IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.-6, Issue-5, May 2018 E-ISSN: 2347-2693

# Enhanced-Role Based Access Control (E-RBAC) with Trust Factor for Cloud Software- as-a-Service Paradigm

[1*]N. Geetha, [2]M. S. Anbarasi,

[1]Department of Computer Science and Engineering, Pondicherry Engineering College, Pondicherry, India
[2]Department of Information Technology, Pondicherry Engineering College, Pondicherry, India

*Corresponding Author: great.geetha@gmail.com

Available online at: www.ijcseonline.org

Accepted: 18/May/2018, Published: 31/May/2018

***Abstract***— Software-as-a-Service (SaaS) paradigm is one of the most popular forms of cloud services in today's multi-tenant technological architecture. The role of multi-tenancy architecture is to offer services to its tenants with customized features of applications they need. Data isolation and resource sharing between multiple tenants in such architecture is more complicated task. Access control models takes accountability of the verification mechanism, the administration and the proper governance of the resources and related services. New architectural model is therefore required to maintain simple relation between the providers and multiple tenants in the system with a strong security feature. SaaS paradigm also needs an effective portability and orchestration mechanism over a virtualized infrastructure. To address these issues, we present a novel architecture called the E-RBAC (Enhanced- Role Based Access Control) model to enhance the security and access control over the services in the SaaS infrastructure by calculating the trust of the roles assigned. We also present a comparative analysis of SaaS provisioning with and without E-RBAC security model.

***Index Terms***— Cloud Computing, SaaS, Multi-Tenancy Architecture, RBAC.

## I. INTRODUCTION

Cloud Computing is viably used to enhance versatility, accessibility, flexibility and security of IT services in numerous application territories. It embraces favorable circumstances of numerous advances, for example, virtualization, service-oriented architecture, and Utility computing to enable clients and service providers to cut expenses on framework organizations and activities. Cloud computing frequently has three main parts: Infrastructure as-a-Service (IaaS), Platform-as-a-Service (PaaS), and Software-as-a-Service (SaaS). Multi-Tenant architecture (MTA) is regularly utilized as a part of SaaS where various tenants can utilize a similar code storage area in the SaaS to create applications. One tenant application might be a work in progress, while SaaS is executes other tenant applications at a similar time.

Security and authorization is one of the essential features in implementation of the cloud in which trust and access control forms the security ideas of cloud computing paradigm. Access control mechanism in a cloud situation is apprehensive in enabling a client to access cloud resources and related services. Conventional access control depends on personality based confirmation, and it needs to set up an assembled security administration space (Chen et al. 2008).

Access control remains a test in SOA in light of the fact that authentication, authorization and information dispersal may take put crosswise over obscure (potentially untrusted) endpoints. An SOA customer connects just with the front-end service and has no information of the service orchestration that satisfies the request. In this manner, it can't foreordain every one of the services that will partake in collaboration and approach its information.

Access control framework is a gathering of strategies and parts that decide the substantial client to get to the resources and related services that they need. The authorized users get to access and the requested services are put away in the entrance security policy. One of the major roles of any access control framework is to secure data from users with unauthorized access. In every access control framework there is a property, techniques, and capacities which are gotten from either policy or policy set (Srivatsa et al. 2007). It is not only the Access control framework that can satisfy all the security prerequisite of the multi-area cloud but there are other mechanisms too to check for proper authorization. In this way, trust should tie with get to control to meet the security prerequisite of the multi-space cloud.

With several study made on the area, influenced by cloud and Intercloud situations investigations and in addition related work on access control for clouds, we present the Enhanced-Role Based Access Control (E-RBAC) approach which formalize the RBAC connected for the multi-tenancy pattern. It not just intends to give a versatile and adaptable resources and elements administration of the traditional RBAC, yet additionally contains related policy requirements encouraging appointments also, coordinated efforts among tenants and clients in multiple levels. The expanded model is connected for Intercloud situations with the trading tokens approach for fine-grained dynamic trust establishment. To encourage trait based policy assessment and actualizing the proposed display, we apply an effective component to change complex coherent articulations in approaches to minimized choice charts. Our model of the multi-tenant access control framework for Inter-cloud is also experimented. Assessments show that our framework has great execution as far as number of cloud resources, customers and arrangements.

