Software System Security

BOJJAPREMNATH

Unit 4

Security Practice

* Cloud and IoT security : cloud computing - cloud security concepts - cloud security approaches, Transport Layer Security: TLS - HTTPS SSH ; Electronic Mail Security : PGP, S/MIME - IP security - Web Security; IP Security ; IPSec

* Cloud Computing

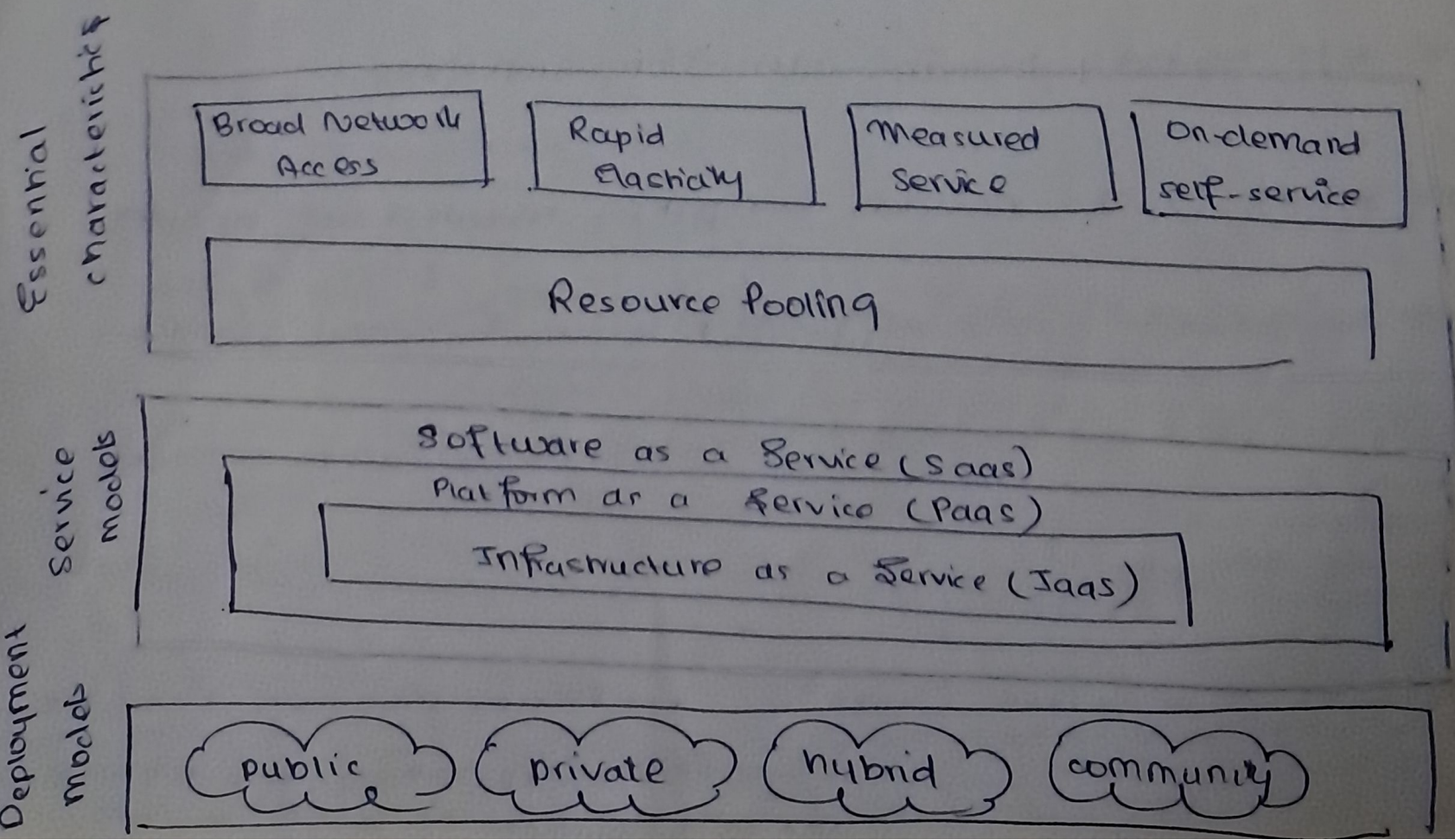
→ Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources, that can be rapidly provisioned and released.

→ The cloud model has:

(i) 5 essential characteristics

(ii) 3 service models

(iii) 4 deployment models



5 Essential Characteristics

(i) Broad Network Access : capabilities are available over the network and accessed through standard mechanism

eg. mobile phones, laptops and PDAs

(ii) Rapid Elasticity : ability to expand and reduce resources according to one's specific service requirement.

(iii) Measured Service : Cloud systems automatically control & optimize resource use by leveraging a metering capability for each service like storage, processing, bandwidth & active user accounts

(iv) On-demand self-service : A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed w/o requiring human interaction each time.

(v) Resource pooling : The provider's computing resources are pooled to serve multiple consumers, with different physical & virtual resources dynamically assigned and reassigned according to consumer demand

3 Service Models

A. Software as a Service (SaaS) . → Allows consumers to use the provider's applications running on a cloud infrastructure

→ SaaS saves the complexity of software installation, maintenance, upgrades and patches.

→ Examples : GMail
Salesforce

B. Platform as a Service (Paas) → can deploy consumer-created applications onto the cloud infrastructure using programming languages and tools supported by the provider

→ Paas is an operating system in the cloud.

C. Infrastructure as a Service (Iaas) → The capability provided to the consumer is to provision processing, storage, network & the consumer is able to run arbitrary software, which can include OS & applications.

Deployment Models

A. Public Cloud : → cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services
→ cloud provider responsible for infra, operation. & data.

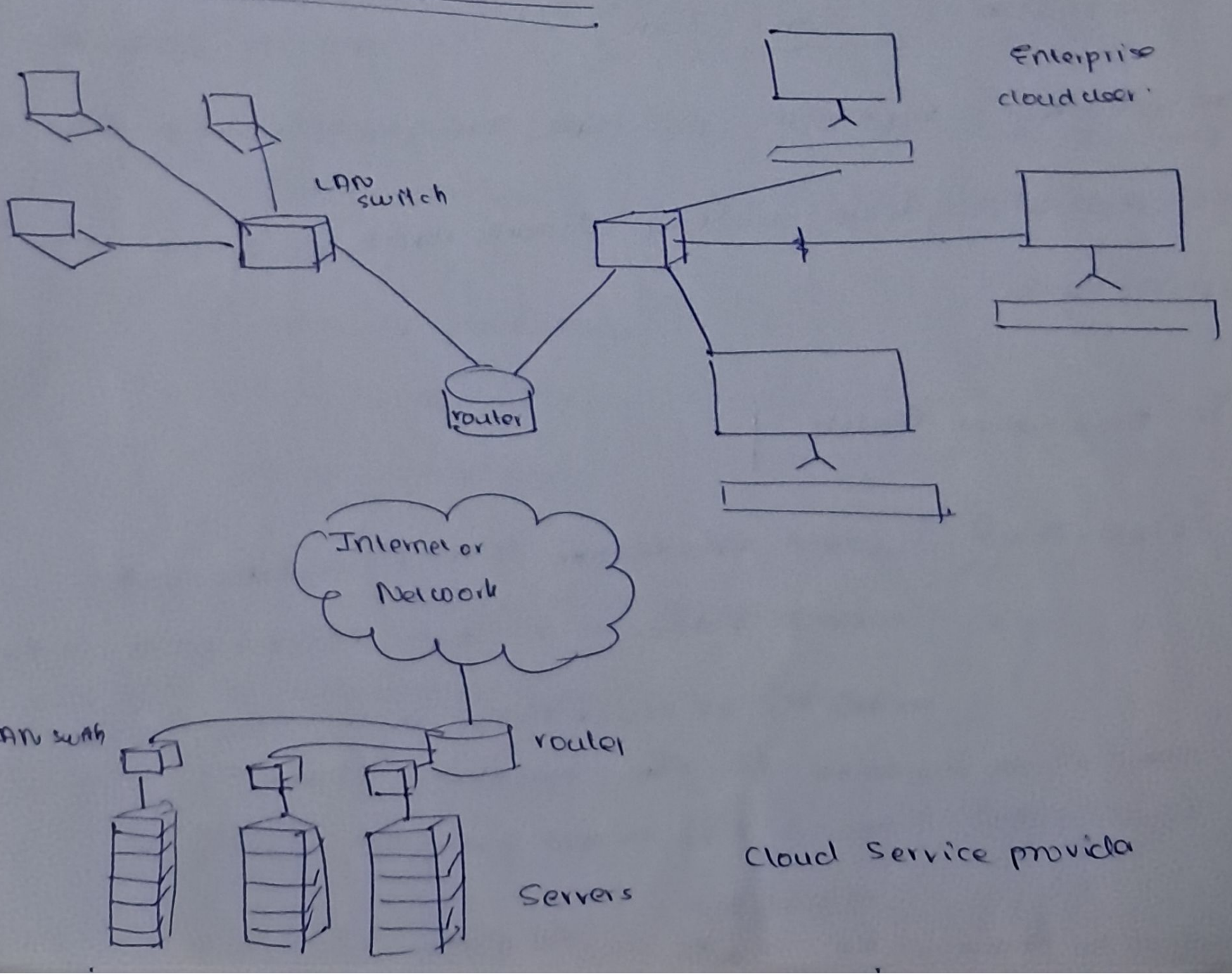
B. Private Cloud : → cloud infrastructure is operated solely for an organization.
→ may be managed by org or by 3rd party

→ The cloud provider (CP) is responsible only for the infrastructure and not for the control.

c. Community Cloud - Cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns

d Hybrid cloud : The cloud infrastructure is a composition of 2 or more clouds (private, community, or public) that are unique entities.

* Cloud Computing Architecture



→ An enterprise maintains workstations within an enterprise LAN or set of LANs, which is connected by a router through a network

→ The CSP maintains a massive collection of servers, with which it does network management, redundancy & has security tools

* 5 Major Actors

1. cloud consumer
2. cloud provider
3. cloud auditor - an independent entity that can assure that the CP conforms to a set of standards
4. cloud broker - used when cloud services are too complex for a cloud consumer to easily manage. The cloud broker can provide:
   (i) service intermediation
   (ii) service aggregation
   (iii) service arbitrage
3. cloud carrier - an intermediary that provides connectivity and transport of cloud services from CSP to consumer

* Role of CP in Saas, Paas and Iaas

Saas

→ CP deploys, configures, maintains and updates the operation of software applications on a cloud infrastructure, so that the services can be provisioned to cloud consumers

→ consumers of saas can directly provide their members with access to software applications

Paas

→ CP manages the computing infrastructure & maintains the runtime stack, databases and other middleware.

→ consumers can develop, test, deploy & manage the applications hosted in a cloud environment.

Iaas → CP acquires the physical computing resources underlying the service including the servers, network, storage & hosting infrastructure.

→ consumer uses Iaas for their fundamental computing needs.

* Database Environments in Cloud Computing

A. **Multi Instance Model**

→ provides a unique DBMS running on a VM instance for each cloud subscriber.

→ This gives the subscriber complete control over role definition, user authorization, and other admin tasks related to security.

B. **Multi Tenant Model**

→ provides a predefined environment for the cloud subscriber that is shared with other tenants - tag data w/ a subscriber identifier

→ Tagging gives the appearance of exclusive use of the instance, but relies on the CP to establish & maintain a sound db env.

* Cloud Security Threats and Countermeasures.

1. **Abuse and Nefarious use of cloud computing**
   - stricter initial registration & validation processes
   - introspection of customer network traffic
2. **Malicious Insiders**
   - enforce strict supply chain mgmt
   - conduct a comprehensive supplier assessment

3. **Insecure Interfaces and APIs** - analyze security model
- ensure that strong authentication & access controls are implemented.

4. **Shared Technology Issues**

5. **Data loss or leakage** - implement strong API access control
- encrypt and protect integrity of data in transit
- implement strong key generation, storage management & destruction process.

6. **Account of service hijacking** - 2-factor auth
prohibit sharing credentials

7. **Unknown risk profile** - client codes control host

*IAM (Identity and access management)

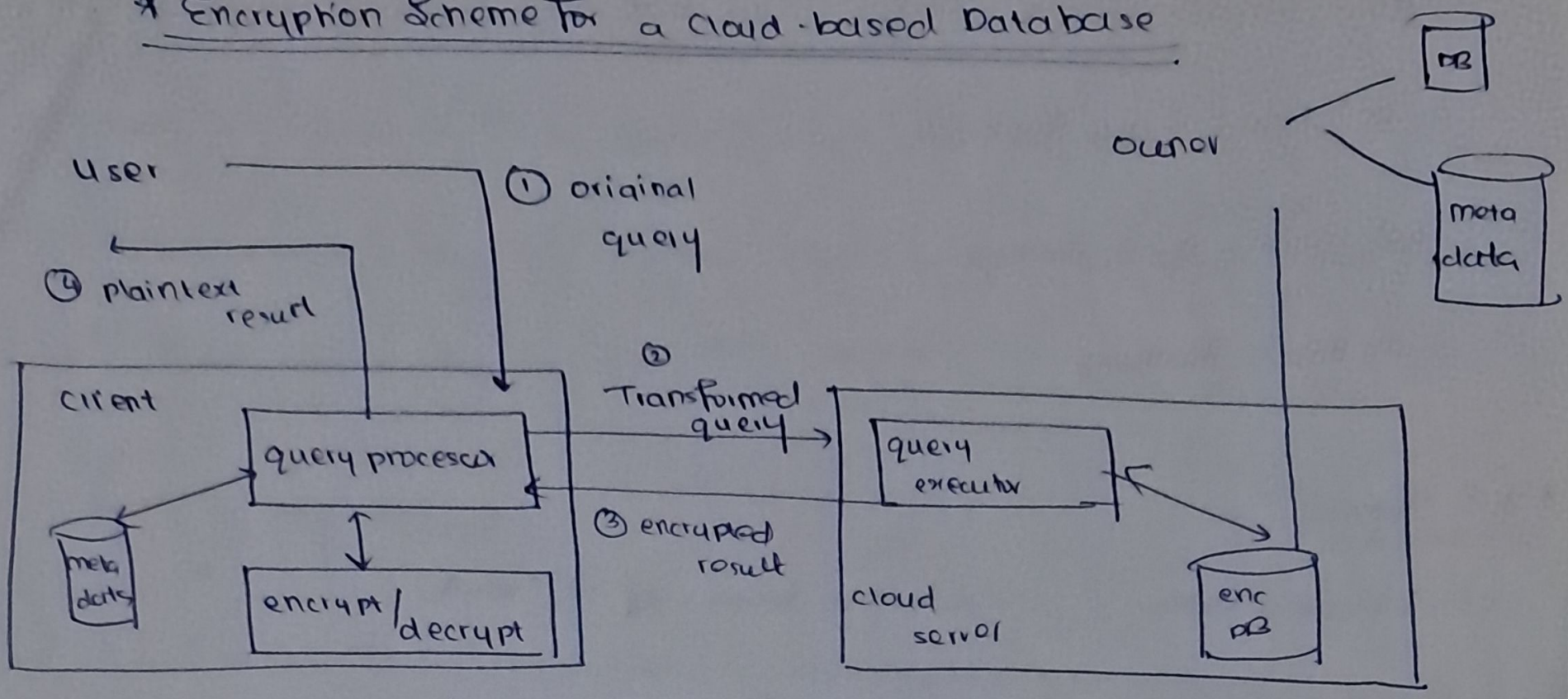
→ Includes people, processes and systems that are used to manage access to enterprise resources by assuring that the identity of entity is verified, and then granting the correct level of access based on this assured identity.

→ One aspect of identity management is identity provisioning, which has tools with providing access to identified users and subsequently deprovisioning or denying access

→ IAM is used by the CSP to authenticate users in a trustworthy manner.

→ The access control requirements in Saas, Paas, Iaas environments include establishing trusted user profile and policy information, and using it to control access within the cloud service

* Encryption Scheme for a cloud-based Database



has 4 entities
① Data Owner
② User
③ Client
④ Server

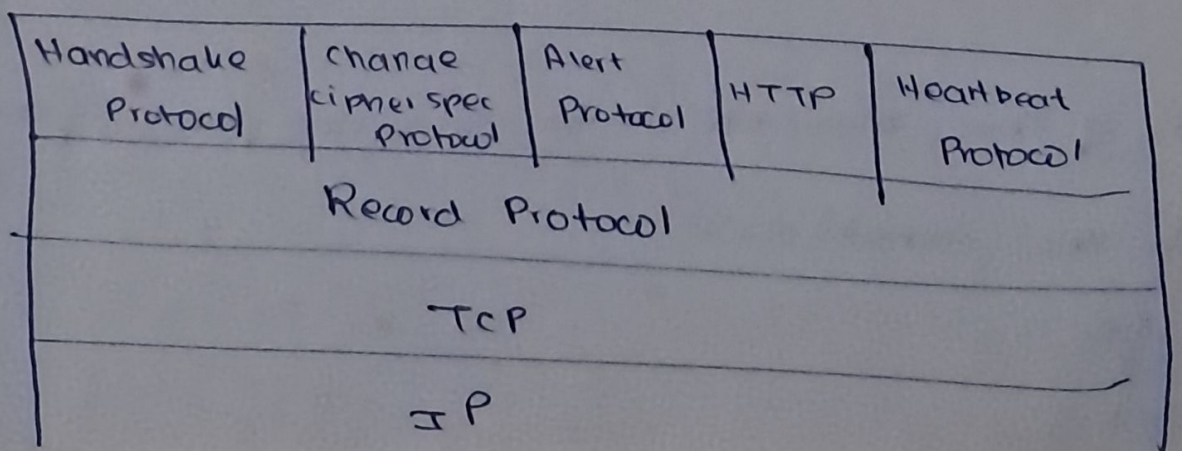
* TLS

→ TLS is an internet standard that evolved from a commercial protocol Secure Socket Layer (SSL)

→ TLS is a general purpose service implemented as a set of protocols that rely on TCP.

→ TLS is an upgraded version of SSL that fixes existing SSL vulnerabilities. TLS authenticates more efficiently and continues to support encrypted communication channels

TLS Protocol Stack



→ Three higher layer protocols are defined as part of TLS

(i) Handshake Protocol

(ii) Change Cipher Spec Protocol

(iii) Alert Protocol

* TLS Services

(i) Fragmentation : divide into blocks of 2^{14} bytes

(ii) Compression: compress each fragment of data using lossless compression

(iii) Message Integrity - SSL Uses a keyed hash fn

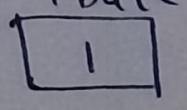
(iv) Confidentiality - Original data and MAC are encrypted using symmetric key cryptography

* TLS Protocols

① Change Cipher Spec Protocol

→ consists of a single message which consists of a single byte with the value 1.

→ The sole purpose of this message is to cause the pending state to be copied into the current state



② Alert Protocol

→ used to convert TLS-related alerts to the peer entity

→ each message in this protocol consists of 2000 bytes. The first byte takes the value → warning, → fatal to convey the severity of the message.

→ If fatal, TLS immediately terminates the connection.

→ The second byte contains a code that indicates a specific alert

③ Handshake Protocol

→ This protocol allows the server and client to authenticate one another and to negotiate an encryption & MAC algo.

→ The message format is as follows:

1byte	3bytes	≥0 bytes
Type	Length	content

client

server

client - hello

server - hello

Phase1 - establish security capabilities including protocol version, session ID, cipher suite, compression method

certificate

server key exchange

certificate request

server hello done

Phase2 send cert, key exchange, request certificate

certificate

client key exchange

certificate - verify

Phase3 client sends cert if request, along w/ key exchange & cert verification

change cipher spec

finished

change cipher spec

finished

Phase 4 : change cipher suite & finish handshake protocol

* HTTPS

→ refers to the combination of HTTP and SSL to implement secure communication between a web browser and web server.

→ If https is used, the URL begins with https://

→ When HTTPS is used, the following elements of the communication are encrypted.

(i) URL of the requested doc

(ii) contents of the document

(iii) content of browser forms

(iv) cookies between server ↔ browser

(v) contents of HTTP header

Connection Initiation

→ agent acting as the HTTP client also acts like the TLS client

→ client initiates connection to server on appropriate port

→ send TLS ClientHello to begin the TLS handshake

→ finish TLS handshake - then initiate HTTP request

Connection Closure

→ include the following line in a HTTP record: Connection: close.

→ a close - notify alert is absent

*SSH Secure Shell

→ simple, inexpensive to implement

→ used for remote login and X tunneling

→ also provides more general client/server capability

SSH is organized as 3 protocols that run on top of TC.

(i) **TLS** : provides serv auth

data confidentiality, integrity

(ii) **User Authentication Protocol** – authenticate user to server

(iii) **Connection Protocol** – multiplexes multiple logical communication

channels over a single underlying SSH connection

working Client contacts server

server sends client a public cryptography key

serv negotiates params - opens a secure channel

user through client logs onto server

Key SSH features

* Electronic Mail Security

1. S/MIME

→ Secure / Multipurpose Internet Mail Extension (S/MIME) is a security enhancement to the MIME email format standard based on technology from RSA Data Security.

→ S/MIME provides for 4 message-related services

(i) authentication

(ii) confidentiality

(iii) compression

(iv) email compatibility

Authentication

→ established using digital signature

Algorithm : RSA / SHA-256

Action : A hash code of a message is created using SHA-256

The message digest is encrypted using SHA-256 with the sender's private key and included with the message.

Confidentiality

→ established using message encryption

Algorithm AES-128 with CBC

Action : A message is encrypted using AES-128 with CBC with

a one-time session key generated by the sender

→ The session key is encrypted using RSA with the recipient's public key and included with the message

Compression - message compressed for storage / transmission

Email compatibility

Algorithm - Radix-64 conversion

Action : To provide transparency for email applications, an encrypted message may be converted to an ASCII string using radix-64 conversion

* Pretty Good Privacy (PGP)

similar to S/MIME but has a significant differences

Key certification S/MIME uses X.509 that are issued by certificate authorities

In OpenPGP, users generate their own public & private keys and then solicit signatures for their public keys from individuals/ organizations to which they are known (Web of Trust)

Key Distribution OpenPGP does not include the sender's public key with each message, so it is necessary for recipients of OpenPGP msgs to separately obtain the senders public key. Keys may also be on OpenPGP public key server