International Journal of Multimedia and Ubiquitous Engineering
Vol.10, No.5 (2015), pp.221-230
http://dx.doi.org/10.14257/ijmue.2015.10.5.20

Trust Based Service Optimization Selection for Cloud Computing

Xiaohui Li[1,3], Jingsha He[2] and Ying Du[3]

[1]*Computer Science and Technology, Beijing University of Technology, Beijing 100124, China*
[2]*School of Software Engineering, Beijing University of Technology, Beijing 100124, China*
[1]*lixiaohui@emails.bjut.edu.cn*, [2]*jhe@bjut.edu.cn*
[3] *College of Electrical and Information Engineer, Liaoning University of Technology Jinzhou, Liaoning, 121001, China*

Abstract

We present an approach for privacy preservation in cloud computing environment in which we propose to use information entropy and rough set theory with the goal of personalized privacy protection in cloud users during service selection based on trust. In the approach, cloud server is as an active service provider to personalize the cloud user privacy, cloud user selects the service which is quantified by trust for multi-tenant personalized privacy protection needs. We descript user privacy information by the service and trust attributes, design a multi-attribute service quantization algorithm using information entropy and rough set theory for the quality of service. The approach can achieve the purpose of quantitative service and dynamically adjust the supply relationship service based on multi-attribute, analysis shows which can effectively protect user privacy and personalization by quantifying the cloud service.

Keywords: *cloud computing, trust, privacy protection, Information entropy*

1. Introduction

Cloud computing is a kind of "Everything as a Service" computing model, which provides users with convenient and flexible, highly scalable IT resources. In cloud computing, the users focus the service instead of computing resources. The pattern brings us an unprecedented service experience, and the same time transfer the individual clients' security problems to cloud computing center in the process of using the Internet. Just like that patients offer their living habits and other private information to doctors for the disease, and depositors provide their own identity and financial information to save money in the bank. Users choose a cloud computing center that often needs to transfer the data of managing and protecting to the high credibility, high reliability, security, responsible ISP [1]. Thus, in the service resources extremely large cloud computing environment how to combine the characteristics of cloud computing services and individual service need of users closely, provide a sevice selection approach to meet user-centric, variable, adaptive service demand aggregation and intelligent optimization, the formation of a safe and controlled user demand service domain, is the key to enhance the user experience and application promotion.

In this paper, we propose a quantification service approach based on trust, allowing users to select and use the service combined with their own situation and trust in the cloud computing and dynamically adjust user privacy release granularity to meet the user's personality quantification of privacy. At the same time it can have a clear indication for services' selection and optimization. The main contributions of this paper can be summarized as follows.

ISSN: 1975-0080 IJMUE

(1) In this approach, cloud users as decision makers offer service preference based on their privacy information, and then the preference information is an integrated preferences in accordance with the rules to select the information service as the ultimate standard.
(2) It takes a service quantitative approach allowing users to select and use the service, and combining with their own situation and trust in the cloud computing center to dynamically adjust user privacy release granularity to meet the user's individual privacy needs.
(3) It provides a approach to quantify service through information entropy and rough set theory, which resorts to dependency relationship between privacy and trust to evaluate the service provider .It is suitable for cloud computing environments migration time, environmental changes and the dynamic nature of their own development, which can achieve the goal of personalized privacy.

The rest of the paper is organized as follows. In Section 2, we review some related work on cloud user privacy preservation in cloud computing. In Section 3, we present the detailed description of optimization service approach based on trust, including concepts, design idea, algorithm. In Section 4, we describe the experiment we have performed to evaluate the proposed scheme and show some favorable simulation results. Finally, in Section 5, we conclude this paper in which we also discuss some future work.

2. Related Work

Cloud computing offers a unique service model to bring very exciting user experience also bring its unique security problems, including the contradictory of large-scale service resources provided cloud computing environments and user-controllable personalized service is an important topic. To our knowledge, there is already some mechanism to solve the topic.

Literature [2] proposed an implementation of privacy protection in the cloud with keyword search mode, which supports service providers to participate in part of the work to protect tenants decrypt data privacy and user queries privacy. D. Huang *et al.* [3] proposed a new cloud architecture, and compared to existing cloud services, which not only provides users with the computational complexity of services, while focusing on addressing threats to privacy and security management. In order to provide cloud computing environments privacy protection, Literature [4] designed a computable encryption scheme based on matrix and vector operations, to achieve a variety of data encryption through the use of vector and matrix arithmetic. Literature [5] achieved to protect data privacy through multi-layer encryption in relational databases. Munts discussed the existing privacy protection technologies, including K anonymity, anonymous figure and data preprocessing as the massive data released [6].

