Indonesian Journal of Electrical Engineering and Informatics (IJEEI)
Vol. 7, No. 1, March 2019, pp. 22~28
ISSN: 2089-3272, DOI: 10.11591/ijeei.v7i1.612

State level attribute compliance measure based efficient access restriction improved security in cloud environment

A. Surendar, Sadulla Shaik
Department Electronics and Communication Engineering of
Vignan Foundation for Science, Technology and Research, India

Article Info

Article history:

Received Aug 7, 2018
Revised Sep 26, 2018
Accepted Oct 20, 2018

Keyword:

Access restrictions
ACM
Cloud Security
SLACM
User profile

ABSTRACT

Access restriction has been a dominant issue in the security of cloud environment. The problem of access restriction has been handled with different dimension by various researchers. However, the methods of access restriction has not been achieved the expected performance in point of data security. To improve the performance of cloud security, a novel state level measure has been discussed in this paper. By receiving the user request, the proposed method identifies various states and at each state the list of attributes being accessed has been identified. Then for each state identified, an Attribute compliance measure (ACM) has been estimated. The ACM measure has been estimated based on the user profile available for the cloud manager. Based on the ACM measure estimated at each level, a cumulative state level attribute compliance measure (SLACM) has been estimated. According to the SLACM, the method restricts the service access to the user. The proposed method produces efficient results on cloud security performance.

Corresponding Author:

Sadulla Shaik,
Department Electronics and Communication Engineering of
Vignan's Foundation for Science, Technology and Research,
Vadlamudi, Guntur Andhra Pradesh-522213, India.
Email: sadulla09@gmail.com

1. INTRODUCTION

The recent development in the cloud has enabled the organizations to move their data from their own database servers to the cloud where the storage complexity has been reduced. The availability of the cloud has reduced the headache of maintaining dedicated high storage servers which cost huge amount. Also, the organizations would provide various services through the service providers. This enables the users to be able to access the data available in the cloud. In general, the cloud environment is a loosely coupled architecture where the service provider would not knew about the user.

The organizations would maintain various forms of data belongs to their own business, personal information of their employees as well as customer information. For example, the most hospitals maintains the patient information like personal and medical information. They would maintain the details of various scans which claims huge storage space. Similarly, the personal information and the diagnosis result of the patients should be kept in a secure manner which should not be exposed anonymously. So the security of the data available in the cloud is more essential and has to be restricted from malicious access.

In any organization, there will be number of users belongs to various categories. Not all the user type has allowed to access all form of data belongs to different users. So restricting the users according to their nature and responsibility is more essential. Towards restricting the users, there are number of approaches available. The profile based approaches are more common which restrict the users based their profile being maintained by the cloud manager. The cloud manager would maintain various user profiles

which has their nature and responsibility. According to that the set of attributes or set of data has been allowed for them. Similarly, attribute based approaches are available which classifies the attributes into different groups. The user who has the access to the particular type can access the type of data or attribute which falls within the category specified. However, when the cloud services are requested, the service would access various group of data and restricting them based on the profile or attribute will not produce efficient results.

Towards the scope, the state level measure has been discussed in this paper. The method identifies the list of states of any service and what the data being accessed are identified. Using them, the ACM measure on each state has been estimated to compute the SLACM measure. Based on that the user has been restricted. The detailed approach is discussed in the next section.

2. RELATED WORKS

The problem of access restriction in cloud environment has been approached with various techniques. This section discusses set of methods related to the problem.

In [1], an policy based access control approach has been presented. The method extends the work of general Authentication, authorization, and accounting (AAA) approach to improve the virtualization performance. The method maintains various policies in form of XML documents and restrict the user access based on the policy available.

An context based access control with the role based access is presented in [2]. The CARBAC (Context Adaptive range Binary Arithmetic Coding) model maintains different context information and maintains the user profile with the list of context the user has access. According to the details of the profile and the context the user has access, the method restrict the user from illegal access.

Towards the access restriction of collaborative health care system an policy based approach is presented in [3]. The method maintains various policy to different authorities of various domains. Also, the policies are maintained in form of semantics which maintains the relationship between the authorities and the data. According to that the method restricts the access of health care data from the cloud.

