

Cloud Security

Objectives

After completing this unit, you should be able to:

- Define various types of Cloud services & Cloud Models
- Understand key characteristics of Cloud Computing
- Find out the Security issues around Cloud Computing
- Know the best practices and Frameworks around Security Cloud Services



Cloud Computing Architectural Framework

What Is Cloud Computing? – NIST SP 800-145



- Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction
- This cloud model is composed of five essential characteristics, three service models, and four deployment models

Source: <https://csrc.nist.gov/publications/detail/sp/800-145/final>

Cloud Computing Features

Dynamically scalable shared resources accessed over a network (Internal network or Internet):

Shared internally or with other customers

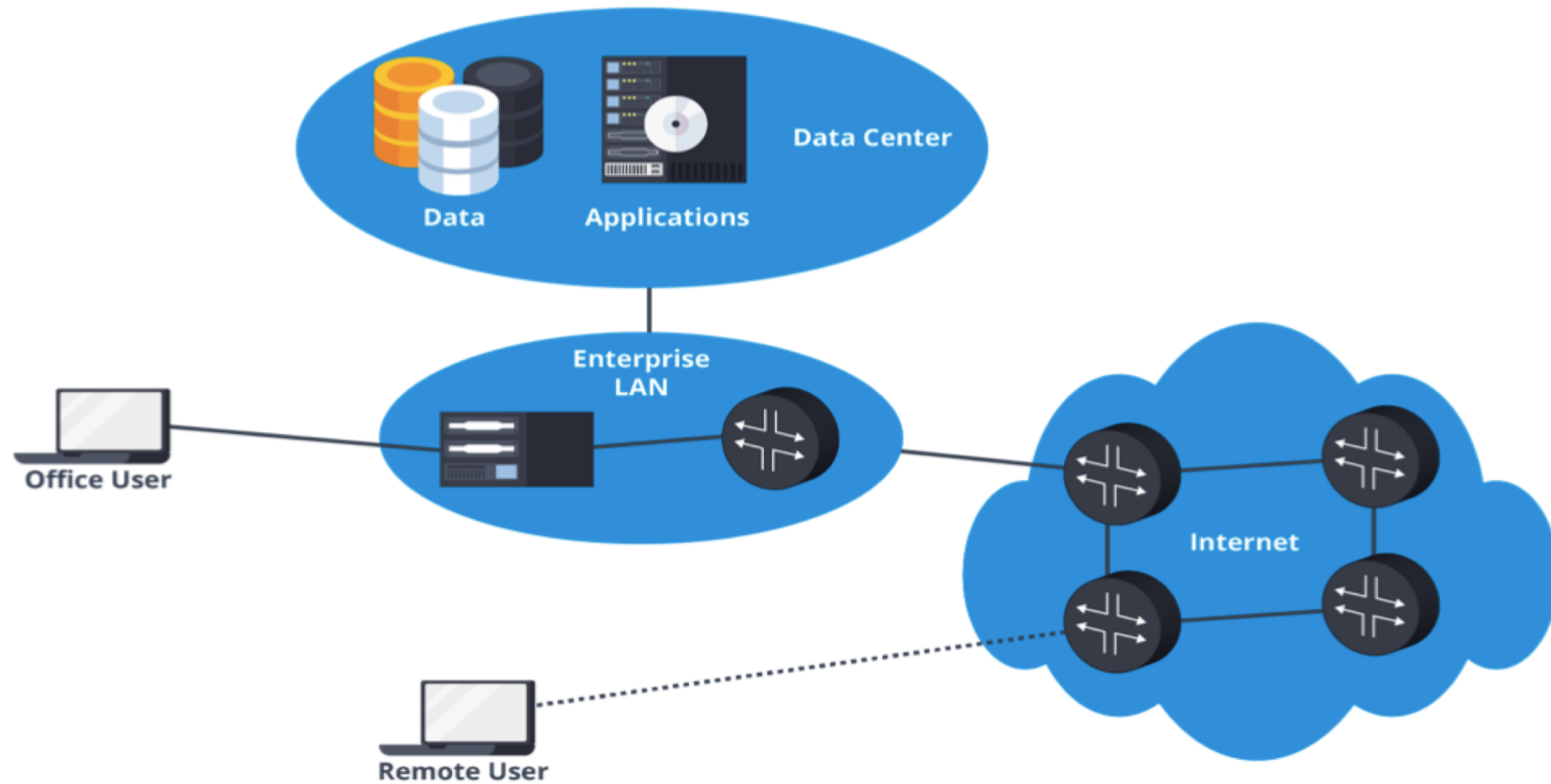
Pay Per Use

Resources = Storage + Compute + Other Services

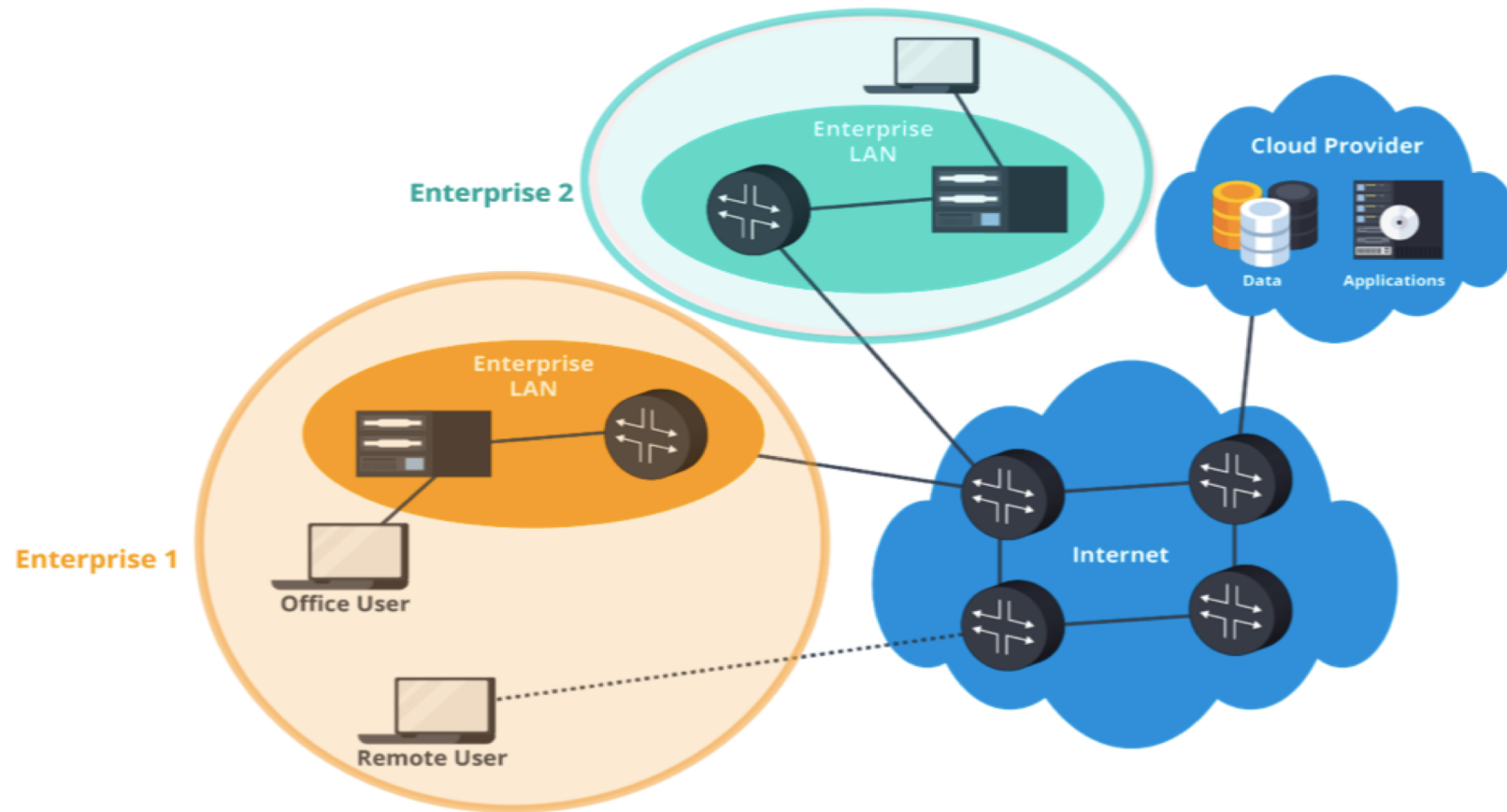
Rent Vs Buy

Reduce Capex (Capital Expenditure) / Fixed Cost


Traditional Data Center Approach



Cloud Approach



Cloud Service Models



IaaS – Infrastructure as a Service – Provider hosts customer VMs or provides network storage. Ex: Amazon Web Services (AWS), Microsoft Azure, Google Compute Engine (GCE)

PaaS– Platform as a Service – Network-hosted software development platform - underlying infrastructure, operating system and so on managed by the provider. Ex: WS Elastic Beanstalk, Windows Azure, Heroku, Force.com and so on

SaaS – Software as a Service – Network-hosted (remote) application - typically accessed via mobile client apps or browsers. Ex: Google Apps, Salesforce, Workday, Concur, Citrix GoToMeeting, Cisco WebEx and so on



