Volume 3, Issue 6, June 2013 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

A New Advance Efficient RBAC to Enhance the Security in Cloud Computing

Parminder Singh
Research Fellow
Sri Guru Granth Sahib World University,
Fatehgarh Sahib, Punjab, India

Sarpreet Singh
Asst. Professor
Sri Guru Granth Sahib World University,
Fatehgarh Sahib, Punjab, India

***Abstract* — Cloud computing is one of the emerging technologies. The cloud environment is a large open distributed system. It is important to preserve the data, as well as, privacy of users. Access Control methods ensure that authorized user's access the data and the system. Current Role Based Access Control architecture has a lot of drawbacks which can be minimized by this proposed architecture. This paper presents a new extended architecture of RBAC which can resolve the security issues and data loss issues by using restriction policy on number of roles, number of users per role and number of transaction per day/hour/user. At the end this work is compared with the previous one and shows that this new advance architecture helps to improve the level of security.**

***Keywords*— Cloud Computing, Access Control, Role Based Access Control, Security, Backup.**

I. INTRODUCTION

1.1 Cloud Computing

Cloud Computing is a boom in the field of development and application modification in this modern world. In the previous age of the development, the use to create applications on the local server and also use to keep them on the local server. If the local server that is the local system crashes, the entire system and application crashed automatically. It was getting into a huge problem all over the world. To overcome this problem, the concept of cloud computing was brought into action. Brand Software Companies like Google, Microsoft, and Facebook started their own cloud over which now these days, data is available in bulk.

The term cloud computing probably comes from (at least partly) the use of a cloud image to represent the Internet or some large networked environment. We don't care much what's in the cloud or what goes on there except that we depend on reliably sending data to and receiving data from it. Cloud computing is now associated with a higher level abstraction of the cloud. Instead of there being data pipes, routers and servers, there are now services. The underlying hardware and software of networking is of course still there but there are now higher level service capabilities available used to build applications. Behind the services are data and compute resources. A user of the service doesn't necessarily care about how it is implemented, what technologies are used or how it's managed. Only that there is access to it and has a level of reliability necessary to meet the application requirements. Cloud computing really is accessing resources and services needed to perform functions with dynamically changing needs. An application or service developer requests access from the cloud rather than a specific endpoint or named resource. What goes on in the cloud manages multiple infrastructures across multiple organizations and consists of one or more frameworks overlaid on top of the infrastructures tying them together. Frameworks provide mechanisms for:

- self-healing
- self monitoring
- resource registration and discovery
- service level agreement definitions

1.2 Architecture of Cloud Computing:

- Hardware layer is responsible for managing the physical resources of the cloud, including physical servers, routers, switches, power and cooling.
- The Infrastructure layer creates a pool of storage and computing resources by partitioning the physical resources using virtualization technologies.
- The platform layer built on two of the infrastructure layer, the platform layer consists of operating systems and application framework. The purpose of the platform layer is to minimize the burden of deploying applications directly into VM containers.
- The application layers at the highest level of the hierarchy, the application layer consists of the actual cloud applications. Its purpose is leverage the automatic scaling feature to achieve better performance, availability and lower operating cost.

