JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

THE EVOLUTION OF AUTHENTICATION PROTOCOLS IN IDENTITY MANAGEMENT: A COMPREHENSIVE REVIEW

1Jyoti, 2Sheetal Kalra
[1]Research Scholar, [2]Associate Professor, [3]Assistant Professor
[1]Department of Engineering & Technology
[1]GNDU, Regional Campus, Jalandhar City, India

Abstract : The introduction of Web 2.0, cloud computing, and the Internet of things (IoT) benefits users and enterprises. However, this development has proven to be a significant call for resolving authentication-related security issues. Identity and access management verifies the legitimacy of users, provides a layer of protection for sensitive user credentials, and grants users access to resources. The idea of federated identity (Single Sign On), which is based on trust relationships between many service providers as well as identity providers, allows users to access several services without having to enter passwords to various service providers. One benefit that Single Sign On offers users is the elimination of the need to remember several passwords for various services. The idea and meaning of identity and access management (IAM), as well as a number of security issues and widely used protocols like OAuth2.0, SAML, LDAP, and Kerberos, have all been briefly covered in this research paper.

IndexTerms – IAM, SAML, LDAP, Kerberos, OAuth.

I. INTRODUCTION

Cloud computing is a blend of heterogeneous resources such as networks, servers, hosts and applications. These resources provide flexible and on demand needed access to the cloud users [1]. The decade of Cloud computing has its impact over the working scenarios of large businesses and organizations. It is being used by commercial fields currently at a large scale. It has revolutionized the world of IT. Cloud computing model provides rapid provision to a shared pool of resources as and when demanded by the users with the minimum service provider interaction. Cloud service providers take care of the identity and manage the cloud environment. Some of the characteristics of Cloud computing include availability of shared resources, flexible scalability of the networks, automation facility and payment as per usage by the users. However, many data leakage incidents have been witnessed in the past. These data leakages are due to the vulnerabilities and susceptibilities in identity and access management. The success of cloud services access depends largely on IAM system.

Cloud environment is classified into different deployment models (i) Private (ii) Public (iii) Hybrid . Private Cloud caters to the need of a particular organization. Virtual Infrastructure is facilitated to many organizations in Public Cloud and largely managed and handled by third party providers. It reduces the overall service cost. A mixture of public and private cloud services is known as Hybrid or Federated Cloud. Specific environments have been deployed for IoT Cloud services. Cloud computing is generally separated into three popular service models as Software as a service (Saas), Platform as a service (Paas) and Infrastructure as a service (Iaas). Cloud also offers service-based architectures like database as a service, Identity as a service and security as a service [2]. Due to the complexity of usage, Cloud services require extensive authentication and authorization mechanism in order to give protection to the data and resources.

Mostly the storage and management of data in Cloud Systems are performed by the Service providers or with the support of third party vendors. The service provider has to make sure that the data and applications stored in the Cloud are safe. The users also need to verify that their authentication credentials are secure or not. There may be some cases where the third party vendors themselves can be malicious attackers. Identity and access management is considered to be one of the best practices in order to provide security to Cloud Systems.

II. SECURITY ISSUES

Cloud computing faces a number of security threats. Cloud service providers try to provide a secure environment to the customers. At the same time the customers try to utilize the resources fully. The Cloud Security Alliance (CSA) did a study over threats confronted by Cloud Computing [2]. CSA considered Identity and Access management as a crucial security issue.

Table 1

Cloud Computing Security Concerns	
Threats	**Countermeasures**
Data Breaches	Identity and Access Management
Weak Identity, Credentials	Encryption
Insecure APIs	Digital Signature
Account Hijacking	Interface security measures
Data Loss	Data Storage security measures
Denial of Service	Network communication security measures

Businesses have changed their working style with the advent of Cloud computing as resources reside on Cloud. Each application residing over Cloud has its own authentication mechanism. As the number of customers increasing so is the concern towards Cloud security. It is crucial to identify the right person. IAM is a solution in order to manage the access towards resources [3]. It verifies the user and authorizes the reliable user to access protected resources based on user's role. IAM systems enable organization to manage identities including people, software, and hardware like robotics and IoT devices. Using IAM, there is no need to remember multiple IDs as well as passwords. IAM offers single sign on (SSO). It manages the identity of the user at all levels of Cloud environment – from application level to virtual infrastructure, network and hardware level. It plays its vital role in user identity management which is similar to the management of life cycle of digital identity of end-user which can be a human or machine. It includes registration, provisioning, propagating, managing, deprovisioning and deregistration [4].

