IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received December 21, 2020, accepted January 9, 2021, date of publication January 26, 2021, date of current version March 23, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3054634

Research on Adaptive Relationship Between Trust and Privacy in Cloud Service

HUAXIANG HAN
College of Engineering Science and Technology, Shanghai Ocean University, Shanghai 201306, China
e-mail: hxhan@shou.edu.cn

This work was supported in part by the Scientific Research Starting Foundation for the Young Teachers of Shanghai Ocean University under Grant A2-2006-00-200374, and in part by the Shanghai Young Teachers' Training and Support Program under Grant A1-2007-20-000213.

ABSTRACT To prevent privacy leakage, cloud services need to take corresponding methods, so participants often face the dilemma of service utility and privacy protection. In this paper, we propose a dynamic adaptive access control model based on trust permission and privacy protection to solve the problem of privacy disclosure and utility in the cloud service. Firstly, we add the concept of obligation and purpose into access control and establish the privacy information tree and privacy policy tree. Secondly, we establish a new trust evaluation and give the corresponding weight algorithm. Thirdly, we quantify the privacy information with the normal space and correlation coefficient method. Further, we propose a tradeoff relationship model between trust permission and privacy protection, each participant can select the corresponding parameters according to the actual requirement and personal preference. Experimental analysis and comparison results verify the feasibility, effectiveness, and superiority of our method. Finally, we summarize the work of this paper and point out the future development direction.

INDEX TERMS Access control, cloud service, privacy protection, trust permission, tradeoff.

I. INTRODUCTION

The convenience and economy of cloud computing services are very popular in the current network services. There are a lot of valuable resources in the cloud system, which has a great attraction to attackers. Due to the complexity of cloud computing structure and the dynamic market environment, cloud users are widely distributed and complex, so only the legitimacy of identity can't guarantee the reliability of behavior. Since an attack is a series of malicious acts, it is necessary to effectively control the identity authentication and access behavior of legitimate users in the cloud, and try to avoid the legitimate users damaging cloud resources through malicious operations.

Privacy is a kind of personal information that has nothing to do with the public interest and group interest and is not wanted or inconvenient to be known by others. Effective identity authentication can not prevent such attacks. So effective control of cloud user behavior is the focus of cloud security research. To prevent privacy data disclosure, data institutions usually adopt certain privacy protection technology to hide the sensitive attributes of users. Whether the processed data will leak the privacy, and how much the impact on the data available is the key factors affecting the data release. Therefore, research on privacy measurement is imminent.

The access control technology is a method of using one or more groups of policies to explicitly grant or control access rights and scope. It can prevent the invasion of illegal users by the improper behavior of legitimate users by controlling the operation of important resources, to ensure the legal use of network and system resources. At present, the traditional access control methods are difficult to adapt to the dynamic and complex network environment, so a new cloud service access model needs to be designed with the following advantages: (1) support and adapt to the dynamic changes of the cloud service environment. (2) The integration of a variety of privacy security protection mechanism, while ensuring fast performance. It provides a reliable privacy protection function.

The quantification of privacy and trust involves many factors. It is an important standard of high reliability and security for cloud services to evaluate the quantification of privacy and trust accurately and objectively. Therefore, it is necessary to construct a suitable weight method based on

The associate editor coordinating the review of this manuscript and approving it for publication was M. Anwar Hossain.

its characteristics. The relationship between trust and privacy is very close. To some extent, the two can be said to be opposite to each other, and trust technology is widely used in cloud services. Therefore, it is necessary to put forward a new approach to study the access control of cloud computing services under dynamic trust privacy.

This paper focuses on the properties of services and users as well as trust and privacy. Based on the analysis of the attributes of service and user, the concept of quantifiable service and trust is proposed, and access control has enough scalability and flexibility. At the same time, according to the idea of quantifying trust, privacy, and services, we extend the concept of service and propose an access control model. The main contributions of the paper are summarized as follows:
1) We add the concept of obligation and purpose into access control and establish the privacy information tree and privacy policy tree, propose the privacy disclosure rule.
2) We establish a new trust evaluation model and give the corresponding weight algorithm to effectively overcome the shortcomings of subjective imprecision.
3) We quantify the privacy information with the normal space concept and correlation coefficient method.
4) We propose a tradeoff relationship model between trust permission and privacy protection, give the optimal policy solution, a participant can select the corresponding parameters according to the actual requirement.

The structure of this paper is as follows. In section 2, we conclude some related work on trust, security, and privacy protection in the network service. In section 3, we present the related concept definitions based on trust, obligation, purpose, privacy information tree, trust permission function, and other elements. In section 4, we establish a multi-attribute trust evaluation model based on information entropy. In section 5, we propose a privacy metrics model based on normal space and correlation coefficient method. In section 6, we research and construct a trade-off policy relationship model between privacy and trust. In section 7, we design and discuss several experiments. In section 8, we summarize research and discuss future work.

II. RELATED WORK

A lot of researchers have put forward a variety of schemes and achieved a lot of research results. Based on the research content of this paper, we mainly analyze and compare the two types of research results.

A. PRIVACY METRICS AND MANAGEMENT

Lack of knowledge and control of data sharing will increase the threat to customer data and reduce the trust of these systems [1], [2]. Ranchal and Bhargava *et al.* in [3] proposed an efficient solution to implement security policies in web services, which can protect data privacy, enable data owners to control data disclosure decisions, and reduce illegal access risk, however, the execution of policies required high communication performance. Based on the privacy quantity, Kim and Park *et al.* in [4] discussed the factors that affect the willingness of the Internet of things services, which provided enlightenment and insight for the trade-off between privacy and willingness. But it was difficult to adapt to the personal requirement. Martin *et al.* in [5] measured the relative importance of violating privacy expectations to consumer website trust, the results showed that consumers pay more attention to privacy, but it can't provide the ability to control the experience online. Sun *et al.* in [6] proposed an access control model based on trust evaluation and designed relevant experiments to evaluate adaptability, accuracy, and efficiency. However, the relationship between privacy and trust was less. Oukemeni *et al.* in [7] proposed a general framework to guide the development of privacy measurement and provided an indicator to measure privacy protection; however, the operation of privacy parameters is difficult.

To ensure the availability of electronic data sources, Sankar and Rajagopalan *et al.* in [8] proposed a framework to quantify the privacy of personal identifying information and provide quantifiable benefits for multiple legitimate information consumers; however, it needs anonymity guarantee and has a small scope of application. Afifi and Zhou *et al.* in [9] constructed a new multivariate privacy feature quantification model, analyzed the sensitivity of identifiers, and proposed two different measurement methods to quantify privacy disclosure; however, there is a lack of optimization research on the information publication. Wang and He *et al.* in [10] proposed a two-stage framework to calculate the average value, which can achieve the optimal calculation accuracy on the premise of meeting the privacy requirements; however, the influence of the node on the calculation accuracy still needed further study.

B. PRIVACY AND MULTIPLE FACTORS

In cloud service, there are conflicts between privacy protection and utility. Padakandla and Kumar *et al.* in [11] accurately described the utility privacy trade-off in database cleaning, analyzed the general distribution of data, and measured the fidelity between the histogram of the original database and the antivirus database; however, the vulnerability of query response mechanism needed a more pragmatic quantity. Salama and Li *et al.* in [12] used the concept of region to deal with the privacy disclosure, maximize the use of utility and probability location deployment, and meet the requirements of privacy; however, the tradeoff still needs to be further studied from the perspective of game theory. Asikis and Pournaras et al in [13] proposed a general and novel privacy utility trade-off, analyzed the impact of diversity on privacy utility trajectory in information autonomous data sharing; however, it was difficult to meet the personalized privacy protection. Rassouli and Gündüz *et al.* in [14] introduced total variation distance to measure privacy leakage, solved the trade-off between utility and privacy, and provided the boundary of privacy leakage measured by mutual information; however, the accuracy of parameter attribute weight quantization was poor. Khokhar and Chen *et al.* in [15] quantified the trade-off between privacy and utility in health data publishing and proposed an analysis cost model to share personal health data; however, the calculation of this scheme was complex and lacked the research of attribute weight. Sun *et al.* in [16] proposed a trade-off model between privacy and trust, which can effectively protect users' privacy; however, the relationship between privacy and trust was relatively simple and lacked personalized privacy protection methods.

The data owner is usually reluctant to disclose their sensitive personal data and real identities to data consumers. In [17], users can decide to publish data items according to the aggregation opinions, who can adjust the parameters to make a balance between data sharing and privacy protection, but the privacy threshold setting was random. Niu and Zheng *et al.* in [18] proposed an effective combination of authenticity and privacy protection, which adopted encryption and signature to effectively maintain identity protection and data confidentiality; however, it was difficult to adapt to the real data service market. Pham and Yeo *et al.* in [19] designed a context-aware trust management scheme and proposed a secure and flexible framework to manage trust and privacy; however, the protocol was complex and the practicability was low. Verginadis and Patiniotakis *et al.* [20] proposed a new overall access control framework, supported the combination of effective context-aware access control strategies; however; the evaluation of access control rules was complex. In [21], the learning algorithm can converge to equilibrium, each user can achieve a balance between accuracy and privacy, but the game equilibrium research lacked the incentive mechanism.

How to protect the data privacy of statistical information has become the focus of attention. Zhang and Zhou *et al.* in [22] studied the issue of data publishing, used interactive differential privacy policy to count the privacy leakage, but the burden of computation was heavy. Qiao and Liu *et al.* in [23] proposed a data publishing algorithm based on wavelet transform, get a better partition structure, to improve the accuracy of the histogram counting query, but the adaptability was poor. Gai and Zhu *et al.* in [24] proposed a multi-layer access model of privacy protection in fog computing, to achieve the balance between privacy protection and computing costs, but the complexity was high and the burden of communication was heavy.

