ISSN:0975-9646

Towards Novel and Efficient Architecture for Extended-RBAC in Cloud Computing

Parminder Singh , Sarpreet Singh

Department of Computer Science and Engineering,
Sri Guru Granth Sahib World University, Fatehgarh Sahib,
Punjab, INDIA

ABSTRACT-*Today Cloud Computing is very famous technology to share the number of resources. Security and Privacy are the big issues in the Cloud Computing. It is open distributed environment so it is important to preserve the data as well as privacy of users. There is Access Control Method in Cloud Computing that allows only authorized user can access the resources helps to increase the security RBAC is attractive method because the number of roles is significantly less, and users can be classified according to their roles. This paper proposes a model which is Extended O-RBAC using role ontology for Multi-Tenancy Architecture (MTA) in clouds. The ontology is used to build up the role hierarchy for a specific domain. This helps to increase the security by restricts the number of user per role, number of transaction per user. If the cloud is crash or not work properly there is also a concept of backup and restore the data to avoid the lost of important data. In this case chances of loss of data are very less.*

Keywords:- Cloud Computing, Security, Role based Access Control, Ontology, Policy, Multi-tenancy zArchitecture.

I. INTRODUCTION

In Cloud Computing there are thousands of Private and Public vendors whose offering "cloud solution". Public clouds are available from Amazon, Yahoo!, Google. It provide resources like storage and application available to the public over the internet. Private vendors are also available from Citrix, VMware, Eucalyptus etc that is managed by the organization it serves. To provide the security and privacy are the big challenges in Cloud Computing[1]. A security architecture framework should be established with consideration of processes enterprise authentication and authorization, confidentiality, access control ,integrity, non repudiation, security management, etc. In the cloud, due to multi-tenancy architecture (MTA), data from multiple clients are stored and managed by the same software[2]. When the software makes mistake, potentially millions of clients may access private data of other clients. Furthermore, data stored in a cloud may be available to cloud administrators and they may access or modify data for their own benefits. The MTA has increased the security risk due to the sharing of software, data and data schemas by multiple tenants. The cloud providers are responsible for ensuring that one customer cannot break into another customer's data and applications[3]. Access Control methods in Cloud basically a way to restricts, allows access only authorised person. It is mechanism that provide the security so that unauthorised person cannot access the resources for which it is not authorized.. Various access control models are in use, Including the most common Mandatory Access Control (MAC), Discretionary Access Control (DAC) and Role Based Access Control (RBAC). All these models are known as identity based access control models. In all these access control models, user and resources are identified by unique names. Identification may be done directly or through roles assigned to the subjects [4]. Now a day's distributed system are developed rapidly that provide virtual organization with autonomous system. Hence, the access control Mechanism must be flexible to support various kinds of domains and policies.

a) Mandatory Access Control (MAC)[5]:- In 1973 MAC was associated with Bell –LaPadula Model of multilevel security. It describes method that assures Confidentiality of information flows. It is loosely defined access control in which user can access the resources given by administration. Only administrator can define the permission, access policy and usage. It cannot be modified and change by the user. This model is used by intelligent agencies and military to maintain policy access restriction. MAC is considered a good model and straight forward for commercial system that operate in environment like financial institutions where risk of attack is high. MAC is primary developed for purposes where confidentiality is more important than integrity.

b) Discretionary Access Control (DAC)[6]:- Unlike MAC, It is not widely used access control with restricting the access to resources based on user's identity or group to which the user belong. It was implement access control matrices defined by Lampson on system protection. DAC is controlled by the root/administrator or owner. DAC can easily be used to implement least-privilege access. Individual objects can have access control restrictions to limit and it is very cost effective for homes and small business but also have some drawback of this model maintenance of the system and verification of security principles is extremely difficult for DAC systems because users control access rights to owned objects. It is fail to recognize the difference between computer programs and human users.

