FEDERATION OF IDENTITY MANAGEMENT IN CLOUD COMPUTING

Ms. Prathyusha Mekala[1]
3rd Year Student,
Department of Computer Science,
SV U CM & CS, Tirupati.

Prof. Sridevi[2],
Professor,
Department of Computer Science,
SV U CM & CS,, Tirupati.

Abstract: Cloud computing is built on several components for managing and making provision of abundant resources to business, on demand. Identity management is the essential element in cloud computing, and it is an inevitable standard security module that keeps away unauthorized users with unintentional interference to the system. The majority of work is being done to enhance this identity management component to overcome current limitations in authentication mechanisms. Federation among different clouds can be helpful in minimizing overhead and cost in overall identity management. Many cloud service providers are present in the industry with their independent identity management, but very few of them supports the federation among themselves to tackle the whole business collapse situation due to any disaster caused by nature. The Federation among these vendors can bring healthy competition in business markets that will lead to boost the confidence of cloud user in cloud computing. In this paper, our research work addresses a framework for researchers in identity management in cloud computing. The framework takes minimal effort and time for creating and simulating test environment for the generalized cloud environment.

Keywords: *Cloud Computing, Authentication mechanism, Authorization.*

INTRODUCTION

Cloud computing is a newly progressing technique which offers online computing resources, storage and permits users to organize applications with enhanced scalability, availability and fault tolerance. Cloud computing is about storing the stuff on remote servers instead of on own computers or other devices. This information can be retrieved using the internet with any device, everywhere in the world as long as that device can support cloud computing systems. The cloud computing system is comprised of a front-end, which is the client side and a back-end which is a collection of the servers and computers owned by a third party which stores the data. A central server which is a fragment of the back-end follows protocols and uses middleware to communicate between networked computers. Cloud computing accumulates all the computing resources and manages them automatically. Its characteristics describe a cloud computing system: on-need self-service, pooling of resources, access to the internet, and the elasticity of service availability and measurement of services utilized by individual users. Cloud computing is everywhere with tools like Google Drives replacing Microsoft Office, Amazon Web Services replacing traditional enterprise data storage, banking websites replacing branch offices and Drop box storing all our data and files. The cloud even provides different deployment models and service models.

The four deployment models present in cloud computing is:

1. **Public cloud:** In the public cloud, the cloud provider provides resources for free to the public. Any user can make use of the resources; it is unrestricted. The public cloud is connected to the public internet for anyone to leverage.

2. **Private cloud:** In a private cloud, the planning and provisioning of the cloud are operated and owned by the organization or the third party. Here the hosted services are provided to a restricted number of people or group of individuals.

3. **Community cloud:** These types of cloud infrastructures exist for special use by a group of users. These are a group of users who share a common mission or have specific regulatory requirements, and it may be managed by the third party or organizations.

4. **Hybrid Cloud:** Hybrid Cloud provides the best of above worlds. It is created by combining the benefit of different types of cloud (private & public cloud). In these clouds, some of the resources are provided and managed by public cloud and others as a private cloud.

Single sign-on (SSO) is a property of access control of multiple related, yet independent, software systems. With this

property, a user logs in with a single ID and password to gain access to a connected system or systems without using different usernames or passwords, or in some configurations seamlessly sign on at each system. This is typically accomplished using the Lightweight Directory Access Protocol (LDAP) and stored LDAP databases on (directory) servers. A simple version of single sign-on can be achieved over IP networks using cookies but only if the sites share a common DNS parent domain.

For clarity, it is best to refer to systems requiring authentication for each application but using the same credentials from a directory server as Directory Server Authentication and systems where a single authentication provides access to multiple applications by passing the authentication token seamlessly to configured applications as Single Sign-On.

Conversely, single sign-off is the property whereby a single action of signing out terminates access to multiple software systems.

As different applications and resources support different authentication mechanisms, single sign-on must internally store the credentials used for initial authentication and translate them to the credentials required for the different mechanisms.

Other shared authentication schemes include OAuth, OpenID, OpenID Connect and Facebook Connect. However, these authentication schemes require the user to enter their login credentials each time they access a different site or application so they are not to be confused with SSO.