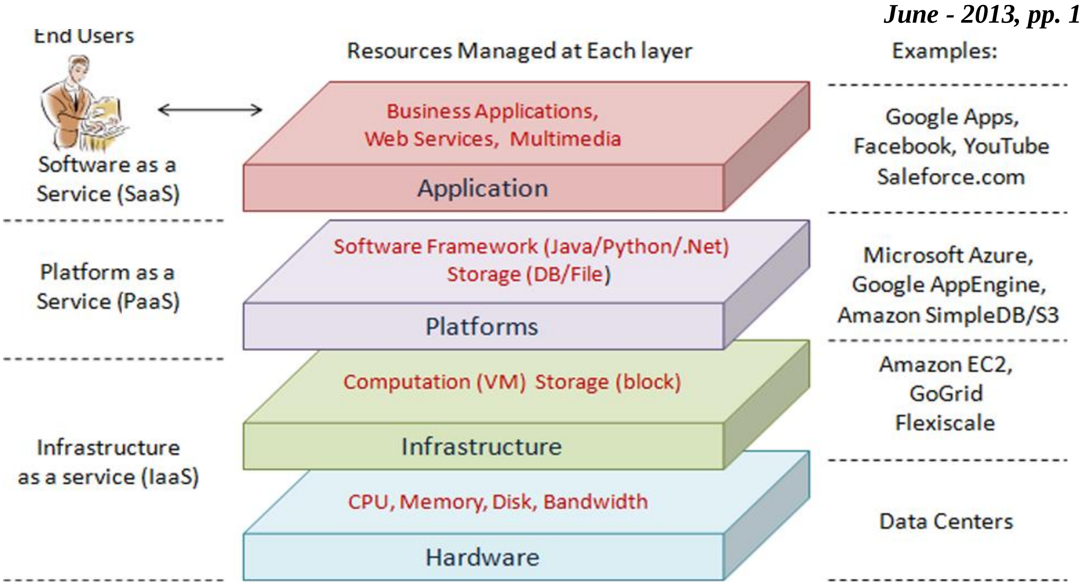

End Users
Resources Managed at Each layer
Examples:
Business Applications, Web Services, Multimedia
Application
Google Apps, Facebook, YouTube Saleforce.com
Software as a Service (SaaS)
Platform as a Service (PaaS)
Software Framework (Java/Python/.Net) Storage (DB/File)
Platforms
Microsoft Azure, Google AppEngine, Amazon SimpleDB/S3
Computation (VM) Storage (block)
Infrastructure
Amazon EC2, GoGrid Flexiscale
Infrastructure as a service (IaaS)
CPU, Memory, Disk, Bandwidth
Hardware
Data Centers

Fig. 1 Cloud Architecture

1.3 Cloud Computing Deployment and Service Model:

- Software as a Service - A SAAS provider gives subscribers access to both resources and applications. SAAS makes it unnecessary for you to have a physical copy of software to install on your devices. SAAS also makes it easier to have the same software on all of your devices at once by accessing it on the cloud. In a SAAS agreement, you have the least control over the cloud.
- Platform as a Service - A PAAS system goes a level above the Software as a Service setup. A PAAS provider gives subscribers access to the components that they require to develop and operate applications over the internet.
- Infrastructure as a Service - An IAAS agreement, as the name states, deals primarily with computational infrastructure. In an IAAS agreement, the subscriber completely outsources the storage and resources, such as hardware and software that they need.

1.4 Advantages of Cloud Computing

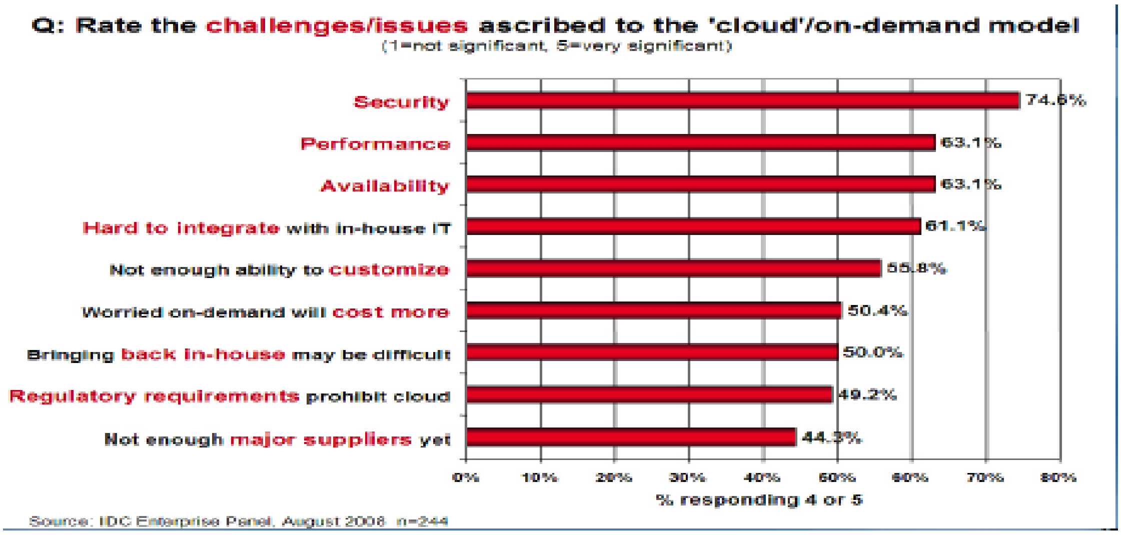
- Lower-cost computers for users
- Better performance
- Less IT infrastructure costs
- Less maintenance costs
- Lower software costs
- Automatic software updates
- Increased computing power
- Unlimited storage capacity
- Increased data safety
- Anywhere access to your documents
- Latest version availability
- Use your computer from anywhere

