IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received December 7, 2018, accepted January 5, 2019, date of publication January 10, 2019, date of current version January 29, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2891589

Research on the Tradeoff Between Privacy and Trust in Cloud Computing

PAN JUN SUN
School of Electronic Information and Electrical Engineering, Shanghai Jiao Tong University, Shanghai 200240, China
e-mail: sunpanjun2008@163.com

ABSTRACT Promoting cloud services must consider the privacy requirements between the user and the provider. Both privacy and trust are related to knowledge about an entity; however, there is an inherent conflict between trust and privacy. In this paper, we research the relationship between privacy and trust in the cloud computing. First, we construct a trust model based on multiple factors, such as direct trust, trust risk, reward-punishment, and feedback trust; the weight of trust factor is determined by class diversity and information entropy theory. Second, we propose a novel privacy metric model with multiple factors, such as privacy preference, credential attribute, interaction history, and privacy feedback, and the weight of privacy factor is based on the maximum dispersion. Third, we propose a tradeoff between privacy and trust; both user and the provider can choose privacy protection or trust establishment priority by personal preference and requirement. Fourth, we demonstrate and compare the tradeoff between privacy and trust, interaction success rate, trust evaluation accuracy, and privacy disclosure rate by different experiments; these simulation results show that the privacy of each partner can be effectively protected.

INDEX TERMS Cloud computing, privacy, trust, tradeoff, information entropy.

I. INTRODUCTION

With the rapid development of internet and information technology, more and more people are putting their data in the public or hybrid cloud [1]. For example, Amazon and SUN have launched cloud computing services, which allow organizations and individuals to use the dynamic computing infrastructure [2]. While users are enjoying a variety of services with convenience, privacy disclosure has become an important issue. Especially, in recent years, there are many scandals about privacy leaks, such as pictures, videos and other personal privacy information and so on [3], [4]. Therefore, it is necessary to take applicable solutions to protect privacy in cloud computing.

A. MOTIVATION

Privacy is a fundamental human right that involves the expression of various legal and nonlegal norms regarding the right to a private life [3], mainly includes location privacy, data privacy, and identity privacy an. However, every cloud transaction is proceeding by a negotiation phase where an entity asks for some credential from the other entity, which implies privacy loss [4], [6], [8], [9], [23]. Trust is a psychological state comprising the intention to accept vulnerability based upon positive expectations of the intentions or behavior of another. Given a threshold, the privacy protection is transformed into a simple judgment problem. If the trust value satisfies a certain threshold condition, the object can access the privacy data [5], [25].

Many articles focus on establishing a trusted infrastructure in cloud computing, which gradually requires a tradeoff between privacy and trust, such as certificate recommendations or transaction history [6], [11], [14], [17]. However, these credentials may lead to a compromise of privacy in the form of revelation of identity, interaction history, personal preferences. Thus, in the network environment, privacy and trust are in an adversarial relationship; the problem requires a tradeoff between privacy and trust, which can be further decomposed as 3 sub-problems [13], [18], [19]:

1) How much trust is constructed by several factors?
2) How much privacy is constructed by several factors?
3) How much privacy is willing to be sacrificed for a certain amount of trust gain?

These questions show how complex optimization of the privacy trust exchange is and involves many factors [20], [23]. How to design an effective solution is still a problem, it is necessary to balance the relations between trust and privacy [24], [26].

B. OUR CONTRIBUTIONS

To solve these above problems, we propose a tradeoff model between privacy and trust in the cloud computing. The main contributions of the paper are summarized as follows.

1) We construct a trust evaluation model based on multiple factors, such as direct trust, trust risk, reward-punishment, and feedback trust, in addition, introduce the weight factor by information entropy theory to describe the trust more accurately and objectively.
2) We propose a novel privacy metric model with multiple factors, such as privacy preference, credential attribute, interaction history, and privacy feedback, and calculate weight by the maximum dispersion.
3) We use the information entropy theory for two aspects: privacy loss and trust gain, and further propose a tradeoff relationship model that can determine the priority of protecting privacy or establishing trust for interaction in the cloud computing.

The rest of this paper is organized as follows. In section II, some related research articles are introduced. In section III, we construct a multi-factor trust metric model. In section IV, a privacy metrics model based on multi-attribute is proposed. In section V, we research and construct a tradeoff relationship model from two aspects: privacy loss and trust gain. In section VI, we design several experiments to compare our research and two other models. Finally, in section VII, we conclude the paper.

II. RELATED WORK

In recent years, because of the continuous efforts of academia and industry, many studies have addressed general privacy issues in cloud computing [1]–[6]. General privacy concerns might have an influence on perceived privacy and trust, because of the inspiration for this article, we mainly introduce the research work between privacy and trust.

Information entropy theory was proposed by Shannon [7]. As an effective tool for information measurement, entropy has shown important contributions in the field of communication, and privacy, which can be naturally quantified by the entropy method. To properly evaluate different privacy preserving schemes, Longpr and Kreinovich [8] proposed to supplement the average privacy loss with the standard deviation to determine how much the actual privacy loss deviates from its average value. In the big data era, personal data can be obtained from several sources, such as internet services and social media. Kim *et al.* [9] proposed a new analytical model to measure the personal information disclosure risk in open data before publishing and formulating the entropy-based re-identification risk to measure the privacy disclosure risk.

Jamar and Almasizadeh [10] introduced the mean privacy approach to intuitively quantify how attackers behave and their predictability. This metric can be considered an appropriate indicator for quantifying the security level of computer systems, which was quantified by an information theoretic. Casas and Hurtado [11] discussed potential risks and attacks of social network site privacy, and presented the measurement and quantification of the social privacy. Simply by relying on the total leaked privacy value calculated with the metric, users can adjust the level of information disclosure. Arnau *et al.* [12] researched the fundamental problem of quantitative measures of the privacy of user profiles and established the critical importance of quantifying privacy to assess, compare, and optimize privacy enhancing technologies.

Rivadulla [13] explored the issues of online privacy considering the new possibilities the internet and other available technologies have provided, which can compel the collector to ask the user for explicit and informed consent before assembling the data. Aldini and Bogliolo [14] and Yang and Chen [15] investigated the tradeoff among the multiple dimensions that characterize the incentive strategies resulting from discussion and discussed the benefits and the implementation issues of two models that differ in the way in which privacy is managed and traded with respect to and cost.

Dependencies between sensitive and useful data results in a privacy utility tradeoff that has strong connections to generalized rate distortion problems. Frey *et al.* [16] formulated the privacy-utility tradeoff problem where the data release mechanism has limited access to the entire data composed of useful and sensitive parts. Basciftci *et al.* [17] established these results for general families of privacy and utility measures that satisfy certain natural properties required of any reasonable measure of privacy or utility, which also uncovered a new, subtler aspect of the data processing inequality for general non-symmetric privacy measures and discuss its operational relevance and implications.

Privacy and trust should be adjusted to guarantee appropriate security, Tyagi *et al.* [18] discussed some valuable assumptions for privacy and trust trade based on pieces of evidence, and constructed a tradeoff model between privacy and trust. Differential privacy is an effective tool to privacy protection. Martin [19] used factorial vignette survey methodology to measure the relative importance of violating privacy expectations to consumers' trust, which can support a reinforcing relationship between privacy and trust in a website online. Wang and Zhang [20] studied an attack model in recommender systems and presented a privacy-preserving recommendation framework based on weighted nonnegative matrix. In order to the convenience of reading the article, some important symbols are given in Table 1.

III. TRUST COMPUTING

Assume that $D_1, D_2, \cdots, D_N \in D(S)$ denote nodes in a cloud system; which are divided into 2 types: service provider and user. According to the dynamics and complexity of trust, assume that the trust relationship function has many factors $(T_1(D_i, D_j), T_2(D_i, D_j), \cdots, T_m(D_i, D_j))$ between D_i and D_j, the decision set is $T = (T_1, T_2 . \cdots T_M)$, $0 \leq T_m(D_i, D_j) \leq 1$, $(m = 1, 2, \cdots, M)$. tr_ω_m expresses the weight factor of $T_m(D_i, D_j)$, and satisfies the following condition

TABLE 1. Symbols of trust and privacy model.