There are some problems in privacy protection and trust quantification in these above articles, such as the lack of accuracy and reliability, the relatively weak practicability, and dynamic adaptability. So we synthesize many factors and give a new solution based on the actual need.

III. THE BASIC MODEL AND RELATED CONCEPTS

In cloud computing, with the unrestricted access of users, services, and resources to the network, the mapping relationship changes dynamically. Therefore, we propose a new model to adapt to the dynamic relationship between the openness of the network environment and the trust permission and privacy (Fig. 1).

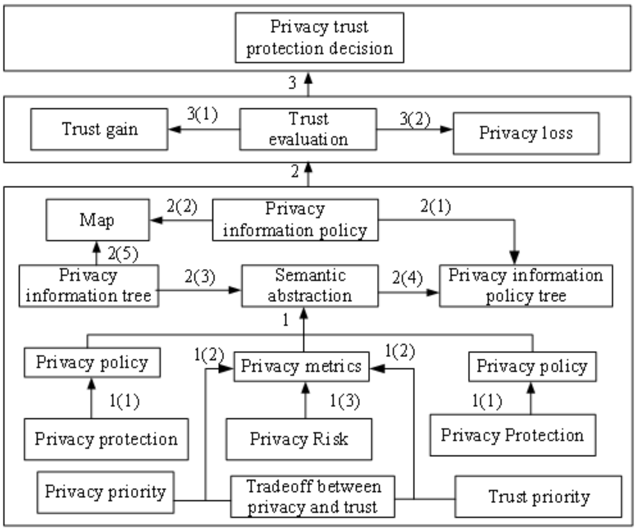


FIGURE 1. The overall framework of the main research content.

A. SERVICE QUANTIFICATION MODEL

1) Definition1: The set $User = \{u_1, u_2, \cdots, u_n\}$ of users in the system $u_i = \{uid_i, uattr_{i1}, uattr_{i2}, \cdots uattr_{in}\}$ refers to a u_i subject that can access network services, which is composed of *uid* and a group of attributes *uattr*.

2) Definition 2: Service set $Service = \{s_1, s_2, \cdots, s_n\}$ is provided by the system for users, $s_i = \{sid_i, sattr_{i1}$ $, sattr_{i2}, \cdots, sattr_{in}\}$ is composed of service *sid* and a set of service attribute identifiers *sattr*.

3) Definition 3: attar refers to the characteristic of an entity in a certain aspect. In this model, it includes user attribute *uattr* and service attribute *sattr*.

4) Definition 4: Condition refers that users should meet to obtain the specified authority. It includes time trigger condition, authorization time condition, etc.

5) Definition 5: Assume that $T_u(uattr, t)$ represents the trust evaluation of user *u*, we can get the formula (1):

$$T_u(uattr, t) = \sum_{i=1}^{n} \omega_i Y_i \tag{1}$$

Y_i is the value of *ith* attribute, ω_i is the attribute weight, t is the time stamp.

6) Definition 6 (Quantify Service Trust): Suppose that $T_s(sattr, condition)$ represents the evaluation of the access control system's trust to the quantitative service s, which is called the service trust degree,

$$T_s(sattr, condition) = \sum_{i=1}^{n} \lambda_i QoS(s_i) \tag{2}$$

where $sattr_i$ is the service attribute set, $QoS(s_i)$ is the value of service s_i, λ_i is the importance of the service s_i, *condition* is the trigger condition. Service trust is the result of attribute calculation and the basis of permit allocation.

7) Definition 7 (Total Trust Evaluation): $TG(uattr, sattr, t,$ $condition)$ represents the trust evaluation of user and service, which is the total trust.

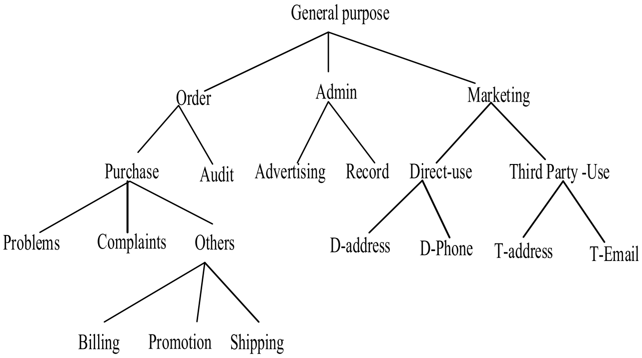


FIGURE 2. Example of purpose tree.

$TG(uattr, sattr, t, condition) = T_u \otimes T_s$ represents the product of the attribute evaluation.

8) Definition 8 (Service Authorization): $S = \{s_1, s_2, \cdots, s_n\}$ can be divided into n units, trust space is recorded as $C = \{c_1, c_2, \cdots, c_m\}, c_i \cap c_j = \emptyset (i \neq j), c_1 < c_2 < \cdots c_m, c_{k+1} > c_k$, besides, C is an ordered partition class, and the function Ψ between user trust and service trust is called trust service authorization. It can be expressed as:

$$\Psi(TG) = \Psi(T_u \otimes T_s) = \begin{cases} s_n, & c_m < T_u \otimes T_s \leq 1 \\ s_{n-1}, & c_{k-1} \leq T_u \otimes T_s < c_k \\ \vdots & \vdots \\ s_2, & c_1 \leq T_u \otimes T_s < c_2 \\ s_1, & 0 \leq T_u \otimes T_s < c_1 \end{cases} \tag{3}$$

When a user requests a service from an access control system, the confidence interval of the service should be determined according to the trust degree $T_u \otimes T_s$.

B. PURPOSE, OBLIGATION AND PRIVACY PROTECTION

In a network system, all the target sets are usually represented by a tree Ω. Each node in the tree Ω is an element of the target set. The edge between two nodes represents the hierarchical relationship among the purpose (Fig. 2).

According to the relationship between the purpose and the object, the purpose can be divided into two categories: the purpose of access and the Intend purpose.

Access purpose: Purpose *AIP* refers to the intention of the access control principal to initiate an access request for resources, which is determined by the access control system.

Intended purpose: the intended purpose refers to the purpose specified when the resource is collected. The intended purpose can be divided into two types: allow and prohibit purpose. The former indicates that the resource provider specifies what the resource can be used, and the latter indicates that the resource provider specifies what the resource cannot be used. For the purpose *IP*, it can be expressed as:

$$IP =< AIP, PIP > AIP, \quad PIP \subseteq \Omega \tag{4}$$

where *AIP* and *PIP* represent the allowable and prohibited purpose sets, respectively, and they are all subsets of the *IP*.

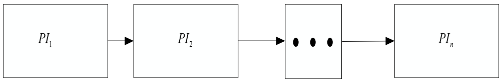


FIGURE 3. Privacy information unit.

According to *AIP* and *PIP* in the destination tree Ω, we can get the compatible destination set *IP*, which is expressed as IP^*. To represent set IP^*, three operators $\uparrow$, $\downarrow$ and $\updownarrow$ are introduced here. For the destination set $\mathbb{Z} \subseteq \Omega$, $\mathbb{Z}^{\uparrow}$ represents the nodes in the $\mathbb{Z}$ and their ancestors, $\mathbb{Z}^{\downarrow}$ represents the nodes in the set $\mathbb{Z}^{\downarrow}$ and their descendants, $\mathbb{Z}^{\updownarrow}$ represents the nodes in the set $\mathbb{Z}$ and their ancestors and descendants, then $\mathbb{Z}^{\updownarrow} = \mathbb{Z}^{\uparrow} \cup \mathbb{Z}^{\downarrow}$:

$$IP^* = \{\mathbb{Z} | \mathbb{Z} \in AIP^{\downarrow}, \mathbb{Z} \notin PIP^{\updownarrow}\} \tag{5}$$

It can also be expressed as $IP^* = AIP^{\downarrow} - PIP^{\updownarrow}$.

Purpose compatibility: gave the expected purpose set *IP*, when the access control system obtains the purpose, it needs to make compatibility judgment. This process is recorded as *compliace_check*(*AIP*, *IP*):

$$compliace\_check(AIP, IP) = \begin{cases} true, & if\ AIP \subseteq IP^* \\ false, & otherwise \end{cases} \tag{6}$$

Here is a specific example of the purpose of compatibility judgment. In the purpose tree (Fig. 2), given $IP =< \{\text{Admin,Direct-Use}\}, \{\text{D-Phone}\} >$, we can get that

$$AIP^{\downarrow} = \{\text{Admin, Advertising, Record, Direct-Use, D-Address, D-Phone}\}$$

$$PIP^{\updownarrow} = \{\text{D-Phone,Direct-Use, Marketing, General Purpose}\}$$

so, $IP^* = \{\text{Admin, Advertising, Record, D-Address}\}$, in this case, the purpose of the access request can be for the elements in the collection IP^*; otherwise, *compliance_check* will return incompatibility.

The obligation also plays an important role in the access control system. All obligations have a corresponding subject, function description, and time baseline, such as $Obligation = \{subject, trigger, action\}$. Once the user's obligations are assigned, they will be tracked and upgraded through the event monitor.

