Although cloud computing has a lot of advantages and compelling reasons in its favor, the key concern in cloud computing continues to be security and unauthorized access. In this chapter, we will compare user access issues between traditional IT and the cloud. **AAA** is an abbreviation for Authentication, Authorization, and Accounting, a traditional and successful battle-tested model for user access, which needs to be adapted to the cloud.

The key data requirements in a cloud are confidentiality, integrity, and availability. This chapter covers the confidentiality aspect. The cloud provider can ensure that the resources are scalable, the process is compliant with regulations, and the services meet the performance and availability requirements. However, they do not provide security assurances.

The cloud providers and users must make sure that the login access is well protected. In the cloud, users have multiple ways to authenticate and check user identities. The login credentials must be encrypted with the Personally Identifiable Information (PII) for security.

The AAA Model

AAA (or triple-a) has traditionally proven to be a battle-tested model for user-access security. The abbreviation is based on the sequence of what happens when a user logs in. This makes the concept easier to understand and remember. The login or security server first checks if the login name and password are legitimate. If so, the user is "authenticated" and permitted in. It then decides the modules of the application or sets of data that he or she can use or view. This is called authorization. The server keeps a log or account of all the resources utilized and the user activities.

Authentication

Validating a user's identity to permit or reject a login is called authentication. It is as if the system requires proof that the user is who he/she claims to be. This kind of access can be required for a system (a router, switch, storage system, server, etc.), an application, or a database. Authentication requires an identifier and its corresponding credential. An identifier could be a login name or a login ID. The credential could be a password, a digital certificate, a calling or called phone number, or a one-time token.

The AAA server compares the entered details with a stored database. If the identifier and credentials match, the user is allowed access to the application or the system. If they do not match, the user is denied access.

Authorization

Authorization permits a user to do certain activities and denies other activities. After accessing a system or application, a user issues a command. The AAA server decides whether the user should be allowed or denied execution of the command.

Compared to authentication, authorization is much more complicated and with several steps. After successful authentication, the AAA or access server provides several user-related information, such as the following:

- Data the user can view
- Data the user can edit
- Commands the user can run
- Applications the user can start
- Level of access within each application or system

This information can be stored in several ways such as a Role-Based Access Control (RBAC) database. Authorization can also be based on the time of day, the IP network, the requested QoS, the number of logged-in users, etc.

Authorization for cloud-based users helps enforce security policies for different cloud resources. All users do not need read or read-write access for all resources. The cloud provider uses a scalable, centralized database of permissions for each user and for each resource (hardware or application). Figure 1 shows the authentication and authorization process for a cloud user:

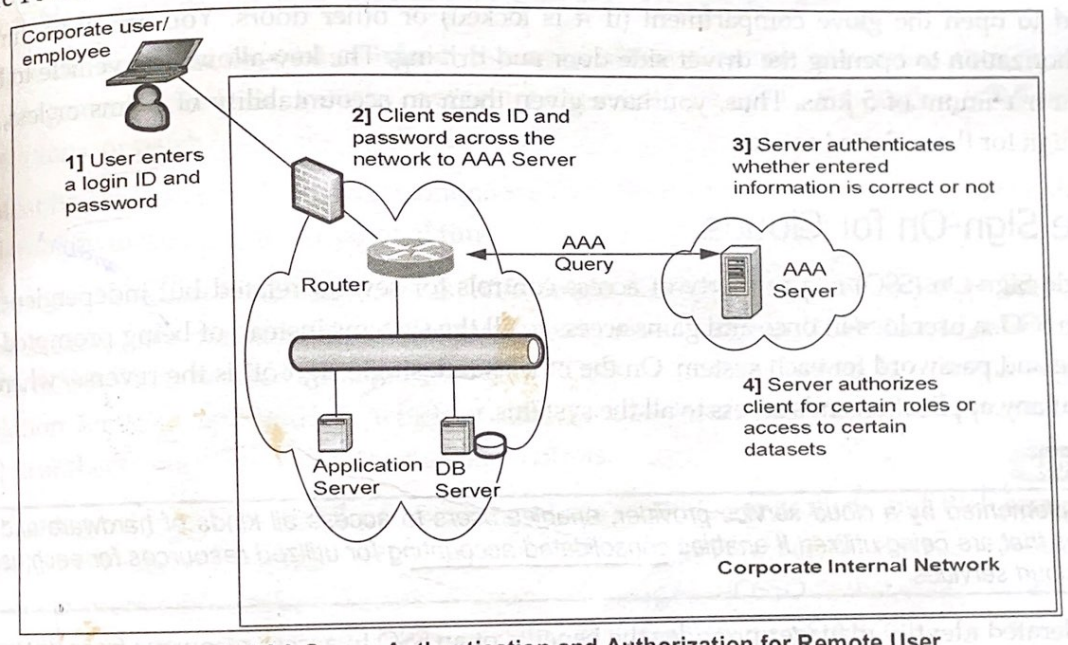

Figure 1: AAA Server Authentication and Authorization for Remote User

Accounting of Cloud Resource Utilization

Accounting does not allow or deny anything. It just keeps a log of resource consumption such as the following:

- Identity of the user
- Amount of resource used
- Start and end time of use

- Amount of data transferred
- Length of connection
- Purpose of using the resource
- Nature of service delivered

Following are the two types of accounting reports:

- **Real Time Accounting Information**—This is delivered concurrently with resource consumption. This is useful for cloud users to track usage and predict the bill, expected at the end of the payment cycle.
- **Batch Accounting Information**—This information is saved and delivered at a later time. Such data is useful for cloud service providers for billing at the end of each payment cycle. The data is also used for studying utilization trends and capacity planning.

A simple example of AAA is valet parking. Many restaurants or hotels that you visit may have a valet parking service. To avail this service, you are required to give the car keys to them. Thus, you are authenticating them to take your vehicle away. However, for security reasons, you may give them a valet key (instead of the regular keys you use). The valet key starts the vehicle but cannot be used to open the glove compartment (if it is locked) or other doors. You are, thus, limiting the authorization to opening the driver side door and driving. The key allows the vehicle to be driven for a maximum of 5 kms. Thus, you have given them an accountability of 5 kms or less, which is enough for the assigned work.

Single Sign-On for Clouds

Single Sign-On (SSO) is a property of access controls for several related but independent systems. With SSO, a user logs-in once and gains access to all the systems instead of being prompted for login name and password for each system. On the other hand, single sign-off is the reverse, where signing out at any application ends access to all the systems.

EXAM PRISM

SSO, implemented by a cloud service provider, enables users to access all kinds of hardware and software resources that are being utilized It enables consolidated accounting for utilized resources for each user across various cloud services.

A federated identity manager provides the benefits of an SSO to access resources from different cloud providers. It has certain disadvantages such as it is a single point of failure. Furthermore, it does not provide access control or custom authentication. However, it has several benefits such as:

- It allows access to resources from different cloud providers using a single authentication.
- It reduces phishing attacks, because users do not have to enter passwords again and again.
- It improves user efficiency and easy access to resources available from the cloud service provider.
- It reduces administrative overhead, because password security has to be enabled and managed only once.

- It centralizes reporting by the cloud provider for better adherence to compliance.

Following are some drawbacks to SSO:

- Unavailability of the SSO server, for example, due to network link failure, disables access to all the systems and applications managed under the SSO. It can prove to be a single point of failure.
- Upon successful access, SSO grants permission to all the resources even though the user may not require access to many of those.
- It does not custom authentication or access control.

SSO requires an increased focus on protecting user credentials and makes the security of access servers and traffic more critical. Cloud service providers can use a One Time Password (OTP) or a smart-card based access. OTP asks the user for a password that is valid for a short time-duration, thus, making it safe from replay attacks. Even if an intruder gets the OTP, he/she cannot use it later, because it expires soon. IT can be related to a hardware such as a security token. A common token is RSA's SecurID. OTPs are also sent as SMSs or e-mails to users to use immediately.

For cloud service providers to successfully use SSO, their implementation must be:

1. Highly- available with 24/7 monitoring.
2. Scalable to meet demands of thousands of users across the globe.
3. Have the ability to support standards deployed within customer enterprises such as identity management solutions, security event management solutions, application administration solutions, or patch/software distribution solutions.
4. Must have regular backups with Continuous Data Replication (CDR) to a remote site and with the ability to rollback at any point of time.

An ideal SSO solution for cloud users is Web Single Sign-On. It enables access to Web portals without creating and maintaining a user-database or access solution. Tools like Java Open Single Sign-On (JOSSO) can be used by cloud providers. JOSSO is an open-source, Java-based single sign-on solution for Web applications, which enables Java Authentication and Authorization Service (JASS) to authenticate users and enforce access controls.

The advantage of JOSSO is that the framework allows multiple applications and Web servers, such as Apache HTTP Server, Tomcat, JBOSS, and PHP (Hypertext Preprocessor Scripting Language), to authenticate users with credential store. Another advantage of JOSSO is that it is easy to integrate with other non-Java applications, because it exposes SSO using SOAP (Simple Object Access Protocol) over an HTTP protocol.

JOSSO communicates with credential stores over a JDBC (Java Database Connectivity) connection or over LDAP (Lightweight Directory Access Protocol). Both are easy to install and customize.