Journal Pre-proof

Evolutionary privacy-preserving learning strategies for edge-based IoT data sharing schemes

Yizhou Shen, Shigen Shen, Qi Li, Haiping Zhou, Zongda Wu, Youyang Qu

PII: S2352-8648(22)00095-5

DOI: https://doi.org/10.1016/j.dcan.2022.05.004

Reference: DCAN 429

To appear in: *Digital Communications and Networks*

Received Date: 23 August 2021

Revised Date: 21 April 2022

Accepted Date: 10 May 2022

Please cite this article as: Y. Shen, S. Shen, Q. Li, H. Zhou, Z. Wu, Y. Qu, Evolutionary privacy-preserving learning strategies for edge-based IoT data sharing schemes, *Digital Communications and Networks* (2022), doi: https://doi.org/10.1016/j.dcan.2022.05.004.

Digital Communications and Networks(DCN)

HOSTED BY

ELSEVIER

Available online at www.sciencedirect.com

ScienceDirect

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

Evolutionary privacy-preserving learning strategies for edge-based IoT data sharing schemes

Yizhou Shen[a,b], Shigen Shen[a,*], Qi Li[a], Haiping Zhou[a], Zongda Wu[a], Youyang Qu[c]

[a]**Department of Computer Science and Engineering, Shaoxing University, Shaoxing 312000, China**
[b]**School of Computer Science and Informatics, Cardiff University, Cardiff CF24 3AA, United Kingdom**
[c]**School of Information Technology, Deakin University, Burwood, VIC 3125, Australia**

Abstract

The fast proliferation of edge devices for the Internet of Things (IoT) has led to massive volumes of data explosion. The generated data is collected and shared using edge-based IoT structures at a considerably high frequency. Thus, the data-sharing privacy exposure issue is increasingly intimidating when IoT devices make malicious requests for filching sensitive information from a cloud storage system through edge nodes. To address the identified issue, we present evolutionary privacy preservation learning strategies for an edge computing-based IoT data sharing scheme. In particular, we introduce evolutionary game theory and construct a payoff matrix to symbolize intercommunication between IoT devices and edge nodes, where IoT devices and edge nodes are two parties of the game. IoT devices may make malicious requests to achieve their goals of stealing privacy. Accordingly, edge nodes should deny malicious IoT device requests to prevent IoT data from being disclosed. They dynamically adjust their own strategies according to the opponent's strategy and finally maximize the payoffs. Built upon a developed application framework to illustrate the concrete data sharing architecture, a novel algorithm is proposed that can derive the optimal evolutionary learning strategy. Furthermore, we numerically simulate evolutionarily stable strategies, and the final results experimentally verify the correctness of the IoT data sharing privacy preservation scheme. Therefore, the proposed model can effectively defeat malicious invasion and protect sensitive information from leaking when IoT data is shared.

KEYWORDS:
Privacy preservation, Internet of Things, Evolutionary game, Data sharing, Edge computing

1. Introduction

The Internet of Things (IoT) can be described as a network that connects all entities with the internet through information sensing devices to realize the function of intelligent identification, operation, and management. The IoT is attracting considerable attention with the continuous development of wireless communications, radio frequency identification, and low-cost sensors. However, IoT network problems, such as security and privacy, are rapidly emerging, and thus, privacy protection is of paramount importance [1, 2, 3, 4, 5].

Edge-based IoT [6] is experiencing rapid growth because traditional cloud computing is unable to immediately handle the massive data generated by edge nodes with the rapid development and wide application of the IoT, big data, and 5G/6G networks [7]. In this architecture, edge computing provides parts of cloud services for IoT devices on the edge of the network. It focuses on solving the problems of high latency, network instability, and low bandwidth [8]. Its applications are initiated on the edge side, resulting in

*Shigen Shen (Corresponding author) (email: shigens@usx.edu.cn).
[1]Yizhou Shen (email: sheny44@cardiff.ac.uk).
[2]Qi Li (email: liqi0713@foxmail.com).
[3]Haiping Zhou (email: hpzhou2885@163.com).
[4]Zongda Wu (email: zongda1983@163.com).
[5]Youyang Qu (email: y.qu@deakin.edu.au).

the faster response of cloud services, which meets the basic IoT requirements in real-time business, application intelligence, and privacy preservation.

However, privacy issues while sharing edge-based IoT data are still challenging due to physical attacks, privacy exposure, service control, and data tampering [9], although edge computing mitigates the communication delays caused by cloud computing. Malware intrusions in IoT networks are becoming increasingly widespread [10, 11]. Specifically, if nodes are attacked and high-privilege systems, such as the operating system are controlled by the attacker, it becomes easy to filch the data stored in a cloud storage system, which places privacy data at great risk [12]. Existing data sharing protocols divulge data with a central node, exposing the source file directly to the platform. Encrypting data reduces the possibility of data leaking during transmission, but it does not restrain malware from stealing documents from the cloud storage system through edge nodes. Hence, preserving data privacy at the edge is becoming progressively important [13, 14].

To solve privacy issues, various scenarios have been proposed, which commonly originate from cache-based architectures [15, 16, 17], trust computing mechanisms [18, 19], and Radio Frequency Identification (RFID) techniques [20, 21]. Nonetheless, there are several limitations in the existing scenarios. Although the cache-based strategy is always utilized in conjunction with k-anonymity, the user movements are easily divulged in the location-based service on the basis of information caching. The trusted platform module, to some extent, enhances the security of the computing platform via cryptography. However, it is vulnerable to malignant attacks due to the exposure of platform configuration. The RFID technique makes it difficult for sensitive user information to be tampered with secure authentication, while this data is probably maliciously revealed.

Moreover, game theory has also been widely utilized in privacy preservation in the last few years [22], providing a theoretical basis for IoT security-associated decision-making. In these models, each player's payoff depends not only on its own strategy but also on the strategies of other participants. Therefore, each player continuously adjusts their strategies according to the opponent's strategy to maximize their own payoffs. In such cases, the choice of a stable strategy is usually worth investigating. Specifically, in the domain of IoT network security, when attackers attempt to filch users' privacy via malicious node attacks or malware dissemination, defenders are required to take appropriate measures to strengthen the security defense mechanism of IoT systems.

In the current work, we proposed a privacy preservation model based on evolutionary game theory and edge computing during IoT data sharing, considering the detection rate, successful diffusion rate, privacy risk factor, and trust gain. An evolutionary game can achieve an equilibrium through constant simulations and strategy adjustment in the whole process, where there exists a Nash equilibrium called an evolutionarily stable strategy. Herein, this game model based on replication dynamics was used to describe the IoT privacy preservation learning strategies considering intrusion detection. The dynamic equations were reproduced to describe the changes while adopting different strategies, and eventually, the optimal strategy was obtained. We eventually analyzed the influence of the above four impact factors on the node evolution stability strategy and provided suggestions for the cloud storage system to refuse the malicious requests from the source and upgrade the privacy preservation. To the best of our knowledge, this is an early work to study optimal privacy preservation strategies based on evolutionary game theory for the edge-based IoT data sharing scheme.

The main contributions of the current work are epitomized as follows:

- We establish an evolutionary IoT data sharing game based on game theory and edge computing. In addition, we further analyze whether the eigenvalues of the model are greater than zero. Then, we assess the stability by the eigenvalues and eventually derive the equilibrium points of this model. Through mathematical modeling, we can observe the stability of each point in every case more intuitively.

- We develop a data sharing framework after analyzing the game process of the privacy preservation model based on replication dynamics, which demonstrates the specific process of decision-making by edge nodes.

- We propose a solution to solve the established evolutionary learning algorithm and derive optimal privacy preservation strategies for the edge-based IoT data sharing scheme. Through a constant trial and error, the strategy is adjusted and improved with time, maximizing the expected revenue and returning the optimal evolutionary strategy.

- We numerically simulate the evolutionary privacy preservation model for edge-based IoT data sharing, illustrating evolutionarily stable strategies of IoT devices and edge nodes. The reliability of this model is verified by observing the convergence of the curve by adjusting the parameters. The simulation experiments ultimately provide suggestions for enhancing the privacy preservation of edge nodes while sharing data.

The rest of the current work is organized as follows: In Section 2, we separately review edge computing-oriented and game theory-based privacy preservation

and expound on the differences between our model and existing models. In Section 3, we construct an edge computing architecture for IoT data sharing. In addition, we propose an evolutionary privacy preservation learning game based on edge computing, providing replication dynamic equations and analyzing evolutionarily stable strategies. Moreover, we develop an application framework and an evolutionary learning algorithm for the edge-computing oriented privacy preservation model. In Section 4, we numerically simulate the model to attain the optimal evolutionarily stable strategies of IoT devices and edge nodes. Then, we investigate the impact of related parameters on strategies selected by IoT devices and edge nodes, which is followed by a conclusion in Section 5.

For better clarification, we provide symbol definitions as shown in Table 1.

2. Related work

It is worth mentioning that data privacy in cloud storage systems has always been a concern of end users. The distributed parallel data processing method causes diverse challenges, including physical attacks, privacy exposure, service control, and data tampering. Therefore, research on data privacy preservation techniques, such as access control and identity authentication, has become important to support and ensure the sustainable development of edge computing. To construct an intelligent and secure network environment, Stergiou et al. [15] proposed a cache decision system in a secure caching scenario combined with IoT, cloud computing, edge computing, and big data. Mukherjee et al. [23] highlighted that although there is less of a delay, intelligent edge computing causes additional security issues, such as malignant assaults focusing on intelligent engines. Rao and Bertino [24] analyzed and proposed several privacy solutions for various types of data in edge applications. To better allocate privacy tasks, Zhang et al. [25] imported a privacy-preserving framework, which can be executed in an actual edge computing platform. Gu et al. [26] raised a dynamic privacy preservation model to ensure the security of data transmission between edge nodes and clients. In [27], Xu et al. suggested an optimization scheme developed on edge computing, improving resource utilization and synchronically protecting privacy. To protect the privacy of requesters and clients, Zhou et al. [28] contrived a context-aware scheme for mobile crowdsensing under an edge computing system. Zhen and Liu [29] proposed a privacy preservation scheme on the basis of mobile edge computing to improve wireless body area networks. They also designed a Merkle tree model and a hybrid signature algorithm to ensure the security performance of IoT nodes. To ensure the security of private data on terminal devices, Li et al. [30] developed an outline for IoT applications accordant with mobile edge computing. It could not only guarantee the integrity of the source but it could also decrease the cost of communication. In [31], Liu et al. unified federated learning with edge computing, providing a privacy preservation framework, which can minimize privacy leakage during data transmission. To prevent sensitive information from being exposed, Du et al. [32] utilized differential privacy to execute intelligent edge machine learning. He et al. [33] attached importance to mobile-edge computing. Their conception ensures user experience and privacy at the same time. Zhao et al. [34] proposed a privacy preservation approach to prevent poisoning attacks in mobile-edge computing, which could also identify the specific location of poisoning through the network. Du et al. noticed that distributed nodes are easy to hack, and thus, privacy preservation in multiaccess edge computing was studied in [35]. Li et al. [36] researched a reliable and distributed algorithm upon edge nodes, preserving confidential information during outsourcing.

With the popularity of the IoT, privacy preservation has received increasing attention. Based on this, to prohibit sensitive information from leaking, game theory has already been widely applied in IoT data privacy preservation. Do et al. [37] presented game models and defense mechanisms of cyberspace privacy to address specific privacy issues with game-theoretic approaches. In [38], Ezhei and Tork Ladani introduced a differential game model, utilizing the data sharing thresholds to assess whether a firm shares security information with central authorities, such as ISACs, which ensured a social optimum. Cui et al. [39] constructed a personalized differential privacy game model to enhance data utility. Qu et al. [40] utilized a dynamic zero-sum game to explore the optimal strategy for protecting location and identity privacy in cyber-physical social networks. In [41], the authors modeled a Stackelberg game for k-anonymity among leaders, followers, and a third-party platform. To tackle the privacy leak caused by IoT devices, Li et al. [42] simulated a trilateral game among users, providers, and antagonists, presenting guidance for scheming a privacy preservation strategy. Xiong et al. [43] also provided a three-party game that supported artificial intelligence for preventing privacy invasion in mobile edge crowdsensing. Similarly, in [44], the authors presented a privacy framework based on a switch-controller mapping mechanism. It could minimize the privacy leak in software-defined networking derived from cyber physical systems. To protect sensitive information, Jin et al. [45] proposed game models, considering the collaboration gain and privacy loss between assailants and collaborators. Riahi Sfar et al. [46] nominated a privacy preservation model between data owners and receivers by utilizing Markov chains. It can protect personal privacy while exchanging the data in intelligent transportation systems. Nosouhi et al. [47] developed an unlink-

Table 1. Symbol definitions.

