Predict the Security Mechanism in Cloud Service

S Govinda Rao
Associate Professor
Department of CSE
GRIET, Hyderabad

***Abstract*— Currently, the cloud computing is hot research both in scholars and enterprise, because of its good features such as low investment, easy maintenance, Flexibility and fast deployment, reliable service. But to truly implement cloud computing, we need to gradually improve it in academic, legal and institutional. Especially, the issue of trust is one of the biggest obstacles for the development of cloud computing. 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 cloud services providers, so the impact and destruction for the software and hardware cloud resources in cloud computing are worse than the current Internet users who use it to share resources. Therefore, that whether user behavior is trusted, how to evaluate user behavior trust is an important research content in cloud computing. mainly discusses evaluation importance of user behavior trust and evaluation strategy, in the cloud computing, including trust object analysis, principle on evaluating user behavior trust, basic idea of evaluating user behavior trust, evaluation strategy of behavior trust for each access, and long access, which laid the theoretical foundation about trust for the practical cloud computing application.**

***Keywords*— Cloud computing, Evaluation Principle, Evaluation Strategy, Behavior Trust.**

I. INTRODUCTION

Currently, the cloud computing is welcome in scholars and enterprise, because of its good features such as low Investment, easy maintenance, flexibility and fast deployment, reliable service. At the same time, cloud computing can also reduce operating costs, improve operational efficiency. So many countries put the financial and material for the cloud computing. The U.S. government expect that the annual growth rate of its spending on cloud computing will be about 40% in the 2010-15, in 2015 it will reach 7 billion U.S. dollars [1].

There are three kinds of cloud services model, namely, Software as a Service (SaaS), Platform as a Service (PaaS) and Cloud Infrastructure as a Service (IaaS). The basic structure of the cloud computing model as shown in Figure 1 , it divided into five levels, from top to bottom is resources provide layer, cloud services provide layer, information transport layer, professional service provider layer, end user layer. The cloud service providers (CSP) use the resources provided by resources layer and their technology (such as Virtualization Technology) to integrate the cloud services, and through the information transport layer to provide these services to users.

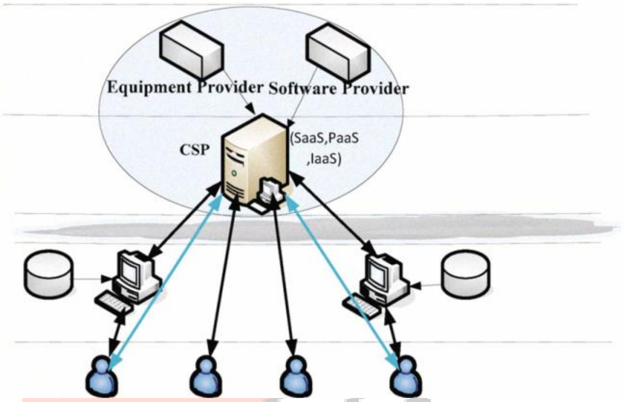

Figure 1. Users and service providers in basic cloud computing architecture.

II. TRUST NEEDS FOR THE SERVICE PROVIDERS AND USERS IN CLOUD COCMPUTING

To truly implement cloud computing, we need to gradually improve it in academic, legal and institutional. Especially, the issue of trust is one of the biggest obstacles for the development of cloud computing. In the cloud computing there need mutual trust of the users and the services providers, neither is dispensable. For instance, because user lacks controllability of data, equipment and environmental, which lead to mistrust of cloud computing, include: data disclosure risk, store location security risk, data being investigated risk, data loss risk, service interruptions and the cloud provider collapse risk. That whether users trust CSP and wish to put their data and daily processing environmental into providers' trusteeship is premise of complete development of cloud computing. Like if we are willing to trust bank, and put our money into bank. Therefore, it is important that if the users trust providers, this is current important research content of the most researchers.

