Airo International Research Journal
Volume 22: March 2020
Issue: 2320:3714

Analyzing authentication and authorization schemes to secure Cloud Services in Multi-tenancy Environment

Tanveer Ahmad[1], Rajiv Pandey[2], Suhel Ahmad Khan[3]

Department of computer science, Amity University, Lucknow (UP) INDIA[1, 2]
Department of computer science, Indira Gandhi National Tribal University, Amarkantak (MP) INDIA[3]

ABSTRACT. *Software as a Services' (SAAS) applications over the cloud are most used services in cloud environment especially for Multi-tenancy. The sharing of the computing resources with other consumers is called multi-tenancy. Mostly public cloud is based on multitenant architecture. Questions related to Performance evaluation and data security being asked from cloud provider at the time of supplying services to vendors. Types of Multi-tenancy, different authentication and authorization schemes along with principle of least privileges being presented. This paper gives a clear picture to the reader, to choose appropriate multi-tenancy environment and authorization scheme for its SAAS services along with details of authentication and authorization in azure cloud .*

.

Keywords: Principle of least privileges; Authentication; Authorization; Cloud Security; Multi-tenancy;

1. Introduction. A platform used for accessing computing resources like servers, physical storage, network, hosted applications over the network are defined as cloud computing. The computing resources will be accessed in sharing mode over the network based on demand. To get near about 100% utilization of the computing resources and save Operational cost, the cloud providers prefer Multi-tenancy concept especially in software as services (SAAS) computing model. Therefore Multi-tenancy environment needs to pay more attention by the researchers.

Multi-tenancy - A single software instance that served multiple users is called multi-tenancy, or tenants. However, in modern cloud computing, this is called shared cloud infrastructure instead of just a shared software instance [1]. In public cloud multi-tenancy defined as a shared software instance. The tenants are isolated from each other via permissions. Isolation of data can be taken care by cloud providers. Benefits of multi-tenancy are better use of resources and lower costs. If set up of cloud infrastructure is not correctly configured then tenant may face the security issue like loss of data, noisy neighbor due to heavy utilization of available resources. A multi-tenant application is more vulnerable to instance failure than a single-tenant application. If a single-tenant instance fails, only the user of that instance is affected. If the multi-tenant instance fails, all users are affected.

Authentication ensures the authenticity of the user and authorization ensures the permission boundary of the end user. There are many ways to authenticate the requestor of the cloud services like, Authentication via username and password, Biometric authentication, Public Key Infrastructure (PKI),Single sign-on (SSO), Trusted Computing Group, and Multi-factor authentication (MFA).

Authorization is a tool to check the utilization limit of the user on the system inside the guardrail The authorization techniques presently exist in multitenant environments are govern by Policy base access control system (PBAC) ,role base access control (RBAC); attribute base access control (ABAC); and user & Password base mechanism.
The principle of least privilege is the idea that at any user, program, or process should have only the bare minimum privileges necessary to perform its function.
The principle of least privilege can be applied to every level of a system. It applies to end users, systems, processes, networks, databases, applications, and every other facet of an IT environment.

This article describes a clear picture to the reader, to choose appropriate multi-tenancy architecture, authentication methodology and authorization scheme for security access SAAS services from cloud. Section 2 describes about delivery model, section 3 describes about related work on authentication & authorization. Section 4 describes multi-tenant architecture, Azure authentication and Authorization analysis. Section 5 focuses on conclusion and future work.

2. Multi-tenant Cloud Computing Model. The cloud computing is divided into deployment model and services delivery model. This section describes about the deployment model, introduction of the cloud provider and their services, example of the delivery model and talk on security concern associated with the delivery models.

Public Cloud - Organizations owning cloud services provide IT infrastructure platform to general public [2]. Examples of public cloud providers are Microsoft azure, Amazon web services and Google app engine etc. The town hall meeting that was conducted by president Obama in 2009 is one of the example of public cloud. By using unsecured application knowingly or unknowingly, corporate sensitive data is getting exposed. Data breach (GDPR issue), Weak authentication and identity management and DDoS issues on which researchers need to work more in case of public cloud.

