical foundation for the system's stability analysis. The Jacobian matrix is shown in Formula (17):

$$J = \begin{bmatrix} j_{11} & j_{12} & j_{13} \\ j_{21} & j_{22} & j_{23} \\ j_{31} & j_{32} & j_{33} \end{bmatrix} \tag{17}$$

Among them,

$$\begin{aligned} j_{11} &= (2x-1)(C_S - P_S\alpha_0 - 2Fz - P_S y + \xi_S y + P_S\alpha_0 y \\ &\quad - P_S\alpha_1 y + Fyz) \\ j_{12} &= x(x-1)(\xi_S - P_S + P_S\alpha_0 - P_S\alpha_1 + Fz) \\ j_{13} &= Fx(x-1)(y-2) \\ j_{21} &= y(y-1)(\xi_H - P_H + P_H\beta_0 - P_H\beta_1 + Fz) \\ j_{22} &= (2y-1)(C_H - P_H\beta_0 - 2Fz - P_H x + x\xi_H + P_H\beta_0 x \\ &\quad - P_H\beta_1 x + Fxz) \\ j_{23} &= Fy(x-2)(y-1) \\ j_{31} &= z(z-1)(2F - R_0 - 2Fy + Ly + 2R_0 y) \\ j_{32} &= z(z-1)(2F - R_0 - 2Fx + Lx + 2R_0 x) \\ j_{33} &= (2z-1)(C_G - 2F - L + 2Fx + 2Fy - R_0 x - R_0 y \\ &\quad - 2Fxy + Lxy + 2R_0 xy) \end{aligned}$$

4.2. Stability analysis

4.2.1. Eigenvalues at equilibrium points

By inserting the 8 local equilibrium points into the Jacobian matrix and following the assumptions provided, we obtain the respective eigenvalues for each equilibrium point. The results are as shown in the Table 3.

The table clearly demonstrates a significant relationship between parameters such as regulatory costs, regulatory benefits, providers' profit growth rates, and fines/subsidies, and the ESS of the three

Table 3
System equilibrium points and eigenvalues.

	λ_1	λ_2	λ_3
$E_{p1}(0,0,0)$	$P_S\alpha_0 - C_S$	$P_H\beta_0 - C_H$	$2F - C_G + L$
$E_{p2}(0,0,1)$	$2F - C_S + P_S\alpha_0$	$2F - C_H + P_H\beta_0$	$C_G - 2F - L$
$E_{p3}(0,1,0)$	$C_H - P_H\beta_0$	$L - C_G + R_0$	$P_S - C_S - \xi_S + P_S\alpha_1$
$E_{p4}(0,1,1)$	$C_G - L - R_0$	$C_H - 2F - P_H\beta_0$	$F - C_S + P_S - \xi_S + P_S\alpha_1$
$E_{p5}(1,0,0)$	$C_S - P_S\alpha_0$	$L - C_G + R_0$	$-\xi_H + P_H - C_H + P_H\beta_1$
$E_{p6}(1,0,1)$	$C_G - L - R_0$	$C_S - 2F - P_S\alpha_0$	$-\xi_H + F - C_H + P_H + P_H\beta_1$
$E_{p7}(1,1,0)$	$-C_G$	$C_S - P_S + \xi_S - P_S\alpha_1$	$\xi_H + C_H - P_H - P_H\beta_1$
$E_{p8}(1,1,1)$	C_G	$C_S - F - P_S + \xi_S - P_S\alpha_1$	$\xi_H + C_H - F - P_H - P_H\beta_1$

Table 4
Parameter values for different propositions.

	P_S	P_H	C_S	C_H	C_G	F	α_0	α_1	β_0	β_1	ξ_S	ξ_H	R_0	R_1	L
Proposition 1	30	25	10	8	44	0	0.24	1.09	0.05	0.31	70	60	5	15	20
Proposition 2	48	37	15	10	40	0	0.19	0.25	0.51	0.59	65	55	2	12	10
Proposition 3	48	37	15	10	40	0	0.41	0.49	0.19	0.62	65	55	10	110	10
Proposition 4	48	37	15	10	40	0	0.92	0.94	0.79	0.86	65	55	2	12	10
Proposition 5	48	37	15	10	33	10	0.07	0.10	0.27	0.62	65	55	30	35	10
Proposition 6	48	37	20	15	27	6	0.45	0.57	0.07	0.17	65	55	45	55	10
Proposition 7	48	37	20	15	16	6	0.00	0.30	0.01	0.10	65	55	17	22	10

major game participants. For simplification of the analysis process, we assume that there is only one regulatory authority responsible for overseeing all large language model providers and application service providers. Based on this assumption, we set parameter values under different propositions and analyze three critical parameter ranges. The parameter values are shown in Table 4.

4.2.2. When $C_G > R_0 + L$

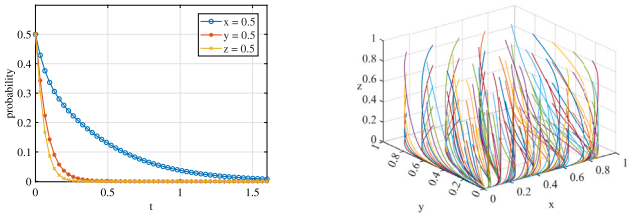
When $C_G > R_0 + L$, the regulatory authority will opt for a lax regulation policy regardless of whether the providers invest due to the high cost of regulation.

Proposition 1. *When the conditions* $0 < \alpha_0 < C_S/P_S$, $\alpha_0 < \alpha_1 < \frac{\xi_S + C_S - P_S}{P_S}$, $0 < \beta_0 < C_H/P_H$, *and* $\beta_0 < \beta_1 < \frac{\xi_H + C_H - P_H}{P_H}$ *are met, as shown in Fig. 6, the system tends to take the strategy combination of non-investment and lax regulation (0, 0, 0), which constitutes an ESS. Evaluating the cost–benefit of the investment return* $E_S(1,0,0) = (1+\alpha_0)P_S - C_S$ *for large language model providers, we find* $E_S(1,0,0)$ *to be less than the non-investment return* $E_S(0,0,0) = (1 + C_S/P_S)P_S - C_S = P_S$. *A similar cost–benefit assessment for application service providers shows that investing in data privacy protection* $E_H(0,1,0) = (1+\beta_0)P_H - C_H$ *does not exceed the straightforward return* $E_H(0,0,0) = (1 + C_H/P_H)P_H - C_H = P_H$. *In addition, the government faces a situation where regulatory costs* C_G *exceed the sum of basic fines and losses* $R_0 + L$, *which in itself is greater than twice the fines and losses* $2F + L$. *In this context, the government is more inclined to opt for lax regulation. In summary, due to limited profit margins, both large language model providers and application service providers will choose not to invest in data privacy protection, while the government opts for lax regulation. Therefore, the system will tend to evolve into a state where all parties choose not to invest and not to strictly regulate, solidifying* $(0,0,0)$ *as the system's ESS under this condition.*

