UNIT -V

Cloud Security

Introduction: -

More, and more organizations are moving their applications and associated data to cloud to reduce costs and reduce the operational and. maintenance overheads, and one of the important considerations is that of security of the daita.in the cloud. Most cloud service providers implement advanced security features similar to those that exist in in-house IT environments.

However, due the out sourced nature .of' the cloud, resource pooling and multi-tenanted; architectures, security remains an important .concern in adoption of cloud computing. :In addition to the traditional vulnerabilities that exist for web app1icatons, the

cloud. applications have additional vulnerabilities because of the shared usage of resources and virtualized resources. Key Security challenges for. cloud applications include:

1)Authentication
2)Authorization
3)Security of Data at Rest
4)Security of Data at Motion
5)Data Integrity
6)Auditing

1)Authentication:-

Authentication refers to digitally confirming the identity of the entity requesting access to some protected information.

In a traditional in-house IT Environment authentication polices are under the control of the organization. However, in cloud computing environments, where applications and data are accessed over the internet, the complexity of digital authentication mechanisms increases rapidly.

2)Authorization:-

Authorization refers to digitally specifying the access rights to the protected resources using access policies. In a traditiona1 in-house IT environment, the access policies are controlled by the organization and can.be altered at their convenience.

An organization, for example, can provide different access policies for different departments.

Authorization in a cloud computing environment requires the use of the cloud service providers services for specifying the access policies.

3)Security of Data at Rest:-

Due to the multi-tenant environments used in the cloud, the application and database servers of different applications belonging to different organizations can be provisioned side-by-side increasing the complexity of securing the. data.

Appropriate separation mechanisms are required to ensure the isolation between applications and. data from different organizations.

4)Security of Data at Motion:-

In traditional in-house IT environments, all the data exchanged between the applications and users remains within the organization's control and geographical boundaries. Organizations

believe that they have complete visibility of all the data exchanged and control the IT infrastructure. With the adoption of tire cloud model, the applications and the data are moved out of the in-house IT infrastructure to the cloud provider. In such a scenario, organizations have to access their applications with the data moving in and out of the cloud over the internet. Therefore, appropriate security mechanisms are required to ensure the security of data in, and while in, motion.

5)Data Integrity: -

Data integrity ensures that the data is not altered in an unauthorized manner after it is created, transmitted or stored.

Due to the, outsourcing of data storage, in cloud computing environments, ensuring integrity of data is important. Appropriate mechanisms are required för detecting accidental and/or intentional changes in the data.

6)Auditing

Auditing is very important for applications deployed in cloud computing environments. In traditional in-house IT environments, organizations have complete visibility of their applications and accesses to the protected information.

For cloud applications appropriate auditing mechanisms are required to get visibility into the application, data accesses and actions performed by the app1ïcation users, including mobile users and devices such as. wireless laptops and smartphones.

CSA Cloud Security Architecture

Introduction: -

The Cloud Security Alliance (CSA) provides a Trusted Cloud Initiative (TCI) Reference Architecture which is. a methodology and a set of tools that enab1e cloud application developers and security architects to assess where their internal IT and their cloud providers are in terms of security capabilities, and to plan a roadmap to meet the security needs of their business.

The Security and Risk Management (SRM) domain within the TCI Reference Architecture provides the core components of an organization's information security program to safeguard assets and detect, assess, and monitor risks inherent in operating activities.

The sub-domains of SRM include:

1)Governance, Risk Management and Compliance:-

This sub-domain deals with the identification and implementation of the appropriate organizational structures, processes, and controls to maintain effective information security governance, risk management and compliance.

2)Information Security Management:-

This sub-domain deals with the implementation of appropriate measurements (such as capability maturity models, capability mapping models, security architectures roadmaps and risk portfolios) in order to minimize or eliminate the impact that security related threats and vulnerabilities might have on an organization.

3)Privilege Management Infrastructure:-

The objective of this sub-domain is to ensure that users have access and privileges required to execute their duties and responsibilities with Identity and Access Management (IAM)

functions such as identity management, authentication services, authorization services, and privilege usage management.

4)Threat and Vulnerability Management:-

This sub-domain deals with core security such. as vulnerability management, threat management, compliance testing, and penetration testing.

5)Infrastructure Protection Service:-

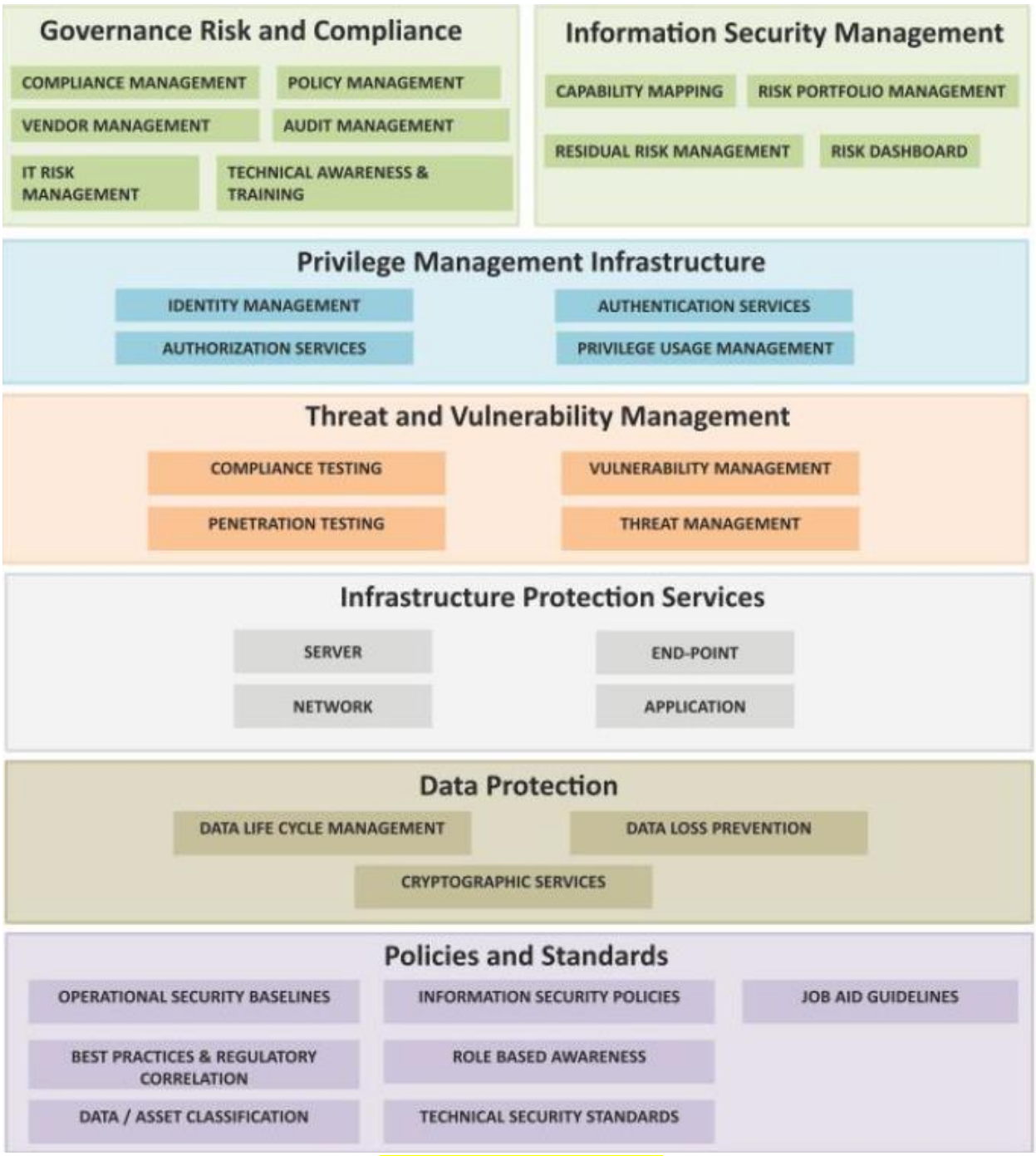
This objective of this sub-domain is to secure Server, End-Point, Network and Application layers.

6)Data Protection

This sub-domain deals with data lifecycle management, data leakage prevention, intellectual property protection with digital rights management, and cryptographic services such as key management and PKI/symmetric encryption.

7) Polices and Standards: - Security policies and standards are derived from risk-based business requirements and exist at a number of different levels including Information Security policy, Physical Security Policy, Business Continuity Policy, Infrastructure Security Po1icies,, Application Security Policies as well as the over-arching Business Operational Risk Management Policy.

Below Diagram shows the SRM domain within the TCI Reference Architecture of CSÄ.



Authenticaiton

Introduction: -

- Authentication refers to confirming the digital identity of the entity requesting access to some protected information.
- The process of authentication involves, but is not limited to, validating at least one factor of identification of the entity to be authenticated.

- A factor can be something the entity or the user knows (password or pin), something the user has (such as a smart card), or something that can uniquely identify the user (such as fingerprints).
- In multifactor authentication more than one of these factors are used for authentication.
- There are various mechanisms for authentication including:
  -SSO
  -OTP

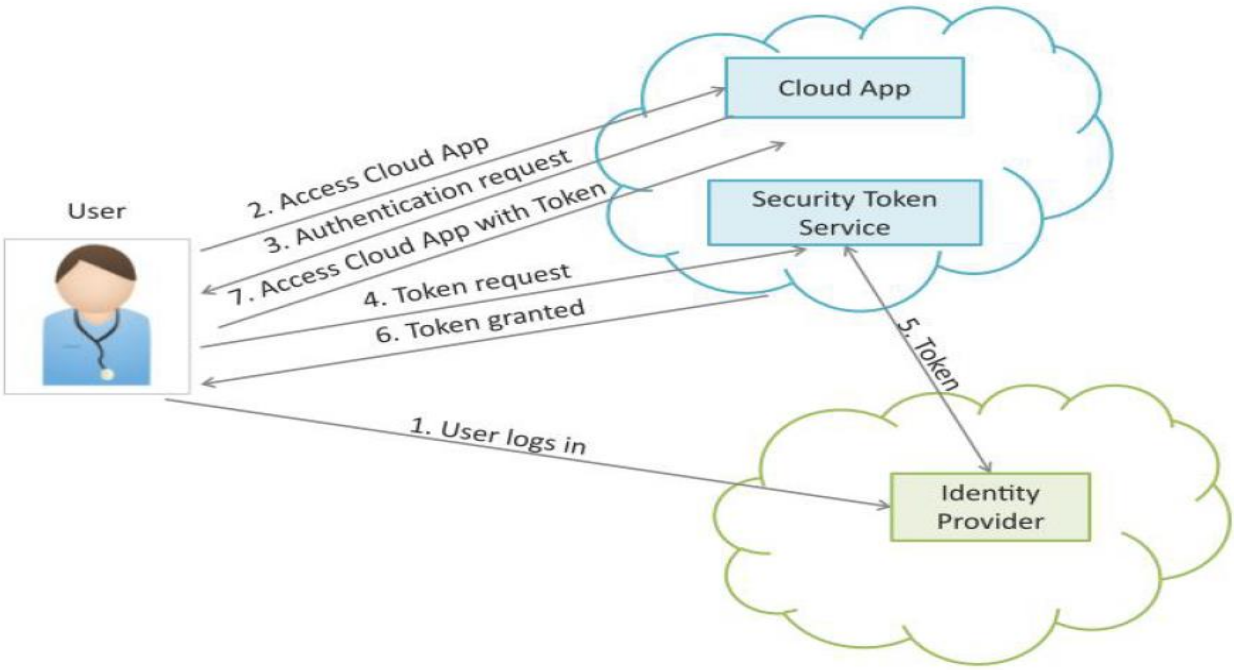
1)Single Sign On (SSO):-

- Single Sign-on (SSO) enables users to access multiple systems or applications after signing in only once, for the first time.
- When a user signs in, the user identity is recognized and there is no need to sign in again and again to access related systems or applications.
- Since different systems or applications may be internally using different authentication mechanisms, SSO upon receiving initial credential translates to different credentials for different systems or applications.
- The benefit of using SSO is that it reduces human error and saves time spent in authenticating with different systems or applications for the same identity.
- There are different implementation mechanisms:
  - SAML-Token
  - Kerberos

a) SAML Token: -

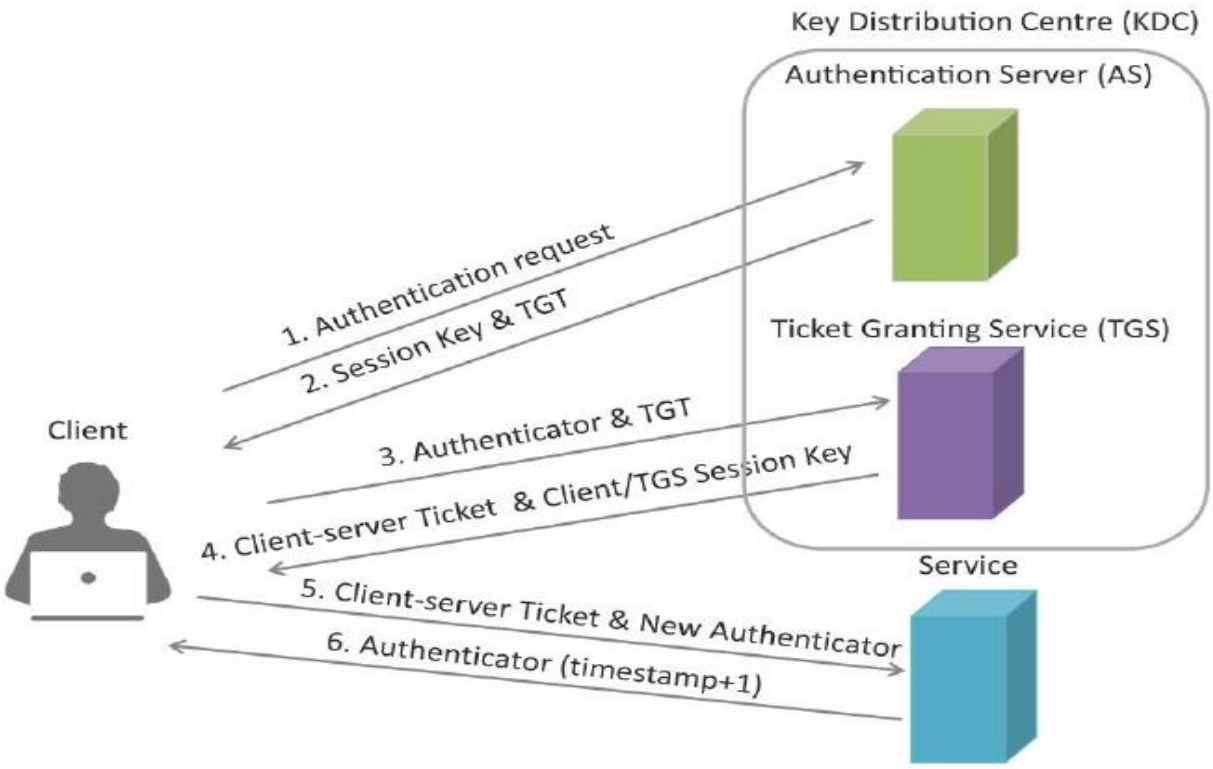
- Security Assertion Markup Language (SAML) is an XML-based open standard data format for exchanging security information (authentication and authorization data) between an identity provider and a service provider.
- SAML-token based SSO authentication
  - When a user tries to access the cloud application, a SAML request is generated and the user is redirected to the identity provider.
  - The identity provider parses the SAML request and authenticates the user. A SAML token is returned to the user, who then accesses the cloud application with the token.
  - SAML prevents man-in-the-middle and replay attacks by requiring the use of SSL encryption when transmitting assertions and messages.
  - SAML also provides a digital signature mechanism that enables the assertion to have a validity time range to prevent replay attacks.

The below diagram shows the Authentication flow for a Cloud Application using SAML SSO



b) Kerberos: -

- Kerberos is an open authentication protocol that was developed At MIT.
- Kerberos uses tickets for authenticating client to a service that communicate over an un-secure network.
- Kerberos provides mutual authentication, i.e. both the client and the server authenticate with each other.
- Below diagram shown Kerberos Authentication Flow:



2)One Time Password (OTP) :-

- One time password is another authentication mechanism that uses passwords which are valid for single use only for a single transaction or session.
- Authentication mechanism based on OTP tokens are more secure because they are not vulnerable to replay attacks.
- Text messaging (SMS) is the most common delivery mode for OTP tokens.
- The most common approach for generating OTP tokens is time synchronization.
- Time-based OTP algorithm (TOTP) is a popular time synchronization based algorithm for generating OTPs.

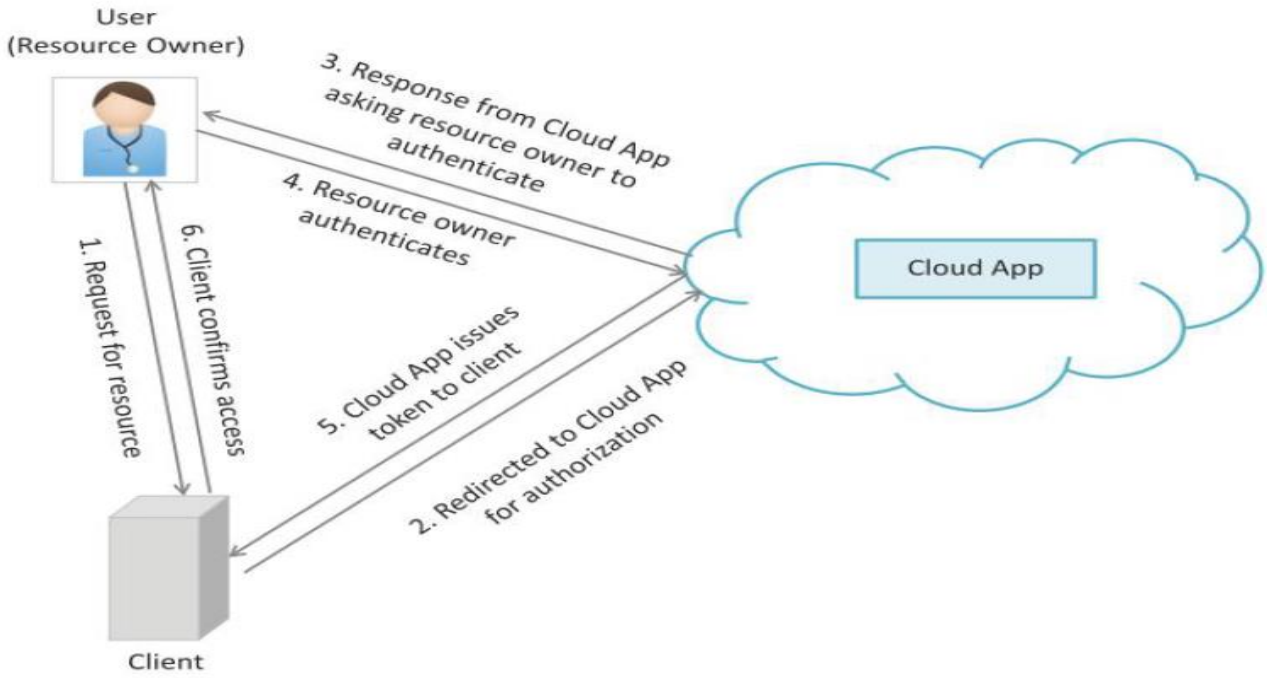
Authorization

Introduction: -

- Authorization refers to specifying the access rights to the protected resources using access policies.
- OAuth:
    - OAuth is an open standard for authorization that allows resource owners to share their private resources stored on one site with another site without handing out the credentials.
    - In the OAuth model, an application (which is not the resource owner) requests access to resources controlled by the resource owner (but hosted by the server).
    - The resource owner grants permission to access the resources in the form of a

token and matching shared-secret.

- Tokens make it unnecessary for the resource owner to share its credentials with the application.
- Tokens can be issued with a restricted scope and limited lifetime, and revoked independently.

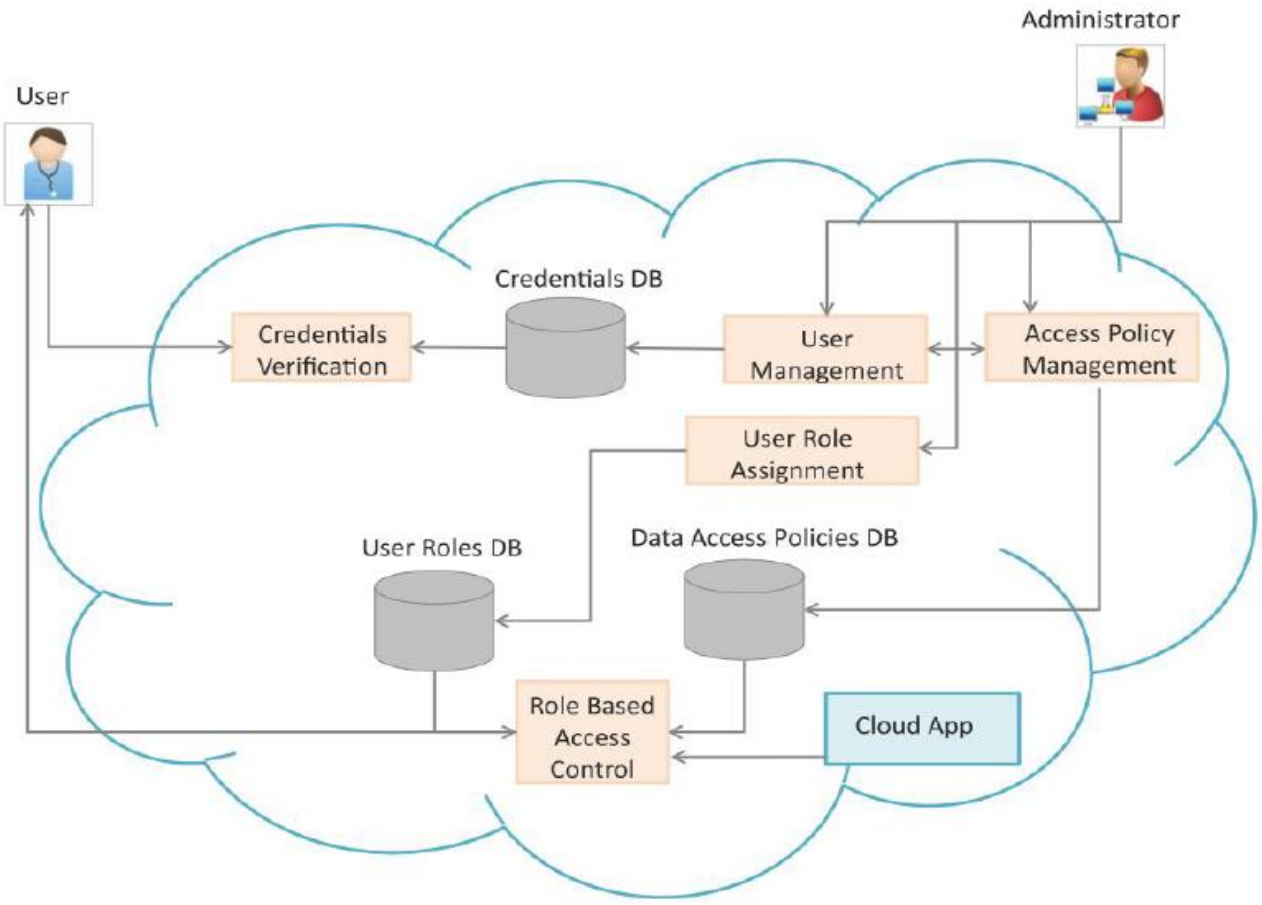


Identity and Access Management

Introduction: -

- Identity management provides consistent methods for digitally identifying persons and maintaining associated identity attributes for the users across multiple organizations.
- Access management deals with user privileges.
- Identity and access management deal with user identities, their authentication, authorization and access policies.
- **Federated Identity Management**
  - Federated identity management allows users of one domain to securely access data or systems of another domain seamlessly without the need for maintaining identity information separately for multiple domains.
  - Federation is enabled through the use single sign-on mechanisms such as SAML token and Kerberos.
- **Role-based access control**
  - Used for restricting access to confidential information to authorized users.
  - These access control policies allow defining different roles for different users.

Below Diagram shows an example of the Role Based Access Control Framework in the cloud.



Data Security

Introduction: -

- Securing data in the cloud is critical for cloud applications as the data flows from applications to storage and vice versa. Cloud applications deal with both data at test and data in motion.

- There are various types of threats that can exist for data in the cloud such as denial of service, replay attacks, man-in the -middle attacks, unauthorized access/modification, etc.

1)Securing Data at Rest: -

- Data at rest is the data that is stored in database in the form of tables/records, files on a file server or raw data on a distributed storage or storage area network (SAN).

- Data at rest is secured by encryption.

- Encryption is the process of converting data from its original form (i.e.,

plaintext) to a scrambled form (ciphertext) that is unintelligible. Decryption converts data from ciphertext to plaintext.

- **Encryption can be of two types:**
    - Symmetric Encryption (symmetric-key algorithms)
    - Asymmetric Encryption (public-key algorithms)

a) Symmetric Encryption:

- Symmetric encryption uses the same secret key for both encryption and decryption.

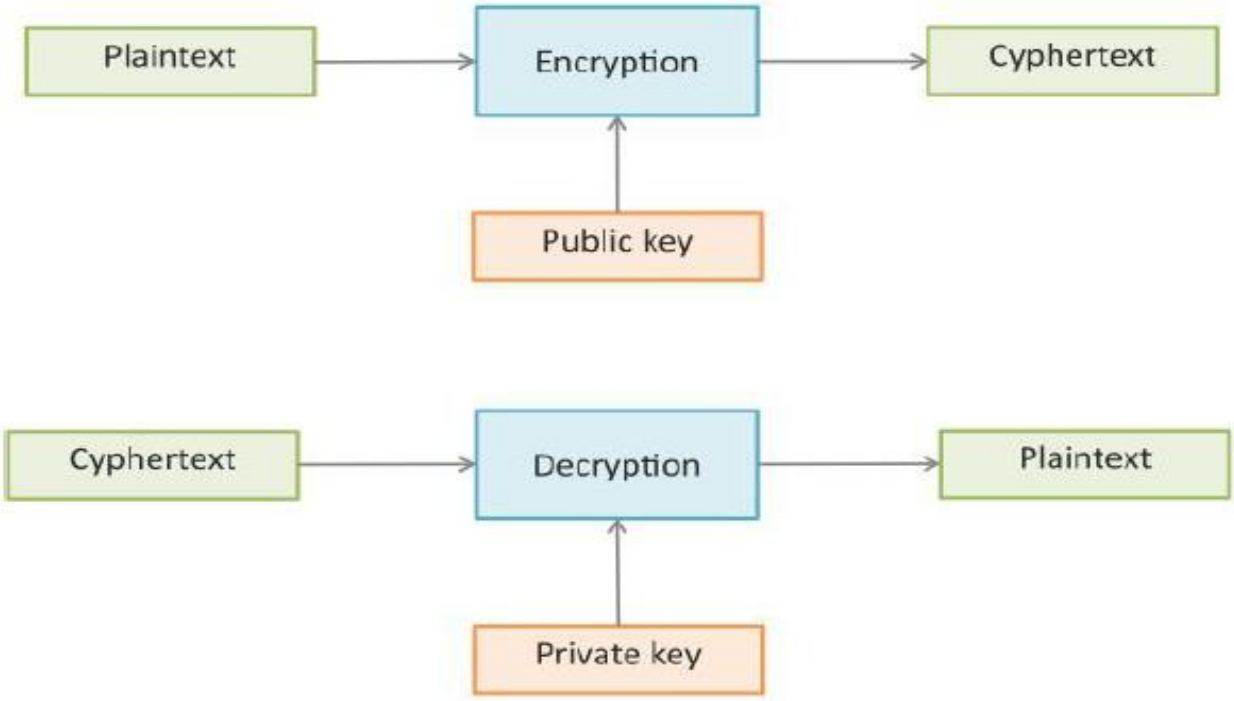
- The secret key is shared between the sender and the receiver.

- Symmetric encryption is best suited for securing data at rest since the data is accessed by known entities from known locations.

- Popular symmetric encryption algorithms include:
    - Advanced Encryption Standard (AES)
    - Twofish
    - Blowfish
    - Triple Data Encryption Standard (3DES)
    - Serpent
    - RC6
    - MARS

b) Asymmetric Encryption:

- Asymmetric encryption uses two keys, one for encryption (public key) and other for decryption (private key).



- The two keys are linked to each other such that one key encrypts plaintext to ciphertext and other decrypts ciphertext back to plaintext.
- Public key can be shared or published while the private key is known only to the user.
- Asymmetric encryption is best suited for securing data that is exchanged between two parties where symmetric encryption can be unsafe because the secret key has to be exchanged between the parties and anyone who manages to obtain the secret key can decrypt the data.
- In asymmetric encryption a separate key is used for decryption which is kept private.

c)Encryption Levels:

Encryption can be performed at various levels described as follows:

- Application
- Host
- Network
- Device

Application:

- Application-level encryption involves encrypting application data right at the point where it originates i.e. within the application.
- Application-level encryption provides security at the level of both the operating system and from other applications
- An application encrypts all data generated in the application before it flows to the lower levels and presents decrypted data to the user.

Host:

- In host-level encryption, encryption is performed at the file-level for all applications running on the host.
- Host level encryption can be done in software in which case additional computational resource is required for encryption or it can be performed with specialized hardware such as a cryptographic accelerator card.

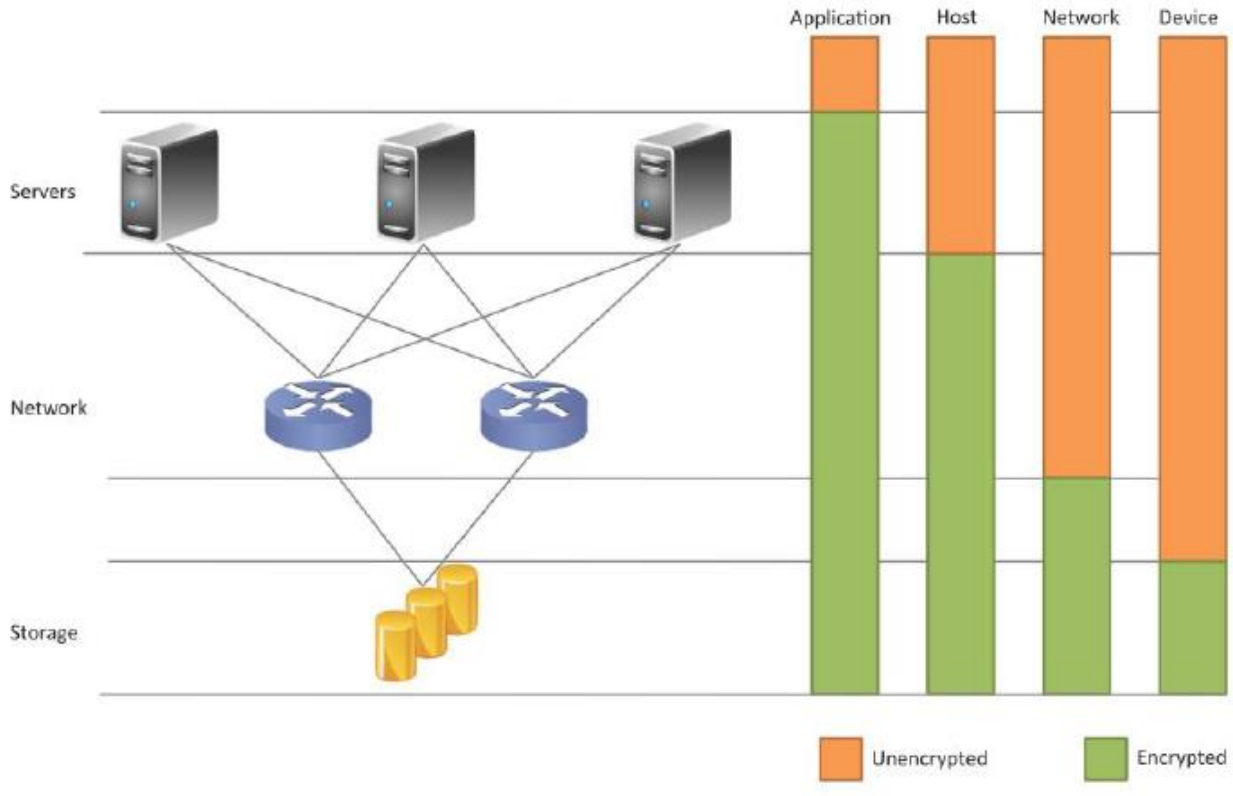
Network:

- Network-level encryption is best suited for cases where the threats to data are at the network or storage level and not at the application or host level.
- Network-level encryption is performed when moving the data form a creation point to its destination using a specialized hardware that encrypts all incoming data in real-time.

Device:

- Device-level encryption is performed on a disk controller or a storage server
- Device level encryption is easy to implement and is best suited for cases where the primary concern about data security is to protect data residing on storage media

Below Diagram shows various Encryption levels:



2)Securing Data in Motion: -

- Securing data in motion, i.e., when the data flows between a client and a server over a potentially insecure network, is important to ensure data confidentiality and integrity.

Data confidentiality:

Data Confidentiality means limiting the access to data so that only authorized recipients can
access it.

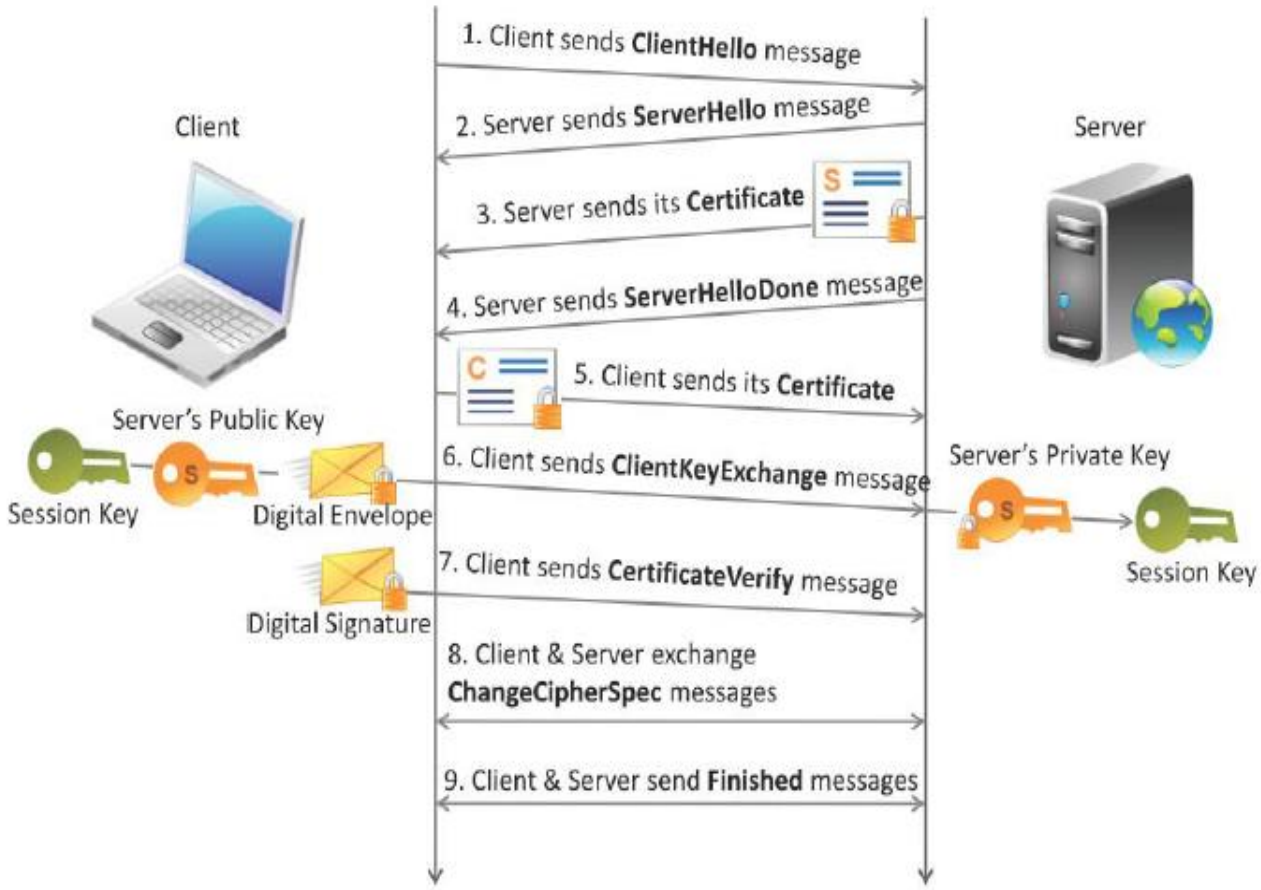
Data integrity:

Data integrity means that the data remains unchanged when moving from sender to receiver.

Data integrity ensures that the data is not altered in an unauthorized manner after it is created, transmitted or stored.

Transport Layer Security (TLS) and Secure Socket Layer (SSL) are the mechanisms used for securing data in motion.

Below diagram shows the TLS Handshake protocol:



TLS and SSL are used to encrypt web traffic using Hypertext Transfer Protocol (HTTP).

TLS and SSL use asymmetric cryptography for authentication of key exchange, symmetric encryption for confidentiality and message authentication codes for message integrity.

Key Management

Introduction: -

Management of encryption keys is critical to ensure security of encrypted data. The key management lifecycle involves different phases including:

Creation: Creation of keys is the first step in the key management lifecycle. Keys must be created in a secure environment and must have adequate strength. It is recommended to encrypt the keys themselves. with a separate master key.

Backup: Backup of keys must be made before putting them into production because in the event of loss of keys, all encrypted data can become useless.

Deployment: In this phase the new key is deployed for encrypting the data. Deployment of a new key involves re-keying existing data.

Monitoring: After a key has been deployed, monitoring the performance of the encryption environment is done to ensure that the key has been deployed correctly.

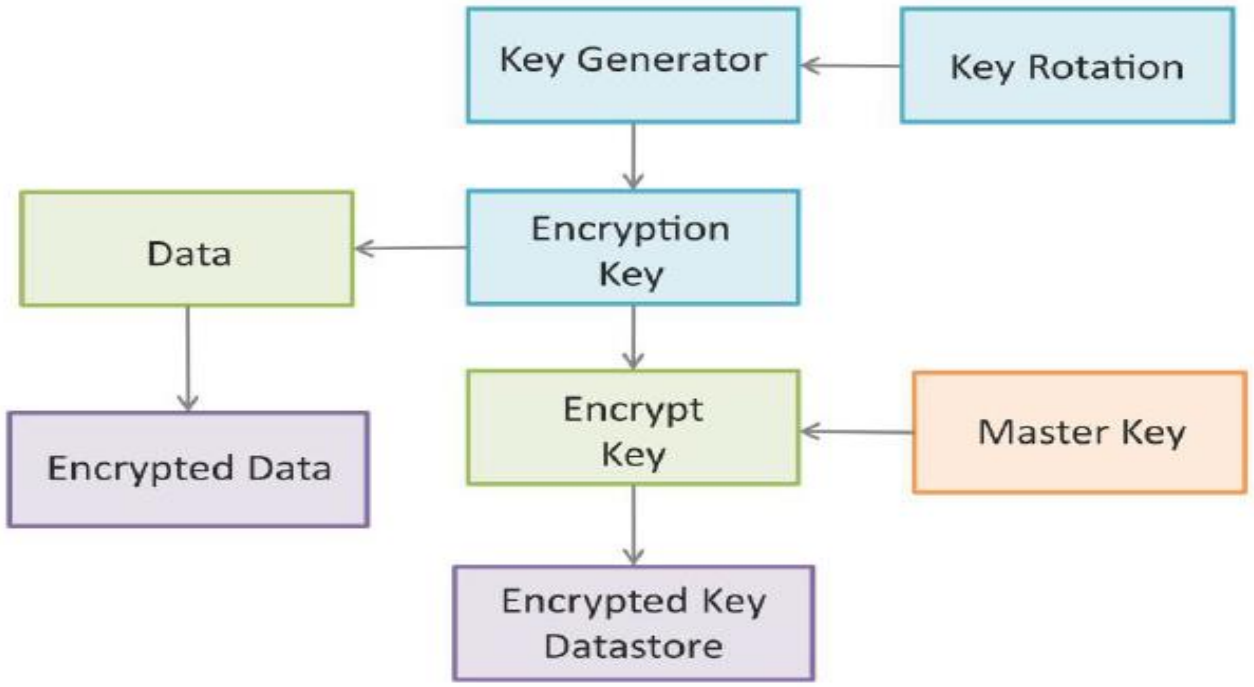
Rotation: Key rotation involves creating a new key and re-encrypting all data with the new key.

Expiration: Key expiration phase begins after the key rotation is complete. It is recommended to complete the key rotation process before the expiry of the existing key.

Archival: Archival is the phase before the key is finally destroyed. It is recommended to archive old keys for some period of time tt› account for scenarios where there is still some data in the system that is encrypted with the old key.

Destruction: Expired keys are finally destroyed after ensuring that there is no data encrypted with the expired keys.

Below diagram shows an example of the key Management approach:



Auditing

Introduction: -

- Auditing is mandated by most data security regulations.
- Auditing requires that all read and write accesses to data be logged.
- Logs can include the user involved, type of access, timestamp, actions performed and records accessed.
- The main purpose of auditing is to find security breaches, so that necessary changes can be made in the application and deployment to prevent a further security breach.

Objectives:

The objectives of auditing include:

- Verify efficiency and compliance of identity and access management controls as per established access policies.
- Verifying that authorized users are granted access to data and services based on their roles.
- Verify whether access policies are updated in a timely manner upon change in the roles of the users.
- Verify whether the data protection policies are sufficient.
- Assessment of support activities such as problem management

Cloud Computing for Education.

Introduction: -

Cloud computing is bringing a transformative impact in the. field of education by improving the reach of quality education to students through the use of online learning platforms and collaboration tools.

In the recent years the concept of Massively Online Open Courses (MOOCs) appears to be gaining popularity worldwide with large numbers students enrolling for online courses.

Some of the Education programs running on the Cloud platforms are listed below:

MOOCs

- MOOCs are aimed for large audiences and use cloud technologies for providing audio/video content, readings, assignment and exams.
- Cloud-based auto-grading applications are used for grading exams and assignments. Cloud-based applications for peer grading of exams and assignments are also used in some MOOCs

Online Programs

- Many universities across the world are using cloud platforms for providing online degree programs.
- Lectures are delivered through live/recorded video using cloud-based content delivery networks to students across the world.

Online Proctoring

- Online proctoring for distance learning programs is also becoming popular through the use of cloud-based live video streaming technologies where online proctors observe test takers remotely through video.

Virtual Labs

- Access to virtual labs is provided to distance learning students through the cloud. Virtual labs provide remote access to the same software and applications that are used by students on campus.

Course Management Platforms

- Cloud-based course management platforms are used to for sharing reading materials, providing assignments and releasing grades, for instance.
- Cloud-based collaboration applications such as online forums, can help student discuss common problems and seek guidance from experts.

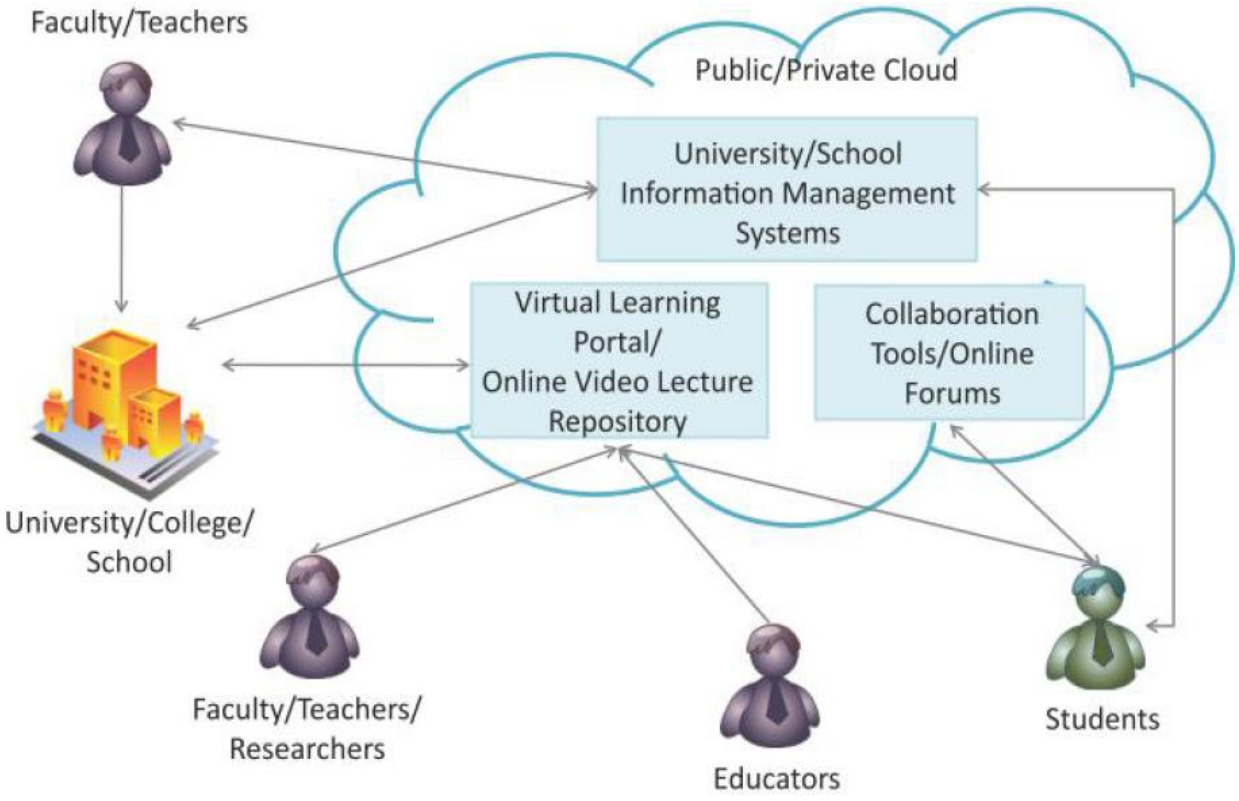
Information Management

- Universities, colleges and schools can use cloud-based information management systems to improve administrative efficiency, offer online and distance education programs, online exams, track progress of students, collect feedback from students, for instance.

Reduce Cost of Education

- Cloud computing thus has the potential of helping in bringing down the cost of education by increasing the student-teacher ratio through the use of online learning platforms and new evaluation approaches without sacrificing quality.

Below diagram shows the generic use of the Cloud for Education:


Faculty/Teachers
Public/Private Cloud
University/School Information Management Systems
Virtual Learning Portal/ Online Video Lecture Repository
Collaboration Tools/Online Forums
University/College/ School
Faculty/Teachers/ Researchers
Educators
Students

******ALL THE BEST******