2011 International Conference on Advancements in Information Technology
With workshop of ICBMG 2011
IPCSIT vol.20 (2011) © (2011) IACSIT Press, Singapore

Different Patterns of Identity Management Implemented in Cloud Computing

Karunanithi. D [+], Kiruthika. B and Sajeer. K

Department of Information Technology, Hindustan University, Chennai, India

Abstract. To overcome the multiple accounts owned by users is by providing Identity as a Service (IaaS) through provision if using different types of patterns of cloud in identity management order to avoid verifying identity of each individual every time when they login.The overall objective of security, private and trust challenges arise from the technological underpinnings of cloud computing is a principle to guide decisions and achieve rational outcomes to confirm that users of cloud environments are given total protections, to strengthen and stabilize a world leading cloud ecosystem.. Hence, our concern is that currently a number of challenges and risks in respect of security, privacy and trust exist that may damage the fulfilment of these policy and so we upgrade in various implementations of cloud computing through patterns of cloud in identity management which reduces the burden associated with user accounts and privileges across multiple target resources, improves the Qos for users through measures such as self service password reset ,real time synchronisation of changes from authoritative identity data sources across multiple target resources.

Keywords: Cloud Computing, Identity Management, OpenIDSecurity, Patterns of IDM.

1. Introduction

Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction [1]. The literature identifies four different broad service models for cloud computing:

- Software as a Service (SaaS), where applications are hosted and delivered online via a web browser offering traditional desktop functionality, eg, Google Docs, Gmail and MySAP [3].
- Platform as a Service (PaaS), where the cloud provides the software platform for systems (as opposed to just software), the best current example being the Google App Engine [6].
- Infrastructure as a Service (IaaS), where a set of virtualised computing resources, such as storage and computing capacity, are hosted in the cloud; customers deploy and run their own software stacks to obtain services. Current examples are Amazon Elastic Compute Cloud (EC2), Simple Storage Service (S3) and SimpleDB [3].
- Hardware as a Service (HaaS), where the cloud provides access to dedicated firmware via the Internet, eg, XEN and VMWare [7].

[+] Corresponding author. Tel.: + 91-9445753975
E-mail address: karunanithid@gmail.com

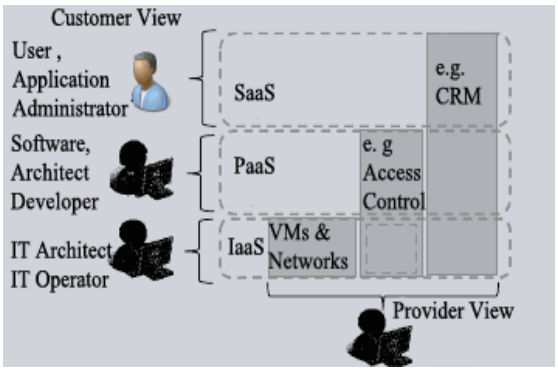

Fig. 1: XaaS Stack Views

2. Architecture of Identity Management

IM takes unique architectural approach to addressing the Identity Management challenge.

2.1. Service Oriented Security

Library of security service including authentication, authorisation, encryption, common audit and logging, Centralized role and permission management through new Authorization Policy Manager. "Identity as a Service", declarative security framework based on Identity Management pattern [6].

2.2. Entitlements Management

Before any organisations consists of Hard-coded security policies, Brittle policy management, Application policy silos and after the organisations they implement Externalized entitlements, Agile business policies, Centralized policy management [3].

2.3. Risk-Based Access Control

Real time fraud prevention, "Auto Learning" behavior profling, Pattern and anomaly detection [5].

2.4. Directory Services

- Scalable Identity Store: Centralized identity storage, Highly scalable - billions of entities
- Virtual Directories: Real-time unified view across disparate data stores, Rapid application deployments with single LDAP view [9].

2.5. Access Management

- Access Control-Web Single Sign-On, Enterprise Single Sign-On for legacy applications, Identity Federation
- Risk-based Access Control-Real-time fraud prevention, Adaptive context-aware security
- Entitlements Management-Externalized and centralized fine-grained authorization
- Web Services Security-Centralized administration of security and management policies for SOA, Secure Token Service [4].

