User Level Trust Evaluation in Cloud Computing

Yashashree Bendale
Vidyalankar Institute of Technology
Wadala-37

Seema Shah
Vidyalankar Institute of Technology
Wadala-37

ABSTRACT

The cloud computing is a hot research area, because of its good features such as low investment, easy maintenance, flexibility, fast deployment and reliable service. At the same time, cloud computing can also reduce operating costs. The issue of trust is one of the biggest obstacles for usage of cloud computing. Today, one of the most important factors for the success of cloud computing is to build trust and security. Trust in cloud computing has a lot of issues like control, prevention, ownership and security.In this paper we have addressed the issue of trust in cloud computing. In cloud computing, users directly use and operate the software and operating system, and even basic programming environment and network infrastructure. So the impact and destruction for the software and hardware cloud resources in cloud computing are worse than the current internet users. Therefore, it is necessary to evaluate user's trustworthiness. So for evaluating the user level trustworthiness,we have defined policy based user level trust is evaluated. The User is categorized into different categories based on the user level trust value, number of policies violated and number of warnings received. This trust evaluation helps us to monitor the abnormal behavior of the user. Depending upon the user behavior, cloud service provider can restrict the user from accessing the cloud resources and also the user can be blacklisted.

Keywords

Cloud Computing, Trust, User level Trust

1. 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, evaluation user level trust and results and discussion.

2. 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].

3. 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.

4. POLICY BASED TRUST EVALUATION

This approach has been proposed in the context of open and distributed services architectures as a solution to the problem of authorization and access control in open systems. The focus here is on trust management mechanisms employing different policy languages and engines for specifying and reasoning on rules for trust establishment. The goal is to determine whether or not an unknown user can be trusted, based on a set of credentials and a set of policies.

In addition, it is possible to formalize trust and risk within rule-based policy languages in terms of logical formulae that may occur in rule bodies.

Currently, policy-based trust is typically involved in access control decisions. Declarative policies are very well suited to specifying access control conditions that are eventually meant to yield a boolean decision the requested resource is either granted or denied.

Policy based decision is used to make user behaviour decision based on the policies set by the administrator for all the users. Basically User level trust evaluation monitors the activities of users with the help of policy violations. Policies are violated by the users. Policies are based on the combination of the parameters.

Following are the lists of parameters used for creating policies:

Table 1: Parameters

Sr. No	Parameters	Description
1	O	Other User
2	Pr	Private Workspace
3	Pb	Public Workspace
4	Fl	File
5	Fd	Folder
6	DA	Data
7	M	Modify
8	C	Create
9	D	Delete

O– Other User

Other User is the user who is accessing the details of another user.

Pr- Private Workspace

Private workspace is workspace of an individual user.

Pb- Public Workspace

Public workspace is workspace of an individual user wherein user can share their data.

DA-Data

Data is any information that is contained in the private workspace or in public workspace in terms of file.

FD-Folder

Folder is a virtual container within a digital file system, in which groups of files and other folders can be kept and organized.

Fl-File

A file is a block of arbitrary information, or resource for storing information, which is available to a computer program and is usually based on some kind of durable storage. A file is durable in the sense that it remains available for programs to use after the current program has finished.

C-Create

Create is the operation that is done by the user on private workspace or public workspace. User can create a dummy files and folders.

D-Delete

Delete is the operation that is done by the user on private workspace or public workspace. User can delete a important files and folders.

M-Modify

Modify is the operation that is done by the user on public workspace. User can modify the contains of a files.

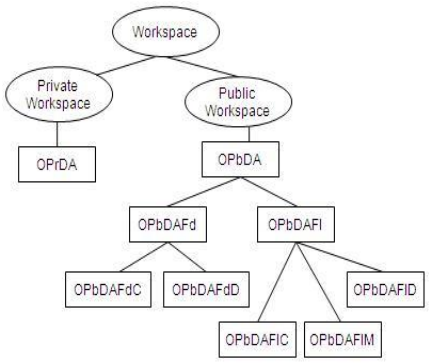

Figure 1: Polices of user level trust evaluation

OPrDA--Other User's Private Data
This Policy stands for Other User's Private Data. When user tries to access the other user's private data workspace, this policy gets violated.

OPbDAFdD--Other Public Data Folder Delete
This Policy stands for Other Public Data Folder Data Delete, when user tries to access the other user's public data and try to delete the folder present in public workspace of the other user, this policy gets violated.

OPbDAFdC-- Other Public Data Folder Create
This Policy stands for Other Public Data Folder Create, when user tries to access the other user's public data and try to create the folder present in public workspace of the other user, this policy gets violated.

OPbDAFlC--Other Public data file create
This Policy stands for Other Public data file delete create, when user tries to access the other user's public data and try to create a file in public workspace of the other user, this policy gets violated.

OPbDAFlD--Other Public data file delete
This Policy stands for Other Public data file delete, when user tries to access the other user's public data and try to delete a file in public workspace of the other user, this policy gets violated.

OPbDAFlM--Other Public data file modify
This Policy stands for Other Public data file modify, when user tries to access the other user's public data and try to modify the existing file in public workspace of the other user.

