Journal of Advances and Scholarly Researches in Allied Education
Vol. 13, Issue No. 1, April-2017, ISSN 2230-7540

Cloud Computing: A Study of Cloud Architecture and Its Applications

Jagdish Kaur*

Assistant Professor, Department of Computer Science, DAV College for Women, Ferozepur Cantt

Abstract – Cloud computing is a defined as a machine that involves delivering hosted services over the Internet. Cloud computing emerges as a new technology shifted from the early techniques such as mainframe architecture to client–server. Cloud computing can be exemplify as fetching third party software and services on internet and paying as per need of individual user. It makes easier scalability and virtualized resources over internet as a service providing cost effective to customers. Cloud computing has proved as a disruptive technology and kick start with the presence of many vendors in cloud computing space. Cloud computing as a substitute for numerous technological approaches and business models such as SaaS, cluster computing, high performance computing signifies that the cloud can be treated as a superset of all the corresponding issues from these paradigms. In this paper we will discuss Life cycle management, Cloud architecture, Pattern in Cloud IDM, Volatility of Cloud relations.

Keywords:- Cloud computing, Life cycle Management, Cloud Architecture, IDM

---------------------------------x---------------------------------

INTRODUCTION

Latest technology expedites different service providers to join their efforts to address a larger business space. It is possible that consumers hold numerous accounts with the service providers like Flipcart, Amazon, etc. The visibility and scope of attributes for every identity has to be conformable against a central trusted policy framing authority, assumed by the systems. In such a system, much is at pale if identities are not managed with extreme care. Such things are routine to high end applications hosted on cloud computing environment. Identity management (IDM) considers an advantage in the whole area of cloud security. Cloud computing is a consolidation of various technologies to conformed the demands of an interdependent puzzle of software and services. This entail various IDM's, based on several technologies to interoperate and function as one centralized body over a carefully shared user space. Hence identity management cloud computing can do lot more that traditional IDMs cannot meet.

Most cloud pitcher has a clear and fix IDM solution with drawbacks that have to be understood. The challenge in this field is that there are ample efforts towards outsourcing the IDM that led to the concept of identity-as-a-service (IaaS) (Open Cloud Manifesto, 2009). IaaS vendors focus on comprehensive, interoperable and quick-to-deploy solutions.

UNDERSTANDING THE NEW DIMENSIONS OF IDM IN CLOUDS

An identity management in cloud computing has to manage certain points: Control points, dynamic composite/decommissioned machines, virtual device or service identities etc. Cloud formation is dynamic with servers launched or terminated, IP addresses dynamically reassigned and services started or decommissioned or re-started. So, unlike traditional IDM, merely managing users and services is not sufficient. When a service or machine is decommissioned, the IDM has to be informed so that future access must be revoked. IDM should save its whole information till it becomes active. At the same time to fetch its relevant saved data, it has to be monitored and granted by the defined access level for that mode as mentioned in SLA. Traditional IDM is not directly responsive for cloud computing due to these peculiarities of cloud.

IDENTITY LIFECYCLE MANAGNEMENT

Lifecycle management consolidates a unified and broad solution for managing the entire lifecycle of user identities and their associated credentials and entitlements. Broadly it is split into two components 1) the provisioning component 2) the administrative component. Administrative components are used to state delegations rules, providing self-service components to edit personal information or create requests to the users. Authorizing of administrative rights to local group or process-in-charge is very important for a volatile and dynamic cloud based scenarios. Decentralizing the tasks will lower the load on the authenticator component and also save time in making access control decisions.

Provision and De-provisioning

In cloud, provisioning means just-in-time or on-demand provisioning and de-provisioning means real time de-provisioning.

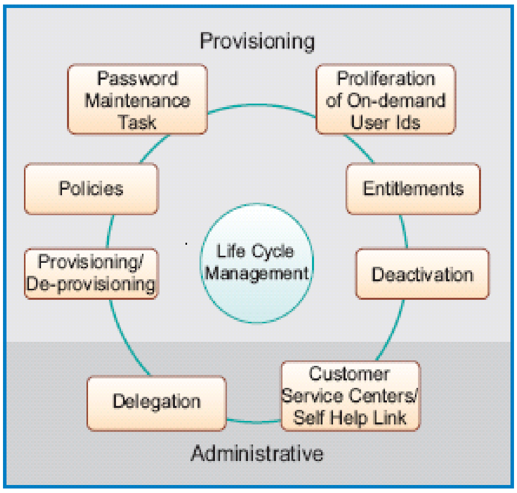

Provisioning
Password Maintenance Task
Proliferation of On-demand User Ids
Policies
Entitlements
Provisioning/ De-provisioning
Life Cycle Management
Deactivation
Delegation
Customer Service Centers/ Self Help Link
Administrative

