

Module-4

Exploring Cloud Infrastructure



Topics..

- Managing the Cloud
- Understanding Cloud Security



Defining Cloud Management

- It is the software and technologies constructed for operating and monitoring various applications, data and services residing in the cloud. The management responsibilities depend on the particular service for based on the deployment.
- Cloud management software tools provide capabilities for managing faults, accounting, security, other performance maintenance and configuration. It contains various types of tasks including performance monitoring-which include response time, uptime and latency, security, compliance auditing and management, disaster recovery etc.
- Cloud computing management includes not only managing resources in the cloud but also managing on-premises resources.



Administrating the Clouds

- Fundamental features offered by traditional network management systems are:
 - Administration of resources
 - Configuring resources
 - Enforcing security
 - Monitoring operations
 - Optimizing performance
 - Policy management
 - Performing maintenance
 - Provisioning of resources



- Network management systems are often described in terms of the acronym **FCAPS**, which stands for these features:
 - **Fault**
 - **Configuration**
 - **Accounting**
 - **Performance**
 - **Security**
- Most network management packages have one or more of these characteristics; no single package provides all five elements of FCAPS.
- Through network frameworks like IBM Tivoli, HP OpenView, and Microsoft System Center, you can access all five areas.



Management responsibilities

- Cloud management service must have the following characteristics:
 - Billing is on a pay-as-you-go basis.
 - The management service is extremely scalable.
 - The management service is ubiquitous.
 - Communication between the cloud and other systems uses cloud networking standards.
- To monitor an entire cloud computing deployment stack, you monitor six different categories:
 1. End-user services (HTTP, TCP, POP3/SMTP)
 2. Browser performance on the client



3. Application monitoring in the cloud(Apache, MySQL)
4. Cloud infrastructure monitoring of services (Amazon Web Services, GoGrid, Rackspace)
5. Machine instance monitoring where the service measures processor utilization, memory usage, disk consumption, queue lengths, and other important parameters.
6. Network monitoring and discovery using standard protocols (Simple Network Management Protocol (SNMP), Configuration Management Database (CMDB), Windows Management Instrumentation (WMI))



- Two aspects to cloud management:
 - Managing resources in the cloud
 - Using the cloud to manage resources on-premises
- Cloud management includes not only managing resources in the cloud, but managing resources on-premises.
- The management of resources in the cloud requires new technology, but management of resources on-premises allows vendors to use well-established network management technologies.



- In the cloud, the particular service model you are using directly affects the type of monitoring you are responsible for.
- Consider the case of an Infrastructure as a Service vendor such as Amazon Web Services.
- You can monitor your usage of resources either through their native monitoring tools like Amazon Cloud Watch or through the numerous third-party tools that work with these sites' APIs



- In IaaS, you can alter aspects of your deployment, such as the number of machine instances you are running or the amount of storage you have, but you have very limited control over many important aspects of the operation.
- You have no control over how network traffic flows into and out of the system, whether there is packet prioritization, how routing is done, and other important characteristics.
- The situation—as you move first to Platform as a Service (PaaS) like Windows Azure or Google App Engine and then onto Software as a Service (SaaS) for which Salesforce.com becomes even more restrictive



- The second aspect of cloud management is the role that cloud-based services can play in managing on-premises resources.
- Microsoft System Center is an example of how management products are being adapted for the cloud.
- System Center provides tools for managing Windows servers and desktops. One of these service sets of System Center was called the System Center Online Desktop Manager (SCODM).
- Microsoft has taken SCODM and repositioned it as a cloud-based service for managing updates, monitoring PCs for license compliance and health, enforcing security policies, and using Forefront protect systems from malware, and the company has branded it as Windows Intune



Lifecycle management

- Cloud services have a defined lifecycle.
 - A management program has to touch on each of the six different stages in that lifecycle:
- *Phase 1.*
 - ✓ Tasks performed in Phase 1 include the creation, updating, and deletion of service templates.
 - *Phase 2.*
 - ✓ This phase manages client interactions with the service, usually through an SLA (Service Level Agreement)



➤ *Phase 3.*

- ✓ Tasks performed in Phase 3 include the creation, updating, and deletion of service offerings

➤ *Phase 4*

- ✓ The chief task during this management phase is to perform service optimization and customization.

