IDENTITY AND ACCESS MANAGEMENT IN CLOUD ENVIRONMENT: MECHANISMS AND CHALLENGES

CSCI 5410 – Serverless Data Processing
Assignment 3 – Part B

Dhrumil Amish Shah (B00857606)
dh416386@dal.ca

Identity and Access Management in Cloud Environment: Mechanisms and Challenges [1]

The study highlights the security issues of cloud computing due to various attacks in the network. The primary concern in cloud computing is secure cloud access. With features like multitenant architecture (Single instance that serves multiple customers) and third-party infrastructure management, security features identity (authentication) and access management (authorization) are essential.

To overcome security issues in the cloud, authors have discussed various techniques such as authentication mechanisms, authorization mechanisms, identity access management systems, security threats in cloud computing, security attacks associated to the threats, and an analysis of ways of overcoming the security concerns. The study concludes by recommending some of the best practices used for implementing cloud-based solutions.

Authentication assures that the person or any application claiming access is the eligible entity. Cloud computing uses either a single or a combination of authentications for improved security. Mechanisms discussed in this paper are physical security mechanisms that protect the data centres from data leaks from insiders or any third party by providing trusted access using access cards, biometrics, facial, fingerprint, palm, iris, or retina recognition. For digital cloud protection, many security mechanisms are established, such as access credentials which are managed using technologies like Lightweight Directory Access Protocol (LDAP) and Microsoft Active Directory (AD). SSH keys to access SSH servers using public-key cryptography or challenge-response authentication. The main advantage of using SSH is that passwords are not transmitted over the network and thereby eliminating guessing of credentials through brute force attacks. Multifactor authentication is another mechanism used for authenticating users involving multiple levels of authentications to allow a user to successfully login into the application. Single Sign-On (SSO) method is used to handle the workload of cloud applications with a large number of user requests. Enterprise SSO and OpenID are some commonly used SSOs for authentication mechanisms.

Authorization assures that the cloud resource requested for access is by an authenticated user authorized to use that specific resource. In cloud computing, authorization is achieved by access control policies or delegations. Centralized access control mechanisms are used by organizations to secure their applications, data associated to it, services, and resources in the application. The access control mechanisms discussed in the study are Mandatory Access Control (MAC), Discretionary Access Control (DAC), Task-based access control, Role Based Access Control (RBAC), and Attribute-based Access Control (ABAC). MAC mechanism allows the system manager to grant access to the users using the operating system. DAC, on the other hand, is discretionary and hence the provisioning of access to the users is done by the owners of the resource. Task-based access control mechanism is defined to provide access to the user to perform a specific task. Role-based access control bifurcates the users in groups to assign permissions to them, or individually for them to have roles that will allow them to access various cloud resources. Attribute-based access control provides the various attributes like subject attributes, object attributes, resource attributes, and environment attributes to be checked before a user is granted access to use the resource. The study then describes the access control management that is done using the Identity and Access Management (IAM) system in any cloud application. Cloud service providers provide IAM as a service to its user to be able to efficiently manage the security of their cloud application. Security is IAM is managed using the Governance, Risk Management, and Compliance (GRC) mechanism where Governance

refers to the organizational hierarchy, Risk Management refers to managing the risks related to the cloud security, and Compliance refers to the completeness of checklist for ensuring the security of the cloud application with respect to the organization policies.
Identity and Access Management (IAM) system is a service designated to administer, monitor, identify, maintain the security in cloud applications. It mainly involves applying organizational policies for authenticating and authorizing users securely in the application. It is used between an enterprise, or even outside the enterprise between a private organization and a service provider. The main task of an IAM system is to locate the crucial resources in a cloud application to establish policies that would govern the security of these identified resources. There are multiple serviceable areas in IAM like identity management and provisioning, authentication management, federated identity management, authorization management and compliance management. Identity management is used to spot resources, users, and the service provisioning information between the parties in deal. This is achieved using the Service Provisioning Markup Language (SPML). Authentication management carries out the process of authentication where it ensures that the digital certificates and passwords being used by every user are securely stored in a safe place. Federated Identity Management verifies cloud services using the organization's selected identity provider. This is done to ensure the privacy, confidentiality, and integrity of services in the cloud application. Authorization management deals with the authorization process for the resources in the cloud application. Compliance management deals with governing the organizational policies and enforcing security on basis of those policies.

Further, the authors describe the security concerns and the attacks associated to each of those threats. The security threats in any cloud applications are influenced with a list of factors such as performance, availability, cost, regulatory requirements, privacy, access and control, auditing and compliance, data control, and legal issues. The various attacks described in the study are based on factors such as Protocols and Standards, Web-Services, Web-Technologies, and Availability of Services. The types of security attacks discussed are Session Hijacking, network-based attacks, cookie theft, TLS attack, Spoofing Attacks, Wrapping attacks, Web sites growth infection, session attacks, manipulation attacks, malware downloads, browser vulnerabilities, Flooding attacks, DNS reflection and amplification attack. The authors have also described ways to overcome these security concerns and attacks.

Lastly, the authors recommend some of the best followed industry practices that help the application developers build secure cloud applications. Some of the practices and standards suggested are the use of multifactor authentication mechanism to allow only legitimate users access the application, OpenID to support encrypted communication in the application, role-based access control mechanism for authorization, and identity & account certification, life cycle management and segregation of duties for governing these access control mechanisms.

References

[1] I. Indu, P. R. Anand and V. Bhaskar, "Identity and access management in cloud environment: Mechanisms and challenges," ScienceDirect, August 2018. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2215098617316750?via%3Dihub. [Accessed 30 October 2021].