The rest of the paper is organized as follows: Section II elaborates the related works on Role Based Access Control Scenarios and the security requirements of cloud computing. Section III describes the issues in the design of Access Control model in cloud. Section IV explains the Proposed Framework called the Enhanced-Role Based Access Control Model with Trust factor. In Section V, the experimental results of the proposed model are discussed. Section VI concludes the findings and comparison results.

## II. Related work

Though RBAC is considered as a fine-grained one and embraced by some small scale scattered applications, conventional RBAC isn't reasonable for extensive scale, open isolated condition and does not satisfy the requirements of the users in multi-domain architecture. In a multi-domain architecture of cloud condition, a RBAC does not provide all the security prerequisite system. Approval in multi-domain is fundamental issue in RBAC display since when a role is relegated to a client it just approves the authenticity of the client's role without thinking about trust of client involved in the system. In Service Oriented Architecture, the client has no mechanism to identify the data being misused by other users in the system. There is less control over the data by the service providers and the owners of the data. To address this major issue in Service Oriented Architecture paradigm, Ranchal (Ranchal et al. 2016) proposed a data centric approach for preserving the data and the privacy information of the users. Authors also proposed an access control policy scheme to protect data and privacy of the users.

As cloud fulfills the requirement of the users on demand, multi-tenant architecture is gaining more attention. MTA allows its tenants to present services to their subtenant programmers to customize their applications in the SaaS infrastructure. In granting resources to the tenants of the system, MTA needs more formal and more secure access control model. Zou (Zou et al. 2017) has identified a solution to this issue by proposing an administrative role based access control model for isolation of access to service and sharing resource relationship. The pre-doled out role of approval is the errand of RBAC, also, it doesn't play out any task on a malicious client by these outcome framework is probably going to have been disregarded. To understand these issues, numerous specialists coordinated trust with access control strategies. Accordingly, trust can be a factor which can satisfy the security prerequisites of access control.

An adaptive algorithm for access control was proposed by Wang (Wang et al. 2011) which included contextual information in the user's identity. This information includes time and security. A combined approach of RBAC and Trust mechanism between the service providers and the users was proposed by the authors. To secure the data and the software that travel around the network to offer software as a service in cloud environment, a combination of role and trust based access control model is proposed by Xie (Xie et al. 2016). The proposed model calculates the weights of trust and the role's behavior in the system. Reputation score is calculated for the users participating in the system. For multi-domain environment, a role and trust based system was proposed by Chaitali (Chaitali et al. 2017) which calculated the direct and indirect trust of the participating clients and service providers participating in the system. The efficiency of the system was experimentally proved.

## III. Issues in the design of access control in cloud

By virtue of the investigation of cloud application situations, access control is more complex in dynamic environment. The difficulties confronting the cloud information access control are essentially reflected in the parts of standardization of cloud stages and brought together specialized guidelines and industry particulars for cloud computing access control. At present, most cloud specialist organizations still utilize conventional access control advances and models as the reference, which isn't useful to the usage and supervision by standardization associations. For fine grained access control, most existing cloud access control depends on client character and a few models even don't take after the base benefit guideline of access control, in this manner bring security risks to multi-tenant condition in the cloud.

Besides the security strategies followed by the traditional access control models, there are still certain issues to be overcome in the design of access control system for cloud as discussed:

### A. *Visibility Issue*

Clients have no information of service cooperation's past the front-end service. They have no methods for guaranteeing that an authenticated substance is getting to just the data for which it is approved.

### B. *Control Issue*

Clients can't determine get to control policies for their data. They have no methods of controlling who gets to their data.

### C. *Policy Infrastructure*

A trusted infrastructure through which customer policies can be dynamically determined what's more, promptly upheld is required to build up a web of trust in SOA.

### *D. Privacy*

A tenant permits the resources including information and altered segments to its subtenants, and in the interim, may not permit its ancestor-tenants or administrative framework to access to them.

