International Journal of Emerging Research in Management &Technology
ISSN: 2278-9359 (Volume-4, Issue-8)

Research Article | **August 2015**

Simulation Study of Different Authentication Protocols Used for Federated Identity Management in Cloud

Meenakshi Bhat*
CSE & Kurukshetra University
Haryana, India

***Abstract*—**

Organizations needed a way to unify authentication systems in the enterprise for easier management and better security. Single-sign-on was widely adopted and provided a solution for keeping one repository of usernames and passwords that could be used transparently across several internal applications. After analyzing various issues regarding authentication of user's in federated systems we have tried to find out the benefits of using OpenID and SAML as authentication protocols in cloud computing. The focus of the thesis is on the simulation study of the authentication protocols SAML and OpenID in Cloudsim using NetBeans. The performance evaluation has been done based on RAM usage and execution time by introducing the concept of Global Broker.

***Keywords*— Authentication, Federated Identity Management (FIdM), SAML, Open ID, Global Broker.**

I. INTRODUCTION

Federated identity management (FIdM) [2] amounts to having a common set of policies, practices and protocols in place to manage the identity and trust into IT users and devices across organizations. Single sign-on (SSO) systems allow a single user authentication process across multiple IT systems or even organizations. SSO is a subset of federated identity management, as it relates only to authentication and technical interoperability. Centralized identity management solutions were created to help deal with user and data security where the user and the systems they accessed were within the same network – or at least the same "domain of control". Increasingly however, users are accessing external systems which are fundamentally outside their domain of control, and external users are accessing internal systems. The increasingly common separation of user from the systems requiring access is an inevitable by-product of the decentralization brought about by the integration of the Internet into every aspect of both personal and business life. Evolving identity management challenges, and especially the challenges associated with cross-company, cross-domain access, have given rise to a new approach to identity management, known now as "federated identity management". FIdM, or the "federation" of identity, describes the technologies, standards and use-cases which serve to enable the portability of identity information across otherwise autonomous security domains. The ultimate goal of identity federation is to enable users of one domain to securely access data or systems of another domain seamlessly [5], and without the need for completely redundant user administration. Identity federation comes in many flavors, including "user-controlled" or "user-centric" scenarios, as well as enterprise-controlled or business-to-business scenarios.
The various entities [4] used in FIdM are:

Identity Provider:
An entity that is responsible for validating a user's authentication credentials and "vouching for" the user in the scope of a single-sign-on relationship. When vouching for a user, the Identity Provider will issue trusted single-sign-on credentials that are used to identify the user to federation partner. The Identity Provider may also issue the credential and be responsible for the identity proofing prior to issuance and therefore assuming certain liability for the credential.

Service Provider:
An entity that provides services within a federation. This entity acts as the recipient of a single-sign-on event from an Identity Provider. Based on the trust relationship with the Identity Provider, a Service Provider is able to validate Identity Provider-provided single-sign-on credentials for a user.

User:
The end user or an agent acting on the user's behalf, who participates in the federation, using services from both the Identity Provider and the Service Providers, while directly authenticate only to the Identity Provider.

II. AUTHENTICATION PROTOCOLS

The various authentication protocols [13] used for federated identity management in cloud are discussed as under:

SAML:
Security Assertion Markup Language (SAML) [5] is an XML standard that allows a user to log on once to the log on site for all the trusted websites. SAML was released in 2002 with version 1.0 and in 2005 version 2.0 was released. SAML is designed for B2B and B2C transactions. SAML has the following components:

- Assertions: Authentication, attribute, authorization
- Protocols: HTTP, SMTP, FTP, SOAP
- Bindings: SAML over SOAP, SAML over HTTP

SAML defines three roles:

- Identity Provider (IDP): This role will validate the identity of a user who is asking for a service.
- Service Provider (SP): This role will provide services to user.
- Principal: This is typically the user asking for a service from SP and getting validated by IDP.

OpenId:

OpenID [8] was released in 2006 and its functions resemble that of SAML, but instead of limiting the usage to enterprise users, OpenID was designed for consumer apps and services. With OpenID, the enterprise users are also in scope now. OpenID is being provided by majors like Facebook, Google, Yahoo, etc.
Below are the roles that OpenID provides:

- End user who has OpenID and wants to verify the identity.
- Resource Party which is the party that wants to verify the identity of end user.
- OpenID provider which is the party used to verify end user.

OpenID is both an identifier format and an extensible [6] set of protocols for passing identity information. Users enter their identifier at the site they wish to access and are redirected to the appropriate Identity Provider. During this session, the user can move between multiple OpenID Relying Party sites without re-entering their password at the Identity Provider, because the Identity Provider simply checks the session and transparently returns control to the requesting site. The OpenID base protocol is very simple, but can be augmented by additional extensionsto pass registration attributes or to classify the strength of authentication method used at the Identity Provider. The OpenID protocol does not rely on a central authority to authenticate a user's identity. Moreover, neither services nor the OpenID standard may mandate a specific means by which to authenticate users, allowing for approaches ranging from the common (such as passwords) to the novel (such as smart cards or biometrics).The term OpenID may also refer to an identifier as specified in the OpenID standard; these identifiers take the form of a unique Uniform Resource Identifier (URI), and are managed by some OpenID provider that handles authentication.