c) Role Based Access Control(RBAC)[7]:- MAC and DAC create some problems in case for distributed systems and managing the access to resources and system become hard so new access model is introduced known as Role Based Access Control (RBAC).In this method restricting the system access according to the role of authorized user. In 1995 introduced the family of reference model for role based access model in which permission are allotted to user according to the role and user are made member of appropriate role. All grant authorization deals with the role rather than being granted to user. This simplifies the management of permissions or users. User can also reassign easily from one role to another. The role is more stable because an organization's activities or functions usually less change frequently. A study by NIST demonstrates the need of this model in commercial and government sector. role is typically a job function or authorization level that gives a user certain privileges with respect to a file and these privileges can be formulated in high level or low level languages. RBAC models are more flexible than their discretionary and mandatory counterparts because users can be assigned several roles and a role can be associated with several users. There are several challenges in RBAC method like how to define and manage the roles in cloud? how to compare the similarity between ontology and how to transfer one ontology to another? how to define policies associated with different roles? These issues are discussed and find solution by RBAC using Reference Ontology. It provide Reference ontology framework for access control in a cloud to facilitate the design of security system and reduce the complexity of system design and implementation .It exploits the possibility of RBAC to support MTA in a cloud. Ontology information is used to build up the role hierarchy

2. RELATED WORK

"Lijun Mei,W.K. Chan and T.H. Tse[8]""A Tale of Clouds: Paradigm Comparisons and Some Thoughts on Research Issues""IEEE Computer Society Press, Los Alamitos, CA (2008)" says that Cloud computing is an emerging computing paradigm that is increasingly popular. In this paper, a qualitative comparison framework is used to compare cloud computing with pervasive computing and service computing.

"Rajkumar Buyya1,2, Chee Shin Yeo1, and Srikumar Venugopal[9]""Market-Oriented Cloud Computing: Vision, Hype, and Reality for Delivering IT Services as Computing Utilities" says that Cloud computing is a new and promising paradigm delivering IT services as computing utilities. This paper discussed some representative platforms for Cloud computing covering the state-of-the-art. The state-of-the-art Cloud technologies have limited support for market-oriented resource management and they need to be extended to support: negotiation of QoS between users and providers to establish SLAs; mechanisms and algorithms for allocation of VM resources to meet SLAs; and manage risks associated with the violation of SLAs.

"Byron Ludwig and Serena Coetzee[10]""A comparison of platform as a service (PAAS) clouds with a detailed Reference to security and Geo processing service" says that Security is very important when the internet is involved as the internet creates anonymity and removes boundaries. Cloud computing exists on the internet backbone and gives users the ability to connect from anywhere. Hence, security in cloud computing is a vital consideration. This paper discussed the implications of the security measures for the development of geo processing services, such as OGC's WPS, in a PaaS cloud. These results are valuable to all WPS developers.

"Alexander Lenk, Markus Klems, Jens Nimis, Stefan Tai and Thomas Sandholm[11]""What's Inside the Cloud? An Architectural Map of the Cloud Landscape" says that The Cloud computing stack aims at facilitating communication about different Cloud technologies and services, including placing more complex offerings such as Google App and which in turn may be provided as Cloud services themselves, however, requires a good understanding of the numerous emerging Cloud computing technologies as well as of already available services solutions offered in the open Cloud market.

"Ravi Sandhu[12]" "Future Directions in Role-Based Access Control Models" says that the reader that research on RBAC models has just begun and much interesting and challenging work remains to be done. The RBAC arena is intrinsically dominated by practical considerations and offers an opportunity for good theoretical research to be translated into practical impact on products and practice.

"David F. Ferraiolo and D. Richard Kuhn[13]""Role-Based Access Controls" says that in many organizations in industry and civilian government, the end users do not ``own" the information for which they are allowed access. For these organizations, the corporation or agency is the actual ``owner" of system objects, and discretionary access control may not be appropriate. This paper proposed a definition of the requirements and access control rules for RBAC proposed in this paper could be used as the basis for a common definition of access controls based on user roles.