Proposition 2. *When the conditions* $0 < \alpha_0 < C_S/P_S$, $\alpha_0 < \alpha_1 < \frac{\xi_S + C_S - P_S}{P_S}$, *and* $C_H/P_H < \beta_0 < \beta_1 < \frac{\xi_H + C_H - P_H}{P_H}$ *are met, as shown in Fig. 7, the system reaches the system's equilibrium point* $(0,1,0)$ *after 50 evolutions.*

If $C_G > R_0 + L$, a cost–benefit analysis of the regulatory authority yields:

$$E_G(0,1,1) = R_0 - C_G < E_G(0,1,0) \tag{18}$$



(a) The 2D evolution diagram. (b) The 3D evolution diagram.

Fig. 6. Diagram of the evolution path under Proposition 1.

In this case, the regulatory authority will enforce lax regulation. Due to $C_H/P_H < \beta_0 < \beta_1 < \frac{\xi_H + C_H - P_H}{P_H}$, a cost–benefit assessment of the investment return for application service providers is conducted:

$$\begin{aligned} E_H(0,1,0) &= (1+\beta_0)P_H - C_H \\ &> \left(1 + \frac{C_H}{P_H}\right)P_H - C_H \\ &= P_H = E_H(0,0,1) \end{aligned} \tag{19}$$

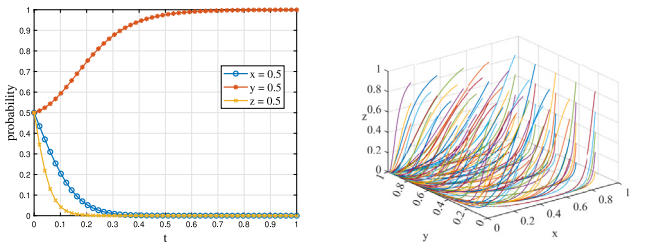
This indicates that the application service provider is inclined to undertake data privacy protection. A cost–benefit assessment of the investment return for large language model providers shows:

$$\begin{aligned} E_S(1,1,0) &= (1+\alpha_1)P_S - C_S \\ &< \left(1 + \frac{\xi_S + C_S - P_S}{P_S}\right)P_S - C_S \\ &= \xi_S = E_S(0,1,0) \end{aligned} \tag{20}$$

Therefore, the large language model provider is not inclined to invest under these conditions.

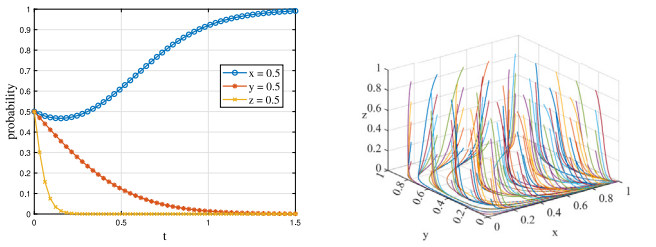
Proposition 3. *When the conditions* $C_S/P_S < \alpha_0 < \alpha_1 < \frac{\xi_S + C_S - P_S}{P_S}$, $0 < \beta_0 < C_H/P_H$, *and* $\beta_0 < \beta_1 < \frac{\xi_H + C_H - P_H}{P_H}$ *are met, as shown in Fig. 8, the system reaches the system's equilibrium point* $(1,0,0)$ *after 50 evolutions.*

Similarly, it is found that $E_G(1,0,1) = R_0 - C_G < E_G(1,0,0)$, hence the regulatory authority is inclined to choose lax regulation. Based on the given parameter range, a cost–benefit assessment of the investment returns for both large language model providers and application service



(a) The 2D evolution diagram. (b) The 3D evolution diagram.

Fig. 7. Diagram of the evolution path under Proposition 2.



(a) The 2D evolution diagram. (b) The 3D evolution diagram.

Fig. 8. Diagram of the evolution path under Proposition 3.

providers yields:

$$\begin{aligned} E_S(1,0,0) &= (1+\alpha_0)P_S - C_S \\ &> (1+C_S/P_S)P_S - C_S \\ &= P_S = E_S(0,0,0) \end{aligned} \tag{21}$$

$$\begin{aligned} E_H(1,1,0) &= (1+\beta_1)P_H - C_H \\ &< \left(1+\frac{\xi_H + C_H - P_H}{P_H}\right)P_H - C_H \\ &= \xi_H = E_H(1,0,0) \end{aligned} \tag{22}$$

Proposition 4. *When conditions* $\frac{\xi_S+C_S-P_S}{P_S} < \alpha_0 < \alpha_1$ *and* $\frac{\xi_H+C_H-P_H}{P_H} < \beta_0 < \beta_1$ *are met, as shown in Fig. 9, the system reaches the system's equilibrium point* $(1,1,0)$ *after 50 evolutions.*

Based on the assumed parameter range, a cost–benefit assessment of the investment returns for both big language model providers and application service providers yields:

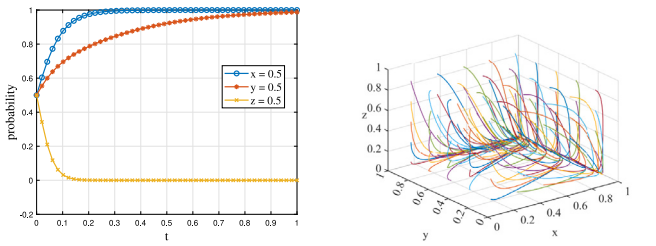
$$\begin{aligned} E_S(1,1,0) &= (1+\alpha_1)P_S - C_S \\ &> \left(1+\frac{\xi_S + C_S - P_S}{P_S}\right)P_S - C_S \\ &= \xi_S = E_S(0,1,0) \end{aligned} \tag{23}$$

$$\begin{aligned} E_H(1,1,0) &= (1+\beta_1)P_H - C_H \\ &> \left(1+\frac{\xi_H + C_H - P_H}{P_H}\right)P_H - C_H \\ &= \xi_H = E_H(1,0,0) \end{aligned} \tag{24}$$

In this case, both large language model providers and application service providers will choose to invest in data privacy protection, while the regulatory authority opts for lax regulation.