➤ *Phase 5.*

- ✓ During Phase 5, you must monitor resources, track and respond to events, and perform reporting and billing functions.

➤ *Phase 6.* Retirement of the service

- ✓ End of life tasks include data protection and system migration, archiving, and service contract termination.



Cloud and Web Monitoring Solutions

Cloud and Web Monitoring Solutions

Product	URL	Description
AbiCloud	http://www.abiquo.com/	Virtual machine conversion and management
Amazon CloudWatch	http://aws.amazon.com/cloudwatch/	AWS dashboard
BMC Cloud Computing Initiative	http://www.bmc.com/solutions/esm-initiative/cloud-computing.html	Cloud planning, lifecycle management, optimization, and guidance
CA Cloud Connected Management Suite	http://www.ca.com/us/cloud-solutions.aspx	CA Cloud Insight, CA Cloud Compose, CA Cloud Optimize, and CA Cloud Orchestrate are described below
Cacti	http://www.cacti.net/	Network performance graphing solution
CloudKick	https://www.cloudkick.com/	Cloud server monitoring
Dell Scalent	http://www.scalent.com/index.php	Virtualization provisioning system that will be rolled into Dell's Advanced Infrastructure Manager (AIM)
Elastra	http://www.elastra.com/	Federated hybrid cloud management software
Ganglia	http://ganglia.info/	Distributed network monitoring



Cloud Management Products

- The core management features offered by most cloud management service products include the following:
 - ✓ Support of different cloud types
 - ✓ Creation and provisioning of different types of cloud resources, such as machine instances, storage, or staged applications
 - ✓ Performance reporting including availability and uptime, response time, resource quota usage, and other characteristics
 - ✓ The creation of dashboards that can be customized for a particular client's needs
- Eg: Amazon CloudWatch, ManageIQ, Cloudkick



Emerging Cloud Management Standards

- Different cloud service providers use different technologies for creating and managing cloud resources.
- Interoperability is a major concern.
- Commonly used standards are:
 - DMTF cloud management standards
 - Cloud Commons and SMI



DMTF Cloud Management Standards

- Stands for Distributed Management Task Force. Established in 1992.
- It is an industry organization that develops industry system management standards for platform interoperability.
- The **Common Information Model(CIM)** is a major standard introduced by DMTF.
- The DMTF organizes itself into a set of working groups that are tasked with specifying standards for different areas of technology.



- **Virtualization Management Initiative (VMAN)** was developed to extend CIM to virtual computer system management.
- VMAN has resulted in the **creation of the Open Virtualization Format (OVF)**, which describes a standard method for creating, packaging, and provisioning virtual appliances.
- OVF is essentially a container and a file format that is open.



- DMTF has created a working group called the [Open Cloud Standards Incubator \(OCSI\)](#) to help develop interoperability standards for managing interactions between and in public, private, and hybrid cloud systems.
- The group is focused on describing resource management and security protocols, packaging methods, and network management technologies.



Cloud Commons and SMI

- CA Technologies; once known as Computer Associates, has taken some of its technologies for measuring distributed network performance metrics and repositioned its product as following:
 - CA Cloud Insight, a cloud metrics measurement service
 - CA Cloud Compose, a deployment service
 - CA Cloud Optimize, a cloud optimization service
 - CA Cloud Orchestrate, a workflow control and policy based automation service
- Taken together, these products form the basis for CA's Cloud Connected Management Suite.



- CA acquired Nimsoft which has a monitoring and management package called Nimsoft Unified Monitoring that creates a monitoring portal with customizable dashboards.
- The system can gather information from up to 100 types of data points and can work with both Google and Rackspace cloud deployments.
- Among the data points that can be monitored are resource usage and UPS status.
- At the heart of CA Cloud Insight is a method for measuring different cloud metrics that creates what CA calls a Service Measurement Index or SMI.



