International Journal of Smart Home
Vol. 10, No. 11, (2016), pp. 39-50
http://dx.doi.org/10.14257/ijsh.2016.10.11.04

Trust Based Service Selection in Cloud Computing Environment

Xiaohui Li[1], Hongxing Liang[2] and Xing Zhang[1]

[1]*College of Electrical and Information Engineer, Liaoning University of Technology*
Jinzhou, Liaoning, 121001,China
[2]*Jinzhou 65631 Force ,Jinzhou, Liaoning 121001,China*
lixiaohui@emails.bjut.edu.cn

Abstract

In order to meet cloud user demand for managed service, we propose a scheme based on trust for cloud service selection. The scheme includes the service chosen and services delivered two parts, which can choose the cloud service through its trust value, to meet the safety requirements premise, and make trust decisions to achieve service controllability. First it make choice of the service in accordance with service attributes weight using AHP, then complete user data delivery rely on trust, which allowing users to combine with their own situation and trust in cloud services dynamically adjusting the cloud user data release granularity to reach the controllability of the service .Instance results show that the scheme is effective and can guarantee service selection under safe and controlled conditions.

Keywords: *cloud computing; trust; AHP; service selection*

1. Introduction

Cloud computing unique service delivery model brings the user very exciting experience, which also brings its unique security problems. It is an important task issue that is the contradictions between cloud computing environment to provide large-scale services and user controllable resource data protection requirements.The researchers had to solve this problem under the cloud started some research, Literature [1] proposed a keyword search to achieve data in the cloud model, which allows service providers to participate in part of the work to protect tenants decrypt data and the data of user queries. D. Huang [2] 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 solving the data and security threat management. Literature [3] designed to calculate an encryption scheme based on matrix and vector operations to provide cloud computing environments data,to achieve data encryption through the use of a variety of computing vectors and matrices. Literature [4] achieved data protection in the relational database through a multi-layer encryption. Munts [5] discussed the existing data processing technology, including K anonymous, anonymous figure and data preprocessing, as the large-scale release of data problems faced some solutions. Roy focused on information flow control and differential data protection technologies into cloud computing to generate phase data in which propose a data protection system airavat, prevent mapreduce calculation authorized private data leaked out. In the data storage and use phase, Mowbray proposed a client-based data management tool that provides user-centric trust model to help users control their sensitive information is stored and used in the clouds [6]. Literature [7] summarized the data of research results in the field have been on all kinds of basic principles of data protection technology, characteristics are described, pointed out

ISSN: 1975-4094 IJSH
Copyright ⓒ 2016 SERSC

the future direction of the data protection technology. Literature [8-10] combined decomposition with data confidential information effectively, and proposed to use the concept of data constraints to achieve information decomposition, proposed the concept of data constraints, used to describe the need to protect the encrypted data attributes and back simultaneously leaked data data combination of attributes, in accordance with the data constraints, after decomposition block pattern information to meet the requirements, wherein the relationship between each data block stored in the client.

In a multi-tenant cloud scenario, as multi-tenant application processing demand, tenant data is constantly changing dynamic, after the completion of the assessment and quantification of trust, making the service directly from a trusted choice quantized value (*ie.*, fixed or static mapping) can not meet the needs of different cloud users, even for the same user to select service may change with different spatial and temporal factors. Therefore, these data protection schemes can not completely solve the problem of dynamic and controllability requirements of cloud environments.

In order to better protect cloud user data and enhance service applications experience, with the user demand for cloud computing services safe and controlled as a starting point, we propose a trust-based service selection scheme, which includes the service chosen and services delivered in two parts. After the user requests a service cloud discovery, service discovery process result returned is a list of services to be elected, including multiple candidate services. In this case, the service selection function will be executed. Service selection is found to get the list, according to a certain strategy, the process of selecting the appropriate service object. Cloud computing environment in a number of candidate services similar type of service, the use of cloud service user right to attribute different weights determined to elect specific service makes the service in the candidate list of services to the greatest extent possible to meet the individual needs of cloud users . In this paper in order to achieve cloud users controllable services to reconcile the contradictions cloud users and service providers to release information between the service selection process will be devided into service chosen and service delivery the two parts. The following will give specific service chosen and service delivery schemes.