Identity and access management provides the following services [2]:

1. Authentication: When a user logs in, authentication is the method used to prove their identity. CSA endorses using federated identification (FDI) and multi-factor authentication (MFA) with the use of biometrics along with tokens and out-of-band passwords. Fingerprints or One time password is also used for strong authentication. In the applications where transactions are to be done, risk factor is calculated. If the risk factor is low only then the truncation is approved otherwise denied.
2. Authorization: An end user must have authorization before using or acting on approved resources. In the same way legitimated end users should be authenticated properly before granting them the access to utilise the approved resources. The success of the authorization depends upon access control. Role-Based Access Control (RBAC) is less desired over Attribute-Based Access Control (ABAC).
3. Identity Management: It includes the formation of digitally approved ID or account in order to grant access to the user for using the resources. Whenever a new employee is appointed in an organization or company, his/her identity is verified and he/she is assigned with a digital identity so that needed resources can be accessed for the completion of tasks. Deprovisioning is the opposite of provisioning where the granted resources are revoked back. This can be accomplished with the help of LDAP and active directory services.
4. Federated Identity: Here Identity managing institutes trust between different heterogeneous administrations. Third party plays a vital role. Federated servers at identity provider stocks user credentials and allow single sign on without the need of passwords. Identity provider authenticates the user on the behalf of service provider. Here token management is performed. There are some standard identity protocols such as SAML, etc. which are used.

A few IAM standards are available which are used in the cloud environment in order to maintain the identity. Security Assertion Markup Language (SAML) 2.0 outlines a framework for switching security information and important credentials between entities (Service Providers, Users).Federated identity is being offered by SAML along with supporting authentication and authorization. The identity provider and the identity reliant both communicate via SAML, which uses XML-based assertions that comprise declarations for authentication, characteristics, and authorization decisions. Open Authentication (OAuth) 2.0 is an Internet Engineering Task Force (IETF) standard. It is used popularly for authorization purpose where a third-party application is allowed a restricted and limited access to the HTTP Services [5]. In this paper a few IAM standards such as SAML, LDAP, Kerberos and OAuth have been discussed in the following sections.

III. SAML

SAML (Security Assertion Markup Language) is XML based protocol. It provides Single sign on facility. SAML is widely used by large businesses and companies. This gives a central point to the enterprises in order to manage identities. It reduces the efforts of the admin [6]. Here the user is not required to enter his password every time of access thus reducing the admin effort to maintain credentials.

In the working process of SAML, there are three main entities- service provider, identity provider and user. In order for SAML to function, the identity provider and service provider must exchange user data with each other, including logins, authentication status, IDs, and other pertinent features. The process of log in becomes easy and simple as user only needs to log in once with a single set of authentication credentials. As a result, whenever a user tries to access web resources such as a website, the identity provider provides SAML authentication to the service provider, who subsequently authorises the user's access.

IV. LDAP

The extensible Lightweight Directory Access Protocol (LDAP) has a definition defined in RFC4510 and protocol specifics documented in RFC4511 [7]. LDAP an open, vendor-neutra protocol is used to save and preserve the data over Directory. There are multiple read operations and a few write operations making this protocol indeed lightweight. LDAP can handle authentication at the same time enabling users to log in once and access a variety of server-side files. There is no need to login again.

An LDAP query generally involves:

- Session connection – Via an LDAP port, the user links to the server.
- Request - After successful connection, user submits a query. For example the user may ask for an email lookup to the server.
- Response – LDAP demands the directory for the same, carries the required information and provide it to the user.
- Completion – Once the user gets its required data, it separates from the LSAP port. This ends the query successfully.

