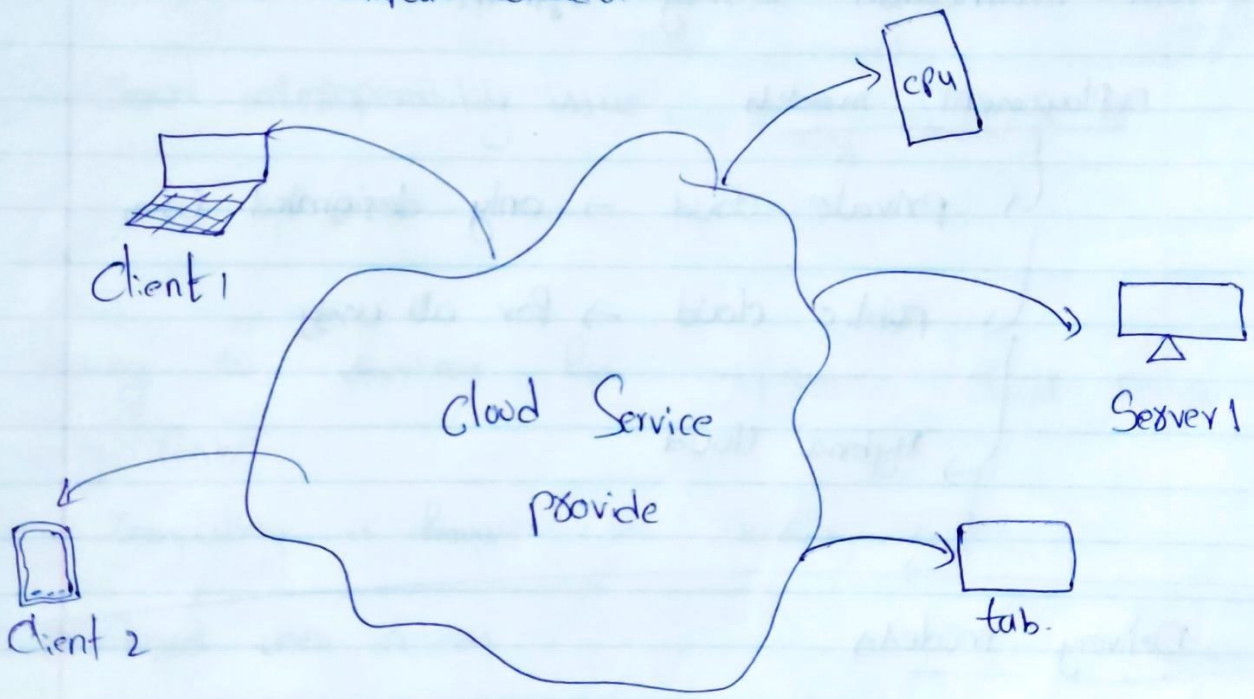
27/05/21

Research Methodology

⇒ Cloud Computing :-

Cloud Computing is the on-demand availability of Computer resources, especially data storage and computing power, without direct active management by the user.

For example :- Azure
Aws
Google Cloud
Compute Canada



If we don't have physical machine what about the Security

↓

issuses related to Security → Hackers
→ Dual Users

↓

Background data processing → Cookies
→ Sessions

↓

↓

Software versions

↓

Payment → Gateway
→ Transaction history
→ failures

↓

Account Management → personal info
→ usage of data

From information Security system

Deployment models

↳ private cloud → only designated users

↳ public cloud → for all users

↳ Hybrid cloud

03/06

Delivery models

↳ Infrastructure as a Service (Iaas) → hardware like servers, networking devices

↳ platform as a service (paas) → development tools like OS, IDE

↳ Software as a service (Saas) → ws, XML

Challenges

① Security → Runing your code on some other hardware (or) cpu.