2. Service Chosen Based on Analytic Hierarchy Process

According to a set of attributes for standardized sort ,chosen service is the first step to make service selection. User choice of service in the cloud computing, there is a release of information services and dynamic regulatory requirements, taking into account the efficiency of the service of choice, this excerpt use the analytic hierarchy process for the chosed service.

Services Chosen: given a set of services to be selected for each service, we need a comprehensive evaluation of their service properties, find a cloud service user satisfaction to be selected from the list of services, or services from this group comprehensive sorting, sorting the results need to reflect the individual needs of cloud users.

2.1. Analytic Hierarchy Process

Analytic Hierarchy Process(AHP)is an effective scheme to determine the effective weight coefficient,particularly suitable for those difficult to analyze complex problems obtain quantitative index [11]. It's a complex problem into an ordered layer of various factors interrelated make principled, based on the objective reality of the fuzzy judgment on the relative importance of each level gives a

 Copyright ⓒ 2016 SERSC

quantitative representation, use of mathematical schemes to determine all the elements the relative weights of the order of importance.

Analytic Hierarchy Process steps:

1 An evaluation of the factors determining the objectives and evaluation indexes $u=\{u_1,u_2,\cdots\cdots,u_p\}$.

2 Judgment matrix

Judgment matrix element values reflect the awareness of the relative importance of each element, the general scale of 1-9 and the countdown. Factors of importance when compared with each other can be used when the ratio of meaningful description, determination of the value matrix element corresponding to take this ratio. Obtain judgment matrix $S=(u_{ij})_{p\times p}$.

3 Calculate the judgment matrix

Calculate the matrix S maximum judgment $\lambda_{\max}$ and its corresponding vector A,which is the importance of this feature vector sort of evaluation factors, that is, the distribution of the weights.

The basic steps of AHP shown in Figure 1:

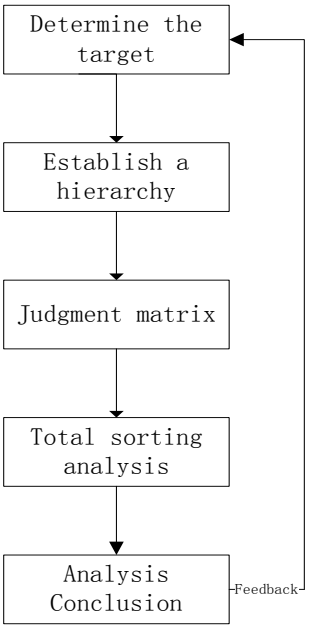

Figure 1. AHP Basic Steps

4. Conformance test

To test the consistency of judgment matrix, consistency index to be calculated $CI=\frac{\lambda_{\max}-n}{n-2}$, the average random consistency index RI. It is a scheme to construct 500 random sample matrix, the constructor is randomly with scale and their reciprocal fill the sample matrix on the triangle, the main diagonal of the value is always 1, the corresponding position of the item transpose the position corresponding to the random number using the above reciprocal. Then calculate the consistency index value for each random sample matrix, the average of these values CI to obtain average random consistency index value $CR=\frac{CI}{RI}<0.10$. When the random consistency ratio, it is considered the results of the analytic hierarchy sort of satisfactory consistency, namely the distribution of the weights is reasonable;

Copyright ⓒ 2016 SERSC

otherwise, to adjust the value of the matrix element of judgment, reassign the value of the weights.

