Trust Model for Distributed Data Sharing in Cloud Computing

Trust for clients

Balaiah Gari Venkat Ranga Reddy
Department of Computer Science and Engineering
Vellore Institute of Technology
Chennai, INDIA

Prassana J
Department of Computer Science and Engineering
Vellore Institute of Technology
Chennai, INDIA

***Abstract*-Now a day's Cloud Computing is the rapid growing technology. It is a new method of delivering the distributed resources over internet on an as-needed basis. It reduces capital and operational expenditure. In the same level to technology, number of cloud service providers of data sharing has increased exponentially in the past few years, providing service with more options for the customers to choose with. Customers are not sure whether they can identify a trustworthy cloud provider only based on their SLA's (Service Level agreements). In this paper a model for Trust Management for sharing data based has been developed, which can help users make an informed choice towards selecting the appropriate cloud service provider as per their requirement. This study presents what the trust is and how trust has been applied in distributed data sharing in cloud computing.**

Keywords: trust; cloud computing; data sharing; attributes; distributed.

I. INTRODUCTION

Cloud computing is giving the resource as a service either a hardware or software over a network. In this the user's data are processed remotely in unknown machines that user don't know where our data is stored and can't be operated. As in this fast growing technology provides many scalable services. It moves user data to the centralized data centers where the fear of losing the control on their data while sharing or lost in any amount of data, so the service provider should be trusted. User's needs to be able to ensure that their data are handled according to the service level agreement which is a contract signed between the customer and the service provider.

Cloud computing presents a new way to supplement the current consumption and delivery model for IT services based on the Internet, by providing dynamically, scalable and often virtualized resources as a service over the Internet. Now a day's most of the persons are accessing the large volumes of data from clouds. In this way they don't provide the security because of the wide adaption of cloud services.

Among the cloud services IaaS (Infrastructure as a service) is highly used in the large enterprises where the physical hardware is virtualized and serves to industrial and personal world. Cloud services are cost saving in real business world, and are successful Instead going to traditional cost in purchasing expensive and generation outdated hardware resources.

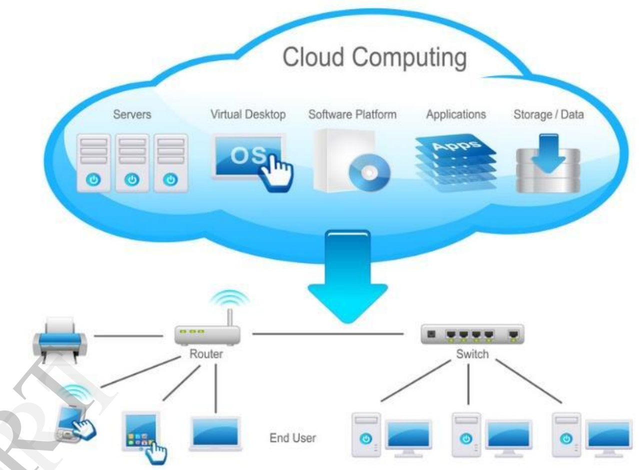

Fig. 1 Overview of the Cloud System

The architectural service layers [8] of cloud computing are:

Software as a Service (SaaS): This service is a Software deployment model whereby a provider licenses an application to customers for use as a service on demand. Examples:

□ Google apps,
□ Salesforce.com,
□ Social Networks.

Platform as a Service (PaaS): Optimized IT and developer tools offered through Platform as a Service (PaaS) for database and testing environments.
Examples:

□ MS-Azure,
□ Operating Systems,
□ Infrastructure Scaling.

Infrastructure as a Service (IaaS): On-demand highly scalable computing, hosting and storage services.
Examples:

□ Mainframes,
□ Storage,
□ Compute.

II. RELEATED WORK

The different type of trust models have been proposed for cloud. Epuru Madhavarao has proposed data sharing in cloud using distributed accountability [15] in which he presents automatic authentication of users and observe the records of the user or data owner. But the provider should be also trustworthy for not losing their data.

Yan and Prehofer proposed an adaptive based trust control model for evaluating and establishing the trust relationships. This model shows about the attributes of the entity and a number of trust control modes supported by the system. In particular his parameters can be adaptively adjusted based on runtime for trust assessment in order to reflect real system context and situation. In this model shows about the attribute-based scheme in which the user records the attribute values with service providers instead of the subjective ratings. The user gets with a service provider captures the difference between the number of requested service and the number of delivered service in terms of service specific attribute values.

III. PROPOSED SYSTEM

Trust Management:

Trust management is an important component on cloud security. From the past few years, many studies have proposed different techniques to address trust management issues. Thus, adding trust mechanism to user-side, as the cloud provider the trustworthiness service for every user request in advance, and should allocate the best resources to the users.