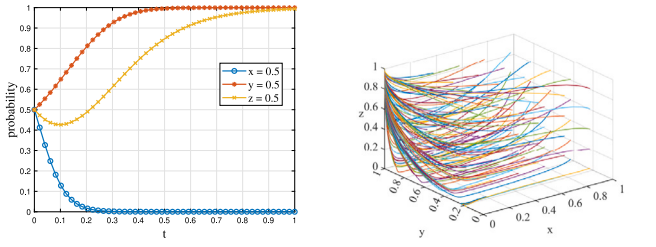
4.2.3. When $2F + L < C_G < R_0 + L$

When the regulatory costs satisfy $2F + L < C_G < R_0 + L$, the regulatory authority will adopt strict regulatory measures. In this case, if only one party among the large language model providers and application service providers invests in data privacy, then the non-investing party will face a fine.



(a) The 2D evolution diagram. (b) The 3D evolution diagram.

Fig. 9. Diagram of the evolution path under Proposition 4.



(a) The 2D evolution diagram. (b) The 3D evolution diagram.

Fig. 10. Diagram of the evolution path under Proposition 5.

Proposition 5. *When the conditions* $0 < \alpha_0 < \frac{C_S-2F}{P_S}$ *and* $\alpha_0 < \alpha_1 < \frac{\xi_S+C_S-P_S-F}{P_S}$ *as well as* $\frac{C_H-2F}{P_H} < \beta_0 < \beta_1 < \frac{\xi_H+C_H-P_H-F}{P_H}$ *are satisfied, as illustrated in Fig. 10, the system reaches the system's equilibrium point* $(0,1,1)$ *after 50 evolutions.*

Knowing C_G, a cost–benefit analysis for the regulatory authority can be performed, resulting in:

$$E_G(0,1,1) = R_0 - C_G > -L = E_G(0,1,0) \tag{25}$$

Therefore, the regulatory authority will choose strict regulation. Additionally, because $\frac{C_H-2F}{P_H} < \beta_0 < \beta_1 < \frac{\xi_H+C_H-P_H-F}{P_H}$, a cost–benefit assessment of the investment return for application service providers leads to:

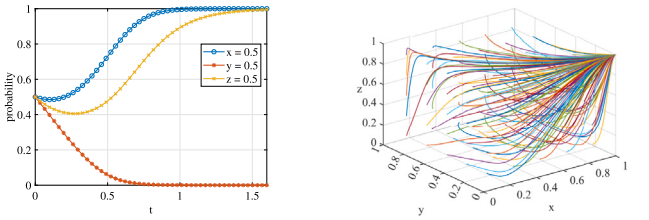
$$\begin{aligned} E_H(0,1,1) &= (1+\beta_0)P_H - C_H + F \\ &> \left(1+\frac{C_H - 2F}{P_H}\right)P_H - C_H \\ &= P_H - F = E_H(0,0,1) \end{aligned} \tag{26}$$

Furthermore, because $0 < \alpha_0 < \frac{C_S-2F}{P_S}$ and $\alpha_0 < \alpha_1 < \frac{\xi_S+C_S-P_S-F}{P_S}$, a similar cost–benefit assessment for large language model providers gives:

$$\begin{aligned} E_S(1,1,1) &= (1+\alpha_1)P_S - C_S \\ &< \left(1+\frac{\xi_S + C_S - P_S - F}{P_S}\right)P_S - C_S \\ &= \xi_S - F = E_S(0,1,1) \end{aligned} \tag{27}$$

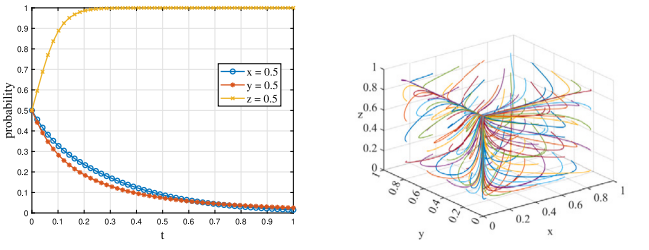
In conclusion, under this scenario, large language model providers will not invest in data privacy protection, application service providers will invest in data privacy protection, and the regulatory authority will choose strict regulation.

Proposition 6. *When the conditions* $\frac{C_S-2F}{P_S} < \alpha_0 < \alpha_1 < \frac{\xi_S+C_S-P_S-F}{P_S}$, $0 < \beta_0 < \frac{C_H-2F}{P_H}$, *and* $\beta_0 < \beta_1 < \frac{\xi_H+C_H-P_H-F}{P_H}$ *are satisfied, as depicted in Fig. 11, the system reaches the system's equilibrium point* $(1,0,1)$ *after 50 evolutions.*



(a) The 2D evolution diagram. (b) The 3D evolution diagram.

Fig. 11. Diagram of the evolution path under Proposition 6.



(a) The 2D evolution diagram. (b) The 3D evolution diagram.

Fig. 12. Diagram of the evolution path under Proposition 7.

If the condition $\frac{C_S-2F}{P_S} < \alpha_0 < \alpha_1 < \frac{\xi_S+C_S-P_S-F}{P_S}$ applies, the cost–benefit assessment for large language model providers' investment return would be:

$$\begin{aligned} E_S(1,0,1) &= (1+\alpha_0)P_S - C_S + F \\ &> \left(1+\frac{C_S-2F}{P_S}\right)P_S - C_S \\ &= P_S - F = E_S(0,0,1) \end{aligned} \tag{28}$$

If the condition $0 < \beta_0 < \frac{C_H-2F}{P_H}$ and $\beta_0 < \beta_1 < \frac{\xi_H+C_H-P_H-F}{P_H}$ applies, the assessment for application service providers' investment return would be:

$$\begin{aligned} E_H(1,1,1) &= (1+\beta_1)P_H - C_H \\ &< \left(1+\frac{\xi_H+C_H-P_H-F}{P_H}\right)P_H - C_H \\ &= \xi_H - F = E_H(1,0,1) \end{aligned} \tag{29}$$

Therefore, in this case, large language model providers will choose to invest in data privacy protection, whereas application service providers will not choose to invest in data privacy protection.