C. PRIVACY INFORMATION AND PRIVACY POLICY TREE

In the current access control system, privacy information usually exists as a whole. In this paper, for a piece of certain privacy information $PI = (PI_1, PI_2, \cdots, PI_i, \cdots, PI_n)$, we can divide the whole information unit into several sub information $PI_1, PI_2, \cdots, PI_i, \cdots, PI_n$ form a chain information flow $PI_1 \rightarrow PI_2 \rightarrow PI_i \rightarrow PI_n$, as shown in Fig 3:

Suppose that $|PI_i|$ is the sensitivity value of privacy information, it has the following properties:

$$|PI_1| \geq |PI_2| \cdots |PI_n| \tag{7}$$

In Fig 4, "Apartment building 69, West, No. 800, Dongchuan Road, Minhang District, Shanghai" can be expressed as

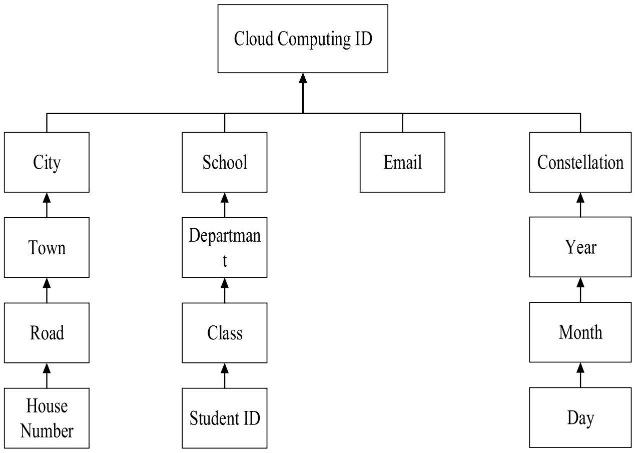


FIGURE 4. Example of privacy information tree Ω_2.

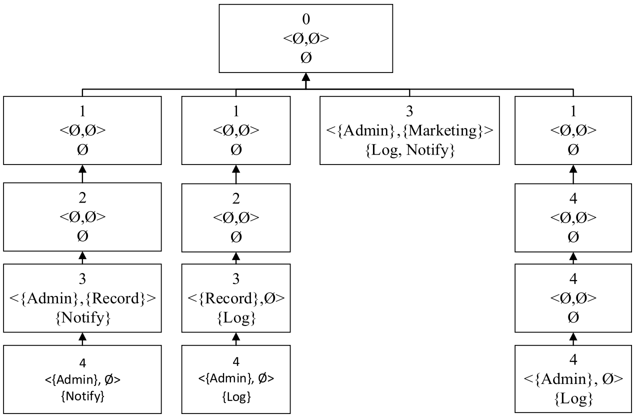


FIGURE 5. Tree example of the privacy policy tree.

"Apartment building 69 → West → No-800 → Dongchuan Road → Minhang District → Shanghai city", the user's privacy information set can be represented as a tree Ω_2, the node-set is represented by IP_2^*.

According to the user's privacy settings for the information unit, we can get the corresponding privacy policy tree Ω_3. The nodes in Ω_3 correspond to the nodes in the Ω_2 one by one. IP_3^* is the node-set of Ω_3, then the mapping relationship is called $Mapping : IP_3^* \to IP_2^*$. For any node $e \in IP_3^*$, it can be expressed as:

$$e = (T_{\min}, IP, OB) \tag{8}$$

Let $\Omega_{2i} = Mapping(e)$, $T_{\min}$ represents the minimum trust level of the node Ω_{2i} in the privacy information tree Ω_2, IP represents the intended purpose of a node Ω_{2i}, OB represents the obligation set IP. The privacy policy tree is shown in Fig 5. From the Figs 4-5, we can see that the policy unit corresponding to the "student number" of the privacy information unit is (4, <Admin,Ø >, {Log}), which means that the minimum trust level of student information is 4, and the access purpose is admin, and the log is required to access the student information, the specific process is in Table 1.

TABLE 1. Algorithm 1.

```
Algorithm 1
Input: $Req, \Omega_2, \Omega_3$
Output: $Result,\ Obligations$
$Result \leftarrow \varnothing, Obligations \leftarrow \varnothing$
$AP \leftarrow Req.AP, S \leftarrow Req.Subject, O \leftarrow Owner(Req.Object)$
for $e$ in $Leaf(\Omega_3)$
  while $e$ is not $\Omega_3.root$
    if $compliace\_check(AP, e.IP)$ is true
      if $Tr(O,S) \geq e.T_{\min}$
        break
      end if
      $e \leftarrow e.parent$
  end while
  $\Omega_{3_i} \leftarrow e$
  while $\Omega_{3_i}$ is not $\Omega_3.root$
    $Obligations \leftarrow Obligations \cup (\Omega_{3_i}.OB)$
    $\Omega_{3_i} \leftarrow \Omega_{3_i}.parent$
  end while
  $\Omega_{2_i} \leftarrow Mapping(e)$
  $X \leftarrow$ null
  while $\Omega_{2_i}$ is not $\Omega_2.root$
    $X.insert(\Omega_{2_i}.info)$
    $\Omega_{2_i} \leftarrow \Omega_{2_i}.parent$
  end while
  $Result \leftarrow Result \cup \{X\}$
end for
```

IV. TRUST EVALUATION

Trust is affected by multi-attribute. The attribute weight is very important to the accuracy of evaluation. This paper uses a comprehensive weight method to overcome the randomness of the subjective method.

A. SERVICE TRUST

If there are n services and each service has m attributes $QoS = \{q_1, q_2, \cdots, q_m\}$. q_{ij} represents the ith service and jth attri-bute, we can get the following expression:

$$QoS = \begin{bmatrix} q_{11} & q_{12} & \cdots & q_{12} \\ q_{21} & q_{22} & \cdots & q_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ q_{n1} & q_{n2} & \cdots & q_{nm} \end{bmatrix} \tag{9}$$

In the attributes matrix QoS, the larger the value of some attributes, the lower the quality of service; the larger the value of some attributes, the higher the quality of service, such as confidentiality, reliability, etc. These values need to be normalized, each element in the QoS can be normalized in formula (10):

$$q'_{ij} = \begin{cases} \dfrac{q_{ij} - q_{\min}}{q_{\max} - q_{\min}}, & q_{\max} - q_{mi}\,n \neq 0 \\ 1, & q_{\max} - q_{\min} = 0 \end{cases} \tag{10}$$

Both $q_{\min}$ and $q_{\max}$ represent the minimum and maximum values of a column in the QoS.

The normalized attribute value is used to calculate the QoS, as shown in formula (11):

$$QoS(s_i) = \frac{1}{m}\sum_{j=1}^{m} q'_{ij} \tag{11}$$

After calculating the comprehensive value QoS of the service and the user's evaluation, the service reputation is calculated as follows:

$$T_s(s_i) = \lambda_i \times QoS(s_i) \tag{12}$$

$T_s(s_i)$ is the trust degree of the service, $QoS(s_i)$ is the comprehensive evaluation value of s_i; q_{ij} is the evaluation value of user u_j for the service s_i, $q_{ij} \in [0, 1]$; $\lambda_i \in [0, 1]$ is the weight value. Calculation of service attributes based on entropy weight is as follows:

$$q_i = -k\sum_{i=1}^{m} p_{ij} \cdot \ln p_{ij}, \quad p_{ij} = q_{ij}\bigg/\sum_{i=1}^{m} q_{ij}, \quad (i \le j \le n), \quad k = 1/\ln m \tag{13}$$

Weight of the jth attribute is

$$\lambda_i = (1-q_i)/\sum_{i=1}^{m}(1-q_i), \quad (1 \le i \le m), \quad 0 \le \lambda_i \le 1, \quad \sum_{i=1}^{m}\lambda_i = 1 \tag{14}$$

B. USER TRUST

Based on the complexity of trust and the related concepts described in the above chapters, we introduce the following trust attribute functions [6], [16].

1) CREDENTIAL TRUST ATTRIBUTE

If there are n services and each service has m attributes $QoS = \{q_1, q_2, \cdots, q_m\}$. q_{ij} represents the ith service and jth attribute, we can get the following expression:

$$Y_1 = \sum_{j=1}^{\mathrm{n}} rc_j/n \tag{15}$$

$RC = \{rc_1, rc_2, \cdots, rc_i, \cdots, rc_n\}$ represents a satisfaction degree, $rc_j \in [0, 1]$ is the satisfaction degree of the jth credential.

2) FEEDBACK TRUST

$$Y_2 = \begin{cases} \dfrac{\sum_{k=1}^{n}(\rho(F_k) \times Y_1(F_k))}{\sum_{k=1}^{n}\rho(F_k)} & n \ne 0 \\ 0 & n = 0 \end{cases} \tag{16}$$

$$\rho(F_k) = \begin{cases} 1 & , \quad level = 0 \\ \prod_{m=0}^{n} Y_1(u_m, u_n) & , \quad 6 \ge level > 0 \end{cases} \tag{17}$$

$\rho(F_k)$ is a trust feedback factor, $\{F_1, F_2, \cdots F_n\}$ is set of feedback node, according to the "Six Degrees of Separation" [25], $6 \ge level \ge 0$ represents the layer of the feedback trust node.

3) OBLIGATION TRUST

$$Y_3 = \frac{\sum_{d\in D} d \times \nu \times GB}{\sum_{d\in D} d \times \nu * GB + \sum_{d\in D} d \times \nu * OB} \tag{18}$$

ν represents the obligation weight; d represents the number of successful obligations; OB represents the number of fail obligations in a certain time; GB represents the number of obligations in a certain time; D is the total number of obligations in the system [6].