Notation	Meaning
$D(S)=\{D_1,D_2,\cdots,D_N\}$	N entities of system
T_1 , T_2 , T_3 , T_4	Trust function
tr_ω_m	Weight of $T_m(D_i,D_j)$
$TG(D_i,D_j,S,t)$	Trust between D_i and D_j
$RS=\{RS_1\cdots,RS_i,\cdots,RS_N\}$	N level trust degree
$\Theta(TG(D_i,D_j))$	Trust decision
$T^{(i)}$	Decay time factor
$R(D_i,D_j)$	Risk function
$S=\{s_1,s_2,\cdots,s_P\}$	Service level
level	The level of a trust tree
$\rho(F_k)$	Feedback weight factor
$F(D_i)=\{F_1,F_2\cdots,F_n\}$	Feedback entities of D_i
$\eta\in[0,1]$	Quality factor
$\chi\geq 1$	Distance factor
$H(T_m(D_i,D_j))$	Entropy function of T_m
CD_m	Diversity of $T_m(D_i,D_j)$
ST , IT , TM , SP	Privacy preference
$\lambda=[\lambda 1,\lambda 2,\lambda 3,\lambda 4]$	Weight of privacy preference
Y_1 , Y_2 , Y_3 , Y_4	Privacy function
ω_i	Weight of privacy function
$GP(D_i,D_j)$	Privacy between D_i and D_j
$A=(A_1\ldots A_j\ldots A_m),j<m$	Private attribute set
H_{tp}	Relation between H_1 and H_2 ,
H_1	Privacy loss
H_2	Trust gain
ϕ	Parameter of privacy loss
ψ	Parameter of trust gain
e_t	Evaluation error at time t
E_{di}	Privacy disclosure of *ith* access
rq	Possible interaction access

formula (1):

$$0\leq tr\_\omega_m\leq 1,\quad \sum_{m=1}^{M} tr\_\omega_m=1 \tag{1}$$

$TG(D_i,D_j,S,t)$ represents the total trust evaluation between entity D_i and entity D_j, it can be expressed as formula (2):

$$TG(D_i,D_j,S,t)=\sum_{m=1}^{M} tr\_\omega_m T_m(D_i,D_j) \tag{2}$$

where S is the service provided by D_j, the category and quality of service can be determined by $TG(D_i,D_j,S,t)$, when the value of $TG(D_i,D_j,S,t)$ is higher, the quality of service is better, where t is the interactive time stamp.

A. TRUST DECISION FUNCTION

In the process of trust decision, operation is determined by the map relationship between trust and authority. Assume that the total trust degree $TG(D_i,D_j)$ has N level $RS=\{RS_1,\cdots,RS_i,\cdots,RS_N\}$, $0\leq RS_i\leq 1$ $(i=1,2,\cdots \mathrm{N})$. RS is an order division of space; the service provider can provide service set $S=\{s_1,s_2,\cdots,s_P\}$ that is also an order division class, then the trust decision function $\Phi(TG(D_i,D_j))$ between $S=\{s_1,s_2,\cdots,s_P\}$ and $TG(D_i,D_j)$ is defined as formula (3):

$$\Theta(TG(D_i,D_j))=\begin{cases} s_P, & RS_N\leq TG(D_i,D_j)\leq 1\\ s_{P-1}, & RS_{N-1}\leq TG(D_i,D_j)<RS_N\\ \vdots & \vdots\\ s_2, & RS_1\leq TG(D_i,D_j)<RS_2\\ s_1, & 0\leq TG(D_i,D_j)<RS_1 \end{cases} \tag{3}$$

$RS=\{RS_1,RS_2,\cdots,RS_i,\cdots,RS_N\}$ is determined by the application requirements in the cloud computing, when D_i requests service from D_j, permission is determined by the trust degree. For example, a cloud system provides 3 levels of services, $S=(s_1,s_2,s_3)$, s_1, s_2, s_3 represent deny, read and write service, respectively. The corresponding decision space is $RS=\{RS_1,RS_2\}=\{0.3,0.5\}$, and the trust decision function can be expressed as the following formula (4):

$$\Theta(TG(D_i,D_j))=\begin{cases} s_3, & 0.5\leq TG(D_i,D_j)\leq 1\\ s_2, & 0.3\leq TG(D_i,D_j)<0.5\\ s_1, & 0\leq TG(D_i,D_j)<0.3 \end{cases} \tag{4}$$

Assume that the trust degree of D_i is $TG(D_i,D_j)=0.2$, then the decision result is $\Theta(TG(D_i,D_j))=\Theta(0.2)=s_1=$ *deny*. In the following sections, we will introduce direct trust, trust risk, feedback trust, and reward punishment factors to describe the trust relationship.

B. DIRECT TRUST FUNCTION

Direct trust is usually made up of multiple factors, and the relevant attributes can be selected from the database record of the service provider.

1) WEIGHT CALCULATION

To more objectively quantify the multiple indicators, the maximum entropy method is used to determine the factor weight in decision making. There are m users and n attributes of the direct trust evaluation, matrix $E(D)$ is shown in formula (5), e_{ij} is the evaluation score of the *ith* user to the *jth* attribute:

$$E(D)=\begin{bmatrix} e_{11}, & e_{12}, & \cdots & e_{1n}\\ e_{21} & e_{22} & \cdots & e_{2n}\\ \cdots & \cdots & \ddots & \cdots\\ e_{m1} & e_{m2} & \cdots & e_{mn} \end{bmatrix} \tag{5}$$

Entropy weight method: $E = (e_{ij})_{m\times n}$

$$e_j = -k\sum_{i=1}^{m} p_{ij}\cdot \ln p_{ij}, \quad p_{ij} = e_{ij}/\sum_{i=1}^{m} e_{ij} \quad (i \le j \le n), \quad k = 1/\ln m \tag{6}$$

The *jth* attribute weight:

$$W_j = (1-e_j)/\sum_{j=1}^{n}(1-e_j), \quad (1 \le j \le n)$$

$$0 \le W_j \le 1, \quad \sum_{j=1}^{n} W_j = 1 \tag{7}$$

2) DECAY TIME FACTOR

Trust computing is closely related to time, so it is necessary to introduce the decay time factor. In the section, let's take a few assumptions: t_i is the time span of the *ith* transaction service; t_i^1 represents the start time of the *ith* transaction; t_i^2 indicates the end time of the *ith* transaction; t_0 is the time of user successful registration; n is the number of interactions between the user and the service provider; so, the decay time factor $T^{(i)}$ can be expressed as formula (8):

$$T^{(i)} = \frac{1}{2}\left[\frac{t_i - t_0}{\sum_{j=1}^{n}(t_j - t_0)} + \frac{t_i^2 - t_i^1}{\sum_{j=1}^{n}(t_j^2 - t_j^1)}\right], \quad and \quad \sum_{i=1}^{n} T^{(i)} = 1 \tag{8}$$

3) CALCULATION DIRECT TRUST

According to formulas (6), (7) and (8), $T_1(D_i, D_j)$ is the direct trust evaluation between D_i and D_j, and n is the number of interactions as shown in formula (9):

$$T_1(D_i, D_j) = \sum_{j=1}^{n} e_j W_j T^{(i)} \tag{9}$$

C. FEEDBACK TRUST FUNCTION

Feedback trust is an important part of total trust, which is based on the transfer content of the entity, such as D_i trusts D_j, and D_j trusts D_k, so D_i also trusts D_k, and so on. There are many recommendation paths in the feedback trust, but how to choose and aggregate trust paths efficiently is an important problem.

Assume that D_i is a parent entity, all the neighbors are child nodes, a neighbor also has a neighbor, so we can construct a multilevel weighted direction trust tree (WDT, a sample is shown in Fig. 1). It is expressed as formula (10):

$$WDT(D_i) = (\langle D(S), DTR\rangle, T_1) \tag{10}$$

where $D(S)$ is a collection set of entities, DTR represents the direct trust relationship between the parent and child entities, and T_1 is the direct trust value. In the WDT, the level of the root entity is $level = 0$, the level of the direct neighbor of the root entity is $level = 1$, the level of the neighbor's neighbor is $level = 2$, and the rest of the nodes follow the arrangement.

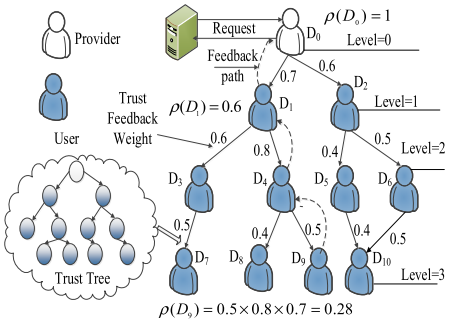


FIGURE 1. A WDT example of computational feedback trust.

