Partners Universal International Research Journal (PUIRJ)

Volume: 01 Issue: 01 | Jan-Mar 2022 www.puirj.com

Multi-Tenant Cloud Environment and its Authorization

Tanveer Ahmad[1], Rajiv Pandey[2], Mohammad Faisal[3]

[1,2]Department of Computer Science, Amity University, Lucknow (UP) INDIA.
[3]Department of computer application, Integral University, Lucknow (UP) INDIA.

---***---

Abstract- *Software as a Service (SAAS) applications delivered via the cloud are the most popular services in the cloud, particularly for multi-tenancy. Multi-tenancy refers to the sharing of computer resources with other users. Multitenant architecture is commonly used in public clouds. When offering services to vendors, cloud providers are asked questions about performance evaluation and data security. The many types of multi-tenancy, various authentication and authorization techniques, as well as the idea of least privileges are all discussed. This article provides the reader with a clear image of how to pick the right multi-tenancy environment and authorization method for their SAAS applications, as well as data on authentication and authorization in the Azure cloud.*

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

1.INTRODUCTION

The cloud computing is a platform for accessing computer resources such as servers, physical storage, networks, and hosted applications through the internet. On demand, computer resources will be accessed over the network in a sharing mode. Cloud providers like the multi-tenancy idea, especially in the software as a service (SAAS) computing model, to attain close to 100% utilization of computing resources and minimize operational costs. As a result, researchers should pay greater attention to the multi-tenancy environment.

Multi-tenancy - Multi-tenancy, or tenants, refers to a single software instance that serves several users. Instead of merely a shared software instance, this is referred to as shared cloud infrastructure in modern cloud computing [1]. Multi-tenancy is described as a shared software instance in the public cloud. Permissions separate the renters from one another. Cloud providers may take care of data isolation. Multi-tenancy has the advantages of improved resource use and cheaper expenses. If the cloud infrastructure is not properly set up, tenants may have security issues such as data loss or a noisy neighbour owing to the intensive use of available resources. Instance failure is more likely in a multi-tenant application than in a single-tenant application. Only the user of a single-tenant instance is affected if the instance fails. All users are affected if the multi-tenant instance fails.

Authentication verifies the user's validity, whereas authorization ensures the end user's permission boundary. Authentication by username and password, Biometric authentication, Public Key Infrastructure (PKI), Single sign-on (SSO), Trusted Computing Group, and Multi-factor authentication are all options for authenticating the requestor of cloud services (MFA).

Authorization is a method for determining a user's system use limit inside the guardrail. Policy-based access control (PBAC), role-based access control (RBAC), attribute-based access control (ABAC), and user-and-password-based mechanisms regulate the authorization strategies currently used in multitenant systems.

The concept of least privilege states that every user, programmed, or process should only have the privileges required to carry out its task.

The least privilege concept can be implemented at any level of a system. End users, systems, procedures, networks, databases, applications, and every other aspect of an IT ecosystem are all affected.

This article gives the reader a clear image of how to pick the right multi-tenancy architecture, authentication approach, and authorization system for cloud security access SAAS services. Section 2 discusses the delivery paradigm, whereas Section 3 discusses associated authentication and authorization operations. Multi-tenant design, Azure authentication, and authorization analysis are discussed in Section 4. The conclusion and future work are discussed in Section 5.

2.COMPUTING MODEL FOR MULTI-TENANT

There are two types of cloud computing deployment models and service delivery models. This section discusses the deployment model, introduces the cloud provider and their services, gives an example of a delivery model, and discusses security concerns related to delivery methods.

Public Cloud - Cloud service providers deliver IT infrastructure platforms to the general public [2]. Microsoft Azure, Amazon Web Services, and Google App Engine are examples of public cloud providers. The town hall meeting held by President Barack Obama in 2009 is an example of public cloud. Corporate sensitive data is exposed when employees use an insecure application, whether deliberately or inadvertently. In the case of public cloud, researchers should focus more on data breach (GDPR problem), weak authentication and identity management, and DDoS difficulties.

Private cloud – An organization's cloud infrastructure is operated or controlled by it or a third-party operating from within or outside the business [3]. There is a high-security firewall linked with private cloud. HPE offers Helien cloud suite software, VMWARE offers vRealize suite cloud management platform, Microsoft 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, to name a few private cloud providers and their services. Inside the enterprise, there is a danger of compromise through a host attack vector using local apps such as browsers or document readers. On a private cloud, there may be security issues (1 Hypervisor is unlatched. When it comes to scalability and consistency, (2) patch management, and (3) proper setup 4) Unsafe API.