1.5 Disadvantages of cloud computing

- Internet connection is required
- Low-speed connections are not recommended
- Sometimes is slow
- Stored data might not be secure
- Your data is 100% in the cloud

II. SECURITY IN CLOUD COMPUTING

Cloud computing is becoming very popular computing paradigm for network applications in open distributed environments. In essence, the idea is to host various application servers in a virtual network environment (Cloud) and offer their use through the concept of (Web) and other services. Contrary to classical network applications approach in the form of client–server model, in a cloud environment users do not access individual application servers, do not establish direct connections with them, do not send request messages directly to those servers, and do not receive direct replies from them. Instead, clients access those application servers through cloud access proxies, special servers that perform publishing and exporting various (usually Web) services available in a cloud. In such environments, security has much more important role than in classical network, client– server, environments. Not only that the same, standard, security services are needed (authentication, authorization, confidentially, integrity, authorization, etc.), but their provision must be offered to clients transparently and in an environment comprising distributed components and delegated authorities. Cloud computing makes security not only much more important, but also much more difficult to organize and manage, due to the transparent nature of cloud resources, components, and services. There are still many open and interesting issues regarding cloud computing paradigm and standards are still evolving. But, it is a general opinion that security is indeed one of the most important issues. In the recent IDC report over 74% of users think that security is dominant issue for widespread use of cloud computing services:



Source: IDC Enterprise Panel, August 2008 n=244

Fig. 2 Importance of Security for Cloud Computing Environments

2.1 Major Risks of Cloud Computing Security

There are a lot of security issues in cloud computing service environments such as virtualization, distributed big data processing, serviceability, traffic-handling, application security, access control, authentication, cryptography and etc. Especially, data access using various resources needs user authentication and access control model for integrated management and control in cloud computing environments. Cloud computing security is a hot topic for research, its freshness, interestingness and recognition created an appeal for researches to pursue this topic in specific. Many security concerns evolved while weighing the benefits of using cloud computing over local resources. Below are the major risks introduced by the cloud are:

- Data Storage
- Legal and Regulatory Risks
- Privacy and Confidentiality
- Availability
- Integrity
- Computationally feasible
- Proper usage metering
- Internal and external attacks
- Abusing cloud's resources

III. ACCESS CONTROL MODELS IN CLOUD COMPUTING

Research on access control models was started in the 1960s and 1970s by the two thrusts of mandatory and discretionary access control. Mandatory access control (MAC) came from the military and national security arenas whereas discretionary access control (DAC) had its roots in academic and commercial research laboratories. These two thrusts were dominant through the 1970s and 1980s almost to exclusion of any other approach to access control models. In the 1990s we have seen a dramatic shift towards pragmatism. The dominant access-control model of the 1990s is role-based access control (RBAC).

3.1 MAC-In the Mandatory Access Control (MAC) mode, users are given permissions to resources by an administrator. Only an administrator can grant permissions or right to objects and resources. Access to resources is based on an object's security level, while users are granted security clearance. Only administrators can modify an object's security label or a user's security Clearance.