Figure1: The Identity Life Cycle Management

Just-in-time provisioning reveal the federation of user accounts without sharing prior data, based on some trust model. Service Provisioning Markup Language (SPML) give XML based structures for representing provisioning or de-provisioning requests designed for identity lifecycle management (RSA's contribution to Cloud security guidelines, 2009**)**. SPML efficiently uses Service Administered Markup Language (SAML) affirmation and ease a complete trust model between senders and receivers. SAML describes an XML based framework for interchange security information for enabling SSO or identity federation regardless of the underlying architecture. OASIS Security Services is engaged on developing a SAML 2.0 profile for SPML. SAML can guide SPML to create trust and quantity, a subject against which the SPML provisioning request is targeted. This makes just-in-time provisioning and real time de-provisioning possible.

ENTITLEMENT

Entitlement refers to the set of attributes that specify the access rights and privileges of an authenticated security point. Due to shortcomings of interoperable portrayal of this information mien a challenge as the information needs to be traded among different cloud based service providers. In the awol of interoperable format, expensive and customized syntactic translation components are needed. The semantic aspect still remains to be tackled.

While some applications like SalesForce have predefined control for entitlement and authorization control for numerous attributes (O'Auth, 2007).

Proliferation of On-demand User ID

Proliferation of on-demand user ID is a big issue in cloud computing IDM as the happening of multiple identities for the same user in multiple service providers' security repositories cannot be ruled out. A simple way to overthrown this issue is by the adoption of Open ID mechanism (Illustration of Open ID). Open ID works by making one primary user id as the key to authenticate a single end user with multiple service providers. However, the main problem in this scenario lies in the trust propagation and development of trusted relationships (Vaquero, et. al., 2009).

CLOUD ARCHITECTURE

Cloud architecture plays an important role in choosing your IDM, SaaS or the all-in-one Platform-as-a-Service (PaaS) (Jain, 2009). SaaS need only application access, whereas PaaS will need system access as well as application access. They need a common IDM that can merge well into the existing authentication mechanism. The third type of cloud architecture is Infrastructure-as- a-Service (IaaS), which is not specified explicitly, since the IDM precondion of PaaS and IaaS are comparable. Consider one of the most common SaaS IDM exercise using ping identity. Ping identity works by arranging the technology behind the firewall and making the identities exportable (SPMLS, 2003) This IDM mechanism allows integration of a number of authentication methods such as Microsoft Windows based authentication, LDAP authentication, CA site minder, etc. It is deployed on top of the existing authentication infrastructure and the deployment is quite useful and fast. It needs the help of SAML to transfer credentials. It can be anticipated as a layer of abstraction over the traditional IDM that fights the challenges of IDM.

PaaS is commonly defined as the delivery of a computing platform and solution stack as a service. It includes workflow capabilities for application design, application development, and application services such as team collaboration, web service integration. PaaS IDM certainly scales up to add all these features.

PaaS IDM has to mention various functional modules like source control, test modules, development communities.

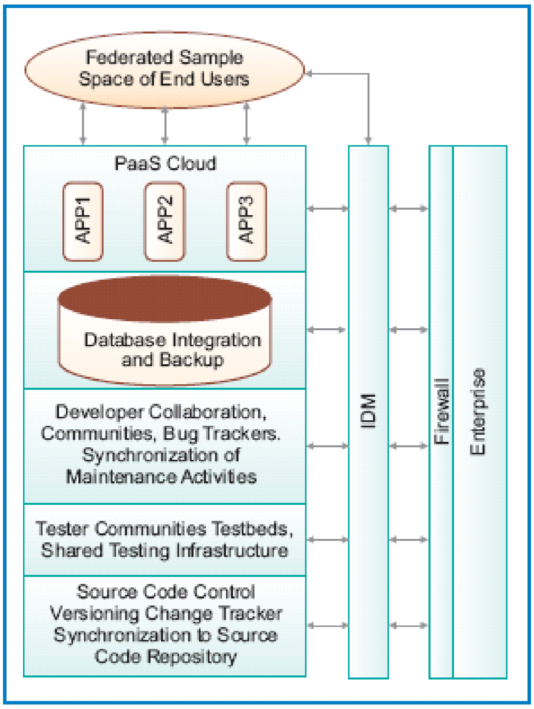

Federated Sample Space of End Users
PaaS Cloud
APP1
APP2
APP3
Database Integration and Backup
Developer Collaboration, Communities, Bug Trackers. Synchronization of Maintenance Activities
Tester Communities Testbeds, Shared Testing Infrastructure
Source Code Control Versioning Change Tracker Synchronization to Source Code Repository
IDM
Firewall
Enterprise