Monitoring the data:

In SLA for the trust attributes it mainly depends on the factors security, reliability and availability. Trusted attributes can be get from monitoring agents who are responsible of getting the evidences of the number of request in distributed data sharing, number of responses, number of illegal connections and the bandwidth of the network etc., computing agents are responsible for the collecting indirect evidences through calculations and statics where we get the average ratio of the monitored values. The trust evaluation is done on the user side as the service data is embedded for them by software agents. There is no need of any request for clients by the server. The above key attributes can be evaluated by the software agents as they can get the denial, success ratios by the time slots of the service to the client cloud, the attributes of the illegal connections through anti-virus software used at clients that can be easily detected and can be evaluated.

Normalization of attributes:

The attribute values is called an evidence. This values are normalized thereby reducing the computational burden of DTEM (Dynamic trust evaluation module).

1. Mean range

As we know the minimum and the maximum values of the attributes can be calculated by

$$x_i = \frac{v_i - min(v_i)}{max(v_i) - min(v_i)}$$

Where v_i is the real attribute value. Thereby calculated values will be range of [0, 1].

2. Statistical normalization

In this statistical normalization where it converts the normal distribution data into the standard normal distribution data in the range mean zero and unit variance.

$$x_i = \frac{v_i - \mu}{\sigma}$$

3. Ordinal normalization

Ordinal normalization is to rank the continuous value of an attribute and then normalize the rank into [0, 1]. Let r be the rank of a given value in an attribute, the ordinal normalization is

$$x_i = \frac{r - 1}{max(r) - 1}$$

.

Here the ordinal normalization attribute values ranges in [0, 1].

4. *Frequency normalization*

In the frequency normalization consider the proportion to the total sum of the attributes which is defined as

$$x_i = \frac{v_i}{\sum_i v_i}$$

Frequency normalization which scales an attribute into [0, 1].

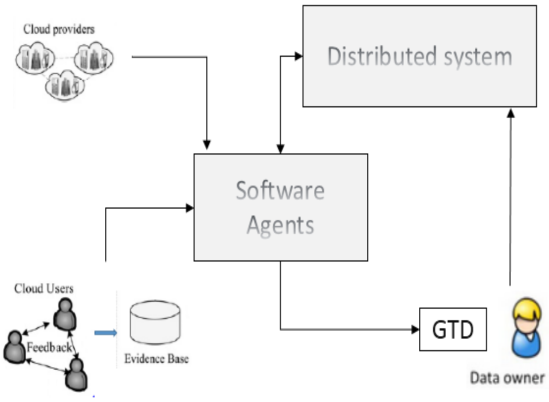

Fig. 2 GTD calculation for Distributed data sharing

Calculation of GTD:

A user of the distributed data sharing in cloud will trust if his past service is best. The service performance is checked over multiple interactions how good it is. Our trust model focuses on forecast the real time GTD of cloud service.

The values of the trust attributes obtained by agents are arranged in a time period Γ, and Γ is a set of time slot units. If a time period is divided by n, then Γ = {1, 2… t…, n}. Let Ω = {N1, N2… Np} denote p services in the cloud, let Tt(Ni) denote the real-time (or short-term) trust degree (RTD) of Ni at time t. We define Tt(Ni) as follows Tt(Ni) = rt×{x1,x2, . . . ,xk , . . .xm}^{T}

Where $x_{k\,\in}$ [0, 1], $\sum_{k=1}^{m\,x\,k}$=1. The normalized evidence vector rt = (rt1, rt2… rtk… rtm… rtk). We say that rt is a sample of RTD measurement, and it is an m-dimensional vector. $x_{k\ is}$ the weight which assigned to this normalized evidence. In the time period Γ, we can obtain a time series G = {T1, T2 . . . Tn}. After the GTD can be calculated by the following formula

$G_n\,(N_i) = G \times A^T$

WhereA={a1,a2…an}

```
Enter into the log on information
if (an SLA is accomplished between the user and the cloud manager)
  then
     The user evaluate the GTD of the selected service provider;
if (the GTD satisfies the requirement)
  then
     The user interacts with the service provider;
     repeat
       The user monitors the interaction, and records monitored data in the evidence;
       According to a fixed period, the user calls the DTEM to update the trustworthiness of the provider with respect to the evidences;
       On the basis of the evaluated result, the user can decide whether to continue service with the provider;
     until (the service is completed.)
  end if
end if
```

Fig. 3 Algorithm 1: Calculation of GTD for evaluating trust.