More Flavors Of Cloud Computing Service Models

DaaS – Data as a Service

Customer queries against provider's database

NaaS – Network as a Service

Provider offers virtualized networks (e.g. VPNs)

IPMaaS – Identity and Policy Management as a Service

Provider manages identity and/or access control policy for customer

Cloud Deployment Models

Private Cloud

- Provisioned for exclusive use by a single enterprise
- Multiple business units may use it as appropriate
- Ownership, Management & Operation may be executed by a combination of parties (internal & external)
- May be hosted on-premises or externally (on third party cloud provider's premises)

Community Cloud

- Provisioned for exclusive use by a particular community of consumers
- Multiple collaborating enterprises may use it as appropriate
- Ownership, Management & Operation may be executed by a combination of parties (internal & external)
- May be hosted on-premises or externally (on third party cloud provider's premises)

Public Cloud

- Provisioned for use by anyone in general
- Ownership, Management & Operation may be executed by a combination of parties (internal & external)
- Typically hosted on premises of the cloud provider

Hybrid Cloud

- Usually provides add-on services to other cloud models such as load balancing, cloud bursting
- A mix of multiple cloud models (private, community, public)
- Ownership, Management & Operation may be executed by a combination of parties (internal & external)
- Typically hosted on-premises of the cloud provider