Private cloud – Private cloud infrastructure is operated or managed by an organization, for it or a third-party functioning from within or outside the organization [3]. In private cloud there is a high security firewall associated with. Few of the private cloud provider and its services are HPE that offers Helien cloud suite software, VMWARE that offers vRealize suite cloud management platform, Microsoft that offers Hyper – V virtualization & Microsoft windows servers with many features of Cloud & Microsoft Azure stack and AWS offers Virtual private cloud (VPC) and Cloud storage. Threat and security concern may be possible like inside the organization may be risk of compromise through a host attack vector explaining local applications such as browsers or document viewers. Security challenges on private cloud may be faced (1) Un-patch of Hypervisor At the time of scalability and consistency, (2) During patch management (3) During in appropriate configuration 4) Insecure API.

Hybrid Cloud – The combination of private and public cloud is termed as Hybrid cloud. This combination together behaves as single entity. Bonding between these entities are based on remarkable technologies that make portability of application and its data hassle free. Good part of hybrid cloud is that some hybrid deployment is required during spike in demand and this can be achieved by CLOUD BURST concept. A cloud burst generally happens when an application is deployed dynamically into the internal infrastructure of the firm. Cloud burst dynamic deployment also happens when the demand spike occurs [4]. Hybrid cloud data centers are available at both on premises and on public cloud and it manage the load by application delivery controller (Load balancer).

3. Related Work. The related work on Multi-tenancy and authorization model has been described in this section.

Naveed G et al presented biometric authentication techniques in which physiological traits of human beings are used to identify or verify the authenticated user [5]. Finger print, Iris, Facial, Retina all are together create a powerful security. At large scale this methodoly is hard to implement.

Tayibia et al presents review on SSO enabling technologies and discusses SSO architectures, protocols and analysis related to growing use of SSO. SSO is an access control method that allows a user to access multiple domains on a single step of authentication, but if somehow user credential is breached the n multiple cloud services will be hamper.

Ashok Kumar et al proposed Collaborative PKI will be considered as a novel step towards the use of both the technology of Kerberos and GnuPG [6].Public Key Infrastructure (PKI) is a repository and management system for digital certificates. This proposed framework may face performance issue in multi-tenant environment due to heavily encryption and decryption involvement.

Deepa et al proposed data security architecture with a robust, dynamic and feasible Multi-Factor Authentication (MFA) scheme which integrates more than one factors
Like knowledge, possession, location and time, for cloud user authentication [7].

Shruti et al presented the state-of-art of multi-tenancy in cloud. In multi-tenancy the tenants who are sharing the resources doesn't have right to modify the application configuration and data [8]. In this paper researcher are planning to provide an authorization model based on principle of least privileges which will secure cloud services in multi-tenant environment.

J.Vijay et al presented identity management mechanism that provides directory services for application access management [9]. Different filters like exception, action and result has been considered by Vijaya's custom authorization. To apply the said filters different config setting s needs to be updated like ADGroup, Attribute, PharmaBrossard. In this paper researcher are planning to provide an authorization model based on principle of least privileges which will secure cloud services in multi-tenant environment.

AWS Lambda concept has been introduced to achieve Multi-tenancy in AWS cloud. AWS Lambda uses lambda authorizers. Lambda authorizer's uses bearer token
or Oath authentication is. It receives caller's identity in token called token authorizers. Request Authorizers receive the caller identity as a JSON which contains stage variables, headers, context variables and query string [10].

Azure Active Directory (Azure AD) is Microsoft's cloud based identity and access management service (ACS).it helps your sign in and access resources [11]. The ACS solves time consuming problems. In this paper researcher are planning to provide an authorization model based on principle of least privileges which will secure cloud services in multi-tenant environment.

Deqing Zou et al presented a framework which is addressing security issues on software defined network (SDN) controller [12].
More detail on azure authentication and authorization given in next section.

4. Multi-tenant architecture, Azure authentication and Authorization analysis.

The Main requirement of multi-tenancy is that the software provider gets many requests from customers with the customized needs. The software cannot be maintained easily if there are

different implementations of the product. Multi-Tenancy allows single software to be served between the multiple customers by using customized settings option .Multi-Tenancy means sharing the application software between multiple users who have different needs.

