ISSN: 2278 – 7798
International Journal of Science, Engineering and Technology Research (IJSETR)
Volume 1, Issue 5, November 2012

Survey on User Behavior Trust Evaluation in Cloud Computing

Mr. Bhupesh Kumar Dewangan, Mr. Praveen Shende

***Abstract*—Cloud computing may be defined as management and provision of resources, software, applications and information as services over the cloud (internet) on demand. Cloud computing is a model for enabling convenient, on demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction [2]. With its ability to provide users dynamically scalable, shared resources over the Internet and avoid large upfront fixed costs, cloud computing has recently emerged as a promising hosting platform that performs an intelligent usage of a collection of services, applications, information and infrastructure comprised of pools of computer, network, information and storage resources. However along with these advantages, storing a large amount of data including critical information on the cloud motivates highly skilled hackers thus creating a need for the security to be considered as one of the top issues while considering Cloud Computing. In this paper we explain the cloud computing along with its open secure architecture and emphasize on various security threats 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.**

***Index Term*-Cloud Computing,Evaluation of user behavior trust; Evaluation Principle; Evaluation Strategy**

1. INTRODUCTION

Cloud computing is the collection of virtualized and scalable resources, capable of hosting application and providing required services to the users with the "pay only for use" strategy where the users pay only for the number of service units they consume. A computing

Cloud is a set of network enabled services, providing scalable, QoS guaranteed, normally personalized, inexpensive computing infrastructures on demand, which could be accessed in a simple and pervasive way. [3]

1.1. CHARACTERISTICS OF CLOUD COMPUTING

Cloud computing exhibit five essential characteristics defined by NIST (National Institute of Standards and Technology) [2].

1. On-demand self-service. A consumer can unilaterally provision computing capabilities.

2. Broad network access. Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms.
3. Resource pooling. The provider's computing resources are pooled to serve multiple consumers, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand.
4. Rapid elasticity. Capabilities can be rapidly and elastically provisioned, in some cases automatically, to quickly scale out and rapidly released to quickly scale in.
5. Measured service. Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service.

1.2. OPEN SECURITY ARCHITECTURE OF CLOUD COMPUTING

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 (laaS). The basic structure of the cloud computing model as shown in Figure 1 ,it divided into five levels, from top t o 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.

Mr.Bhupesh Dewangan, CSE Department,, CSVTU University/CSIT Collage, Durg,India.
Mr.Praveen Shende, CSE Department,, CSVTU University/CSIT College, Durg,India.

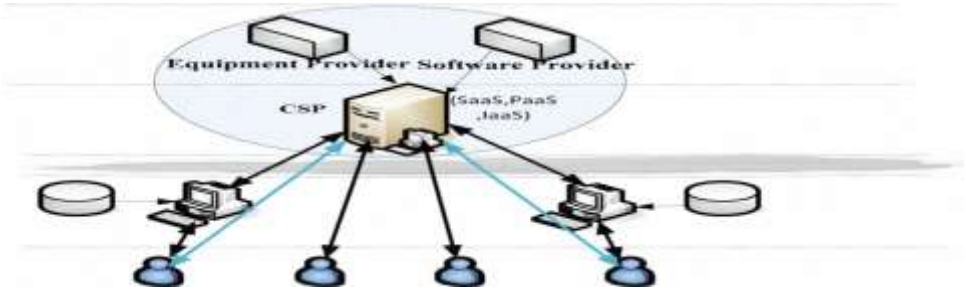

Figure 1. users and service providers in basic cloud computing architecture

1.3 Obstacles and Opportunities of Cloud Computing

The following table shows the top ten obstacles and opportunities of cloud computing.

Table1. Obstacles and opportunities of cloud computing.

No	Obstacle	Opportunities
1	Availability/Business Continuity	Use Multiple Cloud Providers
2	Data Lock-In	Standardize APIs; Compatible SW to enable Surge or Hybrid Cloud Computing
3	Data Confidentiality and Auditability	Deploy Encryption, VLANs, Firewalls
4	Data Transfer Bottlenecks	FedExing Disks; Higher BW Switches
5	Performance Unpredictability	Improved VM Support; Flash Memory; Gang Schedule VMs
6	Scalable Storage	Invent Scalable Store
7	Bugs in Large Distributed Systems	Invent Debugger that relies on Distributed VMs
8	Scaling Quickly	Invent Auto-Scalar that relies on ML; Snapshots for Conservation
9	Reputation Fate Sharing	Offer reputation-guarding services like those for email
10	Software Licensing	Pay-for-use licenses

Despite of these obstacles as well as opportunities and advantages, cloud computing raises several security issues and hence security is still the primary concern of many customers who want to leverage public cloud services.