- The Cloud Commons has built a dashboard called the **CloudSensor** that monitors the performance of the major cloud-based services in real time.
- The Service Measurement Index (SMI) is based on a set of measurement technologies forming the SMI Framework.
- It measures cloud-based services in six areas:
 - **Agility**
 - **Capability**
 - **Cost**
 - **Quality**
 - **Risk**
 - **Security**
- These form a set of **Key Performance Indicators** (KPI) that can be used to compare one service to another.



Understanding Cloud Security



Understanding Cloud Security

- Cloud security a major concern.
- We are sharing our systems with others and many times outsourcing their operations as well.
- Service providers have developed new technologies to address them.



- Different types of cloud computing service models provide different levels of security services.
- You get the least amount of built in security with an Infrastructure as a Service provider, and the most with a Software as a Service provider.
- Data stored in the cloud should be transferred and stored in an encrypted format.
- We can use proxy and brokerage services to separate clients from direct access to shared cloud storage.
- Logging, auditing, and regulatory compliance are all features that require planning in cloud computing systems.



Securing the Cloud

- Cloud computing has all the vulnerabilities associated with Internet applications, and additional vulnerabilities arise from pooled, virtualized, and outsourced resources.
- Areas of cloud computing that are identified as troublesome:
 - Auditing
 - Data integrity
 - e-Discovery for legal compliance
 - Privacy
 - Recovery
 - Regulatory compliance



- Risks in any cloud deployment are dependent upon the particular cloud service model chosen and the type of cloud on which you deploy your applications.
- The following analysis needs to be performed in order to evaluate your risks.
 1. Determine which resources (data, services, or applications) you are planning to move to the cloud.
 2. Determine the sensitivity of the resource to risk. Risks that need to be evaluated are loss of privacy, unauthorized access by others, loss of data, and interruptions in availability.




3. Determine the risk associated with the particular cloud type for a resource.
4. Take into account the particular cloud service model that you will be using.
5. If you have selected a particular cloud service provider, you need to evaluate its system to understand how data is transferred, where it is stored, and how to move data both in and out of the cloud.



- One technique for maintaining security is to have “golden” system image.
- It helps to take a system image off-line and analyze the image for vulnerabilities or compromise.
- Many cloud providers offer a snapshot feature that can create a copy of the client’s entire environment
- A snapshot includes not only machine images, but applications and data, network interfaces, firewalls, and switch access.
- If you feel that a system has been compromised, you can replace that image with a known good version.



The AWS Security Center (<http://aws.amazon.com/security/>) is a good place to start learning about how Amazon Web Services protects users of its IaaS service



Sign in to the AWS Management Console | Create an AWS Account | English

AWS

Products

Developers

Community

Support

Account

Related Resources

AWS Economics Center

AWS Security Credentials

AWS Multi-Factor Authentication (AWS MFA)

AWS Products & Services

AWS Solutions

Case Studies

Testimonial

"The improved computer security includes, but is not limited to, greater protection against network attacks and real time detection of system tampering."

- Recovery Accountability and Transparency Board on the expected security benefits from moving Recovery.gov to the AWS cloud.

AWS Security Center

This page contains the following categories of information. Click to jump down:

Overview

Certifications and Accreditations

Security Bulletins

Background Information

Security Credentials

Overview

Amazon Web Services (AWS) delivers a highly scalable cloud computing platform with high availability and dependability, and the flexibility to enable customers to build a wide range of applications. In order to provide end-to-end security and end-to-end privacy, AWS builds services in accordance with security best practices, provides appropriate security features in those services, and documents how to use those features. In addition, AWS customers must use those features and best practices to architect an appropriately secure application environment. Enabling customers to ensure the confidentiality, integrity, and availability of their data is of the utmost importance to AWS, as is maintaining trust and confidence.