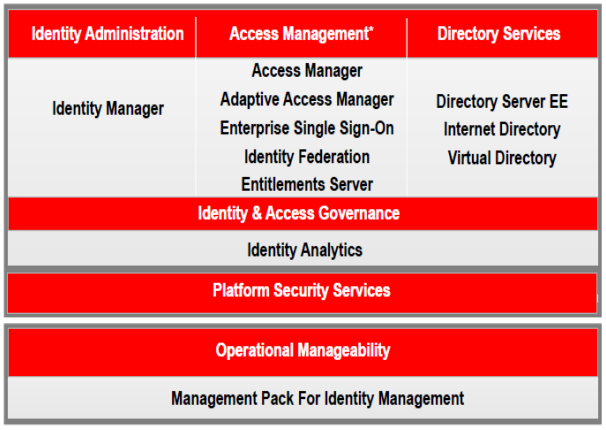

Fig. 2: Architecture of Identity Management

2.6. Identity Administration

- User Provisioning / Deprovisioning-Integrated Identity Administration, Automate user lifecycle management, Self service approval and workflow, Automated Password reset, Identify and remediate orphaned accounts, Central visibility into "who has access to what"
- Role Management-Automate role lifecycle management, Model business roles and map to IT roles [9].

2.7. Identity & Access Governance:

Identity Analytics- Role Mining and Entitlement Warehouse, Business-friendly Dashboards and Compliance Reports, Role and Entitlement Attestation/Certification, Preventive and Detective Segregation of Duties Management, Correlated reports across Identity and Access attributes [9].

3. Process of Cloud Computing to be Implemented with Identity Management

- Cloud computing is an emerging style of IT delivery in which applications, data, and IT resources are rapidly provisioned and provided as standardized offerings to users over the web in a flexible pricing model [1].
- Cloud computing is a way of managing large numbers of highly virtualized resources such that, from a management perspective, they resemble a single large resource. This can then be used to deliver services with elastic scaling [3].

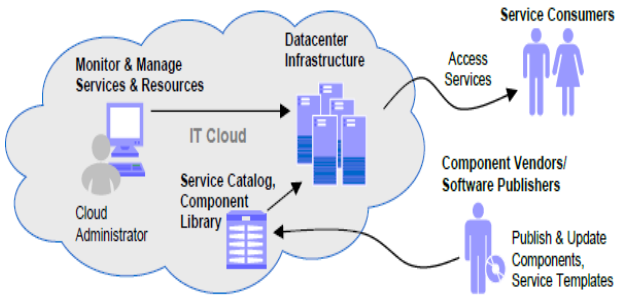

Fig. 3: Cloud with Identity Management

4. Integration of Identity Management Service on Cloud

Identity Management Requirements in Cloud environment are following:

4.1. Web Access Control:

- Shared Web access control Infrastructure for multiple web applications in the Cloud.
- Policy-based Access Control across wide range of Web resources.
- Single Sign-On for multiple Web Applications in the Cloud.
- Multi-tenant support [12].

4.2. Federated Identity / On-boarding:

- Coordinating authentication and authorization with enterprise or third party systems
- Trust between SOA-based initiatives by connecting user
- Standards-based Single Sign-On across web domains [12].

4.3. Life-cycle Identity Management

- Enables common model of identity, entitlements, obligations and policy ,
- Automatic role based user access life-cycle management,
- Periodic policy validation,
- Auditing of all user provisioning operations [10].

4.4. Privileged User Monitoring:

- Especially privileged administrators of Cloud provider Logging Activities
- Physical Monitoring
- background Checking [11]

4.5. Security Governance, Risk Management and Compliance

- Client access to tenant-specific log and audit data,
- Effective incident reporting for tenants
- Visibility into change, incident, image management
- SLAs, option to transfer risk from tenant to provide Support for forensics [6]

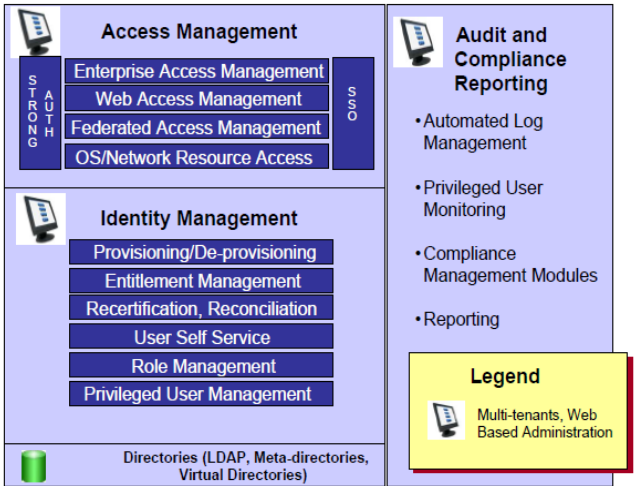

Fig. 4: Integration of IDM with Cloud

5. Major Issues

There is no proper protection in context aware security as described below:

Fraud Problems occur in implementation of Patterns of Identity Management are Misuse, StolenCredentials and Session Hijacking [9].

