Hindawi
Wireless Communications and Mobile Computing
Volume 2020, Article ID 8891889, 13 pages
https://doi.org/10.1155/2020/8891889

Research Article

A Privacy-Preserving Personalized Service Framework through Bayesian Game in Social IoT

Renwan Bi,[1] Qianxin Chen,[1] Lei Chen,[2] Jinbo Xiong,[1] and Dapeng Wu[3]

[1]*Fujian Provincial Key Laboratory of Network Security and Cryptology, College of Mathematics and Informatics, Fujian Normal University, Fuzhou 350117, China*
[2]*College of Engineering and Computing, Georgia Southern University, GA 30458, USA*
[3]*Chongqing Key Laboratory of Optical Communication and Networks, Chongqing University of Posts and Telecommunications, Chongqing 400065, China*

Correspondence should be addressed to Jinbo Xiong; jbxiong@fjnu.edu.cn

Received 25 June 2020; Revised 10 September 2020; Accepted 4 October 2020; Published 17 October 2020

Academic Editor: Ximeng Liu

It is enormously challenging to achieve a satisfactory balance between quality of service (QoS) and users' privacy protection along with measuring privacy disclosure in social Internet of Things (IoT). We propose a privacy-preserving personalized service framework (Persian) based on static Bayesian game to provide privacy protection according to users' individual security requirements in social IoT. Our approach quantifies users' individual privacy preferences and uses fuzzy uncertainty reasoning to classify users. These classification results facilitate trustworthy cloud service providers (CSPs) in providing users with corresponding levels of services. Furthermore, the CSP makes a strategic choice with the goal of maximizing reputation through playing a decision-making game with potential adversaries. Our approach uses Shannon information entropy to measure the degree of privacy disclosure according to the probability of game mixed strategy equilibrium. Experimental results show that Persian guarantees QoS and effectively protects user privacy despite the existence of adversaries.

1. Introduction

The rapid development of cloud computing and big data technologies has greatly promoted work productivity and life quality. Along with such advancement, there come frequent user privacy disclosures that have attracted wide attention from academia and the industry [1]. In recent years, thanks to the marriage of wireless technologies [2] and mobile communications, social networks (SNs) have become an indispensable part of life [3]. Social networks enable communications and services far beyond instant messaging compared to traditional messaging services and applications [4]. The content of transmission has also become more diverse, including text, voice, image, video, and other multimedia data [5]. Data owners (e.g., mobile and smart device users) enjoy personalized services by gaining various application privileges while data collectors (e.g., service providers and application developers) obtain vast amounts of personal sensitive and security-critical data through privileged interfaces [6]. Such user data become attractive targets of attacks and are subject to serious privacy disclosures [7, 8].

According to the "China Privacy Risk Index Analysis Report" published by the trusted institutions in 2018, mobile Internet applications in the social category have an average of 11,014 users per App, and the average amount of data acquired can reach up to 21.24 pieces/user, which is the most among all categories of Apps. At present, the number of user data leakages increased by 15.46% from 2018, and the privacy risk index increased by 26.66% [9]. Users inevitably leave a trail of footprints in the real world while accessing online services from a mobile device [10]. For example, people share various information on Twitter, and even when the original blog is deleted, relevant comments remain on the web [11]. Additionally, 267 million Facebook users' information, including names, gender, email addresses, and social identity, are stolen in April 2020 and sold on the dark web [12]. Thus, protecting user's privacy and security is critically important yet challenging in social networks.

Social networking aspects, in recent years, have been extended to the Internet of Things (IoT) that autonomously build social relationships for smart devices to discover new objects and their services [13, 14]. The marriage of IoT and social network enables advanced and deep interactions among people and between people and the environment. Such advancement leads to the emergence of social IoT [13], where social approaches are employed for managing large volumes of user data with connected IoT devices [6, 15]. This can result in a greater challenge for user privacy in social IoT. Efficient and effective IoT nodal interactions rely on the establishment of trustworthy relationship among nodes [15, 16]. This is particularly important in helping overcome the perceptions of uncertainty and privacy risk [17, 18].

Two main reasons contribute to vast amounts of user privacy disclosure in social IoT [19]: technical deficiencies and economic interest conflicts among all participants. Therefore, the privacy protection of social IoT users should also be analyzed from these two aspects. At present, from the technical perspective, user privacy is protected mainly through anonymity [20, 21], differential privacy [22, 23], network access control [24, 25], and ecosystem [26] in social IoT.

Anonymity protection [20] hides private data in a data block so that other users are incapable of associating a user's real identity information with the collected data blocks. This is also a common problem of anonymous protection schemes, and it is difficult to defend against background knowledge attacks. Differential privacy protection [22, 27] adds small amounts of Laplace noise into the original data prior to publishing the data for added fuzziness where other users are incapable of distinguishing between the real data and the fuzzy data. Zhang et al. [27] attach importance to the social connection of users, consider the existence of untrusted service providers and malicious attackers, and propose and implement an effective IoT service with differential privacy protection. Despite the high data utility, it is difficult to implement personalized privacy at the user level according to the user's security requirements using differential privacy [23]. Network access control [24, 28] decides whether to grant authorized access by analyzing the credibility and closeness among visitors. While it implements privacy protection according to the wishes of data owners, it lacks an effective privacy measurement scheme.

Among the notable research works on the security and privacy of social IoT [19], Frustaci et al. addressed that security and privacy issues are a great challenge for IoT and yet they are also enabling factors to create a "trust ecosystem" [26]. Particularly, in their discussions of the importance of trust, excellent flexibility is considered as a critical factor to deal with changeable security conditions and personalized security requests. Users or nodes having defined personalized security and privacy policies should be facilitated to help in decision-making [26].

Considering big data privacy protection from the perspective of users' interests and economics, the existing literatures [29] mainly describe the benefits and costs of participants by employing game theory, simulate the rational selection process, and formulate the optimal privacy protection scheme through Nash equilibrium [21]. To some extent, these methods make up for the defects of technical schemes; yet how to balance the data utility and efficiency of privacy protection is still a difficult open issue.

In order to tackle this problem, this paper proposes the Persian framework, aiming at providing personalized services to social IoT users on the basis of protecting user privacy. Particularly, in order to resist against adversaries with background knowledge, static Bayesian game theory is applied to the strategic struggle between CSP and adversaries. The contributions in this paper are summarized as follows:

(i) *Implementing User Classification*. Aiming at the difficult problem of users' discrete attribute classification, we adopt the fuzzy uncertainty reasoning method to classify users according to the membership function and expert rules

(ii) *Defining Trust and Security Responsibilities of the CSP*. We construct a trust management center (TMC) that supervises the CSP's behavior and evaluates each service. TMC employs the incremental update strategy to manage the reputation of the CSP, so as to avoid CSP from proactively disclosing user privacy

(iii) *Achieving a Satisfactory Balance between Quality of Service (QoS) and Privacy Protection*. We use the mixed strategy equilibrium to explain the correctness of the CSP making services strategies against different types of adversaries. Moreover, we utilize Shannon information entropy to measure the privacy disclosure, thereby providing a theoretical basis for users' privacy protection in social IoT. Experimental results show that the Persian framework achieves the correct user privacy classification and trust assessment, while privacy disclosure is limited to a low degree

The rest of this paper is organized as follows: The related work is overviewed in Section 2. We illustrate the preliminaries, including fuzzy uncertainty reasoning and Bayesian game theory in Section 3. The system model and security model are introduced in Section 4. In Section 5, we present the modules of the Persian framework in detail, including user classification, trust management, Bayesian game, and privacy measurement. Experiments and evaluation are described in Section 6, and the study is concluded in Section 7.

2. Related Work

In social IoT, protecting user privacy has been a research hotspot due to frequent user privacy disclosures. Existing literatures mainly present from the two aspects of technology and economic interests. Anonymity, differential privacy, access control, and trust management are often adopted to protect users' privacy in social IoT.

Liu et al. [30] proposed a k-anonymous algorithm, which generates an initial weighted social network and reduces the adjustment of relation weight through the sorting process. It improves anonymity efficiency and resists against

1neighborhood attacks. However, this approach does not significantly improve the utility of anonymous data. Xie and Zheng [31] proposed a differential social network anonymous algorithm satisfying k-anonymity and l-diversity. For the key nodes and general nodes, the proposed algorithm uses different types of anonymous operations to transfer anonymous objects from privacy attributes to anonymized sensitive attributes. Based on implementing privacy protection, the proposed algorithm improves the utility of anonymous data. Furthermore, an indicator (UL) is constructed to measure the data utility loss. Chen et al. [32] proposed a classification data clustering scheme based on rough entropy and DBSCAN clustering algorithm, which effectively balances data utility and anonymity performance of mobile social networks. Nonetheless, it falls short on formal security analysis against the attacker.