Key Characteristics Of Cloud Computing

Multi-tenancy & Resource Pooling

- Shared resources amongst multiple customers with enough segmentation so that each user has its separate control & usage space

On-demand Self-service

- Customer can simply provision computing resources on demand dynamically without manual intervention or help-desk support

Broad Network Access

- Capabilities are openly available over the network & across devices

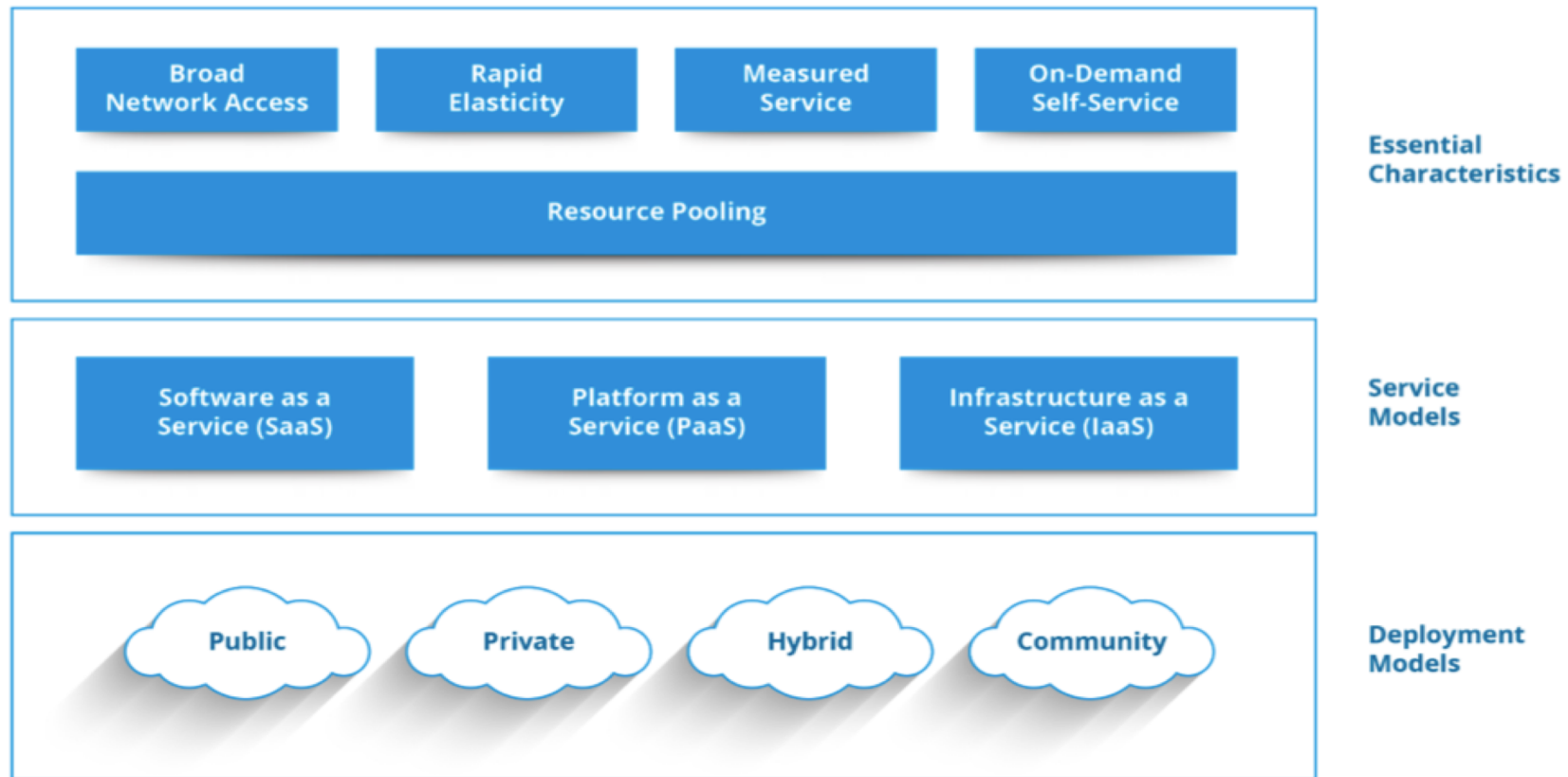
Rapid Elasticity

- Flexible & Automatic provisioning or de-provisioning as per the demand. Resources seem to be virtually unlimited to the consumer

Measured Service

- Transparent Monitoring, Controlling, Reporting of the utilized service to both the provider & consumer (tenant)

Visual Summary – Cloud Computing



Cloud Computing Pros And Cons

Benefits

Pay per use model -
limiting wastage

Faster time to roll-
out new services

Efficient Resource
Sharing

Reduced Costs
(Capex Vs Opex)

Concerns

Uncertainty around
interoperability,
portability & lock-in

Availability & reliability

Security and privacy

Compliance &
regulatory laws
mandate on-site
ownership of data

Facets Of Cloud Security



Key Questions For Cloud Adoption

Before adopting cloud services, there are four key questions:



Cloud Computing – High Level Concerns

High-Level cloud security concerns



Cloud Security Risk Analysis

Security Risk Analysis Methodology

Identify Key Assets & Properties

- Which assets are we trying to protect?
- What properties of these assets must be maintained?