Roy proposed a privacy protection system airavat, which integrate the information flow control and differential privacy protection technologies into the cloud data generation and evaluation phase, prevent unauthorized private data leaked during mapreduce calculation process, and support the calculation results to close automatically. In the data storage and use phase, Mowbray proposed a client-based privacy management tool that provides user-centric trust model to help users control their storage and use sensitive information in the cloud [7]. Literature [8] summarized the privacy of research results in the field, and described the basic principles of privacy protection technologies, then pointed out the future direction of privacy protection technologies. Literature [9-11] had effective combination confidential information and data decomposition. They proposed to achieve information decomposition using the concept of privacy constraints, which describe

the data attributes needing to be encrypted and simultaneously back to the privacy of the data leaked. According to these privacy constraint information through the decomposition, to satisfy the requirements of the block pattern, the relationship among each data block stored in the client.

Personalized search refers to search experiences that are tailored specifically to an individual's interests by incorporating information about the individual beyond specific query provided. Access control filter [12] is a preliminary authorization scheme that checks if the current user can perform the requested controller action. The authorization is based on user's name, user IP address and request types. Access Control Lists are filters that enable you to control which routing updates or packets are permitted or denied in or out of a network. They are specifically used by network administrators to filter traffic and to provide extra security for their networks.

In multi-tenant cloud application scenarios, as demand of multi-tenant application processing and tenant data are constantly changing dynamics, these privacy protection approaches cannot completely solve the dynamic and controllability requirements privacy and diversity personalized problems under the cloud. In order to better protect user privacy and to enhance the user experience of cloud services, we propose a trust-based service optimization approach to achieve the secure and controlled user needs.

3. Preliminaries

3.1. Relevant Definitions

Pawlak [13] proposed information system in rough set theory, the concept of information system reflects the dynamic changes in the properties and uncertainty of the system.

R sets [14-17] were introduced simultaneously by Lotfi A. Zadeh and Dieter Klauain 1965 as an extension of the classical notion of set. In classical set theory, the membership of elements in a set is assessed in binary terms according to a bivalent condition — an element either belongs or does not belong to the set. By contrast, fuzzy set theory permits the gradual assessment of the membership of elements in a set[18-20]; this is described with the aid of a membership function valued in the real unit interval [0, 1]. The relevant theory is as follows:

Definition: A rough set is a pair (*A*,*m*) where *A* is a set and m:A[0,1]. For a finite set $A = \{x_1,...,x_n\}$, the fuzzy set (*A*,*m*) is often denoted by $\{m(x_1) / x_1,...,m(x_n) / x_n\}$.Then *x* is called not included in the fuzzy set(*A*,*m*)if m(x) = 0, x is called fully included if m(x) = 1, and x is called a fuzzy member if 0 < m(x) < 1.The set is called the support of (*A*,*m*).

Definition: Information system

Information System: four-tuple

$S = (U, A, V, f)$, where U is non-empty finite set of objects called domain,that is $U = \{x_1, x_2, ...x_m\}$; A is the set of attributes ,that is $A = \{a_1, a_2, ...a_n\}$;*V is* the set of possible attribute values repectively. f is the information function , that is given an object and an attribute maps it to a value ,that is $f: U \times A$. $\forall x \in U, a \in A$, 有 $A = C \bigcup D$.The set of attributes A can be partitioned by two disjoint subsets,the condition attributes C and the decision attributes D.

Definition: rough membership function

Rough membership function is defined as follows: $\mu_X^B(x)$ is a conditional probability When x belongs to the set X that considered with attributes B, we can

get the degree of roughness membership function value from the data calculation directly. That is

$$\mu_X^B(x) = \frac{\left|X \cap I_B(x)\right|}{\left|I_B(x)\right|}$$

3.2 Relevant Definitions

Quantification Service. For a particular information service, It is the cloud server deterministic representation in the cloud computing. We get the value through certain policies in specific contexts (time, space, events) when the cloud user put forward the service requests.

Private Information Sets. U is all the specific information in cloud service, composed of $A_1, A_2, ..., A_n$ among them independent of each other, the initial state A is a collection of the cloud user information, that is $A_1 \cup A_2, ..., A_{n-1} \cup A_n \to U$, x_i refers to the type of cloud service information, $X = \{x_1, x_2, ...x_n\}$ consisting service information collection of cloud users

Service Preferences. Matrix $R = (r_{ax})_{m \times n}$, where $r_{ax} \in [0,1]$ each element of private information set A have a row , each element of the type of information X in the matrix occupies a column, then each element of the matrix can be expressed as $r[a, x]$, the default value of a matrix is 1.