Figure 2: Paas IDM

For the sake of simplicity, the PaaS IDM could use a Role-Based Access Control (RBAC) system to grasp each of this and its user space. An RBAC system for source control will provide minimum set of privileges to the developer accounts and necessary services, depending on the assurance of the applications hosted on the platform. For test communities, IDM manages tester accounts, privileges, auto run test suites and knowledge collaboration portals of the tester communities required for hosting a test bed. The cloud could also predict IDM to handle the database challenges, by controlling the access and synchronization with the in premise segments. IDM can also be used to handle the SaaS based challenges of federated user space.

Vender lock-ins creates limitation for PaaS due to that complex IDM solution designed for PaaS is concluded useless while migrating to another cloud.

USER CENTRIC ACCESS CONTROL

The conventional model of application-centric access control, where each application keeps track of its collection of users and manages them, is not feasible in cloud based architectures. The main reason behind is the user space may be shared across applications that can lead to data replication, making mapping of users and their privileges a backbreaking task. It also requires the user to remember multiple accounts/passwords and maintain them properly. Cloud requires a user centric access control where every user request to any service provider is bundled with the user identity and claim information (Emig, et. al., 2007). User identity will have identifiers that identify and define the user. The identity is tied to a domain, but is portable. User centric approach leaves the user with the ultimate control of their digital identities. User centric approach also said that the system maintains a pool of information for every user, in order to search how best to react to in a given situation to a given user request.

FEDERATION OF IDENTITIES

On the internet, it is common that every user ends up with multiple credentials and multiple access permissions across different applications provided by different service providers. These splinter logins present a challenge to the users and service providers in forms of synchronization of shared identities and security. There is a strong need for an underlying identity system that is trusted across the web and within enterprises and unambiguously identifying users.

Combination of identities manage by the numerous service providers on the cloud is very critical to cloud based service composition and application integration. One of the main issues in this regard is the naming heterogeneity.

The user identity mapping in the previous environments have been one-to-one, or in other words, single user ID to single user profile. In cloud architectures the mapping dispute is many-to-one, one-to-many and pseudonyms. Pseudonyms are used for privacy protection details, when a user does not want his identity to be tracked as his expedition various domains.

Another issue is the trust relation setup between the service providers of the unite world. Currently it is based on policy files framed by the local authority, depending on various factors like the domain trust information automatically fed in by the trust authorities. This model lacks scalability and flexibility as it doesn’t meet cloud computing demands. Cloud scenarios require dynamic trust propagation and dynamic authorization.

VOLATILITY OF CLOUD RELATIONS

In a conventional model, the IDM is based on the long-term relation of a user to an organization or trust domain. In the era of e-commerce world in cloud, the relationships change dynamically and quickly, and the IDM has to incorporate all that. Any retrieval or cache of the volatile data has to be done very carefully. The possible harm of using old data should be studied. For example, if the user has changed his password login with old password, it should be restricted and locked in all the applications. There are so many challenges for this model exist .i.e. Live data fetching, domain name resolution, canonicalization of the data likes URL, account IDs.

SCALABILITY

Cloud needs the ability to scale to hundreds of millions of transactions for millions of identities and thousands of connections – with short/rapid deployment cycles. Performance has to be N+1 scalable across the globe and deployments agile and quick (weeks not quarters/years). With the software today it takes ~6 months to make a single SAML/SSO connection and it doesn't address the access control and compliance issues. Open Cloud Manifesto said that clouds have to dynamically scale up and down, so that nobody needs to hoard resources to handle peak hours (UCI).

INTEROPERABILITY

The mass expects the cloud to provide an IDM solution that can interoperate with all existing IT systems and existing solutions as such or with minimum changes. Cloud is used to perform various kinds of authentication mechanism such as the Microsoft Windows authentication, SSO, LDAP, SAML, OPENID and OAUTH, Open Social, Face Book Connect. The grammatical barriers have to be linked. It requires an authentication layer of abstraction to which any model of authentication can be plugged in and off dynamically.