② Costing model → organisation data transferred between public / private cloud

③ Charging model →

④ Service level Agreement → Controling / lack of control on Computing resources

⑤ Migrate → movement

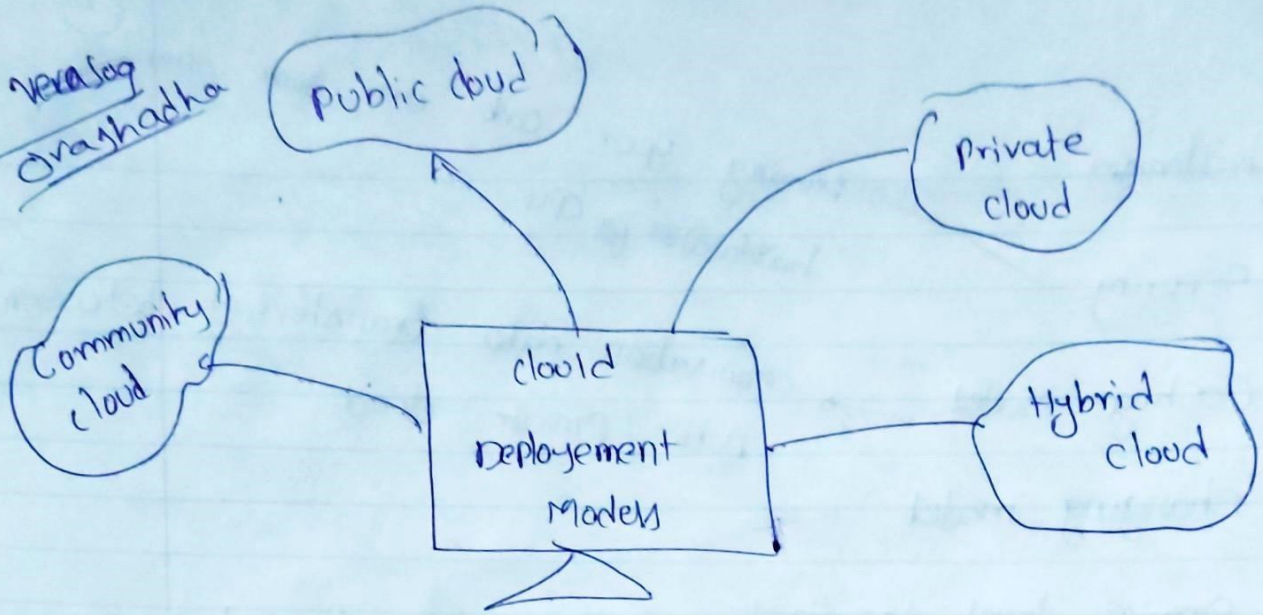
⑥ Cloud interoperability issue → Hazy Cloud.

According to Gartner from 2011 (Seven Cloud Computing Security Risks)

Cloud Computing is fraught with Security risks

* Privileged user access
* Regulatory Compliance
* Data location
* Recovery
* Data Segregation
* investigative support
* long term viability

Veralog
Avashadha



Denial of service

↳ Attack of web servers

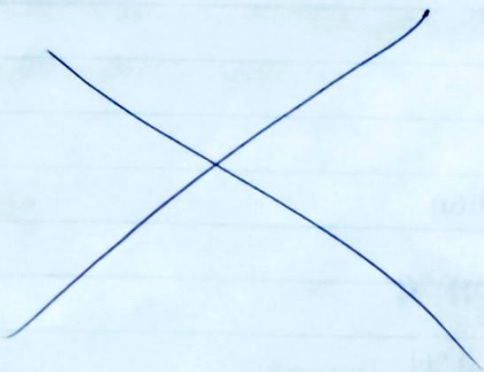
Account hijacking

↳ Http protocol.