Trust Attribute. In a particular context, the entity determines the behavior of related entities, and response to the result based its judgment to determine the appropriate act.

Annotation: In this cloud computing services in the life cycle of a particular context referred to as service attributes, as the specific context of another main cloud users, there is a dependency relationship between equivalent privacy of its users and service attributes in the service selection process services interdependencies and constraints on the amount of property relations and trust property. We focus on optimizing cloud services users active service.

4. Preliminaries

In the section, we first introduce the approach design ideas and algorithm in detail.

4.1 Design Idea

Trust based service optimization selection approach in the cloud computing triggered by the cloud clients' need, the process as followed:

1) cloud users as decision makers giving service preferences according to their own set of privacy and analyzing various properties of the service, then mapping between privacy information and service
2) To form personalized service information based on the private information to quantify the presence of the service, and make service selection
3) To quantify the presence of the service, and make service selection by interdependencies between service attributes and cloud service users trust attributes

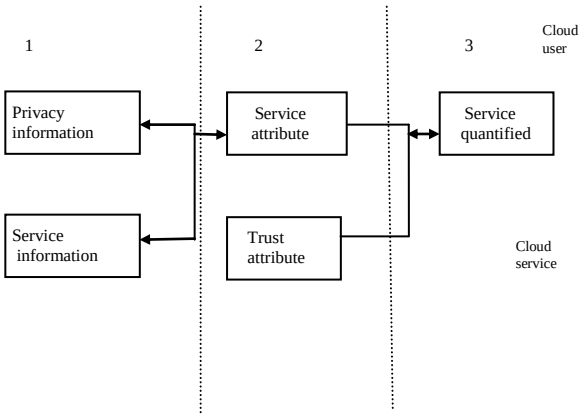

Figure 1. Work Process Description

Description: In this paper, the cloud users as policy makers obtain service preferences based on their own privacy information, the approach refers to role-based access control relevant ideas, specific information, private information collection, information category correspond to users roles and permissions. Privacy Information sets describe the user's private information, each private information set has the appropriate select permissions for information category, categories of information, such as entertainment, news, etc. the specific information provided by cloud computing services belong to categories of information. Privacy information set map to the corresponding categories of information that has the right to choose specific information. Described in Figure 1.

4.2 Algorithm Description

The algorithm consists of the following five steps:

Step1: According to their own set of privacy preferences given service, and then analyze various properties of the service, and the mapping between privacy information and service

This segment process the context information by four steps.

1. Service preference matrix initialization, the default value of 1,privacy information is 0 service preferences is 1, that is the entire service, privacy information is 1 service preferences is 0

2. let A be a finite universe U = {X_1, X_2, ..., X_n}fuzzy sets, U is the collection of all information in the cloud server, A is the collection of cloud user information composed byA_1, A_2, ..., A_n. X is the element of U in the cloud server, that is the composition of our cloud user information service set. Assume cloud users $A_i \in A$ measure $X_i \in X$ obtain a matrix $R = (r_{ax})_{m \times n}$ that service preferences

3. Calculate for each type of information to be selected x_i weight factor w_i , get integrated preference value μ_k^i which means that private information on the type of information service preference value $F = \sum_{i=1}^{n} w_i \mu_k^i$,

4. To get specific information from the comprehensive set of preferences applying rough numbers equivalent mapping relation. Described in Figure 2.

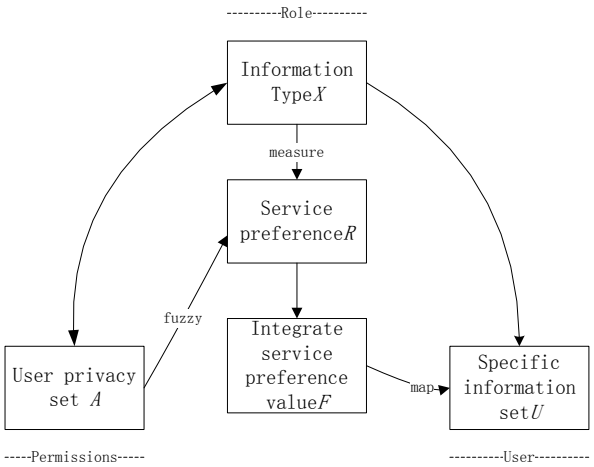

Figure 2. Process Description

Step2: Calculate d_i each attribute C to D for each service object x_i, where $d_i = \mu_{D_i}^{C_i}(e) = \left|X_{C_i} \bigcap D_i\right| \Big/ \left|X_{C_i}\right|$, X_{C_i} is the object set corresponding to the condition attribute C_i as e