TRANSPARENCY

Security measures assumed in the cloud must be made available to the customers to gain their trust. Chances are always there that the cloud infrastructure is secured with respect to some needs and the customers are looking for a different set of security. The important aspect is to see that the service of cloud meets the security needs of the application and this can be done only through full transparency. Open Cloud platform strive stress on transparency in clouds, as the consumer's doubt to host their applications on a shared infrastructure, on which they do not have any control (UCI). Transparency can be achieved by complete audit logging and control.

PATTERNS IN CLOUD IDM

Based on the insights gained so far three patterns in cloud IDM can be concluded. The ideal scenarios for each pattern are also mentioned.

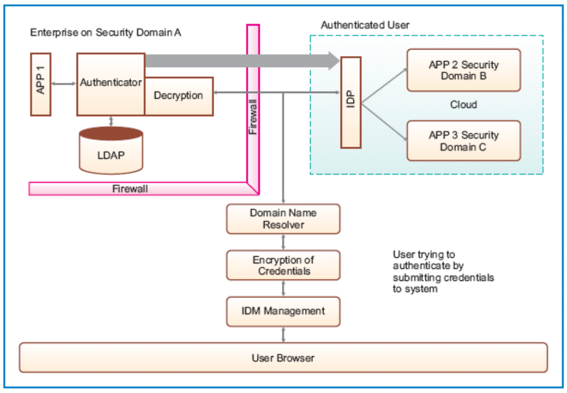


Figure 3: Trusted IDM Pattern

TRUSTED IDM PATTERN

This pattern is proposed for a smaller or even for a private cloud that requires security. Scalability is definitely not a feature of this cloud. Take the example of Google App Engine (appengine.google.com) that follows this pattern convince that the scalability is not a major issue at the moment as the number of requests that could be tunneled through concurrently is really big. The main advantage of the pattern is that the process of authentication is always performed within the firewall. The username and passwords are submitted to the IDM component and it takes the responsibility of encrypting and tunneling the credentials through a secure channel to the authenticator. IDM is independent of the authentication mechanism. Hence deployment and integration is fast and efficient. Once the user is authenticated with username and password by any authentication mechanism, then rest of the appropriate servers trust the user. The attributes of the user can be shared using SAML.

EXTERNAL IDM

This pattern is very similar to the pattern discussed earlier, but here the credentials are submitted directly to the authenticator [Fig. 4]. The credentials can be collected by a different browser window, channeled by SSL. The pattern is designed for a public cloud. The IDM focus only on domain resolution and triggering of the authenticator to resolve the authentication. Ping identity adopted this framework. In ping identity the problem of domain resolution is done by referring to a spreadsheet of valid users that is always kept updated. External IDM can be done with methods such as standard domains name resolution, discovery or YADIS protocol, or XRDS query depending on the underlying technology used.

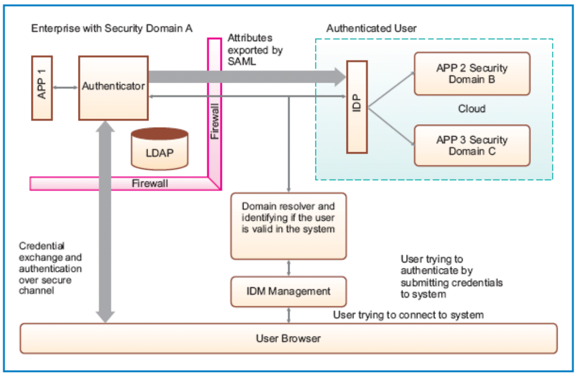

Enterprise with Security Domain A
Attributes exported by SAML
Authenticated User
APP 1
Authenticator
LDAP
Firewall
Firewall
IDP
APP 2 Security Domain B
Cloud
APP 3 Security Domain C
Domain resolver and identifying if the user is valid in the system
Credential exchange and authentication over secure channel
User trying to authenticate by submitting credentials to system
IDM Management
User trying to connect to system
User Browser