2.2. Scheme Instance

Assuming cloud user wants to choose a cloud service, The candidate S_1, S_2, S_3, , using four categories of time, space, user trust, behavior historical to measure the services satisfaction, the decision analysis shown in Figure 2:

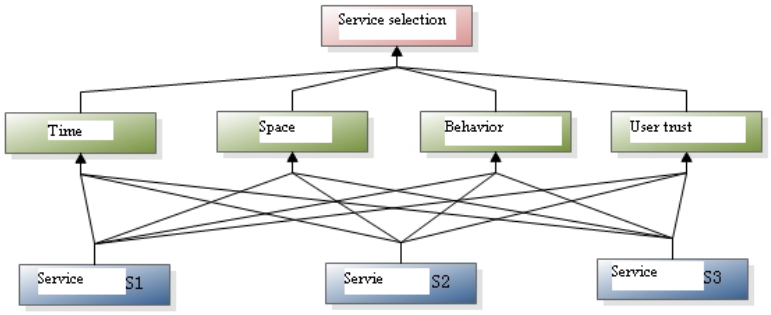

Figure 2. Services Selection Hierarchy Model

Cloud users based on their preferences for services will get four factors pairwise comparison, the judgment matrix as shown in Figure 3.

	1.0000	4.2035	1.0000	1.0000	0.3033
	0.2379	1.0000	0.2085	1.0000	0.1000
	1.0000	4.7965	1.0000	4.2035	0.4488
	1.0000	1.0000	0.2379	1.0000	0.1479

Figure 3. Judgment Matrix

Among the factors listed in the left side of comparators, the factors listed above who are being compared to elements (access to services) listed in the upper left corner of an element on a level that compares the left and top of the element .That is a level (sub-criteria) terms. Diagonal fill 0, that each element not compare with their own. Remaining small box filled figures are positive integers m, on behalf of pairwise comparison of the two sides and score, calculated, consistency ratio of 0.2090, the right to obtain the historical behavior of the service weight of 0.448, the maximum characteristic root λ_{max} is 3.2174;

Each element for each weight factor to obtain the right to the service shown in Figure 4, has a weight of (0.3033,0.1,0.4488,0.1479).

Copyright ⓒ 2016 SERSC

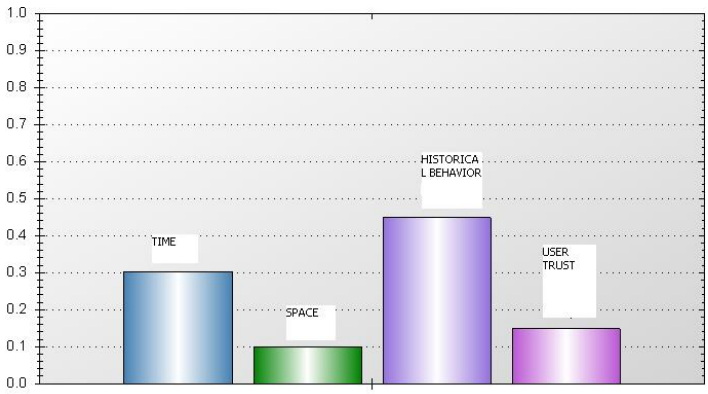

Figure 4. Factor Weight

Similarly Level 3 programs (S_1, S_2, S_3) relative to each factor Level 2 determine the matrix as shown in Figure 5:

1.0000	5.0823	7.9177	0.7337
0.1968	1.0000	4.0823	0.1990
0.1263	0.2450	1.0000	0.0672

Figure 5. Time Factor Judgment Matrix

Time (consistency ratio: 0.1; on the "service access" Weight: 0.3033;: 3.104)

1.0000	5.3059	6.6941	0.7309
0.1885	1.0000	3.3059	0.1899
0.1494	0.3025	1.0000	0.0792

Figure 6. Space Factor Judgment Matrix

Space (consistency ratio: 0.1; on the "service access" Weight: 0.1;: 3.104)

1.0000	5.0000	5.0000	0.6928
0.2000	1.0000	4.0000	0.2199
0.2000	0.2500	1.0000	0.0873

Figure 7. User Trust Factor Judgment Matrix

Users trust value (consistency ratio: 0.209; for "service access" Weight: 0.1479;: 3.104)

1.0000	4.0000	5.0000	0.6567
0.2500	1.0000	5.0000	0.2606
0.2000	0.2000	1.0000	0.0827