On the other hand 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. For instance, in the PaaS service, because it 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. Therefore, how to evaluate and manage the trust of user behavior is an important research content in cloud computing.

In the cloud computing, the first user trust is the user's identity trust, but we only have the user identity trust in the cloud is not enough, the issue of user behavior trust also must be evaluated and managed. Traditional authorization and authentication main solve the issue of user's identity trust, but does not solve the problem of trust on user's behavior. For instance, the cloud computing is used as ordering the digital electronic resources. The database supplier used the cloud computing to build the large-scale library of digital resources (E-resource data cloud),which not only reduce the investment of purchase equipment and personnel training, but also transfer routine maintenance of equipment systems, safety precautions to CSP, and the related function software can directly run on the cloud server. Only if the users access the network, they can easy get the electronic resources, needn't to download the viewer beforehand. The ultimate user is the user who has ordered the electronic resources. We can use the traditional authentication method to authenticate user identification, but these are not enough. Because that some users (such as some students in the university) often use the tools to download large quantities electronic resources, which they have paid, or set up proxy server without permission for seeking illegal gains. In this case, the user's identity is trusted. However, the user behavior is not trusted. We often see some users are warned and even the account is closed because of misconduct. Therefore, in cloud computing environment, only to solve the user's identity trust is not enough, user's behavior trust must be combined to the identity trust to solve the problem of how to CSP trust user.

The possible reasons leading to user behavior mistrust is (1) subjective vandalism behaviors, such as commercial competitors, or against persons; (2) the cloud software, systems and infrastructure damage were broken by user errors or configuration errors; (3) Malicious software result in user behavior mistrust. (4) Easy-lose devices such as cell phone and PDA may result in identification authentication error. No matter what causes make the user mistrust, CSP must to monitor user behavior in order to ensure the credibility of the user's identity and behavior.

III. EVALUATION OBJECT OF BEHAVIOR TRUST IN CLOUD COMPUTING

In basic structure of the cloud computing, there are two categories objects: service provider and user, but providers and user are not absolute concepts. For instance, the service of electronic resources with cloud computing, for the electronic resources supplier (ERS) and CSP, the user is ERS the service provider is CSP; but between ERS and electronic resources subscriber, the user is subscriber, the service provider is supplier. So the behavior trust of the service provider to user includes two kinds: One is the trust of CSP to the ERS; the other is the ERS to the subscriber. in the two kinds of trusts, the trust of CSP to ERS is the basis trust, it includes various behaviors monitoring for electronic resources supplier on subjective, objective, deliberate, incorrect operation etc. If they trust each other, then the ERS may put their various behaviors monitoring of subscriber into providers' trusteeship, who are good at technology to deal with the trust supervision of users' behaviors, which will improve the effect of trust supervision on the users' behavior.

In the user's computing architecture, there are three service providers. They are CSP, enterprise service provider (ESP) and Internet service provider (ISP). Users were divided into three types: (1) the general cloud user (CU) who directly uses cloud computing; (2) enterprise cloud user (ECU) not only use the local resources, but also use the function of cloud computing to build its own service industry; (3) enterprise user (EU), who only uses the service from enterprise. Due to that the ECU also provides the service to the EU, the ECU is also the service provider of EU. So it has two identities, ESP and ECU. For CSP, there are two kinds users, CU and ECU. In terms of theory, we should have 12 pairs of trust, but only 10 pairs in fact as shown in Figure.2, because ECU and ESP has dual role at the same time.

Of course, the practical trust also includes six kinds of trusts among the providers. In this paper, the trust of service provider to user will be discussed, it includes: ESP-EU, CSP-CU, CSP-ECU and the trust of Internet service provider to its users: ISP-CU, ISP-ECU, ISP-CSP. The trust of ISP to its users has been studied for a long time; furthermore, we have dedicated "trusted network" for studying it [2]. So trusts which between service providers and users are CSP-CU, CSP-ECU and ESP-EU. In cloud computing we mainly research the former two, because both the CU and the EU are terminal users for CSP, we can combine the two in one, they are called cloud user (CU). Thereby, the research model can be simplified as shown in Figure 2.