Because the effects of each layer are different, a feedback weight factor is introduced to adjust the polymerization calculation accuracy. In an interaction process, the entity D_j needs to evaluate the feedback trust degree of the entity D_i, $\{F_1, F_2, \cdots, F_l\}$ is a feedback entity set, F_k is a feedback entity, so the feedback trust (such as Fig. 1) function is defined as:

$$T_2(D_i, D_j) = \begin{cases} \dfrac{\sum_{k=1}^{l}(\rho(F_k)\times T_1(D_k, D_j)}{\sum_{k=1}^{l}\rho(F_k)} & l \ne 0 \\ 0 & l = 0 \end{cases} \tag{11}$$

where l is the number of feedback entities, and $\rho(F_k)$ is the weight factor of feedback trust according to the "six degrees of separation" [21] it is expressed as formula (12):

$$\rho(F_k) = \begin{cases} 1, & level = 0 \\ \prod_{m=0}^{l} T_1(D_m, D_n), & 6 \ge level > 0 \end{cases} \tag{12}$$

where $T_1(D_m, D_n)$ represents the direct trust degree from D_m to D_n according to formula (10), *level* is the level of the feedback trust. For example in Fig. 1, $level = 1, \rho(D_1) = 0.5$; $level = 2$, then $\rho(D_3) = 0.5 \times 0.6 = 0.30$; when $level = 3$, $\rho(D_9) = 0.8 \times 0.6 \times 0.5 = 0.24$. Assume that the entity D_0 requires the feedback trust of the entity D_{10}, and there are two entities D_5 and D_6 interacting with D_{10}; the mutual direct trust degree is $T_1(D_5, D_{10}) = 0.4$, $T_1(D_6, D_{10}) = 0.5$. According to formula (12), $\rho(D_5) = 0.4 \times 0.6 = 0.24$ and $\rho(D_6) = 0.5 \times 0.6 = 0.30$. According to formula (11), $T_2(D_0, D_{10}) = (0.24 \times 0.4 + 0.3 \times 0.5)/(0.24 + 0.3) \approx 0.45$. According to formula (12), with the increment of *level*, the value of $\rho(F_k)$ gradually decreases. To improve the aggregation speed of feedback trust, we introduce quality factor and distance factor to adjust the scale of the feedback trust.

The quality factor $\eta \in [0, 1]$ is defined as a normal constant number; if $T_1(D_i, D_j) \ge \eta$, the feedback information is credible; if $T_1(D_i, D_j) < \eta$, the feedback information is incredible. Not only the quality factor can effectively control the scale of feedback trust aggregation, but also can reduce the malicious feedback entities with low trust value and improve the security of the system.

Distance factor $\chi \geq 1$ is also defined as a normal number, which is used to control the propagation depth of feedback trust. $level(D_i, D_j)$ represents the level distance between D_i and D_j, and when $level(D_i, D_j) \leq \chi$, the entity will forward the information to the neighbor entity; otherwise, it will stop the transmission, and can improve computing efficiency of feedback trust.

Algorithm 1 Compute Feedback Trust

Input: l, χ, η
Output: $T_2(D_i, D_j)$
1: $F(D_i) = \{F_1, F_2, \cdots, F_l\}$ represents the feedback entity of D_i;
2: **construct** WDT by formula (10);
3: **for** (all $D_k \in F(D_i)$)
4: **calculate** $T_1(D_i, D_j)$ by formulas (5), (6), (7), (8), (9);
5: **calculate** $\rho(F_k)$ by formula (12);
6: **calculate** $T_2(D_i, D_j)$ by formula (11);
7: **End**.

The feedback function (formula (11), (12)) are given to show how to aggregate k number of feedback entities. Therefore, malicious feedback can be avoided by improving quality factor η. For example, when $\eta = 0.4$, an entity with a trust value of less than 0.4 will not be adopted by the system; thus, malicious feedback will be avoided; the specific feedback trust algorithm is given above.

D. REWARD-PUNISHMENT FUNCTION

In the process of trust value calculation, the honest entities should be rewarded; the malicious entities must be punished. Therefore, we introduce reward punishment function to the trust evaluation, which can encourage both sides to take honest actions and increase the probability of successful interaction, and is expressed by the formula (13):

$$T_3(D_i, D_j) = 1 - \frac{\sum_B F(D_i, D_j)}{B} \tag{13}$$

where $\sum_B F(D_i, D_j)$ represents the number of failure times, and B is the total number of transaction times. Because malicious entities often interrupt or deny service, the transaction failure rate of the cooperation entities becomes high, and the reward-punishment function can punish those bad behaviors.

E. TRUST RISK FUNCTION

According to [28] and requirements for quality of service, the risk function can be expressed as formula (14).

$$\begin{aligned} R(D_i, D_j) &= s_j \times (1 - TG(D_i, D_j, S, t)) \\ &= \Theta(TG(D_i, D_j, S, t)) \times [1 - TG(D_i, D_j, S, t)] \end{aligned} \tag{14}$$

where s_j represents the quality of service provider of D_j. According to experience, when the value of s_j is greater, the risk is greater. Trust risk function refers to the cognition of the uncertainty between service provider and user, it can be expressed the formula (15):

$$T_4(D_i, D_j) = 1 - R(D_i, D_j) \tag{15}$$

According to formula (14) and (15), risk and service have an inverse proportional relationship between $T_4(D_i, D_j)$ and $R(D_i, D_j)$.

F. WEIGHTS OF TRUST ATTRIBUTES

Based on the connotation and definition of information entropy [7], we can obtain the decision attribute function that is expressed as the following formula (16):

$$\begin{aligned} H(T_m(D_i, D_j)) = &-T_m(D_i, D_j) \log_2 T_m(D_i, D_j) \\ &- (1 - T_m(D_i, D_j)) \log_2 (1 - T_m(D_i, D_j)) \end{aligned} \tag{16}$$

where $T_m(D_i, D_j)$ represents the certainty of the *mth* metric attribute function, and $1 - T_m(D_i, D_j)$ represents the uncertainty of the *mth* attribute function.

Assume that the evaluation values of $T_2(D_i, D_j)$ and $T_1(D_i, D_j)$ are

$$\begin{bmatrix} T_1(D_i, D_j) & 1 - T_1(D_i, D_j) \\ 0.99 & 0.01 \end{bmatrix}$$

and

$$\begin{bmatrix} T_2(D_i, D_j) & 1 - T_2(D_i, D_j) \\ 0.5 & 0.5 \end{bmatrix},$$

so $H(T_1(D_i, D_j)) = -0.99 \log 0.99 - 0.01 \log 0.01 = 0.08$.

$H(T_2(D_i, D_j)) > H(T_1(D_i, D_j))$ show that the uncertainty of $T_2(D_i, D_j)$ is more than $T_1(D_i, D_j)$. According to formula (16), the entropy function of the decision factor is $0 \leq H(T_m(D_i, D_j)) \leq 1$, and it is symmetrical-axis of $T_m(D_i, D_j) = 0.5$.

Because information entropy can only reflect the uncertainty of the event, the symmetry of entropy function is not conductive to decision making. Therefore, we introduce formulas (17) and (18) to correct this limitation, and define CD_m as the class diversity of decision factors $T_m(D_i, D_j)$, $(m = 1, 2, \cdots, M)$:

$$CD_m = \begin{cases} 1 - \frac{1}{\log_2^P} H(T_m(D_i, D_j)), & T_m(D_i, D_j) > 0.5 \\ 0 & T_m(D_i, D_j) < 0.5 \end{cases} \tag{17}$$

The weight tr_ω_m of the decision function is calculated by formula (18):

$$tr\_\omega_m = CD_m / \sum_{m=1}^{M} CD_m, \ 0 \leq tr\_\omega_m \leq 1, \ \sum_{m=1}^{4} tr\_\omega_m = 1 \tag{18}$$

When the entropy of the decision factor is no greater than 0.5, CD_m is 0, so it can effectively reduce risk by filtering out some unstable factors.

TABLE 2. Weight of decision factor.

m	$T_m(D_i, D_j)$	$1-T_m(D_i, D_j)$	$H(T_m(D_i, D_j))$	CD_m	tr_ω_m
1	0.6	0.4	0.9708	0.5818	0.2968
2	0.4	0.6	0.9708	0	0
3	0.8	0.2	0.7205	0.6896	0.3516
4	0.8	0.2	0.7205	0.6896	0.3516

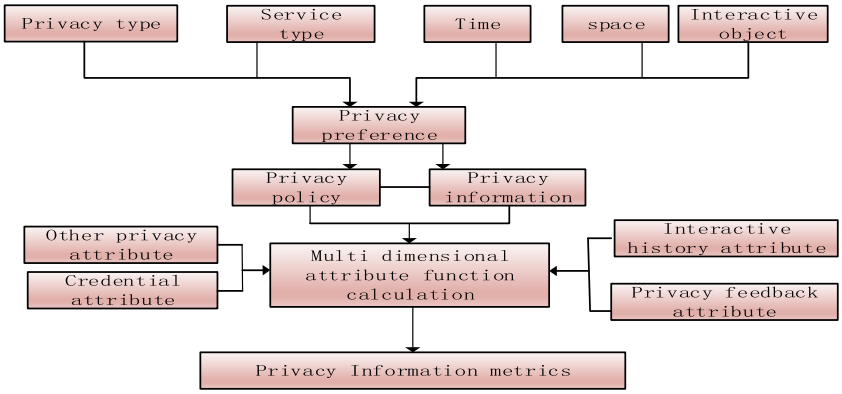


FIGURE 2. Architecture of privacy metrics based on multi-factor.