Li et al. [33] proposed an MB-CI strategy for protecting the edge weights of social networks, which retains most of the shortest paths under the premise of satisfying differential privacy, effectively reducing the error caused by noise and improving the accuracy of published data. At the same time, it effectively resists against the consistent reasoning attacks on data records without user-level privacy protection.

Wang et al. [34] proposed a data publishing algorithm (RescueDP) satisfying differential privacy to protect real-time and spatiotemporal crowd-sourced data in social networks. They also proposed an enhanced neural network algorithm, which accurately predicts statistical data with added noise, thereby improving the utility of published data. Huang et al. [35] proposed a differential privacy protection method (PBCN) based on clustering and noise, aiming at achieving a "trade-off" between data availability and privacy protection level. Jahid et al. [36] proposed an encryption-based access control architecture (EASiER) to address privacy disclosure in online social networks. It transfers access control from the social network provider to users and implements fine-grained access control for dynamic social contacts using attribute-based encryption. Hu et al. [24] constructed a multiparty access control (MPAC) model and proposed a specific multiparty strategy specification scheme and strategy evaluation mechanism to protect the shared data associated with multiple users in online social networks against collusion attacks.

The existing literature also proposed a number of personalized privacy protection schemes. Cai et al. [37] proposed a data disinfection method for centralized processing of user configuration files and relationships among users. By controlling the set of user attributes and the relationship among users to hide sensitive information, the proposed method resists against the set inference attack in the process of data publishing in social networks. Cai et al. [38] proposed a privacy-preserving scheme for interactive messaging by leveraging user credibility and social behaviors, which guarantees the privacy protection in the process of information exchange through information confusion and sensitive attribute substitution. In order to solve the trust difficulties, Sharma et al. [39] proposed a novel solution in the form of fission computing. The proposed solution relies on the edge-crowd integration for maintenance of trust and preservation of privacy rules in Social IoT, using crowdsources as mini-edge servers and entropy modeling for defining trust between the entities.

Additional literature also considers privacy protection from the perspective of interests and puts forward a number of effective schemes and models utilizing game theory. Jin et al. [40] applied game theory to trajectory privacy protection. For any two sensing nodes in the network, this method selects the best strategy through the Bayesian game analysis to resist against the dishonest attacks of internal nodes, thus protecting the trajectory privacy of users. Hu et al. [41] proposed a multiparty control game, which extends the research on strategy selection among rational controllers in multiparty access control. The Nash equilibrium is used to explain the optimal strategy selection state, and no controller has any valid reason or authority to change its settings to deviate from the equilibrium, which solves the privacy conflict of collaborative data sharing in online social networks from the perspective of interests. Wu et al. [29] proposed an extended game model to solve the problem of privacy and utility equilibrium in the publishing of multicorrelated privacy data, which solves the differential privacy parameters according to Nash equilibrium, thereby improving data utility. Shan et al. [42] proposed a forwarding control mechanism for social networks based on game theory. By calculating the game revenue matrix of the publisher and forwarder and comparing the probability of dishonest forwarding with the threshold set by the publisher, this approach protects the privacy of publishing content according to the personalized privacy requirements of the publisher. Xiong et al. [21, 23] also actively applied game theory to the privacy protection of the application environment.

Xiong et al. [43] conducted a comprehensive survey on the privacy measurement and quantification of big data. Serjantov and Danezis [44] used the Shannon entropy to describe the effective size of anonymous sets. Lin et al. [45] employed mutual information to measure privacy disclosure under the data protection mechanism. Diaz et al. [46] utilized conditional entropy to describe adversaries' observation ability and indirectly measured the level of protection mechanism. Additionally, Chen et al. [47] proposed an information surprise indicator to measure the surprise degree that still exists after an adversary acquires user attributes.

3. Preliminaries

3.1. Fuzzy Uncertainty Reasoning. Fuzzy reasoning [48] is a method of uncertainty reasoning, which is suitable for any situation where the input fluctuates in a specific range. Also, the output is also fuzzy, rather than precise. The fuzzy concept is regarded as a membership degree [49], reflecting the closeness of input or output with a fuzzy set in the universe. If the membership degree equals 1, it means that the variable values belong to the fuzzy set completely; if the membership degree equals 0, it means that no elements belong to the fuzzy set absolutely. A membership value in (0, 1) means that some elements, but not all, belong to the fuzzy level to some extent. The membership function replaces the positive or negative results with the fuzzy evaluation results, which is helpful for

considering the influence of multiple factors. Generally, the membership function of the gradient type is widely accepted, as shown in Figure 1. Upon finding the membership, the rule activation is performed. The fuzzy output is generated by the activation of finite rules.

3.2. Bayesian Game Theory. The static Bayesian game (SBG) model [50] is also known as static incomplete information game. The type set of all participants is known. Any participant can only infer the probability that other participants belong to a certain type at a certain time, but cannot determine other participants' type and cannot determine the relevant action strategies or benefit. Furthermore, all participants choose action strategies simultaneously in the game. Even if there are differences in the order of choosing, the participants who choose the strategy posterior do not have the knowledge of the selected strategy. SBG model [50] can be represented by a quintuple, $\mathrm{SBG} = (\Gamma, T, P, S, U)$, which is described as follows:

(1) Participant set is $\Gamma = \{1, 2, \cdots, n\}$, where $n \geq 2$, because it is meaningless to discuss a game with only one participant. Any participant $i (i \in \Gamma)$ is a rational decision-maker with the ability of independent selection, whose goal is to maximize their expected benefit and choose action strategies

(2) Participant type set is $T = \{T_1, \cdots, T_n\}$, where T_i represents the participant i's types, $i \in \Gamma$, and $|T_i| \geq 2$. If each participant has only one candidate type (i.e., $\forall i \in \Gamma$ and $|T_i| = 1$), at the point, the static incomplete information game will become the static complete information game

(3) The probability set of participants' inference about the types of other participants is $P = \{P_1 < t_{-1} | t_1 >, \cdots, P_n < t_{-n} | t_n > \}$, where $P_i < t_{-i} | t_i >$ represents the probability of participant i's inference about the types of other participants. Meanwhile, t_i represents participant i's type, and t_{-i} (i.e., $\{t_1, \cdots, t_{i-1}, t_{i+1}, \cdots, t_n\}$) represents all participants' type other than participant i

(4) The participants' strategy set is $S = \{S_1(T_1), \cdots, S_n(T_n)\}$, where $S_i(T_i)(i \in \Gamma)$ (i.e., $S_i = \{s_i(1; t_i), \cdots, s_i(m; t_i)\}$) represents participant i's strategy set and $s_i(j; t_i)(j \in \{1, \cdots, m\})$ represents participant i's strategy

(5) The benefit function of participants is $U = \{U_1(T_1), \cdots, U_n(T_n)\}$, where $U_i(T_i)(i \in \Gamma)$ represents the participant i's benefit. Since $U_i = u_i(s_1, \cdots, s_{i-1}, s_{i+1}, \cdots, s_n; t_i)$, participant i's benefit is related to its own type and the strategy chosen by other participants

4. System Model and Security Model

We introduce important notations and descriptions in this paper, as shown in Table 1.

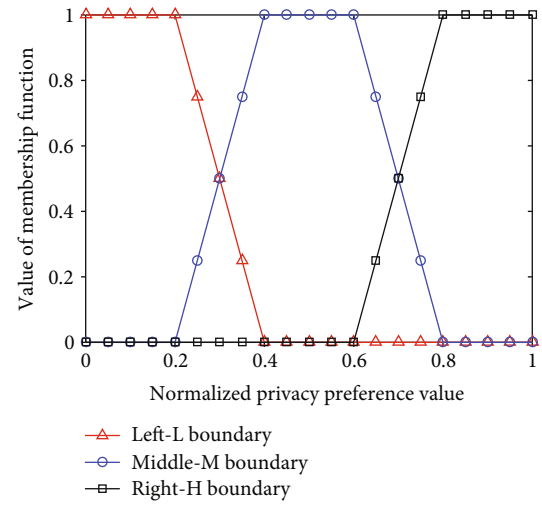

Figure 1: Membership function.

Table 1: Main notations and descriptions.