Figure 8. Historical Behavior Factor Judgment Matrix

Historical behavior (consistency ratio: 0.209; for "service access" Weight: 0.4488;: 3.2174)

Level 3 to Level 2 of the relative priority matrix:

Copyright ⓒ 2016 SERSC

$$W = \begin{bmatrix} 0.7337 & 0.7309 & 0.6928 & 0.6567 \\ 0.199 & 0.1899 & 0.2199 & 0.2606 \\ 0.0672 & 0.0792 & 0.0873 & 0.0827 \end{bmatrix} . \begin{bmatrix} 0.3033 \\ 0.1 \\ 0.4488 \\ 0.1479 \end{bmatrix} = \begin{bmatrix} 0.6929 \\ 0.2288 \\ 0.0783 \end{bmatrix}$$

The result shown in Figure 9, the preferred order of the service is: S1, S2, S3

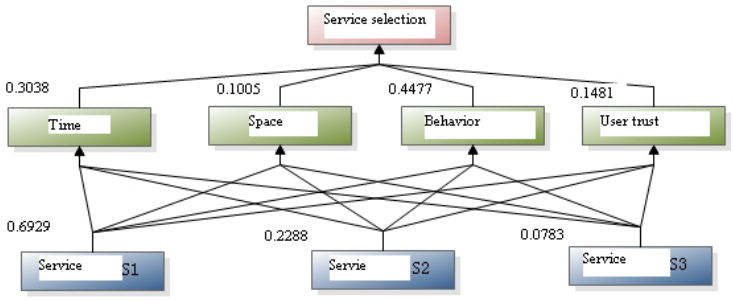

Figure 9. Each Element Weight of the Decision Goal

Through examples, the scheme can make the choice of the service based on service attributes preference of cloud users, and cloud users themselves trust as one of the factors to ensure the security of cloud service provider environments.

3. Trust Based User Data Delivery Scheme

Trust in the cloud computing environment is unequal, after obtaining mutual trust cloud users as decision makers select cloud services, cloud users want control over their own data delivery, from the user data protection (managed services) we will deliver cloud user data described as a dynamic process, allowing users to put trust in cloud-based user data delivery scheme in the selection and use of services, combined with their own situation can dynamically adjust the granularity of user data releases, managed services to meet the needs of users.

3.1. Scheme Design Idea

Cloud user data control based on trust disclosure process described as follows:

(1) cloud users standardized management control over the collection of the data, given a cloud user control over data collection p;

(2) quantify the value of the trust according to the service, if the service is T_i, with the control p, then when the service trust value $T_h \geq T_i$, the service should be able to have control p over the data collection; and if the trust value of the service $T_l < T_i$, service may not have p;

(3) using the data control authority to find a strategy based on trust value can be delivered to the service.

We propose a cloud user data disclosure scheme based on trust, which uses role-based access control related idea: The user belongs to a role that has certain privileges, rights in data delivery process based on trust in the mapping into a cloud service because of a kind of trust that users have some cloud data control. Here the user access control, roles and permissions correspond to cloud services, service trust value, cloud data control user privileges. Assuming quantization interval for cloud users trust $[0,1]$. According to the service level of trust requirements, cloud users

 Copyright ⓒ 2016 SERSC

control over all of its data classification, require the same degree of confidence, merged into the same collection, and ultimately merge to form a control collection n, and according to the requirements of the respective trust Sort; by a cloud of user data to deliver the Step 2 we use the threshold theory [12-13], describing cloud user data control over the trust threshold, and the design data control mapping scheme based on trust threshold, the enactment of Section 3 step trust value search strategy can be delivered to the data control service based. In summary cloud user data delivery scheme trust based designed in Figure 10.

