UNIT-5 DSCC

Trust, Reputation & Security Management:

Trust: refers to belief of one peer on another, based on his direct experiences with peer

Reputation: a collective opinion on a peer by other peers based on recommendations.

Trust Matrix for computing reputations:

$M(t) = m_{ij}(t)$

⇓

local score issued by node i in evaluating node j at a time t.

Reputation vector

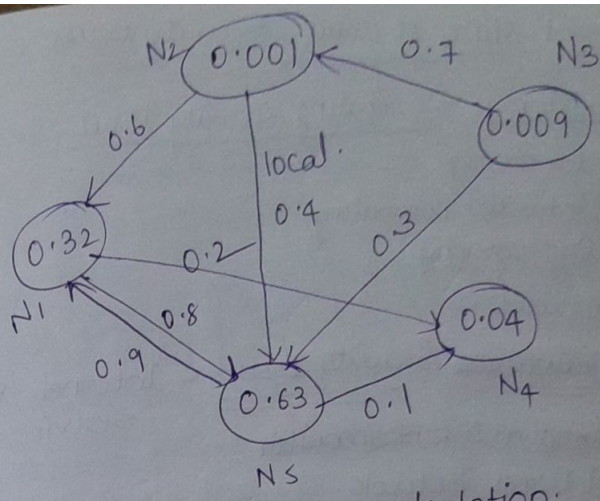
$V(t) = \{v_1(t), v_2(t), v_3(t), v_4(t), v_5(t)\}$

$= \{0.32, 0.001, 0.009, 0.04, 0.63\}$

$$M(t) = \begin{bmatrix} 0 & 0 & 0 & 0.2 & 0.8 \\ 0.6 & 0 & 0 & 0 & 0.4 \\ 0 & 0.7 & 0 & 0 & 0.3 \\ 0 & 0 & 0 & 0 & 0 \\ 0.9 & 0 & 0 & 0.1 & 0 \end{bmatrix}$$

→ All fractions in the range (0, 1)

0 → no trust 1 - 100 → trust.



→ Global reputation score calculation:

for Node N5:

$$v_5(t+1) = m_{15}(t) \times v_1(t) + m_{25}(t) \times v_2(t) + m_{35}(t) \times v_3(t)$$

$$= 0.8 \times 0.32 + 0.4 \times 0.001 + 0.3 \times 0.009 = 0.2573.$$

$$V(t+1) = \{v_1(t+1), v_2(t+1), v_3(t+1), v_4(t+1), v_5(t+1)\}$$

$$= \{0.5673, 0.0063, 0, 0.1370, 0.2573\}.$$

* Design objective of Reputation Systems:

1. High Accuracy
2. Fast Convergence Speed.
3. Low overhead
4. Adaptive to peer dynamics
5. Robust to malicious peers.
6. Scalability

→ Current state of cloud security issues

* Data storage & computing security issues:
  → Data storage
  → Untrusted computing
  → Cryptography
  → Malware.

* ~~Virtualization~~ Security Issues = Internet & services.
  → ~~Virtual machine monitor~~
  → Internet Protocols.
  → Web services
  → Web technologies

* Virtualization issues:
  → Virtual Machine Monitor
  → Malware
  → Mobility
  → Network virtualization

* Network security issues & Access & control issues:
  → Mobile platforms
  → Physical access
  → user credentials
  → Authorization.

* Software security issues:
  → platform & frameworks
  → user frontend.

* Cloud Security:

→ Security models are based on various SLAs between providers & users.

→ 3 basics cloud security environments:
  * facility security in data centers demands on-site security yr round.
  * Network security demands fault-tolerant external firewalls, intrusion detection systems (IDSes) and third party vulnerability assessment.
  * platform security demands SSL & data decryption, strict password policies & system trust certification.

→ Cloud components that demand special security protection:
  * Protection of servers from malicious software attacks such as worms, viruses & malware.
  * Protection of hypervisors (or) VM monitors from software-based attacks & vulnerabilities.
  * Protection of data & info. from theft, corruption, and natural disasters.
  * Providing authenticated & authorized access to critical data.

→ CIA triad helps for cloud security
  ⇓
  Confidentiality, Integrity, Availability

* Identity and Access Management:

→ Enables the right individuals to access the right resources at the right times for right reasons.

→ Single Sign On is a property of access control of multiple related, but independent systems.

→ IAM means management of individual users, their authentication, authorization, privileges.

*→ Myths & Misconceptions:

→ IAM is too big and complex.
→ If users are trustworthy, you don't need IAM.

*→ Benefits:

→ Reduced help desk costs & improved service.
→ Eliminated security threat
→ Scaling of administrative staff.
→ Reduced security risk, auditing costs
→ accuracy.

*→ Identacor: IAM solution.