In Table 2, the values of $H(T_1(D_i, D_j))$, $H(T_2(D_i, D_j))$, $H(T_3(D_i, D_j))$ and $H(T_4(D_i, D_j))$ are 0.9708, 0.9708, 0.7205, 0.7205, respectively; this means that the average uncertainties of $T_1(D_i, D_j)$ and $T_2(D_i, D_j)$ are greater than $T_3(D_i, D_j)$ and $T_4(D_i, D_j)$. This finding reflects the symmetry of a decision factor and indicates that the information entropy cannot describe the subjective meaning of events. In Table 2, $tr\_\omega_3 = 0.3516$, and $tr\_\omega_1 = 0.2968$, which indicates that $T_3(D_i, D_j)$ is more important than $T_1(D_i, D_j)$. According to formula (1), (2) and (18), so, the total trust degree of Table 2 can be expressed as $TG(D_i, D_j, S, t) = 0.6 \times 0.2966 + 0.3516 \times 0.8 = 0.4592$.

G. TRUST EVALUATION ALGORITHM

In the section, based on above trust attributes, factors, and corresponding functions, we synthesize and put forward a total trust evaluation algorithm that can be used to determine whether to provide the service to requester in a cloud computing system.

According to algorithms (1) and (2), the cloud service system can decide to accept or refuse the user's request, whether s_j conforms with the total trust function $TG(D_i, D_j, S, t)$. If $\Psi(TG(D_i, D_j, S, t)) \geq s_j$ is true, the system can provide services s_j to D_i; otherwise, it refuses the request. In addition, the authorization operation mapping relationship between service and trust can be adopted by actual requirement.

Algorithm 2 Total Trust Computing

Input $N, n, H, \chi, \eta, LEVEL, M$
Output $TG(D_i, D_j, S, t)$
1: $F(D_i) = \{F_1, F_2, \cdots, F_n\}$;
2: **calculate** the decision factors:
3: $T_1(D_i, D_j) \rightarrow$ direct trust function,
4: $T_2(D_i, D_j) \rightarrow$ feedback trust function,
5: $T_3(D_i, D_j) \rightarrow$ reward-punishment function,
6: $T_4(D_i, D_j) \rightarrow$ trust risk function;
7: **calculate** tr_ω_m of decision function;
8: **calculate** total trust $TG(D_i, D_j, S, t)$;
9: **End**.

IV. PRIVACY METRIC

To meet the requirement of privacy protection, the privacy metric requires a comprehensive investigation of multiple influencing factors and relative objective weight method [6], [30]. In the paper, we assume that it includes the following parts: privacy preference of the participants, the credential attributes, privacy interaction history, the privacy feedback and weight of privacy attribute; the details are shown in Fig.2.

A. PRIVACY PREFERENCE FUNCTION

Assuming that privacy preference includes 4 parts: ST represents service type; IT represents preference of interacting entity; TM represent temporal preference; SP represents spatial preference, they are represented as follows:

$$\begin{aligned} &ST[st_1, st_2, \cdots st_m] \\ &IT[it_1, it_2, \cdots it_n] \\ &TM[tm_1, tm_2, \cdots tm_y] \\ &SP[sp_1, sp_2, \cdots sp_z] \end{aligned} \tag{19}$$

These above four vectors represent some requirements and can construct matrix R_1, which is expressed as formula (20):

$$R_1 = \begin{bmatrix} r_{11} & r_{12}, & \dots & r_{1m} \\ r_{21} & r_{22}, & \dots & r_{2n} \\ r_{31} & r_{32}, & \dots & r_{3y} \\ r_{41} & r_{42}, & \dots & r_{4z} \end{bmatrix} \tag{20}$$

where $r_{ij} \in [0, 1]$ represents the satisfaction of the service to the *jth* constraint for the *ith* preference, the privacy preference function Y_1 is expressed as the following formula (21):

$$Y_1 = \lambda 1 \times \sum_{j=1}^{m} r_{1_j}/m + \lambda 2 \times \sum_{j=1}^{n} r_{2_j}/n + \lambda 3 \times \sum_{j=1}^{y} r_{3_j}/y + +\lambda 4 \times \sum_{j=1}^{z} r_{4_j}/z \tag{21}$$

$\lambda = [\lambda 1, \lambda 2, \lambda 3, \lambda 4]$ represents the weight of the privacy preference attribute.

B. CREDENTIAL ATTRIBUTE FUNCTION

Assume that $RC = \{rc_1, rc_2, \cdots, rc_i, \cdots, rc_n\}$ represents a restricted credential set, and $SC = \{sc_1, sc_2, \cdots, sc_j, \cdots, sc_n\}$ represents the satisfaction matrix of a privacy credential set, $sc_j \in [0, 1]$ is the satisfaction degree for the *jth* credential. The credential attribute function Y_2 is shown as follows:

$$Y_2 = \sum_{j=1}^{\mathrm{n}} sc_j/n \tag{22}$$

C. INTERACTION HISTORY FUNCTION

$SH = \{(sh_{ij}^{(1)}, sh_{ij}^{(2)}, \cdots, sh_{ij}^{(l)}, \cdots, sh_{ij}^{(h)})\}$, $l \in [1, h]$, $sh_{ij}^{(l)}$ is the privacy information between D_i and D_j, h represents the number of privacy interactions, $sh_{ij}^{(1)}$ represents the oldest interaction, $sh_{ij}^{(h)}$ represents the latest interaction, and the direct interactive history function Y_3 are shown as formula (23) and (24):

$$Y_3(D_i, D_j) = \begin{cases} \sum_{l=1}^{h} sh_{ij}^{(l)} \times hw(l)/h, & h \neq 0 \\ 0, & h = 0 \end{cases} \tag{23}$$

$$hw(l) = \begin{cases} 1 & l = h \\ hw(l-1) = hw(l) - 1/h & 1 < l < h \end{cases} \tag{24}$$

where $hw(l)$ represents the weight of the interactive history between D_i and D_j.

D. PRIVACY FEEDBACK FUNCTION

Assuming that the interaction has a disclosure risk between D_i and D_j, the legal disclosure privacy information is $PI = (pi_1, pi_2, \dots, pi_m)$, $PI' = (pi'_1, pi'_2, \dots, pi'_n)(m \geq n)$ is the illegal disclosure privacy information, the amount of PI and PI' are expressed as $PA = (pa_1, pa_2, \dots, pa_m)$ and $PA' = (pa'_1, pa'_2, \dots, pa'_n)$, privacy feedback function Y_4 is the formula (25):

$$Y_4(D_i, D_j) = (\sum_{j=1}^{n} \varsigma_j \times pa'_j)/(\sum_{i=1}^{m} \varsigma_i \times pa_i) \tag{25}$$

$\varsigma = (\varsigma_1, \varsigma_2, \dots, \varsigma_m)$, $\sum_{i=1}^{m} \varsigma_i = 1$, $\varsigma_i \geq 0$, $i, j = 1, 2, \cdots m$ is a weight vector of privacy information.

E. WEIGHT OF PRIVACY ATTRIBUTE

The effect of multiple attributes is different, so we propose a weight method [25]. Let $W = (\omega_1, \omega_2, \cdots, \omega_m)$ express the weight vector of the privacy attribute function, according to the literature [22], "Or metric method" is: $Orness(W) = \frac{1}{m-1} \sum_{i=1}^{m} (m-i)\omega_i$; the dispersion degree is $Disp(W) = -\sum_{i=1}^{m} \omega_i \ln \omega_i$, further, $0 \leq Disp(W) \leq \ln m$, which meets these following three conditions:

$$\max imize: \ -\sum_{i=1}^{m} \omega_i \ln \omega_i \tag{26}$$

$$Orness(W) = \alpha, \quad \alpha \in [0, 1] \tag{27}$$

$$\sum_{i=1}^{m} \omega_i = 1, \quad \omega_i \in [0, 1], \ i = 1, 2, \cdots m \tag{28}$$

From formula (26), (27), (28) and the maximum dispersion principle [22], we can get formula (29), (30), (31), (32):

$$\alpha = Orness(W) = \frac{1}{m-1} \sum_{i=1}^{m} (m-i)\omega_i \tag{29}$$

$$\ln \omega_i = \frac{i-1}{m-1} \ln \omega_m + \frac{m-i}{m-1} \ln \omega_1 \Rightarrow \omega_i = \sqrt[m-1]{\omega_1^{m-i} \omega_m^{i-1}} \tag{30}$$

$$\omega_1[(m-1)\alpha + 1 - m\omega_1]^m = [(m-1)a]^{m-1}[((m-1)a - m)\omega_1 + 1] \tag{31}$$

$$\omega_m = \frac{((m-1)\alpha - m)\omega_1 + 1}{(m-1)a + 1 - m\omega_1} \tag{32}$$

In practical applications, participant can set reasonable values of α and calculate $\omega_1, \omega_i, \omega_m$ by formulas (30), (31), and (32). According to above privacy functions, we propose algorithm 3 for calculating the weight of privacy attributes.