Investigation support :-

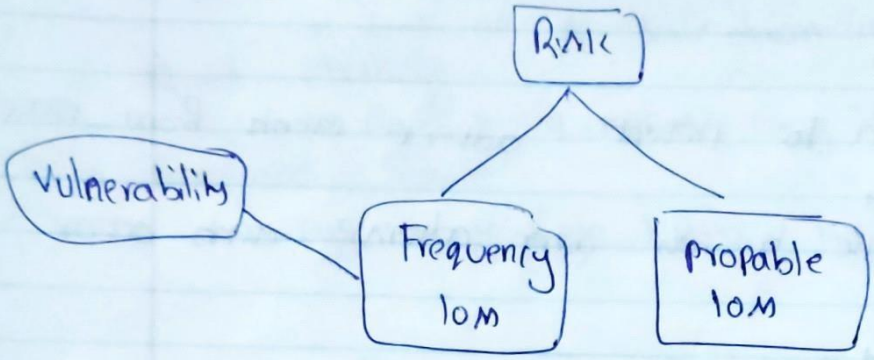
↳ logs

↳ History / Access control

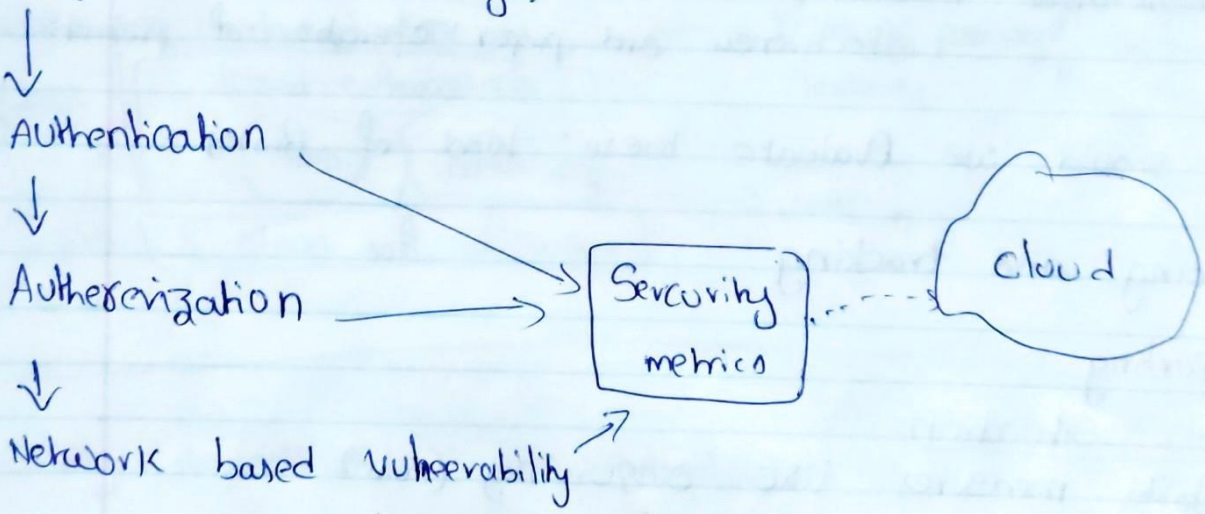


Vulnerabilities :-

-> key factor of security is vulnerability
-> it's kind of risk factor



Is there any cloud specific vulnerabilities ?
if yes, what are they ?



vulnerabilities in cloud Architecture

(1) Poor key management for connecting VM to the local machine (or) vice versa

(2) Network Security → How about other person logged on the same VM at same time
→ is there any n/w monitoring

Risk :-

Annualized loss Expectation

Information Security :-

* Protection measures

This aim to prevent adverse events from occurring

* Detection measures

Alert the business when adverse events occur

* Response measures

Deals with Consequences of adverse events

* Assurance measures

effectiveness and proper operation of protection.

How should we Evaluate these kind of Risks

→ tracing and tracking

→ Reporting

Current Situation:-

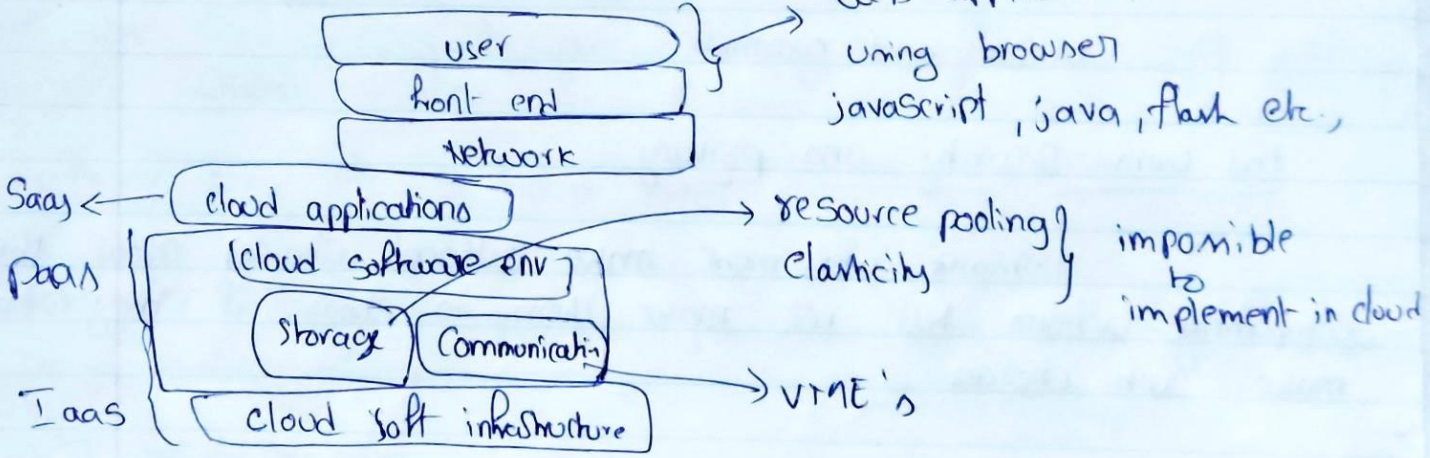
availability measures like acquiring (cost)
Managing
maintaining

Managing Risk :-

↳ liability transfer → disclaims, transfers
↳ identification → pooling and hedging
↳ mitigation
↳ retention

Essential characteristics of Vulnerabilities

- → On demand self service
  - ⇒ without human interaction we can order (or) manage ex:- web portal
- → Ubiquitous network access
  - ⇒ cloud services via n/w
- → Resource pooling
  - ⇒ scale up & scale down immediately
- → Rapid elasticity
  - ⇒ cloud services realised using homogenous infrastructure
- → measured Service
  - ⇒ pay as you go business models.



