Feasibility of User Level Trust in Cloud Computing

Ms. Yashashree Bendale,
Computer Engineering
SIESGST, Nerul
Mumbai, India

Prof. Seema Shah
Computer Engineering
VIT, Wadala
Mumbai, India

***Abstract*— Cloud computing has recently emerged as a buzz word in the distributed computing. Today the issue of trust is one of the biggest obstacles for wide usage of cloud computing. When the element trust is absent in a cloud computing environment then this computing model will face a lot of challenges. One of the most important factors for the successful deployment and usage of cloud computing is to build trust and security in a cloud. Here the user directly operates the software and the operating system, so the effect and damage of the cloud resources are worse than that of the internet. Therefore, it is necessary to evaluate whether the user is trustworthy or not. In this paper, we have discussed feasibility of trust in cloud computing, which can be possible through building a trust model for evaluating user-level trust in cloud computing environment. We have further explained the approach and principles for the evaluation of user trust in cloud computing. Finally we laid down the foundation for the user trust evaluation. In future we propose to evaluate user level trust in a live cloud environment.**

Keywords*— *Cloud Computing, Trust, User level Trust.

I. INTRODUCTION

Cloud computing is acting as a buzz word in the distributed computing community. It is believed that cloud is going to reshape the IT industry as a revolution. Cloud computing is the delivery of computing as a service rather than a product, where by shared resources, software and information are provided to computers and other devices as a utility over a network. In the cloud computing, due to users directly use and operate the software and operating system, and even basic programming environment and network infrastructure provided by the cloud service providers. The effect and damage for the software and hardware of cloud resources are worse than the current internet users who use it to share resources. Trust is the biggest obstacle for the development of cloud computing. Therefore it's important to address the issue of trust in cloud computing. The user behavior here is referred as the failed operation which has violated certain security policy.

The concept of trust has been studied in disciplines ranging from economic to psychology, from sociology to medicine, and to information science. It is hard to say what trust exactly is because it is a multidimensional, multidisciplinary and multifaceted.

Trust is an old but an important issue in daily life. Trust generally plays a major role in establishing a relationship between entities and has been studied for a long time, mainly by social scientists. Currently, trust is widely used in many kinds of internet environment, such as e-commerce, peer-to-peer network, mobile ad hoc networks [1] and wireless sensor networks. Trust has become more popular since the traditional network security mechanisms such as Firewall, Access Control and Certificate Authority etc. cannot predict the user's behavior. User trust gives the evidence to avoid the interaction with the malicious users and to increase the possibility of cooperation to achieve the goals among the users. Li Wen [2] has proposed a trust model for user behaviour trust in trustworthy internet. They proposed a novel trust model including direct trust based on direct experiences and indirect trust. This model combines direct as well as indirect trust.

This paper is organized as follows. In the first section we have given overview of trust. The next two sections describe about trust in cloud computing and feasible approach for evaluation user level trust.

I. OVERVIEW OF TRUST

The concept of trust has been studied in disciplines like economic, psychology, sociology etc. It is hard to say what trust exactly means because it is a multidimensional, multidisciplinary concept. We can find various definitions of trust in the literature. Common to these definitions are the notions of confidence, belief, faith, hope, expectation, dependence, and reliance on the goodness, strength, reliability, integrity, ability, or character of a person or thing. Generally, a trust relationship involves two parties: a truster and a trustee. The truster is the person or entity who holds confidence, belief, etc. on the reliability, integrity, ability, etc. of another person or thing, which is the object of trust - the trustee [3].

Although trust has been recognized as a difficult concept hard to narrow down, the critical characteristics of trust can be summarized. Trust is subjective because the level of trust considered sufficient is different for each individual in a certain situation. It is the subjective expectation of the truster on the trustee's behavior that could influence the belief. Trust is also dynamic as it is affected by many factors. We trust a system less if it gives us insufficient information about its expertise. Mere claims such as "secure cloud" or "trust me" don't help much to boost the trust level of consumers [4].