6. Challenges of Using Idm Patterns In Cloud Services

They should provide the following

- Authentication—Proving who the user is
- Authorization—Determining access rights and user privileges
- Access control—Managing means of access,
- Audit—Reporting and audit controls [4].

6.1. Identity Management Challenges divided into Technical

- Applications are typically not the ‘owner’ of identities
- Updates to identities synchronization across authoritative stores
- Lack of understanding of technology to implement solution
- Lack of planning a solid solution

6.2. Business

- Technical solution conforms to business goals and processes
- Data ownership
- Political concerns, 4.Legal concerns (Compliance)

6.3. Purpose of a Good IdM Solution

- Streamline tactical processes
- Provide a cohesive identity and access management solution [12].

7. Implementing Different 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.

7.1 Trusted IDM Pattern

This pattern is intended for a smaller or even for a private cloud that requires security. Scalability is definitely not a feature of this cloud. But Google App Engine (appengine.google.com) that follows this pattern assures that the scalability is not a major concern at the moment as the number of requests that could be tunnelled through simultaneously is quite large. The main feature of the pattern is that the authentication is always performed within the firewall. The credentials are submitted to the IDM component and it takes care of encrypting and tunnelling 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 in by any authentication mechanism, then rest of the participating servers trust the user. The attributes of the user can be shared using some mechanism like SAML. Authorization can be effectively handled by XACML [13] .

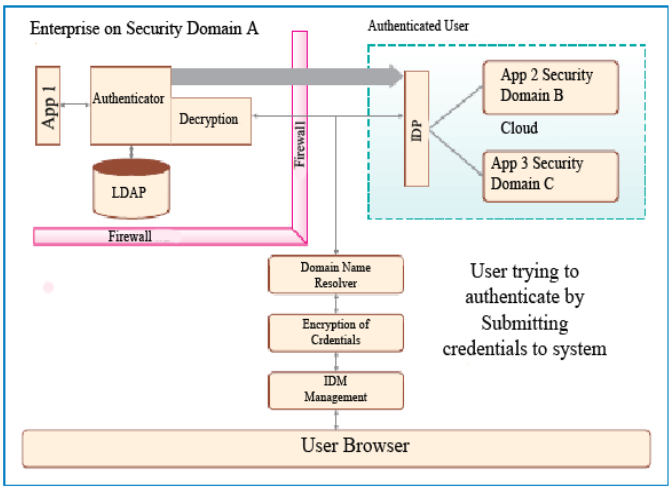

Fig. 5: Trusted IDM Pattern

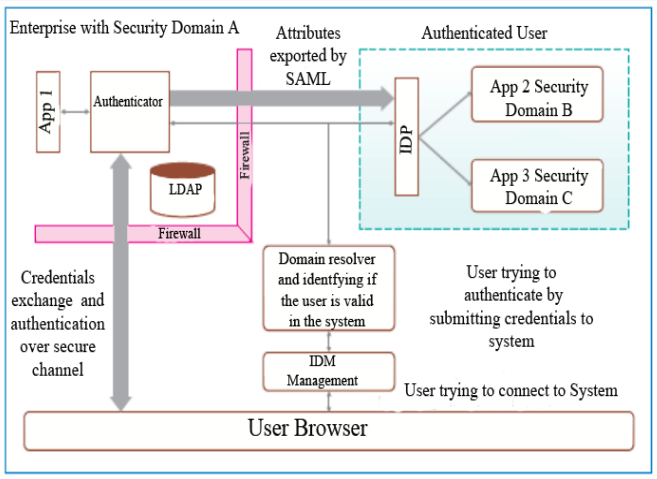

Fig. 6: External IDM

7.2 External IDM

This pattern is very similar to the initial pattern but for the fact that the credentials are submitted directly to the authenticator The credentials can be collected by a different browser window, channelled by SSL. The pattern is intended for a public cloud. The IDM concentrates only on domain resolution and triggering of the authenticator to resolve the authentication. This is the architectural pattern adopted by ping identity. In ping identity, domain resolution is done by referring to a spreadsheet of valid users that is always kept updated. It can also be achieved through other mechanisms like standard domains name resolution, discovery or YADIS protocol, or XRDS query, etc., depending on the underlying technology u

7.3 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. OAuth is again an open protocol that enables a user to grant permission to a consumer site to access a provider site without any sharing of credentials. SPML is used for XML based IDM LC. This is extremely useful for an e-commerce web world where there are multiple service providers based on a common user space. The central identity system, understands all technologies used for authentication like SAML, OpenID, OAuth, etc. Let us assume that the central identity system to be collection of modules, each handling a technology, taking to a common user space and a policy database. The information is converted to different formats, depending on the technology used like OpenID, or SAML, or WS-Security and conveyed to the participating service providers [13].