4.2.4. When $C_G < 2F + L$

Regulatory authorities consider not only the direct economic benefits when making policy decisions but also social welfare and indirect losses that may result from inadequate regulation. Therefore, when $C_G < 2F + L$, due to the low regulatory costs and potential high risks, the regulatory authority will opt for strict regulation.

Proposition 7. *When the conditions* $0 < \alpha_0 < \frac{C_S-2F}{P_S}$ *and* $0 < \beta_0 < \frac{C_H-2F}{P_H}$ *are met, as shown in Fig. 12, the system reaches the system's equilibrium point* $(0,0,1)$ *after 50 evolutions.*

Given the parameter interval condition $C_G < 2F + L$, we perform a cost–benefit analysis of the regulatory authority's return on policy enforcement:

$$E_G(0,0,1) = 2F - C_G > L = E_G(0,0,0) \tag{30}$$

Moreover, because $0 < \alpha_0 < \frac{C_S-2F}{P_S}$ and $0 < \beta_0 < \frac{C_H-2F}{P_H}$, we perform a cost–benefit analysis of the investment returns for big language model providers and application service providers, concluding that:

$$\begin{aligned} E_S(1,0,1) &= (1+\alpha_0)P_S - C_S + F \\ &< \left(1+\frac{C_S-2F}{P_S}\right)P_S - C_S + F \\ &= P_S - F = E_S(0,0,1) \end{aligned} \tag{31}$$

$$\begin{aligned} E_H(0,1,1) &= (1+\beta_0)P_H - C_H + F \\ &< \left(1+\frac{C_H-2F}{P_H}\right)P_H - C_H + F \\ &= P_H - F = E_H(0,0,1) \end{aligned} \tag{32}$$

In conclusion, under this scenario, the ESS is where both large language model providers and application service providers do not invest in privacy protection, and the regulatory authority opts for strict regulation.

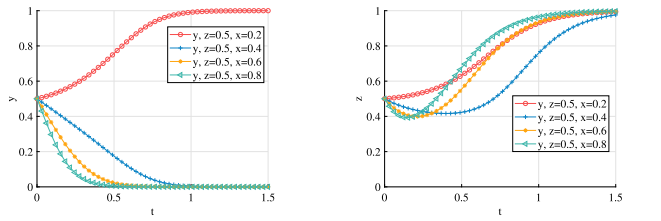
5. Simulation analysis

5.1. Initial probability analysis

In the simulation experiments, we follow the stability analysis described in the previous section, use the same initial parameters as Proposition 6, and adjust the initial probability combinations of the three parties in investment and regulation strategies in increments of 0.2 to examine the impact of different initial probabilities on the system's long-term evolutionary trends. Figs. 13, 14, and 15 show the evolutionary curves, where x represents the probability of large language model providers choosing to invest in privacy protection, y represents the probability of application service providers choosing to invest in privacy protection, and z represents the probability of privacy regulatory authorities choosing a strict regulatory policy.

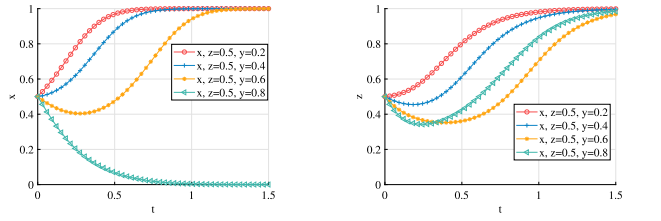
As shown in Fig. 13, when we set the initial values of y and z to 0.5, and gradually increase x from 0.2 to 0.8 in increments of 0.2, application service providers switch from a tendency to invest in privacy protection to a strategy of not investing in privacy protection. This indicates that the marginal returns on privacy protection investment decrease for application service providers as the probability of large language model providers investing increases. Therefore, application service providers tend to "free ride", benefiting from the investments of large language model providers without investing in privacy protection themselves. At the same time, the evolution speed at which application service providers take the strategy of not investing in privacy protection accelerates with the increase of x. This accelerating trend can be interpreted as large language model providers gaining a more prominent position in shaping the landscape of privacy protection as their probability of investing in it increases. This change further diminishes the marginal benefits for application service providers in investing in privacy protection, thus reducing their motivation to continue investing in privacy measures. Moreover, the evolution speed of regulatory authorities following strict regulation policies shows a dynamic evolution pattern of first decreasing and then increasing. This pattern may reflect the wait-and-see strategy adopted by regulatory authorities in the early stages of the game, where they might prefer to assess the effectiveness of their regulatory policy through market reactions. In this stage, more lenient regulation might be to facilitate the natural development of the market and collect relevant data to customize regulatory policies more accurately. As time advances and their understanding of data privacy risks deepens, regulatory authorities strengthen regulatory measures to ensure privacy security.

Fig. 14 shows the evolution of large language model providers and regulatory authorities in their privacy protection decisions when x and z are set to 0.5, and y is gradually increased from 0.2 to 0.8 in increments of 0.2. As y increases progressively, we observe a reduction in the willingness of large language model providers to invest in privacy protection strategies, ultimately shifting to a strategy of not investing in privacy protection. This strategy shift, similar to the behavior pattern



(a) Effect on the evolution of y. (b) Effect on the evolution of z.

Fig. 13. The effect of a change in x on the evolution of the system.



(a) Effect on the evolution of x. (b) Effect on the evolution of z.

Fig. 14. The effect of a change in y on the evolution of the system.

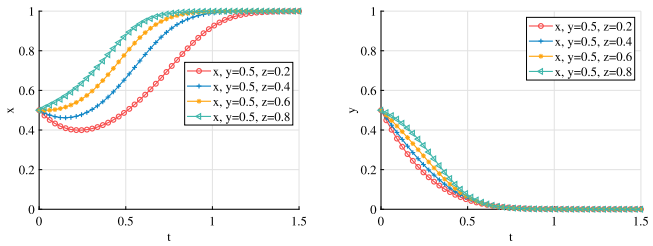
of application service providers shown in Fig. 13, reflects the strategic adjustments of large language model providers after considering the policy of regulatory authorities and the behavior of market participants. It further emphasizes the interaction and adaptability of all parties in their privacy protection investment decisions. Additionally, the evolution speed at which regulatory authorities choose the strict regulatory strategy also shows a dynamic evolution pattern of decreasing first and then increasing, implying that regulatory authorities seek a balance between enforcement efficacy and cost efficiency.