Similarly towards the access restriction in collaborative multi cloud environment an efficient approach is presented in [4]. The author performs a detailed survey on the stage in which the part of collaboration can be performed. In [5], the problem currency exchange in the cloud has been analyzed. The method adapts the linear regression model to predict the currency rate prediction according to the data present in the cloud.

In [6], the author presents an auditing system to ensure the correctness of the data. The method enables the user in validating the correctness of data and ensures the storage guarantee. In [7], the author present a cloud based storage scheme which enables security in block level. Also an indirect mutual trust based access control is enforced for the security of the cloud data.

Towards the blocking of military information leakage an efficient document control system is presented in [8]. The method has been designed to restrict the malicious access of defense documents using the watermarking techniques. The user has been restricted based on their role and there are various security levels defined. In [9], a unified approach for the access control system in attribute level is defined. The author enforces lattice based access control in a hierarchical manner. In [10], the author present a secure BPMN (Business Process Management Notation) system which enforces secure chain towards the enforcement of access control at the run time.

All the above discussed approaches has the problem of restricting malicious access and produces poor results in access control.

3. STATE LEVEL ACCESS COMPLIANCE MEASURE BASED APPROACH

In this method, the user request has been received and identifies the service being requested. Then for the identified service, the list of states being available has been identified. For each stage of the service, the method identifies the list of attributes being accessed. Using the details identified, the method estimates access compliance measure to restrict the user from malicious access. The detailed approach is discussed in this section.

The Figure 1, shows the architecture of the proposed state level access compliance measure based access restriction algorithm. Also, the Figure 1, shows various functional components incorporated in the proposed system.

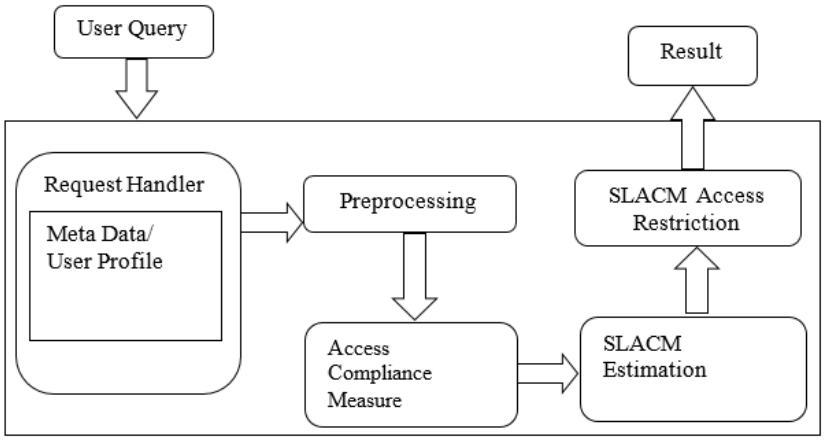

Figure 1. Architecture of SLACM Based Access Restriction Approach

4. PREPROCESSING

Preprocessing is the process of identifying the service being requested and its various states possible. In this stage, the request handler receives the user request Ur and identifies the service being claimed by the user. Any service would have various numbers of states according to the input data being given. So, in this stage, the method identifies the list of all states the service would navigate and at each state it would access various data on the fly. Such attribute list at each state has been identified. Identified state and attribute list has been given to the next stage to perform validation.

Algorithm:
Input: Service Request Sr
Output: State List Sl, Attribute List Al.
Start
Read service request Sr.
Service Ser = Identify service requested Sreq$\in Sr$
Identify list of all states of the service.
$Sl = \sum States \in Ser$
For each state Sl_i
Identify list of all attributes Al_i being accessed.
$Al_i = \sum_{i=1}^{size(Md)} Md(i) \rightarrow Sl_i(Ser)$
$Al = \sum Al \cup Al_i$
End
Stop

The above discussed algorithm identifies the list of all attributes being accessed by the service at each state. The identified states and attribute list has been given to the next stage of access restriction.

