Volume 9, Special Issue No. 1, February 2018

ISBN: 978-93-5300-455-2

International Journal of Advanced Research in Computer Science
(ISSN: 0976-5697)

RESEARCH PAPER

SHRI SHANKARLAL SUNDARBAI SHASUN JAIN COLLEGE FOR WOMEN
ICRACC 2018
(23rd–24th February 2018)

Available Online at www.ijarcs.info

Behaviour Analysis Model with Level Based Access Restriction Algorithm for Cloud Security Development

J. Persis Jessintha
Assistant Professor,Department of Computer Science
Bishop Heber College
Tiruchirapalli, India
persisjessintha@gmail.com

Dr. R. Anbuselvi
Associate Professor, Department of Computer Science
Bishop Heber College
Tiruchirapalli,India
r.anbuselvi@yahoo.com

ABSTRACT

The access restriction in Cloud Computing Environment is being done with different methods and measures. However the user has to trust the Cloud Service Provider (CSP) and the CSP has to trust the user, the trust plays a vital role in access restriction. Since trust depends on the behavior of the cloud user, calculating trust using the behavior is very much needed. To improve the performance of cloud security and access restriction performance, a Behavior Based Multi Profile Access Restriction (BMPR-FL) Fuzzy logic Algorithm is presented in this paper. A behavior analysis model is adapted which tracks the user's previous access. Based on the access trace, the list of user access to the services requested, and their successful completion has been verified. The method generates fuzzy rules using the access data and the details of access measures. Using the fuzzy rule generated and access details, the method estimates the secure access weight (SAW), based on which the user will be restricted.

Keywords: Cloud Computing, Cloud Security, Access Restriction, User Profile, Behavior Analysis.

I Introduction

The modern computing technology has shifted the internet world to another extend. It enables the access of the service can be performed at any instant with any device with internet enabled. The most organizations has number of operation division in distributed locations. However, they enable the development process could be done in a collaborative manner and allows their employee to perform their task from their location where they are. Such location independent access of various services increases the throughput performance of the organizations considered. In the next stage, not all the organizations has the capability to enforce such independent access due to the cost. This introduces the enforcement of cloud computing, which enables the service can be accessed from anywhere which is provided by any service provider. The service provider provides services can be access through their interface but the resource will be in the same place. The user has just to register with the network and then he/she will be allowed to access the services.

There are many organizations maintain different information related to their own and their employees and customers. They store their data in the cloud due to the higher cost it claims. Not all the organizations cannot offer such huge amount to by the storage devices. The cloud service providers like Yahoo, Amazon and Google provides such cloud space to store their information and can be retrieved at any point of time. Such data can be accessed through certain services provided for the registered user[1][2].

However the services are allowed to be access based on trust and registration, Not all the user behave like genuine but perform different malicious activities. The cloud security is the major challenging issue in allowing the user to access different data from the cloud[3]. In many situation, there will be different sensitive secret information present in the cloud which has to be secured from illegal access. This requires certain strategic approach in enforcing access restriction[4]. There are number of access restriction algorithms available in recent days. The attribute based access restriction [1][6] is the popular approach which enforces the access in attribute level. The traditional trust based approaches cannot be applied because the trust has been verified by a third party. Because it is necessary to hold the secret information of the customers also.

The cloud has number of registered users and each user has been allocated with certain access protocols. A user will have access to any service when he is allowed. Such collection will be present in the user profile where it contains number of information about the user as well as the list of services the user can access. In this case, the user will be verified for the grant of access to the service. By doing so, the user can be stopped at the entry level but there are situation where even the registered user with granted access would perform illegal activity in accessing the services. By submitting different information to the service access the user would try to malformed the service. Such phenomenon has to be considered.

This requires the analysis of user behavior in enforcing the access restriction in cloud environment. The user's actions and behavior in accessing the service has to be monitored. The user may access the service initially but he may drop the further activities or he may finish the service in an incomplete stage. Even the user would submit malformed data to the service in the intension to perform any malicious activity. Not only the malicious activity but he may try to steal the other user information. Such activity must be monitored by the system and to perform access restriction in an efficient manner.