II Litetreture Review

TRUST NEEDS FOR THE SERVICE PROVIDERS AND USERS IN CLOUD COMPUTING

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 user trust providers, this is current important research content of the most researchers.

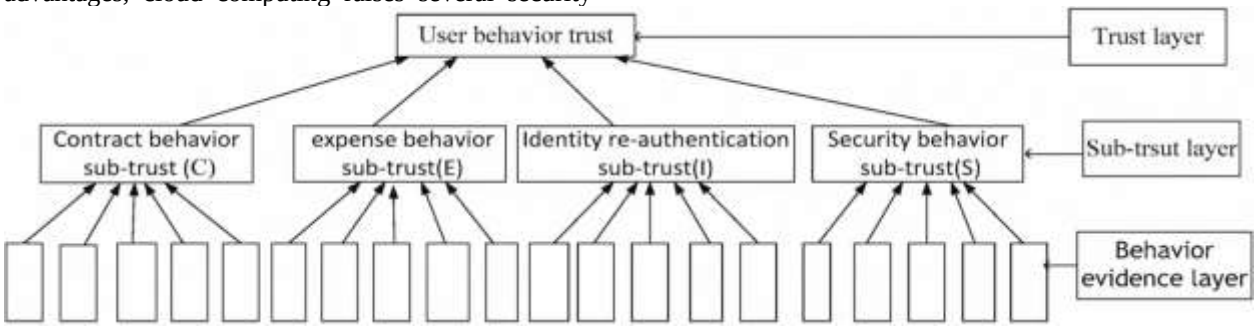

Figure 2. user behavior trust evaluation Hierarchy in cloud computing

III. METHODS FOR EVALUTION STRATEGY

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

1) Network flow detection tool, such as Bandwidthd [5], 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[6], 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 [7], 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 [8], it provides nearly real-time traffic monitoring and multicriterial 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 [9];

6) Using hardware to get evidence directly such as NetScout's, nGenius hard Probes[10];

7) The information reproduced by other security product, such as Firewalls, access control system and other evidence Network monitors[15].

IV. SOLUTIONS FOR EVALUTION STRATEGY

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)[15]. 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[11].

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 (F AHP) based on triangular fuzzy numbers to weaken AHP's subjectivity, which makes the evaluation results more objective. Detailed evaluation steps see[12].

C. FANP based Evaluation strategy for each access

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 (F ANP) 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[13].

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 tmerelated, 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[14].

V RESULT

Security Scheme	Suggested Approach	Strengths	Limitations
Data Storage Security[16]	Uses homomorphic token with distributed verification of erasure-coded data towards ensuring data storage security and locating the server being attacked.	1. Supports dynamic operations on data blocks such as: update, delete and append without data corruption and loss. 2. Efficient against data modification and server colluding attacks as well as against byzantine failures.	The security in case of dynamic data storage has been considered. However, the issues with finegrained data error location remain to be addressed.
User identity safety in cloud computing	Uses active bundles scheme, whereby predicates are compared over encrypted data and multiparty computing.	Does not need trusted third party (TTP) for the verification or approval of user identity. Thus the user's identity is not disclosed. The TTP remains free and could be used for other purposes such as decryption.	Active bundle may not be executed at all at the host of the requested service. It would leave the system vulnerable. The identity remains a secret and the user is not granted permission to his requests.
Trust model for interoperability and security in cross cloud[17]	1. Separate domains for providers and users, each with a special trust agent. 2. Different trust strategies for service providers and customers. 3. Time and transaction factors are taken into account for trust assignment.	1. Helps the customers to avoid malicious suppliers. 2. Helps the providers to avoid cooperating/serving malicious users.	Security in a very large scale cross cloud environment is an active issue. This present scheme is able to handle only a limited number of security threats in a fairly small environment.
Virtualized defence and reputation based trust management	1. Uses a hierarchy of DHT-based overlay networks, with specific tasks to be performed by each layer. 2. Lowest layer deals with reputation aggregation and probing colluders. The highest layer deals with various attacks.	Extensive use of virtualization for securing clouds.	The proposed model is in its early developmental stage and needs further simulations to verify the performance.
Secure Virtualization[18]	1. Idea of an Advanced Cloud Protection system (ACPS) to ensure the security of guest virtual machines and of distributed computing middleware is proposed. 2. Behaviour of cloud components can be monitored by logging and periodic checking of executable system files.	A virtualized network is prone to different types of security attacks that can be launched by a guest VM. An ACPS system monitors the guest VM without being noticed and hence any suspicious activity can be blocked and system's security system notified.	System performance gets marginally degraded and a small performance penalty is encountered. This acts as a limitation towards the acceptance of an ACPS system.
Safe, virtual network in cloud environment[17]	Cloud Providers have been suggested to obscure the internal structure of their services and placement policy in the cloud and also to focus on side-channel risks in order to reduce the chances of information leakage.	Ensures the identification of adversary or the attacking party and helping us find a far off place for an attacking party from its target and hence ensuring a more secure environment for the other VMs.	If the adversary gets to know the location of the other VMs, it may try to attack them. This may harm the other VMs in between.