Notations	Descriptions
m	Trust depth
λ	Trust penalty factor
μ	Benefit factor
k	Background factor
θ	Trust threshold
δ_j^l	The reputation of CSP in j-th service
σ_j	Average reputation of CSP in previous j services
s	Action strategy set
u	Action benefit set
U	Total benefit of participant
P^*	Probability under mixed strategy equilibrium
H	Privacy information entropy

4.1. System Model. In social IoT, we mainly focus on how a CSP provides personalized services for users. The system model includes four entities: Users, CSP, TMC, and adversaries ($\mathscr{A}$), as shown in Figure 2.

(i) *Users* own multiattribute data, and obtain personalized services in exchange of providing private data and individual preferences to CSP

(ii) *CSP* is the back-end server of various applications in social IoT, which obtains user data through the application privilege interface and provides personalized services according to users' individual preference. Meanwhile, CSP plays static Bayesian game with adversaries and makes strategies

(iii) *TMC* is responsible for supervising CSP's behaviors, including managing and updating CSP's reputation.

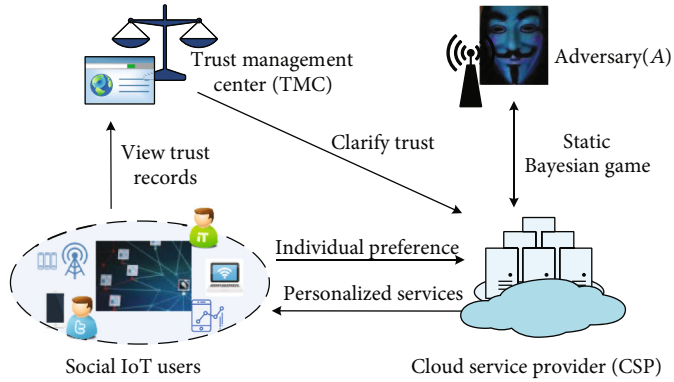

Figure 2: System model.

Social IoT users choose whether to trust CSP based on the reputation provided by TMC

(iv) $\mathscr{A}$ are malicious individuals or organizations in social IoT to obtain user private data by compromising communication links between users and CSP. Meanwhile, $\mathscr{A}$ play strategic game with the CSP to maximize their own benefits

4.2. Security Model. We consider that the proposed Persian framework is implemented in a semitrusted security model [51–53]. CSP is considered as an honest-but-greedy entity. On the one hand, it is supervised by the TMC and strictly implements protocols. On the other hand, it also hopes to obtain tremendous benefits through one-off privacy trafficking. TMC is regarded as a fully-trusted entity, which is in charge of managing the reputation of CSP without possessing any private information. $\mathscr{A}$ use rational judgment to attack adaptively. Their owned background knowledge can increase the probability of obtaining privacy. If $\mathscr{A}$ believes that there is no benefits from launching an attack, or if the CSP's strategy choices are indistinguishable, the Persian framework is considered secure.

5. The Construction Modules of Persian Framework

In this section, we illustrate the construction of the Persian framework in detail, including user classification, trust management, Bayesian game, and privacy measurement module.

5.1. Overview of Persian Framework. Above all, we explain the basic principles of the Persian framework, as illustrated in Figure 3. On the user side, users in social IoT score for each attribute according to their subjective security requirements. Having received the normalized multiattribute scores, the user classification module obtains individual privacy preferences based on fuzzy uncertainty reasoning. Before CSP provides personalized services to users, it is necessary to establish trust relationship, which is the responsibility of TMC with notarization. At the same time, there is a strategic game relationship between CSP and $\mathscr{A}$, and the hybrid strategy equilibrium results are used in

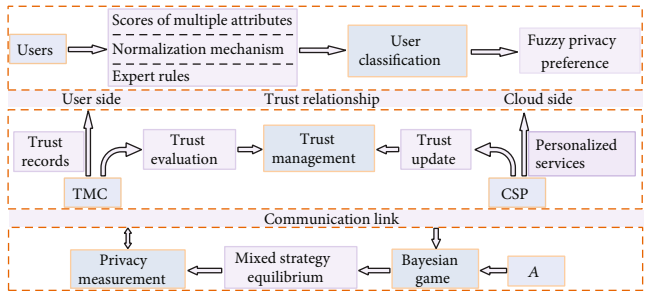

Figure 3: Overview of Persian framework.

privacy measurement module. Finally, TMC evaluates the services provided by CSP and performs trust update synchronously. Before each request for a service, users check the average reputation of CSP from TMC to determine whether to open data access to CSP. In essence, these entities constrain each other to provide users with secure personalized services.

5.2. Classifying User Privacy Level. Users in social IoT have multiple attributes of privacy data, mainly including natural attributes, social attributes, and behavioral attributes. Natural attributes are users' own identity information, such as names, ages, typically independent from external factors. Social attributes, such as occupational status, marriage status, among others, are a feature of users' integration into the society affected by social factors. Behavioral attributes represent users' pursuit of individual preferences and lifestyle, such as shopping preferences, and habits. Different users have different individual security requirements for each private attribute. In this section, based on users' individual privacy preference [54], we employ fuzzy uncertainty reasoning to classify users as the basis for the CSP to provide the corresponding level of service.

5.2.1. Normalizing User Attribute. In order to measure users' security requirements for private data, we define DP, degree of privacy preference, $(\mathrm{DP}_i = \{\mathrm{Name}_i, \mathrm{Age}_i, \mathrm{Occu}_i, \mathrm{Marr}_i, \mathrm{Shop}_i\}, i = 1,\cdots,5)$. Through a comprehensive investigation, we use users' natural attributes (Name and Age), social

Table 2: DP of user attribute.

Users	Name	Age	Occu	Marr	Shop
$u1$	8	2	9	10	4
$u2$	7	3	4	5	7
$u3$	5	6	7	7	3
$u4$	2	8	1	6	8
$u5$	9	1	7	4	3

Table 3: NDP of user attribute.

Users	Name	Age	Occu	Marr	Shop
$u1$	0.86	0.14	1	1	0.2
$u2$	0.71	0.29	0.38	0.17	0.8
$u3$	0.43	0.71	0.75	0.5	0
$u4$	0	1	0	0.33	1
$u5$	1	0	0.75	0	0

attributes (Occu and Marr), and behavioral attributes (Shop) as references. Anonymous users give a score (0–10 points) according to their subjective privacy requirements. We randomly selected five questions, as shown in Table 2.

Definition 1. Degree of privacy preference (DP) is used to measure users' attention to private data. The lower DP is, the lower the users' attention to data will be; otherwise, the higher the users' attention to data will be.

Since fuzzy reasoning requires the input to be numerical data within the interval [0,1], we adopt linear function to normalize DP. Taking the j-th attribute as an example, the normalization process is shown in Formula (1). After the same treatment, the normalized DP (NDP) is shown in Table 3.

$$\mathrm{NDP}_{i,j} = \frac{\mathrm{DP}_{i,j} - \min\left(\mathrm{DP}_{i,j}\right)}{\max\left(\mathrm{DP}_{i,j}\right) \min\left(\mathrm{DP}_{i,j}\right)}, i = 1, \cdots, 5. \quad (1)$$

5.2.2. Fuzzy Uncertainty Reasoning. Here, we use fuzzy reasoning of Mamdani [55] type to classify users. The advanced expert rules are shown in Table 4. The input fuzzy sets (Name, Age, Occu, Marr, and Shop) are composed of "high" and "low," which are represented by symbols "H" and "L," The output fuzzy sets (NDP) are composed of "high," "medium," and "low," which are represented by symbols "H," "M," and "L." We use u_3's attribute vector in Table 3 ([0.43, 0.71, 0.75, 0.5, 0]) as the fuzzy input. We can then obtain the membership degree of each input attribute to the fuzzy level through calculating the membership function, as illustrated in Table 5. Clearly, four rules are activated, namely,

13. NDP = L; min $(0.67,1,1,0.5,1) = 0.5$;
15. NDP = M; min $(0.67,1,1,0.5,1) = 0.5$;
29. NDP = M; min $(0.33,1,1,0.5,1) = 0.33$;
31. NDP = H; min $(0.33,1,1,0.5,1) = 0.33$;

The more satisfied the preceding part is, the stronger the rule will be, and the more instructive output will be. Since logic "and" is the link among the conditions in the preceding part, the strength of the four rules is determined by the "minimum value" method. Finally, we employ the central average defuzzy method to calculate the fuzzy output, and obtain the NDP's approximation result equaling 0.462 through computing Formula (2). Therefore, u_3 obviously belongs to the M level.

$$\mathrm{NDP} = \frac{\sum \bar{y} \cdot \mu(\bar{y})}{\sum \mu(\bar{y})} = 0.462. \quad (2)$$

In Formula (2), $\bar{y}$ represents the maximum of fuzzy level interval, and $\mu(\bar{y})$ represents NDP's membership value about the fuzzy level.