In the experiment depicted in Fig. 15, we fix x and y at 0.5 and increase z from 0.2 to 0.8 in increments of 0.2. The results show that the evolution speed of large language model providers selecting the "invest in privacy protection strategy" accelerates with the increase of z, while the corresponding evolution speed for application service providers shows a deceleration trend. However, compared to the rate of change in speed for large language model providers, the change in evolution speed for application service providers is not significant. This phenomenon may reflect the quick response capacity of large language model providers in the face of policy changes, possibly due to their dominant market position or a high emphasis on public image. In contrast, application service providers may face more significant inertia when adjusting their investment strategies. Especially in the context of cost pressure sensitivity and limited strategic flexibility, they may prefer to maintain the existing strategy landscape rather than take on new investment risks. This conservative strategy evolution reflects the value application service providers place on the stability of current decisions and their cautious consideration of resource commitments in uncertain environments.

5.2. Partial parameter analysis

5.2.1. Analysis of parameters related to large language model providers

As shown in Fig. 16, when only large language model providers invest in user privacy protection, their profit growth rate can reach α_0. When both parties invest in user privacy protection, a win–win situation is achieved, and the profit growth rate for large language model providers can reach α_1. We set the initial values of α_0 and α_1 to 0.35 and 0.45, respectively. To study the impact of different profit growth rates on system evolution, we adjust these two parameters downward to 0.25 and 0.35 to simulate a low-growth rate environment. At the same time, we also increase them to 0.45 and 0.55, and 0.55 and 0.65, to explore



(a) Effect on the evolution of x. (b) Effect on the evolution of y.

Fig. 15. The effect of a change in z on the evolution of the system.

system evolution behavior in a higher profit growth rate environment. In the lower growth rate combinations, *i.e.*, ($\alpha_0 = 0.25, \alpha_1 = 0.35$) and ($\alpha_0 = 0.35, \alpha_1 = 0.45$), we observe that the system's evolution trend initially tends towards state $(0, 0, 0)$. However, as the evolution process continues, the system eventually tends towards stability in state $(0, 1, 1)$. It can be suggested that in a low-growth rate environment, there may not be enough incentives to encourage large language model providers to invest. Therefore, their willingness to invest in privacy protection at the early stages of system evolution is not strong. In the higher growth rate conditions, specifically when ($\alpha_0 = 0.45, \alpha_1 = 0.55$) and ($\alpha_0 = 0.55, \alpha_1 = 0.65$), the system's initial evolution trend also develops towards state $(0, 0, 0)$. But over time, this trend changes, and the system gradually stabilizes at state $(1, 0, 1)$. It can be speculated that as time progresses, the large language model providers may realize that investing in privacy protection can provide a relative advantage in a high growth rate environment. Application service providers, on the other hand, may consider free-riding to gain additional benefits from the investments of large language model providers. Meanwhile, regulatory authorities may adopt strict regulatory strategies to ensure the market's health and sustainable development, especially when application service providers are not actively investing in privacy protection. Additionally, based on the projection on the x–y plane, the curve span is smaller under lower growth rate combinations, while the curve span is larger under higher growth rate combinations. It is inferred that in the initial state, considering the low profit growth rate of large language model providers due to fierce market competition or high costs in the initial stages of business expansion, they may be more inclined towards direct and short-term benefits in their decisions, rather than investing in privacy protection immediately. This is because investment in privacy protection often takes time to generate returns, and its benefits may not be significant before a certain market share is reached. As the profit growth rate increases gradually and the market matures, large language model providers have accumulated substantial capital and have successfully gained a certain market share. At this stage, they start seeking long-term, sustainable development strategies. Investing in privacy protection technology becomes a key strategy not only to enhance brand image and increase customer trust but also a wise move to ensure advantages in an increasingly competitive market. Furthermore, with the strictening of data protection regulations, compliance with privacy protection has also become an essential factor that businesses must consider.

5.2.2. Analysis of parameters related to application service providers

As shown in Fig. 17, the profit growth rate for application service providers is β_0 when only they invest in user privacy protection, while it is β_1 when both parties invest. The initial values of β_0 and β_1 are set to 0.45 and 0.5, respectively. To examine the impact of different profit growth rates on system evolution, we adjust these parameters downward to 0.35 and 0.40 and upward to 0.55 and 0.60, and 0.65 and 0.70 to simulate both low and high-growth rate environments. Under the low growth rate settings of ($\beta_0 = 0.35, \beta_1 = 0.40$) and ($\beta_0 = 0.45, \beta_1 = 0.50$), the system initially tends towards an evolution to the state where

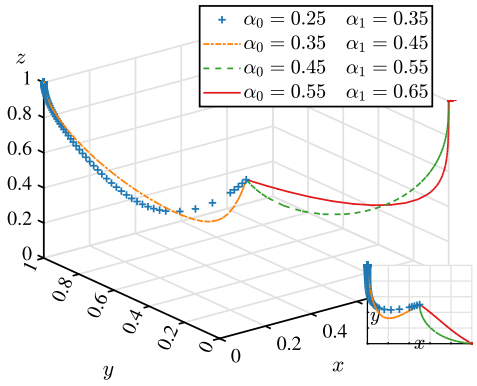


Fig. 16. Effect of changes in α on evolutionary pathways.

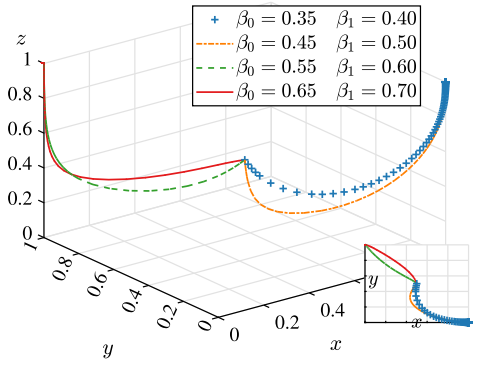


Fig. 17. Effect of changes in β on evolutionary pathways.

all parties do not invest and there is no regulation $(0, 0, 0)$. However, as time progresses, this trend changes and stabilizes at $(1, 0, 1)$. This trend possibly reflects that in such environments, application service providers' rational choice based on the free-riding effect is to not invest in privacy protection as they gain significant benefits for free from the investment of large language model providers. Under the higher growth rate combinations ($\beta_0 = 0.55, \beta_1 = 0.60$) and ($\beta_0 = 0.65, \beta_1 = 0.70$), application service providers also initially evolve towards non-investment and non-regulation state $(0, 0, 0)$. As evolution progresses, the system finally stabilizes at state $(0, 1, 0)$, suggesting that when the market has great growth potential, the attraction of free-riding wanes for application service providers who are more inclined to improve their market position by investing in user privacy protection. Observing the evolutionary curves of application service providers projected on the x–y plane, we find their distribution to be more evenly spread compared to large language model providers, hinting at a higher sensitivity to market fluctuations. This could be due to application service providers directly facing consumers and needing to quickly adapt to changes in consumer demands and regulations. Thus, in their decisions on investing in privacy protection, application service providers are showing themselves to be more proactive and flexible.