Symbol	Definition
α	Detection rate
β	False alarm rate
γ	False alarm lose
δ	Rate of successful diffusion
ε	Privacy risk factor
ξ_A	Gain obtained by successful access to privacy
ξ_P	Gain obtained by successful privacy preservation
ϱ	Gain obtained by the trust of normal requests
ξ_D	Gain obtained by malware diffusion
ξ_C	Gain obtained by normal requests
ξ_S	Gain obtained by successful detection
ς_D	Cost incurred by malware diffusion
ς_C	Cost incurred by normal requests
ς_S	Cost incurred by successful detection
p	Probability of IoT devices requesting maliciously
q	Probability of edge nodes denying IoT devices requests

able coin protocol to desensitize privacy data through an anonymity technique, which protects Bitcoin users' sensitive information. Liu et al. [48] designed a game model for participants to acquire an optimal payment strategy, providing sufficient privacy preservation in crowdsensing. In [49] Liu et al. modeled a bilateral game framework to achieve profit maximization and privacy preservation simultaneously in spectrum sharing. Wu et al. [50] propounded a game model of security assault and guard, considering the actions of attackers. Mengibaev et al. [51] introduced a heterogeneous interaction mechanism to establish an evolutionary game framework for investigating security assurance on the internet. Du et al. [52] associated evolutionary dynamics with a game theoretic framework, urging individuals to focus on their privacy preservation online. Sun [53] built an evolutionary game model and obtained the optimal privacy preservation strategy for early adaptation in the network.

Compared to the above work, we concentrate on seeking evolutionary privacy preservation learning strategies for edge-based IoT data sharing. The current privacy preservation schemes are mainly divided into three categories: k-anonymity [41, 54], access control [55, 56], and differential privacy [57, 58, 59]. K-anonymity requires publishers to desensitize data prior to publication. Access control restricts access to privacy information. Differential privacy distorts sensitive data via noise addition techniques. However, we notice that there is a prisoner's dilemma between IoT devices and edge nodes. Therefore, to solve the problem of privacy preservation from the source more effectively, data-sharing privacy preservation based on evolutionary game theory is studied from the perspective of obtaining revenue in the current work, and a privacy preservation data sharing model is established for edge-based IoT networks. We next display the comparison between our proposed method and other games in Table 2 for further emphasizing our contributions.

3. Evolutionary privacy preservation learning game for edge-based IoT networks

3.1. Problem statement

The IoT data sharing architecture of edge computing studied in the current work is shown in Fig. 1, which mainly includes a core infrastructure, edge nodes, and an IoT layer. Data sharing starts from a cloud storage system deployed in the core infrastructure, which provides access to the core network and the management of centralized cloud computing for edge devices. Note that edge nodes are ones of the core components in edge computing while sharing IoT data. They provide users with nearby edge computing services instead of sending all data back to a central place for processing, increasing bandwidth, and reducing latency. Ultimately, the shared data is received by the IoT layer, consisting of various IoT networks, each of which includes all sorts of smart devices, such as mobile terminals and IoT equipment.

Under such an edge-based IoT data sharing architecture, the massive data generated by edge devices involve personal privacy, which makes the privacy preservation problem particularly prominent. It is also notable that private data is partially or completely stored in edge data centers, causing the separation of ownership and control. In this case, it is easy to bring about data security problems, such as data leaks and illegal data operation. The data confidentiality and integrity cannot be guaranteed. In addition, there is a contradiction that it must effectively prevent IoT devices from trying to make a malicious

Table 2. Comparison between the proposed method and other games.

Paper	Scenario	Game Type	Advances	Drawbacks
Ezhei et al. [38]	Network security information sharing systems	Differential game	• Obtain a data sharing threshold determining whether a company shares their security information	• Belong to a perfectly rational game
Cui et al. [39]	Personalized differential privacy schemes	Differential game, Bayesian game	• Propose a model requiring less overall privacy budget and higher data utility • Eliminate the uncertainty of data utility measurement	• Belong to a perfectly rational game
Qu et al. [40]	Cyber physical social networks	Dynamic multistage zero-sum game	• Preserve location privacy and identity privacy • Achieve a fast convergence with a reinforcement learning algorithm	• Belong to a perfectly rational game
Zhang et al. [41]	Social networks	Stackelberg game	• Propose a model achieving high security in location-based services • Analyze the security and performance in different situations	• Belong to a perfectly rational game
Li et al. [42]	IoT netwroks	Three-party game	• Address private data transactions in IoT networks	• Belong to a perfectly rational game
Xiong et al. [43]	Mobile edge crowdsensing	Three-party game	• Protect the privacy of perceived data • Obtain a Nash equilibrium among player strategies, player profits, and constraint conditions	• Belong to a perfectly rational game
Sivaraman et al. [44]	Smart grids based on software defined networks	noncooperative game	• Present a privacy framework with a switch-controller mapping mechanism	• Belong to a perfectly rational game
Jin et al. [45]	Collaborative security systems	Zero sum game, non-zero sum game	• Attain collaborative security scenarios with privacy awareness • Deduce the optimal strategy in a complete cooperative game • Demonstrate the existence of Nash equilibrium in an incomplete cooperative game	• Belong to a perfectly rational game
Liu et al. [48]	Crowdsensing	Dynamic game	• Learn a Payment-privacy Protection Level (PPL) of platforms and participants • Speed up the acquisition of payment-PPL strategy	• Belong to a perfectly rational game
Liu et al. [49]	Spectrum Sharing Systems	Stackelberg game	• Protect users' location information • Show the payoff between the privacy protection levels and user utilities	• Belong to a perfectly rational game
Wu et al. [50]	Local differential privacy	Zero sum game	• Construct a zero-sum game between a defender and an attacker to solve the privacy issue • Raise a mutual information privacy protection method	• Belong to a perfectly rational game

Mengibaev et al. [51]	Social networks	Evolutionary game	• Introduce a heterogeneous interaction pattern to discuss the privacy protection in social networks	• Not highlight IoT network features
Du et al. [52]	Social networks	Evolutionary game	• Analyze information protection through user interactions and decisions	• Not highlight IoT network features
Sun [53]	Cloud service systems	Evolutionary game	• Increase the accuracy of replication dynamic equation	• Lead to serious delay in cloud service systems
Current work	Edge-based IoT schemes	Evolutionary game	• Propose an optimal protection strategy selection algorithm • Construct an evolutionary privacy preservation learning game describing edge-based IoT features • Propose an algorithm maximizing the expected revenue and returning the optimal evolutionary strategy	• Approximately obtain the equilibrium point

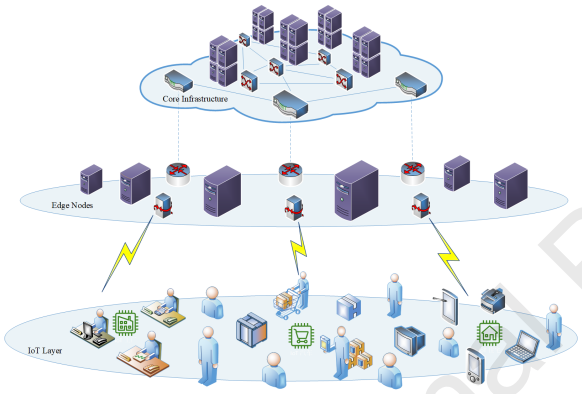

Fig. 1: Edge computing architecture for IoT data sharing.

request for stealing this kind of information while allowing access to privacy-related information. Thus, an urgent problem to be solved is researching privacy preservation from the perspective of payoff, establishing a privacy preservation model based on game theory, and further seeking an optimal privacy preservation strategy to protect user privacy, while also sharing edge-based IoT data.

3.2. Game construction

Definition 1. The evolutionary privacy preservation learning game for edge-based IoT networks is denoted by a quad $(\mathbb{P}, \mathbb{R}, \mathbb{D}, \mathbb{E})$, where:

- $\mathbb{P}$ = {IoT devices o, Edge nodes ϵ} represents a set of players.
- $\mathbb{R} = \mathbb{R}_M \times \mathbb{R}_N$ represents a set of IoT devices requests, where $\mathbb{R}_M$ represents malicious requests and $\mathbb{R}_N$ represents normal requests.
- $\mathbb{D} = \mathbb{D}_G \times \mathbb{D}_D$ represents a set of edge nodes responses, where $\mathbb{D}_G$ represents granting IoT requests and $\mathbb{D}_D$ represents denying IoT requests.
- $\mathbb{E}$ = {IoT devices revenue υ, Edge nodes revenue ξ} represents a set of expected revenue.

In the proposed game, two players, namely, IoT devices o and edge nodes ϵ are considered. IoT devices may make malicious requests, represented by $\mathbb{R}_M$, or make normal requests, represented by $\mathbb{R}_N$. Similarly, edge nodes may grant the requests through intrusion detection, represented by $\mathbb{D}_G$, or deny the requests through intrusion detection, represented by $\mathbb{D}_D$. Additionally, $\mathbb{E}$ represents the set of the expected revenue of IoT devices o and edge nodes ϵ, represented by υ and ξ, respectively.

Utilizing the symbols defined in Table 1, we construct a payoff matrix of the evolutionary privacy preservation learning game, as presented in Table 3. In the first case, IoT devices make malicious requests and edge nodes grant the requests, which means malware diffuses successfully. At that time, IoT devices receive a malware diffusion gain $(1-\alpha)\delta\xi_D$, whereas they incur a malware diffusion cost ς_D and need to bear a detection loss $\alpha\xi_S$. During this period, the privacy is accessed by the IoT devices that receive a gain $\varepsilon\xi_A$. In contrast, the edge nodes will earn a gain due to a successful detection, but they stand a loss $(1-\alpha)\delta\xi_D$ due to an error detection. Edge nodes should also bear the loss $\varepsilon\xi_A$ caused by privacy leaks and a detection cost ς_S. Therefore, the revenue of IoT devices and edge nodes are $(1-\alpha)\delta\xi_D + \varepsilon\xi_A - \alpha\xi_S - \varsigma_D$ and $\alpha\xi_S - (1-\alpha)\delta\xi_D - \varepsilon\xi_A - \varsigma_S$, respectively.

In the second case, IoT devices make malicious requests and edge nodes deny the requests, which means the nodes successfully defend the malware. At that time, IoT devices receive a gain $\delta\xi_D$ due to malware diffusion but incur a malware diffusion cost ς_D, and bear a detection loss $\alpha\xi_S$. In contrast, the edge nodes earn a gain $\alpha\xi_S$ due to a successful detection, but they stand a loss $\delta\xi_D$ due to malware diffusion and a successful detection cost ς_S. Edge nodes also earn a gain $\varepsilon\xi_A$ because of successful privacy preservation. Therefore, the revenue of IoT devices and edge nodes are $\delta\xi_D - \alpha\xi_S - \varsigma_D$ and $\alpha\xi_S + \varepsilon\xi_A - \delta\xi_D - \varsigma_S$, respectively.

In the third case, IoT devices make normal requests and edge nodes grant the requests, which means that the nodes have secure access to privacy data. At that

time, the IoT devices acquire a gain ξ_C and an additional trust gain ϱ due to the normal request, but they also sustain a cost loss ς_C. In terms of the edge nodes, they acquire a gain ξ_P because of successful privacy preservation, while there is a successful detection cost ς_S. Therefore, the revenue of IoT devices and edge nodes are $\xi_C + \varrho - \varsigma_C$ and $\xi_P - \varsigma_S$, respectively.

In the fourth case, IoT devices make normal requests and edge nodes deny the requests, which means the nodes make an error detection. The expected revenue of IoT devices is similar to that of the third case. Furthermore, the edge nodes must pay a loss $\beta\gamma$ due to the false alarm and a detection cost ς_S. Therefore, the revenue of IoT devices and edge nodes are $\xi_C + \varrho - \varsigma_C$ and $-\beta\gamma - \varsigma_S$, respectively.

3.3. Evolutionary privacy preservation strategies analyses

In this section, we analyze the replication dynamics of IoT devices and edge nodes, as well as obtain the equilibrium point by solving the replication dynamic equations. Finally, we investigate the evolutionarily stable strategies of the two sides of the game. The conclusion can provide suggestions for edge nodes to realize privacy preservation during the process of IoT data sharing.