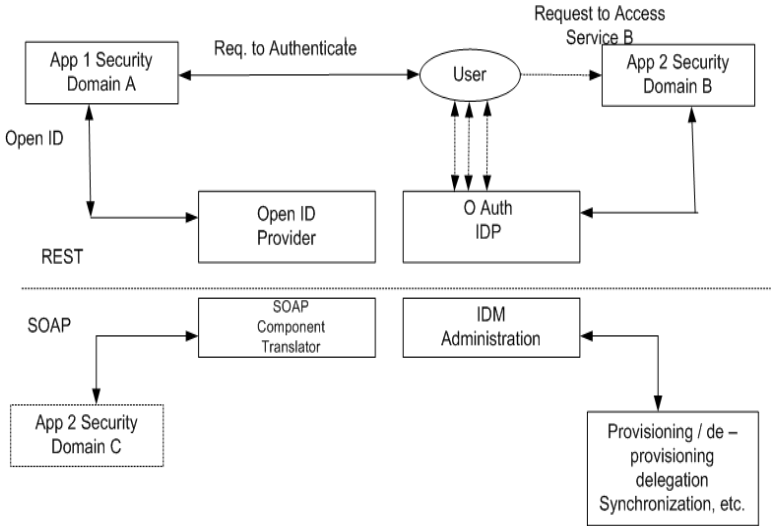

Fig 7: Interoperable IDM Pattern

8. Conclusion

Cloud computing with various applications being performed has several logins are used widely in enterprise hence, By implementing Identity Management established unique login credentials for all its users and gave IT the ability to manage users in one central location.IM provide with productivity enhancing tools for all users . Using a secure user name and password user access their One Login Portal where all web applications are just one click away. Inturn, IT can efficiently manage access to the organisation portfolio of cloud application. The following features influenced the Organisation decision to use one login 1.Authentication 2.Password management 3.Security Policies

9. References

[1] Amazon Web Services, '*Overview of Security Processes*', August 2010. As of November2010: http://awsmedia.s3.amazonaws.com/pdf/AWS_Security_Whitepaper.pdf.

[2] Armbrust, Michael et al., 'Above the Clouds: *A Berkeley View of Cloud Computing', University of California at Berkeley*, Technical Report No. UCB/EECS-2009-28, 10 February 2009. As of 25 November 2010: http://www.eecs.berkeley.edu/Pubs/TechRpts/2009/EECS-2009-28.pdf

[3] Article 29 Data Protection Working Party & Working Party on Police and Justice, *'The Future of Privacy: Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data*',WP168, 2009. As of 25 November 2010 http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp168_en.pdf

[4] Amazon, AWS and EC2 resources ,Google App Engine articles, The Open Group, The Open Group Architecture Framework (TOGAF), *Definition of the term "Architectural Principle*", http://www.opengroup.org/architecture/togaf8-doc/arch/chap29.html

[5] Armbrust, Michael et al., 'Above the Clouds: *A Berkeley View of Cloud Computing*', University of California at Berkeley, Technical Report No. UCB/EECS-2009-28, 10 February 2009. As of 25 November 2010: http://www.eecs.berkeley.edu/Pubs/TechRpts/2009/EECS-2009-28.pdf

[6] Sun_CloudComputing.pdf http://pdftop.net/preview/

[7] M. Jensen, J. Schwenk, N. Gruschka, and L. L. Iacono, "*On Technical Security Issues in Cloud Computing," in Cloud Computing, 2009*. CLOUD '09. IEEE International Conference on, 2009, pp. 109-116.

[8] Sun Microsystems, Inc. "Sun ONE Identity Management."http://wwws.sun.com/software/sunone/wp-identity_mgnt.pdf (26 Jan 2003)

[9] Identity Management Strategy Overview Post Sun Acquisition Update Cullen Landrum

[10] Identity Management in SharePoint 2010 Rick Taylor,Senior Technical Architect,Perficient.

[11] Birman, Ken, Gregory Chockler & Robbert van Renesse, 'Toward a Cloud Computing Research Agenda', ACM SIGACT News, 2009/40(2).

[12] Securing the Cloud through Comprehensive Identity Management Solution Millie Mak Senior IT Specialist.

[13] SETLabs Briefings VOL 7, NO 7 ,2009 ,*Cloud Computing Identity Management* ,By Anu Gopalakrishnan