5.2.3. Analysis of parameters related to regulatory authorities

When regulatory authorities adopt a lax regulatory approach, if companies do not invest in protecting user privacy, this will result in a reputation loss L for the regulatory authorities. To quantify such loss and to explore its influence on regulatory policies, we set the baseline value of L to 35 and simulate its effects on system evolution as it changes between 5 to 95. Simulation outcomes (see Fig. 18) reveal that with the gradual increase in reputation loss L, the system's evolutionary equilibrium point transitions from $(1, 0, 0)$ to $(1, 0, 1)$. This shows that reputation loss plays an important role in the strategic adjustments of

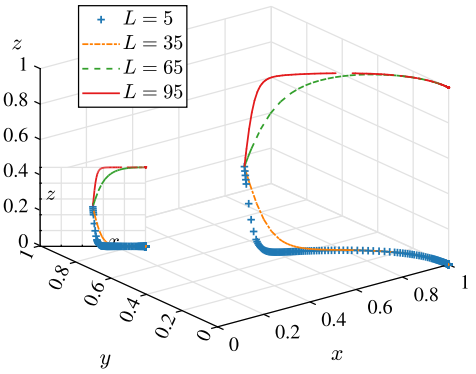


Fig. 18. Effect of changes in L on evolutionary pathways.

regulatory authorities: as reputation losses compound, the authorities face much-growing public opinion pressure, lowering public trust in the regulators, and raising doubts about their policies. This dual pressure from public sentiment and the political environment compels the regulatory authorities to abandon their lax regulatory stance and adopt a stricter regulatory policy. Additionally, observing the projection of their evolutionary curves on the $x - z$ plane, a uniform curve distribution suggests that regulators might be trying to find the optimal intensity of regulation throughout the entire range of reputation loss fluctuation to maintain a positive public image while ensuring the market runs healthily.

To explore the impact of the fines F imposed by regulatory authorities on the dynamic system's evolution, we set the range of fines F from 3 to 12 and monitor how this change affects the system's path and speed to reach the equilibrium point $(1, 0, 1)$. Simulation results (as detailed in Fig. 19 reveal that as F increases from 3 to 12, the system initially tends to evolve toward an intermediate state $(1, 0, 0)$. This phenomenon is particularly evident when F is at lower values. It is conceivable that low levels of fines do not pose an effective deterrent to application service providers, hence their willingness to invest in privacy protection is greatly reduced. Also, under this level of fines, the rewards are too low for large language model providers, likely insufficient to cover their costs of investing in privacy protection, thereby deterring them from such investments. Moreover, regulatory authorities may also lack the motivation to implement strict regulation in a low-fin environment, possibly because the costs of strict regulation exceed the fine revenue or the expected compliance effect. As the system continually evolves, particularly when fines F gradually increase, the system state tends to evolve toward the final state $(1, 0, 1)$, where the regulatory authority adopts a "strict regulation" policy, large language model providers choose to "invest in privacy protection", and application service providers opt not to "invest in privacy protection". Additionally, by looking at the projection on the x–y plane, it can be found that the evolutionary curves span a greater range between $F = 3$ and $F = 6$, indicating that regulators and providers are quite sensitive to changes in fines within this range. Specifically, as fines gradually increase from lower levels, they might quickly alter the cost–benefit analysis of providers, prompting them to adjust strategies to adapt to the new regulatory environment. This strategy adjustment may include investing in privacy protection measures to avoid higher fines. Therefore, when fines increase initially, the change in the system state is significant, leading to a large curve span. However, within the intervals of $F = 6$ to $F = 9$ and $F = 9$ to $F = 12$, the curve span decreases, likely because providers have adapted to a higher fine mechanism. At this stage, providers might have increased their investment in privacy protection or found a balance between the fine and the cost of non-compliance. As fines continue to rise, the marginal effect of fines may diminish, thus the evolution speed of the system state slows down, reflected in the projection map as a decreased curve span.

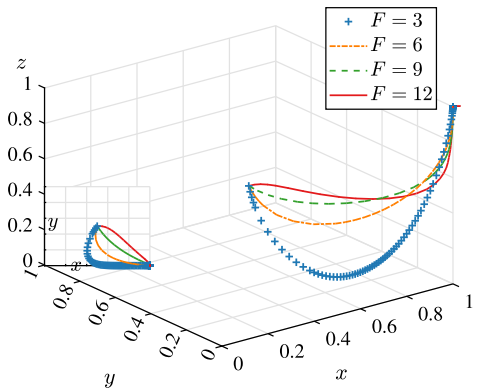


Fig. 19. Effect of changes in F on evolutionary pathways.

6. Conclusion and future works

In the era of large language models, the protection of user data privacy becomes an urgent issue. This article establishes a tripartite evolutionary game model by analyzing the interactive behavior between large language model providers, application service providers, and privacy regulatory authorities. Based on this, we analyze the influencing factors and evolutionary paths of different decision combinations of the above-mentioned three game participants. According to the simulation results, we propose the following conclusions and future works:

(a) Large language model providers play a critical role in data privacy protection. Our findings suggest that as regulatory authorities strengthen oversight strategies and market focus on privacy protection grows, large language model providers can achieve higher profits and gain a competitive edge by investing in privacy protection. Thus, providers must continuously improve privacy protection technologies to ensure user data security and enhance service quality. This not only helps safeguard user interests but also boosts corporate reputation and market competitiveness, creating a virtuous cycle. This provides clear guidance for industry practices, emphasizing the importance of privacy protection investment for long-term business development.

(b) For application service providers, actively investing in data privacy protection not only improves service quality but also secures an advantage in competitive markets. The findings indicate that application service providers need to adapt their privacy protection investment strategies flexibly under different regulatory environments and market conditions. Particularly, when large language model providers increase their privacy protection investments, the strategic choices of application service providers will directly affect their profitability and market position. Therefore, application service providers should follow the study's recommendations to actively engage in privacy protection, thereby strengthening their market competitiveness.