This paper introduces a behavior analysis model to monitor the user access and restrict the user access based on the previous access history. The previous history can be used to estimate different measures in restricting the user access in the cloud. The detailed approach will be discussed in detail.

II Literature Survey

Predicate Based Access Control (PBAC) [7], is introduced to overcome the problems in Attribute Based Access Control method.Providing User Security Guarantees in Public Infrastructure Clouds [8], describe a framework for data and operation security in IaaS, consisting of protocols for a trusted launch of virtual machines and domain-based storage protection.Quantitative Reasoning about Cloud Security Using Service Level Agreements [9], develop two evaluation techniques, namely QPT and QHP, for conducting the quantitative assessment and analysis of the secSLA based security level provided by CSPs with respect to a set of Cloud Customer security requirements. These proposed techniques help improve the security requirements specifications by introducing a flexible and simple methodology that allows Customers to identify and represent their specific security needs.Flexible Data Access Control Based on Trust and Reputation in Cloud Computing [10], propose a scheme to control data access in cloud computing based on trust evaluated by the data owner and/or reputations generated by a number of reputation centers in a flexible manner by applying Attribue-Based Encryption and Proxy Re-Encryption.Privacy protection based access control scheme in cloud-based services [11], present an access control system with privilege separation based on privacy protection (PS-ACS). In the PS-ACS scheme. Towards temporal access control in cloud computing [12], resent an efficient temporal access control encryption scheme for cloud services with the help of cryptographic integer comparisons and a proxy-based re-encryption mechanism on the current time. Keyword Search With Access Control Over Encrypted Cloud Data [13], propose a scalable framework where user can use his attribute values and a search query to locally derive a search capability, and a file can be retrieved only when its keywords match the query and the user's attribute values can pass the policy check. Using this framework, we propose a novel scheme called KSAC, which enables keyword search with access control over encrypted data. KSAC utilizes a recent cryptographic primitive called hierarchical predicate encryption to enforce fine-grained access control and perform multi-field query search. Meanwhile, it also supports the search capability deviation, and achieves efficient access policy update as well as keyword update without compromising data privacy.

Secure and Efficient Attribute-Based Access Control for Multiauthority Cloud Storage [14], resent secure and cost-effective attribute-based data access control for cloud storage systems. Specifically, we construct a multiauthority CP-ABE scheme that features the system does not need a fully trusted central authority, and all attribute authorities independently issue secret keys for users. Then each attribute authority can dynamically remove any user from its domain such that those revoked users cannot access subsequently outsourced data; Also cloud servers can update the encrypted data from the current time period to the next one such that the revoked users cannot access those previously available data; and the update of secret keys and ciphertext is performed in a public way.

Fine-Grained Data Access Control Systems with User Accountability in Cloud Computing [15], present a way to implement, scalable and fine-grained access control systems based on attribute-based encryption (ABE). For the purpose of secure access control in cloud computing, the prevention of illegal key sharing among colluding users is missing from the existing access control systems based on ABE. This paper addresses this challenging open issue by defining and enforcing access policies based on data attributes and implementing user accountability by using traitor tracing. Furthermore, both the user grant and revocation are efficiently supported by using the broadcast encryption technique.

III Behavior Analysis Model with Level Based Access Restriction

The behavior analysis model maintains number of user profile where each profile contains number of information about the users and the list of services the users has access. Also, the method monitors the access of different services the user performs and stores them to the access traces. Using the access trace the method compute the secure access weight for different services. Based on the service access weight computed, the method grants or restricts the user access.

