ACCFLA: Access Control in Cloud Federation using Learning Automata

Behnaz Seyed Taheri
Department of Computer Engineering, Mahallat Branch, Islamic Azad University, Mahallat, Iran

Mostafa Ghobaei Arani
Department of Computer Engineering, Parand Branch, Islamic Azad University, Tehran, Iran

Mehrdad Maeen
Department of Computer Engineering, Yadegare Imam Khomeini (RAH) Branch, Islamic Azad University, Tehran, Iran

ABSTRACT

In recent years, cloud computing has been applied increasingly and most of the companies, have considered some kinds of cloud strategies to use in their organizations. Growing request for services causes overload on a single cloud. Cloud federation is an ideal solution to overcome continuous increasing requests by users. Identity management and access control are from challenging subjects of cloud federation which for has been offered approaches like identity federation, although it is not an optimum approach. There is needed a more effective, accurate and safe approach. This paper offered an approach to access control based on risk and trust parameters, depending on learning automata in cloud federation. Results of simulation shows that proposed approach prevents access of unauthorized user to the resources of federation by decreasing primary trust for novice user also by increasing risk for high sensitive resources.

Keywords

Cloud Computation, Access Control, Cloud Federation, Learning Automata.

1. INTRODUCTION

Cloud computing is currently one of the most popular technologies and developing a successful example of distributed computing. Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (networks, servers, applications, and services, etc.) that quickly with minimum effort management or service provider interaction of supply and release dates [1]. In another definition, cloud computing, refers to both Applications are provided as services over the Internet and also the hardware and systems software in the data centers that provide a service.

A single cloud, with an increase in service requests from clients, encounters to overload and reduces performance. To enhance the capabilities of the cloud, inter-operability among the clouds seem necessary. If the interaction takes place between the clouds, Both users and providers, it will be a win-win situation, so that on the one hand, users request will be meet and On the other hand, Providers may be earn income of their idle computing resources[3].

One of the inter-operability clouds Cases, is the creation of federation between clouds. Cloud Federation, when home cloud overload is incurred, it focuses on borrowing computing resources from external cloud as well as when home cloud is free , it focuses on renting resources to external clouds. in fact, it is an approach for collection different clouds In order to share resources and data to increase scalability and availability, and enable message transfer and cooperation between the clouds, so that existing resources in different cloud platforms, can provide services for a service and with solving the problem of overload on a single cloud, responds to more user requests [4]. Due to the increasing number of users to create a federation of clouds, the development of methods for authentication and access control, privacy, and confidentiality of distributed environments, dynamic and heterogeneous requirements. One common approach to management and authentication, is creating identity federation. Identity federation is a type of identity management in which identity providers and service providers share user identity in safe circle. Difference between identity federation and Cloud federation, is, cloud federation is creating by resources sharing but identity federation is creating by user sharing and information sharing [5-7].

Today, identity Federation cannot be properly accountable to cloud users because in identity federation to communicate, needed to previous security negotiations or, in other words, to security signing an agreement. This prevents the dynamic cooperation between clouds, on other hand, from other problems this approach, are limited scalability and flexibility that Causes cloud identity fails in response to increasing development cloud federation users. Communication and cooperation between the clouds, the last of which has advantages, has challenges such as securing resources and information to follow. Therefore, more secure approach, more accurate and of course easier to control access to resources in the cloud federation is required to users and their clients ensure the resources and their vital information have protection against the unauthorized users. This paper offers a developed approach for dynamic access control using learning Automata. Our proposed approach, remove necessity of Identity federation and uses only two metrics, trust and risk, for decide to grant/deny access request to resources.

The remainder of this paper is organized as follows: Second section introduces access control in cloud federation and the third section is devoted to related work. In fourth section, the learning Automata is described, in fifth section our proposed approach is presented. Sixth section is devoted to evaluation of the proposed approach and finally, conclusions and future work are discussed in seventh section.

2. ACCESS CONTROL IN CLOUD FEDERATION

Due to increasing users of cloud federation and importance of controlling users in access to exist resources in cloud federation, developing approaches to authentication and access control for cloud federation environment is necessary. Tools and methods of access control ensure that network users and information resources accessed only by authorized personnel and are protected from unauthorized use [8].

Access control actually is a policy which authorizes to access a system, designates or limits it, also controls and records all activities toward access a system. in addition it discovers identity of users who tries to have unauthorized access to system. The mechanism is vital for security and preservation of various kinds of networks. Access control compromises from two respective stages of identification and authorization. Accomplishing the two mentioned stages meet in all models of access control [9].

The first stage is confirming identities. It means identifying users carefully and successfully. In this stage user should introduce him/ herself. The question of this stage is" who are you?" and users should introduce themselves in response of it showing documents of identification like username , password, digital signature, ID card or anything else. In recent years confirming identification has got easier. Most of the operational systems or programs use technologies like Active Directory, LDAP, SSO.

Second stage reviews users' licenses. In this phase the entire of user's allowed activities will be recorded. User should offer licenses, certificates and credentials and system reviews all of them. If they would be credited, access license will be issued, user will know licensed and will be able to access the system and its resources.

2.1 Access Control Approaches

Access control approaches, depending on their use of identity federation can be classified into two general categories of access control approaches, static and dynamic access control approaches:

A) Static Access Control Methods (Classic): In these methods, identity federation is used as a medium. Clouds should implement information which prepared by system about users.one of the problems of the method is its necessity to previous negotiations and agreements. It can be very time consuming in huge and long processes. So that it prevents of dynamic interactions. Because dynamic interactions will be accomplished when entities can be united quickly to make federations without any previous agreements or negotiations. These methods encounter problems included lack of flexibility, scalability and lacking adjustment with immediate changes in dynamic cloud environment. Of the most common methods are ABAC and RBAC [10].

B) Dynamic Access Control Methods: Dynamic access control methods are applied to have more flexible access control showing current changes to share information and resources. Dynamic methods compared to static ones, works based on predefined policies to review decision making for access when a subject requests to access to an object). One of the most common methods is Risk-based access control. So the risk of allowing access will be measured. If the risk is less than standard level, so that Permissions Access Will be granted. [11].

