I-RBAC (Managing Identities with Role Based Access Control) for Private Cloud

Authors

Priya P. Sharma¹ Chandrakant P. Navdeti²

Information Technology Department SGGS IE&T, Nanded, India
Email-priyasharma2090@gmail.com¹, navdetichandarakant@gmail.com²

ABSTRACT

Concurrent to the swift developments in cloud computing and its related services, an emerging trend has been witnessed to use the cloud for large-scale data storage. This has led to the stemming of an important security issue of a controlled and restricted access to the stored data and also the management of the identities of a large number of cloud users. A number of IT industries have started establishing a private cloud within the organization and are hosting various applications like HRMS, Financial Management, etc. in the on premise cloud. With an increase in the number of private cloud users, there is an additional concern for identity management security. Solutions provided by traditional access management methods prove inefficient in providing unauthorized accessing security and to ensure user privacy while providing the private cloud user to public cloud resources. In this paper describes I-RBAC mechanism which is a set of two major security concepts in Industry Identity Management and Role Based Access Control. The primary objective of identity management in cloud is managing identity information so that access to resources, data and services is controlled properly. (RBAC), which provides flexible controls and management by having two mappings, users to roles and roles to privilege/permissions on data objects. This paper discusses the implementation for private cloud based on these two major concepts.

Keywords—identity, SAML, private cloud, provisioning, security, approval, cloud, RBAC, identity management

1. INTRODUCTION

Cloud computing is perceived as a boon in the field of development and application modification for the modern world. In the previous age of development, users used to create applications on the local server and used to keep them on the local server. If the local server crashed, the entire system and the applications would crash automatically. This was witnessed as a showstopper for an organization and its dependencies all over the world. To overcome the problem of server crashing, cloud computing was brought into action. For
most enterprises, the advantages of cloud applications are driving significant operational changes in IT. Some of the major enterprise applications being moved onto the cloud are Enterprise Resource Planning, Human Resources, Finance, and Sales &Marketing, according to a member survey of the Open Data Centre Alliance. The aforesaid survey reported that the members are scaling cloud adoption 15 percent faster than previously forecast. Half say they will run more than 40 percent of their IT operations in a private cloud by the year 2015. A quarter of the respondents are planning to use the public cloud to run their applications. A three-fourth are looking forward to harness applications deployed on public-private cloud partnership [2].

At present, there are three typical deployment options available for the private, public and hybrid cloud applications. They are:

- Infrastructure-as-a-Service (IaaS)
- Platform-as a Service (PaaS), and
- Software-as-a-Service (SaaS).

Irrespective of the numerous benefits provided by cloud, it is crucial to be aware of the hidden and visible risks while dealing with cloud architecture on a business perspective. The two most important concerns for an IT professional before moving to the cloud architecture should be Security and Privacy. These hold true irrespective of your role, a vendor, a broker or a customer. Instance of security breach with private enterprises have been reported, and public clouds are also not insulated from these situations. The most basic security and privacy example includes data storage and data transfer protection; vulnerability management and remediation; personnel and physical security; application security; data privacy; and identity management.

Given its architecture, an emerging choice for certain organizations are private cloud computing, nevertheless it comes with its own security challenges. Major Fields of concern include user lifecycle management, compliance, and federated identity management for collaboration with partners, suppliers, and customers, access management, etc.

1.1 Existing System

Back in the days of client-server computing model, managing identity was a lot simpler. In such scenarios, the users were primarily limited to a desktop PC with another set of credentials to a bunch of servers, setting up Access Control Lists; distribute roles and that was it. But with the expansion of servers, there was a multiplication of applications and the ‘endpoints’ shifted from desktop to remote devices and there was an integration of servers to other domains [8].

As time passed by, we started using directory services for providing a Single Identity Management repo to help propagate identity across the entire organization. Now, there is a bombardment of external service providers, Financial apps, Storage on cloud, social networking and related medium, workflows, CRM, collaborations, networking and emails to name a few. Though these are business critical, they do not directly link to traditional directory services.
As in a private cloud, the workflow is simple. Take the case of Identity and access management, an admin creates groups, users and bestows upon the users the required privileges. With an increase in the number of the users, their data also increases in parallel. The primary objective of cloud is sharing and managing the identity of cloud users in a continuous and secure fashion. As information multiplies with every passing time frame, it lies susceptible to potential point failure or human factor open. As human factor creeps in, an enormous oversight potential can be caused due to which volatile and sensitive data can be stored at unsecure locations and can be exposed to unauthorized users. Unsecured storage can make the data vulnerable at the hands of hackers leading to a security breach. User identity and access management coupled by the provision of resources to a large number of users applying the traditional mechanisms will only escalate the security issues.