Assuming known trust cloud users with the services provided, associated weights formula;

$$b_i = (\prod_{j=1}^{m} a_{ij})^{1/m}, i=1,2,...,m \qquad (1)$$

$$w_j = b_j \Big/ \sum_{k=1}^{m} b_k, j=1,2,...,m \qquad (2)$$

Step3: Comparing each trust attributes of service object D_i to be selected to derive judgment matrix ,and calculate the geometric mean of the line element (by Equation 1);

Step4: Calculate weight coefficient for each service object to be selected in the trust property (by Equation 2)

Step5: Quantify the value of computing services $G = \sum_{i=1}^{n} w_i d_i$, the algorithm ends.

4.3 Simulation Results

To validate the algorithm to quantify the effectiveness of the service, the application of the algorithm is given below.

Assume there are four cloud service providers and one cloud user in a cloud computing environment, cloud user release three kinds of privacy information, gender, age, occupation, then *A={female,38,teacher}*.Types of information *X* are news, sports, entertainment and health. Cloud user prepare three kinds of privacy based information to select the type of information in four specific categories of information, service preferences as shown in Table1.Service attributes including time attribute {0,1,2}, respectively, busy, running, idle, space attribute {} denotes the distant near, local; preference {} means never provided, providing, over; trust property {} is expressed as low, medium and high. Specific information is as follows in Table 2. We can obtain the choice of specific optimization service by the algorithm As shown in Figure 3.

Table 1. Service Preferences

	X1	X2	X3	X4	
A1	0.2	0.1	0.4	0.3	—
A2	0.3	0.1	0.2	0.4	—
A3	0.4	0.3	0.1	0.2	—
—	1	1	1	1	1
—	1	1	1	1	1

Table 2. Specific Information

Service preference	time space			trust	value
x1	2	0	2	2	0.937
x2	1	0	1	0	0.803
x3	1	0	1	1	0.882
x4	0	0	1	0	0.726

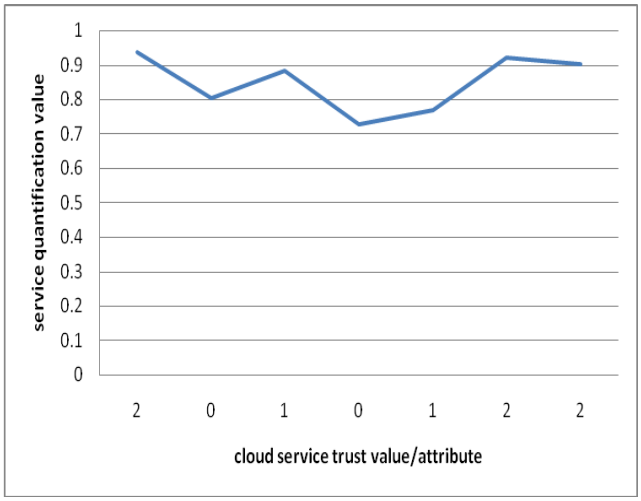

Figure 3. Relationship between the Trust Value and Service

As can be seen from Figure 3, the choice of trust services in our approach has a clear influence, but not as the sole criterion for selection, the service choice is integrated decision problem of various factor, which has close contact with the context of real-time services and the privacy information relevant service properties.

5. Conclusion

In this paper, we presented a service optimization approach for privacy protection in cloud computing in which we quantify service relying on trust through information entropy and rough set theory. We define privacy release as a dynamic and flexible process to choose and use service with cloud users privacy and trust for cloud that offers a new perspective for service selection in cloud computing. In addition, it can meet the users' personalized privacy needs, while quantifying services, possessing a clear indication for the service optimization. Simulation results show that the performance of our approach is obvious and it can help to achieve less privacy loss and more fine-grained during exchange of privacy

information in the cloud computing. And analysis shows that the approach is suitable for cloud computing environments time migration, environmental change and the dynamics of their own development to achieve personalized privacy protection purpose.