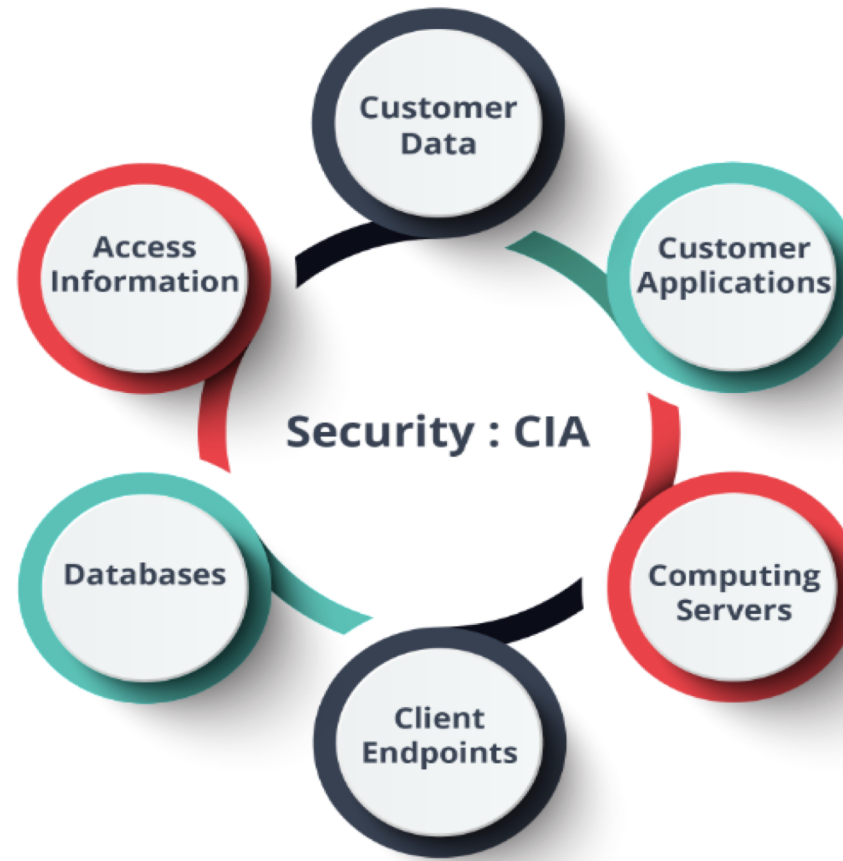
Identify Threats

- What attacks can be performed?
- What are the other likely threats such as: failures, natural disasters and so on