Assume the instance of the problems faced by any user provisioning approach pertaining to direct assignments. You have to set access privileges for some a thousand employees, multiply that by the number of applications in the infrastructure. Also be reminded of the fact that employee work responsibilities are in a state of constant flux and we quickly realize that a more efficient solution is desired.

Traditional methods that exist might not be able to secure the Enterprise applications, the data that comes with it along with managing the user’s identities. Presently number of identity management with distributed and desolate access control solutions are being developed and at the commissioned. Private cloud calls for an effective answer and approach. Acknowledging the fact that a number of major security issues and identity management concerns have not seen their resolution at the hands of traditional methods, we propose a solution based on a combined concept of identity management and role based access control with Single Sign-On using Security Assertion Mark-up Language as an authentication mechanism.

Owing to a shortage in administrative accountability, lack of effective secure release controls, limited implementation of strong inter-application authentication, feeble monitoring of privileged activities and enforcement of privileged activity policies, shortage of change controls, poor implementation of consistency in password change policies has led rise to privileged(role based access control) identity management. These issues are countered by using Privileged Identity Management implementation, which helps in cushioning the impact of all these challenges as they tend to focus on the privileged user environment within an organization.

Our paper emphasizes on the use of Identity Management coupled with Role-Based Access Control (RBAC) under the private cloud environment. This would lead to each user being assigned one-to-many roles whereas each role is assigned distributed privileges. As a matter of fact, such distributed assignment of authority can comfortably lead to the management of accessibility rights of users. This in turn maintains application independence and isolation of data thereby improvising on performance of the entre process and security in the much needed cloud environment [10].

1.2 The Need for another system
A major concern for business is identity management today is the increasing number of web-based applications, the buildup of users in private cloud, and the snowballing of data. To give you an idea, just try recollecting the number of usernames and password you punch in every day. You must definitely be logging into your company portal, your mails, benefits systems, some or the other cloud based app, etc. Just try to multiply it by the security implications this has. You will need dedicated resources for identity store management, provisioning a deactivation of users that are no longer with the organization and responding to password requests. Imagine the man hours you could save by truncating at least a quarter of the passwords and their associated costs.

As a vision and need to properly control the resources, data, applications and services, the basic role of Identity Management in Cloud is set as managing personal identity information. It has been perceived as an area of industry security that goes ahead to offer the genuine benefits beyond its scope by bringing down the risk associated with security breaches. Centralizations of the log in the procedures of different applications in a single system providing accessibility with only one password can be bought about by Single Sign-On. Only the application that the user is entitled to, will be made available after punching in the right password. In short, this provided for the users to access all the systems with only one password.

The paper is presented as follows: in section II we have discussed about our related works, section III describes the terminologies, which are basic building blocks to implement the prototype, in section IV we have presented the architecture of I-RBAC, and lastly implementation of prototype is explained in section V.

2. RELATED WORKS

To secure the cloud resources from unauthorized and unwanted access is the numoro uno step in providing secure and reliable cloud computation. Today, there are many could computing platforms that are available that help in the implementation of Role based access control and Identity Management. But for enhancements to the capabilities, there are still many researches that are in progress. We still face some inefficiency in the existing solutions used by different cloud providers available in the market.

We can take an example of AWS IAM, which enables cloud customers in managing user and user permissions to secure their resources in clouds. But, a number of limitations for IAM implementing enterprise cloud customers can be identified. Let’s have a look at a few of them [3]; We observe that IAM facilitates the direct assignment of permission to users. With an increase in the number of users and the outsourcing computing infrastructure of IaaS, the result can be very unexpected and titanic in volume.

   a. Since the number of users increase and the mapping between the users and permissions het complicated, the management costs are also bound to go high.

   b. A number of privately implemented clouds continue to face still faces identity crisis or related problems like -security of users, data, provisioning the resources to users, access control management, etc.
Network protection and security along with the assurance that private integrity of the intellectual property of users is pitched high on the list of most large organizations. Additionally, a number of strict privacy protocols tend to impose enhanced levels of confidentiality. Take the example of; health care and insurance companies, Banking and Financial institutions, IT industry, etc. This implicates, Identity management has come a long way to establish itself as a critical component in ensuring information security and access control. There are still many organizations that rely on individual, user-based identity management mechanisms built into the operating system and individual software applications. But, with an increase in the number of users and applications, the task of supporting this system tends to become more time-consuming, unyielding and cost ineffective. Users tend to get annoyed by the mention and the need of remembering multiple passwords. Help desks and supporting services like Customer care and BPO’s get spammed by the plethora of requests for lost, forgotten and wrong passwords coupled with new joiner registrations and account closure of former employees.

