Project Title:
Distributed and Cloud-based Network Defense System for NRENs (DCNDS)

Series 1 Workshop

(10 –11 April, 2019)

Workshop on Cloud-based Web Security Best Practices and System Configuration Overview

ASIACONNECT
DISTRIBUTED AND CLOUD-BASED NETWORK DEFENSE SYSTEM FOR NRENs

European Union

Asi@Connect

TEIN
COOPERATION CENTER

by

Md. Saiful Islam

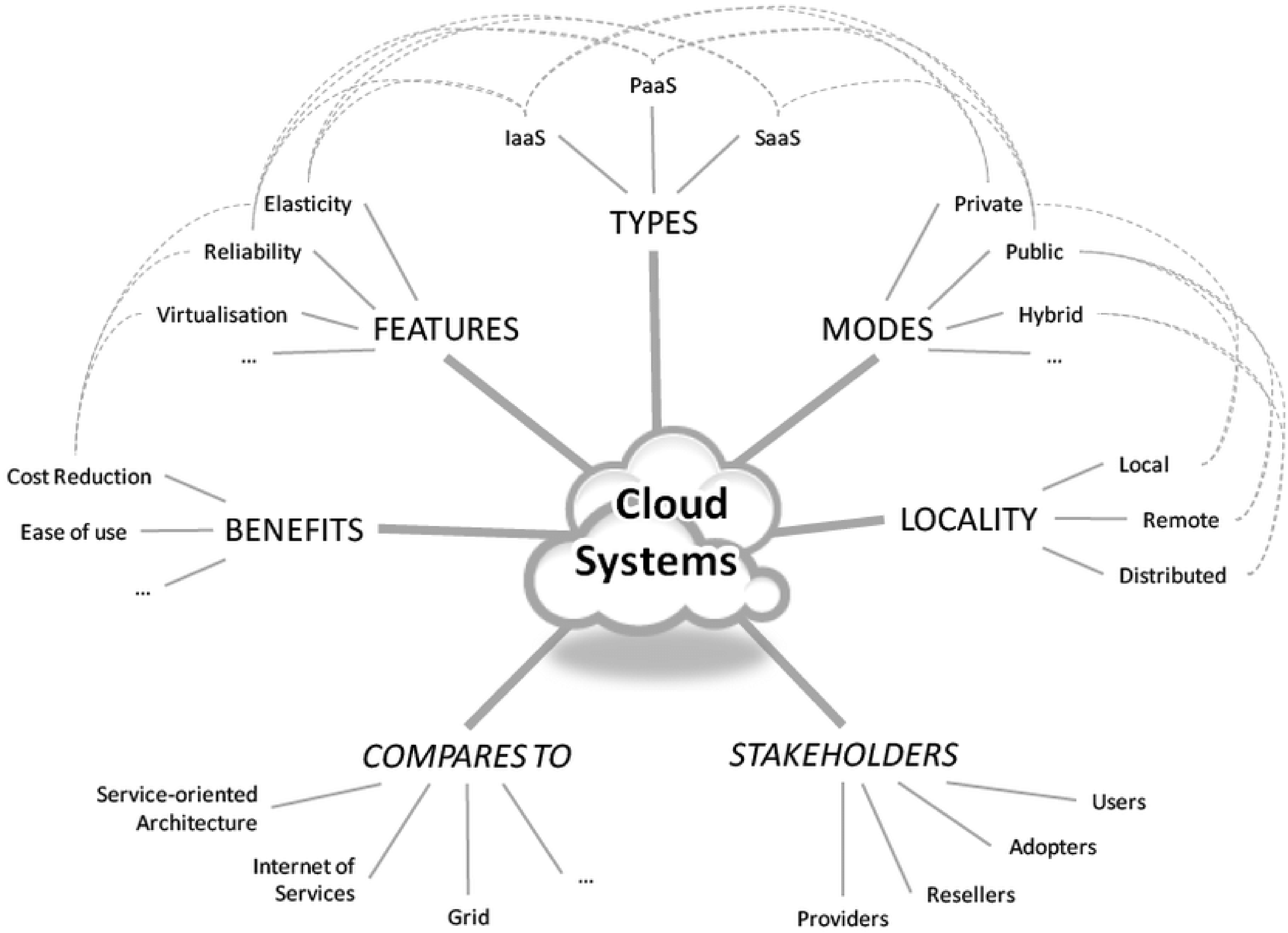
Institute of Information and Communication Technology
Bangladesh University of Engineering and Technology

ASIACONNECT
DISTRIBUTED AND CLOUD-BASED
NETWORK DEFENSE SYSTEM
FOR NRENs

European Union

Asi@Connect

TEIN
COOPERATION CENTER


PaaS
IaaS
SaaS
TYPES
Elasticity
Reliability
Virtualisation
...
FEATURES
Private
Public
Hybrid
...
MODES
Cost Reduction
Ease of use
...
BENEFITS
Cloud Systems
LOCALITY
Local
Remote
Distributed
COMPARES TO
Service-oriented Architecture
Internet of Services
Grid
...
STAKEHOLDERS
Users
Adopters
Resellers
Providers

Outline

- Challenges of cloud computing,
- Security triad and security threats in cloud
- Security issues in cloud,
- Categorization of attacks based on cloud components.

Challenges of Cloud Computing

Like any new technology, the adoption of cloud computing is not free from issues.