At a high level, we've taken the following approach to secure the AWS infrastructure:

- Certifications and Accreditations.** AWS has successfully completed a SAS70 Type II Audit, and will continue to obtain the appropriate security certifications and accreditations to demonstrate the security of our infrastructure and services.
- Physical Security.** Amazon has many years of experience in designing, constructing, and operating large-scale data centers. AWS infrastructure is housed in Amazon-controlled data centers throughout the world. Only those within Amazon who have a legitimate business need to have such information know the actual location of these data centers, and the data centers themselves are secured with a variety of physical barriers to prevent unauthorized access.
- Secure Services.** Each of the services within the AWS cloud is architected to be secure and contains a number of capabilities that restrict unauthorized access or usage without sacrificing the flexibility that customers demand. For more information about the security capabilities of each service,



The Security Boundary

- Security boundary in cloud computing is defined based on the particular model of cloud computing we use.
- It provides a framework for understanding what security is already built into the system and who has responsibility for a particular security mechanism.
- It defines the boundary between the responsibility of the service provider and the customer.
- Various deployment models (community, hybrid, private, public clouds) and Service models (IaaS, PaaS, SaaS) provides different security boundaries.



- Cloud Security Alliance (CSA) is an industry working group that studies security issues in cloud computing and offers recommendations to its members.
- The CSA partitions its guidance into a set of operational domains.
- CSA considers multi-tenancy to be an essential element in cloud computing.
- Multi-tenancy adds a number of additional security concerns to cloud computing that need to be accounted for.
- In multi-tenancy, different customers must be isolated and their data must be segmented.
- To provide these features, the cloud service provider must provide a policy-based environment that is capable of supporting different levels and quality of service, usually using different pricing models.