→ cutting edge cloud security
→ fast & easiest access possible.
→ maximize user experience
→ supports all web apps which support Security Assertion Markup language (SAML) authentication standard.

* Why? IAM?

→ Weak Passwords
→ Centralized Access Control
→ Multi-factor authentication.
→ Phishing & Spear phishing

} Security

→ Single Sign On
→ Integrated Apps
→ Application Management
→ Password reset

} Productivity

→ Single identity
→ Streamline Passwords / Eliminate Passwords.
→ Data analytics & audits

* Federated Cloud Computing:

Issues of Cloud Computing:

→ Limited Scalability
→ Lack of interoperability
→ No built-in business service management.

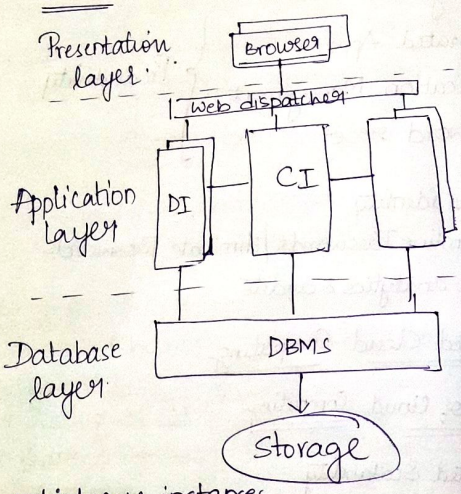
*→ To address these issues; a model for business-driven federation of cloud computing providers is presented; where each provider can buy & sell on-demand.

* SAP Systems:

→ used for variety of business apps.

→ SAP system components consists of generic parts customized by configuration & parts custom coded for a specific installation.

→ 3 tier:



DI → dialogue instances

CI → central instance

* ~~Federated cloud~~

* Virtualized data center:

→ Consider a data center that consolidates the operation of different types of SAP applications.

→ the data centre is offered by the IT department of an enterprise for internal users.

→ Typical aspects of virtualized data centers:
Infrastructure provider must manage the life cycle of the application for hundreds (or) thousands of customers, while keeping a very low total cost of ownership.

→ Primary Requirements:

1. Automated and fast deployment.
2. dynamic elasticity
3. Automated continuous optimization.

→ Model for federated cloud computing:

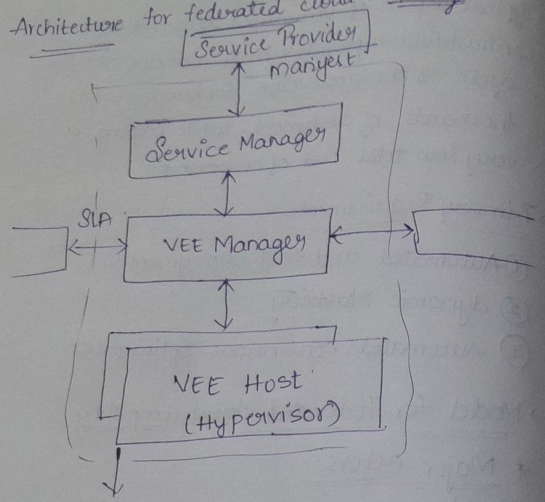
* Major actors:
  - → Service Providers (SPs):
    - → are entities that need computational resources to offer some service.
    - → Resources are leased from Infrastructure providers (IPs)
  - → Infrastructure providers (IPs).

* Service Applications:
  - ↳ a set of software components that work collectively to achieve a goal.

Each Service app is dedicated to VEE.

VEE: Virtual Execution Environment.

Architecture for federated cloud computing:



→ Service Manager: interacts with SPs.
  ↳ 2 complex tasks:
    → deploying & versioning VEEs
    → monitoring & enforcing SLA.

→ VEE Manager: Responsible for placement of VEE and VEEH.

→ VEEH: responsible for the basic control & monitoring of VEEs & their resources.

* Features of Federation Types:

① Framework agreement support
② Opportunistic placement support.
③ Advanced resource reservation support.
④ Federated migration support.
⑤ Cross-site network support
⑥ Public IP addresses retention
⑦ VMI operation support.

* Federation Scenarios:
  → Baseline federation
  → Basic federation
  → Advanced "
  → Full featured.

* Internal Threats
  → 2 virtual zones
  ① Control: Service Manager, VEEM, SMI/VMI interfaces (trusted area)
  ② Execution: VEEH, VEEM, network storage, SI.

Threats:

① linked to authentication/communication of SPs.
② threats related to misbehaviour of service resource allocation.
③ storage data compromising
④ data partitioning b/w VEE.
⑤ compromise data privacy.

→ RESERVOIR site has guaranteed types of isolations: Runtime, Network, Storage &