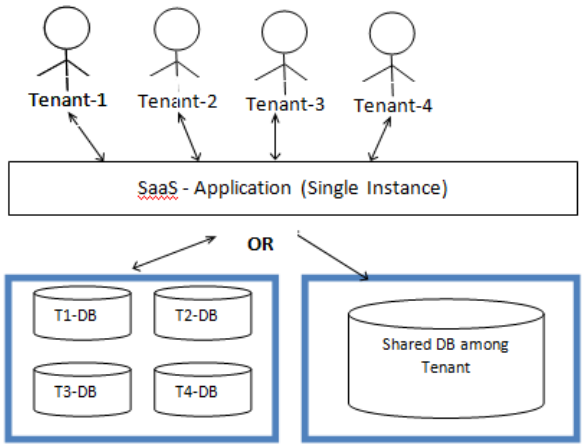


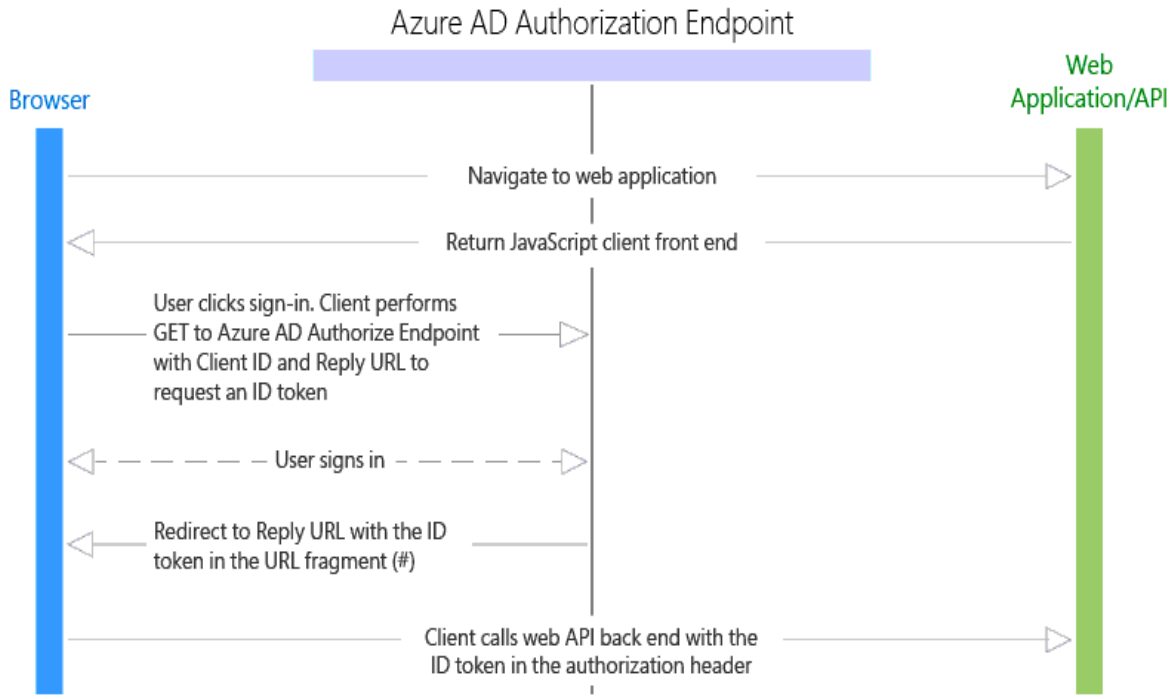
Figure 1: Multi-tenancy High Level Diagram

Figure 1 depicts the high level tenancy diagram where multiple tenants share the single saas application instance. Tenants could have their individual data storage or it could be shared Database, depends on the cloud consumer and provider agreement.