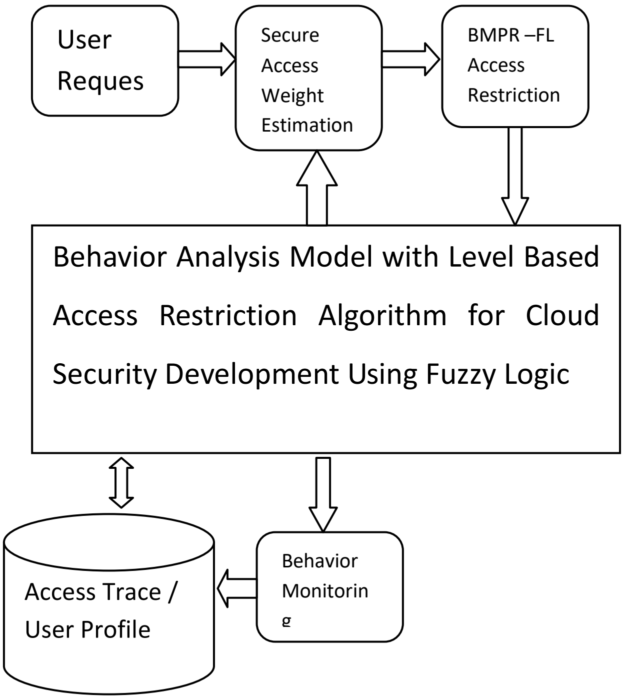
User Reques
Secure Access Weight Estimation
BMPR –FL Access Restriction
Behavior Analysis Model with Level Based Access Restriction Algorithm for Cloud Security Development Using Fuzzy Logic
Access Trace / User Profile
Behavior Monitorin g

Figure 1. General Architecture of BMPR Access Restriction

The Figure 1, shows the general architecture of BMPR access restriction approach and shows different functional stages involved.

Consider N number of services present in the service pool, where K number of users has been registered to the cloud. Among N services, each service N_i would access the data attributes Ø{D_i,..D_n} where only K-p number of user has access to all the attributes of the set Ø. Similarly only K-p number of user has access to all the services of N. Restricting the user k from accessing the service s to which he has no access is the key issue here. There are number of approaches has been discussed to solve this problem and each uses different measures and parameters. This paper consider the level of access for the user which is being computed based on the behavior of the user in accessing the service.

A. Behavior Monitoring:

The behavior of user in accessing the service would vary between different users. For example, consider there exist a service S_i, being accessed by the user u_k, which contains v number of states involved. The user u_i, would access the service and terminate in the v-n state blindly. Such intrinsic behavior can be used in to identify the users trustworthy while providing access to the user. The behavior of the user activity in accessing the services has been monitored here. This is an independent activity which tract the user request, how the request moving and it monitors each stage of the request. At each state of the request, the method tracks the status. Once the service has been terminated then it logs the status and other information to the access trace. Generated access trace being used to perform different activity in access restriction.

Initially, the service requested by the user can be identified from the service request Ur, as follows:

Service requested Sr = Service-ID $\in Ur$ -- (1)

It is necessary to identify and extract the data being submitted to the service Sr. It has been extracted as follows:

Sd =Service-Data$\in Ur$ -- (2)

Now, the number of states the request has been followed has to be identified using the following equation.

State Channel Sc = $\sum States \forall (Sr)$ --(3)

Now for each state present in the state channel, the service data submitted can be extracted using the equation (2).

The status of the request can be identified as follows:

Identify status of request Rs = Ur.Status.

Once all the states and their data and their status has been extracted, the access log can be generated and added to the access log set. The generated access log will be used to perform access restriction by computing the secure access weight.

Generate Access log Acl = $\sum_{i=1}^{size\ (State)} \left((S, Rs, Sed) \in Acl \right) \cup S, Rs, Sed$ --(4)

Here Sed is the service data, Acl-Access log, Rs- Status of request.

Generated log can be added to the trace as follows:

Access trace AT= $\sum (Traces \in AT) \cup Acl$ -- (5)

The behavior monitoring algorithm monitors the state of the request and status of the request to produce the access log to the trace. The traces generated have been used to compute the secure access weight for different user in the next stage to support access restriction to be performed in efficient manner.