Provision for central management of the accounts on a number of target systems could be made using the existing solution, but it demands considerable IT resources to manage connectivity with the target systems. Access to enterprise data is looked up by all, namely customers, partners and employees. However, as the organization grows more complex in nature with addition to new systems, applications and interfaces, it becomes more and more challenging to keep a strict watch on who can access what data. Looking at the risks of permissions that are ineffective, we see that they are many. To name a few, unlawful entry or access to IT resources can create panic to the applications environment. Companies could dampen their image for not meeting security compliance and issues could be raised. In addition, the IT support desk could spend a sizeable amount of their time in resolving these issues, which otherwise could have been used for more productive purposes. On talking to employees form my organizations IT departments, they say that the maximum challenge is faced on two counts. Primarily when an employee commissioning (or de-commissioning, when he/she leaves the organization) is initiated. Assume that the commissioning process is age old, new recruits could spend long hours or worst days to get access to important applications and resources. Conversely, if the user’s records and privileges are not decommissioned correctly, there could be challenges in the form of trespassing data, which could come up as a serious security threat.

And that’s not the end of it. Unlawful users could be exposed to the intranet or service portal, compromising sensitive data. It is expected that the database of the company be able to leverage user identities for authentication and authorization, to decimate trespassing, and enhance the user interface of the portal. There have been cases in some organizations where their provisioning methods were proving futile in handling the increasing compliance demands and the complex nature of the business environment. Going by the existing solutions at hand, there can be a provision of central management of accounts leveraged on multiple target systems, but there are a large number of IT resources that would be involved to manage connectivity with target systems. Take into account the scenario of the organizations private cloud. For the
new recruits, the boarding process depended on manual requests and with was followed by provisioning that too was manual. A new solution was employed in a MODEL AFTER approach for requesting access to new recruits. In time, it was realized that the system was providing more access than required. Thus landing the company in a case of compliance issues. As parts of an effort to get the access rights corrected, the corresponding requests had to be adjusted a number of times, which would lead to complications in accurate tracking of user’s right access. This in turn would lead to prolonged intervals to assign access privileges to new recruits and internal transfers, thus leading affecting the productivity sphere. In the same fashion, revoking access of former employees was a manual process requiring senior management for requesting termination. The same accounts were prevented from getting automated and committing to the system.

The prevailing methods at disposal were short of a centrally controlled authority for profiles of users and their related attributes, thus making the organizations end systems not being unmanned in mapping user profile attributes.

What we tend to do is, proposing an alternative which tries in resolving the limitation which takes into account the above identity management, role based access, identity management, user life cycle management in the private cloud. Our solution finds its roots in the concepts of Identity Management, Role Based Access Control which is in turn is necessitated using XACML and authentication of user SAML SSO, this as a whole we term as ‘IBRAC for cloud’ which helps in forming a safe and secured fix for the cloud enterprise. Assisted by this mechanism, one can enforce policies for enabling access to respective individuals, when this can be accessed enforcing location constraints and also setting time restriction on the duration of the access and the data associated with it. At the onset of the establishment of the credentials, the users who have been authorized will have an SSO access. The same can be used for user on-boarding and layoff process, assigning cross cloud transposing of data i.e. from private to public and vice-versa. The best part is, we can reassure all entitlements in the time period and withdraw them as per the necessity. Here, we take the opportunity to emphasize how a company can take identities based on roles, as a route to make the provisioning possible in an organizations cloud automatically.

3. PRELIMINARIES

A. Role-Based Access Control

There can be two phases for assigning privileges for a user under Role Based Access Control. As shown in the figure 1, we can see that roles have been assigned to identities in the first phase. The second phase lies witness to the fact that a check is performed against the required operations or policies. In Role Based Access Control, Roles have permissions and related privileges, rather than the USER. [2, 4] The factors of responsibility and authority based on the organizations lines might lead roles to have a hierarchical structure. The resources are assigned to the users/identities based on the roles they are attending to [11].
Roles have certain privileges that are granted to them. Suitable users are assigned these roles. As we can see that the different functionalities such as add, delete, query and modification of the granted privileges are applicable to the concept of 'Roles', and not the individual user, this helps greatly in the simplification in privilege management. With respect to the above cited reasons, our paper is proposing identity management coupled with Role Based Access Control, termed as IRBAC which facilitated the integration of a set of Identity Management and RBAC considering the role and responsibilities of a multi-user in a private cloud setup [11].