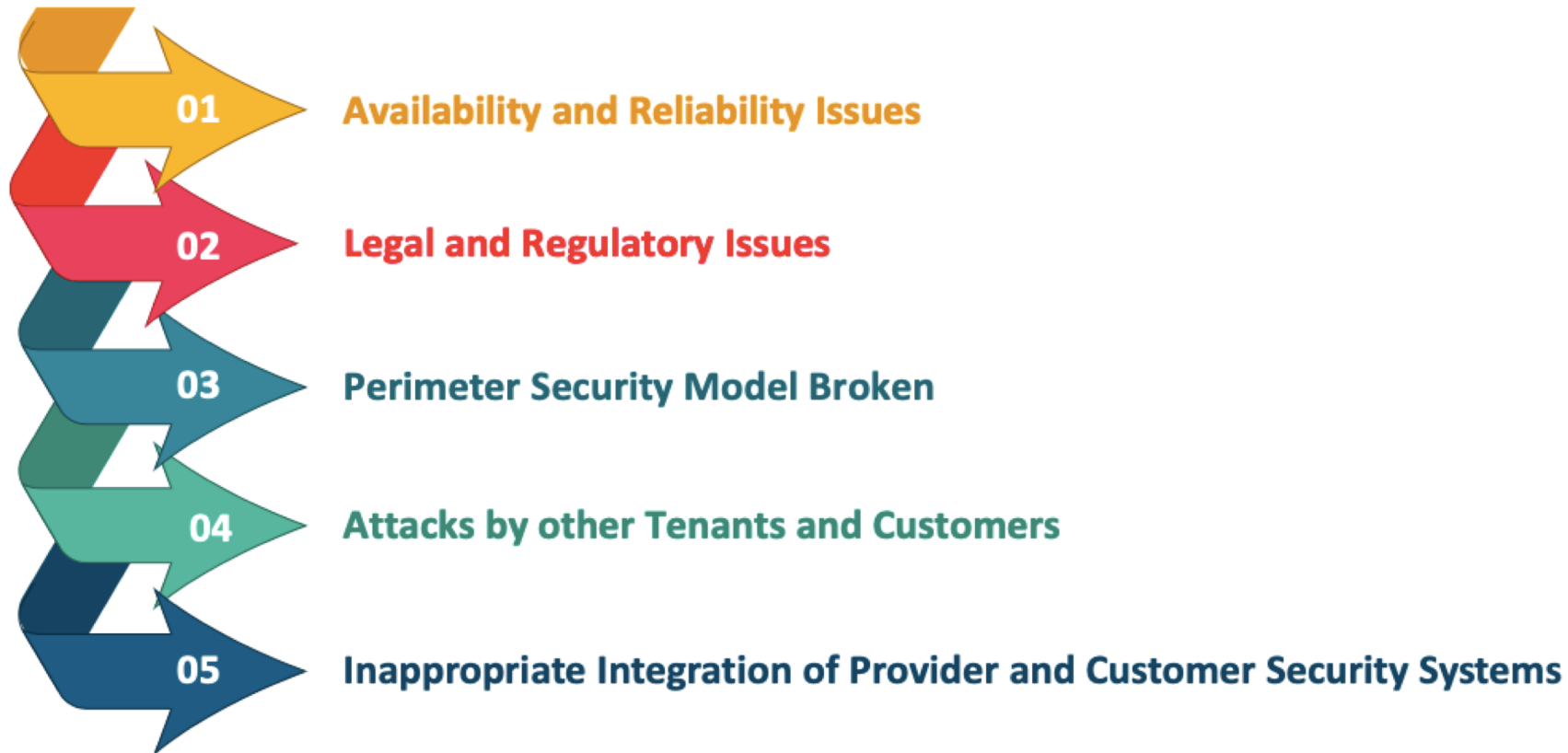
Identify Countermeasures

- How can the attacks be encountered ?

Key Assets Around The Cloud



Key Threats



Availability And Reliability Issues

Threats

Clouds may be less available than in-house IT

Complexity increases chance of failure

Clouds are prominent attack targets

Internet reliability is flaky

Shared resources may provide attack vectors

Counter-measures

Evaluate provider measures to ensure availability

Monitor availability carefully

Plan for downtime

Use public clouds for less essential applications

Legal And Regulatory Issues

Threats

Laws and regulations may prevent cloud computing

Requirements to retain control

Certification requirements not met by provider

Geographical limitations – EU Data Privacy

New locations may trigger new laws and regulations

Counter-measures

Evaluate legal issues

Require provider compliance with laws and regulations

Restrict geography as needed

Perimeter Security Model Broken

Threats

Inclusion of the cloud in the network perimeter of an enterprise lets attackers be inside the perimeter if the cloud is compromised

Non Trusted (shadow) external cloud services - may pose privacy, legal & non-compliance risk

Inappropriate access controls on cloud - could be easily exploited for service disruption, integrity loss & data breach !

Counter-measures

Drop the perimeter (castle based) model & move into a secured federated secure island model



Attacks By Other Customers

Threats

Provider resources shared with untrusted parties

CPU, storage, network

Customer data and applications must be separated

Failures will violate CIA principles

Counter-measures

Hypervisors for compute separation

MPLS, VPNs, VLANs, firewalls for network separation

Cryptography (strong)

Application-layer separation (less strong)

Inappropriate Integration – Of Customer Security Systems

Threats

Disconnected provider and customer security systems

Disgruntled ex-employee retains access to cloud

Security Incidents in cloud not reported to customer

Counter-measures

Integrate identity management with enterprise's central IdAM

Enforce consistent access controls

Integrate detection, monitoring and alerting

May consider using SAML, LDAP, RADIUS, XACML, IF-MAP, etc.

Key Strategic And Tactical Security Concerns – Cloud Security Alliance

Key Concerns – Cloud Security Alliance: Csaguide.V.3.0

	Governance and Enterprise Risk Management		Interoperability and Portability		Application Security
	Legal Issues: Contracts and Electronic Discovery		Traditional Security, Business Continuity, and Disaster Recovery		Encryption and Key Management
	Compliance and Audit Management		Data Center Operations		Identity, Entitlement, and Access Management
	Information Management and Data Security		Incident Response		Virtualization
					Security as a Service

Governance And Enterprise Risk Management

Concerns

- Capability of an enterprise to govern and measure enterprise risk introduced by cloud computing
- Legal issues related to agreements, pre-contractual security due diligence
- Risk assessment of cloud provider
- Responsibility of data protection in case of breaches
- Cross border data flow Vs Risk

Key Recommendations

- In-depth Security Risk Assessment & Pre-contractual security Due-diligence of CSP (cloud service provider)
- Contractual agreements to have appropriate Information security responsibilities in subcontracting chain, incident response obligations
- Monitoring CSP key risk & performance metrics
- Enumeration of Third party relationships of CSP
- Right to periodic Audit of the CSP (rare) Or periodic submission of independent audit reports & certifications by CSP to the B2B client

Legal Issues: Contracts & Electronic Discovery

Concerns

- Potential legal considerations and issues while using cloud computing
- Protection requirements for information , regulatory requirements, privacy requirements, international laws and so on

Key Recommendations

- Contractual agreement is a key legal enforcement tool, hence must be drafted carefully and thus encompass several security and functional requirements along with **SLA** (Service Level Agreements)
- Contractual agreements must restrict cross-border data flow as required
- Security due-diligence of CSP is key & should be done along with enough documentary evidence
- Provision for e-discovery of assets & data as & when required

Compliance And Audit Management

Concerns

- Maintaining & proving compliance with various compliance requirements (legislative, regulatory, other) while using cloud computing

Key Recommendations

- Enterprises to secure Right to periodic Audit the CSP or the third party giving cloud access, CSP or Third party to share independent audit reports to the enterprise on a decided frequency
- Clear communication of Data classification levels, Risk impact to the CSP or Third party
- Thorough risk assessment

Information Management And Data Security

Concerns

- Secure data lifecycle management of the data placed on the cloud
- Responsibilities & Accountability around data security

Key Recommendations

- Contractual obligations specify data retention & data deletion requirements
- Protocol of action & penalties in case of Data breach
- Backups, BCP/DR, Availability and SLAs

