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

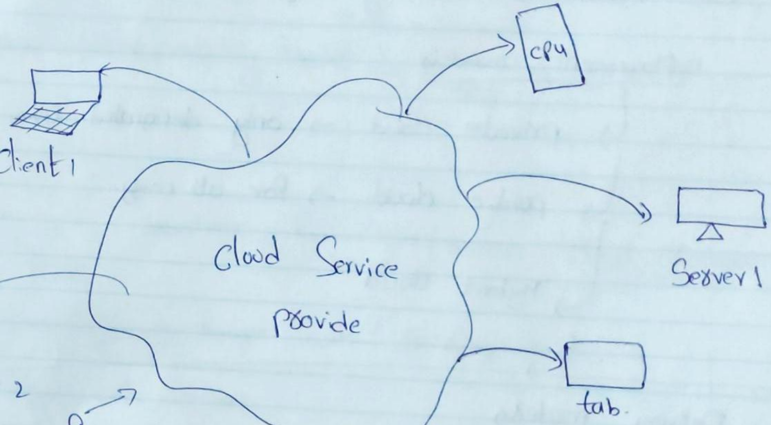


fig1 :- Basic cloud Network

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

03/0

Delivery models
- → Infrastructure as a Service (Iaas) → hardware servers, n device
- → platform as a Service (paas) → developement like Os,
- → Software as a Service (Saas) → ws, XML

3/06/2021

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 / loss of Control on Computing resources
5. Migrate → movement
6. Cloud interoperability issue → Hazy Cloud.

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

Cloud Computing is fraugt with Security risks

- * privileged user access
- * Regulatory Compliance
- * Data location
- * Recovery
- * Data Segregation
- * investigative support
- * long term viabilibity

2.a

3/06/2

Verasog Oraghadha

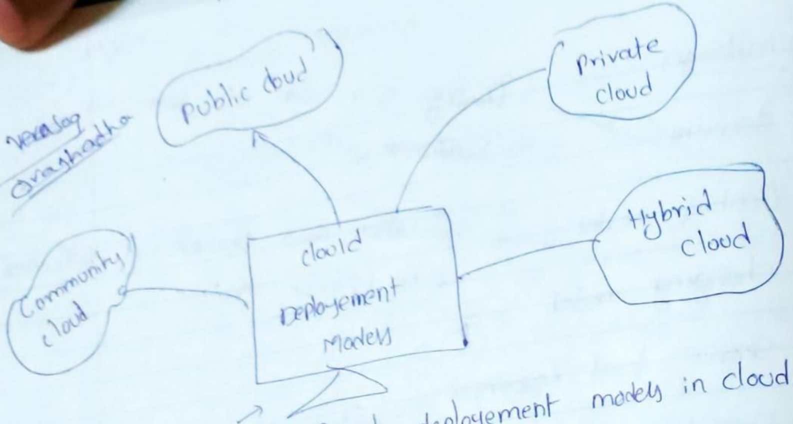


fig2: Different deployement models in cloud platfor

Denial of service

↳ Attack of web servers

Account hijacking

↳ HTTP protocol.

Investigation Support :-

↳ logs

↳ History/Access control

Vulnerabilities :-

3

7/06/21

-> key factor of security in vulnerability
-> its kind of risk factor

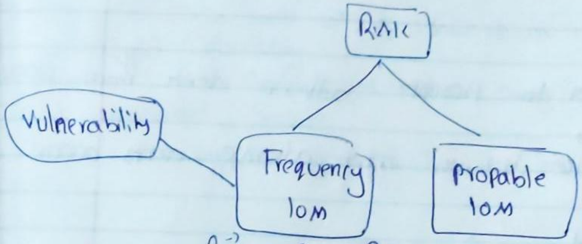
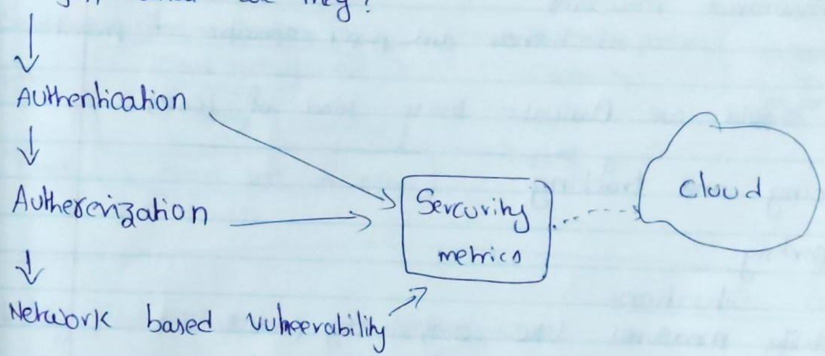


fig3:- Risk Factors

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



vulnerabilities in cloud Architechure

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

Network. Security -> How about other person logged on the same VM at same time

-> is there any n/w monitering

7/06/2

Risk :-

Amortized loss Expectation

Information Security:

- protection measures
  This aim to prevent adverse events from oc
- Detection measures
  Alert the business when adverse events occur
- Response measures
  Deals with consequences of adverse events
- Assurance measures
  effectiveness and proper operation of protectio

How should we Evaluate these kind of Risks

-> tracing and tracking

-> Reporting

Current Situation:-

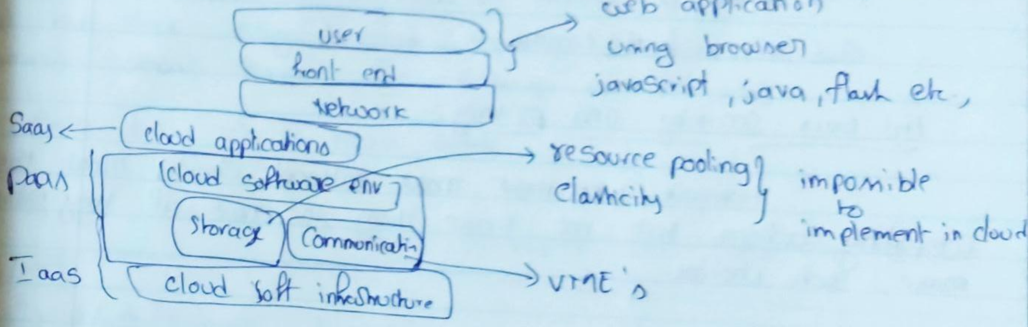
availability measures like acquiring (cost)
Managing
maintaining

Managing Risk :-

↳ liability transfer -> disclaims, transfers
↳ indentification -> 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 realized using homogenous infrastructure
-> measured Service
  => pay as you go business models.



20/06/21

Indentity, Authentication and Authorization

↳ Denial of Service by account lockout -> username & password
↳ weak credential reset mechanisms -> roles for forgetten 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

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:- make rational choices about t

Humans users must make them to choose if they ca

computing actions but not make them
make such choices.

General Security challenges

→ Trusting vendor's Security model → follow the rules

→ customer inability to respond to audit findings → Better to

the o/p

→ Support for investigations

→ Indirect administrator → Direct admin should have acc

→ Loss of physical Control →

→ proper implementations can't be examined.

↳ Control over all implementations (or any area

Transparency (ref by Neal Leavitt)

book Name:- is cloud Computing Really Ready for prime time

↳ {Allmost 75% people are worried about security
{vulnerability to attack by IDC's Gens
Confident
↳ Audits

Reliability:- cloud space (or) client space should work 24/7

and the clock why because recently salesforce.com left

stomers without service for 6 hours on feb 2008

→ Aws Ec2 → 3 hours ~~after~~

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

/06/2021

ef by Ashish kumar, book Name:- world of Cloud computing

security)