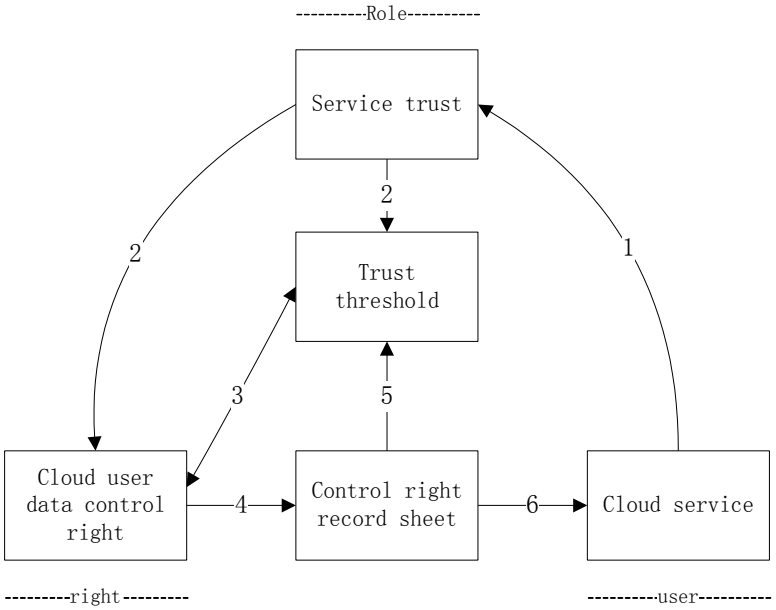

Figure 10. Scheme Design Idea

3.2. Theory and Scheme Steps

Control over the trust threshold: Given a control p, cloud users cloud services based on trust values to determine whether it has the control over the cloud service provider customers after analysis of the historical record, gives the minimum value of the control of the trust requirements ξ, when and only when $T \geq \xi$ the trust services to quantify cloud users control over the data before granting service, ξ known as the cloud user data control p trust threshold.

Authorization logic based trust value of cloud services: before the trust value of cloud services is not available, refused to release control of the cloud user data, that is, control of all data on the cloud user default authorization is refused; corresponding ordered n user control over data determine each data control services required threshold of trust $\xi_0 < \xi_1 < \cdots < \xi_{n-1}$ between the service trust threshold is inherited, that cloud services have the confidence threshold ξ_i is user control over the collection $\{p_0, p_1, \cdots p_{i-1}\}$, the confidence threshold ξ_{i+1} of cloud services also has user data control. A confidence threshold inherited the contents of other one or more trust threshold, we call the former child trust threshold, which the parent trust threshold, child trust threshold inherited his father's trust threshold, parent trust threshold may be more than one, but not mutually exclusive.

Cloud user data delivery record sheet: binding of control and trust between the threshold will be dynamically adjusted according to the number of interactions,

Copyright ⓒ 2016 SERSC

behavioral factors. Adjustment is based on the cloud user data delivery record table, each corresponding to a cloud service provider data delivery record. The list includes: cloud service broker ID, the trust value, the trust threshold, data control, the number of interactions, behavioral feedback. In the user data delivery process, if the same service exists to provide feedback are two acts of bad faith, then increase the control over the trust threshold, update the record and this; if continuous granted control over a certain number of feedback are integrity behavior, reduce the control of the set threshold. Specific adjust the threshold value depends on further service behavior prediction.

Service behavior prediction: provide cloud services based on the behavior of the time series data variation with the passage of time, to predict the behavior of cloud services. Exponential smoothing scheme [14] as a kind of time-series analysis and forecasting scheme to consider the impact of the recent large observation predictive value of this feature, the greater number of more recent observations of its rights. According to exponential smoothing, predict the behavior of cloud services, cloud service providers to predict the behavior of an abstract for a predictive model to observe the behavior of the data cloud services, according to the changing trend, using different exponential smoothing scheme to calculate different smoothing constants spreadsheet selected so that the minimum mean square error of prediction as a smoothing constant, apply predictive models to predict the behavior of the service provider if it is predicted results for the larger good faith authorizes, or refuse authorization.