III. PARAMETERS USED TO SIMULATE SAML AND OPENID

In order to study SAML and OpenId authentication protocols a datacenter broker, a global manager and a global broker have been used.
A cloud broker [10] may be a third-party individual that acts as an intermediary between the purchaser of a cloud computing service and the sellers of that service.

Local broker: a local broker is an entity that manages the use, performance and delivery of cloud services and establishes relationship between cloud service providers and cloud service consumers.

Global broker: a global broker system supports fast provisioning of resource infrastructures needed in service evaluation, system and computational resources, over the multiple clouds.

Datacenter broker: this class models a broker, which is responsible for mediating between service providers and users depending on users' requirements. the broker deploys service tasks across clouds. user-developed scheduling algorithms are implemented in datacenter broker method.

The table below shows the parameters along with their values used to simulate the authentication protocols.

TABLE I PARAMETERS USED

S.NO.	Parameter	OpenID	SAML
1.	Number of Hosts	5	5
2.	Number of VM's	7	7
3.	Number of Cloudlets	109	300
4.	Number of Datacenters	3	3
5.	Total RAM size	4M/15M	4M/15M
6.	Total Execution Time	1.294s	1.981s

Graph:

The figure below shows the time and memory used by the authentication protocols:

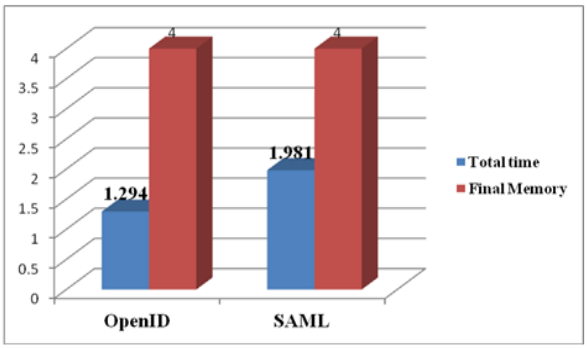

Fig.1 Graph showing Total time and Memory used by OpenID and SAML

IV. CONCLUSION AND FUTURE SCOPE

The implementation of authentication protocols SAML and OpenID has been done using the concept of Global Broker.These protocols implemented Single Sign-On in the Cloud Federation scenario using the CloudSim toolkit, considering multiple Identity Providers and Cloud Service Providers. The simulation results showed the execution time and memory used by these authentication protocols. The simulation study is based on various simulation parameters like number of hosts, virtual machines, cloudlets and execution time and the memory used by these authentication protocols. Our research has a great significance in area where security is of great concern especially across federated systems which allows cooperation on identity processes, policies and technologies across different organizations. The work presented in this paper defines the baseline for carrying out simulation study of the authentication protocols. We can include several other parameters like bandwidth used, throughput of the system etc. for further refining the study of these protocols. Moreover provisioning new identities often incurs some security risk. It is difficult to secure credential storage and to deploy it with proper policies. We can extend the present work with cryptographically strong hash algorithm such as one from the SHA-2 family.

REFERENCES

[1] Simone Cirani, Marco Picone, Pietro Gonizzi, Luca Veltri, and Gianluigi Ferrari, Senior Member, IEEE, "IoT-OAS: An OAuth-Based Authorization Service Architecture for Secure Services in IoT Scenarios", IEEE SENSORS JOURNAL, VOL. 15, NO. 2, FEBRUARY 2015.

[2] Yinzhi Caoy, Yan Shoshitaishviliz, Kevin Borgoltez, Christopher Kruegelz, Giovanni Vignaz, and Yan Cheny, "Protecting Web-based Single Sign-on Protocols against Relying Party Impersonation Attacks through a Dedicated Bi-directional Authenticated Secure Channel", in the Proc. of International Symposium on Research in Attacks, Intrusions and Defenses (RAID), 2014.

[3] Md. Sadek Ferdous and Ron Poet, "Analysing Power Consumption Of Diferent Browsers & Identity Management systems in mobile phones", International Journal of Distributed and Parallel Systems (IJDPS) Vol.3, No.2, March 2012.

[4] Rosa Sánchez, Student Member, IEEE, Florina Almenares, Member, IEEE, Patricia Arias, Student Member, IEEE, Daniel Díaz-Sánchez, Member, IEEE, and Andrés Marín, Member, IEEE, "Enhancing Privacy and Dynamic Federation in IdM for Consumer Cloud Computing", IEEE Transactions on Consumer Electronics, Vol. 58, No. 1, February 2012

[5] Ping Identity,Internet-Scale Identity Systems:An Overview and Comparison,The Whitepaper.

[6] J. Hodges, Technical Comparison: OpenID and SAML, Identity Meme, 17 Jan.2008; http://identitymeme.org/doc/draft-hodges-saml-openid-compare.html.

[7] Susan Landau, Tyler Moore, "Economic Tussles in Federated Identity Management", Harvard University.