Proc. of the Intl. Conf. on Advances in Computer, Electronics and Electrical Engineering
Editor In Chief Dr. R. K. Singh. ISBN: 978-981-07-1847-3

II. TRUST IN CLOUD COMPUTING

Cloud computing need mutual trust of the users and the services providers, neither is replaceable. For example, because user lacks controllability of data, equipment and environmental, which lead to mistrust of cloud computing.
Mistrust in cloud computing can be lead due to the following reasons:

- Data leakage risk
- Storage position security risk
- Data being investigated risk
- Data damage risk
- Service disruptions
- The cloud provider failure risk

The Trust can be thought of two way process as users trust cloud service provider and cloud service provider should trust users. So, whether users trust cloud service provider and wish to put their data and daily processing environmental into providers trusteeship is principle of cloud computing.

Platform as a service of cloud allow user deploy certain types application program, which was created by their own to the servers, and users can control these program and computing environment configuration. So the malicious user may submit a malicious code, this code may occupy CPU time, memory space and other resources, and also may also attack other users, and may even attack the underlying platform that provide operational environment. So it's essential for the cloud service provider to monitor the user behavior [5].

The possible reasons leading to the user behavior mistrust are:
a. Individual destruction behaviors, such as marketable competitors.
b. The cloud software, systems and infrastructure damage were broken by user errors or configuration errors.
c. Malicious software which lead to user behavior mistrust.
d. Identification authentication error.

No matter what causes the user mistrust, cloud service provider must monitor user behavior in order to ensure the trustworthiness of the user's identity and behavior. So it's feasible to evaluate trust in cloud computing.

III. APPROACH FOR EVALUATING USER TRUST IN CLOUD COMPUTING

Security of information system plays a vital role these days. It's important to protect the information system of application on the cloud because of the following reasons: Terminal users access web applications and perform illegal operations on the database to make profits, threatening the information security. User's frequently changing IP addresses, making it difficult to position the source of an information issue. Users can download excessive resources by seating up the proxy server which violates the agreement of cloud service provider and which may cause excessive resource consumption and congestion at the network outlet, affecting normal process of key services Due to these, we need to control and monitor the network access of the user, so it's necessary for the cloud service provider to find the user level trust while accessing the application on the cloud.

Trust model for evaluating the user level trust in cloud computing environment is shown as:

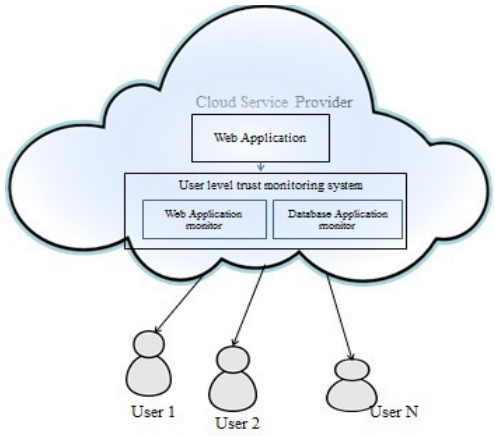

Figure1: Trust model in cloud computing

User trust is based on hierarchical structure model which decomposes complicated user trust into small part called sub-trust. These sub trusts are further divided into more small data unit, namely behavior trust evidences.

Subdivided sub trusts are agreement, security, expense sub-trust and identity re-authentication sub-trust. Agreement sub-trust refers to whether the user conforms to the agreement. For instance, in the use of cloud application, whether the user uses the application according to the rules. Security sub-trust refers to whether the user will attack and damage the cloud resources. For instance, whether the user attempts to attack the digital resources and servers or get account information of other users and commercial competitors in the name of a legitimate user to make a Denial of Service attack. Identity re-authentication sub-trust refers to a situation where the user authentication may be wrong and how to re-authenticate the user identification. For example, if the user is using the default user name and password, it is easy to hack the username and password. Therefore, during important information access, it is necessary to re-authenticate the user identification. It's feasible to identity the behavior trust evidences for each sub-trust. Depending on these evidences we can analyse the user behaviour. [5]

In a figure1 there is layer called user level trust monitoring system, this system will analyse the user behaviour and calculate the user trust. User level trust monitoring system consists of as web application monitoring system, Database application monitoring. Web application monitor system filters packets based on self-defined keywords, file types, and

scripts. Database application monitors database access activities, including user login, logout, and various database operations.