V. KERBEROS

Kerberos is an authentication protocol. It provides an authentication server which is centralized. The main function of this authentication server is to verify the identity of the users and authenticate them to the servers and vice versa. In Kerberos the database is used for client authentication [8]. Kerberos acts as a third-party server which is trusted as well as known as the Key Distribution Center (KDC). Under KDC resides Authentication Server (AS) and Ticket Granting Server (TGS). AS and TGS both are the key players for the successful authentication verification.
The working of these components of Kerberos is as following:

- Authentication Server (AS):
  Initial Authentication is performed by AS. It also does the ticketing process for TGS.

- Database: It contains all the important credentials of the users.

- Ticket Granting Server (TGS):
  TGS grants the ticket for the demanded server.

VI. OAUTH

OAuth stands for Open Authorization. It is an open standard protocol for authorization of an application. The main components used in OAuth are Authorization code, scope, redirect URL and access token. In the first step user grants access to certain kinds of scopes which are available. Scope is basically what kind of information that the application is exchanging for the user. Then the authorization code is exchanged with access token. There can be read scopes as well as write scopes. The redirect It is used to check whether the client/application is valid or not. Redirect URL is generated over server side. Then the server redirects the user to this URL. Access token is granted by the server to the application [9]. OAuth is an authorization framework. The working process of OAuth includes four players. Client: It is the service which is asking for the grant of resources. Owner. It is the user itself. Resource server : The service which holds the resources. Authorization Server: It verifies the resource credentials [2]. During the whole process, two types of tokens are generated – Access token and Authorization token. Both the tokens exist for a limited time. Firstly resource owner contacts client. After that Client associates with the authorization server. Then access token is generated. After this user is redirected by the authorization server with authorization code. OAuth is being used by big giants such as Google, Facebook etc. [10].

VII. CONCLUSION

This paper offers a brief insight and explanation of the identity and access management of Cloud computing and security concerns. SAML is a protocol mainly used by enterprises. LDAP is a protocol used by individuals. It provides the foundation for building Active directories (Microsoft). Kerberos is an authentication protocol mainly used in client server architecture. It is available in many commercial products. OAuth is used popularly for authorization among different web based applications. Our future research will be focused over saving third party involvement in the authentication process and reducing storage requirements of the tokens.

REFERENCES

[1] Indu, I., Anand, P. R., & Bhaskar, V. (2018). Identity and access management in cloud environment: Mechanisms and challenges. Engineering science and technology, an international journal, 21(4), 574-588.

[2] Sharma, A., Sharma, S., & Dave, M. (2015, October). Identity and access management-a comprehensive study. In 2015 International Conference on Green Computing and Internet of Things (ICGCIoT) (pp. 1481-1485). IEEE.

[3] Doshi, R., & Kute, V. (2020, February). A review paper on security concerns in cloud computing and proposed security models. In 2020 International Conference on Emerging Trends in Information Technology and Engineering (ic-ETITE) (pp. 1-4). IEEE.

[4] Kumar, R., & Goyal, R. (2019). On cloud security requirements, threats, vulnerabilities and countermeasures: A survey. Computer Science Review, 33, 1-48.

[5] Shaikh, A. H., & Meshram, B. B. (2021). Security issues in cloud computing. In Intelligent Computing and Networking: Proceedings of IC-ICN 2020 (pp. 63-77). Springer Singapore.

[6] Dobbs, G. B. (2021). Cloud Service Authenticates Via Delegation-SAML. IDPro Body of Knowledge, 1(6).

[7] MM, N. (2022). TRUSTWORTHINESS FOR LIGHTWEIGHT DIRECTORY ACCESS PROTOCOL.

[8] Albaldawi, W. S., & Almuttairi, R. M. (2021, February). Kerberos authentication for big data applications on cloud environment. In Journal of Physics: Conference Series (Vol. 1804, No. 1, p. 012062). IOP Publishing.

[9] Siriwardena, P. (2020). Advanced API security: OAuth 2.0 and beyond. CA, USA: Apress.

[10] Zargar, S., Shahidinejad, A., & Ghobaei-Arani, M. (2021). A lightweight authentication protocol for IoT-based cloud environment. International Journal of Communication Systems, 34(11), e4849.