In algorithm 3, the classification weight vector is determined by m and a. In an application environment, m is a certain value, the key is how to determine a reasonably. According to the Table 3, when $\alpha = 0$, then $\omega_1 = 1$, and $\omega_2 = \omega_3 = \cdots \omega_i = \cdots = \omega_m = 0$; when $\alpha = 1$, then $\omega_m = 1$, $\omega_1 = \omega_2 = \cdots \omega_i = \cdots = \omega_{m-1} = 0$; when $\alpha = 0.5$, $\omega_1 = \omega_2 = \cdots \omega_i = \cdots = \omega_m = 1/m$, when $0 < \alpha < 1$, $a \neq 0.5$,

we can get different values of ω_i.

F. PRIVACY INFORMATION METRIC

According to formula (16), in a similar way, the entropy value of the *mth* factor function is calculated by the following

TABLE 3. The $(\omega_1, \omega_2, \omega_3, \omega_4)$ for different values of a.

Weight	$\alpha = 0$	$\alpha = 0.1$	$\alpha = 0.2$	$\alpha = 0.3$	$\alpha = 0.4$	$\alpha = 0.5$	$\alpha = 0.6$	$\alpha = 0.7$	$\alpha = 0.8$	$\alpha = 0.9$	$\alpha = 1.0$
ω_1	0.000	0.0104	0.0145	0.0983	0.1647	0.2500	0.3474	0.4612	0.5965	0.7646	1.000
ω_2	0.000	0.0434	0.1065	0.2756	0.2133	0.2500	0.2722	0.2757	0.2757	0.1818	0.000
ω_3	0.000	0.1821	0.2520	0.4614	0.2722	0.2500	0.2133	0.1647	0.1647	0.0433	0.000
ω_4	1.000	0.7641	0.5965	0.1647	0.3474	0.2500	0.1671	0.0984	0.0451	0.0103	0.000

Algorithm 3 Weight of the Privacy Attribute

1: **if** $0 < m \leq 2$
2: **then** $\omega_1 = a$,
3: $\omega_2 = 1 - a$;
4: **if** $m > 2$
5: **then** $\omega_1[(m-1)\alpha + 1 - m\omega_1]^m = [(m-1)a]^{m-1}[((m-1)a - m)\omega_1 + 1]$,
6: $\omega_m = \frac{((m-1)\alpha - m)\omega_1 + 1}{(m-1)a + 1 - m\omega_1}$;
7: **for** $i = 2$ to $m - 1$ do
8: $\omega_i = \sqrt[m-1]{\omega_1^{m-i}\omega_m^{i-1}}$;
9: **when** $\omega_1 = \omega_2 = \cdots = \omega_m = \frac{1}{m}$
10: $\Rightarrow disp(W) = \ln m$, $a = 0.5$;
11: **End**.

Algorithm 4 Multifactor Privacy Information

Input: at the t, the disclosure of private information between the user and provider
Output: compute result of privacy information
1: **calculate** the privacy functions Y_1, Y_2, Y_3, and Y_4;
2: **calculate** the information entropy of Y_1, Y_2, Y_3, and Y_4;
3: **calculate** the weight of the metric attribute function (algorithm 3);
4: **calculate** privacy information results.
5: **End**

formula (33):

$$H(Y_m(D_i, D_j)) = -Y_m(D_i, D_j)\log_2 Y_m(D_i, D_j) - (1 - Y_m(D_i, D_j))\log_2(1 - Y_m(D_i, D_j)) \quad (33)$$

where $Y_m(D_i, D_j)$ indicates the certainty of the *mth* privacy function, $1 - Y_m(D_i, D_j)$ indicates the uncertainty of the *mth* privacy function. Thus, privacy information $GP(D_i, D_j)$ is calculated by the following formula (34):

$$GP(D_i, D_j) = \sum_{m=1}^{4} \omega_m H(Y_m(D_i, D_j)), \quad 0 \leq \omega_m \leq 1, \quad \sum_{m=1}^{4} \omega_m = 1 \quad (34)$$

where $H(Y_m(D_i, D_j))$ is the entropy of the *mth* attribute function; ω_m is the weight of the *mth* attribute function. Further, combining with these above privacy attributes and weight functions, we propose a total privacy computation algorithm (4).

V. RELATION BETWEEN TRUST AND PRIVACY

Data information disclosure means privacy loss; however, the improvement of trust reduces the requirement for privacy [18]. The interest of the data owner is to minimize privacy loss at an acceptable trust level; different people have different knowledge of private information [26]. In the next sections, we make use of information entropy theory for quantifying privacy loss and trust gain to construct a tradeoff relationship model.

A. ESTIMATE AND QUANTIFYING PRIVACY LOSS

Assume that these private attributes are $A = (A_1, A_2, \ldots A_j, \ldots, A_m)$, $j < m$, according to the restricted credentials in section IV, which can be partitioned by a service provider into revealed subsets $R(cs)$ and unrevealed subsets $P(cs)$ to the receiver [24]. Assume that a user has a subset credentials $N_c = \{rc_1, rc_2, \cdots, rc_i, \cdots, rc_n\}$ from $P(cs)$, which satisfies the minimum requirement for building trust. So, the privacy loss problem can be formulated as follows:

$$\min\{\Pr ivacyLoss(N_c \cup R(cs)) - \Pr ivacyLoss(R(cs))|N_c \; satisfy \; trust \; requirement \quad (35)$$

Assume that entity D_i requires entity D_j to achieve trust level TG_a before disclosing a piece of privacy, and currently, the trust level is TG_b between D_i and D_j. Let us consider two situations:

1) If $TG_b \geq TG_a$, the privacy loss can be calculated by formula (33) and formula (34):

$$H(Y_m(D_i, D_j)) = -Y_m(D_i, D_j)\log_2 Y_m(D_i, D_j) - (1 - Y_m(D_i, D_j))\log_2(1 - Y_m(D_i, D_j)),$$
$$GP(D_i, D_j) = \sum_{m=1}^{4} \omega_m H(Y_m(D_i, D_j)), \quad 0 \leq \omega_m \leq 1, \quad \sum_{m=1}^{4} \omega_m = 1.$$

2) If $TG_b < TG_a$, this situation would lead to relative privacy information loss when the private information is disclosed.

Assume that a credential rc_i with respect to an attribute A_j has a finite domain $\{V_1, V_2, \cdots, V_i, \cdots, V_m\}$, the probability of $A_j = V_i$ is $\Pr ob(A_j = V_i|R(cs))$, the probability of $A_j = V_i$ in rc_i is $\Pr ob(A_j = V_i|R(cs) \cup rc_i)$, so the privacy loss is quantified based on entropy:

$$\begin{aligned} H_1 &= privacyloss_{A_j}(rc_i|R(cs)) \\ &= \sum_{i=1}^{m} (-\Pr ob_i \log_2(\Pr ob_i)) \\ &\quad - \sum_{i=1}^{m} (-\Pr ob_i^{\Delta} \log_2(\Pr ob_i^{\Delta})) \\ \Pr ob_i^{\Delta} &= \Pr ob(A_j = V_i|R(cs) \cup rc_i) \\ \Pr ob_i &= \Pr ob(A_j = V_i|R(cs)) \end{aligned} \tag{36}$$

where H_1 expresses average information loss when disclosing a piece of privacy with private attributes. A larger $\Pr ob(A_j = V_i|R(cs))$ indicates less privacy loss and a higher probability of achieving TG_a with TG_b.

B. ESTIMATE AND QUANTIFYING TRUST GAIN

The trust model has already been shown in section III, and we can propose the following formula (37) is to compute the trust gain:

$$trust\_gain = TG_{new} - TG_{old} \tag{37}$$

Privacy loss can impact the trust evaluation in formula (35), TG_{old} and TG_{new} represent the old and new trust of the entity, respectively. According to the above section (V, A), let $P_2 = prob(TG_c/TG_b)$ denotes the probability of achieving TG_c under condition TG_b. $P_{2i} = prob(TG_{ci}/TG_{bi})$ represents the conditional probability of the *ith* credential from the $N_c = \{rc_1, rc_2, \cdots, rc_i, \cdots, rc_n\}$ when disclosing the private information. Let $p'_1, p'_2 \cdots p'_n$ denote the original values of p_{2_i}, and the conditional probability formula (38) is expressed below:

$$P_{2i} = \frac{p'_i}{p'_1 + p'_2 + \cdots p'_n} \tag{38}$$

Based on the above formula (38), the trust gain is expressed as the following formula (39):

$$\begin{aligned} H_2 = -k(\sum_{i=1}^{n} p_{2i} \log_2 p_{2i}) \\ \times (\sum_{i=1}^{n} p_{2i} = 1, k = p'_1 + p'_2 + \cdots p'_n) \end{aligned} \tag{39}$$

Then, H_2 expresses average trust gain by disclosing private information. A greater value of $P_2 = prob(TG_c/TG_b)$ indicates more trust gain because it indicates lower uncertainty for TG_c when disclosing a piece of privacy [25].