3. RELATED WORKS

A variety of approaches to access control in cloud computing has been proposed in this section, it reviews Some of these works that more closer to our proposed approach. McGraw [12] has proposed a Risk-Adaptable Access Control (RAdAC) mechanism. Firstly, the system determines a security risk associated with granting access. Secondly, the system compares the measured risk with the access control policy that identifies the acceptable level of risk for the object being accessed. Thirdly, the system verifies the operational need. If all the requirements for operational need, as specified in the policy, are met then access is granted. RAdAC provides a high-level infrastructure for the granting of exceptions, but it does not itself contain a risk model. The author does not provide details about how to quantitatively measure risk and operational need.

Zhang and colleagues [13] suggested Benefit and Risk- based Access Control model. In the model transactions are based upon benefit and risk vectors. According to configuration there is an allowed transaction graph. If total benefit in system would be higher than risk and it provides special features of graph, so that transactions will be allowed. Situation is usually static and updating a situation causes to increase the problems.

BARAC is an access control model based upon adjustment risks of revealing information and advantages of sharing information. Configuration of the model depends on risk and advantages vector according to any time reading and updating the transaction.

Cheng and colleagues [14] suggested Fuzzy MLS access control model. The model determines amount of risk related to access. System controls high risks information drives according to current operational necessity, error tolerance and risk of environment. They compute risk according to value of information and possibility of their unauthorized revelation. Qun Ni et al. [15] have proposed risk-based access control systems based on fuzzy inferences. They show that fuzzy inference is a good approach for estimating access risks. They introduce fuzzy membership functions for subjects and objects. In order to implement risk-based BLP systems to satisfy simple security properties, they introduce predefined "if antecedent then consequent" rules. For example, if the subject security label is not unclassified and the object security label is classified, then the access risk is low. In both these works, the past behavior of users is not considered to measure risk. Kelly and colleagues [16] suggested Role-Based Access Control model. Access control based on role named RBAC which allows user to have access to the resources according to predefined levels of access for a special role in organization. In this situation persons have essential access according to their roles in the organization.

Ahmed and colleagues [17], offered dynamic approach to risk-based access control (DRAC), based on risk and trust parameters. This approach is used when the user requests a resource from an external cloud. When a user requests a resource, a binary (Subject, Object) are formed. The first component represents the user's trust to resource, the second component represents the amount of risk assignment from the resource to the user, as a result, in this approach calculated to risk and trust, is necessary and vital. Also history users in using resources recorded and according to them, reward or penalty, to be assigned to them. In this approach, risk assignment resources to each user been evaluated, if the amount of risk, the system is considered a threshold is exceeded, the request will be denied access or otherwise access license is issued.

Wang and Jin [18] have proposed a quantified risk-adaptive access control method to protect patient privacy in health information systems. In their model, accessing information (irrespective of whether it is public or highly confidential) that is not required for one's job leads to a high risk score, while accessing relevant information results in a low one. In their model, relevance between medical record and a purpose is determined with a relevance-relation function θ. The authors have mentioned in their paper that the concrete form of the function θ is never known, which makes their approach less generic. Table I compares and categorized related works.

Table1. Comparison of access control approaches

Approach Name	Access control method	Mode of action	Static / Classic	Benefits	Disadvantages
RAdAC [12]	Compatible with risk	It works on computing security risk and operational needs.	Dynamic	1. High accuracy due the security risk and operational requirements in addition to the decision attributes. 2.Calculation Risk On Online	1. Availability parameters for calculating the security risk for all users. 2. Mistrust of users and threat them.
Fuzzy MLS [14]	According to Risk Based on fuzzy	Using both intentional and unintentional information disclosure probability indicator	Dynamic	Having fault tolerance, high performance	Weak probability misuse of indices
Inference Fuzzy [15]	According to fuzzy inference	The mathematical approach used to calculate risk using inference	Dynamic	Obtain unambiguous of the evidence thus combine vague and subjective knowledge and objective evidence	probability unauthorized disclosure of information Conclusion and speed time-consuming due malicious users
DRAC [17]	Based on Risk and Trust	The mathematical approach for the calculation of risk using inference	Dynamic	No need to identity federation in using external cloud resources	Need to identity federation in using home cloud resources
Estimated Compatibility Access Control[18]	Risk-based	Create a connection between medical evidence and disease severity	Dynamic	Estimating faster the severity of the disease	Only in special cases is responsive
BARAC [13]	Risk-based and Benefit-based	1. Use and update transactions and discovery transactions authorized. 2. Balance between the risk of information disclosure and sharing of information.	Static	Inability of users to delete or add transactions to increase profit	Difficulty to upgrade transactions due static
RBAC [16]	Role-based	Based on Importance user role	Static	1.Simply access control management 2.Consistent with the organizational structure	Limit scalability

4. LEARNING AUTOMATA

Learning Automata can be considered a single object that has limited number operations. Learning automata works as follows: at any time one operation among the set of actions is selected and then in a random environment is assessed and their responses will be send to the automata. The automata using this response to selected action for the next stage and thus gradually automata, will identify best practice. Learning algorithm will determine the way in which the automata using that reply environment button to select next action. Environment conditions and the external effects might impact on the automata. Automata and environment create a cycle such that the automata output (α), the input and the output (β), would be the automata input. Automata Performance can be considered a sequence of repetitive cycles in which automata interacts with the environment described.

Figure 1, show the relationship between learning automata and environment.

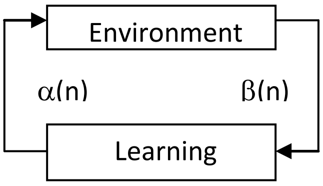

Figure 1: The relationship between automata and environment

In this automata, if action α_i is selected at stage n, and receives a favorable response from the environment, probability $P_i(n)$ related to increases and decreases the probabilities of other actions. In response undesirable, the probability p related to action reducing and probability related to other actions increases. However, changes are made in such a way that the sum is always constant and equal to one stay. Therefore, if the procedure is repeated n α_i is chosen, then the iteration n + 1 are [19-21]:

- For optimal response(β=0):

$$P_i(n+1) = p_i(n) + a\left[1 - p_i(n)\right] \qquad (1)$$

$$p_j(n+1) = (1-a)\, p_j(n) \;\; \forall\, j, j \neq i \qquad (2)$$

- For respond undesirable(β=1):

$$p_j(n+1) = (1-a)\, p_j(n) \;\; \forall\, j, j \neq i \qquad (3)$$

$$p_j(n+1) = \frac{b}{r-1} + (1-b)\, p_j(n) \forall j,\, j \neq i \qquad (4)$$

In the proposed approach, the variable n equal to the number of access requests by users and the variable r (number of actions) consists of two acts grant access or deny access request.