B.Secure Access Weight Estimation:

The secure access weight is the measure which shows the trustworthy of user in accessing the list of attributes belongs to the service claimed. The method estimate the secure access weight at each stage of the service and by identifies the list of attributes the service accessing. Using all these, the method compute the secure access weight by computing the number of time the user has accessed the service or the attributes and the number of times it has been completed in success. This is estimated for each time window of the log. Also the factor of attribute level access is computed based on the number of attributes the user has access and the number of attributes the user does not have access. Using all these information, the method generates the fuzzy rule. Using the fuzzy rule generated and the user access details, the secure access weight has been estimated.

To compute the secure access weight, the user profile Up has been taken as the key with access trace AT.

For the service Sr being requested by the user Uk, the presence of access has been verified in the user profile Up. The verification of the access has been performed as follows:

$\forall (Profile\ p \in Up) if\ U_p$@Sr ,1,0 -- (6)

The equation verifies the presence of the service with the user profile and based on that it returns a value 1 or 0.

If the user has access to the service then, the list of attributes being accessed by the service has been identified as follows:

Identify list of attributes to be accessed Ats = $\sum Attributes@SER$ -- (7)

Further, the user would have access to limited attributes from the attribute set Ats. It is necessary to identify the list of attributes the user has access. It can be performed as follows:

Identify list of attributes the user has access UAAs = $\sum Attributes(Up) \in Ats$ --(8)

Using the values of equation (7) and (8), the attribute level factor can be measured as follows:

Compute Attribute level factor ALF = $size(UAAs) / Size(Ats)$

--(9)

Now the user access behavior value has to be computed. It can be measured by computing the number of times the user has accessed the service and number of times he has accessed in a proper manner. It can be measured as follows:

Compute Total Service Access TSA.

TSA= $\sum_{i=1}^{size\ (AT)} AT(i).User = UR.User\ \&\&\ AT(i).Service == SER$

--(10)

Compute Number of Successful Access NSA.

NSA = $\sum_{i=1}^{size\ (AT)} AT(i).User = UR.User\ \&\&\ AT(i).Service == SER\ \&\&\ AT(i).Status == Success$

--(11)

The NSA and TSA are estimated for each time window log. The using the values of different time window, the method generate the fuzzy rule.

To generate the rule, the method estimates the Minimum and maximum values of both the measures.

Generate Fuzzy Rule R.

Rule R = <TSA.Min, TSA.Max><NSA.Min, NSA.Max>

Using the values of (10) and (11), the secure access weight can be measured as follows:

Compute Secure Access Weight SAW.

SAW = $\frac{(NSA < NSA.Min, NSA.Max > (1,0)) \times NSA}{(TSA < TSA.Min, TSA.Max > (1,0)) \times TSA} \times ALF$

-- (12)

The secure access weight estimation algorithm computes the attribute level factor and secures access weight. The computed weight has been used to perform access restriction later.

C.BMPR-FL Access Restriction:

The behavior model based profile orient access restriction algorithm has been performed for each request being received from the user. The method identifies the user request and computes the secure access weight at each level. The service would have N number of levels or it may access different other services internally. For each service identified in the service life cycle, the method computes the secure access weight. Based on computed weight, the method performs access restriction in the cloud environment.

BMPR-FL Access Restriction Algorithm:

```
Input: User Request Ur, User Profile Up

Output: Boolean

Start

    Read User request Ur.

    Read User profile Up.

    Identify the service ID  SID = Ur.ServiceID.

    Compute secure access weight SAW.

    If SAW> WTh // weight threshold

        Return Boolean

    Else

        Return false

    End

Stop.
```

The BMPR-FL access restriction algorithm identifies the service being requested and computes the secure access weight. Based on the weight being computed, the method returns the Boolean value to allow or deny the request.

IV.Results and Discussion

The proposed behavior analysis model based hierarchical access restriction scheme has been implemented and evaluated for its performance. The method has produced efficient results in different parameters considered.

Parameter	Value
Protocol	BMPR-FL
Tool Used	Advance Java
Number of Services	100
Number of Attributes	500

Table 1: Details of Simulation

The Table 1, shows the details of simulation being used to evaluate the performance of the proposed BMPR algorithm.