4) TRUST RISK

$$RK(s_i) = s_i \times (1 - T_s(s_i)) = \Psi(T_s(s_i)) \times [1 - T_s(s_i)] \tag{19}$$

$$Y_4 = 1 - RK(s_i) \tag{20}$$

s_i represents the quality of service provider. The s_i is greater, the risk is greater. According to formulas (19) and (20), risk and service have an inverse proportional relationship [6].

5) PRIVACY FEEDBACK

$$Y_5|_{Event} = (\sum_{j=1}^{n}|PI'_j|)/(\sum_{i=1}^{m}|PI_i|), \quad m \ge n \tag{21}$$

$PI = (PI_1, PI_2, \ldots PI_m)$ is the privacy interaction information between u_i and u_j, $PI' = (PI'_1, PI'_2, \ldots PI'_n)$ is the disclosure privacy information, $Event$ is expressed as a privacy leak event.
$|PI'| = (|PI'_1|, |PI'_2|, \ldots\ldots |PI'_n|)$ and $|PI| = (|PI_1|, |PI_2|, \ldots\ldots |PI_m|)$ are the value of $PI = (PI_1, PI_2, \ldots PI_m)$ and $PI' = (PI'_1, PI'_2, \ldots PI'_n)$.

6) WEIGHT OF TRUST ATTRIBUTE

$W = (\omega_1, \omega_2, \cdots, \omega_m)$ expresses the eight of the trust attribute [6], [16], [26], we get "Or metric method"

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

and "maximum dispersion degree" $Disp(W) = -\sum_{i=1}^{m}\omega_i \ln \omega_i$, $0 \le Disp(W) \le \ln m$, which satisfies three conditions:

$$\max imize : -\sum_{i=1}^{m}\omega_i \ln \omega_i \tag{22}$$

$$Orness(W) = \alpha, \quad \alpha \in [0, 1] \tag{23}$$

$$\sum_{i=1}^{m}\omega_i = 1, \quad \omega_i \in [0, 1], \; i = 1, 2, \cdots m \tag{24}$$

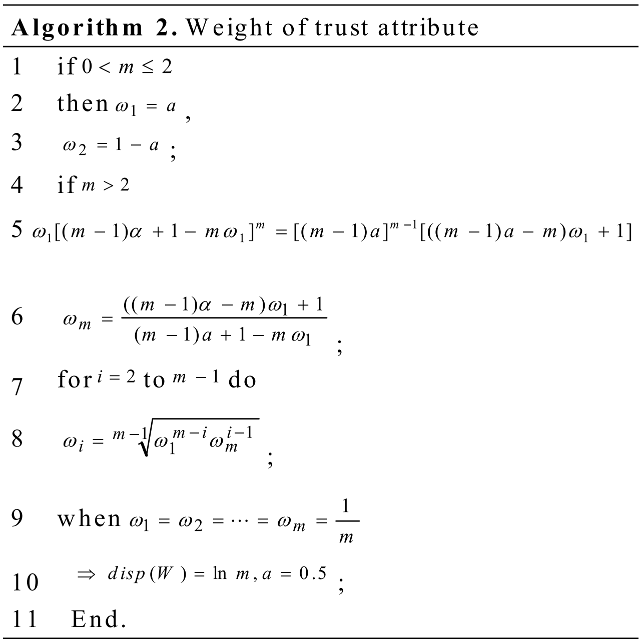
Further, we get formulas (25)-(28):

$$\alpha = Orness(W) = \frac{1}{m-1}\sum_{i=1}^{m}(m-i)\omega_i \tag{25}$$

$$\ln \omega_i = \frac{i-1}{m-1}\ln \omega_m + \frac{m-i}{m-1}\ln \omega_1 \Rightarrow$$

$$\omega_i = \sqrt[m-1]{\omega_1^{m-i}\omega_m^{i-1}} \tag{26}$$

TABLE 2. Algorithm 2.



```
Algorithm 2. Weight of trust attribute
if $0 < m \leq 2$
then $\omega_1 = a$ ,
 $\omega_2 = 1 - a$ ;
if $m > 2$
$\omega_1[(m-1)\alpha + 1 - m\omega_1]^m = [(m-1)a]^{m-1}[((m-1)a - m)\omega_1 + 1]$
 $\omega_m = \frac{((m-1)\alpha - m)\omega_1 + 1}{(m-1)a + 1 - m\omega_1}$ ;
for $i = 2$ to $m - 1$ do
 $\omega_i = \sqrt[m-1]{\omega_1^{m-i}\omega_m^{i-1}}$ ;
when $\omega_1 = \omega_2 = \cdots = \omega_m = \frac{1}{m}$
  $\Rightarrow disp(W) = \ln m, a = 0.5$ ;
 End.
```

$$\omega_1[(m-1)\alpha + 1 - m\omega_1]^m = [(m-1)a]^{m-1}[((m-1)a - m)\omega_1 + 1] \quad (27)$$

$$\omega_m = \frac{((m-1)\alpha - m)\omega_1 + 1}{(m-1)a + 1 - m\omega_1} \quad (28)$$

In Table 2, *m* is a definite value, the key is how to give the value of *a* reasonably.

V. PRIVACY MEASUREMENT ANALYSIS

Whether the data will leak the privacy, how much the impact on availability is the key factor. To make the expression of privacy information, we propose a measurement model.

A. METRIC SPACE

In mathematics, the distance between any elements can be definable in the metric space.

Definition 9. (Metric Space): Suppose that $\Re$ is a non-empty set, for two elements x, y in the $\Re$, $\Phi(x, y)$ represents the distance between two elements, which has two characters: (1) $\Phi(x, y) \geq 0$, $\Phi(x, y) = 0$, and $x = y$; (2) If $z \in \Re$, $\Phi(x, y) < \Phi(x, z) + \Phi(y, z)$.$\Phi(x, y)$ is the distance between two points x, y. $(\Re, \Phi)$ is called as metric space according to the distance.

According to the definition 9, the following properties can be obtained:

$$\Phi(x, y) = \Phi(y, x), \quad x, y, z \in \Re, \\ \times |\Phi(x, z) - \Phi(y, z)| < \Phi(x, y).$$

Norm is a basic concept in performance analysis, which is often used to measure the length or size of each element in the metric space. Let $n(n_1, n_2, \cdots, n_k)$ be a vector, $A = (a_{i,j})_{m \times n}$ is a matrix:

Vector 1-norm

$$||n||_1 = \sum_{i=1}^{k} |n_i| \quad (29)$$

Vector 2-norm

$$||n||_2 = (\sum_{i=1}^{k} n_i^2)^{\frac{1}{2}} \quad (30)$$

Matrix F-norm

$$||A||_F = (\sum_{i=1}^{m}\sum_{j=1}^{n} a_{i,j}^2)^{\frac{1}{2}} \quad (31)$$

B. PRIVACY QUANTITATIVE MODEL

In this paper, the privacy vector is defined as an index in the measurement space, and its influence size in the privacy value is determined by the relationship among the influential factors. The privacy vector (2-norm) is used to represent the size of the privacy value.

Assume that a piece of privacy information is $PI_i = (\theta_1, \theta_2, \cdots, \theta_i, \cdots, \theta_n)$, θ_i represents the privacy factor related to the user's privacy, then the privacy value $|PI_i|$ of PI_i can be expressed as

$$|PI_i| = \sqrt[2]{(\beta_1\theta_1)^2 + (\beta_2\theta_2)^2 + \cdots (\beta_n\theta_n)^2} \\ = \sqrt[2]{\sum_{i=1}^{n} (\beta_i \times \theta_i)^2}, \quad i = 1, 2, \cdots, n. \quad (32)$$

where β_i is the weight coefficient of the influence factor θ_i.

The correlation coefficient is an objective weight method to eliminate the influence of duplicate information on the comprehensive evaluation results, which have significant theoretical and practical significance. Calculate the correlation coefficient matrix, the original data contains *n* factors, standardize the original data, then the correlation coefficient matrix:

$$R = \begin{bmatrix} r_{11} & r_{12} & \cdots & r_{1n} \\ r_{21} & r_{22} & \cdots & r_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ r_{n1} & r_{n2} & \cdots & r_{nn} \end{bmatrix} \quad (33)$$

After standardization, it can be simplified as:

$$R = (r_{ij})_{nn} \quad (34)$$

Calculate the sum value of $(1 - r_{ij})$ in the *j*th column:

$$\sum(1 - r_{i1}), \quad \sum(1 - r_{i2}), \cdots \sum(1 - r_{ij}) \quad (35)$$

The result of $\sum(1 - r_{ij})$ row vector is larger, the influence in the comprehensive evaluation system is greater, so we should give more weight.

Assume that I_i is the information quantity of *ith* factor, the various results of indicators can be considered by selecting the standard deviation σ_i. The conflict characteristics between the *ith* standard and other standards are measured by

$\sum(1-r_{ij})$, r_{ij} represents the correlation coefficient between the *ith* and the *jth* factors, I_i can be expressed as follows:

$$I_i = \sigma_i \sum_{i=1}^{n} (1 - r_{ij}) \tag{36}$$

The result I_i is larger, the amount of data in the *ith* criterion is larger, and the importance is more. Therefore, the weight β_i of the *ith* factor is as follows:

$$\beta_i = I_i / \sum_{i=1`}^{n} I_i \tag{37}$$

VI. TRADEOFF RELATIONSHIP BETWEEN PRIVACY AND TRUST

The relationship between service providers and consumers is dynamic, it can be divided into three categories: privacy protection priority, trust permit priority, and the tradeoff between privacy and trust.