5. PROPOSED APRROACH

Proposed approach, without the use of identity federation and created secure circle, user behavior in the use of resources should be carefully considered. In addition, from measure risk arising from assignment resource to users and amount trust to users in correct using from resource help automata, for enforcement access Control uses and based on the Request denied access or permissions issue. Our approach Proposed risk-based offer in three parts, based -on trust, based -on risk and based-on access measure. In other words, first reviewed access control based- on metrics risk and trust separately, and in finally, described access control based -on combination of these two metrics (access control metric).

5.1 Trust-based Access Control with Learning Automata

In the proposed approach for calculation trust, first users are classified into different security levels. Then this security levels sorted according to their sensitivity to each level, that considered a variety Which represents the user's security level; as a result, security levels are mapped into a sequence of numbers. Individual in a system are classified to following security levels:

Security levels={Top Secret, Secret, Confidential, Unclassified }

ls={4,3,2,1}

In the proposed approach, user's experiences in the use of resources are considered. If the user is successful to use the resource, there will be recorded the reward and otherwise penalties for him. Hence the calculation of reward history

($H^+(s,o)$) and penalty history ($H^-(s,o)$) at each user request is required. Because trust depends to security level (ls) and history reward, as a result from equation 5 uses to calculate the amount of trust.

$$T_V = l_s \times \left[1 + H^+(s,o)\right] \qquad (5)$$

In equation (5), the reason of adding 1 to $H^+(s,o)$ is that to keep the trust at least equal to the security level of the user if the variable would be zero. To calculate variable reward history, the ratio probability of grant access to all the possibilities, equation (6) can be used.

$$H^+(s,o) = \left[\frac{P_i(n)}{\left(P_i(n) + P_j(n)\right)}\right] \alpha^{(1/(1+Pi(n)))} \qquad (6)$$

In the above equation the variable α, is the growth rate of the trust as a result of increased rewards and its amount in the interval (1, 0). On the other hand, the system defines a trust threshold, and proposed approach is based on the simulation results, equation (7) is determined.

$$T_{vo} = 1.5\, l_s \qquad (7)$$

Whenever, automata environment receives favorable response (β = 0), in fact, the desirability of a user's performance and reward them , in fact, the result is equivalent to True $T_v \geq T_{vo}$ condition. Thus, equation (8) is determined:

$$If\ \beta = 0\ and\ \mathrm{T_V} \geq \mathrm{T_{VO}}\ then \qquad (8)$$

$$\{$$

$$P_i(n{+}1) = P_i(n) + a\left[1{-}P_i(n)\right];$$

$$P_j(n{+}1) = (1{-}a)\, P_j(n) \quad ;\ i \neq j$$

$$CR = CR + 1$$

$$\}$$

As can be observed, in optimal state environment response to automata, the possibility of grant access increased and probability of deny access reduced. The variable CR, equal to the number of times that the user will receive reward Finally, if the number of reward received by the user, is less than the number of penalties received, access request is rejected, Otherwise Access license is issued. See Figure 2, this Figure shows the calculated trust by learning automata.

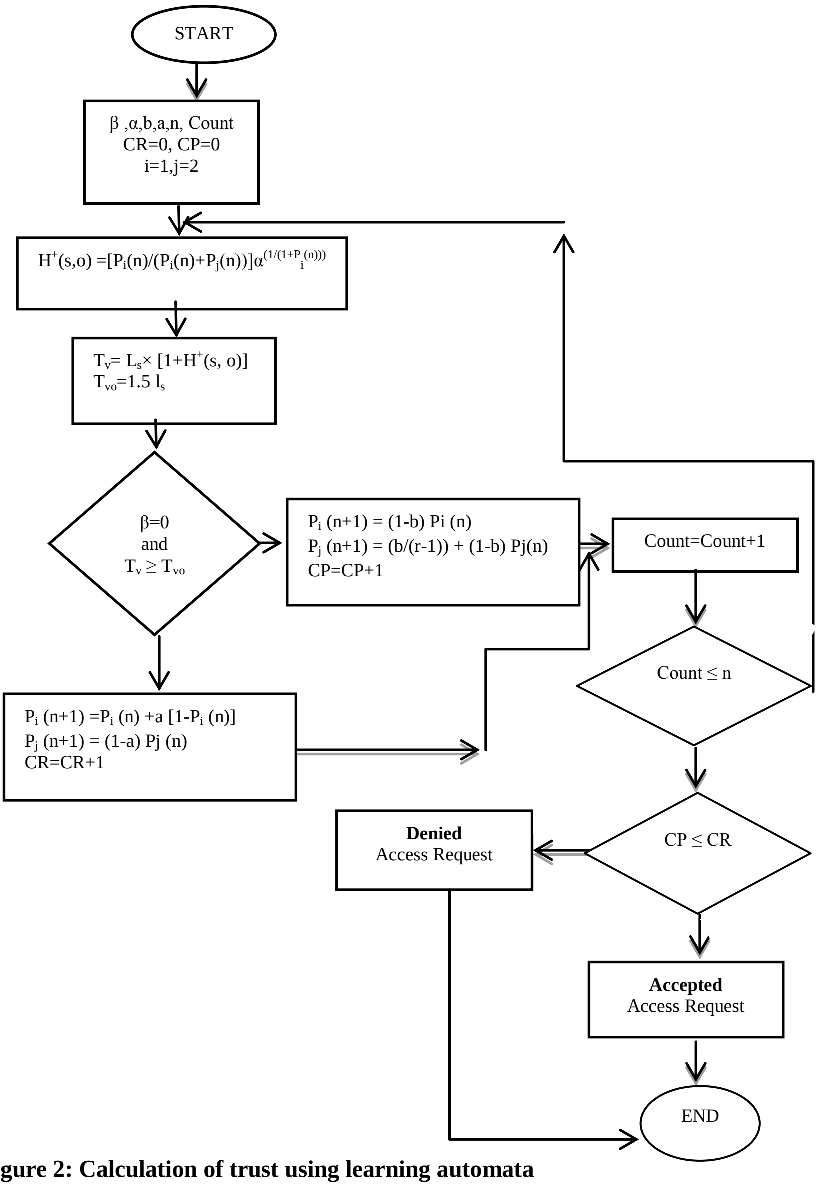

Figure 2: Calculation of trust using learning automata

5.2 Risk-based Access Control with Learning Automata

The proposed approach for calculation of risk, first resources is classified into different Sensitivity levels. Then this Sensitivity levels sorted according to their sensitivity to each level, considered a variety which represents the resources' Sensitivity level, as a result, security levels are mapped into a sequence of numbers. Resources in a system are classified to following sensitivity levels:

Sensitivity levels= {Top Secret, Secret, Confidential, unclassified }

lo={4,3,2,1}

Because the risk depends to the sensitivity of the source (lo), and penalties history (H^-(s,o)), as a result, equation (9) is determined to calculate of Risk:

$$R_V = l_o \times \left[1 + H^-\left(s, o\right)\right] \qquad (9)$$

In equation (9), reason of adding 1 to H^-(s,o) is that if this variable is zero, the risk will be at least equal to the security sensitivity level of the user. To calculate variable penalty history, the ratio probability of deny access to all the possibilities can used equation (10):

$$H^-\left(s, o\right) = \left[\frac{P_j\left(n\right)}{\left(P_i\left(n\right) + P_j\left(n\right)\right)}\right] \alpha^{(1/(1+P\ j\ (n)))} \qquad (10)$$

In the above equation the variable α, is the growth rate of the risk as a result of increased penalty and its amount in the interval (1, 0). On the other hand, the system defines a risk threshold, and proposed approach is based on the simulation results, equation (11) is determined:

$$\mathrm{R}_{\mathrm{vo}} = 1.5\,\mathrm{l}_{\mathrm{o}} \qquad (11)$$

Whenever automata receives undesired response from environment (β = 1) actually refers to the undesirable user performance and penalties him are recorded. The result is equivalent to the condition True $R_v \geq R_{vo}$ is. Thus, equation

(12) is determined:

$If\ \beta = 1\ and\ R_v > R_{vo}\ Then\ \{$

$$P_i(n+1) = P_i(n) + a\,[1 - P_i(n)] \qquad (12)$$

$$P_j(n+1) = (1-a)\,P_j(n) \quad \forall\ \text{j},\ i \neq j$$

$$cp = cp + 1$$

$\}$

As can be observed in the undesirable response to automata likely not to grant increases and decreases probability of grant access. Variable CP, penalties equal to the number of times that the user receives. Finally, if you get penalties by the user count is less than the number of reward received access request is rejected; otherwise it is a permissions issue. See Figure 3, it shows Figure calculation risk using learning automata.

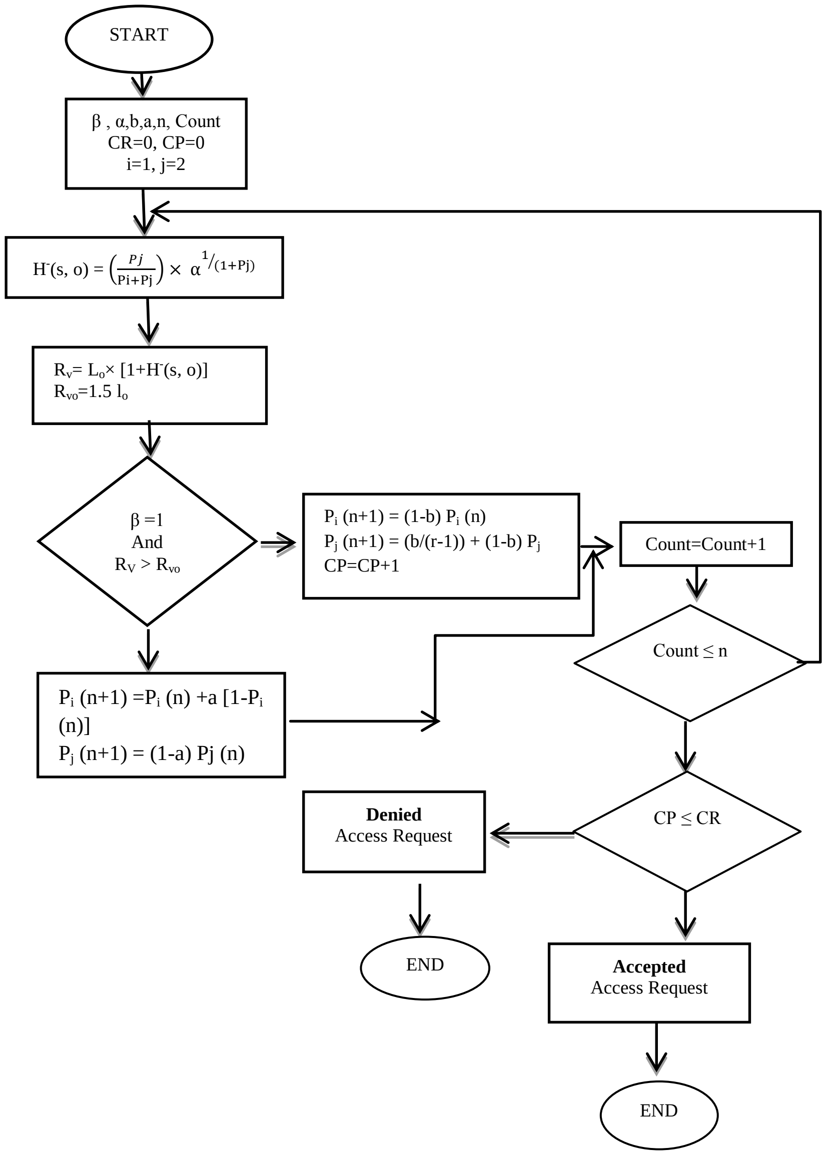

Figure 3: Calculation risk using learning automata

5.3 Metric –based Access Control with Learning Automata

This Section uses combined access parameter in order to consider connection between metrics of risk and trust. So there is dedicated a value of weight for risk and trust which their total sums always will be 1. The weights (W_1, W_2) will be calculated according to risk-based or trust-based access controls. So that W_2 will be larger than W_1, if it is studied according to risk-based and vice versa. If the calculated measure is smaller than (T_{vo}), access request will be rejected otherwise it will be allowed. See Figure 4, it shows the Figure of calculation of combined access parameter using learning automata which is calculated according equation 13.