Advantages of MAC

In MAC information integrity will increase and also it prevents the flow from low objects to high objects. This information controlling will achieve the integrity. MAC mostly used in military and government applications. MAC provides multilevel security .Prevents from unauthorized users from making changes. When we consider the flow of information in the vertical order it will provide the multilateral security. In MAC every access to the user will be mediated so the information that is accessed through cloud is more secure. Here access is authorized or restricted to objects based on the time of day depending on the security level on the resource and user credential. Scalability in MAC is lower and also it won't be adapt to all type of applications.

Disadvantages of MAC

The major drawback in MAC is that once the security level is identified to particular subject in the hierarchy it won't modify the security level.

3.2 DAC-In the Discretionary Access Control (DAC) model, access to resources is based on user's identity. A user is granted permissions to a resource by being placed on an access control list (ACL) associated with resource. An entry on a resource's ACL is known as an Access Control Entry (ACE). When a user (or group) is the owner of an object in the DAC model, the user can grant permission to other users and groups. The DAC model is based on resource ownership.

Advantages of DAC

The DAC mechanism provides the flexibility of usage on information. This method will maintain the authorization database which consist number of authorized user.

Disadvantages of DAC

In DAC there is no assurance on flow of information and also there is no restriction on the usage of information this will make the confusion on the usage of information and also information will be lost. It can be easily attacked by third parties. There is no consistency on information. There might be the chance to steal the copy of original message without owner's permission. Sometimes owner may change the DAC policies by inserting malicious program.

3.3 Role Based Access Control- According to [RBAC] regulating access to computer or network resources based on the roles of individual users within an organization. Role based Access Control (RBAC) model is more emphasized recently due to its simple, scalability, fine-grained control ability, and has been proven to be efficient to improve security administration with flexible authorization management. In this context, access is the ability of an individual user to perform a specific task, such as view, create, or modify a file. Roles are defined according to job competency, authority, and responsibility within the organization.

Within an organization, Roles are created for various job functions. The permissions to perform certain operations are assigned to specific roles. Members of staff [or other system users] are assigned particular roles, and through those roles assignments acquire the computer permissions to perform particular computer system functions. Since users are not assigned permission directly, but only acquire them through their role [or roles], management of individual user rights becomes a matter of simply assigning appropriate roles to the user's account, simplifies the common operations, such as adding a user, or changing a user's department.

3.3.1 Three primary rules defined for RBAC

1) Role assignment:**-** A person can exercise a permission only if the person has selected or been assigned a Role.

2) Role authorization:**-** A person's active role must be authorized for the person. This rule ensures that users can take on only roles for which they are authorized.

3) Permission authorization:**-** A person can exercise a permission only if the permission is authorized for the person's active role. With rule1 and rule2, this rule ensures that users can exercise only permission for which they are authorized.

Advantages of RBAC

It provides hierarchy roles of access based on many applications. Roles are assigned based on the least privilege for the particular object, so this will minimize the damage of information by intruders. Separation of roles will be maintained so there is no chance of misuse of information because each user assigned to individual roles. This separation of roles can be either static or dynamic. RBAC provides the classification of user based on their executing environment.

Role Based Access Control has following administrative policies. Those are Centralized, Hierarchical, Cooperative, Ownership, and Decentralized. In large distributed system centralized access right is not appropriate.

Disadvantages of RBAC

Sometimes it is difficult to reach which privilege to which user it has been associated with a particular role. Permissions associated with each role can be deleted or changed based on the privilege of role change. Job roles are assigned based on the least privilege but still change of role of user might have some confusion when considering the permissions of each user associated with that role.