### *E. Autonomous Tenants*

A framework executive can make occupants and lease assets to them, yet can't meddle with occupants' interior undertakings. Moreover, because of protection separation, part benefit legacy never again exists in the framework scope. What get to benefit can/can't be acquired and what assets can/can't be cross-level controlled are not quite the same as customary MTA frameworks.

For fine grained access control, most existing cloud access control depends on client character and a few models even don't take after the base benefit rule of access control, in this way bring security dangers to multi-tenant condition in the cloud. For access control in cloud computing, cloud clients, cloud resources and system condition are always showing signs of change, making conventional, static and brought together access control unequipped for fulfilling the dynamic security needs. Thus the proposed E-RBAC model tries to overcome the identified issues to satisfy the interoperability of cross-domain authorization including the policy for detection and decision of policy conflict.

## IV. PROPOSED MODEL

The multi-tenancy framework enables tenants to work together by means of the between tenant tasks, i.e., a resource of a tenant can be gotten to by either clients of this tenant, or clients of another tenant. The between tenant is upheld by allow contexts i.e., Based on the responsible properties in cloud, in which a bought in cloud resource is solely allocated to a tenant amid a clear lifetime, we have to characterize a requirement on exchange contexts with the goal that a resource can't be provisioned to in excess of one tenant at a particular domain condition. In any case, to ensure that a tenant can't make allow contexts for resources it doesn't have permissions; the framework ought to consider the level of trust on the tenant taking an interest in the framework.

In the design of the trust based administration model, the supposition is to think about trust in cloud figuring as the level of trust identified with the conduct of elements. The trust administration engineering for access control concerning the highlights of cloud registering is appeared. In the layer of elements there exists different sorts of substances, for example, cloud clients, cloud arbitrators and cloud specialist organizations, and every one of these elements partake in the cloud as indicated by their errands. These elements demands administrations and resources from the areas. Access control design checks certifications of the entity and characterizes the arrangements that put away in the policy segment. The model enables the substances to utilize the resource and requested services with the help of trust administration. The trust of a role in a domain involves coordinate trust and proposal trust. Coordinate trust is made on coordinate perception of every entity partaking in the system, while suggestion trust is identified with appropriated entity without coordinate cooperation, otherwise called backhanded trust. The trust assessment process assesses trust level of the participating user with the help of direct or proposal trust. Evaluated trust level of the participating user roles is then put away in repository of trust.

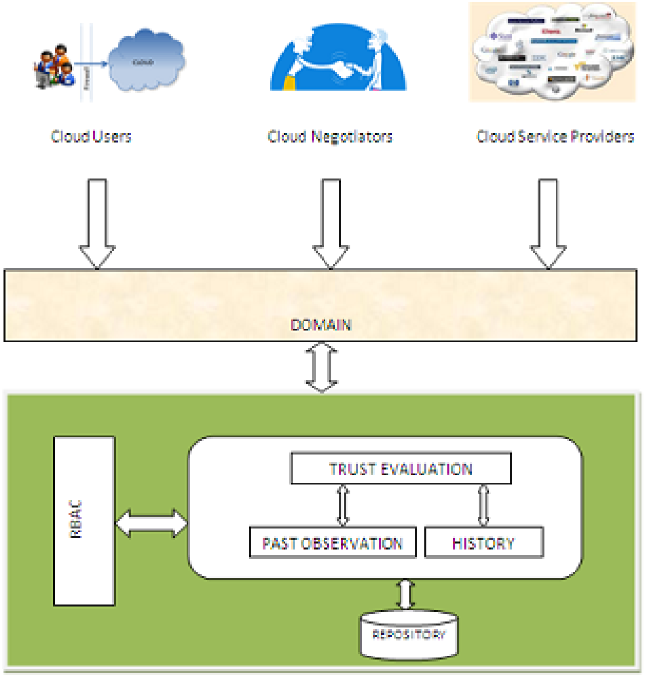

Fig1. Framework for Enhanced – Role Based Access Control.

### *A. Entities of the E-RBAC Model*

The conventional RBAC access control mechanism is used in many concerns that make use of cloud paradigm. The essential assignment of the RBAC model is allotting roles to cloud clients in a predefined manner. The client has different roles with various benefits. In this manner, a fine-grained access control is given to the environment. This paper presents s a revised and fine-grained access control model in light of E-RBAC (Geetha et al. 2018). Components participating in the proposed model are:

User (*Ur*): Ur is the set of entities participating in the system. *Ur* can be an owner of a service, a service by itself or a service provider.