C. TRADEOFF BETWEEN PRIVACY AND TRUST

Both privacy and trust are related to knowledge about an entity; however, there is an inherent conflict between trust and privacy [14], [15], [19]. For example, an online seller might reward a high trust customer with special benefits, such as discounted prices. Normally, he/she can reveal private digital credentials or past interaction histories to gain more trust [18], [26].

When one entity asks for information from another entity, the responder can compute and disclose the privacy information to the requester. We use H_{tp} to express the relationship between privacy loss H_1 and trust gain H_2, which can be expressed by formula (40):

$$H_{tp} = -\phi H_1 + \psi H_2, \quad \phi + \psi = 1 \tag{40}$$

We don't give the specific value of ϕ and ψ, because they can be adjusted by application and preference. According to the relation between privacy loss and trust gain, we give three guidelines for the parameter selection:

1) If it is necessary to balance privacy and trust, participant can choose $\phi = \psi = 0.5$.
2) If it is necessary to trade privacy for trust, participant can choose $\phi < \psi$.
3) If it is necessary to protect privacy, participant can choose $\phi > \psi$.

To illustrate the application of our research, let's explain an interaction example. The requester informs the responder that a set of credentials $N_c = \{rc_1, rc_2, \cdots, rc_i, \cdots, rc_n\}$ could be used, and there is no need to provide all credentials if the required trust can be established. Then, the responder can compute privacy information loss and trust gain for every credential, choose the proper ϕ and ψ to adjust the relationship between H_1 and H_2, and then combine the relevant rules to make privacy protection decisions [26], [27].

VI. EXPERIMENT ANALYSIS AND DISCUSSION

In this section, we design experiments (privacy loss, trust gain, interaction success rate, trust accuracy and privacy disclosure rate) to compare TTPM (tradeoff between trust and privacy model) with TPTV (Never Trust Anyone: Trust-Privacy tradeoffs in Vehicular Ad-Hoc Networks) [18] and PPVT (The penalty for privacy violations: How privacy violations impact trust online) [19].

Experimental environment: Intel Core i7-7500 U, 2.73 GHz 2 Duo CPU, 8G bytes of memory, MATLAB 2015a, Eclipse platform and SQL server. There are two data sets in our experimental evaluations: one is the real-life CENSUS data set at http://www.ipums.org, which contains the personal information of 500K American adults (Table 4); and the other one is the synthetic numeric data set.

A. PERFORMANCE METRICS ANALYSIS

In the section, we design experiments of privacy loss and trust gain under three different environments: privacy protection ($\phi > \psi$) or trust establishment ($\phi < \psi$) preference, balance

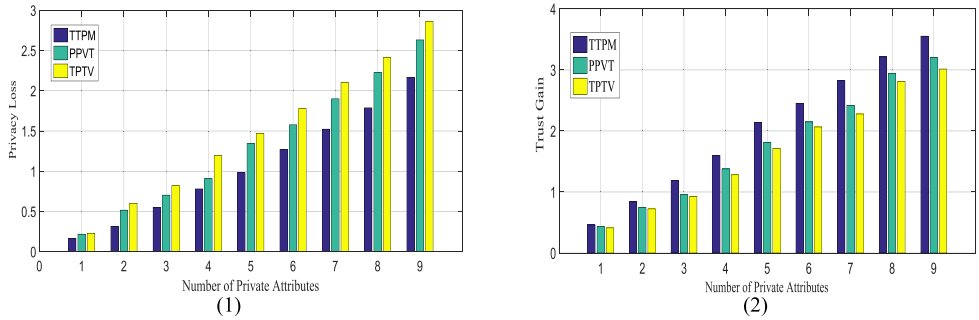


FIGURE 3. Performance comparison under privacy protection preference. (1) Privacy loss. (2) Trust gain.

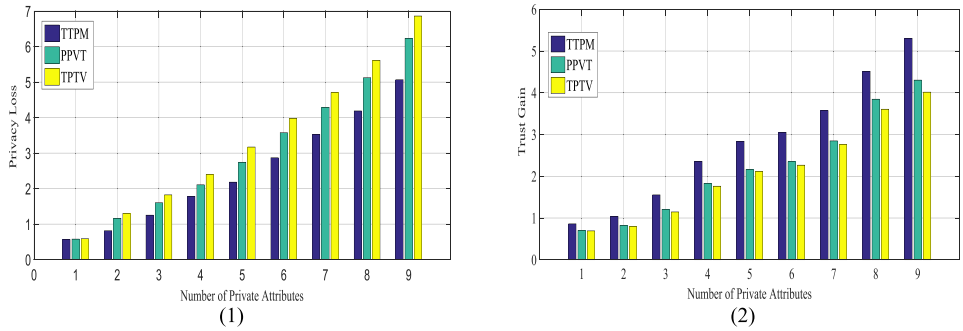


FIGURE 4. Performance comparison under trust establishment preference. (1) Privacy loss. (2) Trust gain.

TABLE 4. Summary of attributes in CENSUS.

Attribute	Number of values
Age	78
Country	83
Education	17
Gender	2
Marital	6
Occupation	50
Race	9
Salary-class	50
Work-class	8

privacy and trust ($\phi = \psi = 0.5$), these specific parameters are as follows:

(1) The disclosure of privacy information requires more than one kind of trust certificates; (2) privacy can be calculated by algorithm 4; (3) there are 9 kinds of private attributes, the categories of disclosure privacy information are randomly generated; and (4) we randomly generate interactions and repeat 50 times, and calculate the average value.

1) PRIVACY PROTECTION PREFERENCE

In the section, we design experiments of privacy loss and trust gain under the privacy protection preference. In the Fig. 3, the horizontal axis represents the number of privacy information categories, and the vertical axis represents the metrics results of private information.

In Fig. 3(1), when the number of privacy attributes is 9, the privacy loss of TTPM is 0.673 and 0.221 less than TPTV and PPVT, respectively. In Fig. 3(2), when the number of private attributes is 9, the trust gain of TTPM is also higher than PPVT and TPTV 0.402, 0.621, respectively. Next, we give specific reasons and explanations of different articles.

The relationship between trust and privacy is simple in the PPVT which also lacks dynamic protection mechanism; TPTV does not study the impact of dynamic trust on privacy disclosure. TTPM not only has not these shortcomings, but also integrates information entropy and multiple factors into privacy and trust model, with the growing number of private attributes, it has clear and stable advantages over TPTV and PPVT.

2) TRUST ESTABLISHMENT PREFERENCE

In the section, we design related experiments of privacy loss and trust gain under the trust establishment preference. Note: these related meanings of the coordinate axis of Figure 4 are the same as the Figure 3.

In Fig.4(1), when the number of private attributes is 9, the privacy loss of TTPM is 1.643 and 0.621 less than TPTV and PPVT, respectively. In Fig.4(2), when the number of private attributes is 9, the trust gain of TTPM is 1.012 and 1.132 higher than TPTV and PPVT, respectively.

Because PPVT can only take compensation according to the privacy deviation, and lack the ability to trust feedback compensation for privacy. In addition, the relationship

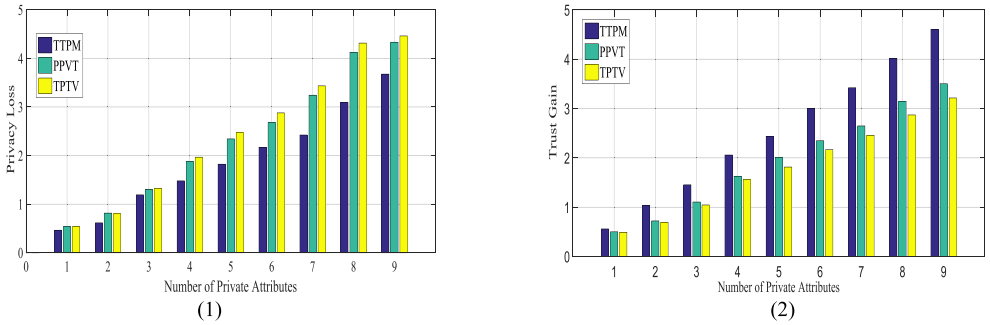


FIGURE 5. Performance comparison under balance privacy and trust. (1) Privacy loss. (2) Trust gain.

between trust and privacy of TPTV is also relatively fixed, trust factor lacks objective and concrete quantification to adapt to dynamic trust environment. TTPM adopts a several factors to trust evaluation, such as trust risk, reward punishment and so on, distance factor and quality factor are used in the feedback trust which can cope with the trust establishment preference environment. Thus, it can obtain less privacy loss and more trust gain than TPTV and PPVT, respectively.

3) BALANCE PRIVACY AND TRUST

In the section, we design related experiments of privacy loss and trust gain under balance privacy and trust. Note: the meanings of the coordinate axis of Figure. 5 are the same as the Figure. 3 and Figure. 4.