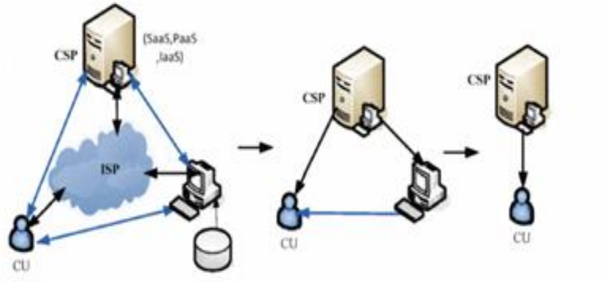

Figure 2. Simplified trust model in cloud computing

IV. EVALUATION PRINCIPLE IN CLOUD COMPUTING

- *Expired behaviour in evaluating can be approximated as a strange 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 natural attenuation over time. So this value can be approximated as a trust value of strange user.

- *Behaviour evaluating effect is in proportion to behaviour time and abnormal degree of behaviour*

The evaluative result of behavioral trust has important relations to user access time. The more recent behaviors will play a more important role in trust evaluation, the more long term behavior has the smaller influence on the trust evaluation due to attenuation. Meanwhile, the evaluative result of the behavioral trust also has an important relationship with each behavior. The more conventional behavior has the smaller influence on trust evaluation, and the more abnormal behavior will play a more important role in trust evaluation.

- *The credibility of trust evaluation is in proportion to number of times of user access cloud resources*

The behavior trust evaluation is constantly formed by accumulating, which is based on a large number of the historical behavior of user. So its results are stable and representative of the "personality characteristics". However, if number of user access is not enough large, then the result is unstable and not representative. Therefore, the trust evaluation of user behavior should be based on a large number of behaviors access.

- *Slow-rise in trust evaluation for prevention of fraud risk*

Trust and risk is a pair of contradictory unity, so we need to guard against the risk even of that we have high trust each other. "Slow rise" is a strategy that is to prevent the user immediately get a high trust value only after a small number of accessing cloud resources, only through a large number of the access, slowly to achieve high trust in the trust evaluation. This is an evaluation strategy to prevent user cheating beforehand.

- *Rapid-decline in trust evaluation for punishment of cheating*

The punishment of non-trust user is very important parameters to trust evaluation. Rapid decline" is an evaluation strategy to punish non-trust behavior afterwards. The overall trust value of user that was rated mistrustful in any time will be quickly reduced. 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.

V. EVALUATION BASIC IDEA IN CLOUD COMPUTING

As the trust is coming from a social science, it has the characteristics such as Subjectivity and ambiguity, and is not conducive to natural science research; this is the difficulty of research of user behavior trust. Basic idea of the paper is "divide and treat" based on hierarchical structure model to decompose complicated user behavior trust(UT) into small sub-trust(ST), then we further subdivided behavior sub trust(ST) into more small data unit, namely behavior trust evidences(BE), after that we compose it again from bottom layer to top layer Scientifically. This kind of first decomposition and then-combination method can solve the uncertainty, subjectivity and ambiguity of evaluation of user behavior trust in cloud computing.

In cloud computing, according to the user behavior contract signed by the service providers and users, user authentication information and authentication failed plan strategy, possible subjective and objective safety risk behavior of users, the cloud resources fees statistics used by user, user behavior trust (UT) can be decomposed into four basic behavior sub-trust, namely security behavior sub-trust (SST), contract behavior sub-trust (CST), expense behavior sub-trust (EST) and identity re-authentication sub-trust(IST).

