CAP470: Cloud Computing
Cloud Access, Storage and File Systems

Unit – IV Part - 1

Access Control in Cloud Computing

- Access control is a security technique that regulates who or what can view or use resources in a computing environment. It is a fundamental concept in security that minimizes risk to the business or organization.
- There are two types of access control:
  - **Physical access control** limits access to campuses, buildings, rooms and physical IT assets.
  - **Logical access control** limits connections to computer networks, system files and data.

Importance of Access Control

- The goal of access control is to minimize the security risk of unauthorized access to physical and logical systems.
- Access control is a fundamental component of security compliance programs that ensures security technology and access control policies are in place to protect confidential information, such as customer data.
- Most organizations have infrastructure and procedures that limit access to networks, computer systems, applications, files and sensitive data, such as personally identifiable information (PII) and intellectual property.
- Access control systems are complex and can be challenging to manage in dynamic IT environments that involve on-premises systems and cloud services.
- After some high-profile breaches, technology vendors have shifted away from single sign-on (SSO) systems to unified access management, which offers access controls for on-premises and cloud environments.

Working of Access Control

- These security controls work by identifying an individual or entity, verifying that the person or application is who or what it claims to be, and authorizing the access level and set of actions associated with the username or Internet Protocol (IP) address.
- Directory services and protocols, including Lightweight Directory Access Protocol (LDAP) and Security Assertion Markup Language (SAML), provide access controls for authenticating and authorizing users and entities and enabling them to connect to computer resources, such as distributed applications and web servers.
- Organizations use different access control models depending on their compliance requirements and the security levels of information technology (IT) they are trying to protect.

Types of Access Control

- The main models of access control are the following:
  - **Mandatory access control (MAC)**
  - **Discretionary access control (DAC)**
  - **Role-based access control (RBAC)**
  - **Rule-based access control**
  - **Attribute-based access control (ABAC)**

- **Mandatory access control (MAC).** This is a security model in which access rights are regulated by a central authority based on multiple levels of security. Often used in government and military environments, classifications are assigned to system resources and the operating system (OS) or security kernel. It grants or denies access to those resource objects based on the information security clearance of the user or device. For example, Security Enhanced Linux (SELinux) is an implementation of MAC on the Linux OS.

- **Discretionary access control (DAC).** This is an access control method in which owners or administrators of the protected system, data or resource set the policies defining who or what is authorized to access the resource. Many of these systems enable administrators to limit the propagation of access rights. A common criticism of DAC systems is a lack of centralized control.

- **Role-based access control (RBAC).** This is a widely used access control mechanism that restricts access to computer resources based on individuals or groups with defined business functions -- e.g., executive level, engineer level 1, etc. -- rather than the identities of individual users. The role-based security model relies on a complex structure of role assignments, role authorizations and role permissions developed using role engineering to regulate employee access to systems. RBAC systems can be used to enforce MAC and DAC frameworks.

- **Rule-based access control.** This is a security model in which the system administrator defines the rules that govern access to resource objects. Often, these rules are based on conditions, such as time of day or location. It is not uncommon to use some form of both rule-based access control and RBAC to enforce access policies and procedures.
- **Attribute-based access control (ABAC).** This is a methodology that manages access rights by evaluating a set of rules, policies and relationships using the attributes of users, systems and environmental conditions.

Building Cloud Computing Environments

- The creation of cloud computing environments encompasses both the development of applications and systems that leverage cloud computing solutions and the creation of frameworks, platforms, and infrastructures delivering cloud computing services.
  - Application development
  - Infrastructure and system development
  - Computing platforms and technologies

Application development

- Applications that leverage cloud computing benefit from its capability to dynamically scale on demand like web applications.
- Another class of applications that can potentially gain considerable advantage by leveraging cloud computing is represented by resource-intensive applications.
- Cloud computing provides a solution for on-demand and dynamic scaling across the entire stack of computing. This is achieved by
  - providing methods for renting compute power, storage, and networking;
  - offering runtime environments designed for scalability and dynamic sizing;
  - providing application services that mimic the behavior of desktop applications but that are completely hosted and managed on the provider side.

Infrastructure and system development

- Distributed computing, virtualization, service orientation, and Web 2.0 form the core technologies enabling the provisioning of cloud services from anywhere on the globe. Developing applications and systems that leverage the cloud requires knowledge across all these technologies.
- Infrastructure-as-a-Service solutions provide the capabilities to add and remove resources, but it is up to those who deploy systems on this scalable infrastructure to make use of such opportunities with wisdom and effectiveness.
- Platform-as-a-Service solu- tions embed into their core offering algorithms and rules that control the provisioning process and the lease of resources.

Computing Platforms and Technologies

- Development of a cloud computing application happens by leveraging platforms and frameworks that provide different types of services, from the bare-metal infrastructure to customizable applications serving specific purposes.
  - Amazon web services (AWS)
  - Google AppEngine
  - Microsoft Azure
  - Hadoop
  - Force.com and Salesforce.com
  - Manjrasoft Aneka

Web Applications

- A **web application** (or **web app**) is application software that runs on a web server, unlike computer-based software programs that are run locally on the operating system (OS) of the device.
- Web applications are accessed by the user through a web browser with an active network connection.
- These applications are programmed using a client–server modeled structure: the user ("*client*") is provided *services* through an *off-site server* that is hosted by a third-party.
  - Examples of commonly-used web applications include: web-mail, online retail sales, online banking, and online auctions.

- **Web application** helps to exchange information on the internet and also helps to perform a secure transaction on web sites.
- Web applications are popular as the web browser is available in **default**, we don't need any installation of software on computers with operating systems.
- For example, Facebook (a social networking web application), Flickr (a photo-sharing web application), and Wikipedia are majorly used example of a web application.
- Technically, a web application consists of two types of scripts:
  - **Client-side scripts:** JavaScript, HTML, and other client-side scripting languages are used to design the web forms to present information to users.
  - **Server-side scripts:** ASP and other server-side scripting languages are used to perform business logic and database related operations like storing and retrieving information.

Web API

- In computer programming, an application programming interface (API) is a set of subroutine definitions, protocols, and tools for building software and applications.
- API is some kind of interface which has a set of functions that allow programmers to access specific features or data of an application, operating system or other services.
- Web API is the enhanced form of the web application to provide services on different devices like laptop, mobile, and others.
- Today, all kind of businesses use the internet as a cost-effective way to expand their business in the international market.

- Web API as the name suggests, is an API over the web which can be accessed using HTTP protocol. It is a concept and not a technology. We can build Web API using different technologies such as Java, .NET etc.
  - For example, Twitter's REST APIs provide programmatic access to read and write data using which we can integrate twitter's capabilities into our own application.