INTERNATIONAL JOURNAL OF PURE AND APPLIED RESEARCH IN ENGINEERING AND TECHNOLOGY

A PATH FOR HORIZING YOUR INNOVATIVE WORK

IDENTITY MANAGEMENT IN CLOUD COMPUTING

MISS. SNEHALATA D. ULHE

Department of MCA, Prof. Ram Meghe Institute of Technology & Research, Badnera (Maharashtra), India.

Accepted Date: 05/03/2015; Published Date: 01/05/2015

Abstract: Cloud computing has become very popular nowadays. Cloud computing is actually the combination of different technologies. It provides computation, software application, data access, data management and storage resources without requiring cloud users to know location and other details. The migration of web applications to Cloud computing platform has raised concerns about the privacy of sensitive data belonging to the consumers of cloud services. The online security concerns are increasing. Authentication, authorization and Audit can be the part of identity management. Powerful Identity management is need of cloud computing.

Keywords: Access Control, Cloud Computing, IDM

Corresponding Author: MISS. SNEHALATA D. ULHE

Access Online On:

www.ijpret.com

How to Cite This Article:

Snehalata D. Ulhe, IJPRET, 2015; Volume 3 (9): 357-360

PAPER-QR CODE

INTRODUCTION

In Cloud Computing, computing is provided as service rather than as a product. Shared resources, software and information are provided to computer and other devices as utility over network. Cloud computing is combination of different technologies.

For business, different service providers may come together to form a new business space. It may happen that single user have Multiple accounts with different service providers. The visibility and scope of attributes for every identity has to be verified against a central trusted policy framing authority, assumed by the systems. Identity management (IDM) can be considered as important aspect in cloud security.

Nowadays, web applications preferring Cloud computing platform which increased concerns about the privacy of sensitive data belonging to the consumers of cloud services. It becomes difficult for users to verify that service provider following privacy laws or not. The username and password combination is used by most of the service providers but it has threat of phishing attack.

Identity management system can provide solution for such problems.

With the help of IDM consumers can choose which personal data they want to disclose, how it will be disclosed. They can decide how their information can be used. They can verify which privacy policies are used by service provider.

IDENTITY LIFECYCLE MANAGEMENT

Lifecycle management includes integrated solution for managing the entire lifecycle of user identities and their associated credentials and entitlements.

It can be divided into two component-first is provisioning and second is administrative components.

Administrative component deals with delegations rules, providing self-service components to change personal details or make requests to the users. Delegation of administrative rights to local group or process-in-charge is crucial for a volatile and dynamic cloud based scenarios.

Decentralizing the tasks will reduce the load on the authenticator component and also save time in making access control decisions.

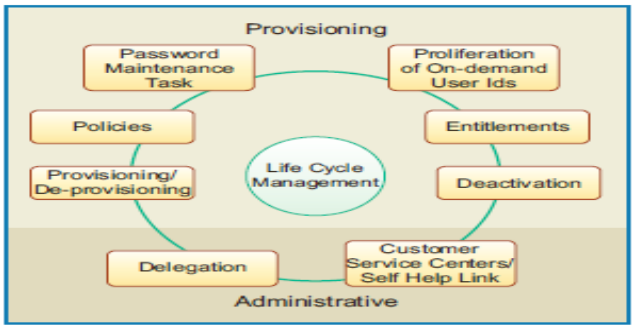

Fig a: Identity Lifecycle Management

CLOUD ARCHITECTURE

Selection of IDM depends on cloud architecture, SaaS or PaaS. SaaS requires only application access and PaaS will require system access as well as application access. Both require a common IDM that can integrate well into the existing authentication mechanism. IaaS and Paas requirements are comparable.

USER CENTRIC ACCESS CONTROL

The traditional model of application-centric access control in which each application keeps track of its collection of users and manages them, is not feasible in cloud based architectures.

This is more so, because the user space may be shared across applications that can lead to data replication, making mapping of users and their privileges a herculean task. It also requires the user to remember number of accounts/passwords and maintain them. Cloud requires a user centric access control where every user request to any service provider is bundled with the user identity and entitlement information. User identity will have identifiers or attributes that identify and define the user. Although, identity is tied to a domain, it is portable. With User centric approach user can control their digital identities.

UNSTABLE CLOUD RELATIONS

In a old model, the IDM is based on the Long lasting relation of a user to an organization or domain. In cloud computing, which represents the current e-commerce world, the relationships change with dynamism and quickly, and the IDM has to incorporate all that. Any retrieval or cache of the volatile data has to be done cautiously.

The possible damage of using old data should be studied. Like, if the user has changed his password login with old password, it should be restricted and locked in all the applications that are participating in the identity federation.

TRANSPARENCY

Security actions assumed in the cloud should be available to the customers to gain their trust. It may happen that cloud infrastructure is having some security options and users searching some different type of security option. The important point is to see that the cloud provider meets the security requirements of the application and this can be achieved only through total transparency.

DIFFERENT PATTERNS IN CLOUD IDM

There are three different pattern of cloud IDM.

- Trusted IDM Pattern.
- External IDM Pattern.
- Interoperable IDM Pattern.

CONCLUSION

In Cloud computing, security is the important issue which should be taken into consideration. Using Identity management we can provide security in cloud computing. For different scenario different pattern are available. We can make cloud more secure using Identity Management.

REFERENCES

1. OPENID, http://openid.net/, 2010.

2. Open Cloud Manifesto, Spring 2009.

3. [C. Sample and D. Kelley. Cloud Computing Security: Routing and DNS Threats, http://www.securitycurve.com/wordpress/, June 23, 2009.

4. Ashish Jain, A blog on Ping Identity, Jan 12, 2009.