20/06

Identity, Authentication and Authorization

- ↳ Denial of Service by account lockout → username & password
- ↳ weak credential reset mechanisms → rules for forgotten and reset the credentials.
- ↳ insufficient (or) faculty authorization checks
  - ↳ URL's attacks
- ↳ Coarse authorization control
  - ↳ duty seperation at work
- ↳ Insufficient logging & monitoring possibilities.
  - ↳ logs

General Trustworthy large scale systems

Build trustworthy large scale systems for important social applications

For ex:- voting
health records
law enforcement

Epidemic style attacks

→ Spam → makes it hard to read mail

→ denial of service → down critical sites

→ virus and worms

End users security and privacy:-

Humans users must make rational choices about their computing actions but not make them to choose if they cannot make such choices.

General Security challenges

→ Trusting vendor's Security model → Follow the rules

→ Customer inability to respond to audit findings → Better to check the o/p of every check

→ Support for investigations

→ Indirect administrator → Direct admin should have access

→ Loss of physical Control →

→ proper implementations can't be examined.

↳ Control over all implementations. Low any area in your dad space.

Transparency (ref by Neal Leavitt)

Book Name :- Is cloud Computing Really Ready for prime time

- Almost 75% people are worried about security
- vulenerability to attack by IDC's Gens
- Confident.
- Audits

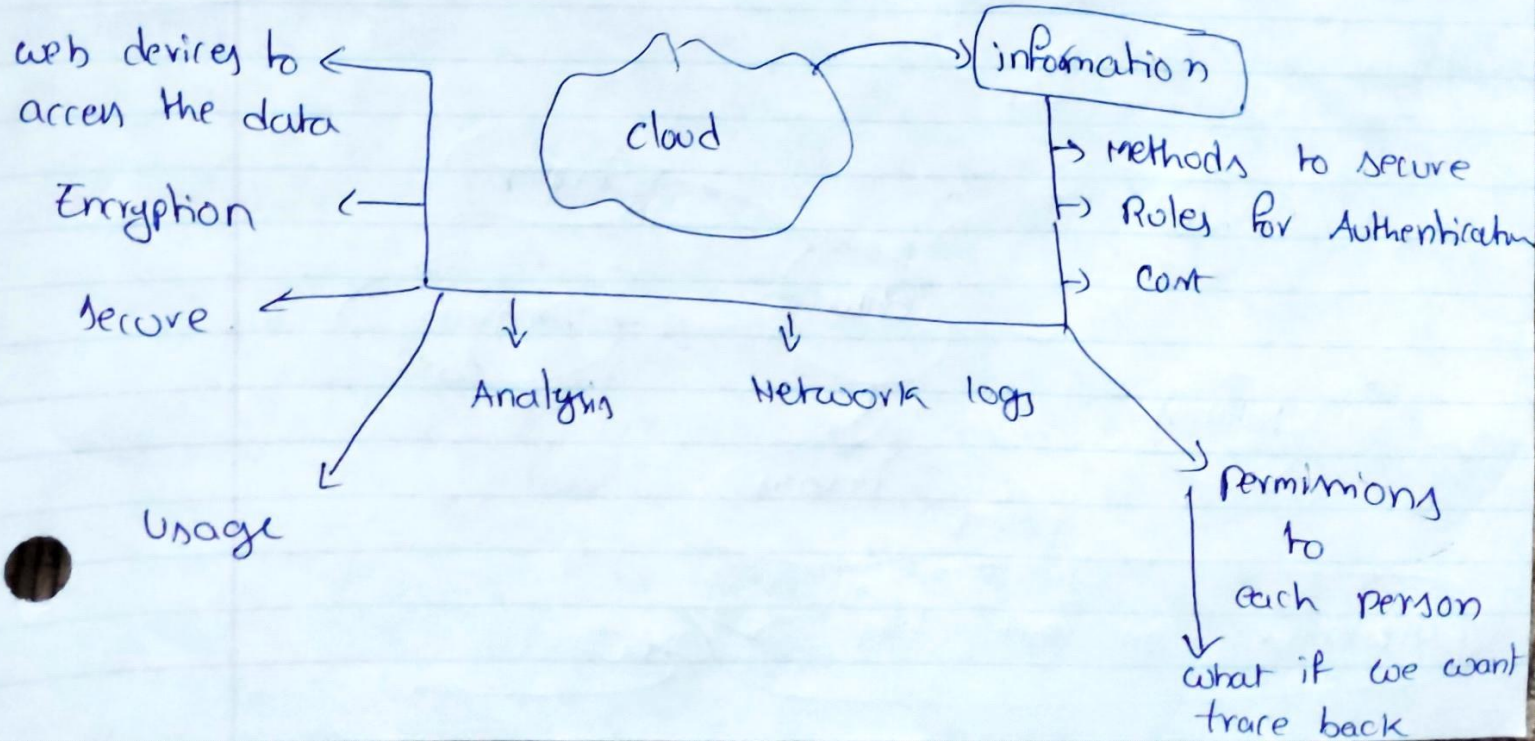
Reliability :- cloud space (or) client space should work 24/7 round the clock coz because recently Salesforce.com left customers without service for 6 hours on Feb 2008.