ACM Estimation:

The access compliance measure represent the degree of access the user has towards the attributes being accessed. It has been measured based on the user profile available and the meta data. Using these two, the method identifies the list of attributes the user has access from the attribute list and the list of attributes the user has no access from the list. Using these two, the access compliance measure for any state has been estimated. The estimated measure has been used to perform access restriction

Algorithm:
Input: User Profile Uprofile, Meta Data MeD, State S
Output: ACM.
Start
Read Uprofile, MeD, State list Sl, Attribute List Al.
Identify the attributes of state S.
$As = \sum Attributes(Al(s))$
Compute no of attributes allowed NA^2.

$NA^2 = \sum_{i=1}^{size(As)} As(i) \in Uprofile\ (User)$
Compute no of attributes not allowed NANA.
$NANA = \sum_{i=1}^{size(As)} As(i) \notin Uprofile\ (User)$
Compute ACM = $\frac{NA2}{NANA} \times size(As)$
Stop

The above discussed algorithm identifies the list of all attributes being accessed by the service at each state. The identified states and attribute list has been given to the next stage of access restriction.

Access Compliance Measure (ACM) Estimation:

The access compliance measure represents the degree of access the user has towards the attributes being accessed. It has been measured based on the user profile available and the meta data. Using these two, the method identifies the list of attributes the user has access from the attribute list and the list of attributes the user has no access from the list. Using these two, the access compliance measure for any state has been estimated. The estimated measure has been used to perform access restriction.

Algorithm:
Input: User Profile Uprofile, Meta Data MeD, State S
Output: ACM.
Start
Read Uprofile, MeD, State list Sl, Attribute List Al.
Identify the attributes of state S.
$As = \sum Attributes(Al(s))$
Compute no of attributes allowed NA^2.
$NA^2 = \sum_{i=1}^{size(As)} As(i) \in Uprofile\ (User)$
Compute no of attributes not allowed NANA.
$NANA = \sum_{i=1}^{size(As)} As(i) \notin Uprofile\ (User)$
Compute ACM = $\frac{NA2}{NANA} \times size(As)$
Stop

The above discussed algorithm estimates the access compliance measure for the state identified based on the attribute list and the user profile available.

SLACM Based Access Restriction:

The proposed access restriction algorithm receives the user request from the user. The received user request has been preprocessed to identify the list of states and attributes of the service claimed. Then for each state of the service, the method estimates the access compliance measure (ACM). Using the ACM of states estimated, the method estimates SLACM measure. According to the SLACM value of the user towards the service, he has been restricted.

Algorithm:
Input: User request Ureq
Output: Boolean
Start
Receive user request ureq.
[State list Sl, Attribute list Al] = Preprocessing (Ureq)
For each state s of Sl
ACM_s = Estimate Access Compliance Measure (s, Al_s)
End
Estimate SLACM = $\frac{\sum_{i=1}^{size(Sl)} ACM(i) > Th}{size(Sl)} \times 100$
If SLACM> ATH then //ATH-access threshold
Allow
Else
Deny
End
Stop

The above discussed algorithm shows how the user has been estimated for his access compliance measure at each state. Using the ACM value of each state, an SLACM measure has been estimated based on which the user has been restricted from malicious access.

5. RESULTS AND DISCUSSION

The proposed access restricted algorithm has been implemented using advanced java. The method has been evaluated for its efficiency using varying number of users and attributes types. In each case the method has produced efficient results on different parameters considered. The method has produced the following results. Table 1 shows the details of simulation parameters being used to evaluate the performance of the proposed approach.

Table 1. Details of simulation parameters

Parameter	Value
Tool Used	Advanced Java
Number of resources	2000
Number of users	300
Number of Data Types	200
Number of states	20
Size of trace	3 million

The security performance and the efficiency in access restriction has been measured for the proposed algorithm and has been compared with the efficiency of other methods [11]. The proposed method has produced higher security performance compare to other methods, i.e Scalable Tool for Resource Management (Storm), RBAC (Role-based access control), CARBAC, IERPS (Intelligent Enterprise Risk Practitioners), and MLAR (Middle Latency Auditory Response). The comparison result has been presented in Figure 2. The proposed SLACM algorithm has produced higher security performance than other methods.