Interoperability And Portability

Concerns

- CSP Lock-in
- Technology dependence and monopoly
- Interoperability between different CSPs

Key Recommendations

- Prefer Open Source / open standards / well known technology stack
- Consider migration assistance while features pre-procurement
- Consider potential portability mechanisms, alternatives, costs & availability of such support in case of CSP breakdown

Traditional Security, Business Continuity & Recovery

Concerns

- Way in which selected Cloud stack (& CSP) affects overall security, BC (business continuity) & DR (disaster recovery)
- How the adoption of selected cloud stack would impact CIA in worst case scenarios

Key Recommendations

- CSP to demonstrate industry standard security best practices & baselines
- Tenant organization to periodically Review BCP/DR plans of CSP (covered via periodically shared independent audit reports as well)
- Right to Audit CSP when possible
- Stringent Incident monitoring & communication

Data Center Operations

Concerns

- Effective evaluation of a CSP's data center architecture & operations - for security assurance and reliability to the tenant organization

Key Recommendations

- CSP to demonstrate adoption of industry standard security best practices around data center architecture, setup & operations
- CSP to demonstrate appropriate BCP/DR plans to be evaluated by the tenant organization so as to ensure it gels well for the association from security perspective
- Appropriate Contractual obligations for SLAs & Uptimes



Incident Response

Concerns

- Adequate Incident Detection, Response, Alerting & Remediation is the key both at CSP & Tenant levels
- Smooth, Timely & Secure incident information flow is also an important factor during the relation between CSP & Tenant

Key Recommendations

- Ensure appropriate clauses mandate the CSP to inform breaches / incidents to the tenants in timely manner
- Enforce encryption requirements on sensitive / PII information flow between the involved parties
- Review Security Architecture of the cloud stack & also conduct Threat modelling & impact analysis from IT Security operations point of view

Application Security

Concerns

- Security of software application running on a chosen cloud Or being developed in the cloud
- Selection of appropriate Cloud Model (SaaS/ PaaS/ IaaS) for a given requirement

Key Recommendations

- Enumerate and consider security use cases right from the beginning of application development lifecycle
- Ensure appropriate security controls are embedded for inter-host communications
- Choice of appropriate development models & architecture that balances security & utility the best
- Ensure enough segregation of service boundaries, user levels and so on, at the design level

Encryption And Key Management

Concerns

- Identification of appropriate encryption usage and scalable management of keys

Key Recommendations

- Plain text data stored on cloud could be very risky and usually considered as lost & hence is a high risk scenario especially when the data consists of PII or sensitive elements
- Applications to store data properly encrypted with correct choice of algorithms in the backend
- Strong Key management is "key" as lost keys defeat the purpose of encryption
- Consider using dedicated Key management cloud solutions – just meant for that job. This should also be done with appropriate contractual obligations set for the scope of association

Identity, Entitlement, And Access Management

Concerns

- Extension of enterprise's identities into cloud
- Using directory services to provide cloud access control
- Using Cloud-based directory services
- Adoption of Cloud-based Identity, Entitlement, and Access Management (IdEA)

Key Recommendations

- Tenant organization to define a clear, robust, decentralized IdAM strategy
- Evaluate & find the best match of the CSP's IdAM policies - with the internal one
- Consider implementing SSO for smooth access to variety of internal applications & then its extension to the multitude of cloud applications

Virtualization

Concerns

- Heavy use of virtualization technology in cloud computing (being the basis)
- Risks around multi-tenancy, VM isolation, VM co-residence, hypervisor vulnerabilities, and so on
- Security issues associated with system and hardware virtualization

Key Recommendations

- Strong Hardening & Regular security patching of Virtualized operating systems & Hypervisors
- Usage of appropriate security controls on Virtualized operating systems
- Strong Access control of Virtualized OS along with physical access to bare metal hypervisors
- Usage of appropriate mirroring solutions for availability concerns
- Ensure secure VM provisioning & minimization of insecure and vulnerable window

Security As A Service

Concerns

- Cloud based - MSSP (Managed Security Service Providers): Third party facilitated Security Assurance, Incident Management, Idam Monitoring , Compliance Attestation and so on

Key Recommendations

- Usually Lot of confidential data is involved While using a cloud based MSSP
- Strong contractual obligations to be set forth with all previously discussed clauses
- Evaluation of track record of the provider in terms of previous breaches (if any) & external communication
- Careful Architectural & Encryption decisions especially around what level of classified data flows out of the client organization to the cloud provider for security testing & how does the result flow back
- Enforcement of Secure Data retention
- Enforcement of Secure Data Deletion
- Secure Communication of breach

Security Attacks

Cloud Security Attacks



Data Level Security Concerns And Attacks

Data Level Attacks cause Sensitive Data leakage to unauthorized parties or data corruption due to application security, inappropriate access controls or misconfiguration

- Confidentiality (Data Leakage)

Integrity (Data Corruption)

- Availability (Denial of Service)

Data Lock – In

- Users may lose data if they migrate from one vendor to another vendor

Data Left – Over

- In-adequately erased data - especially after quitting a cloud service can be dangerous in terms of confidentiality as they may be scoured by non-intended parties

Data Recovery

- Sometimes key servers may break down & cause damage or loss to users' data. Appropriately timed backups at alternative sites is thus important