IV. DESIGN & EXPERIMENTAL RESULTS

In Our approach, we are trying to increase the security by extending the architecture of current RBAC and create new advance RBAC architecture. Problems in current RBAC:

1. There is nothing mentioned in current **RBAC** that how many user would be there per Role. This may lead to a hacking environment.
   E.g.:**-** Suppose somebody hacks the role which we have generate [although cloud computing is very secure]. When the hacker user will try to access the content of the current **RBAC,** then normal RBAC will not restrict him from accessing the content because it allow to do so.
2. Suppose we have made some restriction over the generation of new ID of the specific role. Then also there is the possibility for the hacker to hack the existing ID and to hack the entire transaction.
   To overcome this problem we can put restriction of number of transaction per day. So that in any case if any existing Id gets hacked a minimum amount of damaged.
3. Third problem is that, **RBAC** concept sends data directly to the cloud computing sever, he never keeps a copy for any kind of backup or so.

Suppose if administrator is creating something, he might make a mistake and the data could be in incorrect security format which again leads to the data security threat.

To overcome these problems, we can create "**New Advance RBAC Architecture"** system which a kind of Ontology which can keep backup of the data which is getting send to the cloud server and to restrict the number of users per role.

For this purpose we will have to implement security policies to a local cloud sever just to make sure that the data which is getting stored over the main cloud server has a backup for restoration, if something goes wrong, also if the number of users per role exceeds, the admin of the system should get a alarm or something so that he can come to know that security threats has attacked the system.

4.1 Proposed Model

The proposed model focuses on following new features for advance RBAC with the objective to create New Advance RBAC Architecture for increasing security and is practically implemented using .NET environment for web hosting server & window azure for database.

New features for Advance RBAC:-

- Limit over the number of user per role.
- Limit over the number of transaction per day or per hour.
- Keep backup data for restoration.
- Increase the security.

4.2 Basic Block Design

Role-based access control (RBAC) is Ontology and it is a combination of mandatory and discretionary access control. It is complete Architecture. In the role-based access control model, a 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.

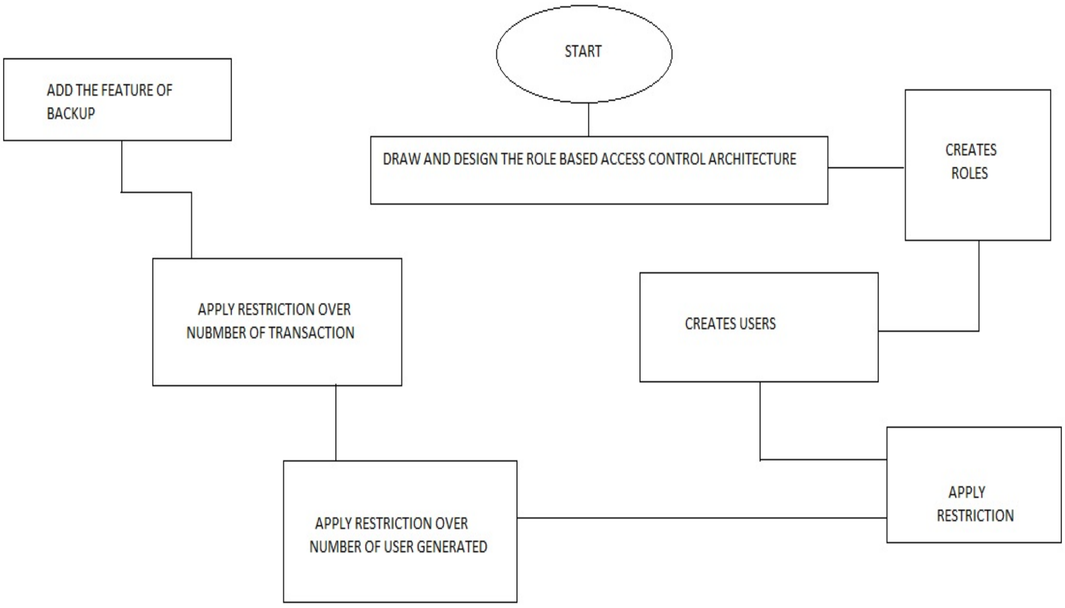

START
DRAW AND DESIGN THE ROLE BASED ACCESS CONTROL ARCHITECTURE
CREATES ROLES
CREATES USERS
APPLY RESTRICTION
APPLY RESTRICTION OVER NUMBER OF USER GENERATED
APPLY RESTRICTION OVER NUBMBER OF TRANSACTION
ADD THE FEATURE OF BACKUP