The accuracy of access restriction and false classification ratio has been measured. The false classification ratio produced by the proposed SLACM algorithm has been compared with other methods [12]. The comparison result is presented in Figure 3 which shows that the proposed SLACM algorithm has produced less false classification ratio than other methods.

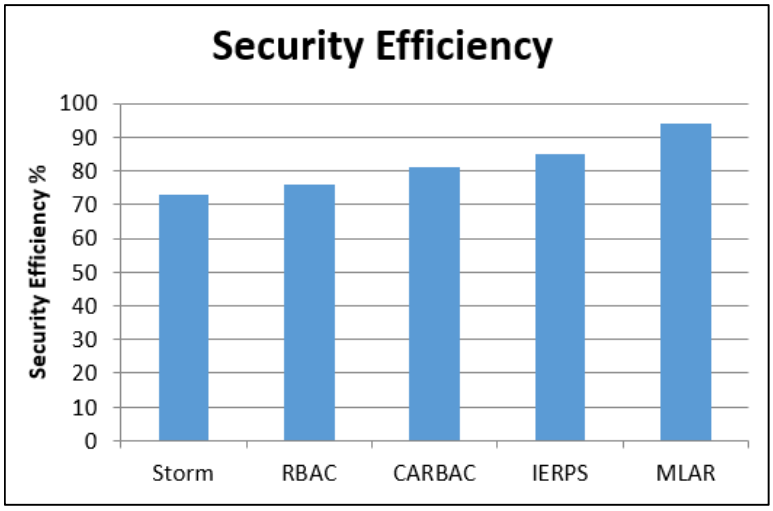

Figure 2. Comparison of security efficiency

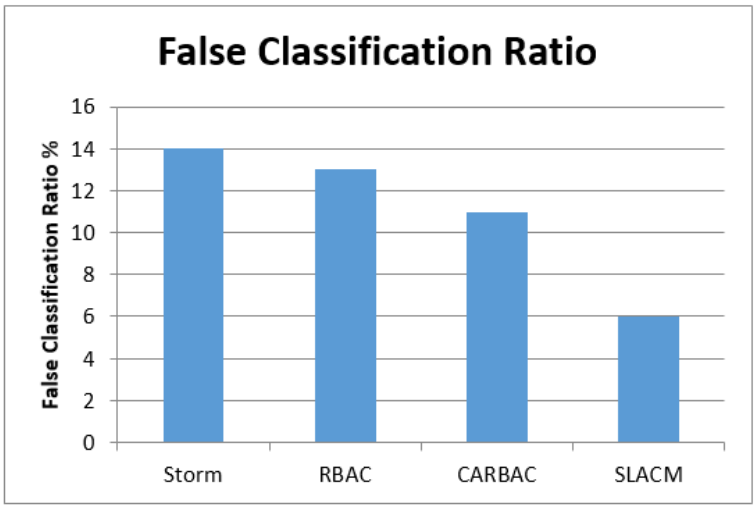

Figure 3. Comparison of false classification ratio

The time taken for the decision making in access restriction has been measured for the proposed SLACM algorithm and compared with the other methods considered. The result depict that the proposed SLACM algorithm has produced less time complexity than other methods. The result time complexity has been presented in Figure 4.