Data Location

- In SaaS model of cloud environment, the user doesn't know where the data is stored which may be an issue from legal or compliance standpoint. The issue can be solved by creating secure SaaS model which can provide reliability to the customer on the location of the data of the user

Application Level Security Attacks: SaaS & PaaS

Malware Injection Attack

- In this attack a malicious executable is injected into the cloud application. Usually this is done by exploiting an open vulnerability in the application
- Strong Application security controls should be embedded throughout the web-application lifecycle

Cookie Poisoning

- An unauthorized access could be made into the application by modifying the contents of the cookie
- A potential solution to prevent this is to encrypt the cookie data & frequent cleaning of cookies

Backdoors, Debug Options, Hidden Field Manipulation Attacks

- Debug option is for the developers who use it to implement any changes requested at later stage in a website since these debug option provides backdoor entry for the developers, sometimes these debug options are left enabled unnoticed, they may provide easy access to the hackers and allow them to make changes in the website. In addition, certain fields are hidden in the web-site and is used by the developers. Hacker can sometime get hold of such fields & manipulate them for performing unauthorized activities
- Strong Application security controls should be embedded throughout the web-application lifecycle

Infrastructure Level Security Attacks: IaaS

Malware and Ransomware Attacks

- In this attack a malicious VM (virtual machine) is injected into the cloud system
- A potential solution to prevent this is to perform the integrity check to the service instances along with deployment of appropriate IDS or IPS, Firewalls, Process monitoring & Anti Malware solutions on the cloud instances

OS Level Exploits (RCE/ EOP)

- Typically in IaaS model, the Operating system management is the responsibility of the tenant. Hence All OS security resides with the tenant
- Lack of appropriate hardening, access controls & security patching could cause RCE (Remote Code Execution) & EOP (Elevation Of Privilege) attacks

Network Level Security Attacks

MITM (Man In The Middle Attack)

- Absence of SSL Encryption usually leads to successful MITM attacks where the attacker controls an ongoing session in an unauthorized manner

Domain Hijacking

- Attacker changes the registration data of a domain without the knowledge or permission from the domain's real owner. This enables the intruders to access the sensitive information

DOS Attack

- When hackers overflow a network server or web server with frequent request of services to damage the network, the denial of service cannot keep up with them, server could not legitimate client regular requests

Network Sniffing

- Another type of attack is network sniffer, it is a more critical issue of network security in which unencrypted data are hacked through network

Cloud Service Provider Level Security Attacks

Guest-Hopping Attack

- An attacker will try gaining access to another parallel virtual machines by attacking one of the virtual machines hosted on the same hypervisor or hardware
- Hypervisor level configuration hardening & security controls are must to prevent this

Malicious Insiders

- In private cloud, it's employee is granted access to the sensitive data of some or all customer administrators
- Such privileges may expose information to security threats
- Integrated IdAM, RBAC, and RuBAC models along with appropriate SOD & Principle of Least Privilege are must to be implemented to avoid this

Inter-VM Side Channel Attack

- It occurs when an attacker deliberately places a malicious VM on a shared physical hypervisor platform, and then accesses shared hardware and cache locations to perform a variety of side-channel/sprawling attacks including DOS (denial of service), hardware utilization detection, remote keystroke monitoring via timing inference and so on

Quiz #1

- Cloud Security in general, refers to protection of
 - a. Cloud Infrastructure
 - b. Applications
 - c. Data
 - d. All of the above

Answer #1

- Cloud Security in general, refers to protection of
 - a. Cloud Infrastructure
 - b. Applications
 - c. Data
 - d. **All of the above**

Answer d:

Explanation: Domain of Cloud Security encompasses securing all the aspects of cloud computing including Data, Applications & the hosting infrastructure. Cloud Security is incomplete without any one of these being focused on

Quiz #2



- R&D department of an organization raises a request for having a dynamic and flexible platform to be able to spin up virtual servers and storage on demand, and also collaborate easily with the third parties involved in a project for data & application sharing needs. Which Cloud model does suit best for this purpose?
 - a. IaaS (Infrastructure as a Service)
 - b. PaaS (Platform as a Service)
 - c. SaaS (Software as a Service)
 - d. NaaS (Network as a Service)

Answer #2

- R&D department of an organization raises a request for having a dynamic and flexible platform to be able to spin up virtual servers and storage on demand, and also collaborate easily with the third parties involved in a project for data & application sharing needs. Which Cloud model does suit best for this purpose?
 - a. **IaaS (Infrastructure as a Service)**
 - b. PaaS (Platform as a Service)
 - c. SaaS (Software as a Service)
 - d. NaaS (Network as a Service)

Answer a:

Explanation: IaaS is the best option for the said requirements. It is easy to deploy VMs of choice on demand also configure the storage & internal configurations for R&D purpose

Quiz #3

- SOC (Security Operations Center) within an organization notices a sudden surge in failed RDP (Remote Desktop) login attempts on a large amount of VMs provisioned on its contracted IaaS public cloud provided by a very reputed vendor. After a short while they notice several successful unauthorized logins rising the possibility of confidential data leakage consisting of customer personal information - stored on those VMs for testing purpose. After investigation it was found that the breach occurred due to a combination of unmonitored & open RDP ports along with very weak passwords set on the VMs. Also it was established that the actual users of these VMs are found to be personnel from the Third Party vendor's organization who was involved in a specific project by the Tenant Organization. Who is accountable for such a data breach?
 - a. CSP (Cloud Service Provider)
 - b. Tenant Organization
 - c. Third Party Organization
 - d. None of the above