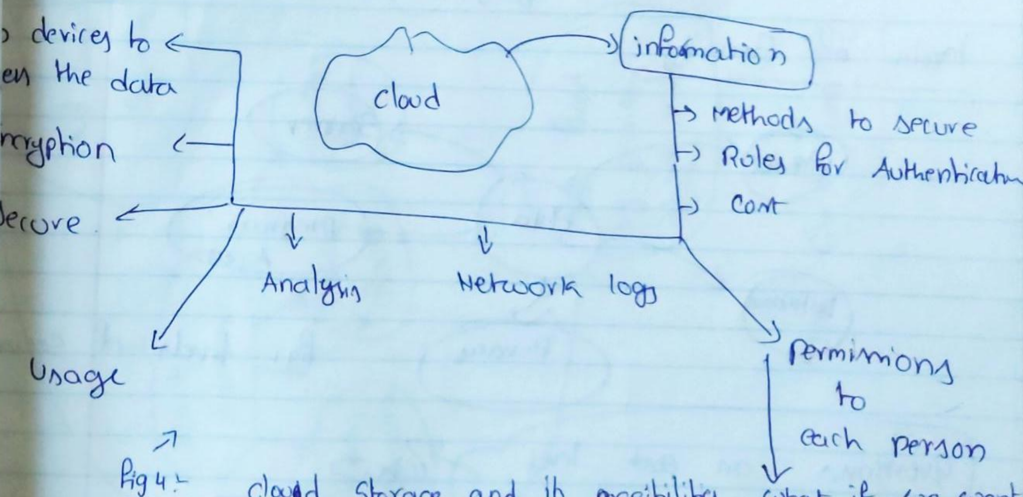


Fig 4:- cloud Storage and its possibilities of security

Cloud Security issues (10/07/2021)

Book Name :- Cloud Security

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
- → payments.

Security risks handled in SLA

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

Recovery

inv Investigation

levels of Security

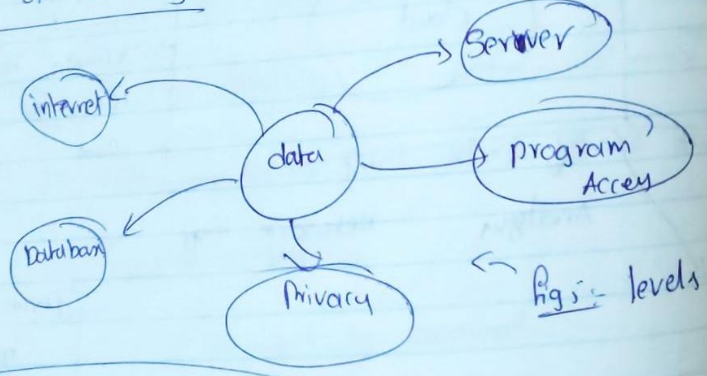


fig 5:- levels of s

Questions on each level

6

15/07/2021

Architecture ⇒ Build in tech specialist.