Fig: 3 Basic Block Design for Advance RBAC Architecture

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. To Create a Architecture which can provide the users of this system an access control through which they can access the content of the system. The administrator of the system can be providing access control by the users of facility. And then RBAC system has been implemented. Our objective and motive is to create an Advance RBAC to enhance the security of entire application. Our objective may also include reducing the burden of administrator of the system. Fig 5 shows the basic block design for new advance RBAC where after designing the RBAC architecture, Roles are created and then restrictions are applied on it. These restrictions are on number of users, number of transactions and also add a new feature of backup.

4.3 System Level Design

Fig 4 shows the System level design for new advance RBAC, where admin performs their restrictions over the existing RBAC. This design describes the working of the new RBAC.

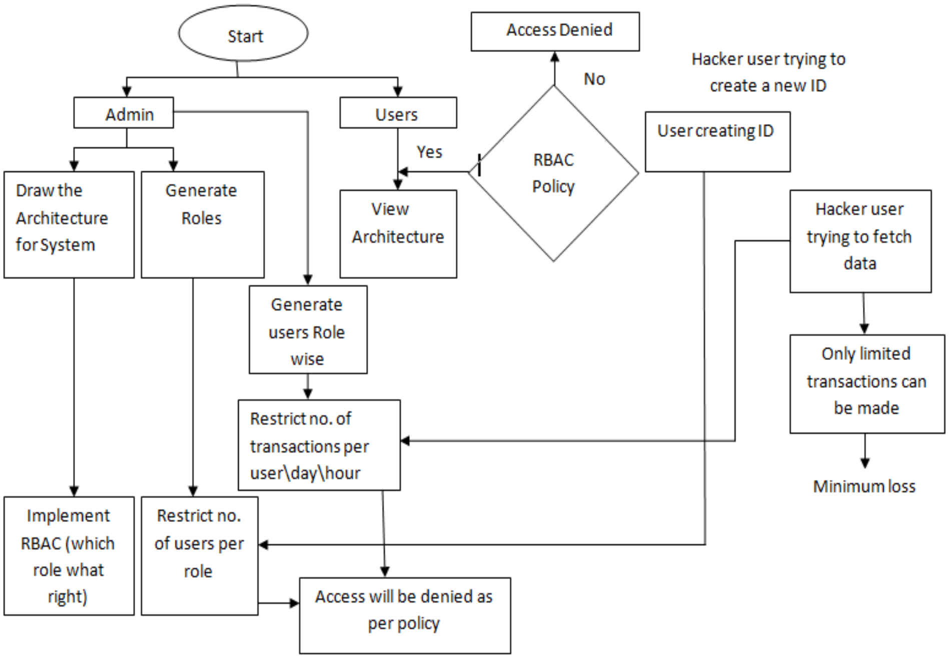

Start
Admin
Users
Access Denied
No
Yes
RBAC Policy
Hacker user trying to create a new ID
User creating ID
Draw the Architecture for System
Generate Roles
Generate users Role wise
View Architecture
Hacker user trying to fetch data
Only limited transactions can be made
Minimum loss
Restrict no. of transactions per user\day\hour
Implement RBAC (which role what right)
Restrict no. of users per role
Access will be denied as per policy

Fig: 4 System Level Design for New Advance RBAC Architecture

This system can be divided into three levels: 1) Admin 2) User 3) Hacker

4.3.1 Admin: In an organization admin create the architecture for system and then generates the roles for all users according to their privileges and also make restriction on the number of users per role. Admin also generate users' role wise where restrictions can be made on number of transactions per day/user/hour. This helps to increase the security level.

4.3.2 User: A new user create new account but according to restriction on number of users per role only limited number of users can create their account and because of this malicious attacks will be lesser. Already existing users can login and get access only if they are valid user.