$$A = W_1 T_V + W_2 R_V$$

$$W_1 T_V + W_2 R_V \geq T_{VO} \qquad (13)$$

$$W_1 + W_2 = 1$$

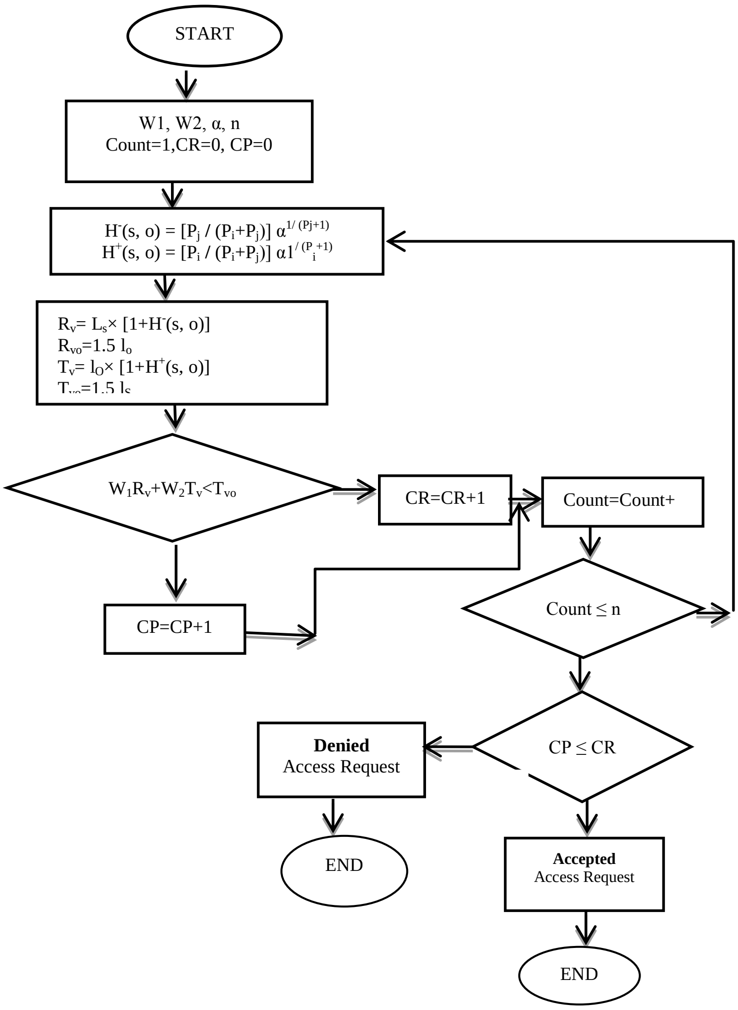

Figure 4: Calculation Acess metric using learning automata

6. PERFORMANCE EVALUATION

This paper uses Dynamic Risk-based Access Control (DRAC) to evaluate suggested approach, Access Control in Cloud Federation using Learning Automata or ACCFLA. There has been simulated and considered for 50 times the requests of users for various security levels to access resources in four different level of sensitivity. In simulation of trust-based access control using learning automata, a novice user obtains small amount of trust but because of flexibility of the approach, user is able to increase the amount of trust to gain access by having suitable behavior in using resource and getting positive response from environment. Otherwise if user is not successful in using resource or getting positive response from environment, he/she will be known as unauthorized user and will not be able to get access. Increasing user’s level of security causes to increase the situation and unauthorized users will not be able to unauthorized access to the all resources by these levels.