(c) For regulatory authorities, establishing effective regulatory policies can not only enhance the overall level of data privacy protection but also promote healthy market competition. Our study provides empirical evidence for policymaking, indicating that regulatory authorities must actively fulfill their duties, develop effective regulatory mechanisms, and implement robust regulatory policies to ensure the effective enforcement of data privacy protection. Simultaneously, regulators should encourage innovation to ensure that regulatory measures do not hinder technological development and market innovation. This provides concrete guidance for real-world policymaking.

(d) For users of large language models, raising data privacy awareness is crucial. The research highlights that users should actively understand and safeguard their data privacy rights and report violations to promote the healthy development of the ecosystem. This provides theoretical support for user education and raising public awareness, calling for the active participation of all sectors of society in data privacy protection.

Future research can further expand the current model to better capture the complex motivations of regulatory authorities and the dynamics of multi-party interactions in the privacy protection ecosystem. Specific directions include:

(a) **Incorporating Additional Motivational Factors**

- **Ethical Responsibility Parameter** (E): Introducing a parameter to quantify the influence of ethical considerations on regulatory decisions. This parameter could be linked to public interest metrics or societal expectations, reflecting the moral obligations of government entities in privacy protection.
- **Dynamic Weighting in Reward Functions**: Modifying the reward function to incorporate both ethical and reputational factors, represented as $R_{\text{total}} = \alpha R_{\text{reputation}} + \beta R_{\text{ethics}}$, where the weights α and β can dynamically adjust based on societal conditions or political contexts.

(b) **Introducing Additional Game Participants**
Future research could include data providers, network security attackers, and other relevant stakeholders, constructing a more complex multi-party evolutionary game model to better simulate the interactions and strategies within the privacy protection ecosystem.

(c) **Balancing Ethical Considerations and Technological Innovation**
Striking a balance between safeguarding personal privacy and promoting technological innovation remains a critical challenge. Future studies could explore practical pathways to achieve this balance, proposing policy recommendations that ensure data security without hindering technological progress.

CRediT authorship contribution statement

Yali Lv: Writing – original draft, Methodology, Conceptualization. **Jian Yang:** Writing – original draft, Formal analysis, Conceptualization. **Xiaoning Sun:** Writing – review & editing, Methodology. **Huafei Wu:** Writing – original draft, Validation.

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 gratefully acknowledge the financial supports by the National Social Science Fund of China (Grant No. 23BJY205), in part by the National Natural Science Foundation of China (Grant No. 72304177) and in part by the MOE (Ministry of Education in China) Project of Humanities and Social Sciences (Grant No. 21YJCZH197 and 22YJAZH080) and in part by the Natural Science Foundation of Shanxi Province, China (Grant No. 202103021224288 and 202303021221184).

Data availability

No data was used for the research described in the article.

References

[1] Devlin J, Chang M-W, Lee K, Toutanova K. BERT: Pre-training of deep bidirectional transformers for language understanding. 2019, arXiv preprint arXiv:1810.04805.

[2] Titus LM. Does ChatGPT have semantic understanding? A problem with the statistics-of-occurrence strategy. Cogn Syst Res 2024;83. http://dx.doi.org/10.1145/3656049.

[3] Haseeb MT, Hammoudeh A, Xia G. GPT-4 driven cinematic music generation through text processing. In: ICASSP 2024-2024 IEEE international conference on acoustics, speech and signal processing. 2024, p. 6995–9.

[4] Dhanaliwala AH, Ghosh R, Karn SK, Ullaskrishnan P, Farri O, Comaniciu D, Kahn CE. General-purpose vs. domain-adapted large language models for extraction of data from thoracic radiology reports. 2023, arXiv preprint arXiv:2311.17213.

[5] Chen W, Wang Q, Long Z, Zhang X, Lu Z, Li B, Wang S, Xu J, Bai X, Huang X, et al. DISC-finllm: A Chinese financial large language model based on multiple experts fine-tuning. 2023, arXiv preprint arXiv:2310.15205.

[6] Eshghie M, Eshghie M. ChatGPT as a therapist assistant: a suitability study. 2023, arXiv preprint arXiv:2304.09873.

[7] Limo FAF, Tiza DRH, Roque MM, Herrera EE, Murillo JPM, Huallpa JJ, Flores VAA, Castillo AGR, Peña PFP, Carranza CPM, et al. Personalized tutoring: ChatGPT as a virtual tutor for personalized learning experiences. Przestrzeń Społeczna (Soc Space) 2023;23(1):293–312.

[8] Lu S, Zhao Y, Chen Z, Dou M, Zhang Q, Yang W. Association between atrial fibrillation incidence and temperatures, wind scale and air quality: An exploratory study for shanghai and kunming. Sustainability 2021;13(9):5247. http://dx.doi.org/10.3390/su13095247.

[9] Garg RK, Urs VL, Agarwal AA, Chaudhary SK, Paliwal V, Kar SK. Exploring the role of ChatGPT in patient care (diagnosis and treatment) and medical research: A systematic review. Heal Promot Perspect 2023;13(3):183.

[10] Yeo YH, Samaan JS, Ng WH, Ting P-S, Trivedi H, Vipani A, Ayoub W, Yang JD, Liran O, Spiegel B, et al. Assessing the performance of ChatGPT in answering questions regarding cirrhosis and hepatocellular carcinoma. Clin Mol Hepatol 2023;29(3):721, Korean Association for the Study of the Liver.

[11] Staab R, Vero M, Balunović M, Vechev M. Beyond memorization: Violating privacy via inference with large language models. 2023, arXiv preprint arXiv:2310.07298.

[12] Lukas N, Salem A, Sim R, Tople S, Wutschitz L, Zanella-Béguelin S. Analyzing leakage of personally identifiable information in language models. 2023, arXiv preprint arXiv:2302.00539.

[13] Wang T, Zhang Y, Qi S, Zhao R, Xia Z, Weng J. Security and privacy on generative data in AIGC: A survey. 2023, arXiv preprint arXiv:2309.09435.

[14] Patil K, Sonune H, Devikar S, Chaudhari V, Ayachit I. A comparative analysis of various techniques of data leakage detection in different domains. In: ICT analysis and applications: proceedings of ICT4SD 2022. Springer; 2022, p. 735–42.