3.3.1. Replication dynamic equations

According to Table 3, the expected revenue of IoT devices making malicious requests is as follows:

$$\begin{aligned} E(RM) = {} & q((1-\alpha)\delta\xi_D + \varepsilon\xi_A - \alpha\xi_S - \varsigma_D) \\ & + (1-q)(\delta\xi_D - \alpha\xi_S - \varsigma_D) \end{aligned} \tag{1}$$

and the expected revenue of IoT devices making normal requests is as follows:

$$\begin{aligned} E(RN) &= q(\xi_C + \varrho - \varsigma_C) \\ &\quad + (1-q)(\xi_C + \varrho - \varsigma_C) \\ &= \xi_C + \varrho - \varsigma_C \end{aligned} \tag{2}$$

Therefore, the average expected revenue of IoT devices according to [10, 60] is as follows:

$$\overline{E(R)} = p * E(RM) + (1-p) * E(RN) \tag{3}$$

Furthermore, the replication dynamic equation of IoT devices is as follows:

$$\begin{aligned} R(p) = \frac{dp}{dt} &= p * (E(RM) - \overline{E(R)}) \\ &= p * (1-p) * (E(RM) - E(RN)) \\ &= p * (1-p) * (q * (-\alpha\delta\xi_D + \varepsilon\xi_A) \\ &\quad + \delta\xi_D - \alpha\xi_S - \varsigma_D - \xi_C - \varrho + \varsigma_C) \end{aligned} \tag{4}$$

However, the expected revenue of edge nodes denying a request is as follows:

$$\begin{aligned} E(DD) = {} & p(\alpha\xi_S + \varepsilon\xi_A - \delta\xi_D - \varsigma_S) \\ & + (1-p)(-\beta\gamma - \varsigma_S) \end{aligned} \tag{5}$$

and the expected revenue of edge nodes granting a request is as follows:

$$\begin{aligned} E(DG) = {} & p(\alpha\xi_S - (1-\alpha)\delta\xi_D - \varepsilon\xi_A - \varsigma_S) \\ & + (1-p)(\xi_P - \varsigma_S) \end{aligned} \tag{6}$$

Therefore, the average expected revenue of edge nodes is as follows:

$$\overline{E(D)} = q * E(DG) + (1-q) * E(DD) \tag{7}$$

Furthermore, the replication dynamic equation of edge nodes is as follows:

$$\begin{aligned} D(q) = \frac{dq}{dt} &= (1-q) * (E(DD) - \overline{E(D)}) \\ &= q * (1-q) * (E(DD) - E(DG)) \\ &= q * (1-q) * (p * (2\varepsilon\xi_A - \alpha\delta\xi_D \\ &\quad + \beta\gamma + \xi_P) - \beta\gamma - \xi_P) \end{aligned} \tag{8}$$

3.3.2. Evolutionarily stable strategy analyses

According to Eq. (4), we let $R(p) = 0$; there are three states as follows:

$$p = 0 \tag{9}$$

$$p = 1 \tag{10}$$

$$q = \frac{\alpha\xi_S + \varsigma_D + \xi_C + \varrho - \varsigma_C - \delta\xi_D}{-\alpha\delta\xi_D + \varepsilon\xi_A} \tag{11}$$

According to Eq. (8), we let $D(p) = 0$; there are three states as follows:

$$q = 0 \tag{12}$$

$$q = 1 \tag{13}$$

$$p = \frac{\beta\gamma + \xi_P}{2\varepsilon\xi_A - \alpha\delta\xi_D + \beta\gamma + \xi_P} \tag{14}$$

Theorem 1: While $q > \frac{\alpha\xi_S + \varsigma_D + \xi_C + \varrho - \varsigma_C - \delta\xi_D}{-\alpha\delta\xi_D + \varepsilon\xi_A}$, $p = 1$ is the only point of convergence of IoT devices selecting an action, meaning that IoT devices make a malicious request to the edge nodes after evolutionarily playing the game.

Proof. See Appendix A.

According to Eqs. (A.2) and (A.3), the phase diagram of Eq. (4) is demonstrated in Fig. 2. It is shown that this curve tends to 1, illustrating that if $q > \frac{\alpha\xi_S + \varsigma_D + \xi_C + \varrho - \varsigma_C - \delta\xi_D}{-\alpha\delta\xi_D + \varepsilon\xi_A}$, then $p = 1$ is the only point of convergence of IoT devices selecting an action.

Theorem 1 indicates that regardless of if the edge nodes choose to grant or deny the request, the revenue of IoT devices making normal requests is always less than that of making malicious requests when the probability of edge nodes denying IoT device requests is greater than the value of an evolutionarily stable strategy. Hence, IoT devices make malicious requests to edge nodes. This strategy behavior incurs IoT data privacy leaks. Therefore, administrators should try to configure the IDSaaS and adjust the parameters

Table 3. Payoff matrix.

IoT devices	Edge Nodes	
	***Detect* & *Grant* (*DG*)**	***Detect* & *Deny* (*DD*)**
Request Maliciously (RM)	$(1-\alpha)\,\delta\xi_D + \varepsilon\xi_A - \alpha\xi_S - \varsigma_D$, $\alpha\xi_S - (1-\alpha)\,\delta\xi_D - \varepsilon\xi_A - \varsigma_S$	$\delta\xi_D - \alpha\xi_S - \varsigma_D$, $\delta\xi_S + \varepsilon\xi_A - \delta\xi_D - \varsigma_S$
Request Normally (RN)	$\xi_C + \varrho - \varsigma_C$, $\xi_P - \varsigma_S$,	$\xi_C + \varrho - \varsigma_C$, $-\beta\gamma - \varsigma_S$

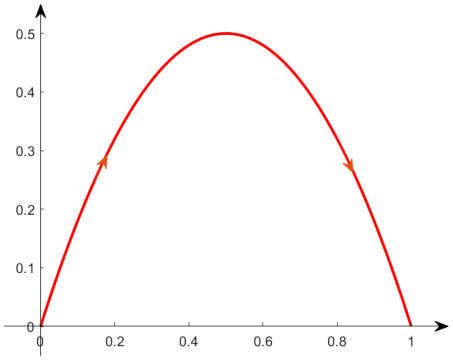

Fig. 2: Phase diagram of replication dynamic equation of IoT devices, such that $q > \frac{\alpha\xi_S+\varsigma_D+\xi_C+\varrho-\varsigma_C-\delta\xi_D}{-\alpha\delta\xi_D+\varepsilon\xi_A}$.

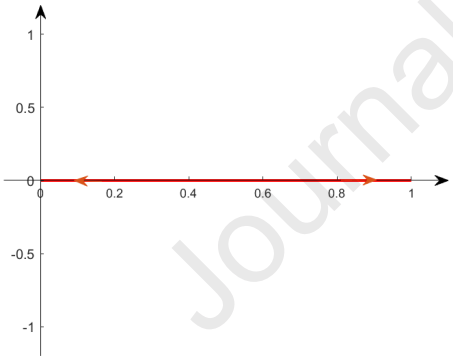

Fig. 3: Phase diagram of replication dynamic equation of IoT devices, such that $q = \frac{\alpha\xi_S+\varsigma_D+\xi_C+\varrho-\varsigma_C-\delta\xi_D}{-\alpha\delta\xi_D+\varepsilon\xi_A}$.

of edge-based IoT networks in practice to avoid satisfying the condition of Theorem 1 to maximally preserve data privacy during the process of IoT data sharing.

Theorem 2: While $q = \frac{\alpha\xi_S+\varsigma_D+\xi_C+\varrho-\varsigma_C-\delta\xi_D}{-\alpha\delta\xi_D+\varepsilon\xi_A}$, there is no convergence point.

Proof: To reach a stable state, it needs to satisfy $R'(p) < 0$. However, if $q = \frac{\alpha\xi_S+\varsigma_D+\xi_C+\varrho-\varsigma_C-\delta\xi_D}{-\alpha\delta\xi_D+\varepsilon\xi_A}$, then $R(p) = 0$ for $\forall p$, as shown in Fig. 3. Hence, there is no stable status in this case. This completes the proof.

Theorem 3: While $q < \frac{\alpha\xi_S+\varsigma_D+\xi_C+\varrho-\varsigma_C-\delta\xi_D}{-\alpha\delta\xi_D+\varepsilon\xi_A}$, $p = 0$ is the only point of convergence of IoT devices selecting

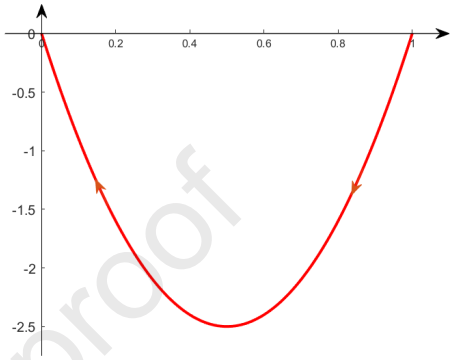

Fig. 4: Phase diagram of replication dynamic equation of IoT devices, such that $q < \frac{\alpha\xi_S+\varsigma_D+\xi_C+\varrho-\varsigma_C-\delta\xi_D}{-\alpha\delta\xi_D+\varepsilon\xi_A}$.

an action, meaning that IoT devices make normal requests to the edge nodes after evolutionarily playing the game.

Proof. See Appendix B.

From Eqs. (B.1) and (B.2), the phase diagram of Eq. (4) is given in Fig. 4. It is proven that this curve tends to 0, emphasizing that if $q < \frac{\alpha\xi_S+\varsigma_D+\xi_C+\varrho-\varsigma_C-\delta\xi_D}{-\alpha\delta\xi_D+\varepsilon\xi_A}$, then $p = 0$ is the only point of convergence in IoT devices selecting an action.

Theorem 3 indicates that regardless of if the edge nodes choose to grant or deny requests, the revenue of IoT devices making malicious requests is always less than that of making normal requests when the probability of edge nodes denying IoT devices requests is less than the value of the evolutionarily stable strategy. Hence, IoT devices make normal requests to the edge nodes, which is beneficial for preserving data privacy during the process of IoT data sharing. Therefore, administrators should keep the current configuration of the IDSaaS and edge-based IoT networks to satisfy the condition of Theorem 3, such that the privacy preservation of IoT data sharing is consistent.

Theorem 4: While $p > \frac{\beta\gamma+\xi_P}{2\varepsilon\xi_A-\alpha\delta\xi_D+\beta\gamma+\xi_P}$, $q = 1$ is the only point of convergence of edge nodes selecting an action, meaning that the edge nodes deny the requests of IoT devices after evolutionarily playing the game.

Proof. See Appendix C.

Based on Eqs. (C.2) and (C.3), the phase diagram of Eq. (8) is displayed in Fig. 5. It is indicated that this curve tends to 1, clarifying that if $p > \frac{\beta\gamma+\xi_P}{2\varepsilon\xi_A-\alpha\delta\xi_D+\beta\gamma+\xi_P}$, then $q = 1$ is the only point of convergence of edge

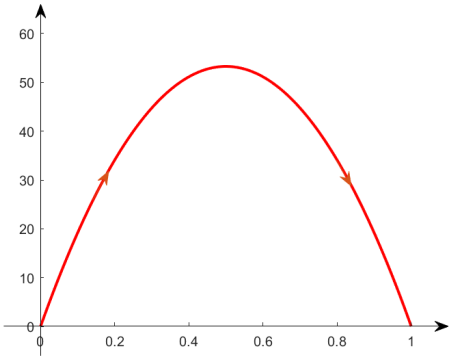

Fig. 5: Phase diagram of replication dynamic equation of edge nodes, such that $p > \frac{\beta\gamma+\xi_P}{2\varepsilon\xi_A-\alpha\delta\xi_D+\beta\gamma+\xi_P}$.

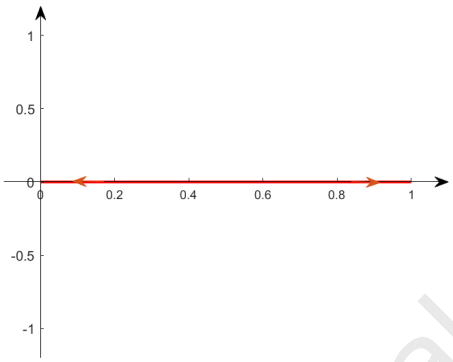

Fig. 6: Phase diagram of replication dynamic equation of edge nodes, such that $p = \frac{\beta\gamma+\xi_P}{2\varepsilon\xi_A-\alpha\delta\xi_D+\beta\gamma+\xi_P}$.

nodes selecting an action.

Theorem 4 explains that regardless of if IoT devices make malicious or normal requests, the revenue of edge nodes granting requests is always less than that of denying requests when the probability of IoT devices making malicious requests is greater than the value of an evolutionarily stable strategy. Hence, the edge nodes eventually deny IoT device requests, preventing the IoT data from leakage.

Theorem 5: While $p = \frac{\beta\gamma+\xi_P}{2\varepsilon\xi_A-\alpha\delta\xi_D+\beta\gamma+\xi_P}$, there is no convergence point.