↳ Identity & Access

- → Roles & Rules
- → dift access to each web page

↳ Availability ⇒ Reliability

↳ response ⇒ outcome

↳ Data protection

Trust

Governance

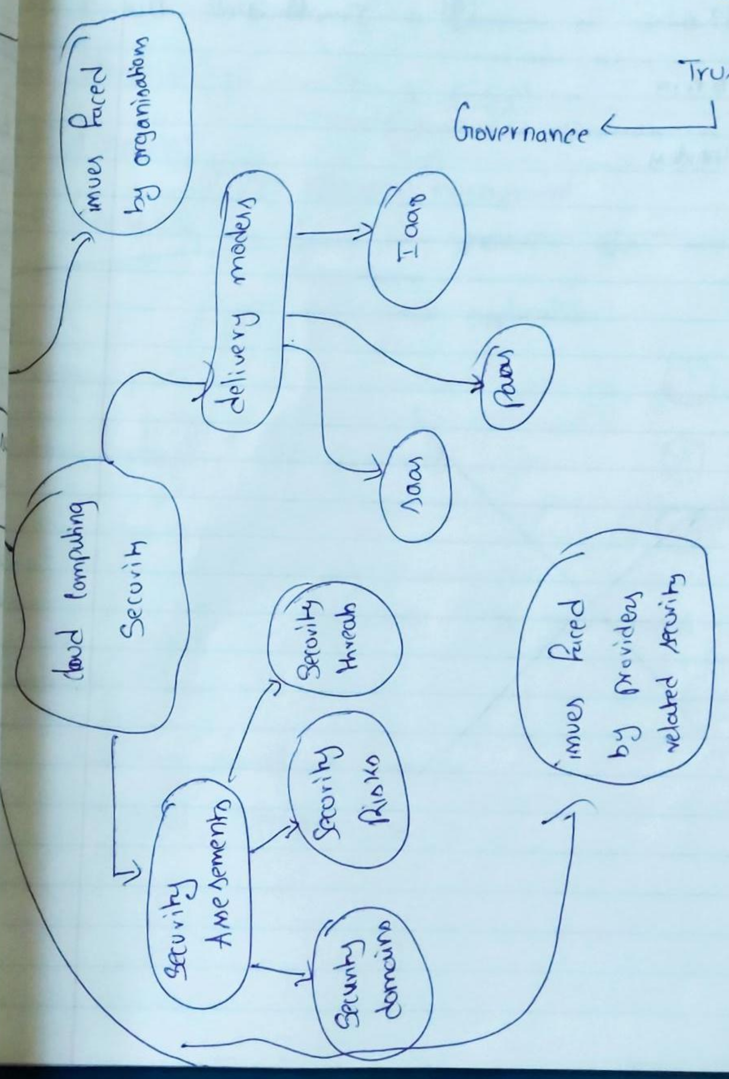


fig 6:- Cloud Computing Security Architecture

15/07/21

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 insides

(7) Abuse of Cloud services

(8) Shared Technology

(9) Insufficient due

Books :- Assesing the Security Risks of Cloud Computing

24/07/2021

Evaluate first using following methods

→ Privileged user Access → threats from outside organisation
Server access
network access

→ Compliance → regulations for new Users
Privacy, regulations

→ Data location → location of data stored
Jurisdiction.

→ Data Segregation → Encryption

→ Availability → discussed already in previous

→ Recovery → 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 → Security Assessment by third party

→ Audit Standard NO. 70 X

Book :- On Technical security issues in Cloud Computing

Security web-services

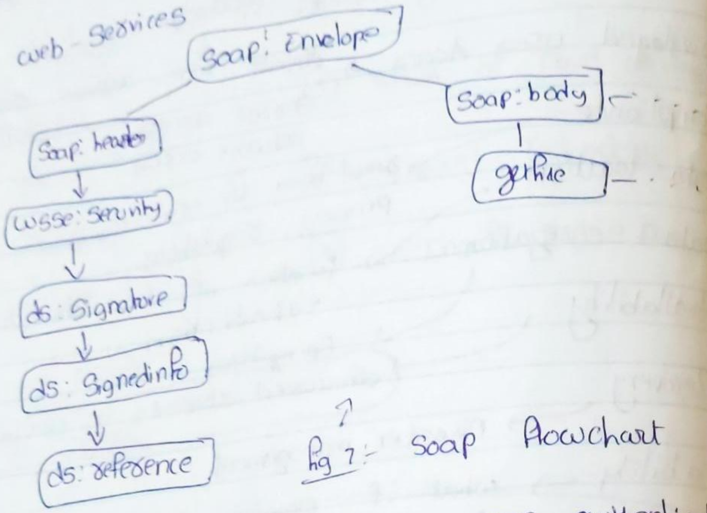


fig 7 :- Soap flowchart

xml Signature main types of attacks are authenticati

(or) integrity.

Browser security :- Client and server using on I/O

How to secure SAML Tokens

TLS Federation

Holder of key Assertion profile

Strong locked same origin policy

Flooding attacks :-

- serious drawbacks
- Excess power usage
- Severe troubles

(Direct and indirect) Denial of Service

26/07/21

Accounting X (already discussed)

Accountability → limits
→ flooding conditions

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 '<' (or) '>'

WSDL Scanning

- avoid common WSDL for all WS
- Clear End point
- omitted operations

Metadata spoofing

- information in meta data
- spoofing metadata
- authenticate and check

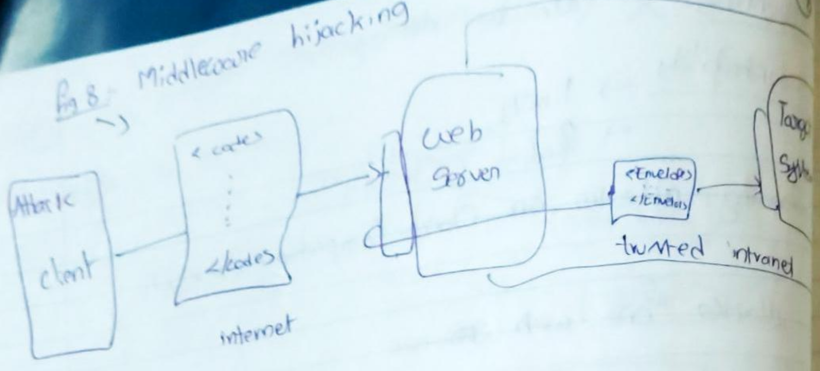
WS-addressing spoofing

- URL call back
- BPEL engine will raise execution fault

middleware Hijacking

- target for attacker's Endpoint URL
- invalid Soap
- fault messages
- indirect flooding