A. Policies

Business goals and SLA’s in an enterprise help in defining and deriving policies. Policies are nothing but a standard protocol that can be deemed as rules governing the choices in behaviour of a system [15]. Factors such as determination of decisions and execution of actions are based on policies. It is best described as an action plan. The language used for writing policies is XACML. The various types of policies are Access Policies, Authorization and obligation, password change policies, Restriction policies and so on [9].

B. Provisioning and De-provisioning

User provisioning also known as account provisioning technology is instrumental in creating, modifying, disabling and deleting user accounts and their related profiles over an IT infrastructure and business application. Approaches such as cloning, roles and business rules so businesses can automate on boarding, off-boarding and other administration workforce processes (for example, new hires, transfers, promotions and terminations) are implemented by provisioning tools. Also, automatic aggregation, and identity co-
relation of data from Human Resources, Customer Relationship Management, email systems and other identity storage systems are done by provisioning systems. HR system changes, management requests are responsible for fulfilment change. A major chunk of user provision implementations are based on regulatory compliance and effectiveness of the security implemented.

Specifically speaking, management of user rights and privileges is known as user account provisioning. It is one of the multiple IDM procedures available, and it defines the separate methods of management an individual’s entity in the digital world, the related authentication and authorization rights. In simple words, provisioning may be defined as the process of creation and co-ordination of accounts, e-mail authorization under the category of rules and roles, and similar responsibilities viz. making provisions of resources that are physical in nature to associate them to new users [1, 9].

C. Extensible Access Control Markup Language (XACML)

XACML as the name suggests is useful in describing a policy language and an access control decision which can be a request or response. Both of these are encoded in XML. General access control requirements are defined in the policy language. It has standard new points that are basically extensions that can be used in defining new functions, data types, combining logic, etc. A condition can be implied using the request response action stating whether a query should be allowed and interpret its result. An answer is always included regarding the response about using the four values: Permit, Deny, Indeterminate (an error occurred or some required value was missing, so a decision cannot be made) or Not Applicable (the request can't be answered by this service).XACML: used to express access control rules and conditions [5].

D. Security Assertion Markup Language (SAML)

Security Assertion Mark-up Language 2.0 (SAML 2.0) describes to a version of SAML standard for data exchange for authentication and authorization between different security domains. It is a protocol based on
XML. It makes use of security tokens that contain statements to pass information regarding a principal. At the two endpoints we have two parties, which in most cases is typically an end user, between a SAML authority which serves as an identity provider and a SAML consumer, which is a service provider. It makes the facilities of web based authentication and authorization scenarios which includes SSO, thus reducing the administrative overhead of distribution of multiple authentication tokens to a particular user entity. We have made use of SAML 2.0 in our implementation [6, 14, 15].

4. ARCHITECTURE

Here, we demonstrate the framework of our security enabled I-RBAC system. It is composed of a private cloud whose users viz. the admins, the IT professionals, etc. are provisioned the resources that available on the cloud. As demonstrated in the figure 2, IBRAC makes the provision of identity and access management for on-board cloud applications. IBRAC serves as a container and manager for Identities. The necessity of a user database at the disposal of the organization is not required. User’s login to I-RBAC can be granted access to the applications that connect it form both, within and external to the domains and platforms.

A. System Components

Let us have a glimpse of the architecture of the components and its enclosing system.

Public Cloud: This can be best described as a third party entity which resides outside the infrastructural boundaries of the company. It comprises of a number of resources, which are provided to the user by means of the I-RBAC mechanism. We have made use of the prevailing service provided by the cloud.

Private Cloud: This finds roots in the concept of privately managing and owning a repository. It can best described as an inbuilt datacentre which is hoisted and managed by a private organization. It boasts of a number of applications like Human Resources Management Systems, Financial systems and multiple other on-board applications that are stored with an organization [2]. Within the private cloud, the apps need to be accessed using Single Sign-On, facilitating the user to memorize a single login credential making use of the I-RBAC methodology. The person once logged in using the mechanism once logged in using the appropriate credentials, need not worry about re-entering the same at a later stage. I-RBAC is used by the private cloud to provide access. (Here soever, we have not addressed any authentication protocol. Any suitable authentication protocol can be implemented as per the needs.)