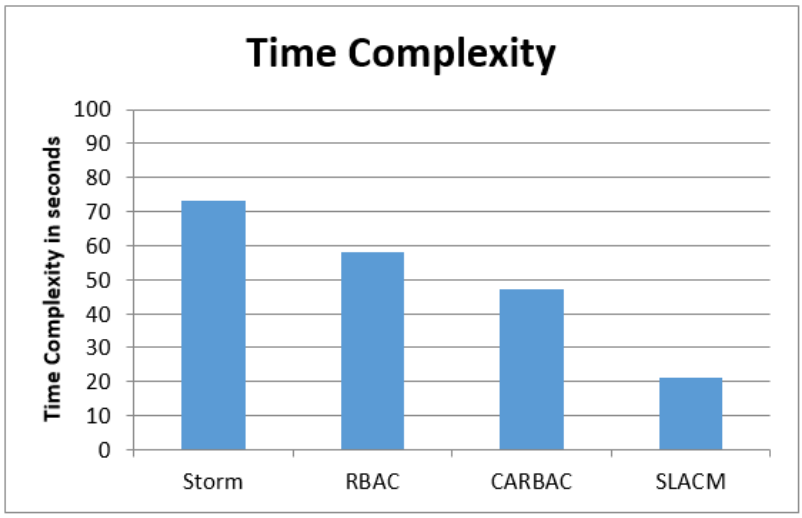

Figure 4: Comparison of time complexity

6. CONCLUSION

In this paper, an efficient access restriction algorithm for the cloud data has been presented. The state level access compliance measure based approach is presented which monitors the states of the service and for each state a set of attributes being accessed has been identified. Similarly for each state, the method estimates the access compliance measure for the user and finally a SLACM measure has been estimated. Based on the value of SLACM measure the user access has been restricted. The proposed algorithm has produced efficient results on access restriction and improves the performance up to 96% with less false classification ratio.

REFERENCES

[1] Y. Demchenko, "Policy Based Access Control in Dynamic Grid-based Collaborative Environment," *International Symposium on Collaborative Technologies and Systems* (CTS'06), pp. 64-73, 2006.

[2] Shu-Ping Lu, Kuei-Kai Shao, Yu-Nung Chao, "The Design and Implementation of Collaboration Service Integration Platform Based on Context-Aware Role Based Access Model," *International Journal of Security and Its Applications*, vol. 8(1), pp. 295-306, 2014.

[3] Daisy Daiqin He, Jian Yang, "Authorization Control in Collaborative Healthcare Systems," *journal of Theoretical and Applied Electronic Commerce Research*, vol. 4, Issue 2, pp. 88-109, 2009.

[4] Ranu Pandey, Sandeep Gonnade, "Assessing Collaboration Framework in MultiCloud Environment," *International Journal of Innovative Technology and Exploring Engineering*, vol. 3, Issue. 12, 2014.

[5] R. Thandeeswaran, S. Subhashini, N. Jeyanthi1, M. A. Saleem Durai, "Secured Multi-Cloud Virtual Infrastructure with Improved Performance," *cybernetics and information technologies XII*, vol. 2, pp. 11-22, 2012.

[6] Cong Wang, Qian Wang, Kui Ren, Ning Cao, Wenjing Lou, "Toward Secure and Dependable Storage Services in Cloud Computing," *IEEE transactions on services computing*, vol. 2, 2012.

[7] Ayad Barsoum, Anwar Hasan, "Enabling Dynamic Data and Indirect Mutual Trust for Cloud Computing Storage Systems," *IEEE transactions on parallel and distributed systems*, 2013.

[8] J. Ho Eom, N. uk Kim, S. hwan Kim, T. M. Chung, "An Architecture of Document Control System for Blocking Information Leakage in Military Information System," *International Journal of Security and Its Applications*, vol. 6(2), pp. 109-114, 2012.

[9] X. Jin, R. Krishnan, R. Sandhu, "A Unified Attribute-Based Access Control Model Covering DAC, MAC and RBAC," *Proceedings of the International Conference on Data and Applications Security and Privacy*, Paris, France, pp. 41-55, 2012.

[10] D. Brucker, I. Hang, G. Luckemeyer and R. Ruparel, "Secure BPMN: Modeling and Enforcing Access Control Requirements in Business Processes," *Proceedings of the 17th ACM Symposium on Access Control Models and Technologies* (SACMAT '12), New York, USA, pp. 123-126, 2012.

[11] Shu-Ping Lu, Kuei-Kai Shao, Yu-Nung Chao, "The Design and Implementation of Collaboration Service Integration Platform Based on Context-Aware Role Based Access Mode," *International Journal of Security and Its Applications*, vol. 8(1), pp. 295-306, 2014.

[12] S. Y. Lin, C. H. Chen, C. C. Lo, "Currency Exchange Rates Prediction based on Linear Regression Analysis Using Cloud Computing," *International Journal of Grid and Distributed Computing*, vol. 6(2), pp. 1-10, 2013.