Role (*Rl*): Role is an entity errand with special tasks to perform with respect to obligations prescribed to the participating entity. Whenever a new entity joins the system, it is assigned to a particular role.

Resource Objects (*Obj*): Resource Objects represents a resource. *Obj* could be a source of data or a domain resource. It also acts as a storage area of information.

Operation (*Opt*): Option is the operation that user tries to perform on the data of cloud services. This can be a Read or Write option.

Permission (*Pr*): The authorization to perform a task such as Read, Write or Execute. Permission is a subset of Object and the Option on the domain. *Pr* is a subset *Obj*, *Opt* X *Rl* where *Rl* is the Role to which the permission is assigned.

Constraints (*Con*): Constraints are the permissions, security policies, trust levels and the user assignments. These constraints are introduced and modified by the administrator.

Session (*Ss*): A mapping done between roles and users.
Set of Privileges (*Pvg*): The rights that the role has on a particular service or resource in the domain.

Trust Levels (*Tl*): It is the measure of reliability of the user or the provider on the domain. This Trust value decides the grant of permission related to a particular role.

Trust Evaluation (*Te*): Computed value for Trust.

Security Policies (*Sp*): Set of Security Rules that govern the domain.

### B. *Evaluation of Trust*

Every one of the resources, data and task are some portion of appropriated conventions intended to be managed by a single control or the organization of single service provider, for example, Amazon, Google Apps et cetera. Every one of the clients and resources apply a similar technique to quantify trust esteems. Accordingly, a computational trust strategy is proposed to assess the height of trust. Also the connection between cloud service users and cloud service provider is calculated for cloud service resources offered in that domain Cloud. Trust components are of two categories; Trust evaluation for previous session and historical trust. These two trust evaluations are calculated and stored in a trust record for service users and service provider participating in the cloud environment.

Several parameters are included in calculating the trust of the participating entities. After calculating the trust of the participating entities thoroughly, the cloud service is assigned to the roles.

Trust is calculated with the following parameters:

$$\mathrm{Te} = \mathrm{W_t}{*}\left(\mathrm{Sp}/\mathrm{NSs}\right) + \mathrm{W_t}\,2{*}\left(\mathrm{C}/\mathrm{Sp}\right)$$

Where,

$\mathrm{T_{pv}} = \mathrm{T_{pv}} - \mathrm{Te}$

$\mathrm{T_{pv}}$ = Value of Trust in Previous sessions

$\mathrm{W_t}1, \mathrm{W_t}2$ = constants for weights for Trust.

NSs = Total no. of interacted sessions.

Sp = Previous action violating the security policy

C = Conflict level (no. of times similar security policy violated)

If Te < Threshold, the user will be denied to access the software.

### C. *Proposed Access Control Algorithm*

Whenever a new request enters the system, the operations are performed according to the algorithm discussed below.

```
Algorithm E-RBAC
    Begin
    Receive Request
    If New_Request  then
        Prepare Access_Request _Permission
                                   (Uid,Rl,Obj,Opt,Con,Ss)
        Perform Role Mapping
        Else
        Grant Access with evaluated Trust Value.

        End if

    If Access_Request_Permission is relevant then
        Check Privilege
        Else
        Raise Message

        End if

    If Requested Access has Privilege then

Calculate the Trust by $Te = W_t1* (Sp/NSs) + W_t2* (C/Sp)$

        End if
    Compose the Requested Cloud Services
    End
```

## V. Experimental results

To prove the efficiency of the system, XACML and Java are utilized to assess the proficiency and execution of access control display in a single domain cloud. It mostly comprises of two sections in particular: trust assessment process and XACML-based approval display. From Table 1 it is clear that when the number of service request increases for different domains, the traditional access control method detects only less number of Trustworthy Roles since it has no information about the previous access of the same role in the domain. Comparatively, the E-RBAC framework detects more number of trustworthy roles. This is because, the framework considers the Trust of the roles based on the behavior of the roles in previous sessions. Hence the performance of the system increases considerably. In turn the orchestration of cloud service also enhances with respect to time.