Security Service Boundary

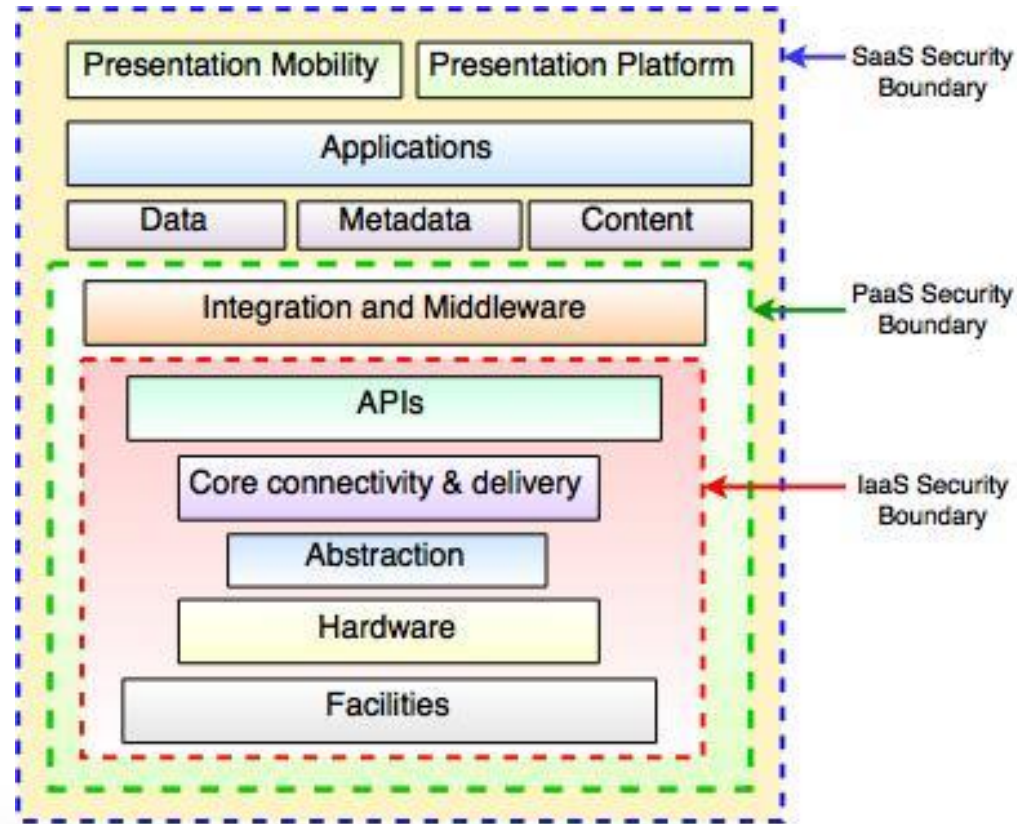


Fig.- CSA Stack Model



- In the SaaS model, the vendor provides security as part of the Service Level Agreement.
- For the PaaS model, the security boundary may be defined for the vendor to include the software framework and middleware layer.
- In the PaaS model, the customer would be responsible for the security of the application and UI at the top of the stack.
- The model with the least built-in security is IaaS, where everything that involves software of any kind is the customer's problem. Numerous



- The CSA functional cloud computing hardware / software stack is the Cloud Reference Model.
- IaaS is the lowest level service, with PaaS and SaaS the next two services above.
- IaaS supplies the infrastructure. PaaS adds application development frameworks, transactions, and control structures. SaaS is an operating environment with applications, management, and the user interface.



- As you ascend the stack, IaaS has the least levels of integrated functionality and the lowest levels of integrated security, and SaaS has the most.
- Each different type of cloud service delivery model creates a security boundary at which the cloud service provider's responsibilities end and the customer's responsibilities begin.
- Any security mechanism below the security boundary must be built into the system, and any security mechanism above must be maintained by the customer.



Security Mapping

- The cloud service model you choose determines where in the proposed deployment the variety of security features, compliance auditing, and other requirements must be placed.
- To determine the particular security mechanisms you need, you must perform a mapping of the particular cloud service model to the particular application you are deploying.



- These mechanisms must be supported by the various controls that are provided by your service provider, your organization, or a third party.
- A security control model includes the security for your applications, data, management, network, and physical hardware.
- You may also need to account for any compliance standards that are required for your industry.



Securing Data

- Brokered Cloud storage access
- Storage location and tenancy
- Encryption
- Auditing and compliance



Brokered cloud storage access

- The problem with the data you store in the cloud is that it can be located anywhere in the cloud service provider's system: in another datacentre, another state or province, and in many cases even in another country.
- To protect your cloud storage assets, you want to find a way to isolate data from direct client access.