5. PROCEDURE TO EVALUATE THE USER LEVEL TRUST IN CLOUD COMPUTING

User level Trust evaluation is done in the following manner:

Step 1: Create a user Profile i.e. Registration
Initially trust value is 5.i.e user is initially neutral
Step 2: Setting up the Policies for the created users.
Step 3: User Logins in to the system, if Login is successful then Trust value is increased by fraction.
$Tp = Tp + 10^{-n}$
N=integer;
Step 4: If User violates the policies, Warning is given
If warning given exceeds 3
Then his trust value will be decreased by following equation:
Trust is been calculated with the help of following equation:
$Tn = W1 * (S/N) + W2 * (C/S)$
$Tp = TP - Tn$
Tp =Previous Trust value
T=Fraction value can be positive or negative
W1, W2 = weight constant.
N= no. of session
S= Previous rule broken (Support).
C=Confidence (Same rule broken no. of times)
And the user would be given warnings.
Step 5: If trust value < below trust threshold
Then User would be blacklisted.
Flag is Set.

6. RESULTS AND DISCUSSION

User will be categorized based on the following trust levels

Table 2: User Trust Level Categorization

Level	Value	Meaning	Description
L0	-5	Distrust	Completely Untrustworthy
L1	0 ≤ Value< 2.5	High Distrust	Lowest Possible Trust
L2	2.5 ≤ Value<5	Low Trust	Not Very Trust Worthy
L3	5 ≤ Value<7.5	Medium Trust	Mean Trustworthiness
L4	7.5 ≤ Value<10	High Trust	More Trustworthy
L5	10	Complete	Completely Trustworthy user

In the above table, we have shown the different categorization of the user based on their trust values.

Level 0: It is been denoted by L0.This level will categories the user whose trust value is -5. Means the user is distrust. User in this category is called as completely Untrustworthy and the user is blacklisted.

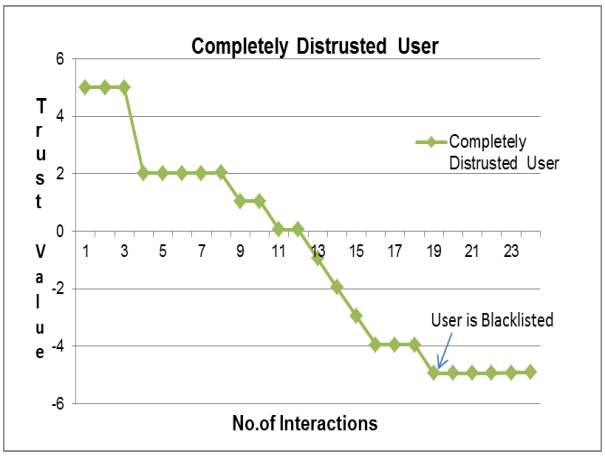

Figure 2: Completely Distrusted User

As we can see from the graph below, from the starting itself user4 is behaving in maliciously, so this trust value is decrementing and reaches to -5. And the user is blacklisted. User4 will have to contact administrator for the next login.

Level 1: It is been denoted by L1.This level will categories the user whose trust value is between 0 ≤ Value< 2.5. Means the user is High Distrust. User in this category is called as Lowest Possible Trust.

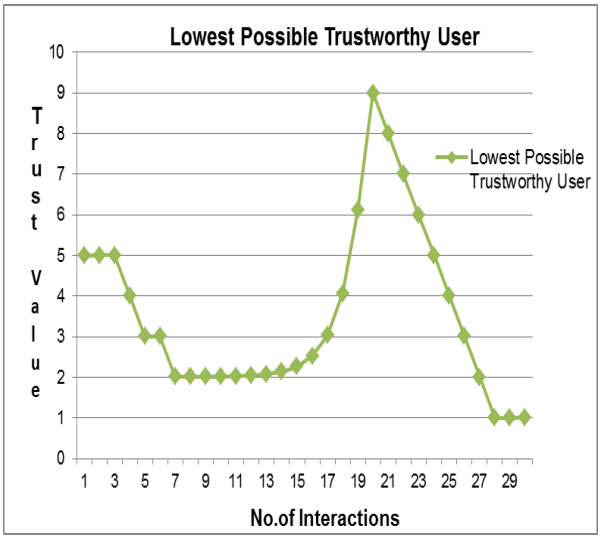

Figure3: Lowest Possible Trustworthy User

Means at the starting itself user try to behave maliciously, and his trust value remains between 0< Trust value<2.5. So we can call such type of user as Lowest Possible Trustworthy User.

Level 3:

It is been denoted by L3.This level will categories the user whose trust value is between 5 ≤ Value<7.5. Means the user is Medium Trust. User in this category is called as Mean Trustworthiness.