3 PROPOSED WORK

This study represents the extension from RBAC using reference ontology to Extended RBAC. This strategy enhance the security by adding the restraint policy and backup and restore policy .if the cloud will crash due to any reason it will help to availability of data at that time also by taking the backup from the cloud and restore the data .

3.1 Users Assignment

There is different users who can uses the architecture. In particular organization like university, companies all having a different types of users and their roles. Firstly give the role to the user according to their capabilities like Teacher, Students, Hod, and Chancellor etc in universities. a reference ontology framework using Role-Based Access Control model which provides an appropriate policy with a specific role instead of specific user, by extending RBAC. This helps to reduce the system design by using the existing template instead of starting from the scratch. For this reference ontology database

is used that contain the number of reference ontology. For example, all IT companies has IT engineers, senior engineers, managers, Project manager etc so they can use the existing template. If user has its own ontology template, it just import to the system and used that ontology.

3.2 Role Assignment

Each user has its own role in an organization. Company user may be manager, employee, Director etc. Role is a named job function within the company that describes responsibility and authority conferred on the member of role .Now the question is how to define the roles for a specific domain?.Ontology is conceptual structure which contains knowledge in a domain and their relationships. It provides useful and valuable information for cloud computing. Each role has a RoleID which is unique for each role. For Example Director has most important role and have more access so put it at top in the role hierarchy.

RoleID	Role
1	Director
2	Principal
3	HOD
4	Teacher
5	……

Table 1 Role definition in University

According to the position of the person assign role to them and give permission to access the resources .Like Admin has permission to access each and every thing. He has an access to read , write ,update but only students have an right to access their own account details. They have an only read and write access but not update anything. Generated role by admin can store on the role database.

3.3 Permission Assignment

In any organization each person has an role in an organization. Particular Access has been given to the user according to their role in an organization. Policy is used as an extension of permission in the framework, including access policy, and Security policy, Restraint policy and Backup and Restore policy. Basically policy is the plan and course of action that should be following and intended to influence and determine decisions, actions and matters.

3.3.1 Policy Specification

Policies are used for improvement of RBAC using Reference Ontology as an extension of permissions in the access control. Policies are derived from business goals and service level agreements (SLA) in enterprises, which are “rules governing the choices in behaviour of a system” [19]. Policies include Access Policy, Security Policy, Restraint Policy, and Backup and restore Policy. The Access Policy define the what type of access has been given to the user .For example Read, Write, delete are the access given to the user according to the role of user. Like admin have an all access rights. But employee can may has an access to read and write but not update any information without the admin permission. There has been a great amount of attention in access control policy languages for web services which accommodate open, large, distributed and heterogeneous environments like the Web (XACML)[20].The Security Policy helps to provide the secure architecture in cloud environment. Security and Privacy are the two big issues in the cloud environment. Here the objective to implement the Extended-RBAC using the reference Ontology. Firstly this policy check the whether the user is authorized to access the resource. It could be positive or negative. Authorized person can access the resources rightly then it gives the positive result otherwise negative. Authorization can define with the role. Secondly it check the obligation that define the what activities he must do.