→ Aws Ec2 → 3 hours ~~after~~.

→ As per sheehan → more providers will come in feature.

24/06/2024

(ref by Ashish kumar, book Name :- world of Cloud computing & security)



Book Name :- Cloud Security issues (10/07/2021)

Service level Agreement → agreement between two parties

- identify, understanding
- areas of Conflict
- Expectations
- Complex issues

- Warranties
- Remedies
- Security
- Business continuity
- Disaster maintenance.

Termination :-

- end of initial term
- Convenience
- Any cause
- payment.

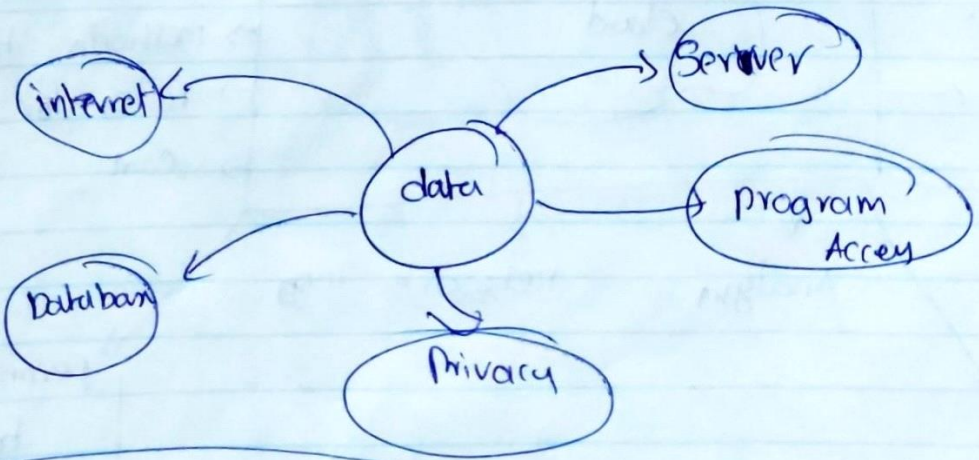
Security risks handled in SLA

- Privileged user access
- Regulatory Compliance
- Data location → segregation

Recovery

inv investigation support

Levels of Security



questions on each level

15/07/2021

Architecture ⇒ Build in tech specialists.

