IJREAT International Journal of Research in Engineering & Advanced Technology, Volume 1, Issue 1, March, 2013
ISSN: 2320 - 8791
www.ijreat.org

Avoiding Unauthorized Access by User Behaviour Analysis in Cloud Computing

M.Praveenkumar[1], R.S.Hemachandran[2] and D.Thaamaraisellvan[3]

[1,2,3] Department of Information Technology, Adhiparasakthi Engineering College, Melmaruvathur-603319, Tamil Nadu, India.

Abstract

Cloud computing is used in various places due to its various features. As it is widely used there are also some threats to cloud computing in which security and creditability always have a major concern [2]. In cloud, Users directly access every resource from the centralized storage system, that brings major effect to them rather than using traditional internet system. The user will login to cloud by using user name and password. Once he login to his account he will have full access to his account. We will not ensure the creditability of the user after he had been authenticated. There are some situations where false authentication is possible due to password leak. In this situation we cannot stop the intruder to access the account without any restrictions by the user at the time of registration [4]. Hence this paper presents the concept of user behavior authentication[1], discusses how to authenticate and control user behavior in the cloud computing environment according to the user's behavior, include establishment of behavior authentication set, mechanisms of behavior authentication and control, corresponding mode of Stochastic Petri Nets, False Negative rates and algorithm performance etc.

Keywords:*Cloud Computing, Behavior Authentication analysis, Authentication Mode, Property Analysis, Re-authentication.*

1. Introduction

The cloud is the next stage in the evolution of the Internet. It provides the means through which everything from computing power to business processes to personal collaboration is delivered to you as a service wherever and whenever you need it. At the same time, cloud computing can also reduce operating costs, improve operational efficiency. 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 cloud consists of five layers that are known as resources provide layer, cloud services provide layer, information transport layer, professional service provider layer, end user layer from the bottom. The cloud service layer integrates the services of the cloud and provides them to the users.

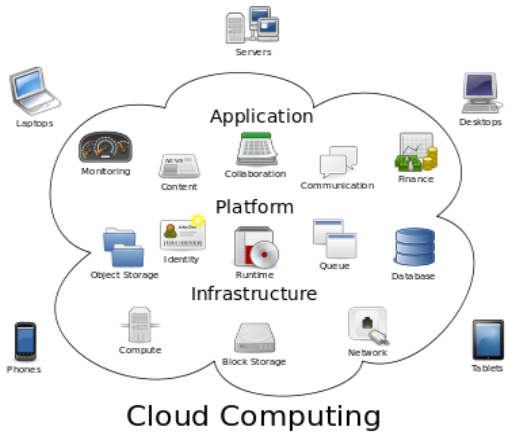

Fig.1 Basics of cloud

This is the basic structure of cloud in various applications. It also have various issues need to be solved of which authentication will have a major concern [2]. The authentication will have a fairly mature technology, but we cannot hold back the phenomenon of failed authentication due to some user's subjective reasons like password leak.

Some reasons are:

1) Mismanagement of passwords.
2) Easy to guess by others.
3) Through public relations
4) Password stealing
5) by using the phishing sites.
6) Loss of the cell phones which they use to login often.

Due to this authentication is perfect but it will not ensure the creditability of the user. This will be a tremendous problem in cloud computing. So we combine the user authentication with user behavior for checking whether he is the lawful owner. We confirm this by checking whether the behavior is consistent with Behavior body accreditation. We will not ensure whether the user is credible even if he is successfully authenticated [1]. We often see some account has been closed due to inappropriate behavior. Every year a list of students name was published by Tsinghai University Library due to their inappropriate behavior. Some other reasons for false authentication is due to Not Trust User(NTU) like a person who left the company but not give up his authority. There are some situations where the

original user itself incredible. Therefore, the credibility of user behavior must also be certified, it is called Behavior Credible Certification[1].

2. Behavior Authentication Set

Definition 1:

User behavior authentication is the validation process subjective to the user subject. The service provider will get the user preferences and the user behavior evidences during the time of registration which will be used for verification of user behavior later. User will use the legal channels to get recover their username and password so the cheater will look to get the maximized benefits as soon as possible.

2.1. Different Behavior abnormal

(1) Behavioral state abnormal: There are some situations where the state of the user will vary from his regular authentication state. If the behavioral state changes require re-authentication identity. We call this set of behavioral state as the behavioral state authentication set T[1];

(2) Behavioral content abnormal: Content of the user will not be the same for every user. We call this set of behavioral content as behavioral content authentication set C.