5.3. Trust Management. Users in social IoT submit data to CSP for personalized service, resulting in losing control of their personal data. In order to provide users with a satisfactory service experience, the trust for CSP needs to be clarified. Trust management [56] is to evaluate the target entity by referring to its historical behavior and reputation in social IoT. When social IoT users request to interact with a CSP, the service policy adopted by the CSP corresponds to a specific reputation value. CSP improves its reputation by providing good QoS. In turn, the reputation provides the basis for users to choose a CSP. We consider service behavior for J times and the reputation function of CSP as shown in the Formula.

$$\delta_j^l \begin{cases} -10 + \lambda & \text{if } l = -1 \\ 0 & \text{if } l = 0 \\ 1 & \text{if } l = L \\ 2 & \text{if } l = M \\ 3 & \text{if } l = H \end{cases}. \quad (3)$$

In (3), $j = \{0, 1, \cdots, J\}$, and $l \in \{-1, 0, L, M, H\}$. If $l = -1$, CSP actively discloses user privacy; if $l = 0$, CSP denies service. Other conditions indicate that CSP provides low, medium, and high QoS, respectively. Specially, we introduce a trust penalty factor λ, which represents the reputation penalty that CSP suffers from betraying trust. The construction function of λ is as below:

$$\lambda = -\sum_{j}{}' = j\text{-}m^{j-1} \mathbb{I}\left\{\delta_{j'}^{l} > 0\right\}, \quad (4)$$

where $|\lambda| \leq m$ is satisfied in any case, and $\mathbb{I}\{\cdot\}$ is a two-value function. If the logic is true, then $\mathbb{I}\{\cdot\} = 1$; otherwise, $\mathbb{I}\{\cdot\} = 0$. Obviously, the deeper the trust relationship of the CSP betrayal is, the greater the reputation penalty will be.

Combined with the above reputation function, it makes sense to think of trust as a threshold. When the CSP's reputation value is greater than the threshold, the user considers the CSP to be credible. To be more realistic, we consider

Table 4: Expert rules.

Num	Name	Age	Occu	Marr	Shop	NDP	Num	Name	Age	Occu	Marr	Shop	NDP
1	L	L	L	L	L	L	17	H	L	L	L	L	L
2	L	L	L	L	H	L	18	H	L	L	L	H	M
3	L	L	L	H	L	L	19	H	L	L	H	L	M
4	L	L	L	H	H	M	20	H	L	L	H	H	H
5	L	L	H	L	L	L	21	H	L	H	L	L	M
6	L	L	H	L	H	M	22	H	L	H	L	H	H
7	L	L	H	H	L	M	23	H	L	H	H	L	H
8	L	L	H	H	H	M	24	H	L	H	H	H	H
9	L	H	L	L	L	L	25	H	H	L	L	L	L
10	L	H	L	L	H	L	26	H	H	L	L	H	M
11	L	H	L	H	L	L	27	H	H	L	H	L	M
12	L	H	L	H	H	M	28	H	H	L	H	H	H
13	L	H	H	L	L	L	29	H	H	H	L	L	M
14	L	H	H	L	H	M	30	H	H	H	L	H	H
15	L	H	H	H	L	M	31	H	H	H	H	L	H
16	L	H	H	H	H	H	32	H	H	H	H	H	H

Table 5: Input attribute vector fuzzification.

Fuzzy level	Membership				
	Name	Age	Occu	Marr	Shop
L	0.67	0	0	0.5	1
H	0.33	1	1	0.5	0

the trust depth m, where the reputation of CSP is only related to the completion of the previous m services. The CSP's reputation on the jth service is shown in the Formula.

$$\sigma_j = \begin{cases} \left(\delta_1^l + \cdots + \delta_{j-1}^l\right)/(j-1), & \text{if } 0 < j \le m, \\ \left(\delta_{j-m}^l + \cdots + \delta_{j-1}^l\right)/m, & \text{if } j > m. \end{cases} \tag{5}$$

When $j = 1$, we initialize σ_j to a small positive number. If $\sigma_j > \theta$, user will trust the CSP. In this way, CSP will not be willing to take the initiative to disclose user privacy for reputation. Moreover, TMC also needs to store and update the reputation of CSP for the next service. If the reputation is updated according to Formula (5), we need to calculate and store the average of m reputations. In order to reduce computation and storage overhead, we propose an incremental update strategy as shown in Formula (6). We only need to store two reputations (i.e., σ_{j-1} and ${\delta_{j-1}}^l$). Another advantage is that users can only check the last time's service reputation of CSP, preventing users from completely rejecting the CSP because of occasional disclosure behaviors.

$$\sigma_j = \begin{cases} \left(\sigma_{j-1}.(j-1) + \delta_{j-1}^l\right)/j, & \text{if } 1 < j < m, \\ \left(\sigma_{j-1}.(m-1) + \delta_{j-1}^l\right)/m, & \text{if } j \ge m. \end{cases} \tag{6}$$

5.4. Static Bayesian Game. In addition to preventing CSP from voluntarily disclosing users' privacy, it is also necessary to resist theft attacks by potential adversaries (A). Therefore, we consider constructing a two-party static Bayesian game (SBG) [50] between the CSP and A to protect user privacy from the perspective of interests.

(1) We consider a strategic game between the CSP and A. Participants set can be formalized as $\Gamma = \{\text{CSP}, \mathscr{A}\}$

(2) We consider two types of adversaries, denoted as $T_{\text{A}} = \{\mathscr{A}_{yk}, \mathscr{A}_{nk}\}$, where $\mathscr{A}_{yk}$ represents the adversary with background knowledge, and $\mathscr{A}_{nk}$ represents the adversary without background knowledge. $\mathscr{A}$'s types set is public knowledge while CSP has only one type

(3) We mainly consider the probability of CSP inferring A's type, then use $P_{yk}\langle\mathscr{A}_{yk} \mid \text{CSP}\rangle$ and $P_{nk}\langle\mathscr{A}_{nk} \mid \text{CSP}\rangle$ to represent the probability that CSP infers $\mathscr{A}$ to be $\mathscr{A}_{yk}$ and $\mathscr{A}_{nk}$, respectively. In this game, $\mathscr{A}$'s type is known only by him/herself. Thus, it is private knowledge, while joint probability $P\langle\text{CSP}, \mathscr{A}_{yk}\rangle$ and $P\langle\text{CSP}, \mathscr{A}_{nk}\rangle$ are public knowledge

(4) The strategy set of CSP denotes $S_{\text{CSP}} = \{s_{\text{YP}}, s_{\text{NP}}\}$, where s_{YP} represents CSP providing services and s_{NP} represents CSP denying services. Note that $YP \in \{\text{LP}, \text{MP}, \text{HP}\}$, indicating that the CSP provides low, medium, and high QoS, respectively. Meanwhile, the strategy set of $\mathscr{A}$ denotes $S_{\mathscr{A}} = \{s_{\text{YA}}, s_{\text{NA}}\}$, where s_{YA} represents A choosing to attack and s_{NA} represents $\mathscr{A}$ choosing not to attack. The strategy set of participants is determined before the game, regarded as public knowledge, while the strategy chosen in the game is private knowledge

Table 6: Benefit matrix of A and CSP.

$\mathscr{A}$	CSP	
	YP	NP
s_{YA}^{nk}	$\left(u_{\mathrm{YA}}^{nk}, u-1\right)$	$\left(u_c^{\mathscr{A}}, u_{\mathrm{NP}}\right)$
s_{YA}^{yk}	$\left(u_{\mathrm{YA}}^{yk}, u-1\right)$	$\left(u_c^{\mathscr{A}}, u_{\mathrm{NP}}\right)$
$^{s}\mathrm{NA}$	$(u_{\mathrm{NA}}, u_{\mathrm{YP}})$	$(u_{\mathrm{NA}}, u_{\mathrm{NP}})$

(5) The benefit function of CSP denotes $U_{\mathrm{CSP}} = \{C, u_{\mathrm{NP}}\}$, where u_{YP} and u_{NP} represent CSP's benefits choosing to provide services and deny services, respectively. The benefit function of $\mathscr{A}$ denotes $U_{\mathrm{A}} = \{u_{\mathrm{YA}}^{yk}, u_{\mathrm{YA}}^{nk}, u_{\mathrm{NA}}\}$, where u_{YA}^{yk} and u_{YA}^{nk} represent $\mathscr{A}_{yk}$'s and $\mathscr{A}_{nk}$'s benefits choosing to attack, respectively, and u_{NA} represents $\mathscr{A}$'s benefit choosing not to attack. Obviously, participants' benefits strongly depends on the participants' types and selected strategies

Upon received user's NDP level, the CSP provides the corresponding QoS. If NDP is H, then the CSP provides low-level services with low service quality, which comes with a low risk of user privacy disclosure, thereby meeting the high-security requirements of users. If NDP is M, then the CSP provides middle-level services. If NDP is L, then the CSP provides high-level services with high quality of service, yet with an increased possibility of user privacy disclosure. Next, we construct a game benefit matrix as shown in Table 6.