→ Identity & Access

→ Roles & Rules
→ diff access to each web page

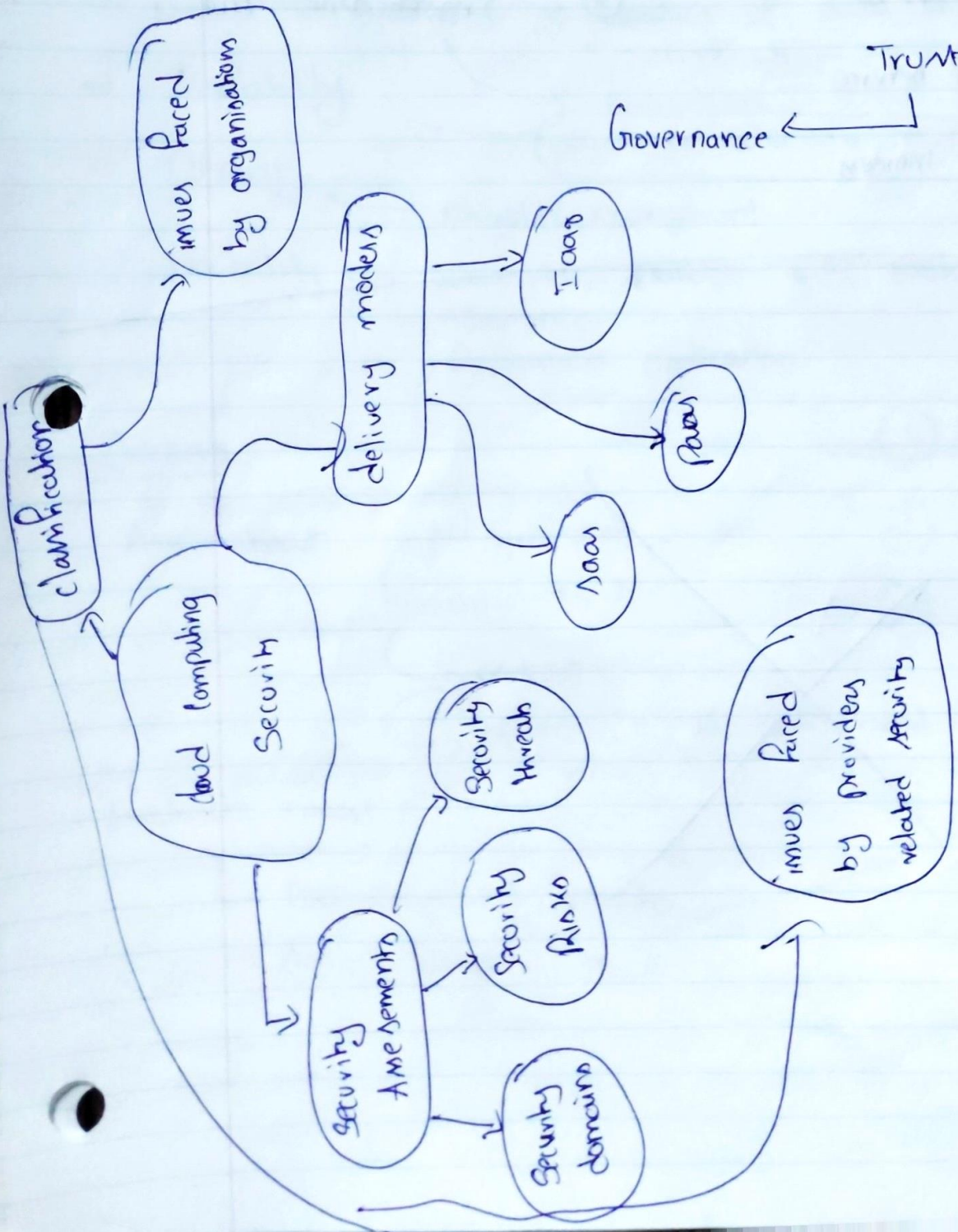
→ Availability ⇒ Reliability

→ response ⇒ outcome

→ Data protection

→ Trust

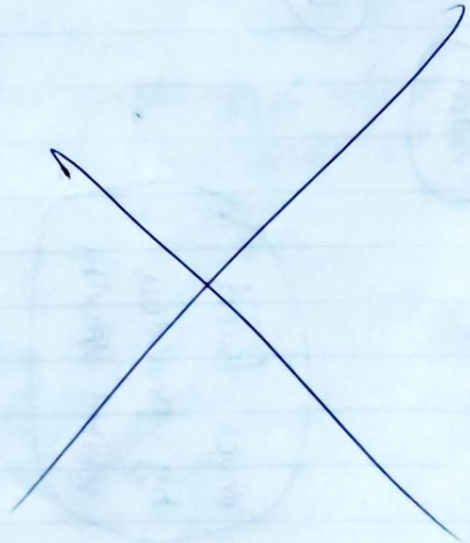
→ Governance



Nine critical threats mention in following book

↳ challenge in cloud Computing

1. Data Breaches
2. Data loss
3. Account Hijacking
4. Insecure API's
5. Denial of service
6. malicious insiders
7. Abuse of cloud services
8. Shared Technology
9. Insufficient due



Book :- Assessing the Security Risks of Cloud Computing (7)

Evaluate firm using following methods 24/07/2021

→ Privileged user Access → threats from outside organisation
  Server access
  network access
→ Compliance → regulations for new users
→ Data location → Privacy, regulations
→ Data segregation → location of data stored
  jurisdiction.
→ Availability → Encryption
→ Recovery → discussed already in previous
  → Disaster management
→ Viability → what if provider goes broke?
  Assurance
  Replacement application.

