IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Volume-6, Special Issue-2, March 2018 E-ISSN: 2347-2693

Time Window Based Frequency Analysis for Efficient Access Control in Cloud Using Fuzzy Logic

J. Persis Jessintha[1*], R. Anbuselvi[2]

[1]Department of Computer Science, Bishop Heber College, Trichy, Tamil Nadu,India
[2]Department of Computer Science, Bishop Heber College, Trichy, Tamil Nadu,India

Available online at: www.ijcseonline.org

Abstract-To improve the performance of access control in cloud environment, different approaches has been discussed earlier. Towards the problem of access restriction, an efficient trust based access control mechanism is presented in this paper. The method maintains the access details of various services of different users in different time window. The time window access logs has various information about the service access and their status of completion. Using the log available, the method estimates the frequency of services being accessed. Also with the status of the services access, the method computes the trust factor. The frequency measures has been computed for different time window for each service. Based on the value of frequency measures, the method generates fuzzy rules. Based on the fuzzy rules generated, the trust factor has been estimated for any user. The method produces efficient results in access restriction and reduces the time complexity as well.

Keywords- Cloud Environment, Access Control, Fuzzy Rules, Frequency Analysis, Time Orient Approach.

I.INTRODUCTION

The cloud environment maintains various resources of different organizations. The cloud service provider provides various services to access the cloud resources. This reduces the cost of maintaining the data for different organizations. Still not all the service and data can be accessed by different users. The users has to be restricted on accessing the services based on different constraints. The cloud has many information related to different users which has to be secured from illegal access. To enable higher security, the data and the services has to be accessed based on certain rules or constraints.

To restrict the user in accessing the services, there are number of approaches available. The premier key based approach, restrict the user based on the key provided. If the user uses the exact key it will be verified by a third party. Based on the key verification, the user will be granted access to the service. This approach has the issue of higher time complexity and the keys would be tampered by any malicious user, which in turn affects the performance of access control. The user profile based approaches are adapted in different situation where the organization has various roles and services. This approach restrict the user based on their profile. The issue with this approach is the attributes being accessed by the services. There may be number of attributes or information which has to be secured but the user may not have access to them. So this approach has the issue of restricting the user in attribute level.

To solve this, the attribute based approaches has evolved[1][4][6]. These methods, restrict the user in attribute level but introduces higher time complexity. Similarly, there are number of methods available for the access restriction[7] in cloud environment[14][15]. By considering all this, this paper introduces a time window based approach with frequency analysis. The user would access various services in each time window and each would have end up with different status. By considering the frequency of service access and their completion status, the frequency analysis can be performed.

On the other side, the fuzzy rules has great impact in access restriction. By considering the frequency analysis in different time window, the fuzzy rules can be generated. Generated fuzzy rules can be used to compute the trust measure. This paper discusses the detailed approach of frequency analysis to restrict the user. The detailed method has been discussed in the next section.

II.LITERATURE SURVEY

There are number of methods has been discussed for the problem of access restriction in cloud environment. This section details different methods towards the problem of access control.Attribute-based Access Control with Constant-size Ciphertext in Cloud Computing [1], proposes a hierarchical attribute-based access control scheme with constant-size ciphertext. The scheme is efficient because the length of ciphertext and the number of bilinear pairing

evaluations to a constant are fixed. Its computation cost in encryption and decryption algorithms is low. In [2], the author discusses a SAT-RBAC model (security and availability based trust relationship in RBAC) and adopts the following elements as the main factors of a trust relationship: the security state and network availability of the host used by a user, the protection state of the service providers that are related to the role. A security-based scheduling model for Cloud environments is presented. Because of the uncertainty of Cloud environments, the trust relationship is divided into three zones: the unbelievable zone, the probable believable zone and the believable zone. Bayesian method is used to estimate the trust probability distribution in the probable believable zone. This paper also provides algorithms to evaluate the values of the main elements of a trust relationship. Cloud Multidomain Access Control Model Based on Role and Trust-Degree [3], presents an access control model based on role and trust-degree. The model combines role-based access control and trust-based access control. Time-Domain Attribute-Based Access Control for Cloud-Based Video Content Sharing: A Cryptographic Approach [4], focus on how to securely share video contents to a certain group of people during a particular time period in cloud-based multimedia systems, and propose a cryptographic approach, a provably secure time-domain attribute-based access control (TAAC) scheme, to secure the cloud-based video content sharing. A Cryptographically Enforced Access Control with a Flexible User Revocation on Untrusted Cloud Storage [5], introduce a cloud storage system that offers cryptographically enforced security. Attribute-based data access control in mobile cloud computing: Taxonomy and open issues [6], provides a comprehensive survey on attribute-based access control schemes and compares each scheme's functionality and characteristic. A Framework for Predicate Based Access Control Policies in Infrastructure as a Service [7], proposed a framework with Predicate Based Access Control (PBAC) in general and then implemented it in Open Stack. The empirical results revealed that the proposed framework can improve the granularity with fine grained access control mechanism.