Since the CSP provides different QoS according to users' individual preferences, it will gain different reputation benefits, as shown in the Formula.

$$u_{\mathrm{YP}} = \begin{cases} 1, & \text{if YP} = \text{LP}, \\ 2, & \text{if YP} = \text{MP}, \\ 3, & \text{if YP} = \text{HP}. \end{cases} \tag{7}$$

Particularly, the benefit of the CSP due to denial of service is $u_{\mathrm{NP}} = 0$, and the loss of the CSP due to attack from adversary is $u_{-1} = -3$. On the other hand, $\mathscr{A}$'s benefit consists of three parts: basic benefit, attack cost, and extra incentive. Thus, we can determine that A's benefit is shown in the Formula.

$$\begin{cases} u_{\mathrm{YA}}^{nk} = u_b^{\mathscr{A}} + u_c^{\mathscr{A}} + u_{\mathrm{YP}}^2.\mu, \\ u_{\mathrm{YA}}^{yk} = u_{\mathrm{YA}}^{nk}.(1+k). \end{cases} \tag{8}$$

In (8), $u_b^{\mathscr{A}}$ represents $\mathscr{A}$'s basic benefit, $u_c^{\mathscr{A}}$ represents $\mathscr{A}$'s attack cost, and the other represents extra incentive refer to benefit factor μ. This means that the higher the QoS provided by CSP, the higher the data quality submitted by users, and the greater the benefits gained from A successfully attacking. When $\mathscr{A}$ chooses not to attack, $u_{\mathrm{NA}} = 0$. Additionally, k is regarded as background factor, and is used to increase $\mathscr{A}$'s benefit.

In order to facilitate the analysis of the incomplete information game, we use the Harsanyi transformation to introduce a virtual participant "nature" (N). N randomly selects both participants' types. $P\langle \mathrm{CSP}, \mathscr{A}_{yk}\rangle$ and $P\langle \mathrm{CSP}, \mathscr{A}_{nk}\rangle$ are public knowledge, where $P\langle \mathrm{CSP}, \mathscr{A}_{yk}\rangle + P\langle \mathrm{CSP}, \mathscr{A}_{nk}\rangle = 1$. $P_{yk}\langle \mathscr{A}_{yk} \mid \mathrm{CSP}\rangle$ and $P_{nk}\langle \mathscr{A}_{nk} \mid \mathrm{CSP}\rangle$ represent the probabilities of the CSP inferring type $\mathscr{A}$, respectively, which can be obtained by Bayesian formula:

$$\begin{cases} P_{yk}\langle \mathscr{A}_{yk} \mid \mathrm{CSP}\rangle = P\langle \mathrm{CSP}, \mathscr{A}_{yk}\rangle / P\langle \mathrm{CSP}\rangle = P\langle \mathrm{CSP}, \mathscr{A}_{yk}\rangle, \\ P_{nk}\langle \mathscr{A}_{nk} \mid \mathrm{CSP}\rangle = P\langle \mathrm{CSP}, \mathscr{A}_{nk}\rangle / P\langle \mathrm{CSP}\rangle = P\langle \mathrm{CSP}, \mathscr{A}_{nk}\rangle. \end{cases} \tag{9}$$

For simplicity, we use P_{yk} and P_{nk} to replace $P_{yk}\langle \mathscr{A}_{yk} \mid \mathrm{CSP}\rangle$ and $P_{nk}\langle \mathscr{A}_{nk} \mid \mathrm{CSP}\rangle$, respectively. Then, we use P_{YP} and P_{NP} to represent the probability of CSP choosing YP strategy and NP strategy (i.e., $P_{\mathrm{YP}} + P_{\mathrm{NP}} = 1$), respectively. Furthermore, we use P_{YA} and P_{NA} to represent the probability of A choosing YA strategy and NA strategy, respectively, (i.e., $P_{\mathrm{YA}} + P_{\mathrm{NA}} = 1$). Next, we calculate the benefits of the CSP choosing YP and NP strategies, as shown in the Formula.

$$\begin{cases} u_{\mathrm{YP}} = & P_{\mathrm{YA}} \cdot u_{-1} + P_{\mathrm{NA}} \cdot u_{\mathrm{YP}}, \\ u_{\mathrm{NP}} & 0. \end{cases} \tag{10}$$

The benefits of $\mathscr{A}$ choosing YA strategy and NA strategy are shown in the Formula.

$$\begin{cases} u_{\mathrm{YA}} = \left[P_{\mathrm{YP}}.u_{\mathrm{YA}}^{yk} + P_{\mathrm{NP}}.u_c^{\mathscr{A}}\right].P_{yk} + \left[P_{\mathrm{YP}}.u_{\mathrm{YA}}^{nk} + P_{\mathrm{NP}}.u_c^{\mathscr{A}}\right].P_{nk}, \\ u_{\mathrm{NA}} = 0. \end{cases} \tag{11}$$

We can obtain the CSP's and $\mathscr{A}$'s benefit, respectively, from the Formula.

$$\begin{cases} U_{\mathrm{CSP}}(P_{\mathrm{YA}}^*, P_{\mathrm{YP}}) = u_{\mathrm{YP}}.P_{\mathrm{YP}} + u_{\mathrm{NP}}.P_{\mathrm{NP}}, \\ U_{\mathscr{A}}(P_{\mathrm{YA}}, P_{\mathrm{YP}}^*) = u_{\mathrm{YA}}.P_{\mathrm{YA}} + u_{\mathrm{NA}}.P_{\mathrm{NA}}. \end{cases} \tag{12}$$

In the static Bayesian equilibrium state, CSP's benefit function U_{CSP} can reach the maximum regardless of what $\mathscr{A}$ chooses. Also, $\mathscr{A}$'s benefit function $U_{\mathscr{A}}$ can reach the maximum regardless of what CSP chooses. Essentially, it means that the strategies of participants are indistinguishable and can be solved by simultaneous equations.

$$\begin{cases} \dfrac{\partial U_{\mathrm{CSP}}(P_{\mathrm{SA}}^*, P_{\mathrm{MP}})}{\partial P_{\mathrm{MP}}} = 0, \\ \dfrac{\partial U_{\mathscr{A}}(P_{\mathrm{SA}}, P_{\mathrm{MP}}^*)}{\partial P_{\mathrm{SA}}} = 0. \end{cases} \tag{13}$$

Therefore, we can obtain the mixed strategy Bayesian equilibrium $(P^*_{\mathrm{YA}}, P^*_{\mathrm{YP}})$, as shown in the Formula.

$$\begin{cases} P^*_{\mathrm{YA}} = \dfrac{u_{\mathrm{YP}}}{u_{\mathrm{YP}} - u_{-1}}, \\ P^*_{\mathrm{YP}} \dfrac{-u_c^{\mathscr{A}}}{\left(u^{yk}_{\mathrm{YA}} - u^{nk}_{\mathrm{YA}}\right).P_{yk} + \left(u^{nk}_{\mathrm{YA}} - u_c^{\mathscr{A}}\right)}. \end{cases} \tag{14}$$

5.5. Privacy Disclosure Measurement. In social IoT, users exchange personalized services from the CSP by providing private data, which will inevitably have the risk of being leaked over communication links. Shannon information entropy [57] is used to measure privacy disclosure, as shown in the Formula below.

$$H(X) = -\sum_{i=1}^{n} P_i.\log\left(P_i\right), \tag{15}$$

where $0 \le P_i \le 1, \sum_{i=1}^{n} P_i = 1$.