Hybrid Cloud –Hybrid cloud refers to the mix of private and public clouds. This combination acts as if it were a single entity. The connection between these organizations is built on cutting-edge technologies that make application and data portability a breeze. The benefit of hybrid cloud is that it requires some hybrid deployment during periods of high demand, which may be accomplished using the CLOUD BURST idea. When an application is dynamically deployed into the firm's internal infrastructure, a cloud burst occurs. When demand spikes, cloud burst dynamic deployment is also used [4]. Application delivery controllers handle the load in hybrid cloud data centers, which are available on-premises and in the public cloud (Load balancer).

3. RELATED WORK

This section describes related work on multi-tenancy and authorisation models.

Biometric authentication approaches [5] were described by Naveed G et al, in which physiological features of human beings are utilized to identify or validate the authorized user. Fingerprint, Iris, Facial, and Retina all work together to provide a strong level of protection. This strategy is difficult to apply on a broad basis.

Tayibia et al. give an overview of SSO enabling technologies, as well as SSO designs, protocols, and analyses in relation to SSO's rising utilization. SSO is an access control approach that allows a person to log into many domains with a single authentication step. However, if a user's credentials are compromised in any way, various cloud services would be hampered.

Collaborative PKI, suggested by Ashok Kumar et al, would be regarded an unique step toward the employment of both Kerberos and GnuPG technologies [6]. The Public Key Infrastructure (PKI) is a digital certificate store and management system. Because of the heavy encryption and decryption involved in this proposed framework, it may have performance issues in a multi-tenant context.

Deepa et al suggested a data security architecture using a Multi-Factor Authentication (MFA) system that incorporates several factors that is resilient, dynamic, and practical.

For cloud user authentication, such as knowledge, possession, location, and time [7].

The goal of this work is to present an authorization model based on the concept of least privilege that will safeguard cloud services in a multi-tenant context.

J.Vijay et al [9] provided an identity management method that offers directory services for managing application access. Vijaya's custom authorization has taken into account several criteria such as exception, action, and outcome. To use the filters, certain config settings, such as ADGroup, Attribute, and Pharma Brossard, must be modified. The goal of this work is to present an authorization model based on the concept of least privilege that will safeguard cloud services in a multi-tenant context.

To accomplish multi-tenancy in the AWS cloud, the AWS Lambda concept was established. Lambda authorizers are used by AWS Lambda. Bearer token or Oath authentication is used by Lambda authorizers. Token authorizers are used to receive the caller's identification. The caller identification is delivered to Request Authorizers as a JSON file including stage variables, headers, context variables, and the query string [10].

Azure Active Directory (Azure AD) is a cloud-based identity and access management service provided by Microsoft (ACS). It assists you in logging in and gaining access to resources [11]. The ACS is used to solve issues that take a long time to solve. The goal of this work is to present an authorization model based on the concept of least privilege that will safeguard cloud services in a multi-tenant context.

Deqing Zou et al [12-15] provided a system for dealing with security vulnerabilities on software defined network (SDN) controllers.

In the following part, we'll go over Azure authentication and authorization in further depth.

4.AZURE AUTHENTICATION AND AUTHORIZATION ANALYSIS

The primary condition for multi-tenancy is that the software supplier receives a large number of requests from customers with unique requirements. If there are several implementations of the product, it will be difficult to maintain the programme. Using customised settings, Multi-Tenancy allows a single programme to be supplied to several consumers. Multi-tenancy refers to the sharing of application software across various users with varying requirements.

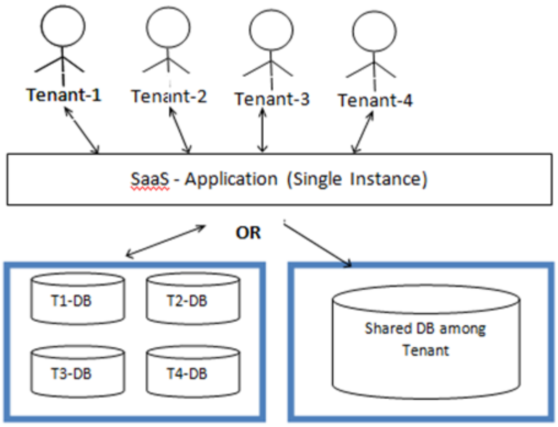

Fig -1: Multi-tenancy High Level Diagram

Figure 1 displays a high-level tenancy structure in which several tenants share a single saas app instance. Tenants may have their own data storage or share a database, depending on the terms of the cloud consumer and provider agreement.