[8] Wolfgang Hommel, Helmut Reiser, "Federated Identity Management in Business-to-Business Outsourcing", B.F. Marques, T. Nebe, R.F. Oliveira (Eds.): Proceedings of the 12th Annual Workshop of HP OpenView University Association (HPOVUA 2005); pp. 81–93, iPortalMais, Porto, Juli 2005.

[9] Aparajita Pandey, Dr. Jatinderkumar R. Saini, "An Investigation of Challenges to Online Federated Identity Management Systems", International Journal of Engineering Innovation & Research Volume 1, Issue 2, ISSN : 2277 – 5668.

[10] Bart Delft, Martijn Oostdijk, Elisabeth Leeuw; Simone Fischer, "A Security Analysis of OpenID", Policies and Research in Identity Management, 343, Springer, pp.73-84, 2010, IFIP Advances in Information and Communication Technology, 978-3-642-17302-8.<10.1007/978-3-642-17303-5 6>. <hal-01054399>.

[11] Amandeep Sandhu, Maninder Kaur, "Modeling Local Broker Policy Based on Workload Profile in Network Cloud", International Journal of Science and Research (IJSR), India Online ISSN: 2319-7064.

[12] Marc Mosch, Stephan Groß and Alexander Schill, "User-Controlled Resource Management in Federated Clouds", Journal of Cloud Computing: Advances, Systems and Applications2014, 3:10 http://www.journalofcloudcomputing.com/content/3/1/10.

[13] Shabnam Sharma, Usha Mittal , "Comparative analysis of various authentication techniques in cloud computing", International Journal of Innovative Research in Science, Engineering and Technology ,Vol. 2, Issue 4, April 2013.

[14] Birgit Pfitzmann and MichaelWaidner ,"Federated Identity-Management Protocols- Where User Authentication Protocols May Go", Springer-Verlag Berlin Heidelberg 2004.
[15] Krishan Kant Lavania , Yogita Sharma , Chandresh Bakliwal, "A Review on Cloud Computing Model", International Journal on Recent and Innovation Trends in Computing and Communication ISSN 2321 – 8169 Volume: 1 Issue: 3 161 – 163.
[16] Jaejung Kim and Seng-phil Hong, "A Consolidated Authentication Model in Cloud Computing Environments", International Journal of Multimedia and Ubiquitous Engineering Vol. 7, No. 3, July, 2012.
[17] Ms. Sangita Rase, Prof. Srinu Dharavath, " Review of Mobile Cloud Computing Framework and Authentication Problems", International Journal of Scientific & Engineering Research, Volume 5, Issue 2, February-2014.
[18] Anu Gopalakrishnan, "Cloud Computing Identity Mnagement", SET Labs Briefings VOL 7 NO 7, 2009.
[19] Deepa Panse, P. Haritha, "Multi-factor Authentication in Cloud Computing for Data Storage Security", Volume 4, Issue 8, August 2014 ISSN: 2277 128X. International Journal of Advanced Research in Computer Science and Software Engineering.
[20] Liliana F. B. Soares, Diogo A. B. Fernandes, Mário M. Freire and Pedro R. M. Inácio, "Secure User Authentication in Cloud Computing Management Interfaces", Department of Computer Science 6201-001.
[21] Jostein Jensen, "Federated Identity Management Challenges", 2012 Seventh International Conference on Availability, Reliability and Security, Norwegian University of Science and Technology (NTNU).
[22] Roberto Baldoni, "Federated Identity Management Systems in e-Government: the Case of Italy", Electronic Government, An International Journal, Vol. x, No. x, xxxx.
[23] http://en.wikipedia.org/wiki/OpenID.
[24] http://www.softwaresecured.com/2013/07/16/federated-identities-openid-vs-saml-vs-oauth/.
[25] "The NIST Definition of Cloud Computing". National Institute of Standards and Technology. Retrieved 24 July 2011.
[26] Yasir Saleem, Muhammad Munwar Iqbal, Muhammad Amjad, Salman Bashir, Muhammad Faisal Hayat, Muhamamd Farhan, Amjad Farooq, Abad Ali Shah, "High Security and Privacy in Cloud Computing Paradigm through Single Sign On", Life Science Journal 2012;9(4).
[27] http://identitymeme.org/doc/draft-hodges-saml-openid-compare 06.html#OpenID.site.
[28] Alejandro Pérez-Méndez, Fernando Pereñíguez-García, Rafael Marín-López, Gabriel López-Millán, and Josh Howlett, "Identity Federations Beyond the Web: A Survey", IEEE COMMUNICATION SURVEYS & TUTORIALS, VOL. 16, NO. 4, FOURTH QUARTER 2014.
[29] Dirk Schreckmann, "An Introduction to Java Development with Net Beans IDE" Net Beans IDE Project Basics Tutorial.
[30] J. Schaad, L. Zhu, and J. Altman, A RADIUS Attribute, Binding, Profiles, Name Identifier Format, and Confirmation Methods for SAML, Feb. 2014, IETF Internet Draft, IETF draft-ietf-abfab-aaa-saml-09.