From A's point of view, the probability P_{YP} and P_{NP} can be inferred. As described in Formula (16), the greater $H(\mathscr{A})$ is, the closer P_{YP} and P_{NP} are, the higher the indistinguishability of A to CSP's strategy, and the lower degree of privacy disclosure. Otherwise, the higher is the degree of privacy disclosure. For instance, if $P_{\mathrm{YP}} = 0.5$, the information entropy is 1, indicating that A is completely confused about the service decision of the CSP.

$$H(\mathrm{A}) = -P_{\mathrm{YP}} \cdot \log\left(P_{\mathrm{YP}}\right) - P_{\mathrm{NP}} \cdot \log\left(P_{\mathrm{NP}}\right). \tag{16}$$

In social IoT, a single game obviously cannot satisfy the user requirement. Therefore, we consider the finite static Bayesian game for J times. Similarly, the privacy disclosure measurement in a long term can be described by Formula (17). It can be used to evaluate the privacy disclosure status of J times of service.

$$H^J(\mathscr{A}) - \frac{1}{J}\sum_{j=1}^{J} P^j_{Yp} \log\left(P^j_{\mathrm{YP}}\right) - P^j_{\mathrm{NP}} \log\left(P^j_{\mathrm{NP}}\right). \tag{17}$$

6. Experiment and Evaluation

In order to better illustrate the feasibility of the Persian framework, we consider that its performance is influenced by three factors: user classification, trust assessment, and privacy disclosure measurement. The experiments were carried out on a workstation with a 3.30 GHz quad-core processor, 8GB memory, and Windows 7 64-bit operating system to simulate and analyze on the Matlab R2016a platform.

6.1. User Classification. In the user classification module, Fuzzy Toolbox [58] is used to conduct fuzzy uncertainty reasoning for users, and the result is used to verify the theoretical calculation. Assuming that the input user is u_3 in Table 2, we synthesize the rule constraints of all input attributes. As shown in Figure 4, rules (13)(15)(29)(31) are activated, and the output NDP is 0.46. It can be seen that u_3 belongs to the M level, which is consistent with the theoretical calculation.

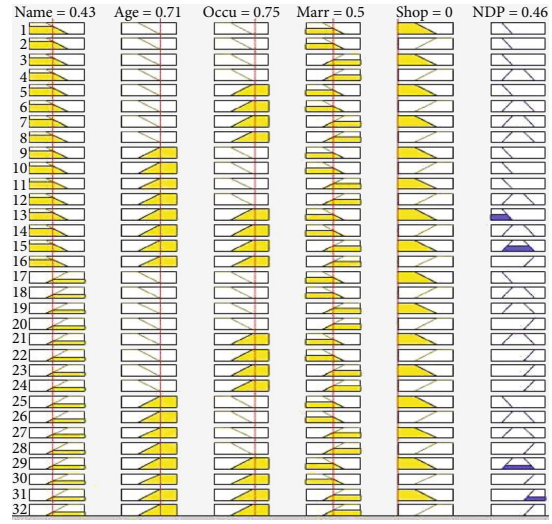

Figure 4: Simulation result of Fuzzy Toolbox.

6.2. Trust Assessment. We evaluate the CSP's trust based on the QoS provided by CSP for J times, and update the CSP's visual trust to users. Users in Social IoT need to check the reputation of the CSP prior to submitting private data to the CSP. Only when CSP's reputation is greater than the trust threshold (i.e., $\theta = 0$), users are willing to trust the CSP and share their privacy. Based on the individual preferences of 30 users (i.e., $J = 30$), we quantified the CSP's active disclosure behavior and indirectly clarified the trust of the CSP.

Figure 5(a) shows that the CSP provides three levels of QoS according to users' individual privacy preferences, and then obtains three ratings of reputation, namely, 1, 2, and 3. It is worth noting that the CSP will be subject to severe reputational penalties if it voluntarily discloses users' privacy in the process of providing services. The CSP chooses to disclose privacy when $j = 3$, and it loses the reputation of 12 units. The attendant consequences are disastrous for the CSP, resulting in a significant decline in service delivery rates. On the other hand, we consider the impact of trust depth on the reputation of the CSP. Figure 5(b) shows that dishonest behaviors of the CSP will lead to the decline of the visible reputation of multiround services. As the depth of trust relationship (i.e., m) increases, the spread of the reputation penalty becomes more serious. Regardless of the situation, there is no reason for the curve in SBG for J times. The CSP is used to actively disclose user privacy in order to maintain visible reputation with users.

6.3. Privacy Disclosure Measurement. It is certain that the CSP provides different levels of QoS according to individual preferences. As a result, the behavioral strategy of A and the CSP may change driven by interests. Figure 6(a) shows the relationship between Nash equilibrium and QoS levels. With the improvement of service quality, the probability of attack is gradually increased because of the temptation of

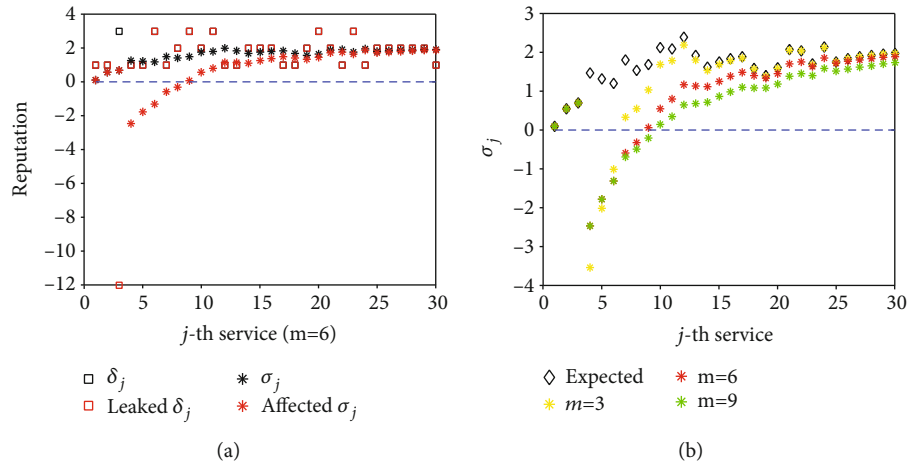

Figure 5: Trust assessment results. (a) The impact of privacy disclosure on reputation; (b) the impact of trust depth on reputation.

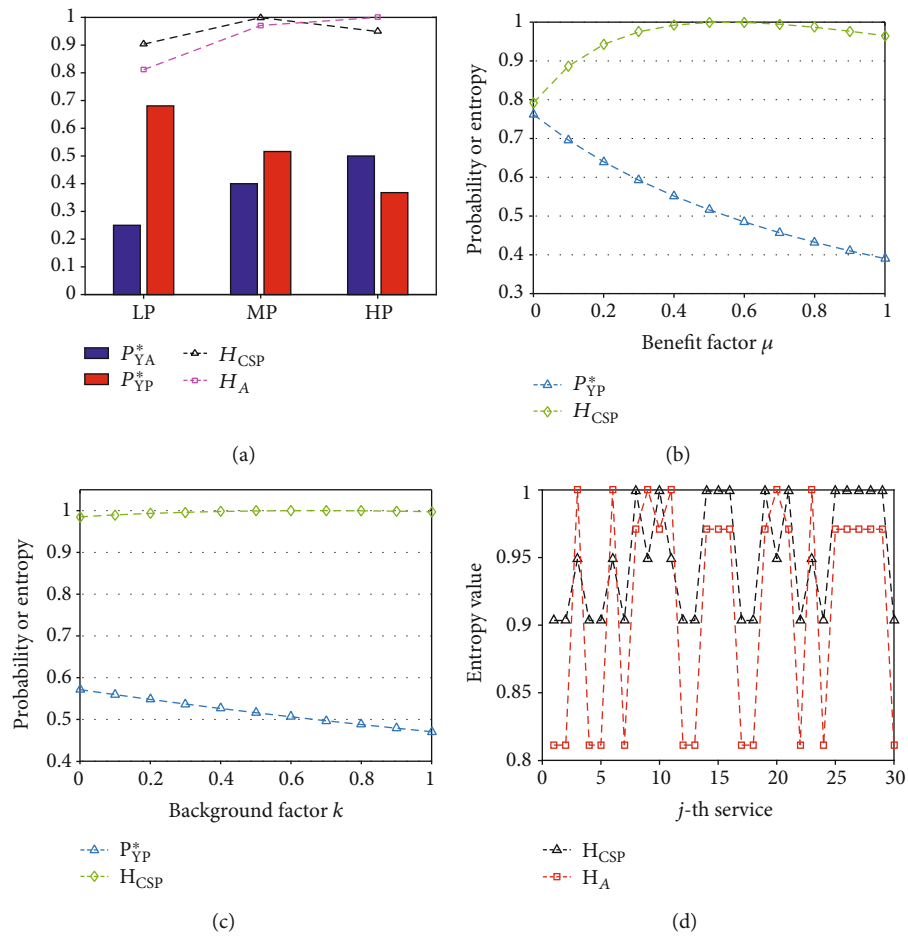

Figure 6: Nash equilibrium results. (a) The relationship between Nash equilibrium and QoS levels; (b) the relationship between Nash equilibrium and benefit factor; (c) the relationship between Nash equilibrium and background factor; (d) Nash equilibrium.