In Fig.5(1), when the number of private attributes is 9, the privacy loss of TTPM is 0.913 and 0.721 less than TPTV and PPVT, respectively. In Fig.5(2), when the number of private attributes is 9, the trust gain of TTPM is 1.062 and 1.412 higher than TPTV and PPVT, respectively. PPVT can only take compensation measures according to the privacy deviation. In the TPTV, the zero-sum relationship between trust and privacy is relatively fixed and lack of dynamic adaptability. TTPM builds a tradeoff model between trust and privacy and adjusts parameters according to requirement, with the increasing numbers of private attributes, which has better adaptability than PPVT and TPTV in balance privacy and trust environment.

B. INTERACTION SUCCESS RATE

Continuing the work of the last section, we compare the interaction success rate among three models. The horizontal axis indicates the number of attributes, and the vertical axis indicates the success rate of the interaction.

In Fig. 6. (1) under privacy protect preference, the interaction success rate is relatively lower; in Fig. 6. (2) under trust establishment preference, the interaction success rate is relatively higher; in Fig. 6. (3) under privacy protect preference, the interaction success rate is relatively moderate. In addition, because of tradeoff relationship between trust and privacy, we can conclude that the success rate of TTPM is stable at

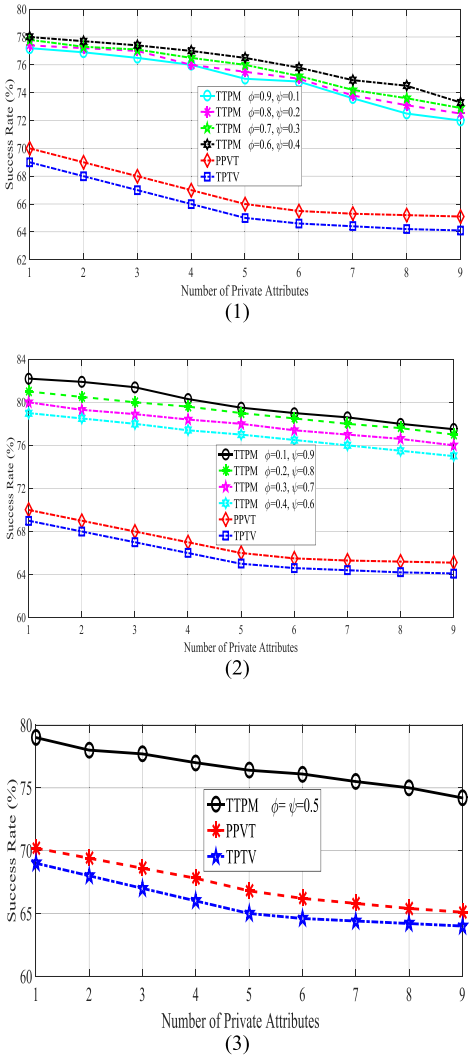


FIGURE 6. Interaction success rate of three models. (1) Privacy protection preference ($\phi > \psi$). (2) Trust establishment preference ($\phi < \psi$). (3) Balance privacy and trust ($\phi = \psi = 0.5$).

approximately 75%, and the choice of parameters ϕ and ψ have an approximately 5% influence on the interaction.

In the PPVT, online trust evaluation is influenced by the penalty of privacy deviation, the privacy protection is rel-

atively weak because of lacking trust feedback to correct privacy. In the TPTV, the relationship between privacy loss and trust gain is relatively fixed and simple. TTPM not only propose trust and privacy evaluation model and construct a tradeoff relationship model between trust and privacy based on information entropy theory, but also can dynamically choose trust gain or privacy protection, so it has a great advantage in the interaction success rate than TPTV and PPVT.

C. ACCURACY OF TRUST EVOLUATION

In the experiment, we generate 50K synthetic data records, and each record contains 1000 attributes, and each attribute value is randomly distributed in the [0, 1].

Due to the influence of many uncertain factors, the evaluation error is inevitable. Accuracy is used to check whether the scheme can accurately provide trust calculation, which can be measured by the error. The smaller the error, the higher the accuracy. Assuming that A_t is the actual trust value, TG_t is the trust evaluation value at time t, there are two methods of MAD (mean absolute deviation) and MAPE (mean absolute percentage error) for measuring the accuracy of the trust evaluation.

1) MEAN ABSOLUTE DEVIATION

$$MAD = \frac{\sum_{t=1}^{n} |TG_t - A_t|}{n} = \frac{\sum_{t=1}^{n} |e_t|}{n} \tag{41}$$

MAD is used to measure the degree of deviation of evaluation result. $e_t = TG_t - A_t$ is the evaluation error at time t, n is the number of experiment times.

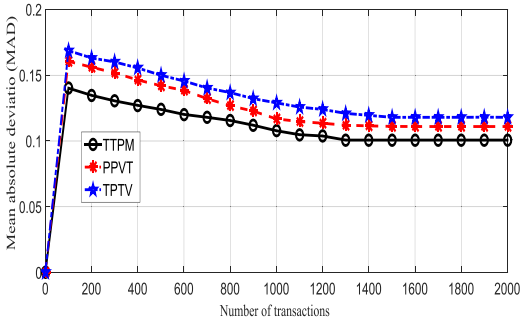


FIGURE 7. MAD in different number of transactions.

In the Fig.7, when the number of transactions is more than 1200, the average MAD of TTPM, PPVT, and TPTV is 0.1027, 0.1110, and 0.1183 respective. TTPM can be able to integrate information entropy into trust evaluation algorithm, so the error of trust evaluation is the lower than PPVT and TPTV.

2) MEAN ABSOLUTE PERCENTAGE ERROR

MAPE is also a measure method of accuracy, which usually can reflect the accursedness of the trust evaluation model. $e_t = TG_t - A_t$ is the error, A_t is the actual trust value at time t, and n is the number of interaction times.

$$MAPE = \frac{1}{n} \sum_{t=1}^{n} |\frac{e_t}{A_t}| (\times 100\%) \tag{42}$$

In the Fig.8, When the number of transactions is more than 1200, the MAPE of TTPM, PPVT and TPTV are 11.6%, 12.8%, 13.6%, respectively. Based on Fig. 7 and Fig. 8, TTPM adopts time decay, trust feedback, the dynamic performance is relatively good, but PPVT and TPTV lack similar mechanisms.

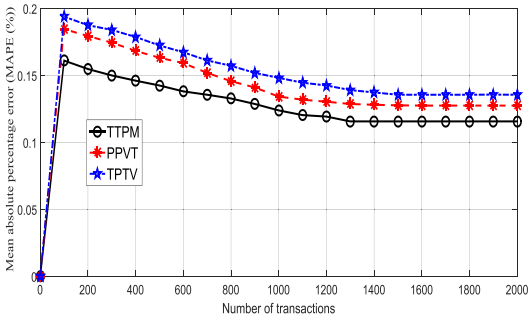


FIGURE 8. MAPE in different number of transactions.

D. PRIVACY DISCLOSURE ANALYSIS

According to the above 50K synthetic data, we further divide the data into three kinds of sensitivity: high (H), medium (M) and low (L).

In this experiment, the interactive request is randomly generated, the trust decision result is based on formula (1) and (2). Suppose that the user's trust T_r is lower than the trust threshold of the interaction requirement in the *ith* request; this is regarded as a privacy disclosure event E_{di}. So, the privacy disclosure rate is defined as the following formula (43):

$$privacy\ disclosure\ rate = \sum_{i=1}^{n} E_{di}/rq \tag{43}$$

where rq represents all possible interaction access, and n is the number of interactions.

Fig. 9, Fig.10 and Fig. 11 show the disclosure rate by varying the portion of L, M, H from 0 to 1, respectively. In the Fig. 9, the privacy disclosure rate of TTPM, PPVT, and TPTV is reduced from 0.389, 0.402, 0.411 to 0. In the Fig. 10, with the increment of M, the privacy disclosure rate of TTPM, PPVT, and TPTV remain stable at 0.265, 0.368, and 0.392, respectively. In the Fig. 11, the privacy disclosure rate of TTPM, PPVT, and TPTV remain stable at 0.481, 0.560, and 0.571, respectively. Based on the experiment results, the privacy disclosure rate of TTPM is relative lower than TPTV and PPVT.

There are zero sum relations between trust and privacy in the TPTV, quantification of privacy is relatively simple, which seriously affects the privacy protection in the cloud computing. In the PPVT, the weight of privacy attribute

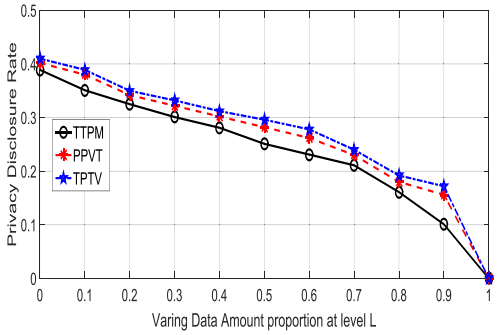


FIGURE 9. Disclosure rate (varying data amount at level L).