Some of the most important challenges are as follows:

1. **Security and Privacy**
2. **Interoperability and portability**
3. **Reliability and availability**
4. **Performance and bandwidth cost**
5. **SLA & service quality**
6. **Lack of knowledge and expertise**
7. **Recovery and loss of data**
8. **Vendor Lock-in**

Cloud Computing is **a security nightmare** and it can't be handled in traditional ways.

John Chambers
Former CISCO CEO

Security and Privacy

- How the businesses address the security and privacy concerns thinking of adopting it? Important!
- The valuable enterprise data will reside outside the corporate firewall **raises serious concerns**.

- Hacking and various attacks to cloud infrastructure would affect multiple clients even if only one site is attacked.

Interoperability and Portability

- The industry lacks standards for APIs and cloud interfaces, interoperability standards, and associated technical standards that allow interoperability of private to private clouds, public to private clouds, and so on.

- Portability refers to the ability of an application to move across environments, not just across platforms. Portability is a form of reusability.

- Due to lack of portability enables the migration of cloud services from one cloud provider to another or between a public cloud and a private cloud is difficult.

Reliability and availability

- Cloud outages experienced by its providers such as *Google and Amazon* are well documented and publicized.
- This has discouraged potential organizations who were thinking of moving into the cloud environment.
- Cloud computing is a trust-based technology where lack of trust inhibits its adoption.

Performance & bandwidth cost

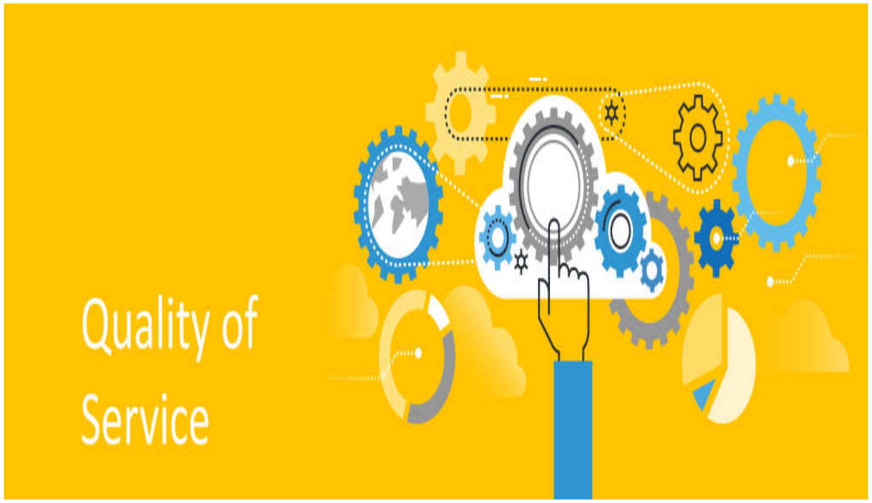
- Any enterprises adopting cloud computing services certainly expect the kind of improved performance that an elastic computing environment should provide.
- Businesses can save money on hardware but they have to spend more for the bandwidth.
- This can be a low cost for smaller applications but can be significan

- But cloud services are not perfect. Questions about performance are sure to arise in even the most efficient, well-designed cloud environment.

Service Quality and SLA

- Service quality is also one of the biggest factors considered by enterprises and for this reason, they don’t shift their business application to the cloud.
- Though there is an SLA, clients fear that the cloud service providers do not provide any guarantee to ensure product applications security keeps the organizations away from having it.

- QoS approaches in cloud computing have become an important topic in the cloud computing area and there remain open challenges and gaps which require future research exploration.



ASIACONNECT
DISTRIBUTED AND CLOUD-BASED
NETWORK DEFENSE SYSTEM
FOR NRENs

European Union

Asi@Connect

TEIN
COOPERATION CENTER

Lack of Knowledge and expertise

- Every organization does not have sufficient knowledge about the implementation of the cloud solutions.
- organizations have not expertise staff and tools for the proper use of cloud technology.

- Despite growth in adoption, a cloud skills gap still exists.

- Firms hunt for candidates with more specialized skills related to public cloud and open source platforms.

Recovery of Lost data

- The potential financial impact from losing customer trust is so high on the threats list.
- Cloud services faces issue of data loss.
- A proper backup policy for the recovery of data must be placed to deal with the loss.

  - Vendors must set proper infrastructures to efficiently handle with server breakdown and outages.

DATA RECOVERY
PC PHONE ACCESS WORLD
INFRASTRUCTURE REMOTE BUSINESS
SECURITY SERVER TABLET
INTERNET IMPORTANT TECHNOLOGY MANAGEMENT MOBILITY DATA
KNOWLEDGE INFORMATION REMEMBER
WORLD NETWORK LAPTOP
TECHNOLOGY REMOTE MOBILE PC TECHNOLOGY
WORKSTATION WORLD DESKTOP MOBILITY
NETWORKING EMAIL TECHNOLOGY NETWORK
INFRASTRUCTURE DESKTOP MOBILITY NETWORKING
WORLD BUSINESS COMPUTER MOBILE SYSTEM SECURITY WORLD
COMPUTING WORKSTATION WORLD DESKTOP

Vendor Lock-In

- The **vendor lock-in** is the situation where customers are dependent on a single **cloud provider** technology implementation and cannot easily move in the future to a different **vendor** without substantial costs, legal constraints, or technical incompatibilities.