4.3.3 Hacker: No malicious users get access to the system because numbers of users get restricted in some limit. But if any case invalid user or hacker get access on the system and trying to fetch data so, because the restrictions or new architecture of RBAC only limited number of transactions can be accessed by him. So, this results minimum loss.

4.4 Results

This proposed model compare with the current RBAC and showing the results in Fig 5 and it concludes that this new advance RBAC architecture having better results. It means security level can be enhanced or improved with the help of this new architecture. This new architecture increase the security by making restriction on number of users per role, number of roles & number of restrictions. One new feature is added into this architecture and that is backup policy which helps to reduce the data loss.

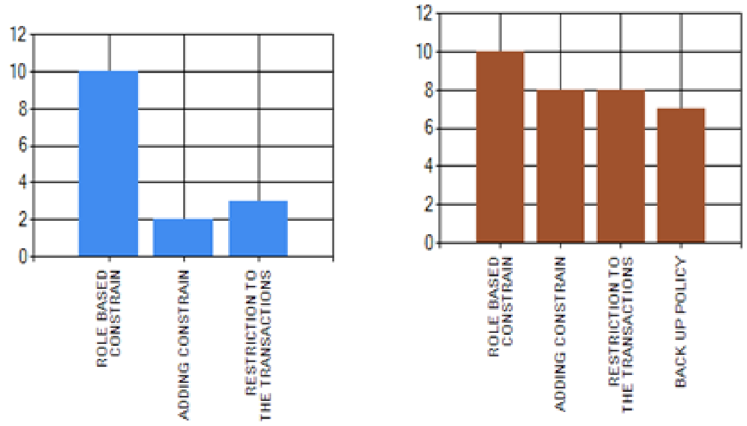


Fig 5 Conventional RBAC & Extended RBAC

V. CONCLUSION & FUTURE SCOPE

The researchers have put a lot to make the cloud computing system secure. For the same purpose time to time new methodologies and ontology has been introduced. One of the ontology is called RBAC system. Role Based Access Control is an architecture which provides the authority to restrict the user if he is not allowed to go on with the content .It has been affective in a lot of Manner. This architecture saves the data from the unauthorized use of the data. The admin panel has all the rights to restrict the user of accessing the data and back again he can again edit the access rights of the user. Proposed Work of Role Based Access Control: The current RBAC system does not talk about the limitations over the number of user per role so that the admin can come to know that is there any fake user in the proposed role category or not . Our work includes the restriction over the roles generated .We can limit the number of users through the admin panel so that the chances of hacking the user id and generating a fake id to access the data will be prohibited.

Future Scope or Role Based Access Control: Although our proposed work proposed a healthy mechanism for the security of data but still there is point of number of transaction by one id of one specific role which could be the loop hole of this Architecture. It means that what happens if a particular id gets hacked and he makes the transaction time by time. In the future , if some mechanism would be applied so that one Id can make a fixed number of transactions , then if the number of transaction will increase by that particular id , the admin will come to know through its monitoring system that unauthorized access has been made and it would be easier to take action against such happenings .

REFERENCES

[1] David F. Ferraiolo and D. Richard Kuhn, "Role-Based Access Controls", 15th National Computer Security Conference (1992) Baltimore, Oct 13-16, 1992. pp. 554 – 563.

[2] Ravi Sandhu, "Future Directions in Role-Based Access Control Models", 2001 Springer, pp - 22-26.

[3] Hazen A. Weber, "Role-Based Access Control: The NIST Solution", October 8, 2003.

[4] Ryan AusankaCrues, "Methods for Access Control: Advances and Limitations"2005.

[5] Paolina Centonze,Gleb naumovich, Stephen J.Fink,Marco Pistoia, "Role Based Access Control Consistency validation", Feb 13,2006.

[6] Ramadan Abdunabi, "Extensions to the Role Based Access Control Model for Newer Computing Paradigms", October 26, 2010.