high data quality, and the CSP tends to choose denying service due to potential attacks. Despite the fact that the CSP provides high QoS, the result of information entropy has declined slightly, just below 1. This suggests that A is still confused about the decision-making of the CSP, and the risk of user privacy disclosure remains at a relatively low level. Further, we explain the relationship between Nash equilibrium and two internal incentive factors μ and k. From Figure 6(b), the attack benefit u_{YA} of adversaries increases with μ, and the probability ${}^{P}{}_{YP}{}^{*}$ of CSP to provide the service

gradually decreases. When $P_{YP}{}^{*}$ is close to 0.5, the service information entropy H (CSP) reaches the maximum, and the privacy protection level reaches its peak. Figure 6(c) shows a similar trend in relationships. The probability of a successful attack by adversaries increases with k, and as a result, CSP tends to refuse to provide services. Likewise, the intensity of privacy protection reaches maximum while k gets close to 0.5.

Additionally, we observe the Nash equilibrium change in the CSP service delivery for J times. Figure 6(d) shows that the information entropy is maintained at a high level. According to Formula (17), we can calculate the average privacy disclosure of 0.9509. As long as the CSP does not actively disclose the user's privacy, the confusion of $\mathcal{A}$ about the CSP's decision will not be decreased. Also, we have clarified the trust in the CSP in Section 5.3. Based on the above, the Persian framework can effectively provide personalized services while keeping privacy disclosure to a minimum level.

7. Conclusion

There are frequent occurrences of user privacy disclosure in social IoT, drawing wide attention in academia and the industry. A few achievements have been acquired, but a number of key techniques are still in need. On the one hand, users have to share their privacy to the CSP to exchange application privileges, so as to enjoy personalized services. On the other hand, users are reluctant to disclose their privacy. Find a satisfactory balance between QoS and privacy protection under the premise of ensuring personalized services is the main contribution of this paper. We proposed a privacy-preserving personalized service framework (Persian) through a static Bayesian game. In this framework, users independently infer their privacy preferences combined with offline fuzzy reasoning. The trust of the CSP is supervised by TMC to ensure normal service operations. The CSP provides users with personalized service according to users' individual preferences. Furthermore, we employ the game mixing strategy equilibrium to achieve privacy protection from the perspective of interests. Meanwhile, we measure privacy disclosure by using information entropy under the proposed framework.

The future work is to further expand the fuzzy reasoning with neural network and consider additional user attributes. We will also consider more types of adversaries and constantly optimize the proposed model to achieve better comprehensiveness and efficiency for privacy protection.

Data Availability

The data used in this paper comes from the comprehensive questionnaire investigation.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work was supported in part by the National Natural Science Foundation of China under grants 61872088, 61872090, U1905211, and 61702105, in part by the Natural Science Foundation of Fujian Province under grant 2019J01276, in part by the Guizhou Provincial Key Laboratory of Public Big Data Research Fund under grant 2019BDKFJJ004, in part by the Science and Technology Research Program of Chongqing Municipal Education Commission under grant KJQN201801316, in part by the Innovation and Entrepreneurship Demonstration Team of Yingcai Program of Chongqing under grant CQYC201903167, and in part by Scientific and Technological Research Program of Chongqing Municipal Education Commission under grant KJZD-K201901301.

References

[1] J. Ni, X. Lin, and X. S. Shen, "Toward edge-assisted internet of things: from security and efficiency perspectives," *IEEE Network*, vol. 33, no. 2, pp. 50–57, 2019.

[2] C. Luo, J. Ji, Q. Wang, X. Chen, and P. Li, "Channel state information prediction for 5g wireless communications: a deep learning approach," *IEEE Transactions on Network Science and Engineering*, vol. 7, no. 1, pp. 227–236, 2020.

[3] G. Liu, Q. Yang, H. Wang, and A. X. Liu, "Three-valued subjective logic: a model for trust assessment in online social networks," *IEEE Transactions on Dependable and Secure Computing*, p. 1, 2019.

[4] D. Wu, B. Liu, Q. Yang, and R. Wang, "Social-aware cooperative caching mechanism in mobile social networks," *Journal of Network and Computer Applications*, vol. 149, p. 102457, 2020.

[5] H. Wang, M. Hempel, D. Peng, W. Wang, H. Sharif, and H. H. Chen, "Index-based selective audio encryption for wireless multimedia sensor networks," *IEEE Transactions on Multimedia*, vol. 12, no. 3, pp. 215–223, 2010.

[6] J. Xiong, L. Chen, M. Z. Bhuiyan et al., "A secure data deletion scheme for iot devices through key derivation encryption and data analysis," *Future Generation Computer Systems (Early Access)*, vol. 111, pp. 741–753, 2020.

[7] D. Wu, J. Yan, H. Wang, and R. Wang, "User-centric edge sharing mechanism in software-defined ultra-dense networks," *IEEE Journal on Selected Areas in Communications*, vol. 38, no. 7, pp. 1531–1541, 2020.

[8] D. Wu, X. Han, Z. Yang, and R. Wang, "Exploiting transfer learning for emotion recognition under cloud-edge-client collaborations," *IEEE Journal on Selected Areas in Communications*, p. 1, 2020.

[9] X. Meng, *China privacy risk index analysis report*, 2020, http://www.tiuchina.com/yjbg/346.html.

[10] H. Wang, C. Gao, Y. Li, Z.-L. Zhang, and D. Jin, "Revealing physical world privacy leakage by cyberspace cookie logs," *IEEE Transactions on Network and Service Management*, p. 1, 2020.

[11] D. Keküllüoglu, W. Magdy, and K. Vaniea, "Analysing privacy¨ leakage of life events on twitter," in *12th ACM Conference on Web Science*, pp. 287–294, Southampton, United Kingdom, 2020.

[12] R. Sobers, "107 Must-Know Data Breach Statistics for 2020," 2020, http://www.sogou.com/link?url=hedJjaC291M8s0HmWVMlqTtIfarcvd6plnEXJCF-KNim9pVlRx94EYkHAapUdxCOVW_atjSnNqI.&query=2020+data+leakage+survey.

[13] M. S. Roopa, S. Pattar, R. Buyya, K. R. Venugopal, S. S. Iyengar, and L. M. Patnaik, "Social internet of things (siot): foundations, thrust areas, systematic review and future directions," *Computer Communications*, vol. 139, pp. 32–57, 2019.

[14] J. Xiong, J. Ren, L. Chen et al., "Enhancing privacy and availability for data clustering in intelligent electrical service of iot," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 1530–1540, 2019.

[15] Z. Lin and L. Dong, "Clarifying trust in social internet of things," *IEEE Transactions on Knowledge and Data Engineering*, vol. 30, no. 2, pp. 234–248, 2018.

[16] T. Cheng, G. Liu, Q. Yang, and J. Sun, "Trust assessment in vehicular social network based on three-valued subjective logic," *IEEE Transactions on Multimedia*, vol. 21, no. 3, pp. 652–663, 2019.

[17] Q. Jiang, Z. Chen, J. Ma, X. Ma, J. Shen, and D. Wu, "Optimized fuzzy commitment based key agreement protocol for wireless body area network," *IEEE Transactions on Emerging Topics in Computing*, p. 1, 2019.

[18] Q. Jiang, N. Zhang, J. Ni, J. Ma, X. Ma, and K. K. Choo, "Unified biometric privacy preserving three-factor authentication and key agreement for cloud-assisted autonomous vehicles," *IEEE Transactions on Vehicular Technology*, p. 1, 2020.

[19] J. Xiong, R. Ma, L. Chen, Y. Tian, L. Lin, and B. Jin, "Achieving incentive, security, and scalable privacy protection in mobile crowdsensing services," *Wireless Communications and Mobile Computing*, vol. 2018, 12 pages, 2018.

[20] C. Liu, Y. Tian, J. Xiong, Y. Lu, Q. Li, and C. Peng, "Towards attack and defense views to k-anonymous using information theory approach," *IEEE Access*, vol. 7, pp. 156025–156032, 2019.