| Domain | No. of Service Requests | No. of Trustworthy Roles identified | |
|---|---|---|---|
| | | Traditional RBAC | E-RBAC |
| Travel | 10 | 4 | 6 |
| Medicine | 12 | 3 | 7 |
| Hotel | 8 | 3 | 6 |
| Billing | 10 | 5 | 6 |
| Security | 7 | 3 | 5 |

Table1. Comparison of Traditional RBAC and E-RBAC

Experiments were conducted by considering different domains like Travel, Medicine, and Hotel etc. As illustrated in Table 1, the number of Trustworthy Roles identified is more in case of the proposed system called the E-RBAC than the traditional RBAC systems. This was confirmed with several different domains taken for the experiment.

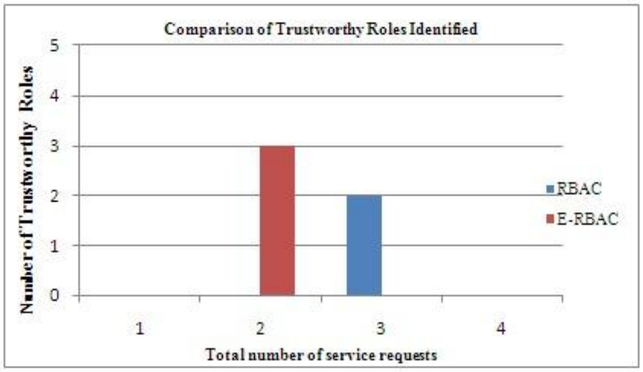

Fig.2 Comparison chart for RBAC and E-RBAC

At the point when an entity gets access to resources and requested services from the domain, its trust degree rots concerning time. Fig. 3 represents the success rate of Traditional RBAC model with the proposed Enhanced-RBAC model.

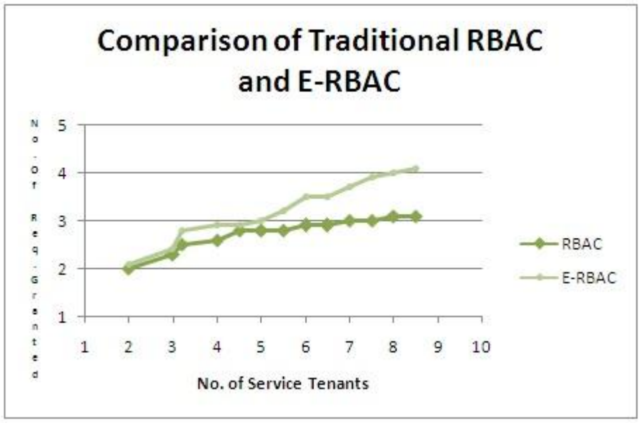

Fig.3 Success Rate for RBAC and E-RBAC

The success rate of the access control is calculated using the number of requested service offered to the user according to the roles to that of total number of cloud services available in the domain. According to the graph the Success rate decreases when the number of service tenants increase with respect to time in Traditional RBAC. In the proposed E-RBAC Model, the success rate increases in accordance with the increase in number of tenants. Every resource is granted to the user roles when the associated trust value is high. Therefore, those user roles with the higher trust value will be able to access many number of cloud resources in that domain.

## VI. Conclusion

In this paper a new Enhanced Role Based Access Control framework has been proposed. The system analyzes the access control requirements for cloud services in multi-tenancy environments. This system calculates the Trust of the Tenant's Role by monitoring their behavior in previous sessions in the same domain. The model introduces a Trust evaluation equation with the help of which the Role's identity and Trust is measured. According to the calculated trust value, the Role is granted with the access. When compared to traditional RBAC, the proposed Enhanced Role Based Access Control produces good results by identifying more number of trustworthy user roles. Experimental results show that the proposed model improvises the success rate of granting access to the trustworthy role.

## REFERENCES

[1] A. Almutairi, M. Sarfraz, S. Basalamah, W. Aref, A. Ghafoor, "A distributed access control architecture for cloud computing,". IEEE software, vol. 29(2), pp. 36-44, March 2012.