[7] Shanshan LI, Qingbo WU, Lianyue HE, Lisong SHAO, Jie YU, "Debit: A Diversity-based Method for Implicit Role Transition in RBAC Deployments", CLOUD COMPUTING 2011 : The Second International Conference on Cloud Computing, GRIDs, and Virtualization.

[8] V.Sathya Preiya,R.Pavithra , Dr. Joshi, "Secure Role based Data Access Control in Cloud Computing", May to June Issue 2011.

[9] Dancheng Li, Cheng Liu and Binsheng Liu, "H-RBAC: A Hierarchical Access Control Model for SaaS Systems", 2011, 5, 47-53.

[10] Hema Andal Jayaprakash Narayanan, Mehmet Hadi Güneş, "Ensuring Access Control in Cloud Provisioned Healthcare Systems", 2011.

[11] Lan Zhou, Vijay Varadharajan and Michael Hitchens, "Enforcing Role-Based Access Control for Secure Data Storage in the Cloud", 2 September 2011.

[12] Wei-Tek Tsai, Qihong Shao, "Role-Based Access-Control Using Reference Ontology in Clouds", 2011 IEEE International Conference on Cloud Computing.

[13] Kan Yang, Xiaohua Jia, Kui Ren, "DAC-MACS: Effective Data Access Control for Multi-Authority Cloud Storage Systems", 2012.

[14] Michael S. Kirkpatrick, Gabriel Ghinita, and Elisa Bertino, "Privacy-preserving Enforcement of Spatially Aware RBAC", January 2012 .

[15] Chang Choi, Junho Choi, Byeongkyu Ko, "A Design of Onto-ACM (Ontology based Access Control Model) in Cloud Computing Environments", 2012.

[16] Abdul Raouf Khan, "ACCESS CONTROL IN CLOUD COMPUTING ENVIRONMENT", VOL.7, NO.5, MAY 2012.

[17] Samy Gerges, Sherif Khattab, Hesham Hassan, Fatma A Omara, "Scalable Multi-Tenant Authorization in Highly-Collaborative Cloud Applications, Vol.2, No.2, April 2013, pp 106~115.

[18] Mustapha Ben Saidi, Anas Abou Elkalam, Abderrahim Marzouk, "TOrBAC: A Trust Organization Based Access Control Model for Cloud Computing Systems", Volume-2, Issue-4, September 2012.

[19] Yan Zhu, Hongxin Hu, Gail-Joon Ahn, Dijiang Huang, and Shanbiao Wang, "Towards Temporal Access Control in Cloud Computing", 2012.

[20] Subhash Chandra Patel, Lokendra Singh Umrao, Dr. Ravi Shankar Singh, "Policy-based Framework for Access Control in Cloud Computing", (ICRTET2012).

[21] Reeja S L, "ROLE BASED ACCESS CONTROL MECHANISM IN CLOUD COMPUTING USING CO – OPERATIVE SECONDARY AUTHORIZATION RECYCLING METHOD", Volume 2, Issue 10, October 2012.

[22] Punithasurya K, Jeba Priya S, "Analysis of Different Access Control Mechanism in Cloud", International Journal of Applied Information Systems (IJAIS), Volume 4– No.2, September 2012.

[23] Canh Ngo, Peter Membrey, Yuri Demchenko, Cees de Laat, "Policy and Context Management in Dynamically Provisioned Access Control Service for Virtualised Cloud Infrastructures", 2012.

[24] Punithasurya K , Esther Daniel , Dr. N.A. Vasanthi, "A Novel Role Based Cross Domain Access Control Scheme for Cloud Storage", International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 2, Issue 3, March 2013.

[25] Sultan Ullah, Zheng Xuefeng, Zhou Feng, "TCloud: A Dynamic Framework and Policies for Access Control across Multiple Domains in Cloud Computing", Volume 62– No.2, January 2013.

[26] Sugata Sanyal, Parthasarathy P. Iyer (Corresponding Author), "Inter-Cloud Data Security Strategies"2013.