Related described as follows:

If the time series is no significant change in the cycle, once the value of the exponential smoothing over point in time as the predicted value of the next point, the prediction model of the Formula (3), which is a value of the period of exponential smoothing.

$$S_t^{(1)} = \alpha y_t + (1-\alpha) S_{t-1}^{(1)} \tag{1}$$

$$S_t^{(1)} = \alpha y_t + \alpha(1-\alpha) y_{t-1} + \ldots + (1-\alpha)^t S_0^{(1)} \tag{2}$$

$$\hat{y}_{t+1} = S_t^{(1)} \tag{3}$$

α is as smooth constant ranges (0,1) whose value depends on the trend of time series, follow the following principles:

When a smaller long-term time-series trends, the smaller (0.1, 0.3); when the time series of significant changes in the long-term trend, but close to stabilize, then take (0.3, 0.6); when the time series of the long-term trend is clearly and fluctuations, the take (0.6, 0.9).

Exponential Smoothing scheme to predict the behavior of the service steps: behavioral observation services rendered trend exponential smoothing scheme selection; select the appropriate smoothing constants spreadsheet; service based on historical behavior of the trust value is calculated exponential smoothing initial value; predictive model-based generation back to the observation period, the availability of predictive value, resulting prediction error; prediction variance calculation under various smoothing constant, select the predicted value determined. Examples of this approach are given below: Suppose there is a cloud service provider feedback evaluation three states are: integrity provided with fraudulent intent, fraud, ranging respectively [0.66,1], [0.34,0.66), (0, 0.34). Read the history of the service three times a trust service providers were evaluated (0.68,0.66,0.73).

 Copyright ⓒ 2016 SERSC

Due to changes in the trend of trust evaluation, selection once predicted exponential smoothing. Desirable forma, taking the average of these three initial value of the observed values, namely

$$S_0^{(1)} = \frac{1}{3}(0.68 + 0.66 + 0.73) = 0.69$$

By the Formula (2) calculating a time series observed exponential smoothing values shown in Table 2.

Table 2. Service Trust Evaluation Value and Exponential Smoothing Values

Time series	1	2	3
Trust evaluation value	0.68	0.66	0.73
$S_t^{(1)}(\alpha = 0.2)$	0.688	0.6824	0.69192
$y_t - \hat{y}_t$	−0.01	−0.028	0.0476
$S_t^{(1)}(\alpha = 0.3)$	0.687	0.6789	0.69423
$y_t - \hat{y}_t$	−0.01	−0.027	0.0511

$\alpha = 0.3$

$S_1^{(1)} = 0.3 \times 0.68 + 0.7 \times 0.69 = 0.687$, $S_2^{(1)} = 0.3 \times 0.66 + 0.7 \times 0.687 = 0.6789$

$S_3^{(1)} = 0.3 \times 0.73 + 0.7 \times 0.6789 = 0.69423$;

When $\alpha = 0.2$ Calculate exponential smoothing each time series, prediction model Equation (3) into the time series, calculate the deviation of the actual and predicted values:

$$y_1 - \hat{y}_1 = 0.68 - S_0^1 = 0.68 - 0.69 = -0.01$$

$\alpha = 0.2$ prediction mean variance:

$$\sigma^2 = \frac{1}{3}\sum_{t=1}^{3}(y_t - \hat{y}_t)^2 = 0.00314976$$

$\alpha = 0.3$ prediction mean variance :

$$\sigma^2 = \frac{1}{3}\sum_{t=1}^{3}(y_t - \hat{y}_t)^2 = 0.00344021$$

When $\alpha = 0.2$ prediction mean variance less than $\alpha = 0.3$ we should select the corresponding prediction model to forecast. Therefore, the behavior of cloud services predictive value of 0.69192 is honest provide.

The main steps of the user data delivery scheme trust based:

(1)The cloud user based on the cloud services trust required to carry out all of its control n Categories;

Copyright ⓒ 2016 SERSC

(2) Cloud user gives a minimum trust threshold ξ control over all of the data set, the average distribution of the sorted collection of value difference, then a set of n control sorted trust threshold are: $\xi_0 = \xi$, $\cdots$, $\xi_{n-1} = \xi + \frac{(1-\xi)(n-1)}{n}$;

(3) The value of a given cloud service T lookup trust threshold, get $\xi_{i-1} \le T < \xi_i$, the cloud service has confidence threshold is less ξ_{i-1} control over the cloud user data;

(4) Quantify the value of trust services, data collection and feedback control of behavior, user data is saved to the cloud delivery records in the table;

(5) Set the threshold value adjustment data based on control of the cloud user record table trigger ε_{i-1} update information delivery;

(6) To grant permission for the collection of cloud services $\{r_0, r_1, \cdots r_{i-1}\}$, and service behavior to predict.

