5.7 Federation in the Cloud

- **connecting multiple cloud computing providers** using a common standard.

- A notable research project being conducted by **Microsoft** called the **Geneva Framework**. This framework focuses on **issues involved in cloud federation.**

Geneva

- described as **claims based access platform**
- **allows for multiple providers *to interact*** seamlessly with others
- it enables developers to incorporate various **authentication models** that will work with any corporate identity system, including **Active Directory, LDAPv3 based directories, application specific databases, and new user centric identity models** such as LiveID, OpenID, and InfoCard systems.

Federation in cloud is implemented by the **use of**

- **Internet Engineering Task Force (IETF**) standard E**xtensible Messaging and Presence Protocol (XMPP**)
- inter domain federation using the Jabber Extensible Communications Platform (**Jabber XCP**).

Session Initiation Protocol (SIP):

- is the foundation of popular enterprise **messaging systems** such as **IBM's Lotus Sametime** and **Microsoft's Live Communications Server (LCS) and Office Communications Server (OCS).**

Jabber XCP:

- is a highly **scalable, extensible, available, and device-agnostic presence solution .**
- built on **XMPP and supports multiple protocols** such as Session Initiation Protocol for Instant Messaging and Presence Leveraging Extensions (SIMPLE) and Instant Messaging and Presence Service (IMPS).
- Jabber XCP is a **highly programmable platform**,
- building next- generation, **presence based solutions**.

- **XMPP (also called Jabber)** protocol :
  - will fuel the **Software as a Service (SaaS) models** .
  - **Google, Apple, AOL, IBM, Live journal and Jive** have used this protocol into their **cloud based solutions.**

- **Polling:**
  - if the user wanted to **synchronize services** between **two servers**, the client **“ping”** the **host** at regular intervals, which is known **as polling .**
  - Polling is how most of us **check our email.**

- **Robust security** is supported via
  - Simple Authentication and Security Layer **(SASL)** and Transport Layer Security **(TLS).**
  - It is flexible and designed to be extended.
- **XMPP** is a **good fit** for **cloud computing**
  - because it allows for **easy two way communication**
  - XMPP **eliminates** the need for **polling** and
  - focus on rich **publish subscribe** functionality

- **XMPP :**
  - It is **XML-based and easily extensible**,
  - perfect for both **new IM (Instant Messaging) features and custom cloud services .**
  - It is **efficient**
  - proven to **scale to millions of concurrent users** on a single service (such as Google's **GTalk**).
  - it has a **built-in worldwide federation model**.

- **XMPP :**
  - is not the only **pub-sub enabler**
  - getting a lot of interest from **web application developers**.
- An **Amazon EC2-backed server :**
  - can run **Jetty and Cometd** from **Dojo**.
  - Comet is based on **HTTP** and in conjunction with the **Bayeux Protocol**, uses **JSON** to exchange data.

- Federation differs from **peering**, which requires a **prior agreement between parties** before a **server-to-server (S2S) link** can be established.
- In the past, peering was more common among **traditional telecommunications** providers (because of the high cost of transferring voice traffic).
- In the brave **new Internet world**, **federation** has become a **de facto standard** for most **email systems** because they are **federated dynamically through Domain Name System (DNS)** settings and server configurations.

Four Levels of Federation

four basic types of federation :

1. **Permissive federation**
2. **Verified federation**
3. **Encrypted federation**
4. **Trusted federation**

1. Permissive federation

- Permissive federation occurs when a server accepts a connection from a peer network server without verifying its identity using DNS lookups or certificate checking.
- The lack of verification or authentication may lead to domain spoofing (the unauthorized use of a third-party domain name in an email message in order to pretend to be someone else), which opens the door to widespread spam and other abuses.
- With the release of the open source jabberd 1.2 server in October 2000, which included support for the Server Dialback protocol (fully supported in Jabber XCP), permissive federation met its demise on the XMPP network.

2. Verified federation

- This type of federation occurs when a server accepts a connection from a peer after the identity of the peer has been verified.
- It uses information obtained via DNS and by means of domain-specific keys exchanged beforehand.
- The connection is not encrypted, and the use of identity verification effectively prevents domain spoofing.
- To make this work, federation requires proper DNS setup and that is still subject to DNS poisoning attacks.
- Verified federation has been the default service policy on the open XMPP since the release of the open-source jabberd 1.2 server.

3. Encrypted federation

- In this mode, a server accepts a connection from a peer if and only if the peer supports Transport Layer Security (TLS) as defined for XMPP in Request for Comments (RFC) 3920.
- The peer must present a digital certificate.
- The certificate may be self signed, but this prevents using mutual authentication.
- If this is the case, both parties proceed to weakly verify identity using Server Dialback.
- XEP-0220 defines the Server Dialback protocol, which is used between XMPP servers to provide identity verification.

- Server Dialback uses the DNS as the basis for verifying identity
- The basic approach is that when a receiving server receives a server-to-server connection request from an originating server, it does not accept the request until it has verified a key with an authoritative server for the domain asserted by the originating server.
- Although Server Dialback does not provide strong authentication or trusted federation, and although it is subject to DNS poisoning attacks, it has effectively prevented most instances of address spoofing on the XMPP network since its release in 2000.
- This results in an encrypted connection with weak identity verification.

4. Trusted federation

- In this federation, a server accepts a connection from a peer only under the stipulation that the peer supports TLS and the peer can present a digital certificate issued by a root certification authority (CA) that is trusted by the authenticating server.
- The list of trusted root CAs may be determined by one or more factors, such as the operating system, XMPP server software or local service policy.
- In trusted federation, the use of digital certificates results not only in a channel encryption but also in strong authentication.
- The use of trusted domain certificates effectively prevents DNS poisoning attacks but makes federation more difficult, since such certificates have traditionally not been easy to obtain.

5.8 Federated Services and Applications

- S2S federation is a good start toward building a real-time communications cloud.
- Clouds typically consist of all the users, devices, services, and applications connected to the network.
- In order to fully leverage the capabilities of this cloud structure, a participant needs the ability to find other entities of interest.
- Such entities might be end users, multiuser chat rooms, real-time content feeds, user directories, data relays, messaging gateways, etc.

- Finding these entities is a process called discovery.
- XMPP uses service discovery (as defined in XEP-0030) to find the aforementioned entities.
- The discovery protocol enables any network participant to query another entity regarding its identity, capabilities and associated entities.
- When a participant connects to the network, it queries the authoritative server for its particular domain about the entities associated with that authoritative server.

- In response to a service discovery query, the authoritative server informs the inquirer about services hosted there and may also detail services that are available but hosted elsewhere.
- XMPP includes a method for maintaining personal lists of other entities, known as roster technology, which enables end users to keep track of various types of entities.
- Usually, these lists are comprised of other entities the users are interested in or interact with regularly.
- Most XMPP deployments include custom directories so that internal users of those services can easily find what they are looking for.

5.9 Future Of Federation

- The implementation of federated communications is a precursor to building a seamless cloud that can interact with people, devices, information feeds, documents, application interfaces and other entities.
- The power of a federated, presence enabled communications infrastructure is that it enables software developers and service providers to build and deploy such applications without asking permission from a large, centralized communications operator.

- The process of server-to-server federation for the purpose of inter domain communication has played a large role in the success of XMPP, which relies on a small set of simple but powerful mechanisms for domain checking and security to generate verified, encrypted, and trusted connections between any two deployed servers.
- These mechanisms have provided a stable, secure foundation for growth of the XMPP network and similar real time technologies