Method	Access Restriction Performance %		
	50 Services	75 Services	100 Services
PBAC	81	85	89
BMPR-Fl	92	95	97.2

Table 2: Comparative Result on Access Restriction Performance

The Table 2, presents the comparative result on access restriction performance produced by different methods on varying number of services. The results show that the proposed BMPR algorithm has improved the access restriction performance in all the number of services considered.

Techniques	Time Complexity in seconds		
	50 Services	50 Services	50 Services
PBAC	56	56	56
BMPR-Fl	31	31	31

Table 3: Comparative Result on Time Complexity

The Table 3, presents the comparative result on time complexity performance produced by different methods on varying number of services. The results show that the proposed BMPR algorithm has reduced time complexity in all the number of services considered.

Techniques	Throughput Performance %		
	50 Services	75 Services	100 Services
PBAC	82	86	91
BMPR-Fl	85	91	98.3

Table 4: Comparative Result on Access Restriction Performance

The Table 4, presents the comparative result on throughput performance produced by different methods on varying number of services. The results show that the proposed BMPR-FL algorithm has improved the throughput performance in all the number of services considered.

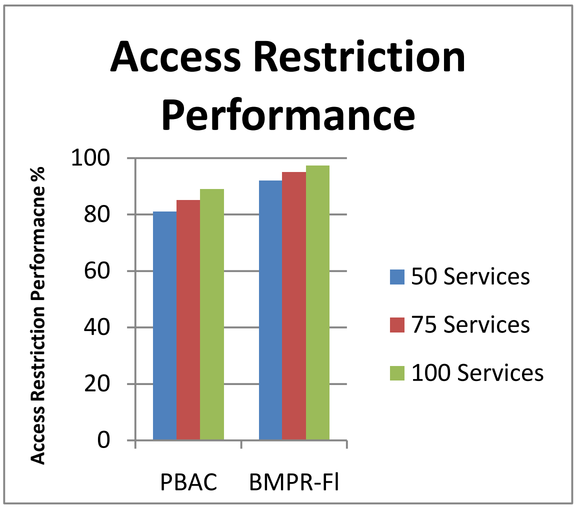

Figure 2: Comparison on Access Restriction Performance

The Figure 2, shows the comparative result on access restriction produced by different methods. The result shows that the proposed BMPR-FL algorithm has produced higher access restriction performance than other methods considered.

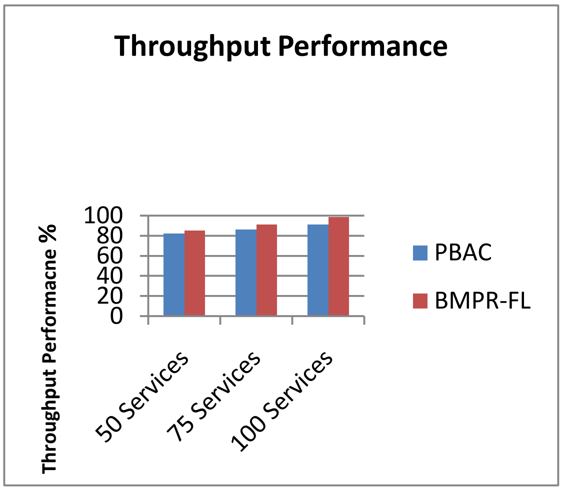

Figure 3: Comparison on throughput performance

The Figure 3, shows the comparison on throughput performance produced by different methods and shows that the proposed BMPR-FL algorithm has produced higher throughput than other methods.