In GTD the user records their own data and choosing of service provider will be based on the past responses. Here we assume that a user has obtained a list of trustworthy acquaintances. In this process feedback depends on the trustworthy acquaintance list. The GTD computing and updating approach is denoted by

$$G_n(N_i) = \begin{cases} \dfrac{r+1}{r+s+2}, & r+s \neq 0 \\ 0.5, & r+s=0 \end{cases}$$

Where r is the total value of positive ratings (>0.5) toward service Ni, and s is the total value of negative ratings (<0.5) towards service Ni. In (7), if (r + s = 0), this means that Ni is a new joined cloud provider. According to Friedman and Resnick [15], we set Gn (Ni) = 0.5 when (r + s = 0).

IV. CONCLUSION

In paper presents the effective mechanism, in getting the trusted cloud service in distributed data sharing. User can get the embedded cloud trust for his distributed system to select a more trustworthy service provider. Using this attributes trust model they can calculate the exact GTD of the service, that data proves the cloud trust effectively.

V. REFERENCES

[1]. Malik, S.; Khan, S; Srinivasan, S., "Modeling and Analysis of State-of- the-art VM-based Cloud Management Platforms" Cloud Computing, IEEE Transactions on , vol.PP, no.99, pp.1,1, 0

[2]. Sundareswaran, S.; Squicciarini, A.C.; Lin, D "Ensuring Distributed Accountability for Data Sharing in the Cloud"Dependable and Secure Computing, IEEE Transactions on , vol.9, no.4, pp.556,568, July-Aug. 2012

[3]. Mishra, R.; Dash, S.K.; Mishra, D.P.; Tripathy, A.,"A privacy preserving repository for securing data across the cloud," Electronics Computer Technology (ICECT), 2011 3rd International Conference on , vol.5, no., pp.6,10, 8-10 April 2011

[4]. Zhidong Shen; Li Li; Fei Yan Xiaoping Wu, "Cloud Computing System Based on Trusted Computing Platform\" Intelligent Computation Technology and Automation (ICICTA), 2010 International Conference on , vol.1, no., pp.942,945, 11-12 May 2010

[5]. Li-qin Tian; Chuang Lin; Yang Ni, "Evaluation of user behavior trust in cloud computing" Computer Application and System Modeling (ICCASM), 2010 International Conference on , vol.7, no., pp.V7-567,V7-572, 22-24 Oct. 2010

[6]. Hwang, K., Kulkarni, S., Hu, Y.: 'Cloud security with virtualized defense and reputation-based trust management'. Proc. IEEE Int. Conf Dependable, Autonomic, and Secure Computing (DASC 09), 2009

[7]. Hwang, K., Li, D.: 'Trusted cloud computing with secure resources and data coloring', IEEE Internet Comput., 2010, 14, (5), pp. 14–22

[8]. Kim, H., Lee, H., Kim, W., Kim, Y.: 'A trust evaluation model for his QoS guarantee in cloud systems', Int. J. Grid Distrib. Comput 2010, 3, (1), pp. 1–10

[9]. Yager, R.R.: 'On ordered weighted averaging aggregation operators in multi-criteria decision making IEEE Trans. Syst. Man Cybern., 1988, 18, (1), pp. 183–190

[10]. S.Pearson and A.Charlesworth, "Accountability as a Way Forward for Privacy Protection in the cloud", Proc.Frist Int'1 Conf. Cloud omputing, 2009.

[11]. Ensuring Distributed Accountability for Data Sharing in the Cloud Author, Smitha Sundareswaran, Anna C.Squicciarini, Member, IEEE, and Dan Lin, IEEE Transactions on Dependable and Secure Computing ,VOL 9,NO,4 July/August 2012

[12]. Nilutpal Bose, Mrs. G. Manimala, "SECURE FRAMEWORK FOR DATA SHARING IN CLOUD COMPUTING ENVIRONMENT, Website: www.ijetae.com, Volume 3, Special Issue 1, January 2013)

[13]. Alhamad, M., Dillon, T., Chang, E.: 'Conceptual SLA framework for cloud computing'. Proc. Fourth IEEE Int. Conf. on Digital Ecosystems and Technologies (IEEE DEST 2010), pp. 606–610

[14]. J. Weitzner, H. Abelson, T. Berners-Lee, J. Feigen-baum, J. Handler,and G.J. Sussman, "Information Accountability", Comm.ACM,vol. 51,no. 6,pp. 82-87,2008

[15]. Friedman, E.J., Resnick, P.: 'The social cost of cheap pseudonyms',JEcon. Manage. Strateg., 2001, 10, (2), pp. 173C199