Azure Authentication - The researcher walks you through the authentication procedure on Azure's public cloud.

1. Authenticates Validates, saves, and refreshes tokens, and injects identity information into request headers to authenticate users with the chosen provider.
2. By injecting the claims in the arriving token into the request headers (Authorization Header), the service makes them available to your code.
3. The host verifies the user's identity and constructs a principal, which is an IPrincipal object that provides the security context in which the code runs. By setting Thread, the host associates the principle with the current thread and Current Principal.
4. An Identity object is connected with the principal and includes information about the user. The Identity. IsAuthenticated property returns true if the user is authenticated, else it returns false.
5. When we activate azure active directory authentication and authorisation, the sign-in endpoint becomes available for user authentication.
6. Authentication tokens from Azure Active Directory are validated.

a. The user accesses the web application using a browser.

b. The program sends the browser the JavaScript front end (presentation layer).

c. The user takes the initiative to sign in, such as by clicking a sign in link. To request an ID token, the browser sends a GET request to the Azure AD authorization API. The application ID and reply URL are included in the query parameters of this request.

d. Azure AD compares the Reply URL to the registered Reply URL defined in the Azure Portal.

e. On the sign-in screen, the user logs in..

f. If authentication is successful, Azure AD generates an ID token and sends it to the application's Reply URL as a URL fragment (#). This Reply URL should be HTTPS in a production application. The returned token comprises user and Azure AD claims that the application need to validate the token.

g. The token is extracted from the answer by the JavaScript client code running in the browser and used to secure calls to the application's web API back end.

h. With the access token in the authorization header, the browser accesses the application's web API back end.

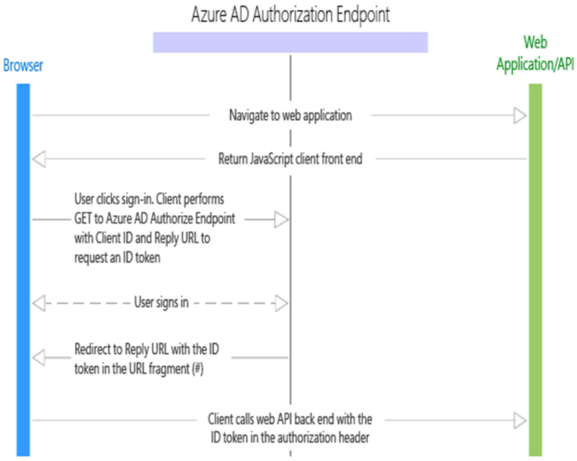
Azure AD Authorization Endpoint
Browser
Web Application/API
Navigate to web application
Return JavaScript client front end
User clicks sign-in. Client performs GET to Azure AD Authorize Endpoint with Client ID and Reply URL to request an ID token
User signs in
Redirect to Reply URL with the ID token in the URL fragment (#)
Client calls web API back end with the ID token in the authorization header

Fig -2: Azure AD Authorization Endpoint

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

- The Azure App Service (Web API) checks the token, and if the token is invalid (Client id, resource, etc.), the return code is 401.
- If the token is legitimate, the app service will forward the request to the actual deployed code, which may or may not validate the token. In certain cases, the code may also

validate the role claims and provide the answer.

5. CONCLUSIONS

The relevance of a multi-tenancy environment, the principle of least privilege, and the authentication and authorization procedure in the Azure cloud are all discussed in this article. In the future, the researcher plans to propose a framework that will examine and report the system's compliance with the principle of least privilege, allowing SaaS services to be safe in a 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

[13] Pandey, D., Wairya, S., Al Mahdawi, R. S., Najim, S. A. D. M., Khalaf, H. A., Al Barzinji, S. M., &Obaid, A. J. (2021). Secret data transmission using advanced steganography and image compression. International Journal of Nonlinear Analysis and Applications, 12(Special Issue), 1243-1257.

[14] Pandey, D., Pandey, B.K. &Wairya, S. Hybrid deep neural network with adaptive galactic swarm optimization for text extraction from scene images. Soft Comput 25, 1563–1580 (2021). https://doi.org/10.1007/s00500-020-05245-4

[15] Pandey, B. K., Pandey, D., Wariya, S., &Agarwal, G. (2021). A Deep Neural Network-Based Approach for Extracting Textual Images from Deteriorate Images. EAI Endorsed Transactions on Industrial Networks and Intelligent Systems, 8(28), e3.