Proof: To reach a stable state, it needs to satisfy $D'(q) < 0$. However, if $p = \frac{\beta\gamma+\xi_P}{2\varepsilon\xi_A-\alpha\delta\xi_D+\beta\gamma+\xi_P}$, then $D(q) = 0$ for $\forall q$, as shown in Fig. 6. Hence, there is no stable status in this case. This completes the proof.

Theorem 6: While $p < \frac{\beta\gamma+\xi_P}{2\varepsilon\xi_A-\alpha\delta\xi_D+\beta\gamma+\xi_P}$, $q = 0$ is the only point of convergence of edge nodes selecting an action, meaning that the edge nodes grant the requests of IoT devices after evolutionarily playing the game.

Proof. See Appendix D.

Considering Eqs. (D.1) and (D.2), the phase diagram of Eq. (8) is explicated in Fig. 7. It is

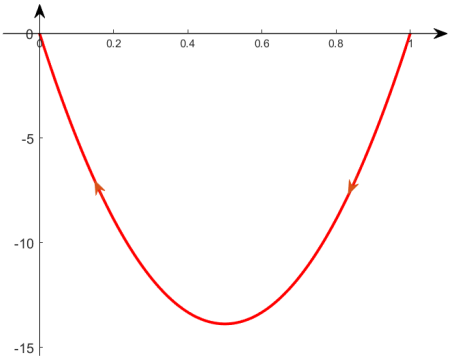

Fig. 7: Phase diagram of replication dynamic equation of edge nodes, such that $p < \frac{\beta\gamma+\xi_P}{2\varepsilon\xi_A-\alpha\delta\xi_D+\beta\gamma+\xi_P}$.

presented that this curve tends to 0, meaning that if $p < \frac{\beta\gamma+\xi_P}{2\varepsilon\xi_A-\alpha\delta\xi_D+\beta\gamma+\xi_P}$, then $q = 0$ is the only point of convergence of edge nodes selecting an action.

Theorem 6 indicates that regardless of if IoT devices make malicious or normal requests, the revenue of edge nodes denying requests is always less than that of granting requests when the probability of IoT devices making malicious requests is less than the value of an evolutionarily stable strategy. Hence, the edge nodes eventually grant IoT device requests.

3.4. Evolutionary privacy preservation stability analysis

Stability analysis provides the optimal choice for the game model. To be specific, the edge nodes can be seen as the players, which are bounded rationally in the game, and it is unable to search out the evolutionarily stable point at the beginning. Thus, they must learn constantly and correct their strategic mistakes gradually in the gaming process. At the end of the game, both sides of the game tend to converge to a stable strategy. Therefore, they acquire a satisfactory result concurrently by stability analyses based on trial and error. Based on Eqs. (4), (8), (A.1), and (C.1), we obtain the Jacobian matrix $\mathbb{J}$ according to [61] as follows:

$$\mathbb{J} = \begin{bmatrix} \frac{\partial R(p)}{\partial p} & \frac{\partial R(p)}{\partial q} \\ \frac{\partial D(q)}{\partial p} & \frac{\partial D(q)}{\partial q} \end{bmatrix} \tag{15}$$

where the equations are as follows:

$$\begin{aligned} \frac{\partial R(p)}{\partial p} &= (1-2p) * (q * (-\alpha\delta\xi_D + \varepsilon\xi_A) \\ &\quad + \delta\xi_D - \alpha\xi_S - \varsigma_D - \xi_C - \varrho + \varsigma_C) \end{aligned} \tag{16}$$

$$\frac{\partial R(p)}{\partial q} = p(1-p)(-\alpha\delta\xi_D + \varepsilon\xi_A) \tag{17}$$

$$\frac{\partial D(q)}{\partial p} = q(1-q)(2\varepsilon\xi_A - \alpha\delta\xi_D + \beta\gamma + \xi_P) \tag{18}$$

$$\frac{\partial D(q)}{\partial q} = (1-2q)(p*(2\varepsilon\xi_A - \alpha\delta\xi_D + \beta\gamma + \xi_P) - \beta\gamma - \xi_P) \tag{19}$$

Then, we analyze the stability of each equilibrium point illustrated in Table 4.

In Table 4, we have the equations as follows:

$$q^* = \frac{\alpha\xi_S + \varsigma_D + \xi_C + \varrho - \varsigma_C - \delta\xi_D}{-\alpha\delta\xi_D + \varepsilon\xi_A} \tag{20}$$

$$p^* = \frac{\beta\gamma + \xi_P}{2\varepsilon\xi_A - \alpha\delta\xi_D + \beta\gamma + \xi_P} \tag{21}$$

$$X^* = \frac{(\beta\gamma + \xi_P)(2\varepsilon\xi_A - \alpha\delta\xi_D)(-\alpha\delta\xi_D + \varepsilon\xi_A)}{(2\varepsilon\xi_A - \alpha\delta\xi_D + \beta\gamma + \xi_P)^2} \tag{22}$$

and

$$Y^* = U^* \frac{V^* W^*}{(-\alpha\delta\xi_D + \varepsilon\xi_A - \alpha\xi_S)^2} \tag{23}$$

where the equations are as follows:

$$U^* = (\alpha\xi_S + \varsigma_D + \xi_C + \varrho - \varsigma_C - \delta\xi_D) \tag{24}$$

$$V^* = (-\alpha\delta\xi_D + \varepsilon\xi_A - 2\alpha\xi_S + \delta\xi_D - \varsigma_D - \xi_C - \varrho + \varsigma_C) \tag{25}$$

and W^* is as follows:

$$W^* = (2\varepsilon\xi_A - \alpha\delta\xi_D + \beta\gamma + \xi_P) \tag{26}$$

From Table 3, we obviously attain the equations as follows:

$$\begin{aligned} &\xi_C + \varrho - \varsigma_C > \delta\xi_D - \alpha\xi_S - \varsigma_D \\ &\Rightarrow \delta\xi_D - \alpha\xi_S - \varsigma_D - \xi_C - \varrho + \varsigma_C < 0 \end{aligned} \tag{27}$$

$$\xi_P - \varsigma_S > -\beta\gamma - \varsigma_S \;\Rightarrow\; -\beta\gamma - \xi_P < 0 \tag{28}$$

and the equation as follows:

$$\begin{aligned} &\alpha\xi_S + \varepsilon\xi_A - \delta\xi_D - \varsigma_S \\ &> \alpha\xi_S - (1-\alpha)\delta\xi_D - \varepsilon\xi_A - \varsigma_S \\ &\Rightarrow 2\varepsilon\xi_A - \alpha\delta\xi_D > 0 \end{aligned} \tag{29}$$

We next derive evolutionarily privacy preservation stable points under two cases.

Case 1: $\xi_C+\varrho-\varsigma_C > (1-\alpha)\delta\xi_D+\varepsilon\xi_A-\alpha\xi_S-\varsigma_D$. This case represents that the revenue of IoT devices making normal requests is more than that of making malicious requests when edge nodes grant IoT devices requests.

Case 2: $\xi_C + \varrho - \varsigma_C < (1-\alpha)\delta\xi_D + \varepsilon\xi_A - \alpha\xi_S - \varsigma_D$. This case indicates that the revenue of IoT devices making normal requests is less than that of those making malicious requests when edge nodes grant IoT device requests.

Theorem 7: Under both Cases 1 and 2, only $(0,0)$ is evolutionarily stable and $(\frac{\alpha\xi_S+\varsigma_D+\xi_C+\varrho-\varsigma_C-\delta\xi_D}{-\alpha\delta\xi_D+\varepsilon\xi_A}, \frac{\beta\gamma+\xi_P}{2\varepsilon\xi_A-\alpha\delta\xi_D+\beta\gamma+\xi_P})$ is the saddle point.

Proof: We assume the matrix as follows:

$$A = \begin{vmatrix} \frac{\partial R(p)}{\partial p} & \frac{\partial R(p)}{\partial q} \\ \frac{\partial D(q)}{\partial p} & \frac{\partial D(q)}{\partial q} \end{vmatrix} \tag{30}$$

and introduce

$$\tau\mathbf{E} = \begin{vmatrix} \tau & 0 \\ 0 & \tau \end{vmatrix} \tag{31}$$

then obtain

$$\begin{aligned} |\tau\mathbf{E} - A| &= \begin{vmatrix} \tau & 0 \\ 0 & \tau \end{vmatrix} - \begin{vmatrix} \frac{\partial R(p)}{\partial p} & \frac{\partial R(p)}{\partial q} \\ \frac{\partial D(q)}{\partial p} & \frac{\partial D(q)}{\partial q} \end{vmatrix} \\ &= \begin{vmatrix} \tau - \frac{\partial R(p)}{\partial p} & -\frac{\partial R(p)}{\partial q} \\ -\frac{\partial D(q)}{\partial p} & \tau - \frac{\partial D(q)}{\partial q} \end{vmatrix} \end{aligned} \tag{32}$$

Based on "stability theory for ordinary differential equations" [62], if and only if both the eigenvalues of the Jacobian matrix are negative, the equilibrium point is stable; if one eigenvalue is positive and the other is negative, it is a saddle point; if both eigenvalues are positive, it is unstable. Thus, we can summarily tabulate the eigenvalues of each point, as shown in Table 5.

When the equilibrium point is $(0,0)$, the matrix is as follows:

$$A = \begin{vmatrix} \delta\xi_D - \alpha\xi_S - \varsigma_D - \xi_C - \varrho + \varsigma_C & 0 \\ 0 & -\beta\gamma - \xi_P \end{vmatrix} \tag{33}$$

We can obtain two eigenvalues τ_1 and τ_2 as follows:

$$\tau_1 = \delta\xi_D - \alpha\xi_S - \varsigma_D - \xi_C - \varrho + \varsigma_C < 0 \tag{34}$$

and

$$\tau_2 = -\beta\gamma - \xi_P < 0 \tag{35}$$

From Eqs. (34) and (35), both eigenvalues τ_1 and τ_2 are less than zero under Cases 1 and 2. Therefore, point $(0,\ 0)$ is evolutionarily stable. Similarly, for $(0,\ 1)$, $(1,\ 0)$, and $(1,\ 1)$, it is easy to obtain eigenvalues τ_1 and τ_2. Then, comparing these two eigenvalues with 0, we can eventually attain that $(1,\ 0)$ is an unstable point, and the stability of $(0,\ 1)$ and $(1,\ 1)$ are unable to be assessed. For, (q^*, p^*), it can be expressed as follows:

$$A = \begin{vmatrix} 0 & X^* \\ Y^* & 0 \end{vmatrix} \tag{36}$$

We can obtain two eigenvalues τ_1 and τ_2 as follows:

$$\tau_1 = \sqrt{X^* Y^*} \tag{37}$$

and

$$\tau_2 = -\sqrt{X^* Y^*} \tag{38}$$

The eigenvalues obviously satisfy $\xi_1 > 0$ and $\xi_2 < 0$ in both Cases 1 and 2. Hence, (q^*, p^*) is a saddle point. Furthermore, for ease of checking, we tabulate the stability of each case, as shown in Table 6. This completes the proof.

Theorem 7 considers the stability of each equilibrium point under the two above cases and seeks out that the equilibrium point $(0,\ 0)$ is an evolutionarily stable strategy through trial and error. In practice, $(0,\ 0)$ represents that IoT devices make normal requests, and the edge nodes grant the requests, preserving sensitive information privacy while sharing IoT data.

Table 4. Stability of each equilibrium point.

Equilibrium Point	$\frac{\partial R(p)}{\partial p}$	$\frac{\partial R(p)}{\partial q}$	$\frac{\partial D(q)}{\partial p}$	$\frac{\partial D(q)}{\partial q}$
$(0,0)$	$\delta\xi_D - \alpha\xi_S - \varsigma_D - \xi_C - \varrho + \varsigma_C$	0	0	$-\beta\gamma - \xi_P$
$(0,1)$	$-\delta\xi_D + \alpha\xi_S + \varsigma_D + \xi_C + \varrho - \varsigma_C$	0	0	$2\varepsilon\xi_A - \alpha\delta\xi_D$
$(1,0)$	$-\alpha\delta\xi_D + \varepsilon\xi_A - \alpha\xi_S + \delta\xi_D - \varsigma_D - \xi_C - \varrho + \varsigma_C$	0	0	$\beta\gamma + \xi_P$
$(1,1)$	$\alpha\delta\xi_D - \varepsilon\xi_A + \alpha\xi_S - \delta\xi_D + \varsigma_D + \xi_C + \varrho - \varsigma_C$	0	0	$-2\varepsilon\xi_A + \alpha\delta\xi_D$
(q^*, p^*)	0	X^*	Y^*	0

Table 5. Eigenvalues of each equilibrium point.