A. PRIVACY PROTECTION PRIORITY $P-T$ *Policy*1

Disclosing the least privacy information to establish a privacy trust relationship, $(P \succ T)/T$ means privacy protection priority:

$$F(T,P) = f_{P_{\min}}(T,P), \quad (P \succ T)/T \tag{38}$$

The steps of policy selection are as follows:

1) PRIVACY INFORMATION SELECTION

Assuming that the trust of the interactive object is T_0, under this condition, according to the privacy protection policy, the disclosure privacy information is $PI(s) = \{PI_1, PI_2, \cdots PI_r\}$, then the amount of privacy information is as follows:

$$|PI1| = \sum_{i=1}^{r} |PI_i| \tag{39}$$

To realize interaction, an entity needs to disclose $|PI2|(|PI2| \leq |PI1|)$, calculate the amount of privacy information of each element in set $PI(s) = \{PI_1, PI_2, \cdots PI_r\}$ respectively, and the result is $\{|\mathrm{PI}_1|, |\mathrm{PI}_2|, \cdots |\mathrm{PI}_r|\}$, select the privacy information from set $PI(s)$.

2) POLICY SOLUTION

In essence, the choice problem of disclosing privacy information is to solve the optimal problem Q_1, the objective function is the minimum value of $|PI3|$, and the solution is the vector $b = [b_1, b_2, \cdots b_r]$.

$$Q_1, \begin{cases} Min\, |PI3| = b_1 \times |PI_1| + b_2 \times |PI_2| + \cdots b_r \times |PI_r| \\ st, \quad |PI3| \leq |PI2| \end{cases} \tag{40}$$

The element $b_i (i \in [1, r])$ in the solution vector $b = [b_1, b_2, \cdots b_r]$ is the Boolean value of the *ith* element in the set $PI(s) = \{PI_1, PI_2, \cdots PI_r\}$, and the disclosure privacy information is $\{|PI_1|, |PI_2|, \cdots |PI_r|\}$.

B. TRUST PERMISSION PRIORITY $P-T$ *Policy*2

Selective private information for maximum trust permission $(T \succ P)/P$ represents permission priority:

$$F(T,P) = f_{T_{\max}}(T,P), \quad (T \succ P)/P \tag{41}$$

The steps of policy selection are as follows:

1) TRUST VALUE EVALUATION

Suppose that the trust is T_0, according to the privacy protection policy, the privacy information disclosed is set $PI(s) = \{PI_1, PI_2, \cdots PI_r\}$, the sum of the privacy information set $PI(s)$ is $|PI1|$.

2) PRIVACY INFORMATION SELECTION

To realize the interaction, the amount of disclosure privacy information is $|PI2|(|PI2| \leq |PI1|)$, and the trust value of $PI(s)$ is $\{T_1, \mathrm{T}_2, \cdots \mathrm{T_r}\}$.

3) POLICY SOLUTION

The choice problem of disclosing privacy information to obtain maximum trust is to solve the optimization problem Q_2, the function is the maximum value of $|PI3|$, and the solution is a vector $b = [b_1, b_2, \cdots b_r]$:

$$Q_2, \begin{cases} Max\, |PI3| = b_1 \times T_1 + b_2 \times T_2 + \cdots b_r \times T_r \\ st, \quad |PI3| \leq |PI2| \end{cases} \tag{42}$$

The element $b_i(i \in [1, r])$ is the Boolean value of the *ith* element in the set $PI(s)$, and the corresponding trust amount of each element in the set $PI(s)$ is $\{T_1, T_2, \cdots T_r\}$.

C. BALANCE PRIVACY AND TRUST $P-T$ *Policy*3

The policy aims to balance between privacy and trust, and satisfies the relationship between the formula (38) and the formula (41). The essence of the policy is as follows:

$$F(T,P) = \phi \bullet f_{P_{\min}}(T,P) + \psi \bullet f_{t_{\max}}(T,P), \quad (\phi + \psi = 1) \tag{43}$$

The steps of policy selection are as follows:

1) PRIVACY INFORMATION SELECTION

To achieve interaction, the amount of privacy information that entities need to disclose is $|PI2|(|PI2| \leq |PI1|)$, both privacy loss and trust gain of $PI(s)$ are $\{|PI_1|, |PI_2|, \cdots |PI_r|\}$ and $\{T_1, T_2, \cdots T_r\}$ respectively, and privacy information is selected from $PI(s)$.

2) PRIVACY LOSS EVALUATION

Assuming that the privacy information requested by the object is the $PI(s)$, the user will call the formula (32), and the amount of privacy loss is $\{|PI_1|, |PI_2|, \cdots |PI_r|\}$.

3) TRUST VALUE EVALUATION

The sum of the privacy information of the $PI(s)$ is $|PI1|$, and the trust evaluation method is called to calculate the $\{T_1, T_2, \cdots T_r\}$ in the $PI(s) = \{PI_1, PI_2, \cdots PI_r\}$.

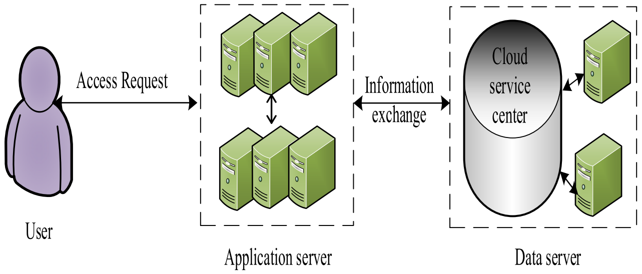


FIGURE 6. Architecture of our experiment.

TABLE 3. Data record of address information.

address_ID	value	access_level
1000	800 Dongchuan Road, Minhang District, Shanghai	1

4) POLICY SOLUTION

The essence of privacy information disclosure selection is to solve the optimal problem Q_3, which balances privacy protection and trust permission, the function is the $|PI3|$, the vector is $b = [b_1, b_2, \cdots b_r]$.

$$Q_3,\begin{cases}|PI3| = b_1 \times (\phi|PI_1| + \psi T_1) + b_2 \times (\phi|PI_2| + \psi T_2)\\ \qquad\qquad + \cdots b_r(\phi|PI_r| + \psi T_r)\\ \phi + \psi = 1\end{cases} \tag{44}$$

The element $b_i(i \in [1, r])$ is the Boolean value of the *ith* element, both ϕ and ψ can be selected by specific application.

VII. EXPERIMENT ANALYSIS

To verify the feasibility of the privacy protection in this paper, our model is implemented in this experiment part. The parameters: Intel Core i5-3230m 2.6GHz processor, 8.0GB memory, 64-bit Windows 10, MySQL server 5.6.

A. SYSTEM IMPLEMENT

In this experiment (Fig.6), the application server deals with the business logic, the database is responsible for queries by the application server.

In the paper, we propose to refine the access control models of trust level and role into 'SimpleAC' [1], [6], [20], which use " access_level represents the privacy settings for address information, as shown in Table 3. For example, three access_level values (0,1,2) are used to represent three privacy settings based on relationship type: "friend visible", "classmate visible" and "relative visible", or three privacy settings based on relationship distance and proximity (0,1,2) are used to represent person visible, friend visible and only self visible.

Further, when user B requests the address information of user A from the application server, the application server will send a query request to the address table in the database server. If the identity of user B meets the requirements of the access level field set by user A, the application server will return the value to user B, otherwise, it will return the empty result or error information.

In Table 4, both item_ID and address_ID are important keys, the number level is the level of the information unit in the privacy information tree, the policy is the privacy and setting $e = (T_{\min}, IP, Ob)$ corresponding to the information unit, the value is the content of the information unit.

When user B requests the address information of user A, the application server will send a query request to the database server, and use the address "ID" field to find the corresponding address information unit, and read it row by row according to the tree "level from low to high".

1) PRIVACY RISK ANALYSIS

To compare the privacy security of "SimpleAC" and our model, there are the following hypothesis.

Hypothesis 1: For each access decision, the system returns the permission with probability pr and the rejection with probability $1 - pr, 0 \leq pr \leq 1/2$.

Hypothesis 2: For privacy information $PI_1, PI_2 \cdots PI_n$, when the system returns the $PI_1 \cdots PI_i$, the privacy risk is i/n, $0 \leq i \leq n$.

Assume that the privacy risks of "SimpleAC" and our model are $PR_1$and PR_2 respectively [1]. Because the "SimpleAC" regards privacy information as a whole, the requester will see the information with probability pr, privacy risk is as follows:

$$PR_1 = pr \cdot 1 + (1 - pr) \cdot 0 = pr \tag{45}$$

In our proposed model, the privacy information is divided into n units, the result probability of $PI_1, PI_2 \cdots PI_n$ is pr^i, the privacy risk of the system can be expressed as follows:

$$PR_2 = pr \cdot \frac{1}{n} + pr^2 \cdot \frac{2}{n} + \cdots + pr^n \cdot 1 = \frac{1}{n}\sum_{i=1}^{n} ipr^i \tag{46}$$

$PR = PR_1 - PR_2$ represents the difference of privacy risk between the "SimpleAC"and our model. We get the change of PR in the cases of $pr = 0.5$ and $pr = 0.4$, as shown in Fig7.

In Fig 7(a), our model has a lower risk than 'SimpleAC', the difference will be more obvious when the number of the information unit is more. In Fig 7(b), we get PR of the probability pr in the case of $n = 3$ and $n = 5$. The difference of privacy risk between the two models increases and then decreases with the change of probability pr, which indicates that probability pr increases to a certain extent, it will affect privacy security.