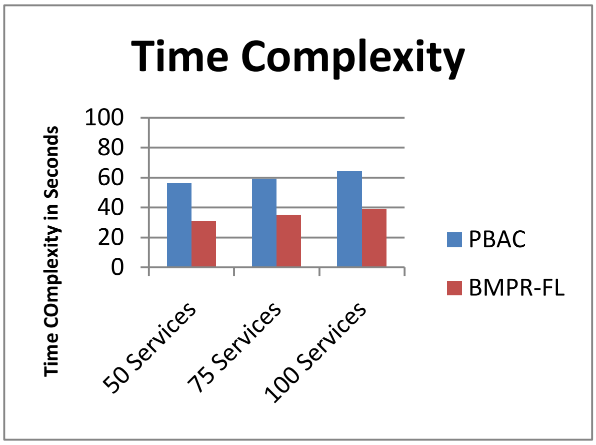

Figure 4: Comparison on time complexity

The Figure 4, shows the comparison on time complexity produced by different methods and shows clearly that the proposed BMPR-FL algorithm has produced less time complexity than others.

Conclusion:

In this paper, a behavior analysis model for access restriction in cloud environment has been presented. The method monitors the service access of the users and logs different state and their status to the access trace. Using the access trace available the method generates the fuzzy rule. Using the rule generated and access trace available, the method compute the secure access weight at each service state and based on that the method grant or deny the service access. The method produces efficient results in access restriction upto 97.2 % and throughput performance has been increased up to 98.3%. Also the time complexity of access restriction has been hugely reduced.

References

[1] Wei Teng ; Geng Yang Attribute-based Access Control with Constant-size Ciphertext in Cloud Computing, IEEE Transactions on Cloud Computing (Volume: PP, Issue: 99), Page(s): 1 – 1, 2015.

[2] Jun Luo, A Novel Role-based Access Control Model in Cloud Environments, JournalInternational Journal of Computational Intelligence Systems Volume 9, 2016 - Issue 1, 2016.

[3] Lixia Xie and Chong Wang, Cloud Multidomain Access Control Model Based on Role and Trust-Degree, Hindawi, Journal of Electrical and Computer Engineering Volume 2016 (2016).

[4] Kan Yang, Time-Domain Attribute-Based Access Control for Cloud-Based Video Content Sharing: A Cryptographic Approach, IEEE Transactions on Multimedia, Vol 18, Issue: 5, May 2016.

[5] Jongkil Kim, Surya Nepal, A Cryptographically Enforced Access Control with a Flexible User Revocation on Untrusted Cloud Storage, Data Science and Engineering , Volume 1, Issue 3, pp 149–160, 2016.

[6] Mehdi Sookhaka,, F. Richard Yua, Attribute-based data access control in mobile cloud computing: Taxonomy and open issues, Elsevier, Future Generation Computer Systems 72 (2017) 273–287.

[7] B.Srinivasa Rao, A Framework for Predicate Based Access Control Policies in Infrastructure as a Service Cloud, Int. Journal of Engineering Research and Applications, Vol. 6, Issue 2, (Part -6) February 2016, pp.36-44.

[8] Nicolai Paladi, Providing User Security Guarantees in Public Infrastructure Clouds, IEEE Transaction on Cloud Computing, Vol. 5, Issue 3, 2017.

[9] Jesus Luna, Quantitative Reasoning about Cloud Security Using Service Level Agreements, IEEE Transaction on Cloud Computing, Vol. 3, Issue 5, 2017.

[10] Zheng Yan, Flexible Data Access Control Based on Trust and Reputation in Cloud Computing, IEEE Transaction on cloud computing, Vol.5 Issue 3, 2017.

[11] Kei Fan, Privacy protection based access control scheme in cloud-based services, IEEE Transaction on China Communications, vol. 14, Issue 3, 2017.

[12] Yan Zhu, Towards temporal access control in cloud computing, IEEE, INFOCOM, 2012.

[13] Zhirong zen, Keyword Search With Access Control Over Encrypted Cloud Data, IEEE Transaction on sensor journal , vol 17, issue 3, 2017.

[14] Jianghong Wei , Secure and Efficient Attribute-Based Access Control for Multi-authority Cloud Storage, IEEE System Journal vol. issue 99, 2017.

[15] Jin Li, Fine-Grained Data Access Control Systems with User Accountability in Cloud Computing, Cloud Computing Technology and Science (Cloud-Com), 2010.