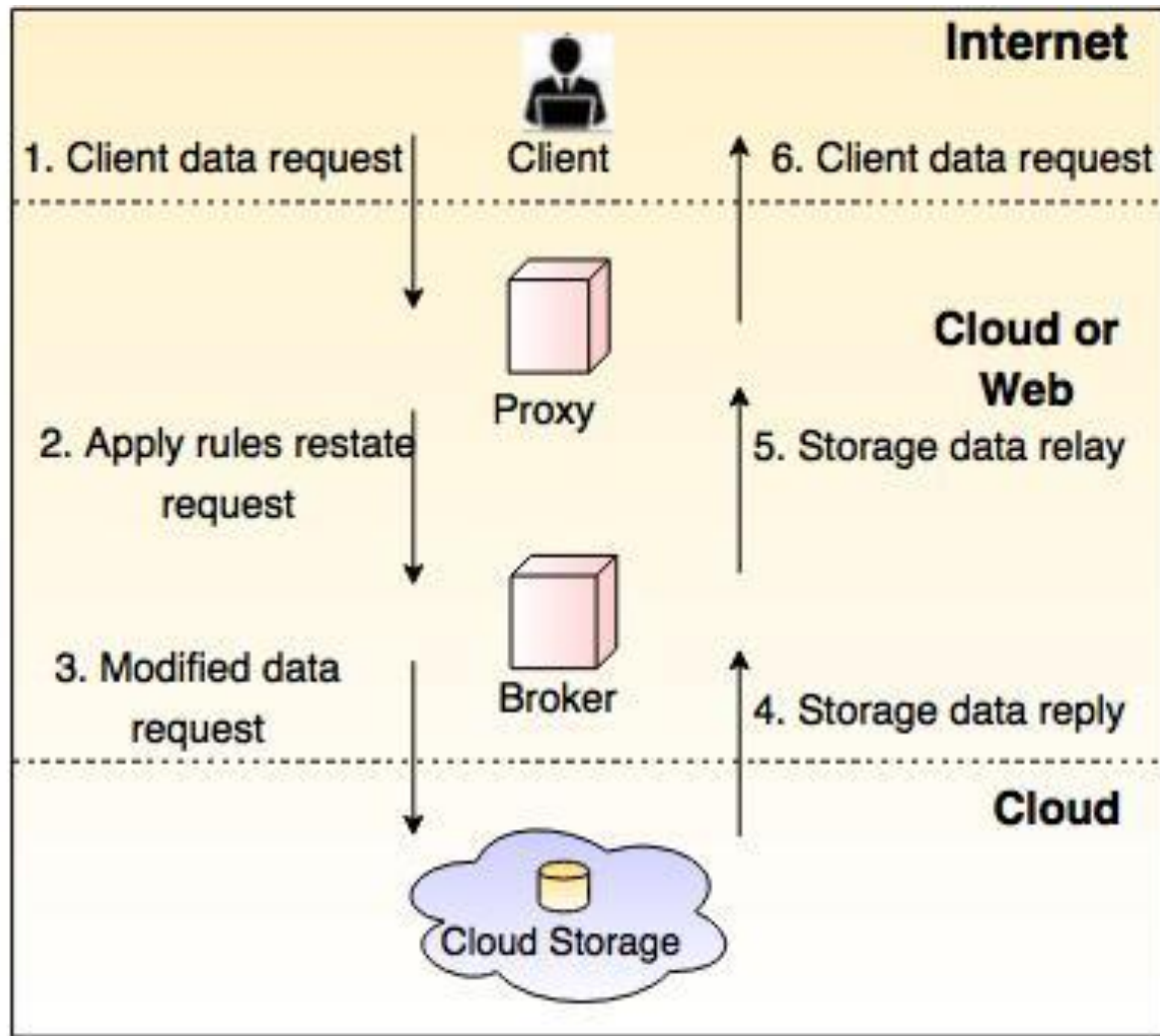
- One approach to isolating storage in the cloud from direct client access is to create layered access to the data.
- Two services are created:
 - ❖ a broker with full access to storage but no access to the client
 - ❖ a proxy with no access to storage but access to both the client and broker
- The location of the proxy and the broker is not important (they can be local or in the cloud); what is important is that these two services are in the direct data path between the client and data stored in the cloud.



Under this system, when a client makes a request for data, here's what happens:

1. The request goes to the external service interface (or endpoint) of the proxy, which has only a partial trust.
2. The proxy, using its internal interface, forwards the request to the broker.
3. The broker requests the data from the cloud storage system.
4. The storage system returns the results to the broker.
5. The broker returns the results to the proxy.
6. The proxy completes the response by sending the data requested to the client.





Storage location and tenancy

- Data stored in the cloud is usually stored from multiple tenants, each vendor has its own unique method for segregating one customer's data from another.
- It's important to have some understanding of how your specific service provider maintains data segregation.
- Another question to ask a cloud storage provider is who is provided privileged access to storage.



Encryption

- Strong encryption technology is a core technology for protecting data in transit to and from the cloud as well as data stored in the cloud.
- The goal of encrypted cloud storage is to create a virtual private storage system that maintains confidentiality and data integrity while maintaining the benefits of cloud storage: ubiquitous, reliable, shared data storage.
- Although encryption protects data from unauthorized access, it does nothing to prevent data loss.
- A common means for losing encrypted data is to lose the keys that provide access to the data.



- Therefore, key management is seriously considered. Keys should have a defined lifecycle.
- Among the schemes used to protect keys are the creation of secure key stores that have restricted role-based access, automated key stores backup, and recovery techniques.
- It's a good idea to separate key management from the cloud provider that hosts your data.
- One standard for interoperable cloud-based key management is the OASIS Key Management



Auditing and compliance

- Logging is the recording of events into a repository; auditing is the ability to monitor the events to understand performance.
- Logging and auditing is an important function because it is not only necessary for evaluation performance, but it is also used to investigate security and when illegal activity has been perpetrated.



you must understand the following:

- Which regulations apply to your use of a particular cloud computing service
- Which regulations apply to the cloud service provider and where the demarcation line falls for responsibilities
- How your cloud service provider will support your need for information associated with regulation.