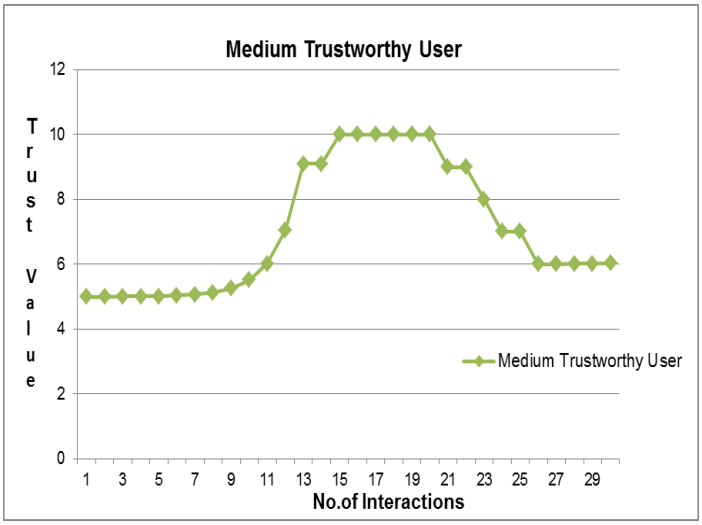

Figure4: Medium Trustworthy User

Level 4:

It is been denoted by L4.This level will categories the user whose trust value is between 7.5 ≤ Value<10. Means the user is High Trust. User in this category is called as More Trustworthy.

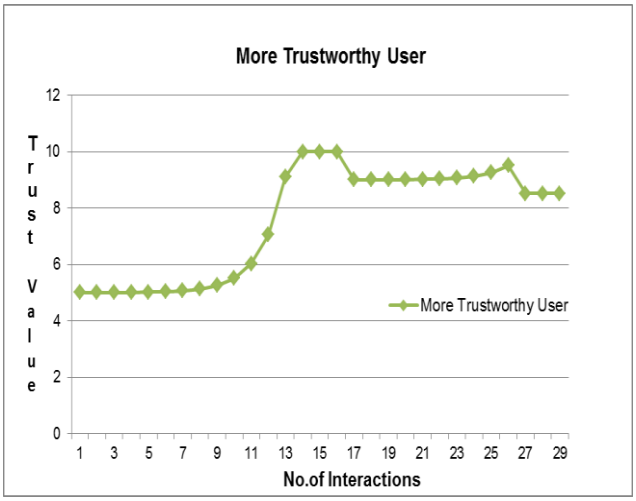

Figure5: More Possible Trustworthy User

Level 5:

It is been denoted by L5.This level will categories the user whose trust value is 10. Means the user is Complete. User in this category is called as Completely **Trustworthy** user.

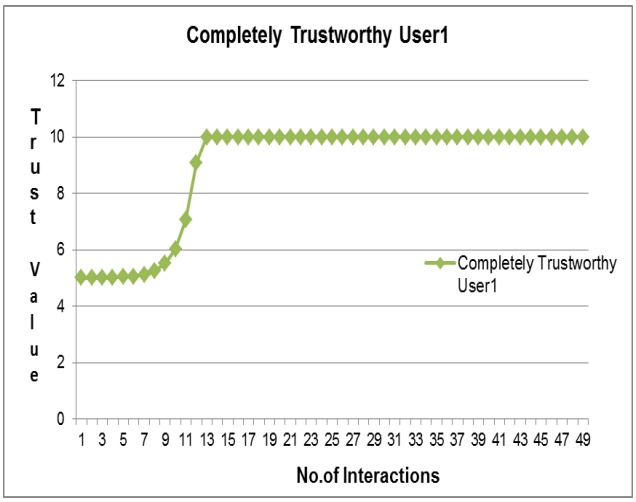

Figure6: Completely Trustworthy User

Discussion

Estimating the expired behavior can be used to identify behavior of a new 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.

Estimation of behavior is in proportion to the behavior time and abnormal degree of behaviour: 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.

The trustworthiness of trust estimation is in proportion to number of times user access cloud resources/application: 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.

Sudden drop in trust estimation results punishment: 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].

7. CONCLUSION AND FUTURE WORK

In the cloud computing, due to users directly use and operate the software and OS, and even basic programming environment and network infrastructure which provided by the CSP, so the impact and destruction for the software and hardware resources in cloud computing are worse than the current Internet users who use it to share resources.

In particular that the subjective as a legitimate user vandalism, such as competitors, hackers and opposition, etc. The increasing trends of the cloud computing force the user level trust evaluation technique for the cloud computing.For these we have set up the private cloud using Ubuntu eucalyptus cloud. User can behave in unambiguous way, so we have developed the user level trust evaluation application on cloud. We developed the SaaS application to monitor the user behavior in private cloud; with this application we evaluate the user level trust. For every action performed by the user, we evaluate the user trust. Depending upon this user trust, cloud service provider will come to know whether the user is trustworthy or not. Accordingly cloud service provider will assign the privileges to the users.

This trust evaluation helps us to monitor the abnormal behavior of the user; depending upon the user behavior cloud service provider can restrict the user for accessing the cloud resources. It also helps cloud service provider to keep track on the user behavior and can easily trace the user behavior.

8. FUTURE WORK

As the number of the registered users increases on the cloud, user level trust evaluation will be overhead. Solution for this problem is that we will create the cluster of the user on the basis of their trust value and monitor the cluster of the user's. We will make cluster based on the previous historical records of the users. And predict the user behavior by making use of Artificial Intelligence.

9. 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.