III.TIME WINDOW BASED FREQUENCY ANALYSIS WITH FUZZY LOGIC

The fuzzy logic based frequency analysis of time window log has been performed over the logs available. The method maintains the access log of different time window generated by the user access. Using the log available the method computes the frequency measures and trust factor. Based on the trust factor estimated the access restriction is **performed. It has the number of stages involved.**

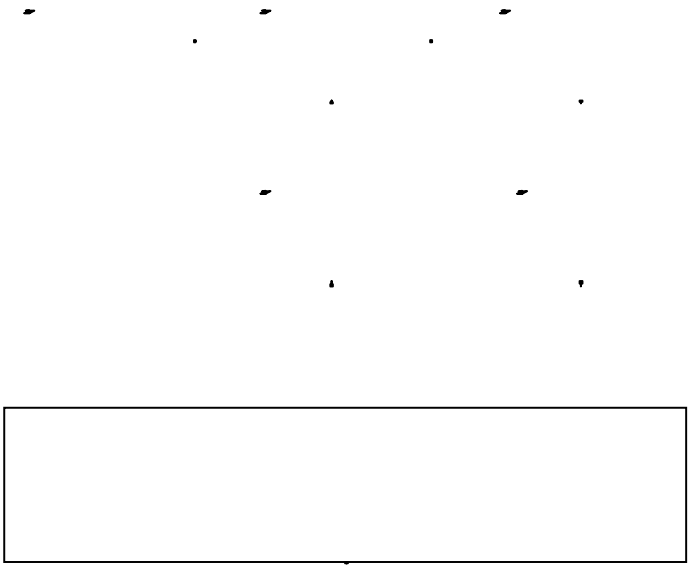

Figure 1: Architecture of Proposed Access Restriction Algorithm

The Figure 1, shows the architecture of proposed frequency measure based access restriction algorithm and shows various stages involved.

A. Fuzzy Rule Generation:

The fuzzy rule represent, the frequency of service being accessed in different time window and how it has been finished. As the method maintains the logs belong to different time window, the frequency of different service access has been identified. The range value is the measure which shows the frequency measure. Each rule has two values as frequency measure and success rate. It has been generated as follows.

First, the logs belong to a specific service has to be identified. It has been identified using the following formula.

Consider the entire log is stored in Al, which represent the access log, from the Al, the logs belong to a specific service S_i, has been separated as follows:

$$\text{Service Log Sl} = \sum_{i=1}^{¿Al} ¿Al(i).Service = ¿Si \quad \text{-- (1)}$$

Once the logs of specific service Si, has been identified, they can be split into different time window based on their generation.

To perform this, the entire time window can be split into number of time window according to the span time.

Consider the time window Tw has N number of span time then it can be split into time window log as follows:

Time window log Twl = $\sum_{i=1}^{¿Al} ¿Al(i).Service = ¿Si \wedge ¿Al(i).Time = Tw_1$

-- (2)

Here Tw_i specifies a specific time window in the entire time window Tw.

When the logs are separated according to the time window, then the frequency measures can be estimated as follows:

Frequency Measure Fm = $\frac{¿Twl}{¿Sl}$ -- (3)

The size(twl) is the number of times the service being accessed at the specific time window where size(sl) is the total number of times the service being accessed.

The frequency measure can be measured for all the time window. Similarly, the success rate can be measured for any time window.

Success rate Sr = $\frac{\sum_{i=1}^{¿Tl} ¿Tl(i).Status = ¿Success}{¿Tl}$

-- (4)

The success rate of the service access can be measured for all the time window.

Once the frequency measure and success rate has been measured for all the time window, then the rule can be generated based on the range values. The range values are the minimum and maximum values of both measures.

B. Trust Factor Estimation:

The trust factor is the measure which represent the user trustworthy in accessing the service. To estimate the trust factor two features has been considered, the one is the access frequency and the other is the success rate. By computing the distance between two measures of the fuzzy rule, the trust factor can be measured.

First the user access frequency is measured as follows:

Access frequency Af = $\frac{Number\ of \times the\ service\ is\ accessed}{Total\ number\ of\ service\ access}$ –(5)

Second the success rate is measured as follows:

Success rate Sr = $\frac{Number\ of \times the\ service\ is\ accessed\ successfully}{Total\ number\ of\ service\ access}$

- - (6)

Once these two measures are computed, then their values are used to compute the trust factor.