[21] J. Xiong, M. Zhao, M. Bhuiyan, L. Chen, and Y. Tian, "An ai-enabled threeparty game framework for guaranteed data privacy in mobile edge crowdsensing of iot," *IEEE Transactions on Industrial Informatics*, p. 1, 2019.

[22] C. Dwork, *Differential privacy*, Springer, NewYork, NY, USA, 2011.

[23] J. Xiong, R. Ma, L. Chen et al., "A personalized privacy protection framework for mobile crowdsensing in iiot," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 6, pp. 4231–4241, 2020.

[24] H. Hu, G.-J. Ahn, and J. Jorgensen, "Multiparty access control for online social networks: model and mechanisms," *IEEE Transactions on Knowledge and Data Engineering*, vol. 25, no. 7, pp. 1614–1627, 2012.

[25] Q. Li, H. Zhu, J. Xiong, R. Mo, Z. Ying, and H. Wang, "Fine-grained multiauthority access control in iot-enabled mhealth," *Annals of Telecommunications*, vol. 74, no. 7-8, pp. 389–400, 2019.

[26] M. Frustaci, P. Pace, G. Aloi, and G. Fortino, "Evaluating critical security issues of the iot world: present and future challenges," *IEEE Internet of Things Journal*, vol. 5, no. 4, pp. 2483–2495, 2018.

[27] L. Zhang, X. Zhu, X. Han, and J. Ma, "Differentially privacy-preserving social iot," in *2019 11th International Conference on Wireless Communications and Signal Processing (WCSP)*, pp. 1–6, Xi'an, China, China, 2019.

[28] Q. Li, J. Ma, R. Li, J. Xiong, and X. Liu, "Provably secure unbounded multi-authority ciphertext-policy attribute-based encryption," *Security and Communication Networks*, vol. 8, no. 18, pp. 4098–4109, 2015.

[29] X. Wu, T. Wu, M. Khan, Q. Ni, and W. Dou, "Game theory based correlated privacy preserving analysis in big data," in *IEEE Transactions on Big Data*, 2017.

[30] C.-G. Liu, I.-H. Liu, W.-S. Yao, and J. S. Li, "K-anonymity against neighborhood attacks in weighted social networks," *Security and Communication Networks*, vol. 8, no. 18, pp. 3864–3882, 2015.

[31] Y. Xie and M. Zheng, "A differentiated anonymity algorithm for social network privacy preservation," *Algorithms*, vol. 9, no. 4, p. 85, 2016.

[32] Z. G. Chen, H. S. Kang, S. N. Yin, and S. R. Kim, "An efficient privacy protection in mobility social network services with novel clustering-based anonymization," *EURASIP Journal on Wireless Communications and Networking*, vol. 2016, no. 1, Article ID 275, 2016.

[33] X. Li, J. Yang, Z. Sun, and J. Zhang, "Differential privacy for edge weights in social networks," *Security and Communication Networks*, vol. 2017, 10 pages, 2017.

[34] Q. Wang, Y. Zhang, X. Lu, Z. Wang, Z. Qin, and K. Ren, "Real-time and spatiotemporal crowd-sourced social network data publishing with differential privacy," *IEEE Transactions on Dependable and Secure Computing*, vol. 15, no. 4, pp. 591–606, 2016.

[35] H. Huang, D. Zhang, F. Xiao, K. Wang, J. Gu, and R. Wang, "Privacy-preserving approach pbcn in social network with differential privacy," *IEEE Transactions on Network and Service Management*, vol. 17, no. 2, pp. 931–945, 2020.

[36] S. Jahid, P. Mittal, and N. Borisov, "Easier: encryption-based access control in social networks with efficient revocation," *Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security*, pp. 411–415, 2011.

[37] Z. Cai, Z. He, X. Guan, and Y. Li, "Collective data-sanitization for preventing sensitive information inference attacks in social networks," *IEEE Transactions on Dependable and Secure Computing*, vol. 15, no. 4, pp. 577–590, 2018.

[38] Y. Cai, S. Zhang, H. Xia, Y. Fan, and H. Zhang, "A privacy-preserving scheme for interactive messaging over online social networks," *IEEE Internet of Things Journal*, vol. 7, no. 8, pp. 6817–6827, 2020.

[39] V. Sharma, I. You, D. N. K. Jayakody, and M. Atiquzzaman, "Cooperative trust relaying and privacy preservation via edge-crowdsourcing in social internet of things," *Future Generation Computer Systems*, vol. 92, pp. 758–776, 2019.

[40] X. Jin, N. Pissinou, S. Pumpichet, C. A. Kamhoua, and K. Kwiat, "Modeling cooperative, selfish and malicious behaviors for trajectory privacy preservation using bayesian game theory," in *38th Annual IEEE Conference on Local Computer Networks*, pp. 835–842, Sydney, NSW, Australia, 2013.

[41] H. Hu, G. J. Ahn, Z. Zhao, and D. Yang, "Game theoretic analysis of multiparty access control in online social networks," *Proceedings of the 19th ACM symposium on Access control models and technologies*, pp. 93–102, 2014.

[42] F. Shan, H. Li, and H. Zhu, "Game theory based forwarding control method for social network," *Journal on Communications*, vol. 39, no. 3, pp. 172–180, 2018.

[43] J. Xiong, M. S. Wang, and Y. L. Tian, "Research progress on privacy measurement for cloud data," *Journal of software*, vol. 29, no. 7, pp. 1963–1980, 2018.

[44] A. Serjantov and G. Danezis, "Towards an information theoretic metric for anonymity," *International Workshop on Privacy Enhancing Technologies*, pp. 41–53, 2002.

[45] Z. Lin, M. Hewett, and R. B. Altman, "Using binning to maintain confidentiality of medical data," *Proceedings of the AMIA Symposium*, p. 454, 2002.

[46] C. Diaz, C. Troncoso, and G. Danezis, "Does additional information always reduce anonymity?," *Proceedings of the 2007 ACM workshop on Privacy in electronic society*, pp. 72–75, 2007.

[47] T. Chen, A. Chaabane, P. U. Tournoux, M. A. Kaafar, and R. Boreli, "How much is too much? Leveraging ads audience estimation to evaluate public profile uniqueness," in *International Symposium on Privacy Enhancing Technologies Symposium*, pp. 225–244, Springer, Berlin, Heidelberg, 2013.

[48] J. Xiong, X. Chen, Q. Yang, L. Chen, and Z. Yao, "A task-oriented user selection incentive mechanism in edge-aided mobile crowdsensing," *IEEE Transactions on Network Science and Engineering*, p. 1, 2019.

[49] N. Werro, *Fuzzy Classification of Online Customers*, Springer, NewYork, NY, USA, 2015.

[50] D. Fudenberg and J. Tirole, *Game Theory*, Massachusetts, Cambridge, 1991.

[51] J. Xiong, Y. Zhang, L. Lin, J. Shen, X. Li, and M. Lin, "ms-posw: a multiserver aided proof of shared ownership scheme for secure deduplication in cloud," *Concurrency and Computation: Practice and Experience*, vol. 32, no. 3, 2019.

[52] X. Liu, R. H. Deng, P. Wu, and Y. Yang, "Lightning-fast and privacy-preserving outsourced computation in the cloud," *Cybersecurity*, vol. 3, no. 1, p. 17, 2020.

[53] J. Xiong, R. Bi, M. Zhao, J. Guo, and Q. Yang, "Edge-assisted privacy-preserving raw data sharing framework for connected autonomous vehicles," *IEEE Wireless Communications*, vol. 27, no. 3, pp. 24–30, 2020.

[54] P. Zhang, C. Peng, and C. Hao, "Privacy protection model and privacy metric methods based on privacy preference," *Computer Science*, vol. 45, no. 6, pp. 130–134, 2018.

[55] M. Blej and M. Azizi, "Comparison of mamdani-type and sugeno-type fuzzy inference systems for fuzzy real time scheduling," *International Journal of Applied Engineering Research*, vol. 11, no. 22, pp. 11071–11075, 2016.

[56] A. Mehmood, I. Natgunanathan, Y. Xiang, G. Hua, and S. Guo, "Protection of big data privacy," *IEEE Access*, vol. 4, pp. 1821–1834, 2016.

[57] T. M. Cover and J. A. Thomas, *Elements of Information Theory*, John Wiley & Sons, Chichester, West Sussex, United Kingdom, 2012.

[58] B. Narasimhan and A. Malathi, "A fuzzy logic system with attribute ranking technique for risk-level classification of cahd in female diabetic patients," in *2014 International Conference on Intelligent Computing Applications*, pp. 179–183, Coimbatore, India, 2014.