[15] Nicholas G, Friedl P. Regulating large language models: A roundtable report. 2024, arXiv preprint arXiv:2403.15397.

[16] Yang L, Dong J, Yang W. Analysis of regional competitiveness of China's cross-border E-commerce. Sustainability 2024;16(3):1007. http://dx.doi.org/10.3390/su16031007.

[17] Yang W, Pan L, Ding Q. Dynamic analysis of natural gas substitution for crude oil: Scenario simulation and quantitative evaluation. Energy 2023;282:128764. http://dx.doi.org/10.1016/j.energy.2023.128764.

[18] Du J, Li J, Li J, Li W. Competition–cooperation mechanism of online supply chain finance based on a stochastic evolutionary game. Oper Res 2023;23(3):55, Springer.

[19] Zhou Y, Rahman MM, Khanam R, Taylor BR. The impact of penalty and subsidy mechanisms on the decisions of the government, businesses, and consumers during COVID-19 — Tripartite evolutionary game theory analysis. Oper Res Perspect 2022;9:100255. http://dx.doi.org/10.1016/j.orp.2022.100255.

[20] Schuur P, Badur B, Sencer A. An explicit Nash equilibrium for a market share attraction game. Oper Res Perspect 2021;8:100188. http://dx.doi.org/10.1016/j.orp.2021.100188.

[21] Vaswani A, Shazeer N, Parmar N, Uszkoreit J, Jones L, Gomez AN, Kaiser Ł, Polosukhin I. Attention is all you need. In: Advances in neural information processing systems, vol. 30, 2017.

[22] Ouyang L, Wu J, Jiang X, Almeida D, Wainwright CL, Mishkin P, Zhang C, Agarwal S, Slama K, Ray A, et al. Training language models to follow instructions with human feedback. 2022, arXiv preprint arXiv:2203.02155, 13.

[23] Zeng W, Ren X, Su T, Wang H, Liao Y, Wang Z, Jiang X, Yang ZZ, Wang K, Zhang X, et al. Pangu-α: Large-scale autoregressive pretrained Chinese language models with auto-parallel computation. 2021, arXiv preprint arXiv:2104.12369.

[24] Xu NRunhua, Baracaldo N, Joshi JBD. Privacy-preserving machine learning: Methods, challenges and directions. 2021, arXiv, abs/2108.04417.

[25] Li H, Chen Y, Luo J, Kang Y, Zhang X, Hu Q, Chan C, Song Y. Privacy in large language models: Attacks, defenses and future directions. 2023, arXiv preprint arXiv:2310.10383.

[26] Behnia R, Ebrahimi MRR, Pacheco J, Padmanabhan B. EW-tune: A framework for privately fine-tuning large language models with differential privacy. In: 2022 IEEE international conference on data mining workshops. IEEE; 2022, p. 560–6.

[27] Kandpal N, Wallace E, Raffel C. Deduplicating training data mitigates privacy risks in language models. In: International conference on machine learning. PMLR; 2022, p. 10697–707.

[28] Xu J, Hong N, Xu Z, Zhao Z, Wu C, Kuang K, Wang J, Zhu M, Zhou J, Ren K, et al. Data-driven learning for data rights, data pricing, and privacy computing. Engineering 2023;25:66–76.

[29] Rajagopal M, Sivasakthivel R, Ramar G, M A, Karuppasamy SK. A conceptual framework for AI governance in public administration – A smart governance perspective. In: 2023 7th international conference on I-SMAC (IoT in social, mobile, analytics and cloud). 2023, p. 488–95.

[30] Hao H, Yang J, Wang J. A tripartite evolutionary game analysis of participant decision-making behavior in mobile crowdsourcing. Mathematics 2023;11(5):1269, MDPI.

[31] Yang J, Yan X, Yang W. A tripartite evolutionary game analysis of online knowledge sharing community. Wirel Commun Mob Comput 2022;1–11, Article ID 4460034.

[32] Zhang X, Fan L, Wang S, Li W, Chen K, Yang Q. A game-theoretic framework for privacy-preserving federated learning. ACM Trans Intell Syst Technol 2024;15(3):35. http://dx.doi.org/10.1145/3656049.

[33] Shah H, Kakkad V, Patel R, Doshi N. A survey on game theoretic approaches for privacy preservation in data mining and network security. Procedia Comput Sci 2019;155:686–91, Elsevier.

[34] Xu L, Jiang C, Wang J, Ren Y, Yuan J, Guizani M. Game theoretic data privacy preservation: Equilibrium and pricing. In: 2015 IEEE international conference on communications. IEEE; 2015, p. 7071–6.

[35] Ju H, Zeng Q, Chu X, Li Y. Cooperative investment strategies of ports and shipping companies in blockchain technology. Oper Res 2024;24(2):32, Springer.

[36] Sagduyu YE. Free-rider games for federated learning with selfish clients in nextg wireless networks. In: 2022 IEEE conference on communications and network security. IEEE; 2022, p. 365–70.

[37] Gupta D, Bhatt S, Bhatt P, Gupta M, Tosun AS. Game theory based privacy preserving approach for collaborative deep learning in IoT. In: Deep learning for security and privacy preservation in ioT. Springer; 2022, p. 127–49.

[38] Collins BC, Xu S, Brown PN. A coupling approach to analyzing games with dynamic environments. 2022, arXiv preprint arXiv:2207.06504.

[39] Łatuszyńska M, Fate S. Combining system dynamics and agent-based simulation to study the effects of public interventions on poverty. Procedia Comput Sci 2022;207:3978–87.

[40] Howick S, Megiddo I, Nguyen LKN, Wurth B, Kazakov R. Combining SD and ABM: Frameworks, benefits, challenges, and future research directions. In: Fakhimi M, Mustafee N, editors. Hybrid modeling and simulation: conceptualizations, methods and applications. Springer Nature Switzerland; 2024, p. 213–44. http://dx.doi.org/10.1007/978-3-031-59999-6_9.

[41] Huang K, Chen B, Lu Y, Wu S, Wang D, Huang Y, Jiang H, Zhou Z, Cao J, Peng X. Lifting the veil on the large language model supply chain: Composition, risks, and mitigations. 2024, arXiv preprint arXiv:2410.21218.

[42] Balayn A, Corti L, Rancourt F, Casati F, Gadiraju U. Understanding stakeholders' perceptions and needs across the LLM supply chain. In: Proceedings of the 2024 CHI conference on human factors in computing systems. 2024, https://arxiv.org/abs/2405.16311.