To be precise, OAuth is not strictly an authentication scheme but an authorization protocol: it provides a way for the users to grant access on their own behalf to other websites or applications using some access keys. The main purpose of the protocol is to exchange the access credentials required for the authorization and not the authentication itself.

RESEARCH METHODOLOGY:

Single sign-on

Single sign-on (SSO) is a session and user authentication service that permits a user to use one set of login credentials (e.g., name and password) to access multiple applications. The service authenticates the end user for all the applications the user has been given rights to and eliminates further prompts when the user switches applications during the same session. On the back end, SSO is helpful for logging user activities as well as monitoring user accounts.

Single Sign-On by using Miniorange

BENEFITS

Benefits of using single sign-on include:

Mitigate risk for access to 3rd-party sites (user passwords not stored or managed externally)

Reduce password fatigue from different user name and password combinations

Reduce time spent re-entering passwords for the same identity

Reduce IT costs due to lower number of IT help desk calls about passwords

SSO shares centralized authentication servers that all other applications and systems use for authentication purposes and combines this with techniques to ensure that users do not have to actively enter their credentials more than once.

COMPONENTS OF SINGLE SIGN-ON

Single Sign-On has two components:

Login Server

The first time that a user seeks access to an application, the Login Server:

- Authenticates the user by means of user name and password
- Passes the client's identity to the various applications
- Marks the client being authenticated with an encrypted login cookie

In subsequent user logins, this login cookie provides the Login Server with the user's identity, and indicates that authentication has already been performed. If there is no login cookie, then the Login Server presents the user with a login challenge.

To guard against sniffing, the Login Server can send the login cookie to the client browser over an encrypted SSL channel.

The login cookie expires with the session, either at the end of a time interval specified by the administrator, or when the user exits the browser. It is never written to disk.

A partner application can expire its session through its own explicit logout.

Single Sign-On Application Programming Interface (API)

The Single Sign-On API enables:

- Applications to communicate with the Login Server and to accept a user's identity as validated by the Login Server
- Administrators to manage the application's association to the Login Server

SINGLE SIGN-ON APPLICATION TYPES

There are two kinds of applications to which Single Sign-On provides access:

Partner Applications

Partner applications are integrated with the Login Server. They contain a Single Sign-On API that enables them to accept a user's identity as validated by the Login Server.

External Applications

External applications are web-based applications that retain their authentication logic. They do not delegate authentication to the Login Server and, as such, require a user name and password to provide access. Currently, these applications are limited to those which employ an HTML form for accepting the user name and password. The user name may be different from the SSO user name, and the Login Server provides the necessary mapping.

SINGLE SIGN-ON AUTHENTICATION METHODS

Single Sign-On can use one of these authentication methods:

Local user authentication

Uses a lookup table within the Login Server schema. This table contains user name, password, Login Server privilege level, and other auditing fields for the user. The incoming password is one-way hashed and compared to the entry in the table.

External repository authentication

Typically relies on an LDAP-compliant directory. In this case, the Login Server binds to the LDAP-compliant directory, then looks up the user credentials stored there. External Authentication includes LDAP and Database Authentication and any others that may be custom-developed.

CONCLUSION

The current framework implementation is supported for SAML-Browser based SSO. With SAML implementation for SSO defined by the OASIS Security Services, CSP in this Cloud Sim framework gets added functionality of deep linking, automatic renewal of sessions. This approach has limitations for command line users of cloud. These users need to invoke browser for authentication before line clients can control cloud resources or services. As a part of future work, enhancement in user profile needs to be done for the command line oriented users. This can be a motivation for researchers in this field to find alternative techniques which enhance this framework by contributing to it. The proposed work was carried out with open source technologies like Java SE, MySQL, and Apache Framework so as to keep the interest of open source contributors. The results of experimentation were promising for the federated cloud environment. The proposed algorithms were found to be efficient and reliable.

REFERENCES

1. Hong Liu, Student Member, IEEE, Huansheng Ning, Senior Member, IEEE, Qingxu Xiong, Member,IEEE, and Laurence T. Yang, Member, IEEE2014, "Shared Authority Based Privacypreserving Authentication Protocol in Cloud Computing."