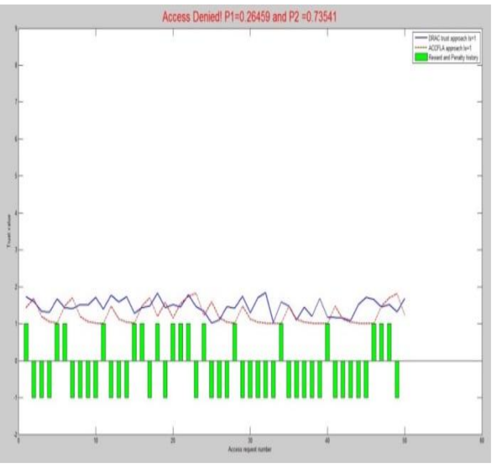

Figure 5: The trust in proposed approach with l_s=1

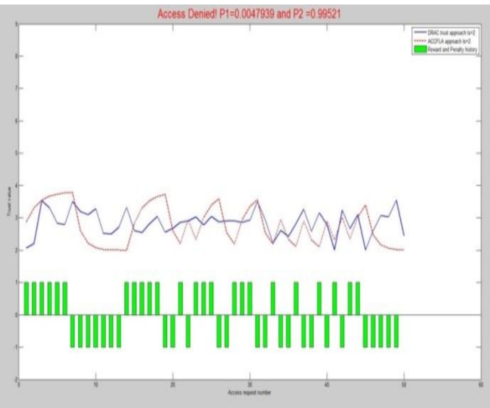

Figure 6: The trust user in proposed approach with l_s=2

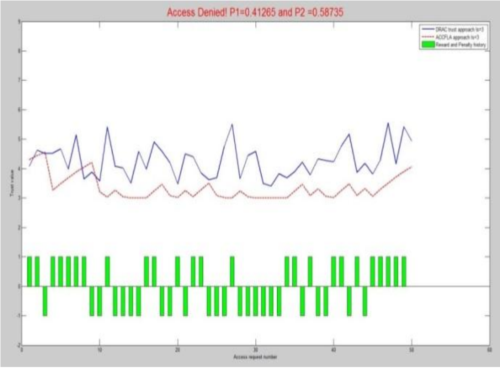

Figure 7: The trust in proposed approach with l_s=3

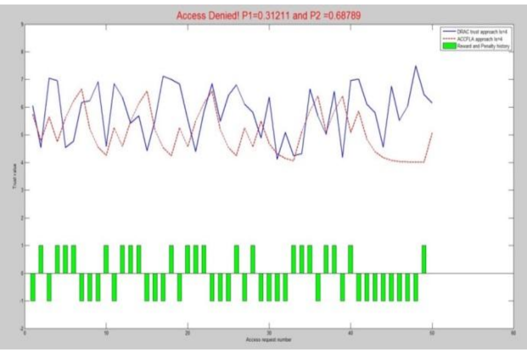

Figure 8: The trust in proposed approach with l_s=4

As you can see in Figure 5, decreasing primary level of trust causes to decrease risk of assigning resource to the unauthorized user. So increasing the number of access requests for authorized user makes a smooth Figure otherwise it will be slope. In Figures 6, 7, and 8, increasing security level of user causes to increase primary trust but if the user will be unauthorized, there will be a large decline in primary trust. The mentioned situation in user with security of level 4 can be seen obviously so authorized users do not believe that they can access to any resource without any condition. Also unauthorized users cannot access to the resource, as they think users of this group have the highest security level so they will be able to access more comfortable than any other levels. In simulated scenario for risk-based access control using learning automata, user obtains a huge amount of risk at first. So that risk of access to resource will be decreased. As if there will be an increase in calculated risk of assigning resource, it shows more confidently the user is unauthorized. Definitely user with suitable behavior will be able to obtain a smaller amount of risk compared to primary risk so the chance of access to resource will be increased and user will prove the authority. Otherwise the system suspects to unauthorized user and the access will be denied. In conclusion, in suggested approach increasing the primary risk causes to consider users' behavior more carefully so authorization of user considers more correctly and decisions making about grant or deny access will be more accurate. As it is obvious in Figure 5, increasing the primary risk of user can prevent from risk of assigning resource to user more quickly. If user is authorized, increasing numbers of request to access, proving authorization by calculated risk, cause a decreasing or horizontal Figure.

more correctly and decisions making about grant or deny access will be more accurate. As it is obvious in Figure 5, increasing the primary risk of user can prevent from risk of assigning resource to user more quickly. If user is authorized, increasing numbers of request to access, proving authorization by calculated risk, cause a decreasing or horizontal Figure.

By increasing the sensitivity of resource in Figures 10, 11 and 12, primary risk and its fluctuations will be increased dramatically. It causes more sensitive, quick and accurate recognition of unauthorized user for more sensitive resources. Because only users with less risk of granting access to them have the right of access to these resources.

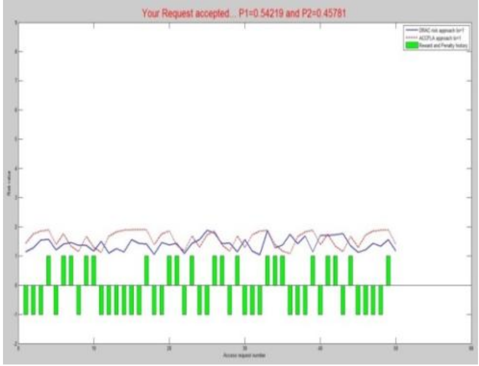

Figure 9: The amount of risk in proposed approach with l_o=1

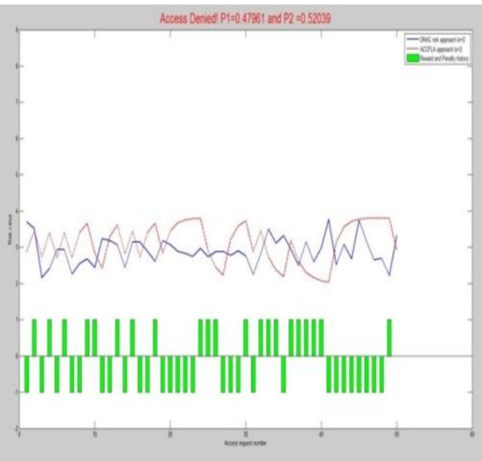

Figure 10: The amount of risk in proposed approach with l_o=2

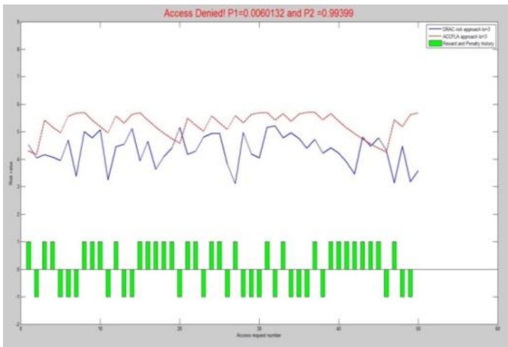

Figure 11: The amount of risk in proposed approach with l_o=3

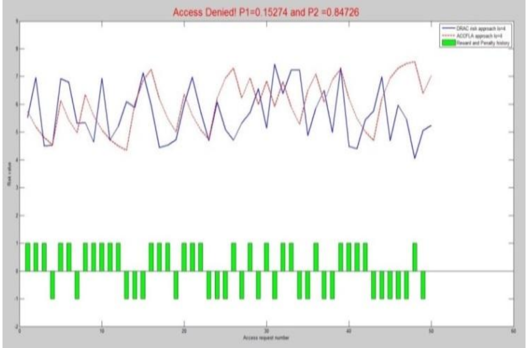

Figure 12: The amount of risk in proposed approach with l_o=4

In simulated scenario for risk-based access control using learning automata, user obtains a huge amount of risk at first. So that risk of access to resource will be decreased. As if there will be an increase in calculated risk of assigning resource, it shows more confidently the user is unauthorized. Definitely user with suitable behavior will be able to obtain a smaller amount of risk compared to primary risk so the chance of access to resource will be increased and user will prove the authority. Otherwise the system suspects to unauthorized user and the access will be denied. In conclusion, in suggested approach increasing the primary risk causes to consider users' behavior more carefully so authorization of user considers

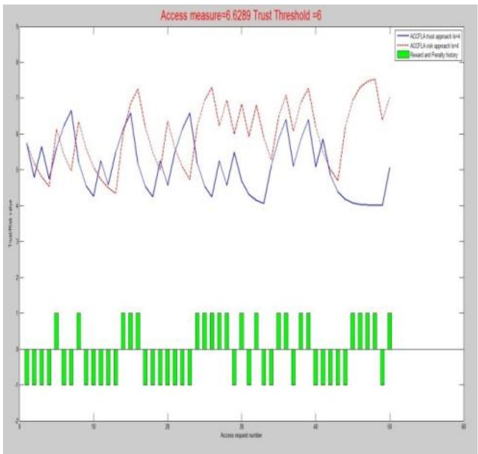

Figure 13: The amount metric -based access control proposed approach with l_S= l_o= 4