- Vendor lock-in is a major barrier to the adoption of cloud computing, due to the lack of standardization.

  - For companies that come to rely heavily on public and hybrid cloud platforms, there is a danger that they become forced to continue with a specific third-party vendor simply to retain operational capacity.

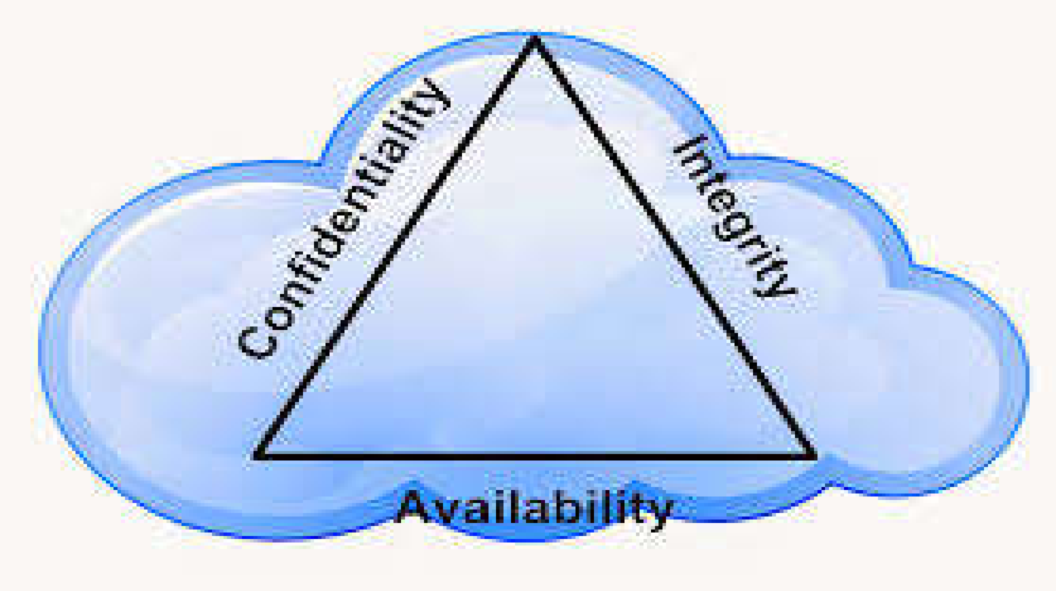
Security triad (CIA) in cloud

- Security can be defined as -

  -***"The state of being free from danger or threat"***

  -***"Security is the right not to have one's activities adversely affected via tampering with one's objects."***

- **3-key requirements for any secure system are:**



Confidentiality

- Fear of loss of control over data-
  - Will the sensitive data stored on a cloud remain confidential?
  - Will cloud compromises leak confidential client data?
- Will the cloud provider itself be honest and won’t peek into the data?

Sources of breaching confidentiality

1.Inside user threats

- SaaS – cloud customer and provider administrators
- PaaS- application developers and test environment
- managers
- IaaS- third party platform consultants

2. External attacker threats

- Cloud providers with large data stores holding credit card details, personal information and sensitive government or intellectual property, will be subjected to attacks from groups, with significant resources, attempting to retrieve data.
- This includes the threat of hardware attack, social engineering and supply chain attacks by dedicated attackers.

3. Data leakage

- A threat from widespread data leakage amongst many, potentially competitor organizations, using the same cloud provider could be caused by human error or faulty hardware that will lead to information compromise

Integrity

- In case of human – integrity is the quality of being honest and having strong moral principles.

- How do I know that the cloud provider is doing the computations correctly?

- How do I ensure that the cloud provider really stored my data without tampering with it?

Sources of breaking Integrity

1. Data Segregation

- The integrity of data within complex cloud hosting environments could provide a threat against data integrity if system resources are effectively not segregated.

2. User Access

- Implementation of poor access control procedures creates many threat opportunities

3. Data quality

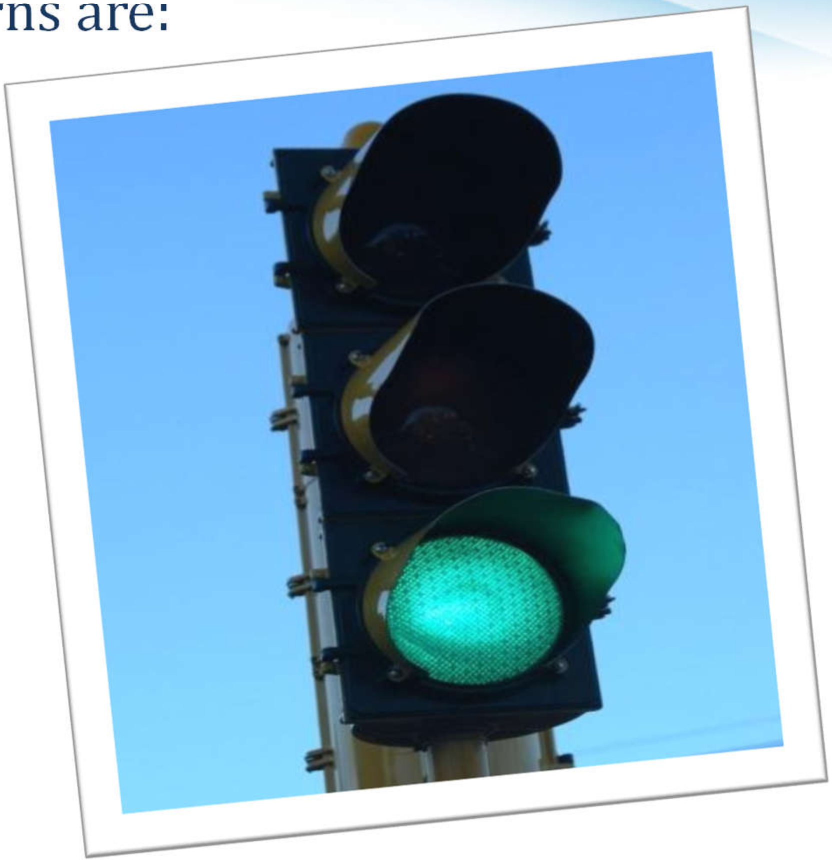
- The introduction of a faulty or mis-configured component required by another cloud user could potentially impact the integrity of data for other cloud users sharing infrastructure.