2) PERFORMANCE ANALYSIS

If the user has n kinds of privacy information, according to the processing of "visible" and "invisible", there are $\prod_{i=1}^{n}(PT_i + 1)$ kinds of possible results, then our system can return 2^n kinds of results, PT_i refers to the number of *ith* information split into subunit. Obviously, $PT_i \geq 1$, then

TABLE 4. Data records in addressitem.

item_ID	address_ID	tree_level	policy	value
1001	1000	1	1,<null,null>,null	Shang hai
1002	1000	2	2,<null,null>,null	Min hang
1003	1000	3	3,<admin,record>,{notify}	Dong chuan
1004	1000	4	4,<admin,null>,{notify}	800

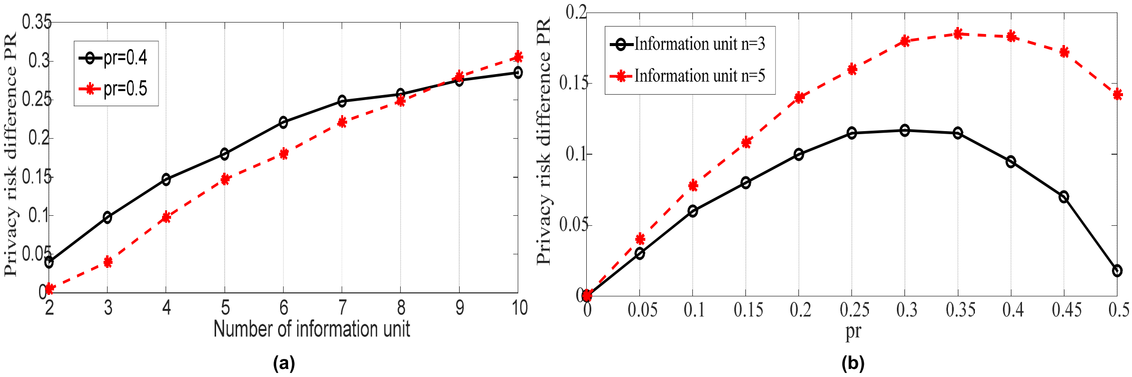


FIGURE 7. Privacy risk difference, (a) in the cases of $p_r = 0.5$ and $p_r = 0.4$ (b) in the case of $n = 3$ and $n = 5$.

TABLE 5. Attributes of QWS.

Attribute	Value
Cost	(0,2000)
Response time(ms)	(0,400)
Reputation	(1,10)
Success rate	(0,100)
Reliability	(0,100)
Location	{shanghai Beijing London}
Privacy	{visible to anyone, visible to the network, not visible}
Number of concurrent	(0,1000)
Availability	(0,100)

$\prod_{i=1}^{n}(PT_i + 1) \geq 2^n$, our system has a finer granularity. Because of the finer granularity of our model, privacy information is no longer the "visible" and "invisible". As long as users can set up reasonable policies in the privacy information tree, there will be no risk of privacy disclosure.

B. PERFORMANCE METRICS ANALYSIS

In this section, we design several experiments to compare with the other two methods, Kirsten *et al.* [5] (The penalty for privacy violations: How privacy violations impact trust online), Xu and Chun *et al.* [17] (Trust-Based Collaborative Privacy Management in Online Social Networks). The dataset is on the http://www.uoguelph.ca/qmahmoud/qws/, (Table 5).

We design experiments of privacy loss and trust value under three different environments: privacy protection ($\phi = 1, \psi = 0$) or trust permission ($\phi = 0, \psi = 1$), the tradeoff between privacy and trust ($0 < \phi, \psi < 1$), these specific parameters are as follows:

(1) The disclosure of privacy information requires more than one kind of trust certificates;

(2) There are 9 kinds of privacy attributes, and the categories of public privacy information are randomly generated;

(3) We randomly generate the service 50 times to calculate the mean value.

1) PRIVACY RISK ANALYSIS

In Figs 8-10, the horizontal axis represents the number of privacy categories, the vertical axis represents the measurement results.

In Fig 8 (a) and (b), under the trust permission priority, as the experimental process progresses, the privacy loss of our model is 0.376 and 0.624 less than [17] and [5], respectively, and the trust value of our model is 0.135 and 0.324 more than [17] and [5], respectively.

In Fig 9 (a) and (b), under the trust permission priority, as the experimental process progresses, the privacy loss of our model is 1.645 and 0.623 less than [17] and [5], respectively, and the 9trust value of our model is 1.042 and 1.352 more than [5] and [17], respectively.

In Fig 10 (a) and (b), under the tradeoff between privacy and trust ($\phi = 0.3, \psi = 0.7$), as the experimental process progresses, the privacy loss of our model is 1.645 and 1.726 less than [17] and [5], respectively, and the trust value of our model is 0.615 and 0.765 more than [5] and [17], respectively.

In Fig 10 (c) and (d), under the tradeoff between privacy and trust ($\phi = \psi = 0.5$), as the experimental process progresses, the privacy loss of our model is 0.686 and

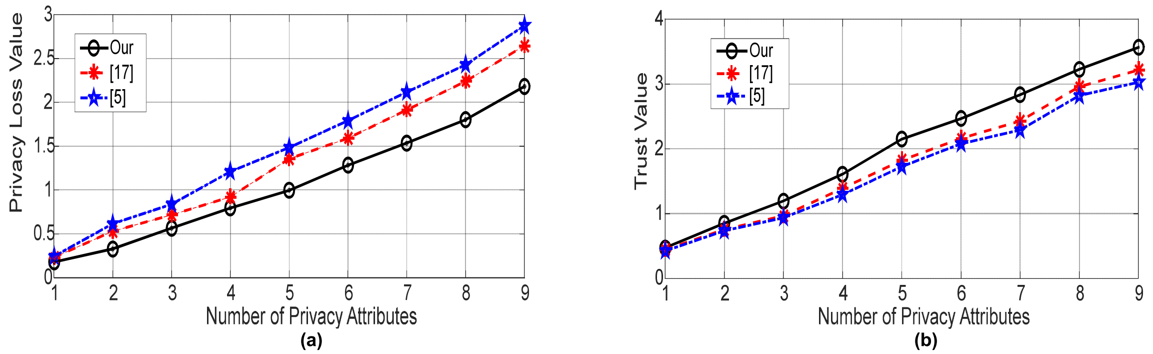


FIGURE 8. Experimental comparison under the privacy protection priority, (a) Privacy loss, (b) Trust value.

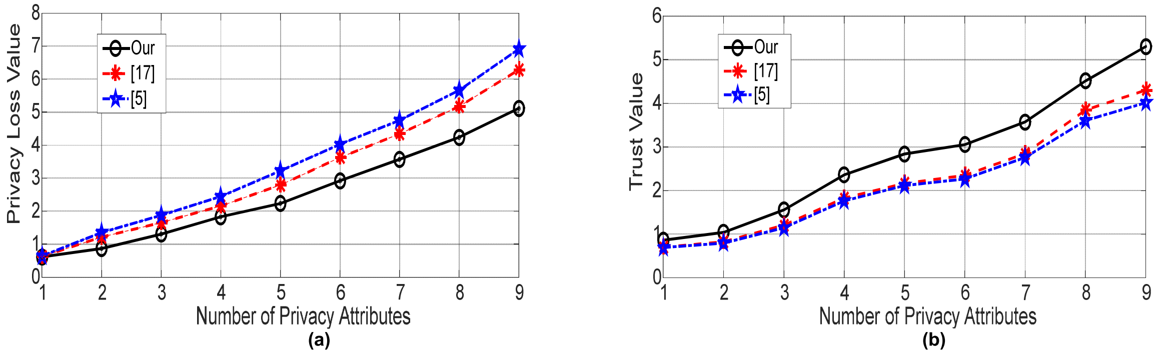


FIGURE 9. Experimental comparison under the trust priority, (a) Privacy loss, (b) Trust value.

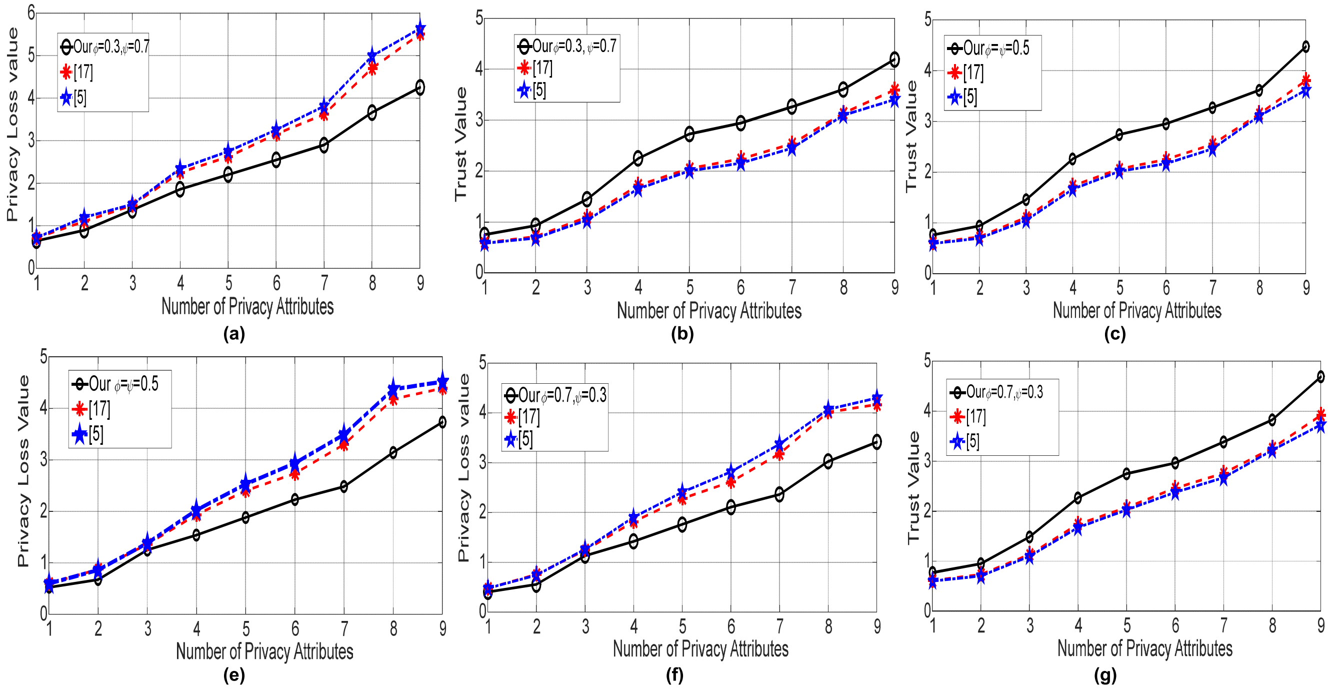


FIGURE 10. Experimental comparison under the tradeoff between privacy and trust, (a) Privacy loss, (b) Trust value; (c) Privacy loss, (d) Trust value, (e) Privacy loss, (f) Trust value.