Acknowledgments

The work in this paper has been supported by National Natural Science Foundation of China (Grant No.61272500). Beijing Natural Science Foundation (4142008). Pre-launch of Beijing City Government Major Tasks and District Government Emergency Projects (Z131100005613030)

References

[1] D. Li, "Technology of cloud computing development report [M]", Science Press references, Beijing: (**2013).**
[2] Q. Liu, G. Wang and J. Wu, "An Efficient Privacy Preserving Keyword Search Scheme in Cloud Computing", Proceedings of the 2009 International Conference on Computational Science and Engineering, (**2009**), pp. 715-720.
[3] D. Huang, X. Zhang, M. Kang, and J. Luo, "Mobicloud: Building secure cloud framework for mobile computing and communication," in Proceedings of 5th IEEE International Symposium on Service-Oriented System Engineering, (**2010**).
[4] H. Wei and X. Gui, « Cloud environment supports privacy protection computable encryption methods », Journal of Computers, vol. 34, (**2011**), pp. 2391-2402.
[5] E. Wu, S. Madden, Y. Zhang, E. Jones and C. Curino, "Relational Cloud:The Case for a Database Service," (**2010**).
[6] V. Muntes-Mulero and J. Nin, "Privacy and anonymization for very large datasets," in Proceedings of the 18th ACM conference on Information and knowledge management, (**2009**), pp. 2117-2118.
[7] D. Feng, M. Zhang, Y. Zhang and Z. Xu, "Cloud computing Safety Research", Journal of Software, (**2011**).
[8] X. Yang, Y. Wang and B. Wang, "Data released in the privacy of sensitive attributes for multi-Protection methods", Journal of Computers, vol. 31, no. 4, (**2008**), pp. 574-587.
[9] V. Ciriam, S. D. C. di Vimercati, S. Foresti, S. Jajodia, S. Paraboschi, and P. Samarati, "Fragmentation and Encryption to Enforce Privacy in Data Storage", in ESORICS, vol. 4734, (**2007**), pp. 171-186.
[10] V. Ciriani, S. Capitani Di Vimercati, S. Foresti, S. Jajodia, S.Paraboschi, and P. Samarati,"Enforcing Confidentiality Constraints on Sensitive Databases with Lightweight Trusted Clients," in Proceedings of the 23rd Annual IFIP WG 11.3 Working Conference on Data and Applications Security XXIII, (**2009**),pp. 225-239.
[11] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtainingdigital signatures and public-key cryptosystems", Commim. ACM, vol. 21, no. 2, pp. 120-126.
[12] S. Haykin, "Adaptive Filter Theory, Fourth Edition [M]", New Jersey: Pearson Hall, (**2002**).
[13] Z. Pawlak, "Rough sets: Theoretical aspects of reasoning about data [M]", Boston: Kluwer Academic Publishers, (**1991**).
[14] L. A. Zadeh, "Fuzzy sets", Information and Control, vol. 3, pp. 338–353.
[15] S. Gottwald, "An early approach toward graded identity and graded membership in set theory", Fuzzy Sets and Systems, vol. 18, pp. 2369–2379.
[16] H. Bandemer, "Fuzzy Local Inference in Fuzzy Knowledge Bases" in V. Novak, J. Ramik, M. Mares, M. Cerny, J. Nekola (eds.), Fuzzy Approach to Reasoning and Decision-Making, 1990, Bechyne, Czechoslovakia, pp. 47-48.
[17] L, YE X D, "No division and the set of periods for treemaps [J]", Ergod Th& Dynam Sys, 1995, vol. 15, pp. 221- 237.
[18] M. Khambatti, P. Dasgupta and K. D. Ryu, "A role-based trust model for peer-to-peer communities and dynamic coalitions [C]", In: Proc. of the 2nd IEEE Int'l Information Assurance Workshop. Charlotte: IEEE Computer Society, (**2004**), pp. 141−154.
[19] M. Khambatti, P. Dasgupta and KD. Ryu, "A role-based trust model for peer-to-peer communities and dynamic coalitions [C]", In: Proc. of the 2nd IEEE Int'l Information Assurance Workshop. Charlotte: IEEE Computer Society, (**2004**), pp.141−154.
[20] M A. Moharrum and M. Eltoweissy,"A Study of Static Versus Dynamic Keying Schemes in Sensor Networks[C]", Proc. of the 2nd ACM Int'l Workshop on Performance Evaluation of Wireless Ad Hoc, Sensor, and Ubiquitous Networks. New York, USA: ACM Press, (**2005**), pp. 122-126.

Authors

Xiaohui Li, she is currently a Ph.D. candidate in the College of Computer Science and Technology at Beijing University of Technology. Her research interests include network security and trust management. Email: lixiaohui@emails.bjut.edu.cn

Jingsha He, he is currently a professor of the School of Software Engineering at Beijing University of Technology. His research interests include network security and wireless communication technologies. Email: jhe@bjut.edu.cn