Trust Factor TF = $\frac{Dist(Af, Rule.Frequency)}{Dist(Sr, Rule.SuccessRate)}$

-- (7)

Computed trust factor has been used to perform access restriction.

C. TBFL Access Restriction:

The access restriction in TBFL approach is performed based on the fuzzy rule and trust factor estimated.. The fuzzy rule is generated using the access details of the user by computing the access frequency and success rate. Based on the fuzzy rule available, the method compute the trust factor. Based on the trust factor computed, the method uses the threshold value to restrict the user in accessing the service.

TBFL Algorithm:

Receive the user request.

Identify user and service requested.

Split the entire log into time window based.

For each time window

Estimate the frequency measure and success rate.

End

Generate Fuzzy Rule

Compute access frequency for the user.

Compute success rate for the user.

Compute trust factor for the user.

If TF> Trust-support then

Allow access

Else

Deny access.

End

The TBFL algorithm generates the fuzzy rule and computes the trust factor. Based on the trust factor estimated, the access restriction is performed.

IV. RESULTS AND DISCUSSION

The Trust based fuzzy logic algorithm for access restriction has been implemented and evaluated for its performance. The method has produced efficient results in different parameters considered.

Parameter	Value
Protocol	TBFL
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 ETFL algorithm[16].

Method	Access Restriction Performance %		
	50 Services	75 Services	100 Services
PBAC	81	85	89
ETFL	84	89	91.6
TBFL	87	91	93.7

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 TBFL algorithm has improved the access restriction performance in all the number of services considered.

Techniques	Time Complexity in seconds		
	50 Services	75 Services	100 Services
PBAC	56	65	76
ETFL	37	46	63
TBFL	33	42	56

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 TBFL algorithm has reduced time complexity in all the number of services considered.

Techniques	Throughput Performance %		
	50 Services	75 Services	100 Services
PBAC	78	85	91
ETFL	81	87	92.3
TBFL	84	91	94.6

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 TBFL 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 ETFL algorithm has produced higher access restriction performance than other methods considered.

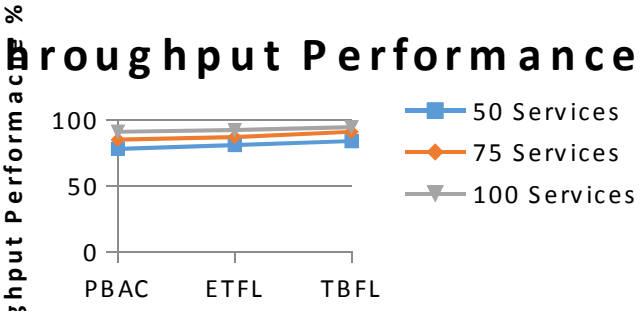

Figure 3: Comparison on throughput performance

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

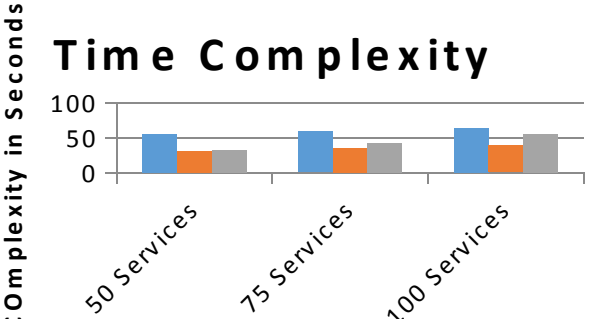

Figure 4: Comparison on time complexity

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

V.CONCLUSION

Towards the development of access restriction performance, an efficient TBFL algorithm is presented in this paper. The method monitors the service access of the users and logs different state and their status to the access trace. The access log has been used to compute the frequency measure and success rate at each time window. The computed measures has been used to generate the fuzzy rules. The same has been used to compute the trust factor for the user request. Based on the trust factor, the method restrict the user from illegal access. The method produces efficient results in access restriction upto 93.6 % and throughput performance has been increased up to 94.6%. 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, Journal International 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]. Sakshi kathuria, "A Survey on Security Provided by Multi-Clouds in Cloud Computing", International Journal of Scientific Research in Network Security and Communication, Vol.6, Issue.1, pp.23-27, 2018.

[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.

[16]. J.Persis Jessintha and Dr.R.Anbuselvi," Aggrandizing Authorization By Enhancing Trust Using Fuzzy Logic In Cloud Environment", International Journal of Applied Engineering Research, **10**, 538-542, 2015.