(3) Behavioral habit abnormal: Every user will have their unique behavior in their habits. User's habit will vary up to a certain level with every user. We call this set it's used to check behavioral habit abnormal as behavioral habit authentication set H

(4) Behavioral security abnormal: Some user will try to get major security issues. According to the current intrusion detection rules, we can gain the behavioral security authentication set S.

(5) Behavioral contract abnormal: Some users will try to violate the user behavior. At this time, we also need to authenticate the behaviors, we call this set it's used to check behavioral contract abnormal as behavioral contract authentication set Q. So we need to have behavior security collections which can be used as a verification proof. There will be no history of records for newly registered users, so the behavior authentication set T, C and H are empty sets.

Definition2:

Set of sufficient behavior authentication (SU), I f authentication fails based on a authentication set SU, which certainly results in user behavior authentication failure, but, If that user behavior authentication failure is not necessarily due to authentication failure based on the authentication set, then we call SU Set of sufficient behavior authentication, in the above authentication sets, S and Q is SU.

Definition 3:

There will be a set of necessary behavior authentication(NE),If the authentication have to be succeed It will be based on NE, then we call NE Set of sufficient behavior authentication, in the above authentication sets, T, C and H is NE.

3.Main Idea of user behavior authentication and control

3.1. The Process of user behavior authentication

Of behavior authentication includes the following three major process:
(1)Before user accessing the ISP, there have three behavior authentications, namely the user Identity authentication(AI), behavior state authentication(AT) and behavior authentication predictions based on historic authentication(AP).If the behavior prediction is successful they will be allowed to proceed further or else it will have a subsequent game risk analysis for decision-making. Prediction is based on the principle of Bayesian networks; the following prediction formula is an example of security behavior authentication:

$$p(T/S)=\frac{p(S/T)p(T)}{p(S)}=\frac{\frac{|S\cap T|}{|T|}\frac{|T|}{n}}{\frac{|S|}{n}}=\frac{|S\cap T|}{|S|} \quad (1)$$

Where T and S respectively represent the results of overall behavior authentication and behavior
Security authentication, n is the number of statistics.
(2) The user will have four real time behavior authentication to access the ISP, namely behavior habit authentication (AH), behavior securityauthentication (AS),behavior contentauthentication (AC) and behavior contract authentication (AQ).
(3) After user accessing the ISP, here has total behavior authentications (AA) and updating of authentication grade, which make preparation for the future behavior authentication and game control of accessing. The user

behavior authentication will have another state namely uncertainty state other than true or false state in the identity authentication. The following figure represents the basic real-time strategy of behavior authentication.

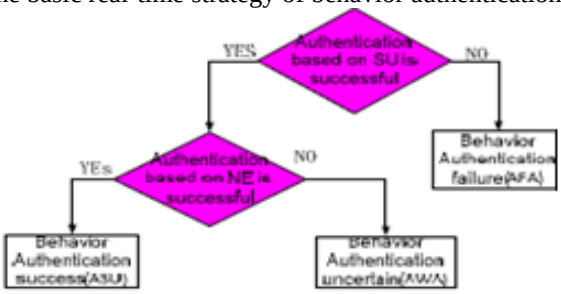

Fig.2Behavioral analysis

3.2. Strategy of Behavioral control takes control measures according three different authentication results:

(1) For user of authentication failure, ISP break through the TCP connection and other methods to interrupt the user's continued access to server.
(2) For user of authentication success, ISP allow user continue access to server.
(3) For user of authentication uncertainty, If no re-authentication for behavior subject, It will ask few security questions to the users (Which were given by him during the time of registration) for which he has to answer in order to continue to access, otherwise the game risk decision to be needed to decide whether to allow user continue to access. Basis of game making [4] is: if ISP's benefits obtained:

$$f_{ben} = -y^{*} Sloss_{acc}^{dec} + (1-y^{*}) Sincome_{acc}^{n\_dec} > 0 \quad (2)$$

Then allow user continue to access, else refuse to access. Where y^{*} and $1-y^{*}$ is respectively the mixed Nash equilibrium strategy of users do not deceiving and deceiving, *dec*0*acc Sloss* is average loss when ISP receiving the user's cheat accessing, *n _ decaccS income* is average normal earnings when ISP receiving the user's no cheat accessing.