Azure Authentication - The researcher explains the step by step authentication process in public cloud Azure

1. Authenticates users with the specified provider, Validates, stores, and refreshes tokens and Injects identity information into request headers.
2. App Service makes the claims in the incoming token available to your code by injecting them into the request headers (Authorization Header).
3. When the host authenticates the user, it creates a principal, which is an IPrincipal object that represents the security context .under which code is running. The host attaches the principal to the current thread by setting Thread.CurrentPrincipal.
4. The principal contains an associated Identity object that contains information about the user. If the user is authenticated, the Identity.IsAuthenticated property returns true otherwise it's false.
5. When we enable authentication and authorization with azure active directory, its sign-in endpoint is available for user authentication.
6. For validation of authentication tokens from the azure active directory.
    a. The user navigates to the web application.
    b. The application returns the JavaScript front end (presentation layer) to the browser.
    c. The user initiates sign in, for example by clicking a sign in link. The browser sends a GET to the Azure AD authorization endpoint to request an ID token. This request includes the application ID and reply URL in the query parameters.
    d. Azure AD validates the Reply URL against the registered Reply URL that was configured in the Azure Portal.

e. The user signs in on the sign-in page.
f. If authentication is successful, Azure AD creates an ID token and returns it as a URL fragment (#) to the application's Reply URL. For a production application, this Reply URL should be HTTPS. The returned token includes claims about the user and Azure AD that are required by the application to validate the token.
g. The JavaScript client code running in the browser extracts the token from the response to use in securing calls to the application's web API back end.
h. The browser calls the application's web API back end with the access token in the authorization header.



Azure Authorization - After authentication process completes, its required to authorize the saas services by below steps.

- Azure App service (Web API) validates the token and if token is not valid (Client id, resource etc) then straight away it will send the response as 401.
- If Token is valid then app service will forward the request to actual deployed code and some time code will also validates the token in some scenarios it will validates the role claims and server the response.

5. Conclusion.

This paper is focused on the importance of multi-tenancy environment, Principle of least privilege concept, Authentication and authorization process in azure cloud. In future, researcher is planning to present a framework, which will analyze and report the

compliant status of the system against Principle of least privilege so that saas services could be secure in multi-tenant environment.

REFERENCES

[1] Webreference:https://www.cloudflare.com/learning/cloud/what-is-multi-tenancy / visited on 10/01/2020

[2] Ronald L.krutz, Russell, Cloud security – a comprehensive guide to secure cloud computing, Dean University. ISBN: 978-0-470-93894-2, 2010

[3] Web-reference https://www.datamation.com/cloud-computing/private-cloud-providers.html visited on 30/09/2018

[4] Noha Xue, Harek Haugerud ,On automated cloud bursting and hybrid cloud setups using Apache Mesos, ,DOI: 10.1109, 8284707,IEEE, CloudTech.2017.

[5] Ghazal Naveed and Rakhshanda Batool, "Biometric Authentication in Cloud Computing". J Biom Biostat 6: 258. doi:10.4172/2155-6180.1000258, 2015

[6] Ashok Kumar J, Gopinath Ganapathy, A Novel Collaborative PKI Framework in Public Cloud,International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878, Volume-8 Issue-5, January 2020

[7] Deepa pause, P. Haritha, Multi Factor Authentication in Cloud Computing for Data storage Security,International Journal of Advanced Research in Computer Science and Engineering, Vol. 4, Issue 8, ISSN: 2277-128X, pp. 14-18,August 2014

[8] Shruti Kanade,Ramesh Manza ,A Comprehensive Study on Multi Tenancy in SAAS Applications, International Journal of Computer Applications (0975 – 8887) Volume 181 pp. 44, March 2019

[9] J. Vijaya Chandra, Narasimham Challa, Sai Kiran Pasupuletti , Authentication and Authorization Mechanism for Cloud Security , International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-8 Issue-6, August 2019

[10] Web-reference https://docs.aws.amazon.com/apigateway/latest/developerguide/apigateway-use-lambda-authorizer.html visited on 09/12/2019

[11] Web-reference https://azure.microsoft.com/en-us/ ,Azure active directory (Azure AD) and API management system (APIM) visited on 15/09/2018

[12] Ronald L.krutz, Russell, Cloud security – a comprehensive guide to secure cloud computing, Dean University. ISBN: 978-0-470-93894-2, 2010