In summary we propose a trust based service selection scheme, from the perspective of cloud services, cloud services trust value as a privilege of the collection filter .Through the filter cloud service can obtain the appropriate permissions set of resources . Trust cloud services to certain rules handle their data set queries to get control over resources, including the consolidation of redundant permissions resources to deal with conflict and other operations authorized permission resources. Combined with their own situation and trust in cloud computing center from the cloud user to dynamically adjust the angle of the user releases the user data granularity, and to predict their behavior provide personalized to meet the data protection needs of users and the service controlled .

4. Conclusion

Cloud computing encapsulates network computing resources, storage resources, software, and other resources for the service, the formation of a huge-scale shared virtual "resource pool." For the same or similar services trust resources, select one of the most appropriate services to meet the security conditions under the premise, to demand personalized services controllable, making trust decisions is a key technical issue of trust management,which is the study point of paper. The paper proposes a service selection scheme based on trust, including service chosen and service data delivery in two stages. First Analytic Hierarchy right to be elected in accordance with the weight of the service attributes make the service selection; then complete user data delivery based on trust , allowing users rely on trust in the choice of service, combined with their own situation and trust in cloud services dynamically adjusting the cloud user data release granularity, to the service of the controllability.The results show that the proposed scheme is effective and can guarantee a safe and controlled service options.

Acknowledgments

The work in this paper has been supported by Liaoning Province Outstanding Young Scholars Growth Program (LJQ2014066). Liaoning Province Science and Technology Program (20121045).

References

[1] 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.

 Copyright ⓒ 2016 SERSC

[2] D. Huang, X. Zhang, M. Kang and J. Luo, "Mobicloud: Building secure cloud framework for mobile computing and communication", Proceedings of 5th IEEE International Symposium on Service-Oriented System Engineering, **(2010)**.
[3] H. Wei and G. Xiaolin, "Cloud environment supports encryption schemes to calculate the privacy", Computer Journal, vol. 34, **(2011)** pp. 2391-2402.
[4] E. Wu, S. Madden, Y. Zhang, E Jones and C. Curino, "Relational Cloud: The Case for a Database Service", **(2010)**.
[5] 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.
[6] F. Deng, Z. Min, Z. Yan and X. Zhen, "Cloud computing security research Software", **(2011)**.
[7] Y. Xiaochun, W. Yazhe, W. Bin and I. Ge, "Data released in the privacy of sensitive schemes for multi-attribute", The Computer Journal, vol. 31, no. 4, **(2008)**, pp. 574-587.
[8] 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.
[9] V. Ciriani, S. C. 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.
[10] 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 scheme for obtainingdigital signatures and public-key cryptosystems Commim", ACM, vol. 21, no. 2, pp. 120-126.
[12] R. Klinger and K. Tomanek, "Classical Probabilistic Models and Conditional Random Fields", Algorithm Engineering Report: TR07-2-013, **(2007)**.
[13] Ambrose in. Threshold study [M] autoregression model and threshold cointegration theory and schemes of value. Economic Science Press, **(2011)**.
[14] M. Jaiganesh, M. Aarthi and A. V. A. Kumar, "Fuzzy ART-Based User Behavior Trust in Cloud Computing", Advances in Intelligent Systems & Computing, **(2015)**.

Author

Xiaohui Li, is currently a lecturer of the college of Electrical and Information Engineer at Liaoning University of Technology and a Ph.D. Her research interests include network security and trust management. Email: lixiaohui@emails.bjut.edu.cn.

Copyright ⓒ 2016 SERSC

Copyright ⓒ 2016 SERSC