Contract behavior sub-trust (CST) is refer to whether user behavior comply with the contract, for example, In the use of digital resource cloud, whether the cloud user use resources according to the regulations, whether excessive downloading, secretly setting of external proxy server. security behavior sub-trust (SST) is refer to whether user behavior with the attack and destruction on the cloud resources, for example, whether user attempts to attack the digital resources and servers, get account information of other users and commercial competitors in the name of a legitimate user to make Denial of Service (DoS) .identity re-authentication sub-trust (IST) is refer to that when the user authentication may be wrong, how to re-authenticate the user identification, for example, If the user uses mobile phones and PDA to access cloud resource, which over the computer equipment is easy to lose, if he also using the default user name and password, it is easy to lost username and password. Therefore, during the important information access, it is necessary to re-authenticate the user identification when the service provider monitor user abnormal behaviour (such as excessive download) .expense behavior sub-trust (EST) is refer to that when users use cloud resources, whether user comply with the agreed terms of resource consumption, not opportunistic, not drill holes of consumption charging, for example, In the use of digital resource cloud, cloud users are generally paid fixed costs annually, if the user exit of the system as soon as possible after information is retrieved, which can maximize the use of electronic resources, Otherwise, in the resource-use peak, other users can not use system resources due to the limitation of the maximum concurrent users. Here the user expense behavior trust is important; service providers should monitor user consumption behavior and reward good users with high trust in expense behavior.

Every behavior sub-trust (ST) can be subdivided into behavior trust evidences (BE), the division of specific examples can be seen in Figure 2. where Cl is the average number of access to file; C2 is average user resource downloads; C3 is the average number of failed sign-on system; C4 is the average number of threads occupied by users;C5 is whether use proxy; El is the average number of establishing file;E2 is the average user throughput; E3 is the number of bytes of data from CSP to the user; E4 is the number of bytes of data from the user to CSP; E5 is the duration of access to the system; I1 is whether IP address is unusual; I2 is Whether the number of enter password exceeds threshold;I3 is Whether the number of enter user name exceeds threshold;I4 is whether the timing of the visit is abnormal; I5 is whether the timing of the location is abnormal; S1 is the average number of users illegal connections; S2 is the average number of users scan the important port; S3 is the average number of times that a user tries to beyond the purview; S4 is whether key words are in sensitive dictionary;S5 is the average number of users to access the "root".

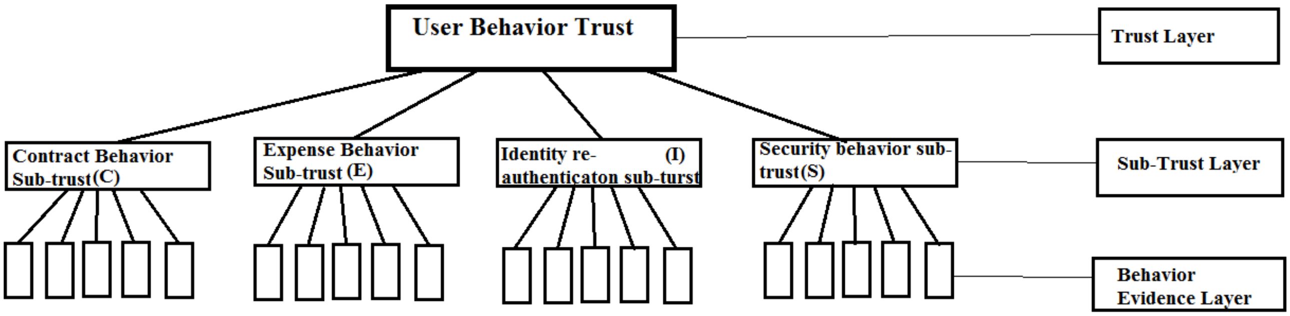
User Behavior Trust
Trust Layer
Contract Behavior Sub-trust(C)
Expense Behavior Sub-trust (E)
Identity re- (I) authenticaton sub-turst
Security behavior sub-trust(S)
Sub-Trust Layer
Behavior Evidence Layer

Figure.3.User Behavior Trust Evaluation Hierarchy in Cloud Computing

VI. ACQUIREMENT OF BEHAVIOR TRUST EVIDENCE

For acquirement of effective evidence, we mainly consider that acquired evidence is comprehensive, true and reliable. The trust evidence can be obtained by using the following methods:

1) Network flow detection tool, such as bandwidth [3], it can get HTTP, TCP, UDP, ICMP, VPN and P2P data flow based on IP, which belong to user performance trust evidence.