4. Model of user behavior authentication and control

4.1. Stochastic Petri Net model of user behavior authentication and control:

As the user's behavior is random, authentication process is concurrent, so we select SPN to describe User behavior. The SPN model of user behavior authentication step and the corresponding control process shown in Figure 3, where three different colors represents three different time authentication periods. Green represents authentication before the behavior; purple represents authentication in the behavior; orange represents authentication after the behavior. Description of transition and status see Table 1.

1. Transition t1 denotes the user access in the SPN model;
2. Transition T2 accepts user accesses in the SPN model;
3. Transition T3 denotes User identity authentication in the SPN model, if identity authentication success, then gain user behavior state with the transition t6 to denote;
4. Full behavior authentication after the behavior, including gain user behavior evidence t50, make behavior authentication concurrently t51---t5n;
5. Determine trust of behavior authentication with the transition t22 to denote, If successful update trust authentication set or don't update it with the transition t23to denote;
6. Transition t7 denotes the Behavior state authentication in the SPN model
(1)If behavior state authentication fails, then make identity re-authentication by asking security questions.
(2)Identity re-authentication with the transition t9 to denote, If it fails, then stop accessing, else whether to continue to access through the game risk analysis for decision-making and turn to t10;
(3)If behavior state authentication success, then make behavior authentication prediction with t24 denotes to get historical authentication results, t25 denotes authentication prediction.
7. Real-time behavior authentication with the transition t11 to denote, regularly gain user behavior evidence with the transition
t12.
8. The real time authentication will have one of the following actions.
(1) Make real-time behavior authentication based on SU, including authentication based on behavior security and contract, with the transition t140 and t141 respectively;
(2) Make real-time behavior authentication based on NE, including authentication based on behavior habit and behavior content, with the transition t130 and t131 respectively;

9. Confirm authentication based on SU with the transition t20 to denote; If authentication fails based on one of set SU, which results in user behavior authentication failure, stop user access, to t4; If authentication success based on all set SU, making behavior authentication based on NE with the transition t15 to denote;
(1) If authentication success based on all set NE, allow user continue to access, turn to t16;
(2) If authentication not success based on all set NE, which show that the abnormal behavior may occur, requiring further
Decision-making with the transition t18 to denote;
10. Confirm if had identity re-authentication before with the transition t19 to denote, if had it before then don't have identity re-authentication
Again and turn to t10 to make risk decision-making based on game theory. If had no it before then make identity
Re-authentication and turn to t8
11. Check user access state with the transition t17 to denote, if the user does not continue to access the system, turn to t4 and end user
Access or turn to t12 and continue access;
12. Decision-making based on game theory with the transition t10 to denote; if result of decision-making is refusing access then interrupts user access or turns to t16 and continue access.

4.2. Effect and Performance Analysis

With the SPN theory, we can analyze the efficiency of behavior authentication and performance and prove the characters of reachability.
(1) Analysis of False Negative rate of behavior authentication which refers to the ratio of no success of behavior authentication, Lead to False Negative of identity authentication may be due to subjective reasons such as losing password; If two different users have same operating system and IP address it may also leads to false negative of behavior state authentication and also if two users request same kind of service False Negative of behavior security authentication may be due to user scan port, modify file permissions or user's excessive downloading files. As the direct control action of behavior authentication only has five, namely, identity authentication, identity re-authentication, behavior security re-authentication, behavior contract authentication and risk decision based game theory. Let the five False Negative rates of authentication control respectively is *I p, I p,S p,Q p* and *G p, then* False Negative rates of behavior authentication *p* is:

$$h = h^{I} * h^{R} * h^{C} * h^{O} * h^{S} \quad (3)$$

From the above analysis we can see, when increase behavior authentication, False Negative rates of user authentication will greatly reduce. The rate of reduction is * * * *RI G Q S p ppp*.