2. Adleman, L., "A subexponential algorithm for the discrete logarithm problem with application to cryptography", Proc. 20th IEEE Found. Comp. Sci. Symp., 1979, 55-60.

3. Ganeshan R. et.al, "Performance analysis of Hyper-Elliptic Curve Cryptosystems over Finite Fields Fp for Genus 2 & 4", IJCSNS Vol. 8 No. 12, Dec 2008.

4. K. Ren, C. Wang, and Q. Wang, "Security Challenges for the Public Cloud," IEEE Internet Computing, vol. 16, no. 1, pp. 69–73,2012.

5. Qian Wang, Cong Wang, Kui Ren, Wenjing Lou, Jin Li, "Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing", Proc. IEEE transactions on parallel and distributed systems, vol. 22, no. 5, may 2011 .

6. OASIS: Assertions and Protocol for the OASIS Security Assertion Markup Language (SAML) V2.0. OASIS Standard (2005)

7. Jaweher Zouari, "An Identity as a service framework for the cloud", IEEE, pp. 1-5, 2016.

8. Yong Yu, "Identity based Remote Data Integrity hacking with perfect data privacy preserving for cloud storage", IEEE, pp. 1-11, 2016.

[9] S. Ioffe, "Full-length video fingerprinting. Google Inc.," U.S. Patent8229219, Jul. 24, 2012.

[10] A. Kahng, J. Lach, W. Mangione-Smith, S. Mantik, I. Markov, M.Potkonjak, P. Tucker, H. Wang, and G. Wolfe, "Watermarking techniquesfor intellectual property protection," in Proc. 35th Annu. DesignAutom. Conf. (DAC'98), San Francisco, CA, USA, Jun. 1998, pp.776–781.

[11] N. Khodabakhshi and M. Hefeeda, "Spider: A system for finding 3Dvideo copies," in ACM Trans. Multimedia Comput., Commun., Appl.(TOMM), Feb. 2013, vol. 9, no. 1, pp. 7:1–7:20.

[12] S. Lee and C. Yoo, "Robust video fingerprinting for content-basedvideo identification," IEEE Trans. Circuits Syst. Video Technol., vol.18, no. 7, pp. 983–988, Jul. 2008.

[13] H. Liao, J. Han, and J. Fang, "Multi-dimensional index on hadoopdistributed file system," in Proc. IEEE Conf. Netw., Archit. Storage(NAS'10), Macau, China, Jul. 2010, pp. 240–249.

[14] Z. Liu, T. Liu, D. Gibbon, and B. Shahraray, "Effective, and scalablevideo copy detection," in Proc. ACM Conf. Multimedia Inf. Retrieval(MIR'10), Philadelphia, PA, USA, Mar. 2010, pp. 119–128.

[15] J. Lu, "Video fingerprinting for copy identification: From researchto industry applications," in Proc. SPIE, 2009, vol. 7254, pp.725402:1–725402:15.

[16] W. Lu, Y. Shen, S. Chen, and B. Ooi, "Efficient processing of knearest neighbor joins using MapReduce," in Proc. VLDB Endowment(PVLDB), Jun. 2012, vol. 5, no. 10, pp. 1016–1027.

Authors Profile

PRATHYUSHA MEKALA, received Bachelor of Computer Science degree from Vikrama Simhapuri University, Nellore in the year of 2013-2016. Pursuing Master of Computer Applications from Sri Venkateswara University, Tirupati in the year of 2016-2019. Research interest in the field of Computer Science in the area of Cloud Computing, Network Security and Software Engineering.

Dr. Mooramreddy Sreedevi, She is Working as a Senior Assistant Professor in the Dept. of Computer Science, S.V.University, Tirupati since 2007. She obtained her Ph.D. Computer Science from S.V.University, Tirupati. She acted as a Deputy Warden for women for 4 years and also acted as a Lady Representative for 2years in SVU Teachers Association, S.V.University, Tirupati. She Published 40 research papers in UGC reputed journals, Participated in 32 International Conferences and 46 National conferences. She acted as a Resource person for different universities. Her current research focuses in the areas of Network Security, Data Mining, Cloud Computing and Big data analytics.