2) Existing invasion detection system (IDS), such as Tcpdump[4], it can get trust evidences such as the times of access, the times of operation failure, transfer delay, the times of scanning port and the rate of buffer overflowing etc. as long as the mode of the network card is set to promiscuous mode ;

3) All kinds of log and Audit trails [5], such as system log, application log, auditing record, network management log, etc, which can reproduce user trust evidence record including user packet and corresponding operating record, such as the number of fragment recomposition;

4) Special data collecting tool, such as Cisco's NetFlow Monitor [6], it provides nearly real-time traffic monitoring and multi criterial data flow selection, using source/destination IP addresses, protocols, etc. it can get user security and performance trust evidence, such as the average number of illegally accessing system and the average number of scan-sensitive-port illegally;

5) Network management software based on standardized protocol such as RMON or SNMP, such as CiscoWorks Software [7];

6) Using hardware to get evidence directly such as Net Scout’s, nGenius hard Probes [8];

7) The information reproduced by other security product, such as Firewalls, access control system and other evidence Network monitors.

VII. EVALUATION STRATEGY FOR EACH ACCESS IN CLOUD COMPUTING

A. *AHP based Evaluation strategy for each access*

After the user access to cloud resources, we can evaluate user behavior trust according to behavior evidence obtained in access. Basic idea of trust evaluation is "divide and treat" based on hierarchical structure model, In figure 2, top-down hierarchical structure shows how to decompose trust, downtop hierarchical structure shows how to combine behavior evidence to form the evaluation of user behavior trust. The most important problem in the combination to be solved is how to determine the weight of sub-trust and behavior evidence; accordingly, we found a very appropriate evaluation method, namely, Analytic Hierarchy Process (AHP). AHP is a combination of qualitative and quantitative analysis of multi-objective decision, which simplifies the complexity of problem analysis, and can test the consistency of the major Subjective mistakes, detailed evaluation steps see [9]

B. *FAHP based Evaluation strategy for each access*

AHP evaluation process depends on the expert's expertise and level of knowledge on the evaluation system, with strong subjectivity. Its Matrix is defined between 1 to 9 integer scales as ratio, with strong subjectivity, which differs from the actual evaluation. Actual evaluation process has obvious ambiguity, its result is not be an exact real number my, but in the interval between my. In order to solve the problem, we use a kind of evaluation methods named Fuzzy Analytic Hierarchy Process (FAHP) based on triangular fuzzy numbers to weaken AHP's subjectivity, which makes the evaluation results more objective. Detailed evaluation steps see [10]

C. *FANP based Evaluation strategy for each access*

$$m\_tru = \sum_{flag_j = \substack{norm \\ punish}}^{m} \left[\frac{(tim_j - tim_1)}{\sum_{j=1}^{m}(tim_j - tim_1)}\alpha + \frac{d_j}{\sum_{j=1}^{m} d_j}(1-\alpha) \right] tru_j$$

In AHP, only the low-level behavior evidence will affect the higher-level sub-trust, while the high-level sub-trust will not adversely affect lower-level evidence. However, practical problems is often a higher-level sub-trust will affect the lower-level evidence for example, a user with low security behavior sub-trust (SST) may use proxy(C5), and internal elements of the same layer are often dependent, so we use Network Analysis Process (ANP) to evaluate user behavior trust to reflect relationship between various behavior evidences. However, ANP also has strong disadvantage of subjectivity of depending on the expert's expertise so we use Fuzzy Analytic Network Analysis (FANP) to evaluate user behavior trust that combine the advantages of ANP and FAHP. We use triangular fuzzy numbers to replace ANP approach's scale from 1 to 9 and set up fuzzy matrix. Detailed evaluation steps see [11].