Equilibrium Point	Eigenvalues
$(0,0)$	$\tau_1 = \delta\xi_D - \alpha\xi_S - \varsigma_D - \xi_C - \varrho + \varsigma_C,\ \tau_2 = -\beta\gamma - \xi_P$
$(0,1)$	$\tau_1 = -\alpha\delta\xi_D + \varepsilon\xi_A - \alpha\xi_S + \delta\xi_D - \varsigma_D - \xi_C - \varrho + \varsigma_C,\ \tau_2 = 2\varepsilon\xi_A - \alpha\delta\xi_D$
$(1,0)$	$\tau_1 = -\delta\xi_D + \alpha\xi_S + \varsigma_D + \xi_C + \varrho - \varsigma_C,\ \tau_2 = \beta\gamma + \xi_P$
$(1,1)$	$\tau_1 = \alpha\delta\xi_D - \varepsilon\xi_A + \alpha\xi_S - \delta\xi_D + \varsigma_D + \xi_C + \varrho - \varsigma_C,\ \tau_2 = -2\varepsilon\xi_A + \alpha\delta\xi_D$
(q^*, p^*)	$\tau_1 = \sqrt{X^*Y^*},\ \tau_2 = -\sqrt{X^*Y^*}$

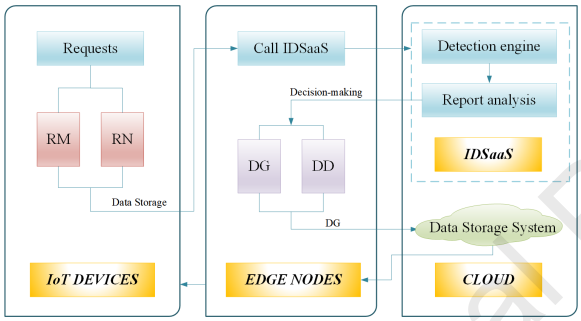

Fig. 8: Application framework of our evolutionary privacy preservation learning game.

3.5. Application framework

Based on the evolutionary privacy preservation learning game, we present a specific data-sharing architecture model as an application framework of our game, which is divided into three parts, as shown in Fig. 8. IoT devices choose to take a malicious request or a normal request and send their requests to the corresponding edge nodes. After receiving these requests, edge nodes then call the IDSaaS deployed in the cloud to detect the requests, and the IDSaaS returns the analysis report back to the edge nodes to determine whether to grant or deny the IoT device requests. If the edge nodes make a decision “grant", it is transmitted to the cloud storage system. In the end, IoT devices finally successfully access the data across edge nodes. This completes a cycle. When a new IoT device would like to access IoT data stored in the cloud storage system, the above cycle starts again. In our framework, attaining the optimal learning strategy for preserving privacy while sharing data is the core, which guides edge nodes to optimally choose the response.

3.6. Evolutionary learning algorithm

Here, we develop an evolutionary learning algorithm to obtain the optimal privacy preservation strategy for edge nodes while sharing IoT data from the perspective of practice. During the loop, the expected revenue of IoT devices making malicious and normal requests is first calculated according to Eqs. (1) and (2). Based on this, the average expected revenue of IoT devices is obtained by Eq. (3), and then the relevant replication dynamic equation is obtained by Eq. (4). Similarly, the expected revenue of edge nodes denying and granting IoT device requests are calculated according to Eqs. (5) and (6). We next acquire the expected revenue and the replication dynamic equations of edge nodes from Eqs. (7) and (8). This process is not suspended until the difference between two probabilities of IoT devices making malicious requests and the difference between two probabilities of edge nodes denying IoT device requests are both less than the predefined minimum boundary. Thus, the optimal strategy of denying malicious IoT device requests is eventually obtained, which can provide a potent foundation for IoT data-sharing privacy preservation.

4. Experimental Performance Evaluations

We utilize MATLAB R2021a to conduct experimental simulations and validate evolutionarily stable strategies for privacy preservation while sharing IoT data. We observe the evolutionary process of IoT devices and edge nodes, as well as verify the correctness of the above evolutionarily stable strategy analyses. Furthermore, we investigate the influence of the detection rate, successful diffusion rate, privacy risk factor, and trust gain on the edge node evolution stability strategy and the influence of the false alarm rate

Table 6. Stability of each equilibrium point in each case.

Equilibrium Point	Case 1			Case 2			Result
	τ_1	τ_2	stability	τ_1	τ_2	stability	
$(0, 0)$	−	−	ESS	−	−	ESS	ESS
$(0, 1)$	−	+	Saddle point	+	+	Unstable	Uncertain
$(1, 0)$	+	+	Unstable	+	+	Unstable	Unstable
$(1, 1)$	+	−	Saddle point	−	−	ESS	Uncertain
(q^*, p^*)	+	−	Saddle point	+	−	Saddle point	Saddle point

Algorithm 1 Evolutionary learning algorithm to obtain privacy preservation strategies for the edge-based IoT data sharing scheme

Input: Game parameters α, β, γ, δ, ε, ξ_A, ξ_P, ϱ, ξ_D, ξ_C, ξ_S, ς_D, ς_C, ς_S

Output: Optimal privacy preservation probability $q(t+1)$

Initialize game parameters α, β, γ, δ, ε, ξ_A, ξ_P, ϱ, ξ_D, ξ_C, ξ_S, ς_D, ς_C, ς_S;
$t \leftarrow 0$; $p(0) \leftarrow 0.5$; $q(0) \leftarrow 0.5$;
Construct the payoff matrix of the evolutionary privacy preservation learning game;
while .True. **do**
  $M \leftarrow q(t)((1-\alpha)\delta\xi_D + \varepsilon\xi_A - \alpha\xi_S - \varsigma_D) + (1 - q(t))(\delta\xi_D - \alpha\xi_S - \varsigma_D)$;
  $N \leftarrow q(t)(\xi_C + \varrho - \varsigma_C) + (1 - q(t))(\xi_C + \varrho - \varsigma_C)$;
  $E(R) \leftarrow p(t) * M + (1 - p(t)) * N$;
  $q(t+1) \leftarrow q(t) + p(t) * (M - E(R))$;
  $D \leftarrow p(t)(\alpha\xi_S + \varepsilon\xi_A - \delta\xi_D - \varsigma_S) + (1 - p(t))(-\beta\gamma - \varsigma_S)$;
  $G \leftarrow p(t)(\alpha\xi_S - (1-\alpha)\delta\xi_D - \varepsilon\xi_A - \varsigma_S) + (1 - p(t))(\xi_P - \varsigma_S)$;
  $E(D) \leftarrow q(t) * G + (1 - q(t)) * D$;
  $p(t+1) \leftarrow p(t) + (1 - q(t)) * (D - E(D))$;
  if $q(t+1) - q(t) < \sigma$ and $p(t+1) - p(t) < \sigma$ **then** // σ is the predefined minimum bound
    EXIT;
  $t \leftarrow t + 1$;
return the optimal privacy preservation probability $q(t+1)$;

on the IoT device evolution stability strategy. The results provide experimental verification for the design of an IoT data sharing privacy preservation scheme.

4.1. Verifying evolutionarily stable strategies of IoT devices

For this experiment, we set initial parameters $\alpha = 0.85$, $\beta = 0.3$, $\gamma = 30$, $\delta = 0.3$, $\varepsilon = 0.75$, $\xi_A = 70$, $\xi_P = 80$, $\varrho = 10$, $\xi_D = 20$, $\xi_C = 10$, $\xi_S = 40$, $\varsigma_D = 5$, $\varsigma_C = 10$, $\varsigma_S = 20$. It can be obtained that

$$q = \frac{\alpha\xi_S + \varsigma_D + \xi_C + \varrho - \varsigma_C - \delta\xi_D}{-\alpha\delta\xi_D + \varepsilon\xi_A} \approx 0.9072 \tag{39}$$

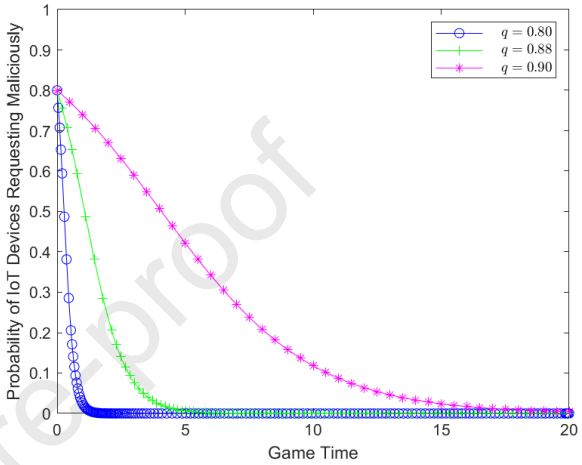

Fig. 9: Evolution curves of IoT devices strategy selection when $q < \frac{\alpha\xi_S + \varsigma_D + \xi_C + \varrho - \varsigma_C - \delta\xi_D}{-\alpha\delta\xi_D + \varepsilon\xi_A}$.

Therefore, we next analyze the strategy selection of IoT devices under two cases $q < 0.9072$ and $q > 0.9072$.

4.1.1. Case 1: Probability of edge nodes denying requests is less than the value obtained by the initial parameters

In this case, the probability of IoT devices making malicious requests is initially set as $p = 0.8$, and the probabilities of the edge nodes denying IoT devices requests q are set as 0.80, 0.88, and 0.90. It shows a downward trend, as shown in Fig. 9. It is notable that the lower the probability of the edge nodes denying IoT device requests, the faster it converges to 0, which means that the IoT devices tend to choose normal requests. For instance, it sharply decreases to 0 during the 2nd game when the probability of edge nodes denying IoT device requests is 0.8, whereas it comes to 0 in the 20th game when the probability of edge nodes denying IoT device requests is 0.9. It is indicated that the normal request is the evolutionarily stable strategy of IoT devices when $q < \frac{\alpha\xi_S + \varsigma_D + \xi_C + \varrho - \varsigma_C - \delta\xi_D}{-\alpha\delta\xi_D + \varepsilon\xi_A}$.

4.1.2. Case 2: Probability of edge nodes denying requests is greater than the value obtained by the initial parameters.

Then, we set the probability of IoT devices making malicious requests as $p = 0.2$ and the probabil-

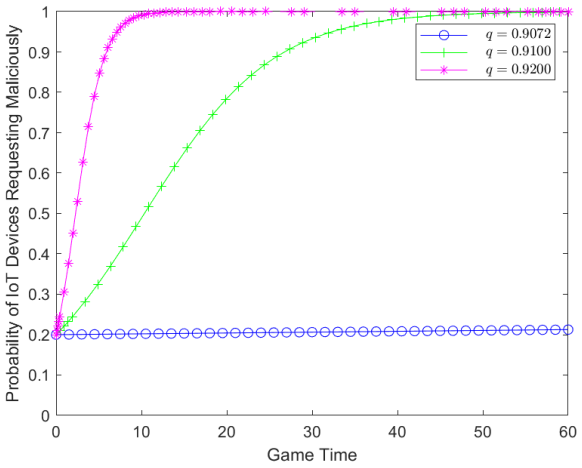

Fig. 10: Evolution curves of IoT devices strategy selection when $q > \frac{\alpha\xi_S+\varsigma_D+\xi_C+\varrho-\varsigma_C-\delta\xi_D}{-\alpha\delta\xi_D+\varepsilon\xi_A}$.

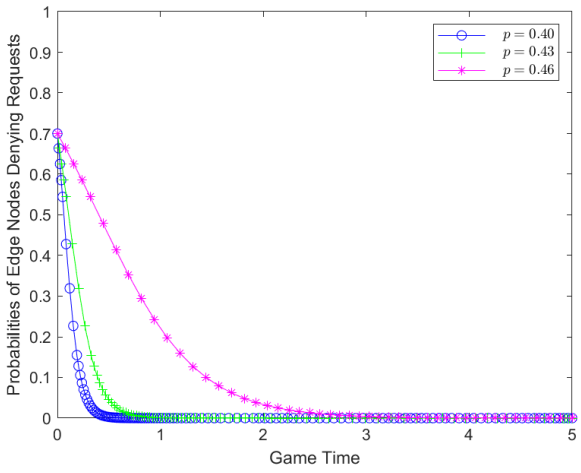

Fig. 11: Evolution curves of edge nodes strategy selection when $p < \frac{\beta\gamma+\xi_P}{2\varepsilon\xi_A-\alpha\delta\xi_D+\beta\gamma+\xi_P}$.

ities of the edge nodes denying IoT devices requests q are set as 0.9072, 0.9100, and 0.9200. There is an upward trend, as shown in Fig. 10. The probability of IoT devices adopting a malicious request remains stable when the probability of the edge nodes denying IoT device requests is 0.9072, meaning that there is no evolution at that time. Furthermore, the higher the probability of the edge nodes denying IoT device requests, the faster it converges to 1, which means that IoT devices tend to choose malicious requests. For instance, it increases to 1 in the 15th game when the probability of the edge nodes denying IoT device requests is 0.92, while it increases to 1 during the 55th game when the detection rate is 0.91. From the analyses above, there is no evolutionarily stable strategy for the edge nodes when $q = \frac{\alpha\xi_S+\varsigma_D+\xi_C+\varrho-\varsigma_C-\delta\xi_D}{-\alpha\delta\xi_D+\varepsilon\xi_A}$, and the malicious request is the evolutionarily stable strategy of IoT devices when $q > \frac{\alpha\xi_S+\varsigma_D+\xi_C+\varrho-\varsigma_C-\delta\xi_D}{-\alpha\delta\xi_D+\varepsilon\xi_A}$.