Fig 8- Middleware hijacking



Countermeasure approaches

-> Schema validation

-> Schema hardening

-> Strict ws- Security policy

-> Event based Soap

-> ws- Security

-> classification

-> 20

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

-> Flooding attacks

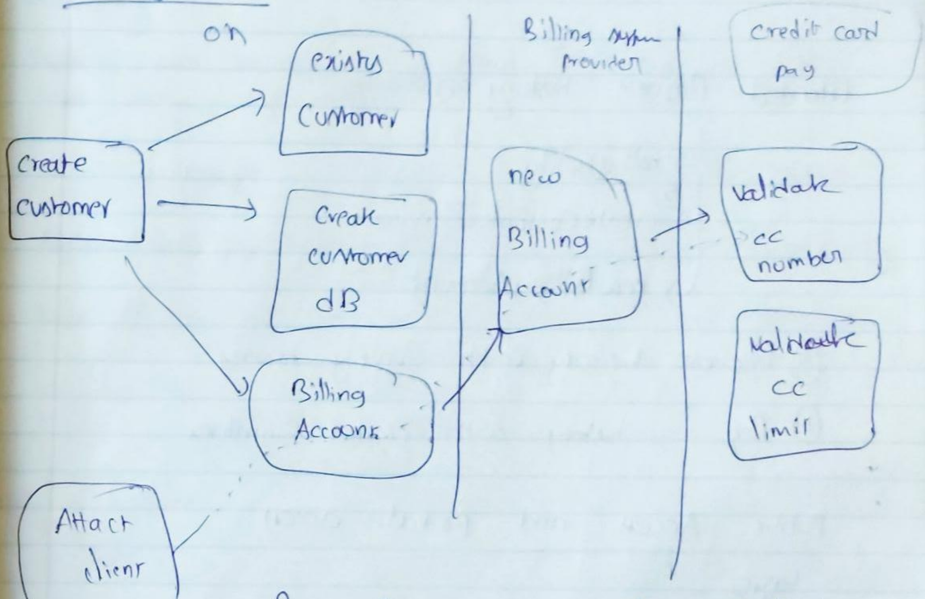


fig 9 :- flooding attacks flow in cloud

ronitoring :- → Application maintainence
→ log Archieve
→ Disaster management

al logging Approach
→ local logging/log files
→ log entries that belong to attack requests.

Request history approach

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

Extended Request history approaches

- reliability
- a. Create Customer Service
- new Billing Accoont

(a) Request history with Security tokens

(b) Req. history with Digital Signatures.

Public Accen and private accen

Keys

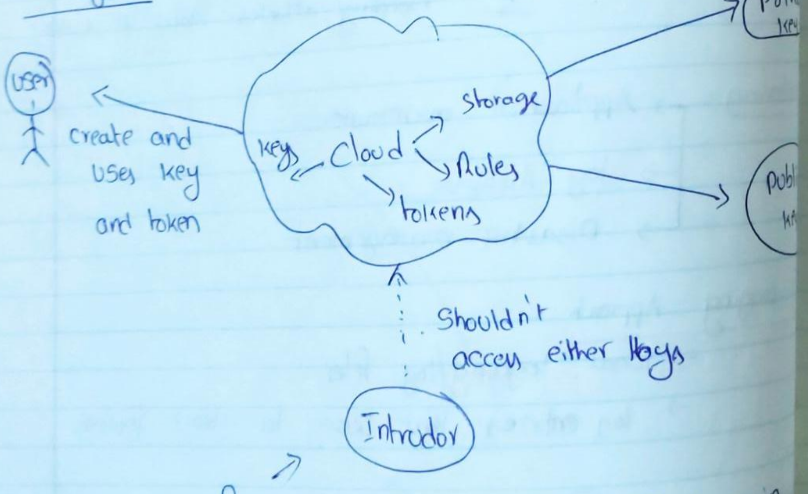


Fig 10 :- Security keys architecture in Cloud platform

Article :- 5 Biggest cloud Computing trends in 2021 7/08/21

-> AI will improve the efficiency and speed of cloud Computing

-> Gaming will increasingly delivered from the cloud, just like music and movies.
    - Example :- Amazon live Streaming for sports

-> Hybrid and on-premise cloud Solutions grow in popularity

-> more of us will be working on virtual cloud desktops
    - desktop as a Service
        - offered by AWS, Azure

Usage on Desktop as a Service

- pay on use
- key management
- Roles
- Software mangement
    - Servers
    - Data Storage
    - cpu
- Public IP Addren (pay on use)
    - No pay if no use of IP addren