Availability

- Its ensure that required **data** is always accessible when and where needed within an organization's IT infrastructure, even when disruptions occur. The concerns are:

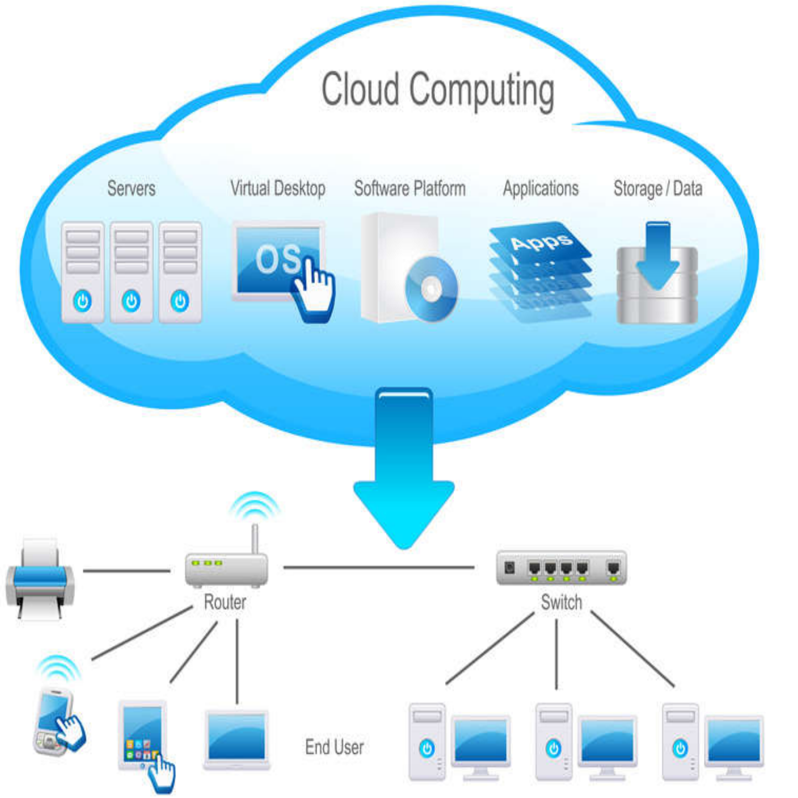
- Will critical systems go down at the client, if the provider is attacked in a Denial of Service attack?
- What happens if cloud provider goes out of business?
- Would cloud scale well-enough?
- Often-voiced concern-

  Although cloud providers argue their downtime compares well with cloud user's own data centers



Causes of unavailability

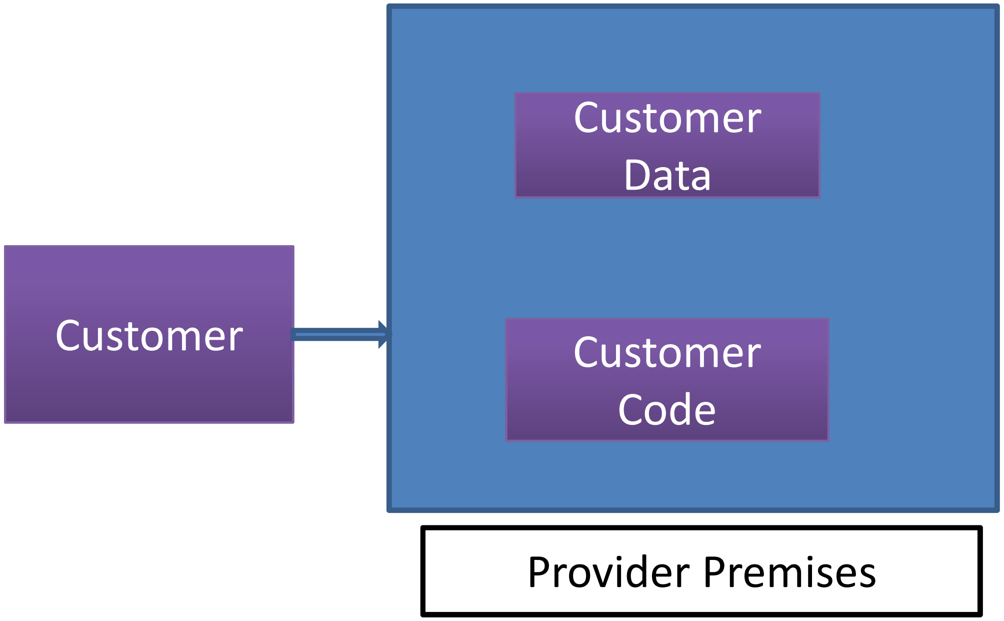
1. Change management,
2. Denial of service threat,
3. Physical disruption,
4. Exploiting weak recovery procedures



Cloud Security !! A major Concern

- Security concerns arising because both customer data and program are residing at Provider Premises.

- Security is always a major concern in Open System Architectures (OSA).



Why Cloud Computing brings new threats?

- Traditional system security mostly means keeping bad guys out.
- The attacker needs to either compromise the auth/access control system, or impersonate existing users.

- Cloud Security problems are coming from :
  - **Loss of control**
  - **Lack of trust (mechanisms)**
  - **Multi-tenancy**

Why Cloud Computing brings new threats?

Consumer's loss of control:

- Data, applications, resources are located with provider.
- User identity management is handled by the cloud.
- User access control rules, security policies and enforcement are managed by the cloud provider.
- Consumer relies on provider to ensure-
  - **Data security and privacy**
  - **Resource availability**
  - **Monitoring and repairing of services/resources**

Cloud Computing brings new threats: SLA

- The on-demand service or utility-based economic model necessitates the use of well-established service level agreements (SLAs).
- An SLA is a part of a service contract between the consumer and provider that formally defines the level of service. **It records a common understanding about services, priorities, responsibilities, guarantees and warranties.**

- Therefore, the main issue for cloud computing is to build a ***new layer to support a contract negotiation phase between service providers and consumers and to monitor contract enforcement*** for building trust to the clients.

service requirements
SLA
provider
client
service delivery

ASIACONNECT
DISTRIBUTED AND CLOUD-BASED NETWORK DEFENSE SYSTEM FOR NRENs

European Union

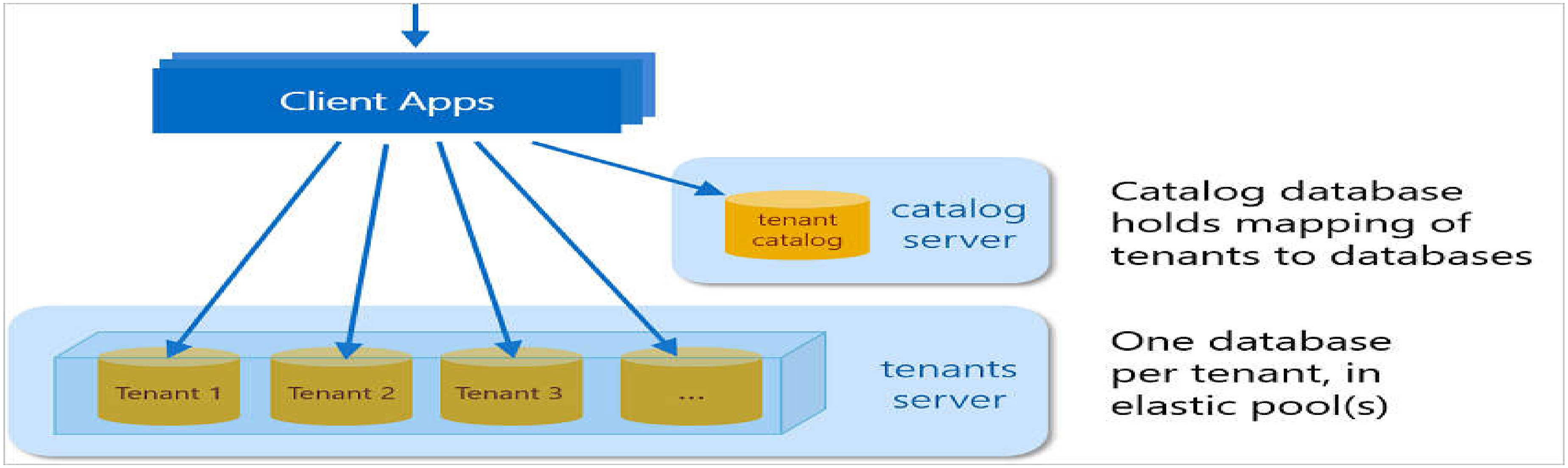
Asi@Connect

TEIN COOPERATION CENTER

Why Cloud Computing brings new threats?

Multi-tenancy :

- Multiple independent users share the same physical infrastructure
- So, an attacker can legitimately be in the same physical machine as the target



Catalog database holds mapping of tenants to databases

One database per tenant, in elastic pool(s)

Security Issues in Cloud

- A security issue is something happening in any assets attacks, misconfiguration, fault, damage, loopholes, and weakness in the system.
- The security issues may be categorized in eight parts as:

i) Data storage and computing security issues,

ii) Virtualization security issues,

iii) Internet and services related security issues,

iv) Network security issues,

v) Access control issues,

vi) Software security issues,

vii) Trust management issues &

viii) Compliance and legal aspects.

Data storage and computing security issues

- Data is a vital part of cloud computing.
- Data stored in the cloud is isolated and inscrutable to the customers.
- data should be consistent during computation, confidential at every stage of processing and perpetually stored to update the records.
- **Issues are:**

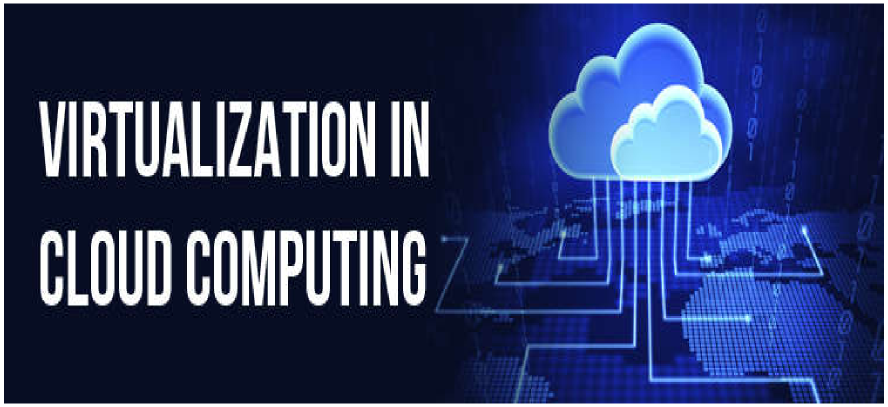
1. **Data storage**
2. **Un-trusted computing**
3. **Data and service availability**
4. **Cryptography**
5. **Cloud data recycling**
6. **Data backup**
7. **Data recovery**
8. **Privacy and integrity**
9. **Malware**

Virtualization security issues

The virtualization software is used to create virtualized services and images, contain several types of virus that may damage or break the virtualized code.

Issues are:

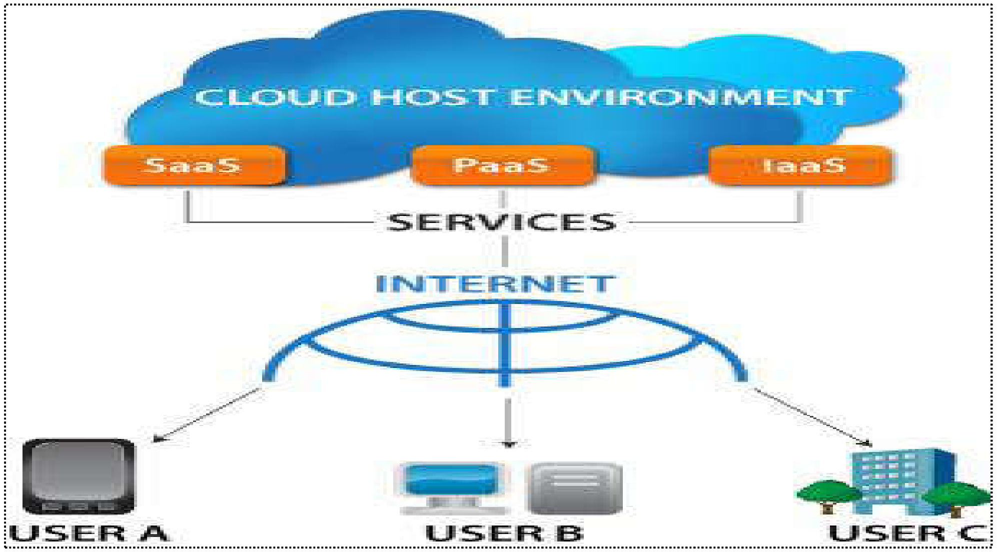
1. **VMs image management**
2. **Virtual machine monitor (VMM)**
3. **Network virtualization**
4. **Mobility**
5. **Issues in virtual machine**
6. **Malware**



Internet and services related security issues

- The cloud services is accessed and managed over the web and standard web browser that is not a safe solution to the end users.
- **Issues are:**

1. Advanced repeated threats and venomous outsiders
2. Internet protocols
3. Web services
4. Web technologies
5. Service availability



ASIACONNECT
DISTRIBUTED AND CLOUD-BASED NETWORK DEFENSE SYSTEM FOR NRENs

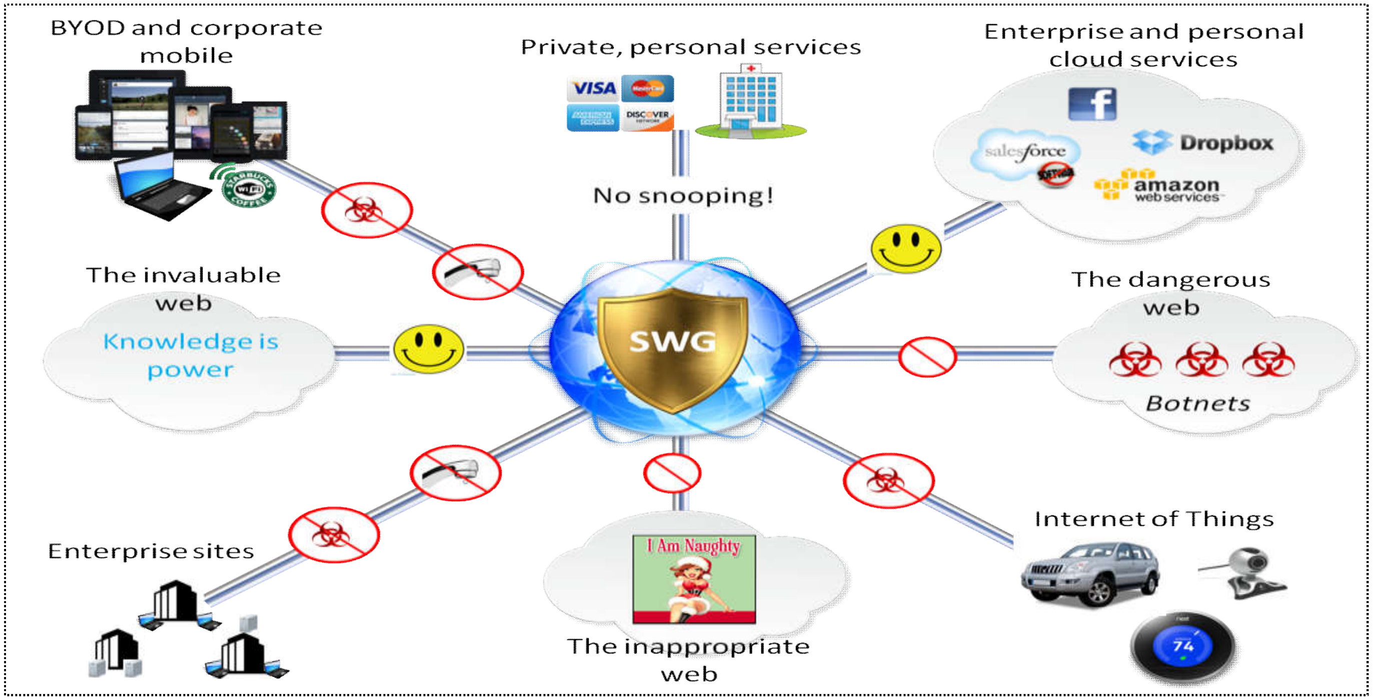
European Union

Asi@Connect

TEIN COOPERATION CENTER

Network security issues

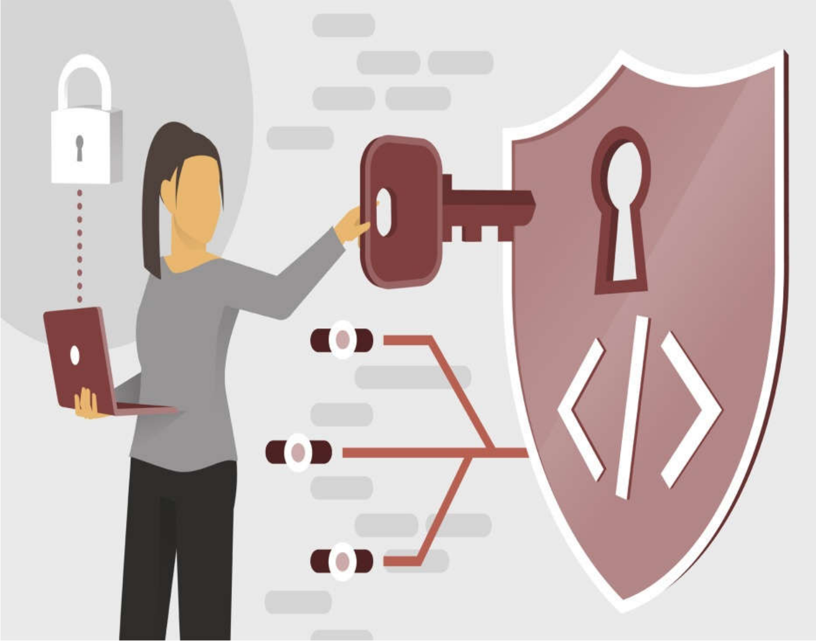
- The network is the basic component of the cloud computing. So, issues are also alive in the network level.
- The network level issues can directly affect the cloud system.



Access control issues

- The access control security is refers to the protection from unauthorized read/write permissions.
- The access security is maintained by authentication with combination of an Email ID or username and password.
- **Issues are:**

1. **Physical access**
2. **User credentials**
3. **Entity authentication**
4. **Authorization**
5. **Management of user identity**



Software security issues

- Software security is the very concerning point in the current situation.
- Nowadays, people write each software program in own ideas and use different programming language.
- That is the reason people unable to measure the software security in the system.
- The system software issue in two subcategories.

1. Platforms and frameworks

2. User front-end

Trust management issues

- Trust is a non measurable parameter in cloud computing. It must be present in between the customer and the cloud provider..
- The trust plays an important role for any system.
- **The various issues are:**

1. Cloud to cloud trust
2. Human aspect
3. Reputation
4. Trust on the audit ability reports

Compliance and legal security issues

- The SLA is a document plays an important role in the cloud business model.
- It contains an agreement between the two communicating parties, all service related information, and terms and conditions of the service.
- **Issues are:**

1. Forensics
2. Acts
3. Legal problems
4. Governance

Attacks based on cloud components

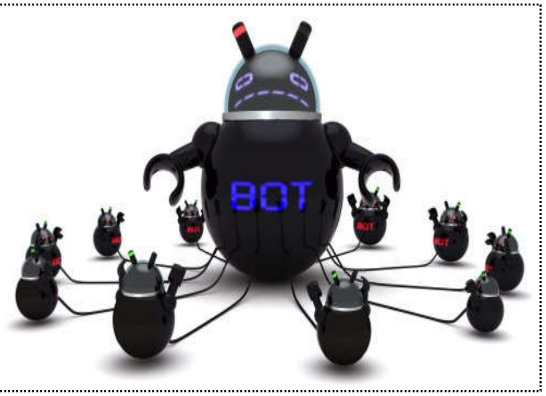
- For performing comparative analysis, attacks on a cloud platform based on its components:

1. **Network (A1),**
2. **Virtual machines (A2)**
3. **Storage (A3) and**
4. **Applications (A4)**

Network based attacks

- An intruder may attack a cloud system through its network which may in turn deteriorate
  the quality of cloud services and may even put data privacy/confidentiality at risk.

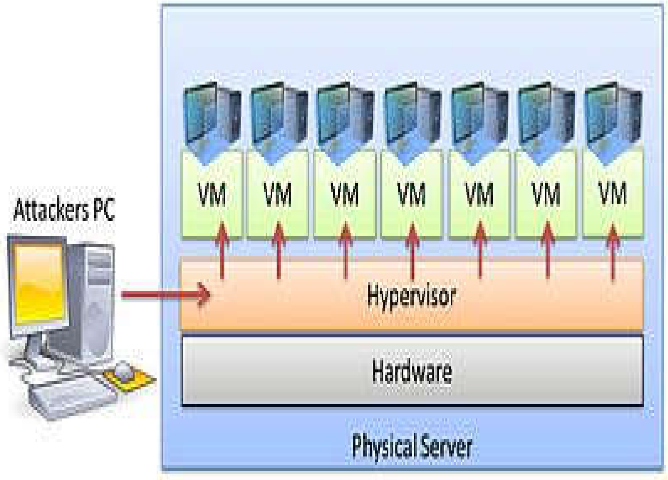
1. **Port scanning**
2. **Botnets**
3. **Spoofing attacks**



Virtual machine based attacks

- On a cloud system, the VM based attacks exploit vulnerabilities in the virtual machines to violate data protection and affect the cloud services.
- Multiple virtual machines being hosted on a system cause several security risks.

1. **Cross VM side channel attacks**
2. **VM creation attacks**
3. **VM migration and rollback attacks**
4. **VM scheduler based attacks**



Storage based Attacks

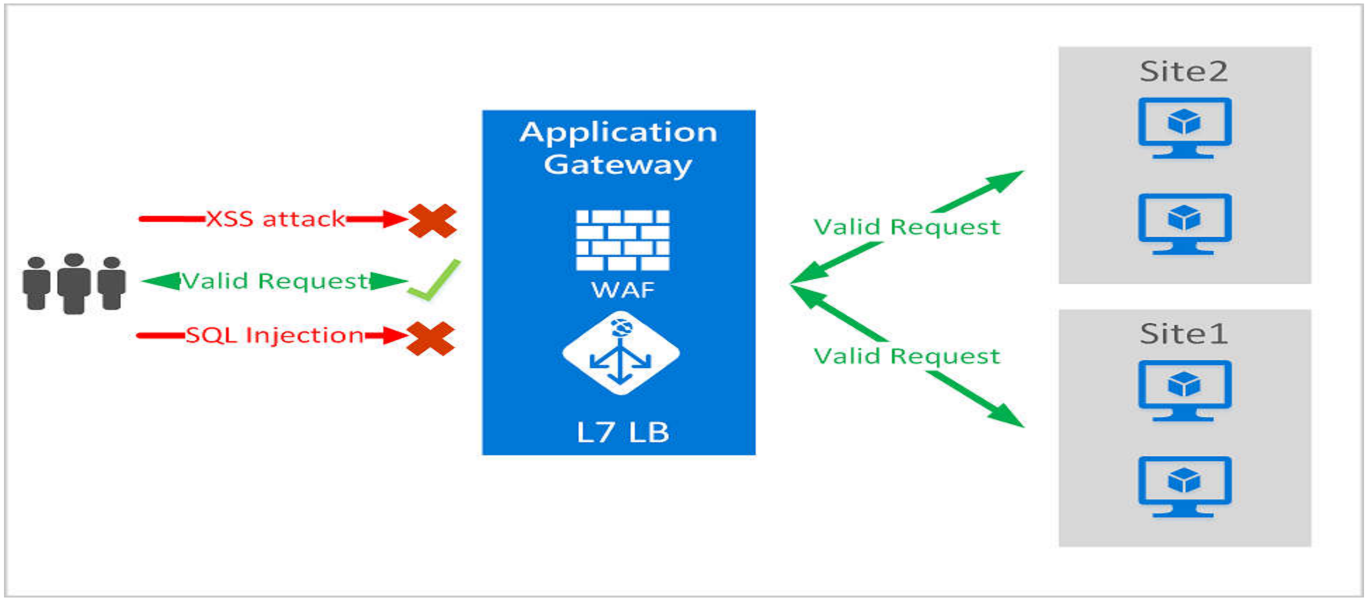
- An attacker from outside or even a malicious insider may steal private data stored on some storage device.
- With access to sensitive information, a large number of vulnerabilities may be exploited by manipulating data if a strict monitoring mechanism is not implemented.

1. **Data scavenging**
2. **Data deduplication**

Application based attacks

- The applications running on a cloud may be exposed to various attacks by injecting code which may trace execution paths and exploit this information for malicious purposes.

1. **Malware injection attacks**
2. **Shared architectures**
3. **Web services & protocol based attacks**



Implications of attacks

- An attack on a cloud may have one or more implications which may deteriorate the provision of data and services on a cloud platform.
- These implications are categorized as follows:

1. **Violation of data protection**
2. **Malicious manipulation of data**
3. **Denial-of-service**
4. **Theft-of-service**

Thank You