Input Business Logic: Well predefined business logics implement the transfer of data from the host system to the I-RBAC target system. They facilitate the following points of action:

- Matching of identities from the leading source systems: For some users (admin, employee, and IT professionals) there are datasets in multiple source systems in private cloud. They have datasets
stored in system for the administration of students and in system for personnel administration. These datasets need to be combined to one identity from the IDM systems.

- Consistency checks of imported data from different source systems in private cloud need to be checked on errors and conflicts.

- Attributes Creation:
The attributes can be created by the I-RBAC system itself. For example the I-RBAC system often creates the login name by itself based on details from the sources e.g. HRMS in private cloud.

Central Base of Identities: This data store will have all identities filed. The central base of identities will be the core of the whole I-RBAC system which needs to meet predefined safety measures.

Output Business Logic: The provisioning of data for the end system of I-RBAC is managed through a business logic which follows the assumptions mentioned below:

- Make provisions for the connected IT systems updating it with the latest data pertaining to the user and the corresponding authorizations.

- Make sure that the end systems have access to only the specified data.

The I-RBAC connects with public to provision the resources in public cloud to the user in private cloud.

B. System Workflow
Consider the system architecture shown in Figure 3, the role of each component is explained in system components section. Now lets us take an example scenario where a new employee joins the organization, his data is entered into HRMS system which is in private cloud, the user is provisioned to the AD(Active) on public cloud. The user now holds the account in AD. We can also have different employees who want to access different applications which he has granted access to in public cloud. The flow is explained in the figure 2.

Following is the typical “in the flow” process:
1. Employee wants to access a resource on public cloud say AD or some application, he raises a request for the same (Provisioning).

2. Employees trying to access the resources are redirected to I-RBAC and this sends an encrypted identity of their profile via HTTPS. The I-RBAC then authenticates the user’s identity.

3. Employees enter their network/AD credentials into the SSO widget to access resources.

4. The I-RBAC then authenticates the user’s identity. This then authenticates the employees to access the application automatically.

5. The Employee once authenticated, is checked for role to grant the access to resource. Once authorized the user is provisioned to the resource (LDAP, application).

6. Employees then see applications to which they have been granted access privileges. *(This is achieved via access policy management).*

7. Only the I-RBAC users, administrator and not the private cloud user is allowed to access the self-service of the I-RBAC for any modification or update if required.

8. Password management and user life cycle management, change management is carried out by I-RBAC.

9. The resource is de-provisioned from the user once the period is over or if the employee is leaving the organization or some reason.

5. IMPLEMENTATION

Based on our design, we have implemented a prototype system to provide I-RBAC services in private cloud and public cloud platform through a web browser interface as well as web services. The core services of the system are implemented in Java. The I-RBAC service is connected to public cloud using the cloud providers SDK and exposed as web services using Web-Logic server. The interfaces of the cloud are exposed as web services, and the web services are hosted in Web-Logic server. Both administrative users and normal users can log into the I-RBAC interface with their usernames and passwords. All entities of the major components in I-RBAC are stored in tables of a relational database. We have used SOA for approval workflow e.g., in request based approval when any approval is required from person’s manager, an approval request will go to his/her manager, in this scenario we have used SOA workflow, and it will evaluate the access policy. An administrative operation results in calling one or more APIs, e.g., to create a user, a group, a permission, or add or remove an access policy in the root user’s public cloud account.

6. CONCLUSION

The I-RBAC scheme we proposed in this paper helps in effective provisioning, user life cycle management, access control in between private and public cloud using the two well-known schemes identity management.
and role based access control. The users’ privileges are clear in the cloud application, which also helps the platform administrator to manage the user’s privileges. The main contribution of this paper is to provide a set of privileges and the identity management scheme for corporations in cloud computing environment. Such a scheme can be used to easily change employee privileges in the event of personnel changes and modify the role privileges directly when adding new functions to the system without the need to modify all employee privileges one by one. Not only does this approach facilitate customization of identity management, but it also reduces human error when a large number of employees need to have resource provisioning and their privileges modified.

REFERENCES

1. gartner.com-it-glossary-user-provisioning, “Gartner, IT-Glossary”,
4. Periswsoftware, “periswsoftware.com-peri_case_studies_rolebased”
6. Wikipedia.org, “SAML2.0”
14. Security Assertion Markup Language, A Brief Introduction to SAML, Tom Scavo, NCSA
15. Security and Privacy Consideration for the OASIS Security Assertion Markup Language (SAML) V2.0, Committee Draft 01, 18 August 2004