Access :-

Ask about → policymakers
→ architects
→ coders
→ operators to understand

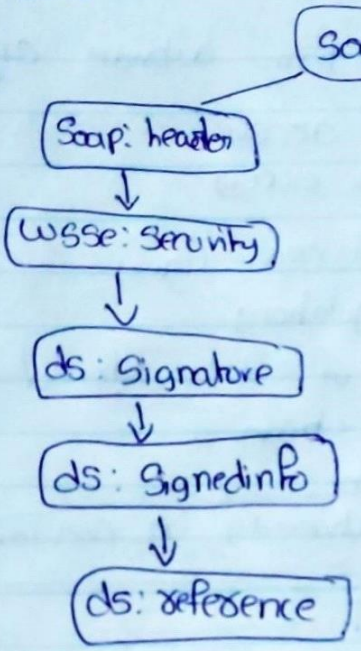
(1) Assurance
(2) Evaluate
(3) Security Assessment by third party

Evaluate risks

→ ISO standard 27001
→ Audit Standard NO. 70 X

Book :- On Technical Security issues in Cloud Computing (25/07/2

Security web-services



xml Signature main types of attacks are authentication (or) integrity.

Browser security :- Client and Server using on I/O devices

How to secure SAML Tokens

- TLS Federation
- Holder of key Assertion profile
- Strong locked same origin policy
- TLS Session binding

Flooding attacks :-

- serious drawbacks
- Excess Power Usage
- Severe troubles

(Direct and indirect) Denial of Service

Accounting × (already discussed)

Accountability → limits
→ flooding conditions

26/07/17

flooding attacks on Cloud Computing (Iaas)

Book :- attacks on web services

Attacks :- **Oversize payload**
→ its category of Denial of Service
→ high memory due to size
→ attack using large Soap message

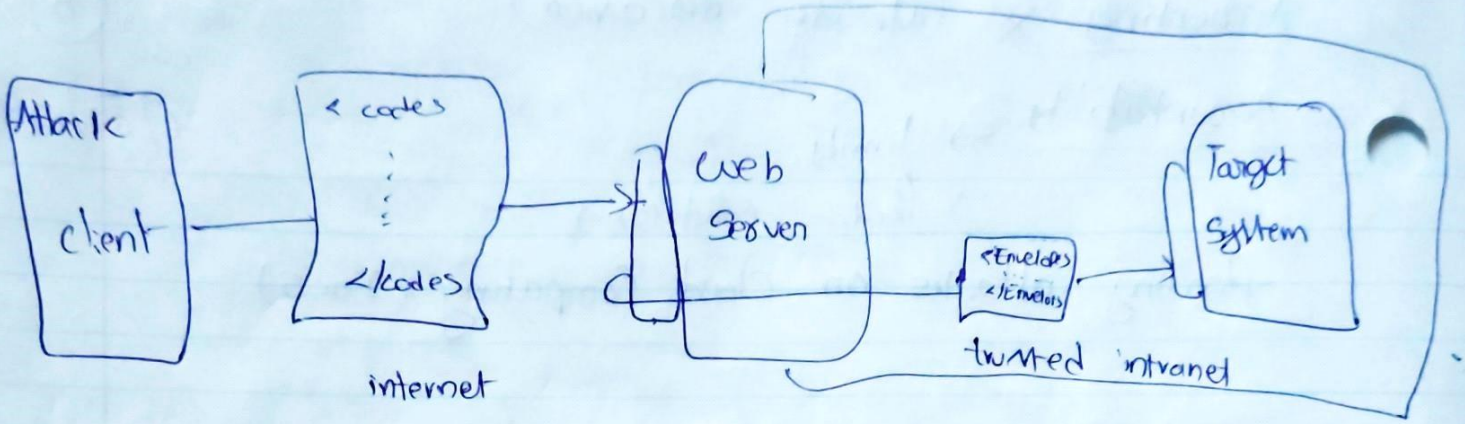
xml injection
→ trying to modify soap msg
→ special characters '<' '&' '>'

WSDL Scanning
→ avoid common WSDL for all WS
→ clear End point
→ omitted operations

Metadata spoofing
→ information in meta data
→ spoofing metadata
→ authenticate and check

ws-addressing spoofing
→ URL call back
→ BPEL engine will raise execution fault

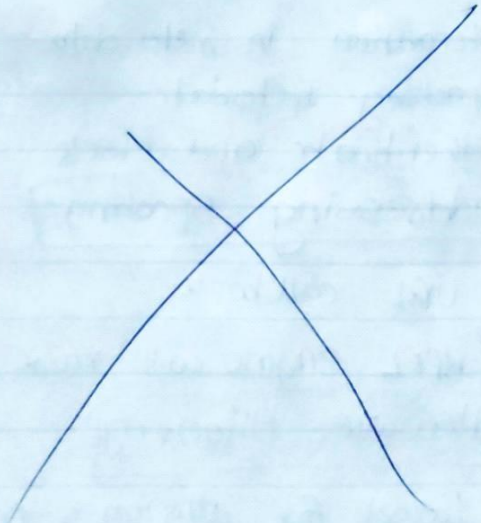
middleware Hijacking
→ target for attacker's Endpoint URL
→ invalid Soap
→ fault messages
→ indirect flooding