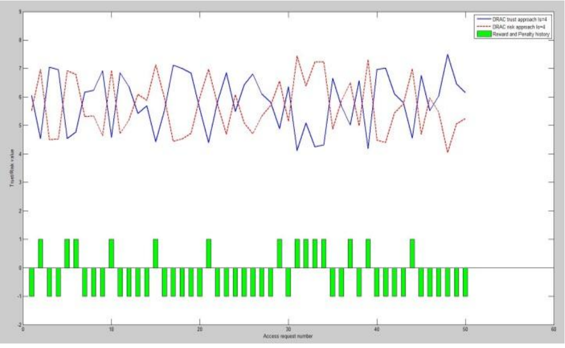

Figure 14: The access metric in DRAC for l_s= l_o= 4

In simulated scenario for measure- based access control using

Learning automata, as can be seen in Figure 13, increasing the risk causes to decreasing trust and vice versa. Also in the Figure, user and resource have the lowest level so that risk and trust Figures are close together. By increasing security level of user and resource in Figure 14, Figures of risk and trust were close together at first then they separated from each other.

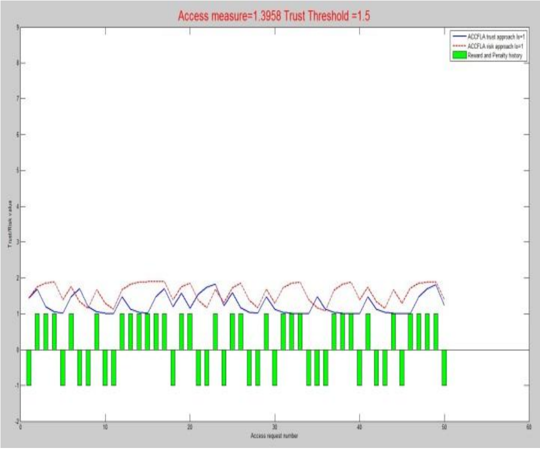

Figure 15: The amount metric -based access control proposed approach for l_s= l_o= 1

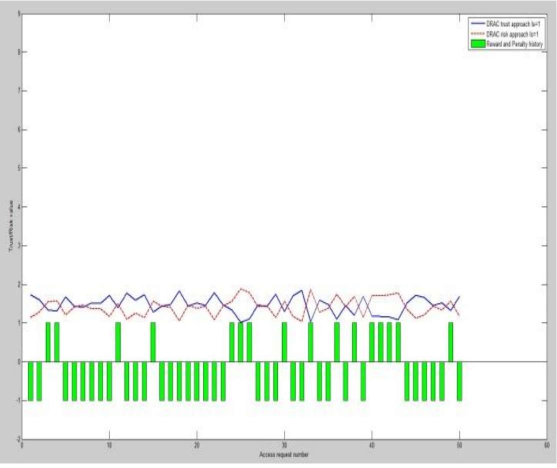

Figure 16: The access metric in DRAC for l_s= l_o= 1

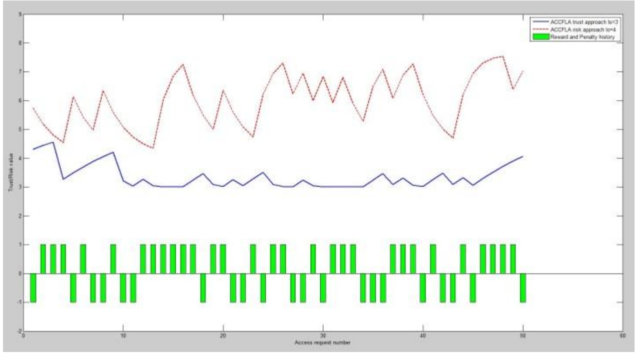

Figure 17: The amount metric-based access control proposed approach for l_s< l_o

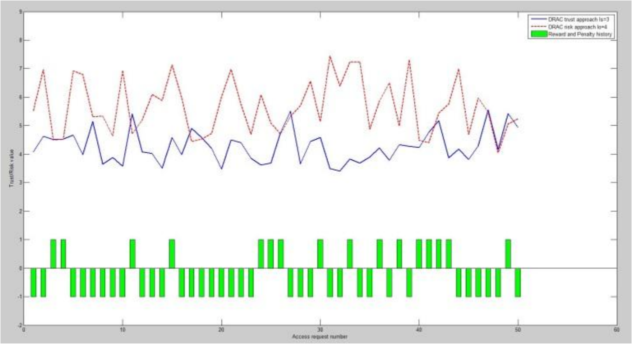

Figure 18: The access metric in DRAC for l_s< l_o

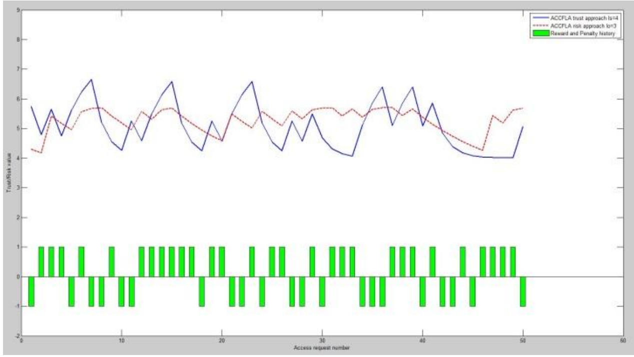

Figure 19: The amount metric -based access control proposed approach for l_s> l_o

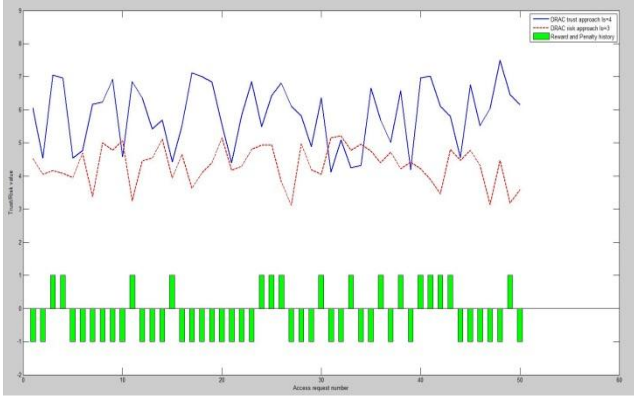

Figure 20: The access metric in DRAC for l_s> l_o

Figure 17 is an exception because in the cloud infrastructure based on BLP access control, security level of user should be larger than resource sensitivity level. So the risk will be more than trust and Figure of risk will be higher than Figure of trust with more fluctuations. But for authorized user the fluctuations decrease and slope of Figure will be smoother. Figure 19 is the most important access metrics. System can recognize unauthorized users by high sensitivity and accuracy so that risk will be decreased and trust Figure will be seen higher.