TABLE 1.Comparison between evaluation strategies of behavior trust

Evaluation Methods	Experts Dependent	Subjectivity Weakening	Correlation between Elements	Consistency Check	Hierarchical Decomposition	Long Term
AHP						
FAHP						
FANP						
DSW						

D. *Double Sliding Window based Evaluation strategy for long access*

Based on the basic criteria of the evaluation, we decide the sliding window to carry out the evaluation of node behavior trust. In that, the trust value not only with the time related, but also with m the number of actual contacts about nodes in the window, and the window's size which control evaluation scale. And also the enough (sliding window size) original evidences were retained, in order to share the trust information or reevaluate the trust for different needs. The movement of window is involved with two factors: the time t and the new node intercourse. As time goes by, the window moves forward, and then some overdue trust records gradually out of the window. In this way, we can ensure that the overall trust value of the node will be decreased when the node doesn't exchange information with others in a long time. When a new intercourse comes, and the window size is fixed, so the record which has the farthest time from the current and wasn't overdue was "squeezed out" thought the window's movement. In this way, we can achieve the goal that the trust evaluation is scalability. Based on the background of actual application on WSNs, by selecting the model factors: the trust effective time period, the window size etc. and updating the window content, it not only effectively control the nodes of deception and punish fraud, but also the algorithm has good scalability.

In computing user behavior trust of effective trust records within windows, the basic idea of calculation is that the more recent, the more abnormal behavior has the greater proportion of comprehensive evaluation, the degree of abnormal behavior is shown by the standard variance of history trust d;, the proportion which each trust for overall trust varies with the record time, we have the formula 1, in this formula, is a scale factor which between the behavior time with the behavior abnormal. More detailed evaluation steps see [12].

VIII. CONCLUSION

Paper mainly discusses evaluation importance of user behaviour trust and evaluation strategy in the cloud computing, including trust object analysis, principle on evaluating user behaviour trust, basic idea of evaluating user behaviour trust, evaluation strategy of behaviour trust for each access, and long access, which laid the theoretical foundation of trust for the practical cloud computing application.

REFERENCES

[1] US Federal Cloud Computing Market Forecast 2010 2015, tabular analysis, publication: http;//www.marketresearchmedia.com 2009.5

[2] Lin Chuang, Tian Liqin. Development of Trusted Network and Challenges It Faces. ZTE Communications, 2008, 6(1): 13-17.

[3] Top 20 IPs by Traffic- Daily, http://bandwidthd.sourceforge.net/demo/ 2009.1 O.

[4] TCPDUMP and LIBPCAP, http;//www.tcpdump.org/, 2010.3

[5] Rebecca Mercuri: On auditing trails. Commun. ACM 03, 46(1): 17-20.

[6] NetFlow Monitor, http//netflow.cesnet.czl,201O.3.

[7] CiscoWorks Software.http://www.cisco.com/public/sw-center/swnetmgmt. shtml, 2006.

[8] nGenius® Probes, http://www.netscout.com/products/probes_home.asp , 2005

[9] Liqin Tian, Anjuan Qiao, Lin Chuang, Ji Tieguo. Kind of Quantitative Evaluation of User Behaviour Trust Using AHP. Journal of Computational Information Systems, 2007, 3(4): 1329-1334.

[10] Guo Shukai, Tian Liqin, FAHP-based User Behaviour trust Computation Tactics. Computer Engineering and Applications, acccepted.

[11] 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, 2010.4

[12] TIAN Li-qin, LIN Chuang. A Kind of Evaluation Mechanism on User Behavior Trust Based on Double Sliding Windows, Tsinghua University Joumal,2010.10