Countermeasure approaches

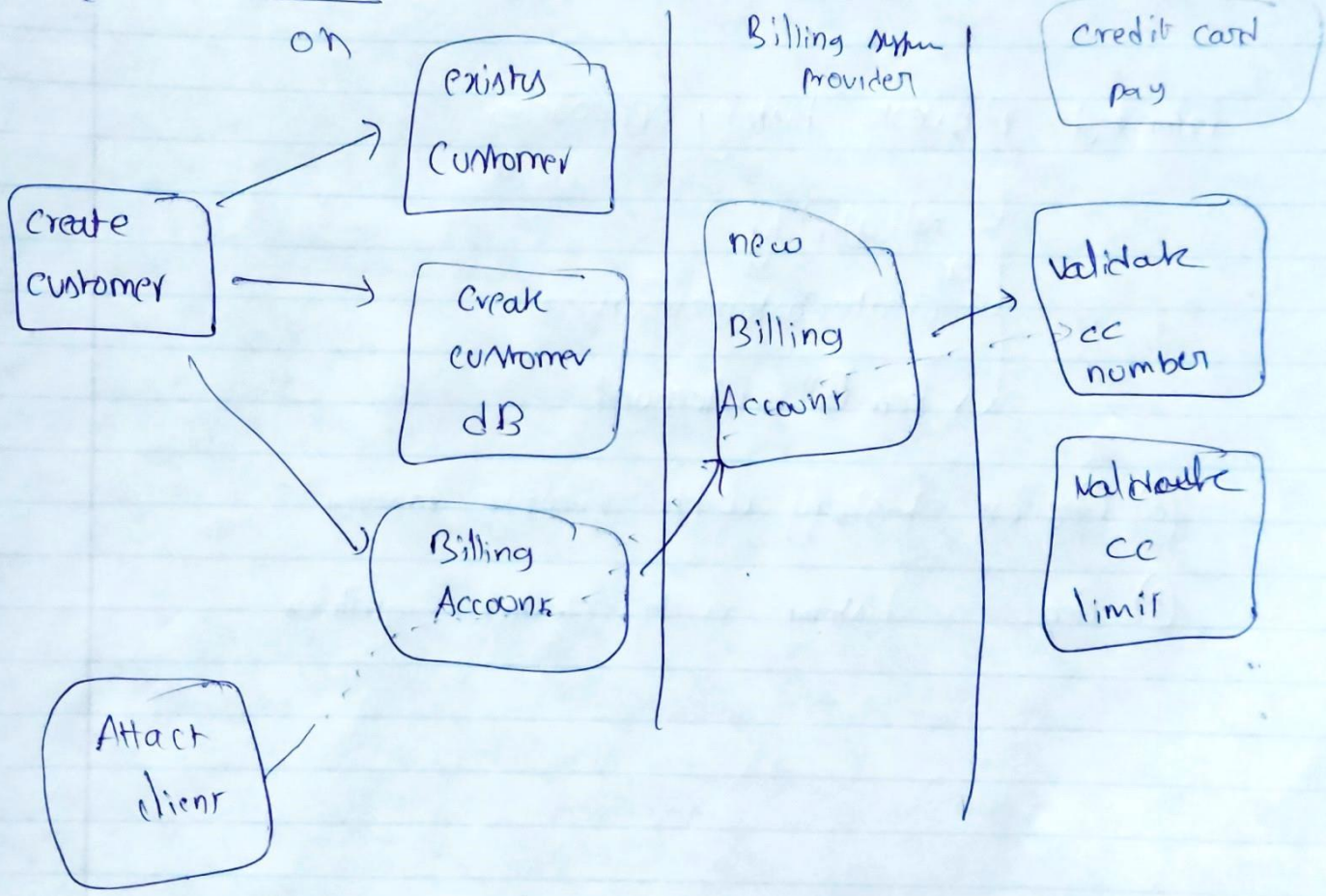
- → Schema validation
- → Schema hardening
- → Strict ws-Securitypolicy
- → Event based Soap
- → ws-Security

→ classification



Book:- Accountability problem of flooding attacks in Service oriented Architectures. 29/07/21

=> Flooding attacks on



monitoring :-
- Application maintainence
- log Archieve
- Disaster management

local logging Approach
- local logging/log file
- log entries that belong to attack requests.

29/02/2024

Request history approach

- → Small log files
- → history block
- → Examine same requests

Extended Request history approaches

- ↳ reliability
  - Ex:-
  - ↳ CreateCustomerService
  - ↳ newBillingAccount

(a) Request history with Security tokens

(b) Req. history with Digital Signatures.