Figure 4: External IDM

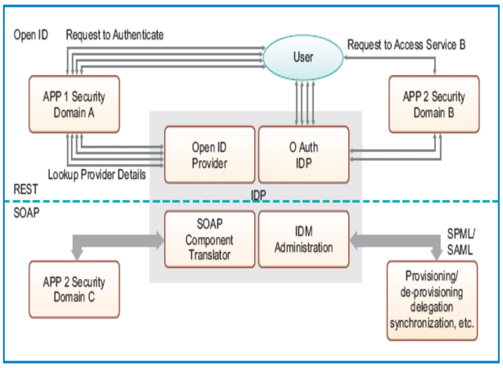


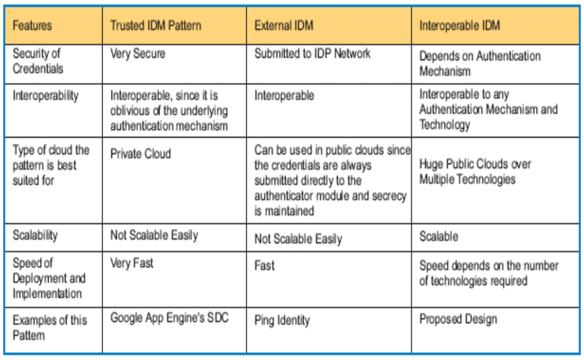
Figure 5: Interpopable IDM

INTEROPERABLE IDM PATTERN

This pattern illustrates a cloud to cloud scenario, using OpenID and OAuth. The identity mechanism used, will understand and interoperate multiple identity schemes. OpenID is an open and decentralized standard for user authentication and access control, by allowing users to logon to multiple services with the same digital ID. Any service provider can authenticate the user in to the system. The information is converted to different formats, depending on the technology used like Open ID, or SAML, or WS-Security and conveyed to the participating service providers.

CONCLUSION

Of the emerging technologies cloud computing has a lot of substance. It has brought a huge set of challenges to tame to produce more benefits. Choice of IDM design for any cloud should be tailored to suit the definition of that particular cloud and open to any kind of enhancements the cloud is bound the main focus in future.



Features	Trusted IDM Pattern	External IDM	Interoperable IDM
Security of Credentials	Very Secure	Submitted to IDP Network	Depends on Authentication Mechanism
Interoperability	Interoperable, since it is oblivious of the underlying authentication mechanism	Interoperable	Interoperable to any Authentication Mechanism and Technology
Type of cloud the pattern is best suited for	Private Cloud	Can be used in public clouds since the credentials are always submitted directly to the authenticator module and secrecy is maintained	Huge Public Clouds over Multiple Technologies
Scalability	Not Scalable Easily	Not Scalable Easily	Scalable
Speed of Deployment and Implementation	Very Fast	Fast	Speed depends on the number of technologies required
Examples of this Pattern	Google App Engine's SDC	Ping Identity	Proposed Design

Table 1: Summary of the patterns

Essentially the design should be capable of incorporating any number of trust domains and of keeping an effective shared user pool. As the IaaS IDM of next generation, a user centric identity management is intended to be a complete all-round solution addressing all possible problems related to cloud IDMs. It may be the reply to the increasing complexity of IDMs. The job is to take away the complexity of IDM away from the enterprises, thereby allowing them to guide their strength and resources on their individual functions, while the IaaS vendors provide the best solution or IDM based on their expertise.

REFERENCES

Ashish Jain (2009). A blog on Ping Identity, Jan 12, 2009. Available on http:// itickr.com/?cat=29

Christian Emig, Frank Brandt, Sebastian Kreuzer and Sebastian Abeck (2007). Identity as a Service – Towards a Service-Oriented Identity Management Architecture, Lecture Note sin Computer Science, 2007. Available on http://www.springerlink.com/content/5865u474424qw751/.

Illustration of Open ID based on Plaxo's use of Yahoo Open ID. Available at: http://www.plaxo.com/api/openid_recipe

Luis M Vaquero, Luis Rodero-Merino, Juan Caceres and Maik Lindner (2009). A Break in the Clouds: Towards a Cloud Definition, Cloud Architectures, Vol 39 No 1, Jan 2009. Available at http://delivery.acm.org/10.1145/1500000/1496100/p50-vaquero.pdf?key1=1496100&key2=0736171521&coll=GUIDE&dl=GUIDE&CFID=50720541&CFTOKEN=61415293

O'Auth (2007). Available at http://oauth.net/OpenID Authentication 2.0 Final, 2007. Available http://openid.net/specs/openid-authentication-2_0.html

Open Cloud Manifesto, Spring (2009). Available at http://www.opencloudmanifesto.orgopencloudmanifesto1.htm

RSA's contribution to Cloud security guidelines (2009). Available at http://www.cloudsecurityalliance.org/guidance

Service Provisioning Markup Language Specification, version-1, June 2003. Available atxml.coverpages.org/PSTCCS-SPMLCORE10.pdf

Unified Cloud Interface Project (UCI). Available at http://groups.google.com/group/unifiedcloud?hl=en

Corresponding Author

Jagdish Kaur*

Assistant Professor, Department of Computer Science, DAV College for Women, Ferozepur Cantt

E-Mail – armaandeep29@gmail.com