Establishing Identity and Presence

- Identities also are tied to the concept of accounts.
- Identities are used to authenticate client requests for services in a distributed network system such as the internet or cloud computing services.
- Identity management is a primary mechanism for controlling access to data in the cloud, preventing unauthorized uses, maintaining user roles, and complying with regulations.



Identity Protocol Standards

- Many protocols that provide identity services form the basis to create interoperability among services.
- Commonly used Identity protocol standards:

1. OpenID

2. XACML and SAML XACML (eXtensible Access Control Markup Language) and SAML (Security Assertion Markup Language)

3. OAuth



OpenID

- OpenID 2.0 is the standard associated with creating an identity and authenticate its use by a third-party service.
- It is the key to creating Single Sign-On (SSO) systems.
- OpenID doesn't specify the means for authentication of an identity; a particular system should execute the authentication process.
- Authentication can be by a Challenge and Response Protocol (CHAP), through smart card, or a biometric measurement.



- In OpenIDL, the authentication procedure has the following steps:
 - 1.The end-user uses a program like a browser that is called a user agent to enter an OpenID identifier.
 - 2.The OpenID is presented to a service that provides access to the resource that is desired.
 - 3.An entity called a relaying party queries the OpenID identity provider to authenticate the accuracy of the OpenID credentials.
 - 4.The authentication is sent back to the relaying party from the identity provider and access is either provided or denied.



XACML and SAML

- The second protocol used is a set of authorization markup languages that create files in the form of XACML and SAML.
 - SAML (Security Assertion Markup Language)
 - XACML (eXtensible Access Control Markup Language)
- SAML is a standard for passing authentication and authorization between an identity provider and the service provider.
- Taken as a unit, OpenID and SAML are used as the standard authentication mechanism for clients accessing cloud services.
- It is particularly important for services such as mashups that draw information from two or more data services.



OAuth

- An open standard called OAuth provides a token service that can be used to present validated access to resources.
- The use of OAuth tokens allows clients to present credentials that contain no account information (userID or password) to a cloud service.
- The token comes with a defined period after which it can no longer be used.



Windows Azure Identity Standards

- The Windows Azure Platform uses a claims-based identity based on open authentication and access protocols.
- These standards may be used without modification on a system that is running in the cloud or on-premises.
- Windows Azure security draws on the following three services:
 1. Active Directory Federation Services 2.0
 2. Windows Azure AppFabric Access Control Service
 3. Windows Identity Foundation (WIF)



Presence

- Presence is used on networks to indicate the status of available parties and their location.
- Presence provides identity, status and location.
- The service that manages presence is called the presence service.
- Many presence services rely on agents called watchers, which are small programs that relay a client's ability to connect.
- Presence information is used in cloud computing services like VoIP, instant messaging services(IM) and GPS.



- Presence is playing an important role in cell phones.
- The presence service is provided by the GPS locator inside the phone, which provides a location through AT&T (the service provider) to the application.
- Presence is an essential and growing component of cloud-based services.
- Microsoft's Windows Identity Foundation is a claims-based presence system.
- A standard called the Extensible Messaging and Presence Protocol (XMPP) can be used with a federation system called the Jabber XCP to provide presence information.



- Jabber XCP is popular because it is an extensible development platform which is platform-independent and supports several communications protocols.
- In SOA protocols such as SOAP/REST/HTTP support unidirectional data exchange. You request a service/data, and a response is supplied.
- SOA architectures don't scale well and can't supply high-speed data transfers required by the services that are based on presence service technologies.
- SOA also has the problem of services that have trouble penetrating firewalls.
- Jabber and XMPP were created to solve these barriers