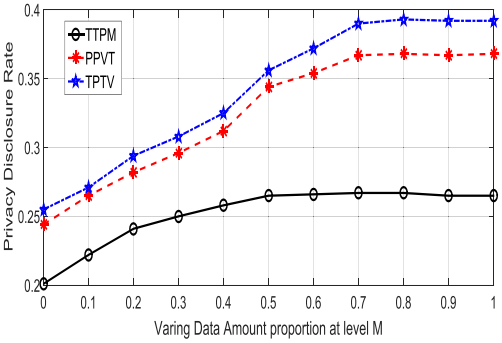


FIGURE 10. Disclosure rate (varying data amount at level M).

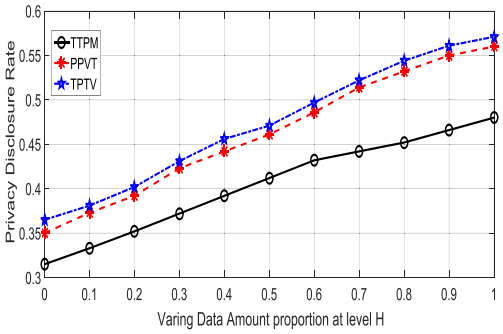


FIGURE 11. Disclosure rate (varying data amount at level H).

lacks quantitative formula, which leads to inaccurate privacy description. TTPM not only can make use of feedback privacy and multi-attribute privacy algorithms to adjust privacy disclosure, but also can adjust the related parameters by preference and requirement. Therefore, it is better than TPTV and PPVT in preventing privacy disclosure.

VII. CONCLUSION

When users interact with businesses and institutions, a paradox between privacy loss and trust gain is inevitable. In this paper, we research the relationship between privacy and trust in the cloud environment. First, we propose a trust evaluation model; second, we propose a novel privacy metric model; third, we propose a tradeoff between privacy and trust, which allow participants to select the service and dynamically adjust the privacy release granularity. Experimental results show that our research can effectively protect user privacy by quantifying trust, service, and other preference factors.

There are still weaknesses in the article; for example, the personalization requirement is still a difficult problem in cloud privacy protection. In addition, there should be a unique framework that can mitigate the problem between privacy and trust, and provide an enforcement mechanism for preserving the privacy of each partner.

REFERENCES

[1] Cloud Security Alliance. (2017). *Security Guidance for Critical Areas of Focus in Cloud Computing V4.0*. [Online]. Available: http://www.cloudsecurityalliance.org/

[2] L. S. Nishad, J. Paliwal, R. Pandey, S. Beniwal, and S. Kumar, "Security, privacy issues and challenges in cloud computing: A survey," in *Proc. 2nd Int. Conf. Inf. Commun. Technol. Competitive Strategies*, 2016, p. 47.

[3] R. K. Kalluri and C. V. G. Rao, "Addressing the security, privacy and trust challenges of cloud computing.," *Int. J. Comput. Sci. Inf. Technol.*, vol. 5, no. 5, pp. 6094–6097, 2014.

[4] J. Daubert, A. Wiesmaier, and P. Kikiras, "A view on privacy & trust in IoT," in *Proc. IEEE Int. Conf. Commun. Workshop (ICCW)*, Jun. 2015, pp. 2665–2670.

[5] J. Prüfer. *Trusting Privacy in the Cloud*. Social Science Electronic, 2014, pp. 2014–2073.

[6] R. Hirschprung, E. Toch, F. Bolton, and O. Maimon, "A methodology for estimating the value of privacy in information disclosure systems," *Comput. Human Behav.*, vol. 61, pp. 443–453, Aug. 2016.

[7] C. E. Shannon, "A mathematical theory of communication," *Bell Syst. Tech. J. Banner*, vol. 27, no. 3, pp. 379–423, Jul. 1948.

[8] L. Longpr and V. Kreinovich, "Entropy as a measure of average loss of privacy," *Thai J. Math.*, pp. 7–15, 2017.

[9] S.-H. Kim, C. Jung, and Y.-J. Lee, "An entropy-based analytic model for the privacy-preserving in open data," in *Proc. IEEE Int. Conf. Big Data (Big Data)*, Dec. 2016, pp. 3676–3684.

[10] J. Almasizadeh and M. A. Azgomi, "Mean privacy: A metric for security of computer systems," *Comput. Commun.*, vol. 52, pp. 47–59, Oct. 2014.

[11] I. Casas, J. Hurtado, and X. Zhu, "Social network privacy: Issues and measurement," in *Web Information Systems Engineering—WISE* (Lecture Notes in Computer Science), vol. 9419. 2015, pp. 488–502.

[12] J. Parra-Arnau, D. Rebollo-Monedero, and J. Forné, "Measuring the privacy of user profiles in personalized information systems," *Future Gener. Comput. Syst.*, vol. 33, pp. 53–63, Apr. 2014.

[13] S. Garcia-Rivadulla, "Personalization vs. privacy: An inevitable trade-off?" *IFLA J.*, vol. 42, no. 3, pp. 227–238, 2016.

[14] A. Aldini, A. Bogliolo, C. B. Lafuente, and J.-M. Seigneur, "On the trade-off among trust, privacy, and cost in incentive-based networks," in *Trust Management VIII* (IFIP Advances in Information and Communication Technology), vol. 430. 2016, pp. 205–212.

[15] L. Yang, X. Chen, J. Zhang, and H. V. Poor, "Cost-effective and privacy-preserving energy management for smart meters," *IEEE Trans. Smart Grid*, vol. 6, no. 1, pp. 486–495, Jan. 2015.

[16] D. Frey, A. Jégou, A.-M. Kermarrec, M. Raynal, and J. Stainer, "Trust-aware peer sampling: Performance and privacy tradeoffs," *Theor. Comput. Sci.*, vol. 512, pp. 67–83, Nov. 2013.

[17] Y. O. Basciftci, Y. Wang, and P. Ishwar, "On privacy-utility tradeoffs for constrained data release mechanisms," in *Proc. Inf. Theory Appl. Workshop*, Jan./Feb. 2017, pp. 1–6.

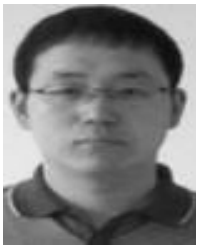
[18] A. K. Tyagi, S. Niladhuri, and R. Priya, "Never trust anyone: Trust-privacy trade-offs in vehicular ad-hoc networks," *Brit. J. Math. Comput. Sci.*, vol. 19, no. 6, pp. 1–23, 2016.

[19] K. Martin, "The penalty for privacy violations: How privacy violations impact trust online," *J. Bus. Res.*, vol. 82, pp. 103–116, Jan. 2018.

[20] X. Wang, J. Zhang, and Y. Wang, "Trust-aware privacy-preserving recommender system," in *Proc. 9th EAI Int. Conf. Mobile Multimedia Commun.*, 2016, pp. 107–115.

[21] J. Lunze, "Six degrees of separation in multi-agent systems," in *Proc. IEEE 55th Conf. Decis. Control (CDC)*, Dec. 2016, pp. 6838–6844.

[22] R. Fullér and P. Majlender, "An analytic approach for obtaining maximal entropy OWA operator weights," *Fuzzy Sets Syst.*, vol. 124, no. 1, pp. 53–57, 2001.
[23] P. G. Shynu and K. J. Singh, "A comprehensive survey and analysis on access control schemes in cloud environment," *Cybern. Inf. Technol.*, vol. 16, no. 1, pp. 19–38, 2016.
[24] L. Sankar, "Utility-privacy tradeoffs in databases: An information-theoretic approach," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 6, pp. 838–852, Jun. 2013.
[25] Z. Movahedi, Z. Hosseini, F. Bayan, and G. Pujolle, "Trust-distortion resistant trust management frameworks on mobile ad hoc networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 2, pp. 1287–1309, Sep. 2016.
[26] J.-D. Rusk, "Trust and decision making in the privacy paradox," in *Proc. Southern Assoc. Inf. Syst. Conf.*, Macon, GA, USA, Mar. 2014, pp. 1–7.
[27] D. Stevenson and J. Pasek, *Privacy Concern, Trust, Desire for Content Personalization*. Social Science Electronic, 2015.
[28] E. Cayirci and A. S. de Oliveira, "Modelling trust and risk for cloud services," *J. Cloud Comput.*, vol. 7, p. 14, Dec. 2018.
[29] G. Bansal, F. M. Zahedi, and D. Gefen, "Do context and personality matter? Trust and privacy concerns in disclosing private information online," *Inf. Manage.*, vol. 53, no. 1, pp. 1–21, 2015.
[30] H. Zhu, "Privacy calculus and its utility for personalization services in E-commerce: An analysis of consumer decision-making," *Inf. Manage.*, vol. 54, no. 4, pp. 427–437, 2017.



PAN JUN SUN received the M.S. degree in control theory and application from the Taiyuan University of Science and Technology, in 2010. He is currently pursuing the Ph.D. degree in information and communion system with Shanghai Jiao Tong University. His research interests include cloud computing, privacy preservation, access control, and trust management.