UNIT –V

1. CLOUD COMPUTING SECURITY CHALLENGES

In traditional data centers, IT managers put procedures and controls in place to build a hardened perimeter around the infrastructure and data they want to secure. This configuration is relatively easy to manage, since organizations have control of their servers' location and utilize the physical hardware entirely for themselves. In the private and public cloud, however, perimeter boundaries blur and control over security diminishes as applications move dynamically and organizations share the same remotely located physical hardware with strangers.

MULTI-TENANCY

Cloud computing users share physical resources with others through common software virtualization layers. These shared environments introduce unique risks into a user's resource stack. For example, the cloud consumer is completely unaware of a neighbor's identity, security profile or intentions. The virtual machine running next to the consumer's environment could be malicious, looking to attack the other hypervisor tenants or sniff communications moving throughout the system. Because the cloud consumer's data sits on common storage hardware, it could become compromised through lax access management or malicious attack. In a joint paper published in November 2009 by MIT and UCSD entitled "Hey, You, Get Off of My Cloud: Exploring Information Leakage in Third-Party Compute Clouds," the authors exhibited the possibility of a side-channel attack in a cloud environment in which an attacker would be able to implant some arbitrary code into a neighbor's VM environment with little to no chance of detection. In another scenario, a security bulletin from Amazon Web Services reported that the Zeus Botnet was able to install and successfully run a command and control infrastructure in the cloud environment.

DATA MOBILITY AND CONTROL

Moving data from static physical servers onto virtual volumes makes it remarkably mobile, and data stored in the cloud can live anywhere in the virtual world. Storage administrators can easily reassign or replicate users' information across data centers to facilitate server maintenance, HA/DR or capacity planning, with little or no service interruption or notice to data owners. This creates a number of legal complications for cloud users. Legislation like the EU Privacy Act forbids data processing or storage of residents' data within foreign data

centers. Careful controls must be applied to data in cloud computing environments to ensure cloud providers do not inadvertently break these rules by migrating geographically sensitive information across political boundaries. Further, legislation such as the US Patriot Act allows federal agencies to present vendors with subpoenas and seize data (which can include trade secrets and sensitive electronic conversations) without informing or gaining data owners' consent.

DATA REMANENCE

Although the recycling of storage resources is common practice in the cloud, no clear standard exists on how cloud service providers should recycle memory or disk space. In many cases, vacated hardware is simply re-purposed with little regard to secure hardware repurposing. The risk of a cloud tenant being able to gather pieces of the previous tenants' data is high when resources are not securely recycled. Resolving the issue of data remanence can frequently consume considerable negotiating time while establishing service agreements between an enterprise and a cloud service provider.

DATA PRIVACY

The public nature of cloud computing poses significant implications to data privacy and confidentiality. Cloud data is often stored in plain text, and few companies have an absolute understanding of the sensitivity levels their data stores hold. Data breaches are embarrassing and costly. In fact, a recent report by the Cloud Security Alliance lists data loss and leakage as one of top security concerns in the cloud. Recent laws, regulations and compliance frameworks compound the risks; offending companies can be held responsible for the loss of sensitive data and may face heavy fines over data breaches. Business impacts aside, loose data security practices also harm on a personal level. Lost or stolen medical records, credit card numbers or bank information may cause emotional and financial ruin, the repercussions of which could take years to repair. Sensitive data stored within cloud environments must be safeguarded to protect its owners and subjects alike.

Parameters for cloud security

There are numerous security issues for cloud computing as it encompasses many technologies including networks, databases, operating systems, virtualization, resource scheduling, transaction management, load balancing, concurrency control and memory management Security issues for many of these systems and technologies are applicable to cloud

computing. For example, the network that interconnects the systems in a cloud has to be secure. Furthermore, virtualization paradigm in cloud computing results in several security concerns. For example, mapping the virtual machines to the physical machines has to be carried out securely. Data security involves encrypting the data as well as ensuring that appropriate policies are enforced for data sharing. In addition, resource allocation and memory management algorithms have to be secure. Finally, data mining techniques may be applicable to malware detection in clouds.

Security Issues faced by Cloud computing

Whenever a discussion about cloud security is taken place there will be very much to do for it. The cloud service provider for cloud makes sure that the customer does not face any problem such as loss of data or data theft. There is also a possibility where a malicious user can penetrate the cloud by impersonating a legitimate user, there by infecting the entire cloud. This leads to affects many customers who are sharing the infected cloud [7]. There are four types of issues raise while discussing security of a cloud.