Table 2: Comparative Analysis for Strengths and Limitations of Some of the Existing Security Schemes

V. CONCLUSION

Paper 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 of trust for the practical cloud computing application

REFERENCES

[1]Survey on Cloud Computing Security**,** Shilpashree Srinivasamurthy,*Department of Computer Science,Indiana University – Purdue University Fort,Wayne,Fort Wayne, IN 46805,srins01@students.ipfw.edu*

[2] The NIST Definition of Cloud Computing, version 15, by Peter Mell and Tim Grance, October 7, 2009, National Institute of Standards and Technology (NIST), Information Technology Laboratory (www.csrc.nist.gov)

[3] Wang, Lizhe; von Laszewski, Gregor; Kunze, Marcel; Tao, Jie. Cloud computing: A Perspective study, *Proceedings of the Grid Computing Environments (GCE) workshop. Held at the Austin Civic Center: Austin, Texas*: 16 November 2008.

[4] Michael Armbrust, Armando Fox, Rean Griffith, Anthony D. Joseph, Randy Katz, Andy Konwinski, Gunho Lee, David Patterson, Ariel Rabkin, Ion Stoica, Matei Zaharia. A view of cloud computing. *Communications of the ACM , Volume 53 Issue 4*, pages50-58. April 2010.

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

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

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

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

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

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

[11] 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.
[12] Guo Shukai,Tian Liqin, FAHP-based User Behaviour trust Computation Tactics. Computer Engineering and Applications,acccepted.
[I3] 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
[14] TIAN Li-qin, LIN Chuang. A Kind of Evaluation Mechanism on User Behavior Trust Based on Double Sliding Windows, Tsinghua University Joumal,201O.1O.
[15] LIN Chuang, Evaluation of User Behavior Trust in Cloud Computing, Department of Computer Science and Technology,Tsinghua niversity,Beijing,China
[16] Cong Wang, Qian Wang, Kui Ren, and Wenjing Lou, "Ensuring Data Storage Security in Cloud Computing", 17th International workshop on Quality of Service,2009, IWQoS, Charleston, SC, USA, pp.1-9, July 13-15, 2009, ISBN: 978-1-4244-3875-4.
[17] Shantanu Pal, Sunirmal Khatua, Nabendu Chaki, Sugata Sanyal, "A New Trusted and Collaborative Agent Based Approach for Ensuring Cloud Security", Annals of Faculty Engineering Hunedoara International Journal of Engineering (Archived copy), scheduled for publication in vol. 10, issue 1, January 2012. ISSN: 1584-2665.
[18] Flavio Lombardi, Roberto Di Pietro, "Secure Virtualization for Cloud Computing", Journal of Network and Computer Applications, vol. 34, issue 4, pp. 1113- 1122, July 2011, Academic Press Ltd. London, UK.

Mr. Bhupesh Kumar Dewangan, received B.E. (Computer Sc.) in year 2005 and in pursuit for M.Tech. (Computer Sc.) From Chhatrapati Shivaji Institute of Technology(CSIT), Durg, Chhattisgarh, India, His interests are Digital Image Processing, Cloud Computing and Data Mining. Also he is having Life Membership of Indian Society of Technical Education, India (ISTE) and Member of Computer Society of India (CSI).

Praveen Shende, received B.E. (Computer Sc.) in year 2009 and in pursuit for M.Tech. (Computer Sc.) From Chhatrapati Shivaji Institute of Technology (CSIT), Durg, Chhattisgarh, India, His interests are Programming Languages(Java, PHP, Zoomla), Cloud Computing and DBMS, Computer Networks, Computer System Architecture.