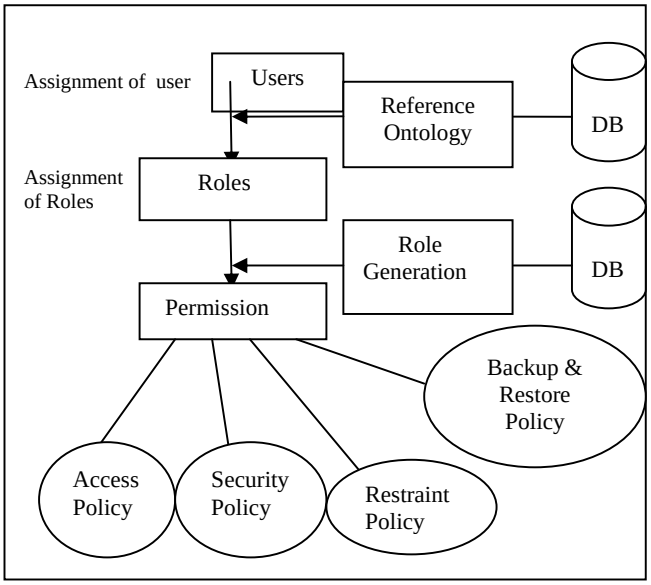

Fig. 2 Extended-RBAC using Reference Ontology

4 WORK SPECIFICATION WITH EXTENDED-ORBAC

With the time , the architecture of the cloud system has changed a lot. In previous times , it was not an easy task to pick up the entire architecture from one system to another system or from one architecture to another architecture .Later on when researches were done in this contrast , somehow the developers found their way to migrate the data but the problem was of secure migration and efficient migration[14] .Till now , researchers have been trying to put data from one end to another through bulk codes .But the problem is , bulk code is not suitable for the migration as it cannot used with each and every platform , also it would consume a lot of time. For the same purpose if we have a look at the development pattern of any system, we will find that XML is one of the lightest languages we have ever known and the good thing about XML is, it is supported by each and every platform .Also the new concept of security is consisted of XML only and that concept is called the web service [15].The main objective is to implement the Role Based access control using reference ontology by adding the policies to enhance the security in the cloud and to keep the backup of the existing data in the cloud. If in any case cloud does not work properly or crash due to any reason so we have a backup of the data and we can restore it in local server as well as in cloud again[16].

5 CURRENT VENDORS SECURELY SUPPORT IN CLOUD

5.1 Amazon EC2

Amazon Elastic Compute Cloud (Amazon EC2) is a web service that provides resizable compute capacity in the cloud. It is designed for developers to make web-scale computing easier. It provides you with complete control of your computing resources and lets you run on Amazon's proven computing environment. Amazon EC2 reduces the time required to obtain and boot new server instances to minutes, allowing you to quickly scale capacity, both up and down, as your computing requirements change. It provide security at multiple levels. The goal is to ensure that data contained within Amazon EC2 cannot be intercepted by non authorized systems or users and that Amazon EC2 instances themselves are as secure as possible without sacrificing the flexibility in configuration that customers demand.

5.2 Windows Azure

Windows Azure [16] is the platform or infrastructure for cloud computing created by Microsoft, for building, deploying and managing applications and services through a global network of Microsoft-managed datacenters. To manage Privacy and Security related concerns, Microsoft has created a Windows Azure Trust Center. Windows Azure Active Directory provides support for Security Assertion Markup Language 2.0 (SAML 2.0) which can be used to enable Single Sign-On/Sign-out from any web or mobile application to Windows Azure Active Directory.

5.3 Saleforce.com

For data security[18] Force.com provide multilayered approach from object level to record level. Each layer secures data using a different approach, and the layers build on each other to provide a deep, configurable defense .Force.com Web services allow data, logic, and metadata to be accessed from outside the Force.com platform by any program that can communicate using SOAP messages over HTTP.

5.4 IBM DB2 V9

IBM DB2 V9 is the database of choice for robust, enterprise-wide solutions and handling high-volume workloads. Optimized to deliver industry-leading performance, DB2 continually adheres to tenets of low operational costs; ease of use and reliability to power today's data applications--and beyond. It uses two approaches to realize data security, filter-based approach at the application level or row-level access control, e.g., Label-Based Access Control (LBAC). The advantage of LBAC is that it controls cross-tenant data access at the DBMS level instead of the application level.