0.825 less than [17] and [5], respectively, and the trust value of our model is 0.545 and 0.746 more than [5] and [17], respectively.

In Fig 10 (e) and (f), under the tradeoff between privacy and trust ($\phi = 0.7$, $\psi = 0.3$), as the experimental process progresses, the privacy loss of our model is 0.605 and 0.754 less

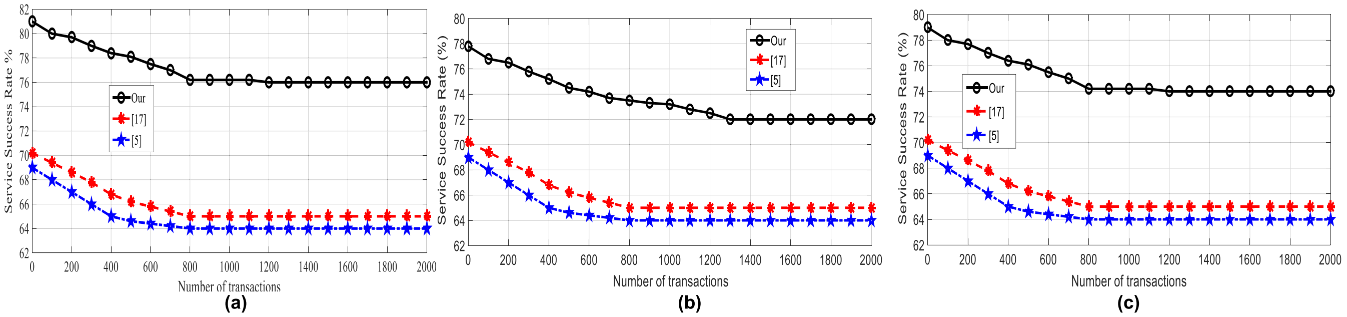


FIGURE 11. Service success rate of three models, (a) Privacy protection priority ($\phi = 1$, $\psi = 0$), (b) Trust permission priority ($\phi = 0$, $\psi = 1$), (c) Tradeoff between privacy and trust ($\phi = \psi = 0.5$).

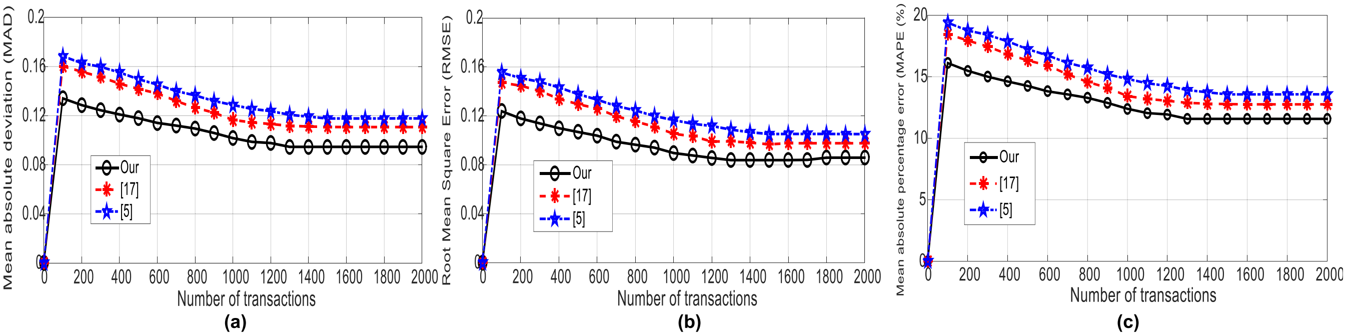


FIGURE 12. Trust accuracy (a) MAD, (b) RMSE, (c) MAPE.

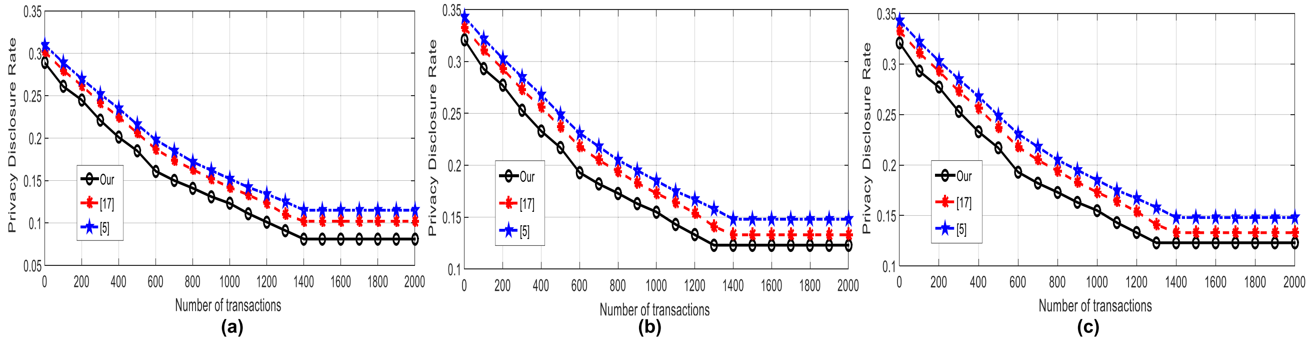


FIGURE 13. Privacy disclosure, (a) privacy protection priority, (b) trust priority, (c) tradeoff between privacy and trust.

than [17] and [5], respectively, and the trust value of our model is 1.005 and 1.225 more than [5] and [17], respectively.

In [5], the relationship between trust and privacy is relatively simple, lacking a dynamic privacy protection mechanism; in [17], there is a lack of impact of trust feedback on privacy disclosure. Our model avoids these shortcomings, integrates the obligation and purpose mechanism and various factors into the privacy and trust model, and establishes a dynamic tradeoff relationship between trust and privacy. With the increasing number of privacy attributes, our model has a better adaptability and has obvious and stable advantages than literature [17] and [5].

2) SERVICE SUCCESS RATE

Continuing with the previous part, we compare the service success rates of the three models. The horizontal axis represents the number of transactions, and the vertical axis represents the service success rate.

In Fig 11 (a), the service success rate is relatively low under the privacy protection priority; in Fig 11 (b), the service success rate is relatively high under the priority of trust authority; in Fig 11 (c), the service success rate is relatively moderate under the trade-off relationship between privacy and trust. In a comprehensive comparison, the service success rate of our model is stable at about 74%, and the selection of parameters ϕ and ψ has about 3% influence on service success rate.

In [5], trust evaluation is affected by privacy deviation penalty, due to the lack of trust feedback to correct privacy, privacy protection is relatively weak. In [17], the relationship between privacy loss and trust value is relatively fixed and simple. We propose a trust and privacy evaluation model, establish a tradeoff relationship and dynamically choose trust permission or privacy protection, so our model is better than [17] and [5].

C. ACCURACY COMPARISON OF TRUST EVALUATION

It is to necessary further study the trust accuracy of this paper, in the next experiments, we introduced synthetic 50K data [16], each data contains 1000 attributes, and the attribute value is in [0, 1].

Suppose that A_{t+1} is the true value at $t+1$, TG_{t+1} is the evaluation value. e_t is the error at the time t, $e_t = TG_{t+1}, -A_{t+1}$, n is the amount of service transaction times. We introduce three performance indices: mean absolute deviation (MAD), root mean square error (RMSE), and mean absolute percentage error (MAPE) to measure the accuracy of trust evaluation.

MAD is expressed as the formula (47):

$$MAD = \frac{\sum_{t=1}^{n} |TG_t - A_t|}{n} = \frac{\sum_{t=1}^{n} |e_t|}{n} \tag{47}$$

RMSE is expressed as the formula (48):

$$RMSE = \sqrt{\frac{\sum\limits_{t=1}^{n} (TG_t - A_t)^2}{N}} \tag{48}$$

MAPE is expressed as the formula (49):

$$MAPE = \frac{1}{n} \sum_{t=1}^{n} |\frac{\mathrm{e_t}}{\mathrm{A_t}}|(\times 100\%) \tag{49}$$

In Fig 12(a), with the gradual advancement of the number of transactions, the MAD of our model, [17], and [5] are finally stable at 0.0928,0.1009 and 0.1145, respectively.

In Fig 12(b), with the gradual advancement of the number of transactions, the RMSE of our model, [17], and [5] are finally stable at 0.0865, 0.1001 and 0.1135, respectively.