Answer #3

- SOC (Security Operations Center) within an organization notices a sudden surge in failed RDP (Remote Desktop) login attempts on a large amount of VMs provisioned on its contracted IaaS public cloud provided by a very reputed vendor. After a short while they notice several successful unauthorized logins rising the possibility of confidential data leakage consisting of customer personal information - stored on those VMs for testing purpose. After investigation it was found that the breach occurred due to a combination of unmonitored & open RDP ports along with very weak passwords set on the VMs. Also it was established that the actual users of these VMs are found to be personnel from the Third Party vendor's organization who was involved in a specific project by the Tenant Organization. Who is accountable for such a data breach?
 - a. CSP (Cloud Service Provider)
 - b. Tenant Organization**
 - c. Third Party Organization
 - d. None of the above

Answer b:

Explanation: The Tenant organization which is the primary contracted customer of the CSP, is accountable because in IaaS cloud computing model - the responsibility & accountability to use appropriate hardening, patching & password complexity remains with the customer (tenant). Third party organization was just using the VM instances provisioned on the allocated contracted cloud by the primary tenant organization & is usually not responsible for configuration of such infrastructure

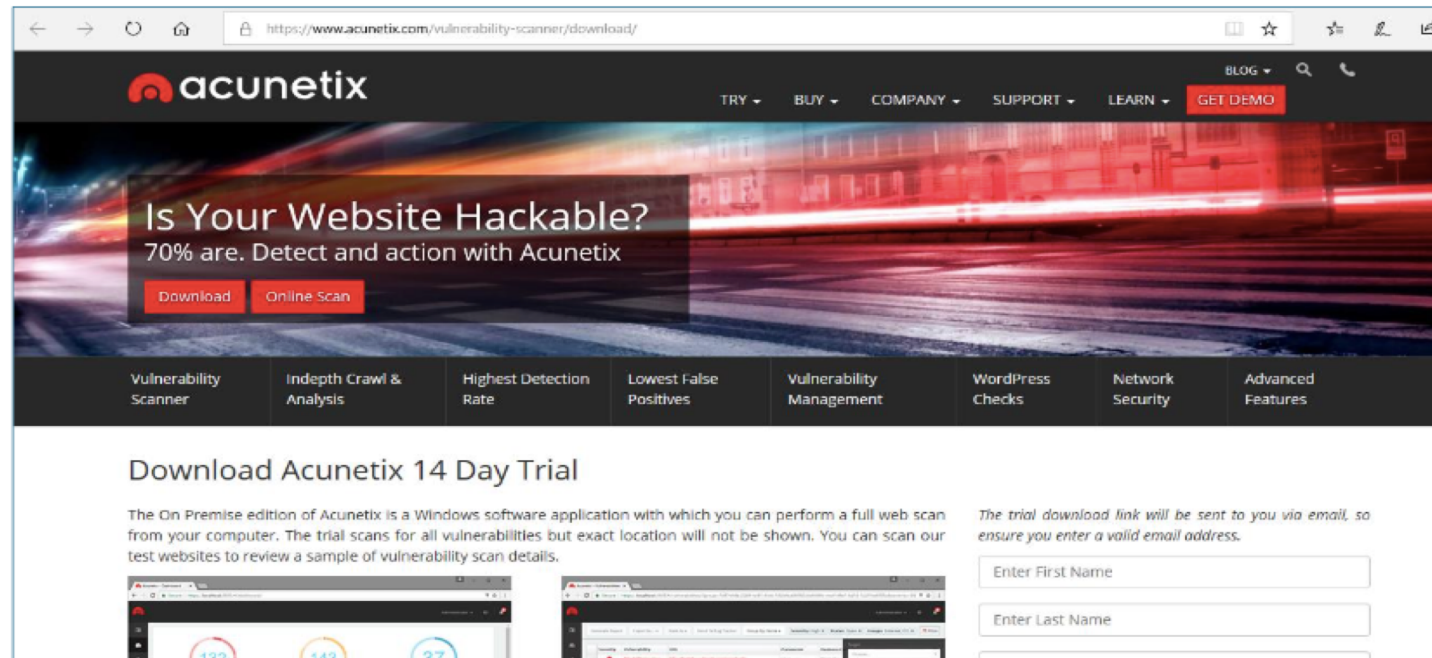
Demo 1: Virtual Machine

- Create a **Virtual Machine** to run a guest operating system
- Install VirtualBox for creating a virtual machine instance
- Download and install **VirtualBox tool** from the link: <https://www.virtualbox.org/>



Demo 2: Cloud Based Application Vulnerabilities

- Cloud based applications are vulnerable for various attacks and hacking
- Scan the web application or website for various vulnerabilities
- Use **Acunetix Web Vulnerability Scanner**
- Download **Acunetix Web Vulnerability Scanner** tool from the link: <https://www.acunetix.com/vulnerability-scanner/download/>



Summary

In this unit, you should have learnt:

- Types of Cloud services & Cloud Models
- Key characteristics of Cloud Computing
- Security issues around Cloud Computing
- Best practices and Frameworks around Security Cloud Services

QUESTIONS PLEASE ☺