4.2. *Verifying evolutionarily stable strategies of edge nodes*

For this experiment, we set the initial parameters $\alpha = 0.85, \beta = 0.3, \gamma = 30, \delta = 0.3, \varepsilon = 0.75, \xi_A = 70, \xi_P = 80, \varrho = 10, \xi_D = 20, \xi_C = 10, \xi_S = 40, \varsigma_D = 5, \varsigma_C = 10, \varsigma_S = 20$. It can be obtained that

$$p = \frac{\beta\gamma + \xi_P}{2\varepsilon\xi_A - \alpha\delta\xi_D + \beta\gamma + \xi_P} \approx 0.4711 \qquad (40)$$

Therefore, we next analyze the strategy selection of edge nodes under two cases $p < 0.4711$ and $p > 0.4711$.

4.2.1. *Case 1: Probability of IoT devices making malicious requests is less than the value obtained by the initial parameters*

In this case, the probability of edge nodes denying IoT device requests is set as $q = 0.7$ and the probabilities of IoT devices making malicious requests p are set as 0.40, 0.43, and 0.46. There is a downward trend, as shown in Fig. 11. Noticeably, the lower the probability of IoT devices making malicious requests, the faster it converges to 0, which means the edge nodes tend to grant the requests. Taking $p = 0.40$ and $p = 0.46$ as examples, the former plunges to 0 in approximately a half game, while the latter requires the 3rd game to fall to 0. It is implied that the granting request is the evolutionarily stable strategy of edge nodes when $p < \frac{\beta\gamma+\xi_P}{2\varepsilon\xi_A-\alpha\delta\xi_D+\beta\gamma+\xi_P}$.

4.2.2. *Case 2: Probability of IoT devices making malicious requests is greater than the value obtained by the initial parameters*

Then, we set the probability of IoT devices making malicious requests as $q = 0.3$, and the probabilities of the edge nodes denying IoT devices requests p are set as 0.4711, 0.4800, and 0.5200. It shows an upward trend in Fig. 12. The probability of the edge nodes denying requests stabilizes when the probability of making malicious requests is 0.4711, meaning that there is no evolution at that time. Moreover, the higher the probability of IoT devices making malicious requests, the faster it converges to 1, which means that the edge nodes tend to deny the requests. A case in point is that it shoots up to 1 in a half game when the probability of IoT devices making malicious requests is 0.52, while it comes to 1 in approximately the 5th game when the probability of requesting maliciously is 0.48. In short, there is no evolutionarily stable strategy for edge nodes when $p = \frac{\beta\gamma+\xi_P}{2\varepsilon\xi_A-\alpha\delta\xi_D+\beta\gamma+\xi_P}$, and denying requests is an evolutionarily stable strategy for edge nodes when $p > \frac{\beta\gamma+\xi_P}{2\varepsilon\xi_A-\alpha\delta\xi_D+\beta\gamma+\xi_P}$.

4.3. *Verifying evolutionarily stable strategies on both sides*

For this experiment, we set the initial parameters $\alpha = 0.85, \beta = 0.3, \gamma = 30, \delta = 0.3, \varepsilon = 0.75, \xi_A = 70, \xi_P = 80, \varrho = 10, \xi_D = 20, \xi_C = 10, \xi_S = 40, \varsigma_D = 5, \varsigma_C = 10, \varsigma_S = 20$. We next analyze the

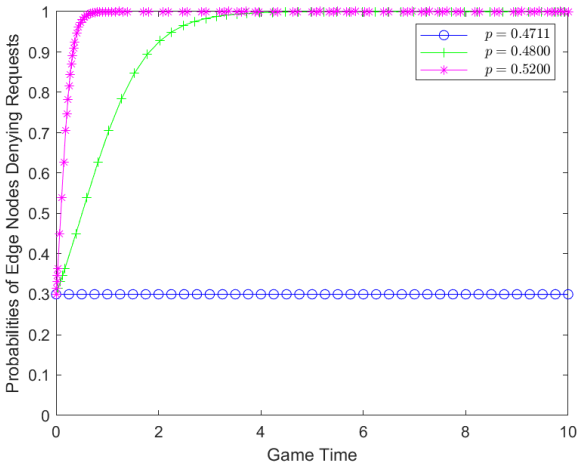

Fig. 12: Evolution curves of edge nodes strategy selection when $p > \frac{\beta\gamma+\xi_P}{2\varepsilon\xi_A-\alpha\delta\xi_D+\beta\gamma+\xi_P}$.

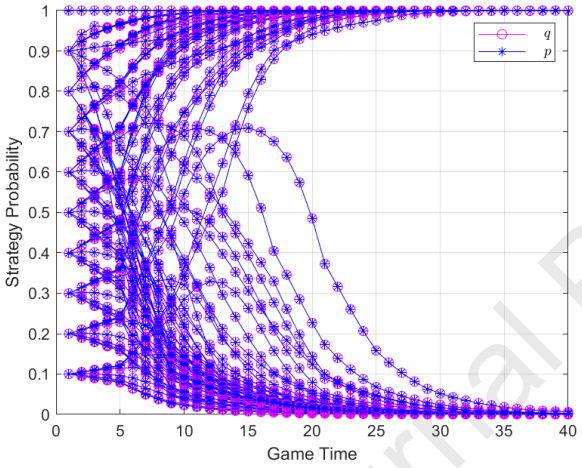

Fig. 13: Evolutionarily stable strategies on both sides while $\xi_C+\varrho-\varsigma_C < (1-\alpha)\delta\xi_D+\varepsilon\xi_A-\alpha\xi_S-\varsigma_D$.

strategy selection of IoT devices and edge nodes under two cases $\xi_C+\varrho-\varsigma_C < (1-\alpha)\delta\xi_D+\varepsilon\xi_A-\alpha\xi_S-\varsigma_D$ and $\xi_C+\varrho-\varsigma_C > (1-\alpha)\delta\xi_D+\varepsilon\xi_A-\alpha\xi_S-\varsigma_D$.

4.3.1. *Case 1: Revenue of IoT devices making normal requests is more than that of making malicious requests when the edge nodes grant IoT device requests*

According to Table 6, we can see that $(0,0)$ and $(1,1)$ are evolutionarily stable points when $\xi_C+\varrho-\varsigma_C < (1-\alpha)\delta\xi_D+\varepsilon\xi_A-\alpha\xi_S-\varsigma_D$. As shown in Fig. 13, the game strategy eventually evolves into *(Request Normally, Detect & Grant)* or *(Request maliciously, Detect & Deny)*, simultaneously verifying that the analysis in Table 6 is true.

4.3.2. *Case 2: Revenue of IoT devices making normal requests is less than that of making malicious requests when the edge nodes grant IoT device requests.*

Then, we reset ξ_C to 20. From Table 6, only $(0,\ 0)$ is an evolutionarily stable point when $\xi_C+\varrho-\varsigma_C > (1-\alpha)\delta\xi_D+\varepsilon\xi_A-\alpha\xi_S-\varsigma_D$, meaning that the game strategy eventually evolves into *(Request Normally, Detect & Grant)*. As shown in Fig. 14, they all converge to 0, illustrating that $(0,\ 0)$ is the stable point, which verifies that the analysis in Table 6 is true. In other words, the edge nodes tend to choose granting requests, and IoT devices tend to adopt requesting normally.

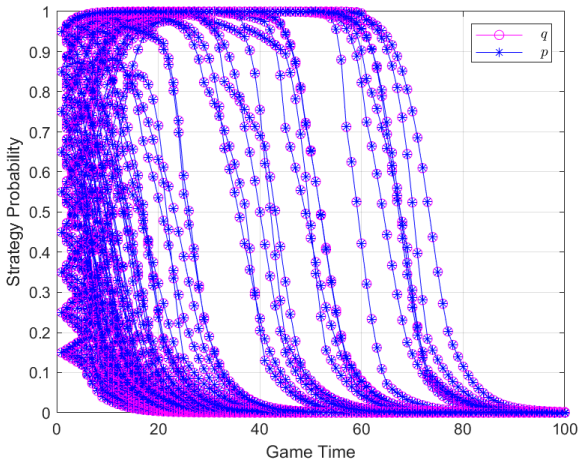

Fig. 14: Evolutionarily stable strategies on both sides while $\xi_C+\varrho-\varsigma_C > (1-\alpha)\delta\xi_D+\varepsilon\xi_A-\alpha\xi_S-\varsigma_D$.

4.4. *Influence of related parameters on IoT device strategy selection*

For this experiment, we set initial parameters $\alpha = 0.85$, $\beta = 0.3$, $\gamma = 30$, $\delta = 0.3$, $\varepsilon = 0.75$, $\xi_A = 70$, $\xi_P = 80$, $\varrho = 10$, $\xi_D = 20$, $\xi_C = 10$, $\xi_S = 40$, $\varsigma_D = 5$, $\varsigma_C = 45$, $\varsigma_S = 20$. We next analyze the influence of the detection rate, successful diffusion rate, trust gain, and privacy risk factor on IoT device strategy selection.

4.4.1. *Influence of detection rate α on the strategy selection of IoT devices*

To assess the effect of the detection rate on IoT device strategy selection, we set $p = 0.5$, $q = 0.1$, and reset α to 0.7, 0.75, 0.8, and 0.9. According to Fig. 15, when the detection rate is low, IoT devices tend to choose malicious requests. Meanwhile, the poorer the detection rate is, the faster it converges to 1. For instance, it almost reaches 1 in the 2nd game when the detection rate is equal to 0.7, while it approaches 1 in the 6th game when the detection rate is equal to 0.75. In contrast, when the detection rate is high, IoT devices tend to choose normal requests. Similarly, the higher the detection rate is, the faster it converges to 0. As a proof, it decreases to 0 in the 1st game when the detection rate is equal to 0.8, while it reaches 0 in the 4th game when the detection rate is 0.9. It is demonstrated that advancing the detection rate can decrease the probability that IoT devices adopt the malicious request strategy, which protects IoT data privacy.

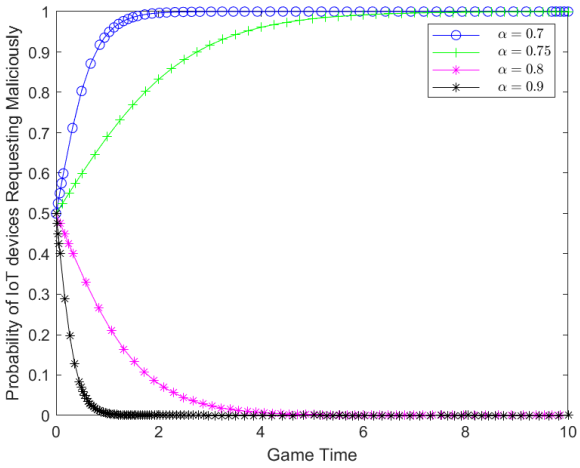

Fig. 15: Influence of the detection rate on IoT device strategy selection.

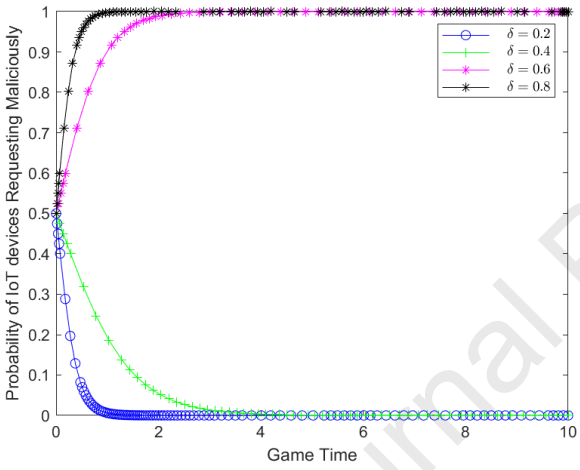

Fig. 16: Influence of the successful diffusion rate on IoT device strategy selection.