7. CONCLUSION AND FUTURE WORKS

By growing number of users in cloud computing technology, controlling the access to resources finds a huge importance. This paper has offered an approach using learning automata based upon Risk, Trust and Access measure parameters. According to daily growing number of users of cloud federation, in suggested approach the limit of measurability has been removed by deleting central parameter of identity federation and lack of existence a secure environment. In addition, suggested approach is a totally dynamic approach as clouds are able to communicate each other without any previous operations. Also any changes in user behavior cause to update all parameters of trust and risk calculation. On the other hand suggested approach is a flexible approach because it is possible to change condition of user from authorized to unauthorized by changing in his/her behavior or vice versa. Also it is possible to use other decision making technics like hidden Markov model (HMM) and decision making tree to develop suggested approach.

8. REFRENCES

[1] R. I. L. S. Foster I., Yong Zhao," Cloud computing and grid computing 360-degree compared", In Grid Computing Environments Workshop, pages 1–10. GCE, Aug 2008.

[2] Michael Armbrust, Armando Fox, Rean Griffith, Anthony D. Joseph, Randy H. Katz, Andrew Konwinski, Gunho Lee, David A. Patterson, Ariel Rabkin, Ion Stoica, and Matei Zaharia. 2010," A view of cloud computing", Commun. ACM 53, 4 (2010), 50–58.

[3] Yisheng Wang, Haopeng Chen, "Dynamic resource arrangement in cloud federation," The 2012 IEEE Asia-Pacific Services Computing Conference(APSCC 2012), Pages: 50-57, Guilin, China, 2012.12.06-2012.12.08, ISBN: 978-1-4673-4825-6.

[4] T. Kurze, M. Klems, D. Bermbach, A. Lenk, S. Tai, and M. Kunze,"Cloud Federation", The Second International Conference on Cloud Computing, GRIDs, and Virtualization, September 2011, pp. 32-38.

[5] Abdul Raouf Khan," Access control in cloud computing enviroment", Department of Computer Sciences, King Faisal University, Saudi Arabia, MAY 2012.

[6] A. Celesti, F. Tusa, M. Villari, and A. Puliafito, "Security and cloud computing: interCloud identity management infrastructure", 19th IEEE WETICE, June 2010, pp. 263-265.

[7] B.Holmer, S.Rubby,"Federated identity management in interCloud ", Der Technischen Universita¨ tmu¨ nchen, 2013, pp.3-9.

[8] Antonio Celesti, Francesco Tusa, Massimo Villari and Antonio Puliafito," Three-Phase Cross-Cloud Federation

Model: The Cloud SSO Authentication", Dept. of Mathematics, Faculty of Engineering, University of Messina Contrada di Dio, S. Agata, 98166 Messina, Italy.2010.

[9] Xixu Fu,Kai jun Wu,XiZhang Gong," Access Control and Security in Cloud Computing Systems", Institute of Information Technology, Shanghai Ocean University, Shanghai, China,2009,4-12,pp.69-89.

[10] Bassam Farroha, Deborah Farroha," Challenges of "Operationalizing" Static System Access Control: Transitioning from ABAC to RADAC", Bassam Farroha, Deborah Farroha, 2011.

[11] Daniel Ricardo dos Santos, Carla Merkle Westphall," Risk-based dynamic access control for a highly scalable cloud federation ", Carlos Becker Westphall Networks and Management Laboratory Federal University of Santa Catarina Florianópolis, Brazil,2013, 40-63.

[12] R. McGraw, "Risk-adaptable access control RADAC, in: Privilege (Access) Management Workshop",NIST–National Institute of Standards and Technology–Information Technology Laboratory, 2009.

[13] L. Zhang, A. Brodsky, S. Jajodia, "Toward information sharing: Benefit and risk access control BARAC", in: Proceedings of the Seventh IEEE International Workshop on Policies for Distributed Systems and Networks, IEEE Computer Society, Washington, D-C, USA, 2006, pp. 45–53.

[14] P.-C. Cheng, P. Rohatgi, C. Keser, P. A. Karger, G. M. Wagner, A. S. Reninger," Fuzzy multi-level security: An experiment on quantified riskadaptive access control", in: IEEE Symposium on Security and Privacy, IEEE Computer Society, Los Alamitos, CA, USA, 2007, pp. 222–230.

[15] Q. Ni, E. Bertino, J. Lobo, "Risk-based access control systems built on fuzzy inferences", in: Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security, ASIACCS '10, ACM, New York, NY,USA, 2010, pp. 250–260.

[16] Kevin Kelly,"Role-Based Access Control Model", 1998, pp.50-93.

[17] Riaz Ahmed Shaikh, Kamel Adi, Luigi Logrippo," Dynamic risk-based decision methods for access control systems "Universit´e du Qu´ebec en Outaouais, Gatineau, Qu´ebec, Canada,2011.

[18] Q.Wang, H. Jin,"Quantified risk-adaptive access control for patient privacy protection in health information systems, in: Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security (ASIACCS '11), ACM, New York, NY, USA, 2011, pp. 406–410.

[19] M. Thathachar and P. Sastry, "Varieties of learning automata: An Overview", IEEE Transactions on Systems, Man and Cybernetics, vol. 32, no. 6, pp. 711-722, 2002.

[20] K. Najim and A. S. Poznyak, "Learning Automata: Theory and Application", Tarrytown, NY: Elsevier Science Ltd., 1994.

[21] K. Narendra and M. A. L. Thathachar, "Learning automata: An Introduction", Prentice Hall, Englewood Cliffs, New Jersey, 1989.