In Fig 12(c), with the gradual advancement of the number of transactions, the MAPE of our model, [17], and [5] are finally stable at 11.21%, 12.71%, 13.05%, respectively.

Our model adopts the mechanism of privacy trust feedback, purpose, and obligation, the relevant weight factors are relatively objective and accurate, both [17] and [5] lack similar mechanisms. So our model is better than [17] and [5] in the trust evaluation accuracy.

D. PRIVACY PERFORMANCE COMPARISON

Based on the above synthetic data set, suppose that the user's trust level is lower than the threshold of *ith* access, this is a privacy disclosure event Ed_i, the privacy disclosure rate ca n be expressed as follows:

$$privacy\ \ disclosure\ \ rate = \sum_{i=1}^{n} Ed_i/rq \tag{50}$$

rq expresses all possible transactions, and n is the number of possible privacy disclosure times.

In Fig 13(a), under the privacy protection priority, as the experimental process progresses, the privacy disclosure rate of our model, both [17] and [5] are finally stable at 0.0628, 0.1045 and 0.1209, respectively.

In Fig13(b), under the trust permit priority, as the experimental process progresses, the privacy disclosure rate of our model, both [17] and [5] are finally stable at 0.1228, 0.1345 and 0.1519, respectively.

In Fig 13(c), under the tradeoff between privacy and trust, as the experimental process progresses, the privacy disclosure rate of our model, both [17] and [5] are finally stable at 0.1128, 0.1245 and 0.1369, respectively.

In literature [17], the trust privacy relationship model lacks the dynamic feedback adjustment mechanism, so it can not protect privacy well. In literature [5], weight of privacy attribute lacks objective quantitative formula, which seriously affects the privacy protection. Our model establishes a privacy information policy tree, which can also perceive and filter potentially unsafe hidden danger through trust privacy feedback and risk obligation factors. Therefore, our model is better than [17] and [5] in terms of privacy disclosure.

VIII. CONCLUSION

In cloud services, participants often face the dilemma of service utility and privacy protection [27]. We establish a dynamic adaptive access control model based on trust permission and privacy protection. Firstly, we add the concept of obligation and purpose into access control, propose the privacy information tree and privacy policy tree; second, establish a new trust evaluation model, and give the weight algorithm; third, we quantify the privacy with the norm space and construct a tradeoff relationship model between trust permission and privacy protection, each participant can select the corresponding parameters according to the actual requirement. Finally, the experimental results show the feasibility and effectiveness of our research and reflect the advantages than the other two models.

There are still some shortcomings in this paper, such as personal requirement is still a problem in cloud privacy protection. In the future, we will need to further improve our approach and provide a mandatory mechanism to protect the privacy of each participant.

REFERENCES

[1] *Security Guidance for Critical Areas of Focus in Cloud Computing V4.0*, Cloud Secur. Alliance, Seattle, WA, USA, 2017.

[2] B. K. Mohanta, D. Jena, S. S. Panda, and S. Sobhanayak, "Blockchain technology: A survey on applications and security privacy challenges," *Internet Things*, vol. 8, Sep. 2019, Art. no. 100107.

[3] R. Ranchal and B. Bhargava, "Epics: A framework for enforcing security policies in composite Web services," *IEEE Trans. Services Comput.*, vol. 12, no. 3, pp. 12–22, May 2019.

[4] D. Kim, K. Park, Y. Park, and J.-H. Ahn, "Willingness to provide personal information: Perspective of privacy calculus in IoT services," *Comput. Hum. Behav.*, vol. 92, pp. 273–281, Mar. 2019.

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

[6] P. Sun, "Research on cloud computing service based on trust access control," *Int. J. Eng. Bus. Manage.*, vol. 12, pp. 1–13, Jul. 2020.

[7] S. Oukemeni, H. Rifa-Pous, and J. M. M. Puig, "IPAM: Information privacy assessment metric in microblogging online social networks," *IEEE Access*, vol. 7, pp. 114817–114836, 2019.

[8] L. Sankar, S. R. Rajagopalan, and H. V. Poor, "Utility-privacy tradeoffs in databases: An information-theoretic approach," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 6, pp. 838–852, Jun. 2013.

[9] M. H. Afifi, K. Zhou, and J. Ren, "Privacy characterization and quantification in data publishing," *IEEE Trans. Knowl. Data Eng.*, vol. 30, no. 9, pp. 1756–1769, Sep. 2018.

[10] X. Wang, J. He, P. Cheng, and J. Chen, "Privacy preserving collaborative computing: Heterogeneous privacy guarantee and efficient incentive mechanism," *IEEE Trans. Signal Process.*, vol. 67, no. 1, pp. 221–233, Jan. 2019.

[11] A. Padakandla, P. R. Kumar, and W. Szpankowski, "The trade-off between privacy and fidelity via ehrhart theory," *IEEE Trans. Inf. Theory*, vol. 66, no. 4, pp. 2549–2569, Apr. 2020, doi: 10.1109/TIT.2019.2959976.

[12] A. M. Salama, M. Li, L. Lazos, Y. Xiao, and M. Krunz, "Trading privacy for utility in database-assisted dynamic spectrum access," *IEEE Trans. Cognit. Commun. Netw.*, vol. 5, no. 3, pp. 611–624, Sep. 2019.

[13] T. Asikis and E. Pournaras, "Optimization of privacy-utility trade-offs under informational self-determination," *Future Gener. Comput. Syst.*, vol. 109, pp. 488–499, Aug. 2020, doi: 10.1016/j.future.2018.07.018.

[14] B. Rassouli and D. Gunduz, "Optimal utility-privacy trade-off with total variation distance as a privacy measure," *IEEE Trans. Inf. Forensics Security*, vol. 15, pp. 594–603, 2020.

[15] R. H. Khokhar, R. Chen, B. C. M. Fung, and S. M. Lui, "Quantifying the costs and benefits of privacy-preserving health data publishing," *J. Biomed. Informat.*, vol. 50, pp. 107–121, Aug. 2014.

[16] P. J. Sun, "Research on the tradeoff between privacy and trust in cloud computing," *IEEE Access*, vol. 7, pp. 10428–10441, 2019.

[17] L. Xu, C. Jiang, N. He, Z. Han, and A. Benslimane, "Trust-based collaborative privacy management in online social networks," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 1, pp. 48–60, Jan. 2019.

[18] C. Niu and Z. Zheng, "Achieving data truthfulness and privacy preservation in data market," *IEEE Trans. Knowl. Data Eng.*, vol. 31, no. 1, pp. 105–119, Jan. 2019.

[19] T. N. D. Pham and C. K. Yeo, "Adaptive trust and privacy management framework for vehicular networks," *Veh. Commun.*, vol. 13, pp. 1–12, Jul. 2018.

[20] Y. Verginadis, I. Patiniotakis, P. Gouvas, S. Mantzouratos, S. Veloudis, S. T. Schork, L. Seitz, I. Paraskakis, and G. Mentzas, "Context-aware policy enforcement for PaaS-enabled access control," *IEEE Trans. Cloud Comput.*, early access, Jul. 9, 2019, doi: 10.1109/TCC.2019.2927341.

[21] L. Xu, C. Jiang, Y. Qian, J. Li, Y. Zhao, and Y. Ren, "Privacy-accuracy trade-off in differentially-private distributed classification: A game theoretical approach," *IEEE Trans. Big Data*, early access, Nov. 29,2017, doi: 10.1109/TBDATA.2017.2777968.

[22] H. Zhang, Z. Zhou, L. Ye, and X. Du, "Towards privacy preserving publishing of set-valued data on hybrid cloud," *IEEE Trans. Cloud Comput.*, vol. 6, no. 2, pp. 316–329, Apr. 2018.

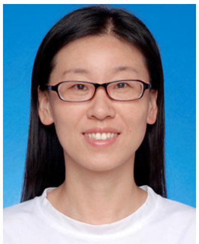
[23] Y. Qiao, Z. Liu, H. Lv, M. Li, Z. Huang, Z. Li, and W. Liu, "An effective data privacy protection algorithm based on differential privacy in edge computing," *IEEE Access*, vol. 7, pp. 136203–136213, 2019.

[24] K. Gai, L. Zhu, M. Qiu, K. Xu, and K.-K.-R. Choo, "Multi-access filtering for privacy-preserving fog computing," *IEEE Trans. Cloud Comput.*, early access, Sep. 19, 2019, doi: 10.1109/TCC.2019.2942293.

[25] C. R. Thornley, L. N. Pham, and J. J. Abbott, "Reconsidering six-degree-of-freedom magnetic actuation across scales," *IEEE Robot. Autom. Lett.*, vol. 4, no. 3, pp. 2325–2332, Jul. 2019.

[26] R. R. Yager, "Weighted maximum entropy OWA aggregation with applications to decision making under risk," *IEEE Trans. Syst., Man, Cybern. A, Syst. Humans*, vol. 39, no. 3, pp. 555–564, May 2009.

[27] P. J. Sun, "Privacy protection and data security in cloud computing: A survey, challenges, and solutions," *IEEE Access*, vol. 7, pp. 147420–147452, 2019.



HUAXIANG HAN received the B.S. degree from Yanshan University, Qinghuangdao, China, in 2006, the M.S. degree from the Taiyuan University of Science and Technology, Taiyuan, China, in 2010, and the Ph.D. degree from Shanghai Jiao Tong University, Shanghai, China, in 2018. She is currently a Teacher with the College of Engineering Science and Technology, Shanghai Ocean University, China. Her current research interests include network control systems, access control, and wireless communication.