4.4.2. *The influence of the successful diffusion rate δ on the strategy selection of IoT devices*

To assess the effect of the diffusion rate on IoT device strategy selection, we set $p = 0.5$, $q = 0.1$ and reset δ to 0.2, 0.4, 0.6, and 0.8, respectively. As seen from Fig. 16, when the diffusion rate is low, IoT devices tend to choose normal requests. Moreover, the poorer the diffusion rate is, the faster it converges to 0. For example, it plunges to 0 in the 1st game when the diffusion rate is 0.2, while it falls to 0 in the 4th game when the detection rate is equal to 0.4. In contrast, when the diffusion rate is high, IoT devices tend to choose malicious requests. The higher the diffusion rate is, the faster it converges to 1. For $\delta = 0.6$, and $\delta = 0.8$, , the former soars to 1 during the 1st game, and the latter grows to 1 in approximately the 3rd game. It is illustrated that minimizing the diffusion rate can decrease the probability that IoT devices adopt the malicious request strategy, which protects privacy while sharing IoT data.

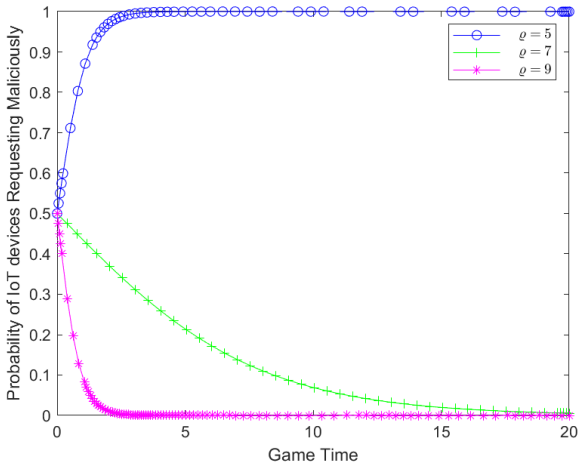

Fig. 17: Influence of the trust gain on IoT device strategy selection.

4.4.3. *Influence of trust gain ϱ on the strategy selection of IoT devices*

To assess the effect of trust gain on IoT device strategy selection, we set $p = 0.5$, $q = 0.1$, and reset ϱ to 5, 7, and 9. As shown in Fig. 17, when the trust gain is low, IoT devices tend to choose malicious requests. For instance, it ascends to 1 in the 3rd game when the trust gain is equal to 5. Conversely, when the trust gain is high, IoT devices tend to choose normal requests. Noticeably, the higher the trust gain is, the faster it converges to 0. A case in point is that it drops to 0 in the almost 20th game when the trust gain is 7, while it plummets to 0 in the 2nd game when the trust gain is 9. It is proven that improving trust gain can increase the probability that IoT devices adopt the normal request strategy to protect privacy while sharing IoT data.

4.4.4. *Influence of the privacy risk factor ε on the strategy selection of IoT devices*

To assess the effect of the privacy risk factor on IoT device strategy selection, we set $p = 0.8$, $q = 0.1$, and reset ε to 0.05, 0.7, and 0.95. There is a downward trend, as shown in Fig. 18. It is noteworthy that the poorer the privacy risk factor is, the faster it converges to 0. For $\varepsilon = 0.05$, $\varepsilon = 0.7$, and $\varepsilon = 0.95$, they all decline to 0 in the 1st, 2nd, and 4th games, respectively. It is verified that decreasing the privacy risk factor can increase the probability that IoT devices adopt the normal request strategy to protect IoT data-sharing privacy.

4.5. *Influence of false alarm rate β on the strategy selection of the edge nodes*

We next analyze the influence of the false alarm rate on the edge node strategy. Thus, we set the initial parameters $\alpha = 0.85$, $\gamma = 10$, $\delta = 0.3$, $\varepsilon = 0.75$, $\xi_A = 70$, $\xi_P = 30$, $\xi_D = 20$, $\xi_S = 40$, $\varsigma_S = 20$, $p = 0.1$, $q = 0.8$, and set β to 0.03, 0.05, and 0.08. According to Fig. 19, it is noteworthy that changes in the false alarm rate

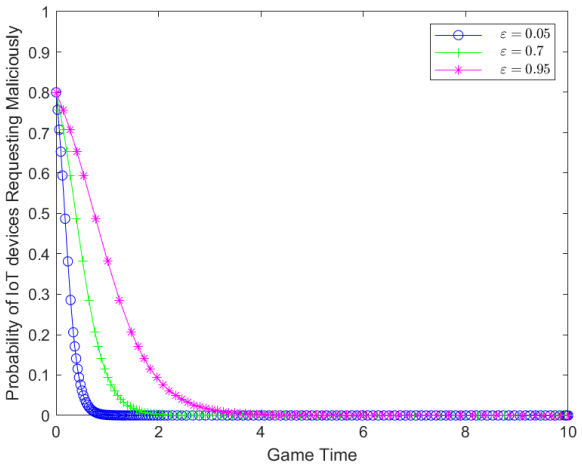

Fig. 18: Influence of the privacy risk factor on IoT device strategy selection.

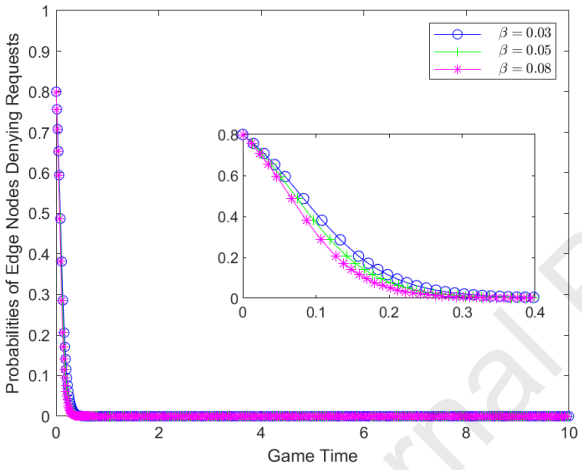

Fig. 19: Influence of the false alarm rate on the edge node strategy selection.

have little effect on the overall situation. They all converge to 0 with the same trend, which means that in this case, the edge nodes adopt the strategy of granting requests.

5. Conclusion and Future Work

In the current work, we have proposed an edge computing-oriented and evolutionary game-based privacy preservation model to acquire the optimal learning strategy for IoT data sharing. In our scheme, the edge nodes first assess whether the request is normal or malicious and then react with action grants or denies when data is released from the cloud storage system. Under this circumstance, malicious requests can be precisely identified and effectively prohibited from the source. Furthermore, we have analyzed the stability of each equilibrium point via the replication dynamic equations and raised a framework and an algorithm for this model, optimizing the expected gain and receiving the best evolutionary strategy. Additionally, the relevant experimental simulations verify that our scheme is superior from the perspectives of reliability and privacy preservation.

For future work, we will focus on other game models, such as signaling games and repeated games, to handle privacy preservation during IoT data sharing. In addition, we will take the privacy preservation of a data sender into consideration instead of a data receiver, minimizing the probability of IoT nodes sending malicious requests. Furthermore, it is highly likely to incur malicious attacks in the process of merging data from different IoT devices. Therefore, privacy preservation under IoT data aggregation is another direction with great promise.

Declaration of competing interest

The authors declare that they have no conflict of interest or personal relationships that could have appeared to influence the work reported in the current work.

Acknowledgements

This work was supported in part by Zhejiang Provincial Natural Science Foundation of China under Grant nos. LZ22F020002 and LY22F020003, National Natural Science Foundation of China under Grant nos. 61772018 and 62002226, and the key project of Humanities and Social Sciences in Colleges and Universities of Zhejiang Province under Grant no. 2021GH017.

Appendix A. Proof of Theorem 1

We take the derivative of both sides of Eq. (4) and obtain the equation as follows:

$$\begin{aligned} R'(p) = (1-2p) * (q * (-\alpha\delta\xi_D + \varepsilon\xi_A) \\ + \delta\xi_D - \alpha\xi_S - \varsigma_D - \xi_C - \varrho + \varsigma_C) \end{aligned} \tag{A.1}$$

To reach a stable state, it needs to satisfy $R'(p) < 0$. Let $p = 0$ and $p = 1$; we obtain the equation as follows:

$$\begin{aligned} R'(0) = q * (-\alpha\delta\xi_D + \varepsilon\xi_A) + \delta\xi_D \\ - \alpha\xi_S - \varsigma_D - \xi_C - \varrho + \varsigma_C > 0 \end{aligned} \tag{A.2}$$

and the equation as follows:

$$\begin{aligned} R'(1) = -(q * (-\alpha\delta\xi_D + \varepsilon\xi_A) + \delta\xi_D \\ - \alpha\xi_S - \varsigma_D - \xi_C - \varrho + \varsigma_C) < 0 \end{aligned} \tag{A.3}$$

Obviously, $p = 1$ is the only point of convergence of IoT devices selecting an action. This completes the proof.

Appendix B. Proof of Theorem 3

To reach a stable state, it needs to satisfy $R'(p) < 0$. Let $p = 0$ and $p = 1$ in Eq. (A.1), we obtain the equation as follows:

$$R'(0) = q * (-\alpha\delta\xi_D + \varepsilon\xi_A) + \delta\xi_D - \alpha\xi_S - \varsigma_D - \xi_C - \varrho + \varsigma_C < 0 \tag{B.1}$$

and the equation as follows:

$$R'(1) = -(q * (-\alpha\delta\xi_D + \varepsilon\xi_A) + \delta\xi_D - \alpha\xi_S - \varsigma_D - \xi_C - \varrho + \varsigma_C) > 0 \tag{B.2}$$

Obviously, $p = 0$ is the only point of convergence of IoT devices selecting an action. This completes the proof.

Appendix C. Proof of Theorem 4

We take the derivative of both sides of Eq. (8) and obtain the equation as follows:

$$D'(q) = (1 - 2q) * (p * (2\varepsilon\xi_A - \alpha\delta\xi_D + \beta\gamma + \xi_P) - \beta\gamma - \xi_P) \tag{C.1}$$

To reach a stable state, it needs to satisfy $D'(q) < 0$. Let $q = 0$ and $q = 1$; we obtain the equation as follows:

$$D'(0) = p * (2\varepsilon\xi_A - \alpha\delta\xi_D + \beta\gamma + \xi_P) - \beta\gamma - \xi_P > 0 \tag{C.2}$$

and the equation as follows:

$$D'(1) = -(p * (2\varepsilon\xi_A - \alpha\delta\xi_D + \beta\gamma + \xi_P) - \beta\gamma - \xi_P) < 0 \tag{C.3}$$

Obviously, $q = 1$ is the only point of convergence of edge nodes selecting an action. This completes the proof.

Appendix D. Proof of Theorem 6

To reach a stable state, it needs to satisfy $D'(q) < 0$. Let $q = 0$ and $q = 1$ in Eq. (C.1). We obtain the equation as follows:

$$D'(0) = p * (2\varepsilon\xi_A - \alpha\delta\xi_D + \beta\gamma + \xi_P) - \beta\gamma - \xi_P < 0 \tag{D.1}$$

and the equation as follows:

$$D'(1) = -(p * (2\varepsilon\xi_A - \alpha\delta\xi_D + \beta\gamma + \xi_P) - \beta\gamma - \xi_P) > 0 \tag{D.2}$$

Obviously, $q = 0$ is the only point of convergence of edge nodes selecting an action. This completes the proof.

References

[1] K. Sha, T. A. Yang, W. Wei, S. Davari, A survey of edge computing-based designs for iot security, Digit. Commun. Netw. 6 (2) (2020) 195–202.

[2] D. Wu, B. Yang, R. Wang, Scalable privacy-preserving big data aggregation mechanism, Digit. Commun. Netw. 2 (3) (2016) 122–129.

[3] Z. Wu, S. Shen, X. Lian, X. Su, E. Chen, A dummy-based user privacy protection approach for text information retrieval, Knowledge-Based Syst. 195 (2020) 105679.

[4] Z. Wu, G. Li, S. Shen, X. Lian, E. Chen, G. Xu, Constructing dummy query sequences to protect location privacy and query privacy in location-based services, World Wide Web 24 (1) (2021) 25–49.

[5] Y. Li, Y. Zhou, A. Jolfaei, D. Yu, G. Xu, X. Zheng, Privacy-preserving federated learning framework based on chained secure multiparty computing, IEEE Internet Things J 8 (8) (2021) 6178–6186.