6 CONCLUSION AND FUTURE WORK

There are number of industries that support the migration of data with security but there are several issues regarding the security and privacy in cloud due to multi-tenancy architecture (MTA) .In this paper, proposed the Extended-RBAC using reference ontology to enhance the security and reduce the complexity of system design and implementation. There is enhancement in Policies in architecture of RBAC using reference ontology. First, The Restraint Policy helps to restrict the number of user per role and number of transaction per user to enhance the security. Second , The Backup and Restore policy helps to take the backup and restoration of data in local server that helps to make the availability of data even if cloud crash. This secure architecture meets the customer demands for services and availability of the data. It would be enhance more to provide extra security. After reading this paper, the reader should have a basic understanding of backup and restoration of ontology of Role-Based Access-Control. As future works, a new back-end database schema to support Extend-RBAC will be investigated. It would also be interested to measure the scalability of Extended-RBAC using reference ontology.

REFERENCES

[1] M. Armbrust, A. Fox, R. Griffith, A.D. Joseph, R.H. Katz, A. Konwinski, G. Lee, D.A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, *Above the Clouds : A Berkeley View of Cloud Computing*, 2009.

[2] Wei-Tek Tsai, Qihong Shao. , "Role-Based Access-Control Using Reference Ontology in Clouds" 2011 Tenth International Symposium on Autonomous Decentralized Systems.

[3] Asoke K. Talukder and Manish Chaitanya, *Architecting Secure Software System*. CRC Press, 2009.

[4] "Rajkumar Buyya1,2, Chee Shin Yeo1, and Srikumar Venugopal""Market-Oriented Cloud Computing Vision, Hype, and Reality for Delivering IT Services as Computing Utilities".

[5] Sylvia Osborn, Ravi Sandhu, and Qamar Munawer . "Configuring role-based access control to enforce mandatory and discretionary access control policies". *ACM Transactions on Information and System Security (TISSEC)*. pp. 85–106.

[6] Ravi Sandhu, Qamar Munawer "How to do discretionary access control using roles". *3rd ACM Workshop on Role-Based Access Control*. pp. 47–54.

[7] Ferraiolo, D.F. and Kuhn, "Role-Based Access Control" (PDF). *15th National Computer Security Conference*. pp. 554–563

[8]."Lijun Mei,W.K. Chan and T.H. Tse""A Tale of Clouds: Paradigm Comparisons and Some Thoughts on Research Issues""IEEE Computer Society Press, Los Alamitos, CA (2008)".

[9]."Rajkumar Buyya1,2, Chee Shin Yeo1, and Srikumar Venugopal""Market-Oriented Cloud Computing Vision, Hype, and Reality for Delivering IT Services as Computing Utilities".

[10]."Byron Ludwig and Serena Coetzee""A comparison of platform as a service (PAAS) clouds with a detailed Reference to security and Geoprocessing service".

[11]."Alexander Lenk, Markus Klems, Jens Nimis, Stefan Tai and Thomas Sandholm""What's Inside the Cloud? An Architectural Map of the Cloud Landscape".

[12]."Ravi Sandhu""Future Directions in Role-Based Access Control Models".

[13]."David F. Ferraiolo and D. Richard Kuhn""Role-Based Access Controls"".

[14]."Ravi Sandhu""Future Directions in Role-Based Access Control Models".

[15] Benjamin Aziz, Simon N. Foley, John Herbert, Garret Swart, "Reconfiguring Role Based Access Control Policies Using Risk Semantics", Journal of High Speed Networks, Vol: 15, No: 3, pp: 261-273, 2006.

[16] R.S. Sandhu, E.J. Coyne, H.L. Feinstein, and C.E. Youman."Role-based access control models", IEEE Computer, Vol:29, No: 2, pp: 38–47, 1996.

[17]"MicrosoftWindowsAzure"http://www.microsoft.com/windowsazure/

[18] Uday O. Ali Pabrai, "HIPAA Security and Role Based Access Control (RBAC),"HIPAA Academy, September 5,2003.