1. Data Issues

2. Privacy issues

3. Infected Application

4. Security issues

Data Issues: sensitive data in a cloud computing environment emerge as major issues with regard to security in a cloud based system. Firstly, whenever a data is on a cloud, anyone from anywhere anytime can access data from the cloud since data may be common, private and sensitive data in a cloud. So at the same time, many cloud computing service consumer and provider accesses and modify data. Thus there is a need of some data integrity method in cloud computing. Secondly, data stealing is a one of serious issue in a cloud computing environment. Many cloud service provider do not provide their own server instead they acquire server from other service providers due to it is cost affective and flexible for operation and cloud provider. So there is a much probability of data can be stolen from the external server. Thirdly, Data loss is a common problem in cloud computing. If the cloud computing service provider shut down his services due some financial or legal problem then there will be a loss of data for the user. Moreover, data can be lost or damage or corrupted

due to miss happening, natural disaster, and fire. Due to above condition, data may not be accessesable to users. Fourthly, data location is one of the issues what requires focus in a cloud computing environment. Physical location of data storage is very important and crucial. It should be transparent to user and customer. Vendor does not reveal where all the data's are stored.

Secrecy Issues:

The cloud computing service provider must make sure that the customer personal information is well secured from other providers, customer and user. As most of the servers are external, the cloud service provider should make sure who is accessing the data and who is maintaining the server so that it enable the provider to protect the customer's personal information.

Infected Application:

cloud computing service provider should have the complete access to the server with all rights for the purpose of monitoring and maintenance of server. So this will prevent any malicious user from uploading any infected application onto the cloud which will severely affect the customer and cloud computing service.

Security issues:

cloud computing security must be done on two levels. One is on provider level and another is on user level. Cloud computing service provider should make sure that the server is well secured from all the external threats it may come across. Even though the cloud computing service provider has provided a good security layer for the customer and user, the user should make sure that there should not be any loss of data or stealing or tampering of data for other users who are using the same cloud due to its action. A cloud is good only when there is a good security provided by the service provider to the user.

2. SOFTWARE AS A SERVICE SECURITY

Cloud computing is becoming increasingly popular in distributed computing environment. Data storage and processing using cloud environments is becoming a trend worldwide. Software as a Service (SaaS)one of major models of cloud which may be offered in a public,

private or hybrid network. If we look at the impact SaaS has on numerous business applications as well as in our day to day life, we can easily say that this disruptive technology is here to stay. Cloud computing can be seen as Internet-based computing, in which software, shared resources, and information are made available to devices on demand. But using a cloud computing paradigm can have positive as well as negative effects on the security of service consumer's data. Many of the important features that make cloud computing very attractive, have not just challenged the existing security system, but have also exposed new security risks

In Software as a Service (SaaS) model, the client needs to be dependent on the service provider for proper security measures of the system. The service provider must ensure that their multiple users don't get to see each other's private data. So, it becomes important to the user to ensure that right security measures are in place and also difficult to get an assurance that the application will be available when needed [15]. Cloud computing providers need to provide some solution to solve the common security challenges that traditional communication systems face. At the same time, they also have to deal with other issues inherently introduced by the cloud computing paradigm itself.

A. Authentication and authorization

The authorization and authentication applications used in enterprise environments need to be changed, so that they can work with a safe cloud environment. Forensics tasks will become much more difficult since it will be very hard or maybe not possible for investigators may to access the system hardware physically

B. Data confidentiality Confidentiality may refer to the prevention of unintentional or intentional unauthorized disclosure or distribution of secured private information. Confidentiality is closely related to the areas of encryption, intellectual property rights, traffic analysis, covert channels, and inference in cloud system. Whenever a business, an individual, a government agency, or any other entity wants to shares information over cloud, confidentiality or privacy is a questions nay need to be asked

C. Availability The availability ensures the reliable and timely access to cloud data or cloud computing resources by the appropriate personnel. The availability is one of the big concerns of cloud service providers, since if the cloud service is disrupted or compromised in any way; it affects large no. of customers than in the traditional model.

D. Information Security

In the SaaS model, the data of enterprise is stored outside of the enterprise boundary, which is at the SaaS vendor premises. Consequently, these SaaS vendor needs to adopt additional security features to ensure data security and prevent breaches due to security vulnerabilities in the application or by malicious employees. This will need the use of very strong encryption techniques for data security and highly competent authorization to control access private data.
.

E. Data Access

Data access issue is mainly related to security policies provided to the users while accessing the data. Organizations have their own security policies based on which each employee can have access to a particular set of data. These security policies must be adhered by the cloud to avoid intrusion of data by unauthorized users. The SaaS model must be flexible enough to incorporate the specific policies put forward by the organization.

F. Network Security

In a SaaS deployment model, highly sensitive information is obtained from the various enterprises, then processed by the SaaS application and stored at the SaaS vendor‘s premises. All data flow over the network has to be secured in order to prevent leakage of sensitive information.

G. Data breaches

Since data from various users and business organizations lie together in a cloud environment, breaching into this environment will potentially make the data of all the users vulnerable. Thus, the cloud becomes a high potential target.

H. Identity management and sign-on process

Identity management (IdM) or ID management is an area that deals with identifying individuals in a system and controlling the access to the resources in that system by placing restrictions on the established identities. Aria of IdM is considered as one of the biggest challenges in information security. When a SaaS provider want to know how to control who has access to what systems within the enterprise it becomes a lot more challenging task..

3.OPEN CLOUD CONSORTIUM

The Open Cloud Consortium (OCC)

- Supports the development of standards for cloud computing and frameworks for interoperating between clouds;
- develops benchmarks for cloud computing; and
- supports reference implementations for cloud computing, preferably open source reference implementations.

The OCC has a particular focus in large data clouds. It has developed the MalStone Benchmark for large data clouds and is working on a reference model for large data clouds.

The Open Cloud Consortium (OCC) is a member driven organization that supports the development of standards for cloud computing and frameworks for interoperating between clouds; develops benchmarks for cloud computing; supports reference implementations for cloud computing, preferably open source reference implementations; manages a testbed for Cloud Computing called the Open Cloud Testbed (OCT); and sponsors workshops and other events related to Cloud Computing. The OCC has a particular focus in large data clouds. It has developed the MalStone Benchmark for large data clouds and is working on a reference model for large data clouds.

The Open Cloud Consortium is organized into different working groups.

Some of the Research project of OCC are

Cloud Standards Coordination Overview and Contributing Organizations

Cloud-standards.org is a Wiki site for Cloud Standards Coordination. The goal of the wiki is to document the activities of the various SDOs working on Cloud Standards. Cloud-standards.org is an initiative for editing and sharing a general cloud computing standardization positioning, in which more relevant cloud standardization initiatives can be seen and related. The first informal proposal of the positioning can be seen at cloud standards positioning.

Open Cloud Testbed (OCT)

This working group manages and operates the Open Cloud Testbed. The Open Cloud Testbed uses the Cisco C-Wave and UIC Teraflow Network for its network connections. Both use

wavelengths provided by the National Lambda Rail. Currently membership in this working group is limited to OCC members who can contribute computing, networking, or other resources to the Open Cloud Testbed.

Project Matsu

Project Matsu is a collaboration with NASA. The goal is to create a cloud containing all of Earth Observing 1 (EO-1) satellite imagery from the Advanced Lander Imager (ALI) and the Hyperion instruments and to make this data available to interested users. This working group is also developing cloud-based services that can assist at times of disasters. The Project Matsu cloud can, for example, be used to assist with image processing so that up to date images can be made available to those providing disaster assistance.

The Open Science Data Cloud (OSDC) Working Group

The Open Science Data Cloud (OSDC) is cloud-based infrastructure that allows scientists to manage, analyze, integrate and share medium to large size scientific datasets. The Institute for Genomic and Systems Biology at the University of Chicago uses the OSDC as the basis for Bionimbus, a cloud for genomics and related data. John Hopkins University uses the OSDC to provide bulk downloads of the Sloan Digital Sky Survey to astronomers around the world. NASA uses the OSDC to make data from the EO-1 satellite available to interested parties. Partial funding for the OSCD is provided by the Gordon and Betty Moore Foundation and the National Science Foundation. OSDC Partners include Yahoo, who contributed equipment to the OSDC and Cisco who is providing access to the Cisco C-Wave.

4.DISTRIBUTED MANAGEMENT TASK FORCE

Distributed Management Task Force (DMTF) standards enable effective management of IT environments. The organization is composed of companies that collaborate on the development, validation and promotion of infrastructure management standards. DMTF management standards are critical to enabling interoperability among multi-vendor systems, tools and solutions within the enterprise.

The DMTF is an industry standards organization working to simplify the manageability of network-accessible technologies through open and collaborative efforts by leading technology companies. DMTF creates and drives the international adoption of interoperable

management standards, supporting implementations that enable the management of diverse traditional and emerging technologies including cloud, virtualization, network and infrastructure.

DMTF spans the globe with member companies and organizations representing varied industry sectors. The DMTF board of directors is led by 14 industry-leading technology companies including: Broadcom Limited, CA Technologies, Dell, Emerson Network Power, Hewlett Packard Enterprise, Hitachi, Ltd., HP Inc., Intel Corporation, Lenovo, Microsoft Corporation, NetApp, Software AG,TIM and VMware.

Supporting implementations that enable the management of diverse traditional and emerging technologies – including cloud, virtualization, network and infrastructure – the DMTF works to simplify the manageability of network-accessible technologies through open and collaborative efforts by leading technology companies.

DMTF standards include:

- *Cloud Infrastructure Management Interface* (*CIMI*) – a self-service interface for infrastructure clouds, allowing users to dynamically provision, configure and administer their cloud usage with a high-level interface that greatly simplifies cloud systems management. The specification standardizes interactions between cloud environments to achieve interoperable cloud infrastructure management between service providers and their consumers and developers, enabling users to manage their cloud infrastructure use easily and without complexity.
- *Common Information Model* (*CIM*) – the CIM schema is a conceptual schema that defines how the managed elements in an IT environment (for instance computers orstorage area networks) are represented as a common set of objects and relationships between them. CIM is extensible in order to allow product specific extensions to the common definition of these managed elements. CIM uses a model based upon UML to define the CIM Schema. CIM is the basis for most of the other DMTF standards.
- *Common Diagnostic Model* (*CDM*) – the CDM schema is a part of the CIM schema that defines how system diagnostics should be incorporated into the management infrastructure.
- *Web-Based Enterprise Management* (*WBEM*) – defines protocols for the interaction between systems management infrastructure components implementing CIM, a concept

of DMTF management profiles, that allows defining the behavior of the elements defined in the CIM schema, the CIM Query Language (CQL) and other specifications needed for the interoperability of CIM infrastructure.

- *Systems Management Architecture for Server Hardware* (*SMASH*) – a DMTF Management Initiative that include management profiles for server hardware management. SMASH 2.0 allows for either WS-Management or SM-CLP (a command line protocol for interacting with CIM infrastructure). SM-CLP was adopted as an International Standard in August 2011 by the Joint Technical Committee 1 (JTC 1) of the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC).
- *System Management BIOS* (*SMBIOS*) – defines how the BIOS interface of x86 architecture systems is represented in CIM (and DMI).
- *Alert Standard Format* (*ASF*) – defines remote control and alerting interfaces for OS-absent environments (for instance a system board controller of a PC).
- *Desktop Management Interface* (*DMI*) – the first desktop management standard. Due to the rapid advancement of DMTF technologies, such as CIM, the DMTF defined an "end of life" process for DMI, which ended March 31, 2005.
- *Redfish* – DMTF's Redfish API is an open industry standard specification and schema designed to meet the expectations of end users for simple, modern and secure management of scalable platform hardware. Created by the Scalable Platforms Management Forum (SPMF), Redfish specifies a RESTful interface and utilizes JSON and OData to help customers integrate solutions within their existing tool chains.
- *Web Services Management* (*WS-MAN*) – The DMTF's Web Services Management (WS-Man) provides interoperability between management applications and managed resources, and identifies a core set of web service specifications and usage requirements that expose a common set of operations central to all systems management.A SOAP-based protocol for managing computer systems (e.g., personal computers, workstations, servers, smart devices), WS-Man supports web services and helps constellations of computer systems and network-based services collaborate seamlessly.
- *Desktop and mobile Architecture for System Hardware* (*DASH*) – a management standard based on DMTF Web Services for Management (WS-Management), for desktop and mobile client systems. WS-Management was adopted as an international standard by ISO/IEC in 2013.[3]

- *Configuration Management Database Federation* (*CMDBf*) – facilitates the sharing of information between configuration management databases (CMDBs) and other management data repositories (MDRs). The CMDBf standard enables organizations to federate and access information from complex, multi-vendor infrastructures, simplifying the process of managing related configuration data stored in multiple CMDBs and MDRs.
- *The Cloud Auditing Data Federation* (*CADF*) – The Cloud Auditing Data Federation (CADF) standard defines a full event model anyone can use to fill in the essential data needed to certify, self-manage and self-audit application security in cloud environments. CADF is an open standard that addresses this need by enabling cross-vendor information sharing via its data format and interface definitions.
- *Platform Management Components Intercommunication* (*PMCI*) – a suite of specifications defining a common architecture for intercommunication among management subsystem components. This suite includes MCTP, PLDM and NC-SI specifications. The Platform Management standard was adopted as a national standard by ANSI in 2013.
- *Virtualization Management Initiative* (*VMAN*) – a suite of specifications based on DMTF's CIM that helps IT managers: Deploy virtual computer systems, Discover/inventory virtual computer systems, Manage lifecycle of virtual computer systems, Create/modify/delete virtual resources and Monitor virtual systems for health and performance. VMAN was adopted as a National Standard by the American National Standards Institute (ANSI) International Committee for Information Technology Standards (INCITS) in June 2012.
- The Network Management Initiative (NETMAN) – addresses today's complex data center and network environments. The initiative will lead the industry toward the unification of network management across traditional, cloud and software defined data center (SDDC) environments with the development of integrated standards to address physical, virtual, application-centric and software defined networks. While cloud, virtualization and software defined networking have eased the use of network functions for consumers, the challenges of deploying and managing the network supporting these infrastructures have magnified. Addressing the current complexity and abstraction, DMTF's NETMAN will provide the necessary standards-based management models and

interfaces to enable consistent, unified and automated provisioning, deployment, configuration, and monitoring of network environments.

5. STANDARDS FOR APPLICATION DEVELOPER

The reasons to adopt standards in cloud computing closely match the same logic that made the universal usability of the Internet a reality: The more accessible data is, the more interoperable software and platforms are, the more standardized the operating protocols are, the easier it will be to use and the more people with use it -- and the cheaper it will be to implement, operate, and maintain. Systems and software designers see this logic in action when they create a cloud platform and don't have to worry about figuring out how to make it work with a dozen or so network protocols. Cloud application developers feel the power of standards when they build an application using a framework that guarantees almost 100 percent success in such areas as data access, resource allocation, debugging, failover mechanisms, user interface reconfiguration, and error, data, and exception handling... not to mention the shouts of joy when a developer realizes that a favored toolkit can integrate into a favored development platform, sometimes with only the push of a button.

Cloud standards that designers and developers can use in 2015 to help make software design simpler, cheaper, and faster.

Cloud Standards Customer Council (CSCC)

CSCC is an end-user advocacy group that seeks to "accelerate cloud's successful adoption" as a means to strengthen 21st century enterprises. It is not really a standards organization but a facilitator; it works with existing standards groups to ensure that client requirements are addressed as standards evolve. This group understands that the transition from a traditional IT environment to a cloud-based environment can require significant changes, so it attempts to guarantee that this transition won't cost end-users the choice and flexibility they enjoy with their current IT environments. Another role of the CSCC is to advocate for the establishment of open, transparent standards for cloud computing; the council believes that the agility and economic efficiencies cloud offers are only possible if the performance, security, and interoperability issues that arise during the transition to the cloud are answered in an open, transparent way.

Distributed Management Task Force (DMTF)

DMTF is an association of industry IT companies and professionals collaborating on and promoting enterprise systems management and interoperability standards with a goal of providing "common management infrastructure components for instrumentation, control, and communication in a platform-independent and technology-neutral way." The DMTF sports several areas of focus.

Open Virtualization Format (OVF)

The OVF standard, adopted as ISO 17203 by the International Organization for Standardization (ISO), creates uniform formatting for virtual systems-based software. OVF is platform independent, flexible, and open, and can be used by anyone who needs a standardized package for creating a virtual software solution that requires interoperability and portability. OVF simplifies management standards using the Common Information Model (CIM) to standardize management information formats; this reduces design and development overhead by allowing for quicker and more costeffective implementation of new software solutions.

Open Cloud Standards Incubator working group

The Open Cloud Standards Incubator working group's goal is to facilitate management interoperability between in-enterprise private clouds and public and hybrid clouds. The components — cloud resource management protocols, packaging formats, and security mechanisms—address the increasing need for open, consistent cloud management architecture standards.

Cloud Management Working Group (CMWG)

CMWG uses the Cloud Infrastructure Management Interface (CIMI) to visually represent the total lifecycle of a cloud service so that you can enhance the implementation and management of that service and make sure it is meeting service requirements. This group can explain how to model the characteristics of an operation, allowing variation of your implementation to be tested prior to final development; it does this with CIM, which creates data classes with well-defined associations and characteristics, as well as a conceptual framework for organizing these components. CIM uses discrete layers: core model, common model, and extension representations.

Cloud Auditing Data Federation Working Group (CADF)

CADF works to standardize "audit events across all cloud and service providers" with the goal of resolving significant issues in cloud computing due to inconsistencies or incompatibilities. It seeks to ensure consumers of cloud computing systems that the security policies required on their applications are properly managed and enforced.

European Telecommunications Standards Institute (ETSI)

ETSI is an organization that produces internationally-applicable standards in information and communications technology to improve systems interoperability, efficiencies, and economies through shared knowledge and expertise.

ETSI Technical Committee Cloud

ETSI Technical Committee Cloud examines issues arising from the convergence of IT and telecommunications. With cloud computing requiring connectivity to extend beyond the local network, cloud network scalability has become dependent on the ability of the telecom industry to handle rapid increases in data transfer; it also works on issues related to interoperability and security

Cloud Standards Coordination (CSC)

The CSC initiative is responsible for developing a detailed set of standards required to support European Commission policy objectives that address security, interoperability, data portability, and reversibility.

Global Inter-Cloud Technology Forum (GICTF)

GICTF is an organization promoting the standardization of network protocols and interfaces in an effort to create a more reliable cloud services network that solves the problems of security, data quality, system responsiveness, and reliability.

International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC)

ISO is a well-known, 70-year old, independent, non-governmental membership organization made up of 163 member countries. It is the world's largest developer of voluntary international technology standards. The IEC is more than 100 years old and is the leading

force behind international standards for all technologies involving the electrical, electronic, and related fields.

6.STANDARDS FOR SECURITY

3.1 INTRODUCTION

The standards assure that users can work well with the vendors. Small organizations show great interest in open standards for Cloud computing since it provides numerous opportunities for them. Large Cloud providers, like Google and Amazon might show little interest to develop open standards for fear of losing their lock on many of their existing customers.

Cloud standards come in three aspects, which are standards for security that help in providing a secured environment for the most important information in the Cloud, standards for end-users/ application developers which enables them to understand the new code very quickly and easily, and standards for messaging which prescribes the format for defining and sending messages.

3.1.1 Standards for Security

The main purpose of security standards is to ensure a secure environment which provides security and privacy of secret information in Cloud. The following are protocols which are not exclusively specific for Cloud security and needed merit coverage too.

Security Assertion Mark-up Language

Security Assertion Mark-up Language (SAML) is basically built on a number of already existing standards like HTTP, SOAP and XML. SAML depends on HTTP as its communication protocol. Most of the SAML transactions are defined in XML standard form.

```
<saml:Assertion A...>
<Authentication>
...
</Authentication>
<Attribute>
...
</Attribute>
<Authorization>
...
</Authorization>
</saml:Assertion A>
```

SAML mainly specifies three components, namely, protocol, assertions and binding. A SAML protocol can be considered as a simple request-response protocol. SAML works with several protocols, like File Transfer Protocol (FTP), Simple Mail Transfer Protocol (SMTP), Hypertext Transfer Protocol (HTTP), and also supports Electronic Business XML (ebXML), BizTalk and SOAP. Assertions are statements which are referred by the service providers to make access control decisions. SAML Assertions are transferred from identity providers to service providers. There exist three types of assertions, namely authentication assertion, attribute assertion and authorization assertion. Authentication assertion is for validating the identity of the user; Attribute assertion consists of specific information regarding the user; and Authorization assertion mainly identifies what a particular user is authorized to do. A SAML binding defines how SAML requests and responses are mapped to standard messaging protocols. The main concept of SAML is that it helps in passing security information between secure web domains through assertions. SAML protocol describes only what is transmitted. It is that the binding defines how the information is transmitted.

Open Authentication (OAuth)

OAuth is an open authentication protocol, which allows applications to obtain user's data in a protected way. It's a simple open standard for secure API authentication. OAuth is a way for publishing and interacting with secured data. This offers a mechanism for users to permit access to private data while protecting private credentials. The main advantage for users in this is that they are completely in control of what the applications can do or what cannot do and also they need not share their passwords with any third party applications like Facebook or Twitter. It is necessary to understand that privacy and security are not guaranteed by this protocol. OAuth itself offers no privacy at all, but are based on other protocols, like SSL to implement that. OAuth is token-based Authentication, that is, the logged-in user has a unique token which is used to access data from the site.

OAuth offers the following major improvements when compared to traditional models like basic auth:

1. OAuth includes working with abstract access tokens which do not share any of the users' passwords.
2. Users can observe the tokens which are active, which means that applications are able to access their data on the provider site.
3. The tokens that are issued from a provider site can be revoked at any given time giving more control to the user.

OpenID

An OpenID provides the user the flexibility to use an already existing identity to login to several websites, without creating new passwords. In this way, users are able to control the amount of information that they want to share with the websites they have visited. With OpenID, the password and account registration will be given only to the identity provider and the task of validating the identity to the participating websites will be taken care of by the provider. Users can create accounts with their choice of OpenID identity providers and will be able to use those created accounts as the basis for logging on to any website that accepts OpenID authentication. It is a Single-Sign-On (SSO) procedure of access control. With this, the users can login once and gain access to resources across various participating systems. OpenID is decentralized. Only standard HTTP requests and responses are used by OpenID authentication. The only thing that is needed is that the user should have an authenticated account at any OpenID provider like Google, my OpenID or LiveJournal.

After the verification of the OpenID identifier, OpenID authentication is confirmed successful, and the user is considered to login into any relying party website. OpenID will not provide its own authentication methods; in fact if an identity provider uses strong authentication, it may be used for secured transactions.

The OpenID works as follows: A user visits a website which displays an OpenID login form that contains only one field for the OpenID identifier. The user has to type the previously registered 'OpenID identifier'.

Secure Sockets Layer/Transport Layer Security

Both Secure Sockets Layer (SSL) and Transport Layer Security (TLS) are cryptographically secure protocols which are designed to provide data integrity and security for communications over TCP/IP (Transmission Control Protocol/Internet Protocol). Transport Layer Security is the successor to SSL. The TLS offers end point authentication and data confidentiality with the help of cryptography. Whenever client and server applications communicate across a network, TLS protocol gives assurance that no other third party may tamper or eavesdrop with any message. The TLS is application protocol independent. The difference between TLS and SSL is that TLS uses the Hashing for Message Authentication Code (HMAC) algorithm over SSL Message Authentication Code (MAC) algorithm.

The TLS protocol mainly includes two layers:

1. TLS Record Protocol: This protocol offers connection security with the help of symmetric data encryption and assures that the connection is reliable.
2. TLS Handshake Protocol: It provides both the server and client to authenticate each other and negotiate regarding encryption algorithm and cryptographic keys before the selected application protocol starts transmitting or receiving any data.

The TLS is performed in the following phases:

1. The client and server negotiate on an appropriate algorithm;
2. A key is exchanged using public-key encryption and authentication based on certification; and
3. A symmetric cipher is used during data exchange.

7. STANDARDS FOR MESSAGING

❖ **Simple Message Transfer Protocol (SMTP)**

- SMTP is usually used for:
    - Sending a message from a workstation to a mail server.
    - Or communications between mail servers.
- Client must have a constant connection to the host to receive SMTP messages.

❖ **Post Office Protocol (POP)**

- Purpose is to download messages from a server.
- This allows a server to store messages until a client connects and requests them.
- Once the client connects, POP servers begin to download the messages and subsequently delete them from the server

- **Internet Messaging Access Protocol (IMAP)**
  - IMAP allows messages to be kept on the server.
  - But viewed as though they were stored locally.
- **Syndication (Atom & Atom Publishing Protocol, and RSS)**

  RSS
  - The acronym “Really Simple Syndication” or “Rich Site Summary”.
  - Used to publish frequently updated works—such as news headlines
  - RSS is a family of web feed formats

  Atom & Atom Publishing Protocol
  - The Atom format was developed as an alternative to RSS

- **Communications (HTTP, SIMPLE, and XMPP)**

HTTP

- The acronym “Hypertext Transfer Protocol.
  - HTTP is a request/response standard between a client and a server
  - For distributed, collaborative,hypermedia information systems.

XMPP(Extensible Messaging and Presence Protocol)

- Used for near-real-time, extensible instant messaging and prsence information.
- XMPP remains the core protocol of the Jabber Instant Messaging and Presence technology

SIMPLE

- Session Initiation Protocol for Instant Messaging and Presence Leveraging Extensions
- For registering for presence information and receiving notifications.
- It is also used for sending short messages and managing a session of realtime messages between two or more participants.

8. END USER ACCESS TO CLOUD COMPUTING

- **Cost Flexibility**
  - **Online Market place**
- **Scalability**
  - **Online Video retailer**
- **Adaptability**

- **Online Entertainment platform**

- **Hidden Complexity**
  - **Access to services having sophisticated technology**
- **Context-driven Variability**
  - **Intelligent Assistants**
- **Access to Information**
  - **Ecosystem**

Cost Flexibility – Online Market place

- Gains access to more powerful analytics online
- Concerned with economy due to "pay-as-you-go" cost structure
- Additionally cloud takes away the need to fund
  - Building of hardware
  - Installing software
  - Paying dedicated software license fees

Etsy – Online Market place

- **Online Market Place for handmade goods**
  - Environment for buyers and sellers together
  - Provides recommendations for buyers.
- **Cloud-based capabilities**
  - Company is able to analyze data from one billion monthly views of its Web site
  - Use the information to create product recommendations

Scalability

- Cloud enables businesses to add or provision computing resources just at the time they're needed

Scalability – Online Video retailer

- Netflix of cloud resources as it meets up and down demand for its Internet subscription service for movies and TV shows
- Netflix streams many movies and shows on demand even at peak times
- Migrate the website and streaming service from the traditional data center to the cloud environment

Adaptability

- Cloud applications adapt to diverse user groups with a diverse assortment of devices

Adaptability – Online Entertainment platform

- ActiveVideo, creator of CloudTV, a cloud-based platform that unifies all forms of content
  - Web, television, mobile, social, video-on-demand – onto any video screen, be it set-top boxes, PCs, or mobile devices
- CloudTV leverages content stored and processed in the network cloud
  - Significantly expand the availability of Web-based user experiences
  - Allow operators to quickly deploy a consistent user interface across diverse set-top boxes and connected devices

Hidden Complexity

- As complexity is masked from the end user, a company can expand its product and service sophistication
  - without increasing the level of user knowledge to utilize
- Upgrades and maintenance can be done in the "background" without the end user having to participate
- Xerox - Cloud Print solution, enables the desired content in printed form wherever they might be by using Xerox's cloud to access printers outside their own organization
  - Printing from the cloud requires quite a bit of data management – with numerous files to be stored, converted to print-ready format and distributed to printers - the
  - complexity is hidden from users

Access to Information – Ecosystem

- Ecosystem connectivity enables information exchange across business partners
- HealthHiway, an online health information network
  - Enables the exchange of health information and transactions among healthcare providers, employers, payers, practitioners, third-party administrators and patients in India
  - By connecting more than 1,100 hospitals and 10,000 doctors, the company's software-as-a-service solution facilitates better collaboration and information sharing, helping deliver improved care at a low cost, particularly important in growing markets

9. MOBILE INTERNET DEVICES AND THE CLOUD.

Advantages of MCC(Mobile Cloud Computing)

- Extending battery lifetime
  - Computation offloading migrates large computations and complex processing from resource-limited devices (i.e., mobile devices) to resourceful machines (i.e., servers in clouds).
  - Remote application execution can save energy significantly.
  - Many mobile applications take advantages from task migration and remote processing.
- Improving data storage capacity and processing power
  - MCC enables mobile users to store/access large data on the cloud.
  - MCC helps reduce the running cost for computation intensive applications.
  - Mobile applications are not constrained by storage capacity on the devices because their data now is stored on the cloud.
- Improving reliability and availability
  - Keeping data and application in the clouds reduces the chance of lost on the mobile devices.
  - MCC can be designed as a comprehensive data security model for both service providers and users:
    - Protect copyrighted digital contents in clouds.
    - Provide security services such as virus scanning, malicious code detection, authentication for mobile users.
  - With data and services in the clouds, then are always(almost) available even when the users are moving.
- Dynamic provisioning
  - Dynamic on-demand provisioning of resources on a fine-grained, self-service basis
  - No need for advanced reservation
- Scalability
  - Mobile applications can be performed and scaled to meet the unpredictable user demands
  - Service providers can easily add and expand a service

- Multi-tenancy
    - Service providers can share the resources and costs to support a variety of applications and large no. of users.
- Ease of Integration
    - Multiple services from different providers can be integrated easily through the cloud and the Internet to meet the users' demands.

MCC Applications

- Mobile Commerce
    - M-commerce allows business models for commerce using mobile devices
    - Examples: Mobile financial, mobile advertising, mobile shopping
    - M-commerce applications face various challenges (low bandwidth, high complexity of devices, security)
    - Integrated with cloud can help address these issues
    - Example: Combining 3G and cloud to increase data processing speed and security level.
- Mobile Learning
    - M-learning combines e-learning and mobility
    - Traditional m-learning has limitations on high cost of devices/network, low transmission rate, limited educational resources
    - Cloud-based m-learning can solve these limitations
    - Enhanced communication quality between students and teachers
    - Help learners access remote learning resources
    - A natural environment for collaborative learning
- Mobile Healthcare
    - M-healthcare is to minimize the limitations of traditional medical treatment (eg. Small storage, security/privacy, medical errors)
    - M-healthcare provides mobile users with convenient access to resources(eg. medical records)
    - M-healthcare offers hospitals and healthcare organizations a variety of on-demand services on clouds
    - Examples
        - Comprehensive health monitoring services
        - Intelligent emergency management system

        - Health-aware mobile devices (detect pulse-rate, blood pressure, level of alcohol etc)
        - Pervasive access to healthcare information
        - Pervasive lifestyle incentive management (to manage healthcare expenses)
- Mobile Gaming
    - M-game is a high potential market generating revenues for service providers.
    - Can completely offload game engine requiring large computing resource (e.g., graphic rendering) to the server in the cloud.
    - Offloading can also save energy and increase game playing time (eg. MAUI allows fine-grained energy-aware offloading of mobile codes to a cloud)
    - Rendering adaptation technique can dynamically adjust the game rendering parameters based on communication constraints and gamers' demands
- Assistive technologies
    - Pedestrian crossing guide for blind and visually-impaired
    - Mobile currency reader for blind and visually impaired
    - Lecture transcription for hearing impaired students
- Other applications
    - Sharing photos/videos
    - Keyword-based, voice-based, tag-based searching
    - Monitoring a house, smart home systems