[6] Z. Chen, W. Liao, K. Hua, C. Lu, W. Yu, Towards asynchronous federated learning for heterogeneous edge-powered internet of things, Digit. Commun. Netw. 7 (3) (2021) 317–326.

[7] M. Wang, T. Zhu, T. Zhang, J. Zhang, S. Yu, W. Zhou, Security and privacy in 6g networks: New areas and new challenges, Digit. Commun. Netw. 6 (3) (2020) 281–291.

[8] Y. Li, H. Ma, L. Wang, S. Mao, G. Wang, Optimized content caching and user association for edge computing in densely deployed heterogeneous networks, IEEE Trans. Knowl. Data Eng. (2020) Article in Press. http://dx.doi.org/10.1109/TMC.2020.3033563.

[9] J. Liu, X. Wang, G. Yue, S. Shen, Data sharing in vanets based on evolutionary fuzzy game, Future Gener. Comput. Syst. 81 (2018) 141–155.

[10] S. Shen, L. Huang, H. Zhou, S. Yu, E. Fan, Q. Cao, Multistage signaling game-based optimal detection strategies for suppressing malware diffusion in fog-cloud-based iot networks, IEEE Internet Things J. 5 (2) (2018) 1043–1054.

[11] S. Shen, H. Zhou, S. Feng, L. Huang, J. Liu, S. Yu, Q. Cao, Hsird: A model for characterizing dynamics of malware diffusion in heterogeneous wsns, J. Netw. Comput. Appl. 146 (2019) 102420.

[12] J. Liu, J. Yu, S. Shen, Energy-efficient two-layer cooperative defense scheme to secure sensor-clouds, IEEE Trans. Inf. Forensic Secur. 13 (2) (2018) 408–420.

[13] T. Wang, M. Z. A. Bhuiyan, G. Wang, L. Qi, J. Wu, T. Hayajneh, Preserving balance between privacy and data integrity in edge-assisted internet of things, IEEE Internet Things J. 7 (4) (2020) 2679–2689.

[14] J. Liu, X. Wang, S. Shen, G. Yue, S. Yu, M. Li, A bayesian q-learning game for dependable task offloading against ddos attacks in sensor edge cloud, IEEE Internet Things J. 8 (9) (2021) 7546–7561.

[15] C. L. Stergiou, K. E. Psannis, B. B. Gupta, Iot-based big data secure management in the fog over a 6g wireless network, IEEE Internet Things J. 8 (7) (2021) 5164–5171.

[16] K. Raichura, N. Padhariya, Bigcache: a cache-based bigdata management in mobile networks, Int. J. Mob. Commun. 15 (1) (2017) 49–68.

[17] H. Jin, D. Xu, C. Zhao, D. Liang, Information-centric mobile caching network frameworks and caching optimization: a survey, J. Netw. Comput. Appl. 146 (2017) 33.

[18] J. Liang, M. Zhang, V. C. M. Leung, A reliable trust computing mechanism based on multisource feedback and fog computing in social sensor cloud, IEEE Internet Things J. 7 (6) (2020) 5481–5490.

[19] B. Gong, J. Liu, S. Guo, A trusted attestation scheme for data source of internet of things in smart city based on dynamic trust classification, IEEE Internet Things J. 8 (21) (2021) 16121–16141.

[20] A. Tewari, B. B. Gupta, Secure timestamp-based mutual authentication protocol for iot devices using rfid tags, Int. J. Semant. Web Inf. Syst. 16 (3) (2020) 20–34.

[21] K. Fan, W. Jiang, H. Li, Y. Yang, Lightweight rfid protocol

for medical privacy protection in iot, IEEE Trans. Ind. Inform. 14 (4) (2018) 1656–1665.

[22] S. Xia, Z. Yao, Y. Li, S. Mao, Online distributed offloading and computing resource management with energy harvesting for heterogeneous mec-enabled iot, IEEE Trans. Wirel. Commun. 20 (10) (2021) 6743–6757.

[23] M. Mukherjee, R. Matam, C. X. Mavromoustakis, H. Jiang, G. Mastorakis, M. Guo, Intelligent edge computing: Security and privacy challenges, IEEE Commun. Mag. 58 (9) (2020) 26–31.

[24] F.-Y. Rao, E. Bertino, Privacy techniques for edge computing systems, Proc. IEEE 107 (2019) 1632–1654.

[25] D. Zhang, Y. Ma, X. Sharon Hu, D. Wang, Toward privacy-aware task allocation in social sensing-based edge computing systems, IEEE Internet Things J. 7 (12) (2020) 11384–11400.

[26] B. Gu, L. Gao, X. Wang, Y. Qu, J. Jin, S. Yu, Privacy on the edge: Customizable privacy-preserving context sharing in hierarchical edge computing, IEEE Trans. Netw. Sci. Eng. 7 (4) (2020) 2298–2309.

[27] X. Xu, C. He, Z. Xu, L. Qi, S. Wan, M. Z. A. Bhuiyan, Joint optimization of offloading utility and privacy for edge computing enabled iot, IEEE Internet Things J. 7 (4) (2020) 2622–2629.

[28] P. Zhou, W. Chen, S. Ji, H. Jiang, L. Yu, D. Wu, Privacy-preserving online task allocation in edge-computing-enabled massive crowdsensing, IEEE Internet Things J. 6 (2019) 7773–7787.

[29] Y. Zhen, H. Liu, Distributed privacy protection strategy for mec enhanced wireless body area networks, Digit. Commun. Netw. 6 (2) (2020) 229–237.

[30] X. Li, S. Liu, F. Wu, S. Kumari, J. J. P. C. Rodrigues, Privacy preserving data aggregation scheme for mobile edge computing assisted iot applications, IEEE Internet Things J. 6 (3) (2019) 4755–4763.

[31] G. Liu, C. Wang, X. Ma, Y. Yang, Keep your data locally: Federated-learning-based data privacy preservation in edge computing, IEEE Netw. 35 (2) (2021) 60–66.

[32] M. Du, K. Wang, Z. Xia, Y. Zhang, Differential privacy preserving of training model in wireless big data with edge computing, IEEE Trans. Big Data 6 (2) (2020) 283–295.

[33] X. He, R. Jin, H. Dai, Peace: Privacy-preserving and cost-efficient task offloading for mobile-edge computing, IEEE Trans. Wirel. Commun. 19 (3) (2020) 1814–1824.

[34] P. Zhao, H. Huang, X. Zhao, D. Huang, Privacy-preserving scheme against poisoning attacks in mobile-edge computing, IEEE Trans. Comput. Social Syst. 7 (3) (2020) 818–826.

[35] M. Du, K. Wang, Y. Chen, X. Wang, Y. Sun, Big data privacy preserving in multi-access edge computing for heterogeneous internet of things, IEEE Commun. Mag. 56 (8) (2018) 62–67.

[36] H. Li, J. Yu, H. Zhang, M. Yang, H. Wang, Privacy-preserving and distributed algorithms for modular exponentiation in iot with edge computing assistance, IEEE Internet Things J. 7 (9) (2020) 8769–8779.

[37] C. T. Do, N. H. Tran, C. Hong, C. A. Kamhoua, K. A. Kwiat, E. Blasch, S. Ren, N. Pissinou, S. S. Iyengar, Game theory for cyber security and privacy, ACM Comput. Surveys. 50 (2017) 30.

[38] M. Ezhei, B. Tork Ladani, Information sharing vs. privacy: A game theoretic analysis, Expert Syst. Appl. 88 (2017) 327–337.

[39] L. Cui, Y. Qu, M. R. Nosouhi, S. Yu, J. W. Niu, G. Xie, Improving data utility through game theory in personalized differential privacy, J. Comput. Sci. Technol. 34 (2) (2019) 272–286.

[40] Y. Qu, S. Yu, L. Gao, W. Zhou, S. Peng, A hybrid privacy protection scheme in cyber-physical social networks, IEEE Trans. Comput. Social Syst. 5 (3) (2018) 773–784.

[41] J. Zhang, L. Xu, P. W. Tsai, Community structure-based trilateral stackelberg game model for privacy protection, Appl. Math. Model. 86 (2020) 20–35.

[42] K. Li, L. Tian, W. Li, G. Luo, Z. Cai, Incorporating social interaction into three-party game towards privacy protection in iot, Comput. Netw. 150 (2019) 90–101.

[43] J. Xiong, M. Zhao, M. Z. A. Bhuiyan, L. Chen, Y. Tian, An ai-enabled three-party game framework for guaranteed data privacy in mobile edge crowdsensing of iot, IEEE Trans. Ind. Inform. 17 (2) (2021) 922–933.

[44] V. Sivaraman, B. Sikdar, A game-theoretic approach for enhancing data privacy in sdn-based smart grids, IEEE Internet Things J. 8 (13) (2020) 10583–10595.

[45] R. Jin, X. He, H. Dai, On the security-privacy tradeoff in collaborative security: A quantitative information flow mame perspective, IEEE Trans. Inf. Forensic Secur. 14 (12) (2019) 3273–3286.

[46] A. Riahi Sfar, Y. Challal, P. Moyal, E. Natalizio, A game theoretic approach for privacy preserving model in iot-based transportation, Intell. Transp. Syst. 20 (12) (2019) 4405–4414.

[47] M. R. Nosouhi, S. Yu, K. Sood, M. Grobler, R. Jurdak, A. Dorri, S. Shen, Ucoin: An efficient privacy preserving scheme for cryptocurrencies, IEEE Trans. Dependable Secur. Comput. (2021) Article in Press. http://dx.doi.org/10.1109/TDSC.2021.3130952.

[48] Y. Liu, H. Wang, M. Peng, J. Guan, J. Xu, Y. Wang, Deepga: A privacy-preserving data aggregation game in crowdsensing via deep reinforcement learning, IEEE Internet Things J. 7 (5) (2020) 4113–4127.

[49] M. Liu, X. Zhou, M. Sun, Bilateral privacy-utility tradeoff in spectrum sharing systems: A game-theoretic approach, IEEE Trans. Wirel. Commun. 20 (8) (2021) 5144–5158.

[50] N. Wu, C. Peng, K. Niu, A privacy-preserving game model for local differential privacy by using information-theoretic approach, IEEE Access 8 (2020) 216741–216751.

[51] U. Mengibaev, X. Jia, Y. Ma, The impact of interactive dependence on privacy protection behavior based on evolutionary game, Appl. Math. Comput. 379 (2020) 125231.

[52] J. Du, C. Jiang, K.-C. Chen, Y. Ren, H. V. Poor, Community-structured evolutionary game for privacy protection in social networks, IEEE Trans. Inf. Forensic Secur. 13 (3) (2018) 574–589.

[53] P. J. Sun, The optimal privacy strategy of cloud service based on evolutionary game, Cluster Comput. 25 (1) (2022) 13–31.

[54] A. K. Das, A. Tabassum, S. Sadaf, D. Sinha, anonymity scheme for privacy preservation in location-based services on iot environment, Int. J. Autom. Control 15 (3) (2021) 340–362.

[55] R. Tourani, S. Misra, T. Mick, G. Panwar, Security, privacy, and access control in information-centric networking: A survey, IEEE Commun. Surveys Tuts. 20 (1) (2018) 566–600.

[56] R. Xu, J. Joshi, P. Krishnamurthy, An integrated privacy preserving attribute-based access control framework supporting secure deduplication, IEEE Trans. Dependable Secur. Comput. 18 (2) (2021) 706–721.

[57] Y. Qu, S. Yu, W. Zhou, S. Chen, J. Wu, Customizable reliable privacy-preserving data sharing in cyber-physical social networks, IEEE Trans. Netw. Sci. Eng. 8 (1) (2021) 269–281.

[58] M. U. Hassan, M. H. Rehmani, J. Chen, Differential privacy techniques for cyber physical systems: A survey, IEEE Commun. Surveys Tuts. 22 (1) (2020) 746–789.

[59] W. Yang, Y. Zhou, M. Hu, D. Wu, X. Zheng, J. H. Wang, S. Guo, C. Li, Gain without pain: Offsetting dp-injected nosies stealthily in cross-device federated learning, IEEE Internet Things J (2021) Article in Press. http://dx.doi.org/10.1109/JIOT.2021.3102030.

[60] J. W. Weibull, Evolutionary Game Theory, The MIT Press, 1995.

[61] R. Akkaoui, X. Hei, W. Cheng, An evolutionary game-theoretic trust study of a blockchain-based personal health data sharing framework, in: 2020 Information Communication Technologies Conference (ICTC), 2020.

[62] G. Teschl, Ordinary Differential Equations and Dynamical Systems, American Mathematical Society, Providence, 2012.

Declaration of interests

☒ 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.

☐The authors declare the following financial interests/personal relationships which may be considered as potential competing interests: