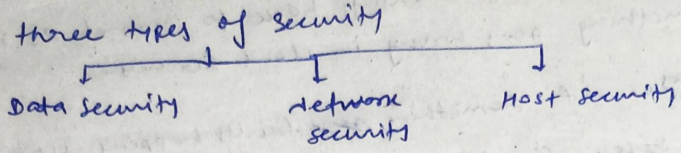
Cloud Security

- Cloud security
- cloud security issues
- legal, regulatory and standard implications
- Disaster Recovery
- three types of security



Regulatory compliance
↳ an organization runs through laws, regulations & guidelines.
↳ legal compliance → laws made by governments.

- traditional data center
  → on-premises data center

Cloud Security :-

It refers to set of rules, procedures and policies that is used to protect data, applications and infrastructure hosted in cloud environments.

It is similar to a guards and locks to keep valuable data safe in a cloud space. It ensures that only authorized user can access and use the data. along with it protects data from unusual threats such as hackers & Malware attacks.

issues in cloud security :-

1. different legal and Regulatory compliance issue -
   Moving from one cloud to another is challenging. each Cloud service providers posses different rules and policies. legal implications, regulatory compliance and standard compliance issues are different in the cloud
2. Access control and Identity Management.
   Managing user access & identities in the cloud can be challenging, especially in multitenants environments, where multiples users or organizations share the same infrastructure.
   weak access controls can lead to unauthorized access or data leaks.
3. Trusting on cloud provider security -

- while moving

- ## Disaster recovery in cloud

Disaster recovery is like having a plan in case something bad happens to your data in cloud such cyber attack, data leakage or data failures.

its about being able to get things back to normal as soon as possible if something goes wrong in cloud servers.

In cloud ~~servers~~ services, if something ~~goes~~ faults happens then the system can often fix itself automatically, and this process easier, faster and sometimes cheaper than traditional methods.

- Problem - * physical detection, good amount of hand work is required { Sol^n - should have a backup data center
  * also testing fully ~~not done~~ is very difficult
  → in cloud it happens automatically } Adv → cost effective, tested abnormal cond^n

- ## Legal, Regulatory & standard implications

- To store data in cloud, everyone needs to follow ~~&~~ some rules provided by cloud service providers.

  Unfortunately, laws and policies are a bit behind the times ~~when~~ when virtualization features comes then ~~it~~ still talks about physical servers not virtual ones.

- Before moving the data or things to the cloud, its important to understand these rules and make sure that our cloud setup follows them. So it is good to double check with experts to be sure

- Sometimes cloud might not ~~fit~~ fit all the requirement for an user, then it can mix with traditional setup. where they can get both facility.

- (location of the cloud storage where data is stored, it also important since each countries have different rules, we need to aware from those rules) Since ~~our~~ user private data is stored at different locations so it ~~considered~~ should follow government rules for that location

- Three types of Security :- → uses (encryption and control access mechanism)
  1. Data security - it is about protecting your data while stored in cloud,
  2. network " - it is about protecting " " while its traveling through the internet (uses firewalls, IDS)
  3. Host " - it is about protecting your computer or servers where the data is stored. (uses system hardening, Antivirus protection ; HIDS, Data segmentation, credential management

- **Data Security :-**

In the cloud, our data is stored on someone else's servers, those servers should need protection. so while choosing ~~the~~ or CSP, we should know how they keep their servers safe and the user responsibilities to keep their data protect at the end.

1. Data security :-

It involves the protection of data stored in the cloud from unauthorized access, alteration or deletion.

↳ control → can't see and server in cloud ~~to~~ it raises concern about the data compromise

methods. (sol^)

i. Encryption : using cryptographic techniques to transform data into a unreadable format, ensuring confidentiality and integrity. (encrypt everything data, backups & network communication and decrypt as per need) - PHP

ii. Access control - Implementing mechanisms where only authorized user can access and modify ~~its~~ data.

iii. ~~Data~~ backup - keep offsite there is a ~~regular~~ procedure, in which ~~reg~~ all data regularly ~~duplicate~~ ~~copy~~ copied the original data and store it in secure location to avoid loss in data.

2. network security - this security focuses on safeguarding communication channels and data traffic within the cloud environment.
   - eg password protection
   - focused on safeguard the integrity of network data.

Two methods

1. Firewalls 2. network Intrusion detection systems

Firewalls :-

A firewall is a network security device that protects a network from unauthorized access. It can be hardware, software or a virtual device.

It filtering examines ~~the packet of data~~ incoming and outgoing packet of data based on ~~the~~ predefined rules and determine whether it allows or block.

It acts as a first line of defence against external threats such as malware attacks & hacking attempts

It allows only specific types of traffic such as HTTP, HTTPS and sometimes FTP.

- Three layered security is provided - (to access sensitive data)

i. Load balancers ii. Application servers (DMZ)

iii. Internal databases. (f — LB — f — DMZ — f — Server)

i. Outer was (f — LB — f — DMZ — f — Server)

Load balancers - A device that distributes incoming network traffic across a group of servers.

- used to meet high volume request from clients

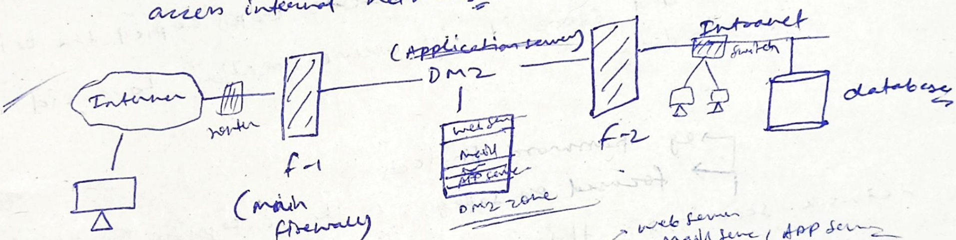
DMZ :- a demilitarized zone (→ An area, where high security is available and surrounded by two firewalls). It acts as a buffer zone bet^n the internet & internal network.

It hosts servers that serves external request like web servers, mail server.

application Server - Internal database - within DMZ, there are application server that uses the internal database to response on request.

- if DMZ not uses then malicious email from authorized mail id can sent. firewall allows it

A main firewalls then DMZ protected by another firewall. and database protected by third firewall. each layer is adding a high level of security. these are the layers, making difficult for attackers to access internal networks.



weakness of three layered - Risk of :- a compromise of any individual servers (web server, Mail server, APP server) inside any given network segment could potentially lead to breach the entire network.

→ In a network setup, if one server within any of the protected segments gets compromized, it could provide an entry point for attackers to breach the network.

for this, its essential to keep strong security on each layer and regular updating software and monitoring network activity.

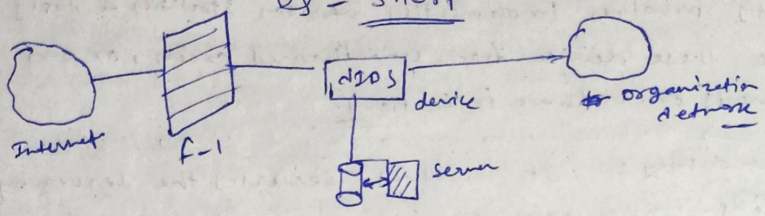
Type

- Packet filtering (stateless, → Limitations) :- this firewall checks each individual piece of data (packet) as it travels through network and decides whether to allow it or block it based on predefined rules.
- Stateful Inspection :- Instead looking at each packet, this type of firewalls, keeps track of overall state of connection & makes more informed decision about whether to allow or block traffic data.
- Application layer :- this types of firewalls understand specific type of internet traffic, like web browsing or email and can make more intelligent decision whether is allowed or blocked based on content of data.

2. NIDS (Network intrusion detection system) → analyze

It is a network device that monitors network traffic for unauthorised activities & potential cyber threats. → detecting

eg - Snort



It can detect known & unknown malware, reduce downtime, Prevent attacks, and detect failure (compromised) devices

Security check

It is passive in nature

It monitors traffic such as hacker used to find weak point or vulnerability in network

It can scans, denial-of-service attacks or attempts to exploit known vulnerabilities by finding weak points,

by sending lots of request Server gets overloaded it stop working

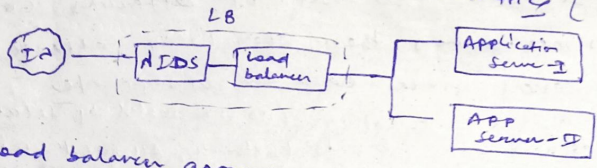
→ Implementation -

one way to Implement dIDS is to have a dedicated server at the front of your network that watches all incoming traffic. (behind the load balancer) act as a intermediate point b/c & next dIPS.

however this setup has a weakness. if the server that hosts dIDS gets compromised, it could silence the detection of further attacks and become a gateway for attackers to enter your network.

alternatives - Instead of putting NIDS on a dedicated server, you can also install it on each individual server in your network. It ensures that every server is protected and reduces the risk of a single point of failure.

↳ Server responsible to monitor the traffic.



- Load balancer approaches creates a single point of failure.
  ↳ when part of a system get fails then entire system gets stop from working
- vulnerability → weak point
- intruder → A system that finds the takes control of load balancer and prevent from further attack.

3. Network segmentation - divide into sub network

each sub network has unique security instead entire network

- Apache on load balancer

3. Host Security

A host can be any device connected to a network, such as a server, desktop computer, laptop or mobile device.

Host security involves implementing various strategies & tools to keep safe these device from unauthorized access, or any cyber threats or malware infections.

i. Server ~~system~~ hardening → remove useless user account & useless services
- It involves securing the server by disabling unnecessary services, removing unused software, and configuring the system with the most secure settings.
- It makes harder for attackers to access the servers.

ii. Antivirous Protection -
- It helps to detect & remove malicious software from your server.
- It is important to choose an antivirous software that offer broad protection & updates frequently to defend against new threats.
  - ↳ How wide is the protection it provides
  - ↳ Avg time when a virus is released & AV provide protection against it

iii. Host instruction detection -
- it is a device used ~~to~~ to monitor the server for any suspicious activity. It detects unauthorized attempts or abnormal behaviour on the server and alert administrators about it
- need CPU power to operate & eat the resources on your server

iv. data segmentation -
- It involves dividing your servers networks into smaller, isolated segments. So that if attackers can get access one servers then they can't attack on another servers since each one is separate
- implementing a zero trust network (no one trusted by default inside & outside network, All need verification to access resources)

v. Credential management -

In this process, it talks about how users access server in the cloud.

one approach is ~~@~~ ↓ cloud provide credentials when the server starts up. ↳ means users don't need to remember the credentials.

another approach is passing user credentials during the server launch process. each user have own a unique credentials.

alternative /

using cloud infrastructure management tools that stores the credentials outside the cloud. and provides keys when it's needed.

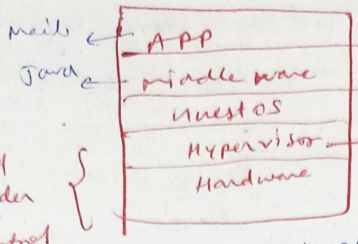
it arises additional attack vector that needs to protect them.

Iaas component stack → hardware + OS + middleware + applesoy

Application
Middleware

Guest OS
↳ Run on VM

VMM
(virtual machine monitor)
↳ Hypervisor



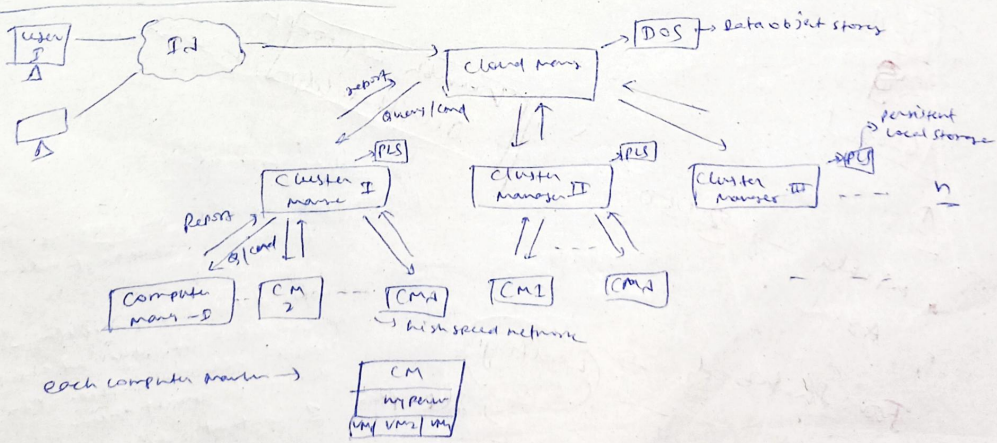
As user can use any. OS in VM.
↳ An Hypervisor uses hardware to make multiple VM and each VM act as one physical system
↳ So user can rent VM.

- three level hierarchy → Top → cloud manager works
  middle → cluster
  bottom → computer

DOS → with cloud manager (stores metadata - user credentials, OS image)
PLS → with cluster manager
↳ it provides disk-like storage to VM
(Persistent local storage)

- computer manager uses xend.-
- three goals for VM Architecture
  equivalence, Resource control, efficiency
- POPEK & Holdberg
- Type 2 VM - xen → Para virtual
  Type 1 VM → microsoft hyper-v → full virtual
  ↳ bare metal

IAAS Cloud Architecture diag → logical view



→ subscriber send cmd/queries to upper layer, and it goes down to each layer ~~then it~~ until the answer get to the querier

IaaS → virtual computer, storage, infrastructure & configuration services (hardware)

fees – cpu per hour, MB stored per hour, network bandwidth, infrastructure used per hr.

Component stack = hardware + OS + middleware + application layer

lower layer → VMM (Hypervisor)

higher layer → guest OS. (Run within VM)

- cloud architecture –
  - Top – layered cloud manager (central control)
  - middle → cluster – (management of all clusters at different location)
  - Bottom level → computer – (running host computer system in which VM created)

Cloud manager responsibility is to have center control and
- provide sign up to user
- generating credential
- public access point

(
- focus on management of resources
- ensuring cloud system perform
- daily operation
- Implementing plan
)

cluster manager – geographically distributed

computer manager – it is connected via high speed network

- cloud manager – public access point to cloud where user login for accounts, manage resources they rent from cloud and accessing data stored in cloud
  - mechanism → Authentication using credentials
  - DOS → Data object storage – → TOP level resource manager
    - it stores user metadata (user credentials) & OS image
    - → single for a cloud (since only one cloud manager in entire cloud)

OS image → file containing OS, file containing data
collection of program & data files needed to a OS can work.
→ it provide resource to user if they are enough available

- cluster manager – responsible to Perform operation of groups of computer connected via high speed network
  - → cloud manager ask it resources can be satisfy or not.
  - → computer manager if return resource then is send to cm.
  - → it receives cmd from cloud manager and send it to computer manager then it return the resources correctly
- PLS (Persistent local storage) → cluster manager (t.
  - → it persistent disk-like storage to virtual machines
  - Provide it retain data even device is shut down
- → cluster manager can instruct the computer manager to perform resource allocation

Aparna

Computer Manager ~~Responsible~~

- it runs on each computer system and uses the virtualization concept to provide VM to users.
- keep track of how many VMs running & ~~are~~ started
- to start, stop, suspend, reconfigure VM → cmd for hypervisor (uses some)

- Virtualization → one computer act as a multiple computer by sharing a single hardware resources.

In virtualization

- Dual boot – Running two different OS on single computer independently. and ~~choose one while starting the computer~~ Switch whenever needed.
  → Provides multiple operating system on same hardware

Hypervisor or virtual machine monitor (a software)

↳ it used to creating the VM & runs guest OS directly to CPU (using hardware resources)

↳ it is a software program.

three goals of VM architecture :– (Popek & Goldberg)

- equivalence, resource control, efficiency → most VM instruction uses direct to CPU without VMM
  VM should be isolated; VM should have complete control on resource (virtualized)

instruction → privillage instruction → cause a trap if executed in user mode
↳ sensitive → change the underlying resource (I/O) (modify the system resistor)

- control sensitive – formal class of SI.
- behavior sensitive –

→ ~~Protected~~
- VMM conforms, if SI is subset of PI are with all three goals

Full virtualization

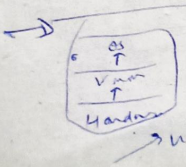
↳ software based
→ VMware & Microsoft
→ used dynamic binary translation
→ open source emulators – QEMU & Bochs
→ guest os completely ~~run~~ isolated due to emulation layer.
→ Total VM possibility.
↳ performance limited

Para virtualization

↳ modified guest
→ VMware, Xen
→ using hypervisor
→ guest os not completely isolated by VM from virtualization layer & hardware
→ API & hypercalls
two approaches
- Recompiling os kernel ~~need drivers~~
- Installing PV drivers

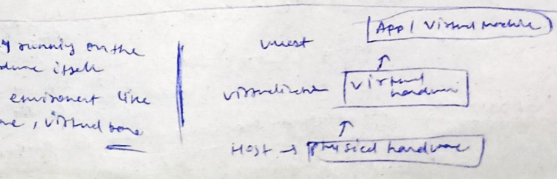
Hardware assisted virtualization (silicon OS)

- unmodified guest OS
  ~~Source~~
↳ full virtualization ~~extended~~ with hardware capabilities



- Host OS → OS actually running on the hardware itself
- Guest OS → OS running in environment like VMware, virtual box

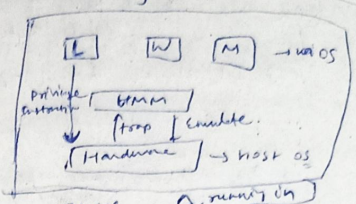
→ Hypervisor



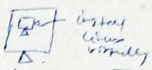
network virtualization

↳ process of logically grouping physical networks & making them operate as single or multiple independent networks

1. Full virtualization — IInd generation (properties, disg. drawbacks)



- each guest OS directly contact with hardware. instead via VMM. (to get nearest resources) then hardware send nearest to the VMM and then VMM send the response to guest OS.
- each guest OS independent of each other
- each guest OS feeling real hardware on its running, (don't aware about virtual environment) running in
- each VMs run independently with its own os & hardware.
- they don't communicate & share resources so they are highly portable
- it does not require any OS modification. provides secure isolation b/t VM.

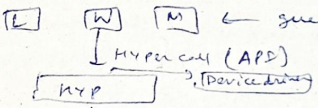


→ disadv
- apps required direct access to the hardware won't function properly in VMs
- in any physical server fault can effect every VM
- due to binary translation it effect on performance

eg- VMware

Partial

2. Para virtualization (OS-assisted virtualization)



- each guest OS sends request to get access resources to the hypervisor. and hypervisor sends request to hardware. then hardware sends the resources to hypervisor and hypervisor sends to guest OS.

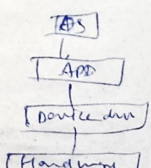
guest OS talking with hardware via VMM. (middle man)

- guest OS knows that it running in virtualized environment. hypercall uses to communication b/t hypervisor & OS.
- it offers improved performance, easier backup, faster migrations & reduced power consumption
- Admin can modify the OS. via drivers.
- it has limited OS options :- . it is less portable
- Partial isolation poses security risk.

→ disadv
- it is generally restricted to experimental use cases.
- modification of guest OS required. (it needed drivers)

→ adv → doesn't use binary translation (improve performance)

eg- Xen



Hardware assisted virtualization

directly

- it provides virtualization through hardware eg- AMD-V
- it eliminates overhead of binary translation, para virtualization (guest OS)

disadv → lack of support from all vendors → companies (IBM companies is support not Atom)

- it is extension of full virtualization

- run on unmodified OS :- → adv
- if this OS does not know that it is running in virtualized environment so they can't get advantage of virtualization (disadv)
  ↳ this resolve only para virtu

Cloud computing, web services & service oriented architecture

Web Services :-

these services are similar to digital messengers that enable different software programs to talk each other across the web. They use a common language (XML or JSON) to understand each others messages and perform tasks. So, if one program needs information or functionality from another, it can request it via a web services.

Def^n

W3C :-

web services as a software application that has a uniform identifier (URI), and its interfaces and bindings can be specified and understood using XML (extensible markup language), a common data ~~form~~

Microsoft :-

web services are programmable application logic, they are accessible using only standard Internet protocols. (rules & conventions on internet).

IBM :-

web services are an interface which provides specific operations and these operations accessible over a network through standardized XML messaging protocol.

SUN :-

it is a software components that can be discovered, combined and recombined to solve users problems or fulfill requests

1. Structured Programing

- A programing paradigm focused on organizing codes into logical structures, making easier to understand and maintain.
- It uses ~~loop~~ control flow structure such as loop, sequence and conditional statement to give direction ~~to~~ to a program.
- the programming language such as C ~~used~~ uses this approach
- the goal of program is to break down a program into smaller parts using modularization or procedure technique. so it becomes easy to read and understand.

Oriented Programing

- It is a programing paradigm that deals with objects and classes.
- It uses principles of encapsulation, polymorphism, inheritance and abstraction
- It provides readability and reusability concept in programing. (security)
- languages like c++, Java and Python are popular example of oops language that supports these concepts.
- each principle ki defn

Distributed computing

- It is a method in which multiple computers connected over internet and together solve a common problem through network
- When developers build a large scale application then they prefer to distributed the tasks across different computer.
- It enables better scalability, fault tolerance and performance optimization by using resources of multiple machine
- In distributed application, different components may run on different computer that makes 2-tier architecture

N-tier Applications -

these applications are divided into multiple layers and each layers does a specific task

for example, a 3-tier application -

1. The user interface running on one computer
2. Business processing ——— another ——
3. the database hosted on third ——

these tier interact with each other over the network to run applications smoothly

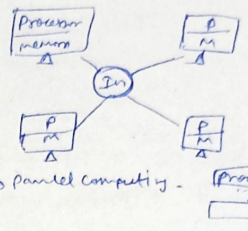
Communication bet^n distributed components -

- for distributed application to work effectively, needed better fast communication,
- communication involves exchanging data and invoking remote procedures.
- various technology used,

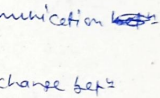
DCE (Distributed computing environment)
CORBA (common object request broker architecture)
DCOM (Distributed component object model)
RMI (Remote method Invocation)

4. Interoperability -

- It is the ability of different software components to communicate and share data effectively, regardless of the platform they come from.
- Achieving interoperability is necessary in distributed computing where components may be developed using diversed technologies.



→ parallel computing -



- Electronic Data Exchange (EDI)

It allows companies to exchange business data and documents electronically using standard format both nationally and internationally.

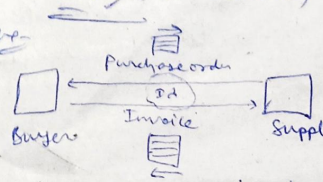
It enables seamless communication and data exchange.

The data / information exchange bet^n companies via EDI follows predefined formats agreed upon by the participating companies.

Advantage

- it reduces the need for manual handling of documents leading to cost saving in printing. → reduction in paperwork
- Time & cost saving - automation of data exchange process saves time & money (e.g. 100 customers ki automatic invoice bhejni)
- Reduced error & increased accuracy - (generate invoice with correct data) since EDI eliminates manual data entry, there is a less chance of human error
- Increased productivity - (at a time deal with huge amount) with streamlined & automated process, each one can focus on more valued tasks.
- Faster trading cycle - it enables faster exchange of information & transaction and improved relationship with trading partners. (jaldi send kar sakte hai)

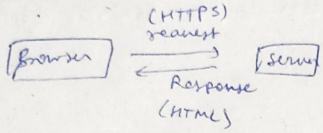
eg -



older days → faxes/mails + through send kiya jata tha

WWW (World Wide Web)

- World wide web is a global network of interconnected computers that allows users to access & share information through hyperlinked documents.
- Users navigate the web using web browsers, accessing resources identified by unique URLs.
- Search engine helps users to find information by exploring relevant web pages
- It operates based on some protocols so that different device can use it.



Web Services

- ~~Building~~
- A web service is a standardized method for propagating message between client & server.
- It allows developers to create applications using existing software components in modular way
- Today entire internet becomes massive library of these prebuilt tools.
- developers can access any function and features hosted on different servers across the web.
- web services use open standards, to communicate effectively between different software components.
- web services communicates using text-based protocols, making it easier to understand & debugging.
- web services provides capabilities similar to EDI but are easier & cheaper to implement.
- web services can be configured to work seamlessly with existing EDI systems. this allows organization to integrate web services into their existing infrastructure either alongside EDI systems or gradually replacing them with the web services.
- web services are distinct from the WWW, which primarily focus on accessing & viewing content through web browsers.
- It ~~does~~ divide components into visual & non-visual parts and enabling interaction through various interfaces ~~is~~ such as web browsers & desktop applications.

Using web services solved three problems :-

i) Interoperability :-

- Traditional methods such as DCOM and RMI were ~~so~~ limited by platform (DCOM apps for windows OS and RMI for Java languages)
- web services overcome this issue by using open standard that ~~make~~ work across platforms & languages.

ii) Firewall traversal :-

Older technology like CORBA and DCOM used non-standard ports, which causes issues with firewalls.
On other hand,
web services uses widely allowed ports 80 (HTTP), making communication easier & more dynamic.

iii) Complexity :-

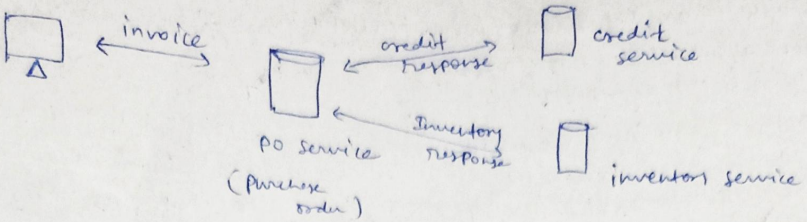
web services are designed to be developer-friendly.
they achieve this through open, text based standards that enable communication bet^n components written in different languages.

- web services can be implemented gradually, reducing cost and minimizing disruption to organizations.

def^n

- A web services similar to a digital messenger that communicates using open protocols like HTTP and SMTP.
- It process messages formatted using XML, a universal data format and form using SOAP.
- The structure of the message is defined using XML. (format)
- The interface of web services is described using WSDL, acting as a guide for consumers.
- web services can be discovered and located using UDDI, making them easier to find and use.

Web based purchase



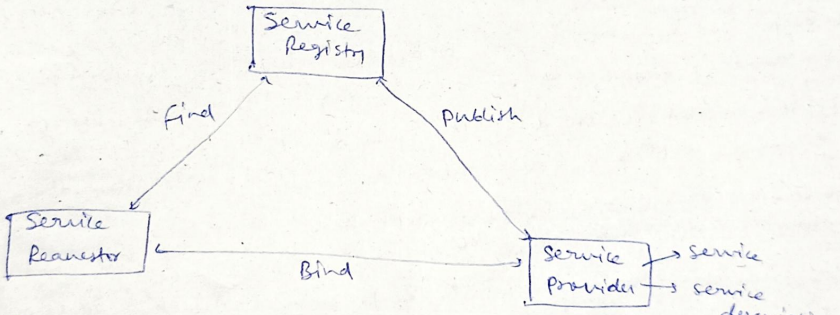
Service oriented Architecture

IBM SoA model is a generic framework that describes how services collaborate within an architecture.

It involved three entities,

1. Service Providers → the service provider is an entity that offer services.
2. Service Reauestor → the service reauestor is an entity that consumes services provided by service provider.
3. Service broker → it helps service reaustors find suitable service providers based on their reauirements.

Web Services model



Roles in web services architecture

1. Service provider : the entity that owns and offers the service. it is responsible for hosting the services and making it available for consumers over the network.
2. Service Reaustor :- it is a consumer that takes services to fulfilled their task. it search the services as per reauirements and then it buys the services from service providers.
3. Service Registry - it is a database which work as a searchable repository of service description within web service architecture.
   - service providers publish descriptions of their services in the registry,
   - service reaustor can query the registry to available services & their details. can select suitable services.

Operation.

1. publish : service provider make services description available by publishing them. so service reauestors can check the services as per need.
2. find :- service reaustors searchly the service description & retriere them either directly or query the service registry.
3. Bind :- service reaustors when found the suitable services then it binds or connect to the service to invoke its functionality at runtime. In this proces, it sends reauest and get response to fulfill their

Web Service components

1. XML - (Extensible Markup Language)
   - it is a universal data representation method.
   - it provides a structural way to represent text based data, makes it easy to understand and process.
2. SOAP - (Simple Object Access Protocol)
   - Standard protocol used for communication in web services.
   - defines set of rules for messages, how they formatted and transmitted over the network.
   - it allows exchange XML based message securely & reliably.
3. WSDL - (Web Services Description Language)
   - standard metadata used to describe services offered by service providers.
   - WSDL files serves as a contract between service providers & consumers provides a medium to use those services.
   - ~~used to write~~ the description of services.
4. UDDI - (Universal Description, Discovery and Integration specification)
   - it is a mechanism used to register & locate web service applications.
   - it provides a directory where service providers can publish the description of their services.
   - ~~Service~~ provides the registration & discovery of web services.

Steps of operation

1. Client queries registry to locate services. (Asking for service)

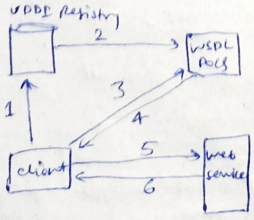
   The client send a query to the service registry to find a specific web service based on its need.
2. Registry Refers clients to WSDL Documents. (get WSDL Docs)

   upon receiving query, the registry provides the client with a reference to WSDL Documents of the requested service.
3. client accesses WSDL Documents. (Provide direction to get the services)

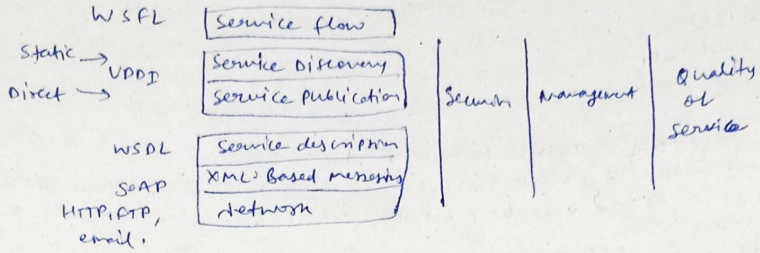
   the client take the WSDL DOCS where it contains detailed information about the service.
4. WSDL provides data to interact with web services

   the client understand the information from the WSDL DOCS, how to interact with web services.
5. client sends SOAP - message request
   - using the info obtain from WSDL, client construct a SOAP message to send a request to the web service
   - this contains necessary data & instructions for web service
6. web service returns SOAP - message response
   - upon receiving ~~request~~ request, it executes the requested operation and send a SOAP message that contains relevant information to the client.

~~Web service Stack~~



Web service stack



In network layer -

HTTP, FTP protocol used to ~~transfer~~ transport the message.

In XML-Based messaging -

message encoded in common XML format for understanding at both ends of connection.

SOAP is used to do operation such as publish, find or bind.

In service description -

WSDL is the standard documents which provides information about service description.

In ~~Dis~~ service discovery -

- ~~Cent~~ Central repository containing location & description of services
- allows web services to publish the description & location.

~~XML~~ Types of web services

- RESTful
- SOAP (JavaScript)

Restful service :- it uses HTTP concept and methods like GET, PUT, POST & DELETE to ~~do~~ access the service. It uses JSON based format (JSON, HTML)

SOAP :- it uses XML Based message format in request & response.

GET → It read the resource
PUT → update the existing
POST → create new resource
DELETE → delete the resource

HTTP Status

404 → Not found
~~400~~ 200 → success
201 → created
401 → unauthorized
500 → server error

- REST → Representational State transfer.

XML

- Extensible Markup Language
- it store data in a structure format.
- it is used to send the data over the internet
- it is widely supported by W3C.
- In XML, we can create own tags, they are not predefined.
- used to exchange data between different platform.
- XML comes from SGML.
- you can define structure using DTD or schema.
  - ↳ it ensure correct syntax.
  - ↳ if XML docs follow proper rules defined by schema then it considered as valid.

XML

- Extensible Markup Language
- describe information
- user can defined own tags
- act as a data base
- case-sensitive
- file name .xml extension

eg.

```
<?xml version="1.0"?>
<contact>
    <name> DKS </name>
    <address> IIEST Shibpur & Address </address>
    <district> Howrah </district>
    <phone> ____ </phone>
    <email> ____ </email>
</contact>
```

- readable for machine & human

HTML

Hypertext Markup language

display information

predefined tags

Static page only show information

not case-sensitive

file name .html extension

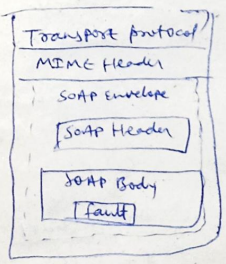
eg.

```
<html>
<body>
    <h2> DKS </h2>
    <b> IIEST Shibpur </b>
    <br>
    Howrah
    <br>
    7061861412
    <br>
    abc@gmail.com
    <br>
</body>
</html>
```

- only readable for human

SOAP (Simple object Access protocol)

- it is a ~~protocol~~ for programs to send message over the internet
- messages are based on XML
- it is platform independent.
- it mainly uses HTTP to move message around.
- A SOAP message enclosed within an HTTP message.
- it is a stateless and supports one way communication.
- it can start from simple application to more complex application for communication.



→ SOAP building blocks

1. Envelope :- this part is necessary & serves as identity the XML docs. as a SOAP message
2. Header :- optional section that can contain additional info. related to the message
3. Body :- a segment that holds the main call & response data
4. fault :- optional section where error ~~described~~ encountered during ~~~~ message processing

Message Structure

1. Request & response message.

SOAP supports two type of messages : Requests & responses.
A request message initiates a method call on a remote object.
A response " returns the result of executing that method.

2. SOAP uses envelope -

- envelope used to wrap the ~~message~~ entire message itself.
- within envelope, message content is structured using a specific xml calendar.
- To distinguish between the envelope & message content, different namespace prefixes are typically used.

SOAP request & response message

see in slides. → 26

Why SOAP?

SOAP gained popularities for several reasons :-

1. failures of other distributed technologies -

Technologies like Unix RPC, CORBA, RMI and DCOM these are platform dependent or language dependent technique.

2. SOAP can work across different OS & programing languages.
3. SOAP message based on XML, making them easy to understand for both machine & human.
4. SOAP imposes no restrictions on the technologies used at endpoints.

SOAP Characteristics :-

it has three major characteristics -

1. Extensibility 2. neutrality 3. Independence

1. Extensibility :-

SOAP is highly extensible. Any new functionalities can add easily.
for ex - security & WS-routing features has added.

2. neutrality - SOAP is transport protocol neutral, it means it can work with different protocol such as HTTP, SMTP or TCP.

3. Independence - SOAP is independent of any specific programming model. this means it can integrated with any programming language & framework.

SOAP Model

1. RPC like message exchange :-
it supports Remote procedure call communication, where request message contains methods & parameters and response message containing the method return values.
2. Flexible message content :-
SOAP allows wide range of content such as XML document

ex-

Request :- used to send a purchase order doc to B2B inbox.

Response :- receive a shipping confirmation & an exceptions report.

SOAP Security

1. HTTP security :- When SOAP is used HTTP protocol then standard security such as HTTP with SSL security is applied to ensure data confidentiality & integrity during transmission.

2. Support for other protocol :-

   SOAP can work with SMTP protocol, so here security issue is considered.

3. WS - Security specification -

   this feature provides a framework to implement various security features including encryption, digital signature, authentication within SOAP message, it ensures data should be protected.

WSDL → web service description language

- it is an XML-based standard vocabulary used for describing web services and their functionalities.
- it serves as a contract between the XML web service & its clients.
- WSDL specifies the structure of request & response message in a clear manner it defines what data, a request must contain & the format of the response.
- it also describes where the service available (its endpoint) and communication protocol that is used to interact with it.

this ensures that client know about finding service and way of communication.

WSDL Documents structure

1 ~~for type~~
- it is a simple XML DOCUMENT.
- it defines the web services using 4 four elements -

i.) Port type - it defines the operation that web service can perform: and client can invoke these operations

ii.) message - this message contains the data which is sent or received among client & web services providers.

iii.) Types - it defines the data type used in web service. this tells about XML schema definition that shows the structure of a message.

iv.) Binding - it defines the communication protocol & message format used by the service.

WSDL

- Binding to SOAP } P.d = 34 — See images

→ <message name> <(name)>

<portType name> <(portTypes)>

UDDI - Universal Description, Discovery & integration

- it is a system for creating and managing online registries that store information in XML format.
- These registry act as repositories where service providers can publish its service details. these information is stored in a structured way.
- user can search the services in the resistry they need. And get access from service providers.
- UDDI can be accessed using SOAP messages, which allow communication over the internet.
- it provides WSDL documents, which makes easy to get service details and how to use it.

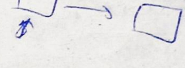
UDDI Roles & operations.

three roles

1. Service registry - this roles involves maintaining registry that stores info about services. it provides support for publishing services and locating services making easy in searching & adding.
2. Service provider - it publish its services to the UDDI Registry, making them available to others to discover & use it
3. Service Requestor.
   - Service requestor, when user or app seeking any functionalities then it initiates a request for this services. and via Service broker easily get the services.
   - once they find the services, they bind / connect to those services via service provider, and start using it.

- How can UDDI be used?

→ ABC.com ——→ UDDI Registry ——→



1. I creates online website
2. UDDI register the website.
3. client stated away about ABC.
4. ABC.com get open and start using it.

• VDDI Benefits -

1. It is making possible to discover right business from millions of online business
2. No. of customers increases due to reaching with new customers
3. - Expanding services & getting market reach
- Provides guidance name for web services.
-