This monitoring system will monitor the user, based on the trust evidences given below:

- IP address is unusual
- number of attempts of enter password exceeds the threshold value
- timing of the visit is abnormal
- user's connections are illegal
- access to files are large in number
- user resource downloads are more than average
- sign-on system has failed often
- proxy is used often

Depending on these behavior evidences we will analyse the activities of the users and evaluating the user level trust.

IV. PRINCIPLES FOR THE ESTIMATION OF USER TRUST IN CLOUD COMPUTING

The user level trust will be evaluated from the following principles:

a. Evaluating the trust of the expired user:
When the record of trust was very old and out of date, the value of the trust evaluation has been natural attenuation in the process of evaluation. This attenuation is not the result of the behavior of user, but the normal attenuation over time.

b. Record-based Trust:
Evaluation of the trust has an important relation with the user access time. Latest records will play an important role in trust evaluation. Out-dated records have the less impact on trust evaluation. The more predictable behavior has the smaller influence on trust evaluation, and the more irregular behavior will play a more significant role in trust evaluation.

c. Repetitive behavior of users:
The behavior trust estimation is regularly formed by gathering, is based on a large number of the historical record of user. So its results are stable and representative. However, if number of user access is not enough large, then the result is unstable and not representative. Therefore, the trust evaluation of user should be based on a large number of behavior accesses.

d. Analysed based action:
The intensity of the reduced trust value is far greater than that gradually increased when finding cheating behavior, which can prompt the user to reduce fraud [6].

V. CONCLUSION AND FUTURE WORK

Cloud computing has recently emerged as a buzz word in distributed computing. Depending on the data value the importance of trust varies from organization to organization. Less the trust cloud provider has in the user, more it will try to analyze and control the activities of the user.

In this paper we have proposed a trust model for the evaluation of the user level trust in cloud computing environment. We are evaluating the user level trust for the web applications hosted on the cloud environment. The user level trust can be evaluated by analysing unusual activities specified for finding trust evidences which are mentioned in the paper. The outcome of the user level trust evaluation will be used for determining the trustworthiness of the user. Simply failing on one or two parameters used for analysing the trustworthiness cannot conclude the trustworthiness or untrustworthiness of the user but definitely it will help in controlling the unusual user activities and also in deciding further plan of action. Further, we are planning to implement trust model in public cloud environment.

REFERENCES

[1] George Theodorakopoulos and John S. Baras "*Trust Evaluation in AdHoc Networks*" *WiSE'04,* October 1, 2004, Philadelphia, Pennsylvania, USA.

[2] Li Wen, Ping Lingdi, Lu Kuijun, Chen Xiaoping "*Trust Model of Users' behavior in Trustworthy Internet*" IEEE computer society 2009

[3] Qiang Guo, Dawei Sun, Guiran Chang, "*Modeling and Evaluation of Trust in Cloud Computing Environments,"* 3rd International Conference on Advanced Computer Control (ICACC 2011)

[4] Khaled M. Khan and Qutaibah Malluhi "*Establishing trust in cloud computing*" IEEE october 2010.

[5] Tian Li-qin,LIN Chaung, "*Evaluation of User Behavior Trust in Cloud Computing*," International Conference on Computer Application and System Modeling, 2010

[6] Ni Yang, Tian Liqin ,Shen Xue-li " *Behavior Trust Evaluation for Node in WSNs with Fuzzy-ANP Method"*, In the 2nd International Conference on Computer Engineering and Technology, 2010.