[2] X. Chen, W. Xu, W. Shen, "Trustworthiness-based dynamic access control for grid application," Journal of Hunan University (Natural Sciences), vol. 35(7), pp. 85–9, July 2008.

[3] M. Srivatsa, A. Iyengar, T. Mikalsen, I. Rouvellou, and J. Yin, "An access control system for Web service compositions," in *Proc. IEEE International Conference on Web services*, pp. 1-8, 2007.

[4] W. Wang, J. Han, M. Song, X. Wang, "The design of a trust and role based access control model in cloud computing," In Pervasive Computing and Applications (ICPCA), 6th International Conference on IEEE, pp. 330-334, October 2011.

[5] Qiong Zuo, Meiyi Xie, Guanqiu Qi, Hong Zhu, "Tenant Based Access Control Model for Multi-tenancy and Sub-tenancy Architecture in Software-as-a-Service", Frontiers of Computer Science, vol. 11(3), 2017.

[6] Masood R, Shibli M A, Ghazi Y, Kanwal A, Ali A. Cloud authorization: exploring techniques and approach towards effective access control framework. Frontiers of Computer Science, vol. 9(2), pp. 297–321, 2015.

[7] Li xia Xie, Chong Wang, "Multi domain Access Control Model Based on Role and Trust Degree", Journal of Electrical and Computer Engineering, vol. 16,2016.

[8] Chaitali Uikey, D.S. Bhilari, "TrustRBAC: Trust Role Based Access Control Model in Multi-domain Cloud Environments",

International Conference on Information, Communication, Instrumentation and Control (ICICIC), 2017.

[9] L. Xia, J. Jing An administrative model for role-based access control using hierarchical namespace. Journal of Computer Research and Development, vol. 44(12), pp. 2020-2027, 2007,

[10] M. Lorch, S. Proctor, R. Lepro, D. Kafura, and S. Shah, "First experiences using XACML for access control in distributed systems," in Proc. ACM workshop on XML security. ACM, pp. 25-37, 2003.

[11] C. Uikey, D. S. Bhilar, "Interaction Modelling using Trust and Recommendation in Cloud Computing Environment". International Journal of Computer Applications. vol. 124(17), pp. 37-44, January 2015.

[12] M. Azarmi, B. K. Bhargava, P. Angin, R. Ranchal, N. Ahmed, A. Sinclair, M. Linderman, and L. B. Othmane, "An endto-end security auditing approach for service oriented architectures," in Proc. IEEE Symposium on Reliable Distributed Systems, pp. 279-284, 2012.

[13] E. M. Ei, T. N. Thinn, The privacy-aware access control system using attribute-and role-based access control in private cloud. Proceedings of the 2011 4th IEEE IC-BNMT. pp. 447-451, 2011.

[14] T. Tavizi, M. Shajari, P. Dodangeh, A usage control based architecture for cloud environments. Parallel and Distributed Processing Symposium Workshops & Ph.D Forum (IPDPSW), 2012 IEEE 26th International. pp. 1534-1539, IEEE (2012)

[15] C. Jincui, J. Liqun "Role-based access control model of cloud computing," Energy Procedia 13, pp. 1056-61, December 2011.

[16] Rohit Ranchal, Bharat Bhargava, Ruchith Fernando, Hui Lei and Zhongjun Jin, "Privacy Preserving Access Control in Service-Oriented Architecture", IEEE International Conference on Web Services, 2016.

[17] Dr. P. Neelakantan, "A Study on E-Learning and Cloud Computing", International Journal of Scientific Research in Computer Science, Engineering and Information Technology, Volume 3, Issue 1, ISSN : 2456-3307.

[18] Geetha.N and M.S.Anbarasi, "Enhanced Role Based Access Control System for Cloud Service Composition in Multi-Tenant Environment", International Journal of Pure and Applied Mathematics, volume 118(11), pp. 349-355, 2018.

[19] R. Sood , R. Sharma, "Cloud Security Threats and Issues-A Review", International Journal of Computer Sciences and Engineering, Volume-5, Issue-4, E-ISSN: 2347-2693.