(2) Analysis and Improvement of behavior authentication performance:
In above model, there have two parallel processes, namely (t51-t5n) and (t130-t140 ...), we can calculate performance equivalent. It has one iteration process, namely (t12-t20-t15-t18-t19-t10-t16-t17-t12), we can calculate performance equivalent there have ten choice processes, we can calculate performance equivalent
By these simplification we can be calculate total model equivalent time. The behavior authentication works by comparing the behavior evidences with the user behavior. Firstly, we standardize different scope and size of behavior authentication evidence before behavior. The evidence expression being specific value within certain scope can be converted into new evidence expression within [0,1] by the piecewise programming statement:
Here max et is the largest value and min et is the smallest value among all evidences. Now all the evidences are expressed within [0, 1] and increase along the positive direction. Secondly, because of the number of user behavior authentication failure is less than the number of user behavior authentication success, to improve the search speed, make ascending order according to deviation degree of abnormal behavior in set of behavior authentication. Third, in order to improve the efficiency of behavior authentication, as long as identity re-certification successful it is no longer repeated.

5.Overall module

The user behavior authentication process will consists of set of process which need to be followed in order to provide access mechanism to the user allow him to continue further.

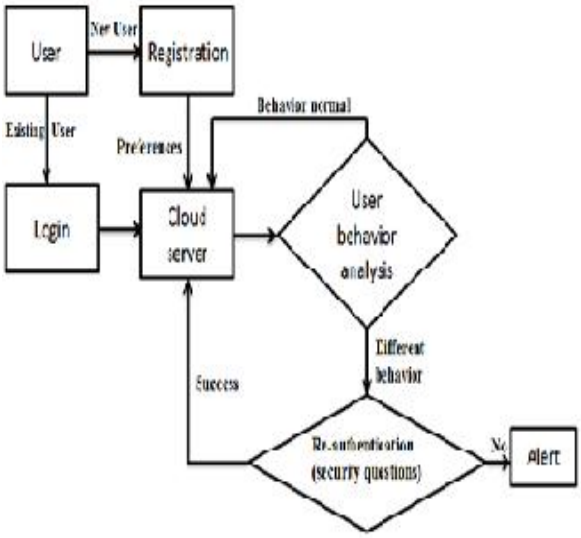

Fig.3 Flow chart

The above figure represents the overall process of the system. Which we need to be do in the user behavior authentication process.

6. Reauthentication and alert

In this, we need to re-authenticate the user if the user behavior has been differs from his original behavior. The preferences of the user and the security questions will be given by the user at the time of user registration[3][6]. Once the user behavior differs from the original behavior the system prompts for re-authentication by means of security questions. If he answers the question he will be provided access to proceed further or else an alert message will be sent to the user and restrict him to access the server further and he will be logged off.

7.Conclusion

The user behavior authentication will be an efficient way to find the creditability of the user and also restricts the hacker/intruder to access the account up to certain level. This method is easy to implement and also reduces the false negative authentication. This system can be added to the existing technology to provide more security to access the cloud computing environment. Hence this system will provide an efficient way to reduce the improper access to the cloud computing environment.

References

1] A kind of user behavior authentication model and analysis in cloud computing by TIAN Li-Qina, b ,*, LIN Chuangc, Ni Yangb, Duxiujuana in science direct 1876-6102 © 2011 Published by Elsevier Ltd. Selection and/or peer-review under responsibility of Singapore Institute of Electronics doi:10.1016/j.egypro.2011.11.590.

2] DaweiSuna,*, GuiranChangb, LinaSuna and XingweiWanga:Surveying and Analyzing Security, Privacy and Trust Issues in Cloud Computing Environments published at 1877-7058 © 2011 Published by Elsevier Ltd. doi:10.1016/j.proeng.2011.08.537

3] A survey on security issues in service delivery models of cloud computing S. Subashini n, V.Kavitha 1084-8045/$ - seefrontmatter& 2010 ElsevierLtd in the Journal of Network and Computer Applications

4] Zhiqiang Fan, Li Zhang, JufangShen, Shouxin Wang: A User's Preference based Method for Web Service Selection in Second International Conference on Computer Research and Development
978-0-7695-4043-6/10 $26.00 © 2010 IEEE DOI 10.1109/ICCRD.2010.34.

5] A survey on gaps, threat remediation challenges and some thoughts for proactive attack detection in cloud computing by Md. TanzimKhorshed, A.B.M. Shawkat Ali ∗, Saleh A. Wasimi in the international conference in future generation computer systems.

6] Knowing the past to understand the present1 e issues in the contracting for cloud based services Andrew Joint*, Edwin Baker in computer law & security re view 27(2011)407e415.

7] Chris Couch, COO of Transverse e printed from BillingViews