



Cloud Security

Module Number: 03

Module Name: Cloud Security Architecture

Version Code: CS1

Released Date: 24-Jan-2019

AIM:

To equip the students with security and control measures of cloud architecture.



Objectives:

The Objectives of this module are:

- Understand the architecture of cloud.
- Illustrate the architecture and reference model of Trusted Cloud Initiative.
- Open stack model of cloud.

Outcomes:

At the end of this module, you are expected to:

- Define different deployment models.
- Understand the risk in managing cloud security.
- Recovery strategy in case of any disaster.

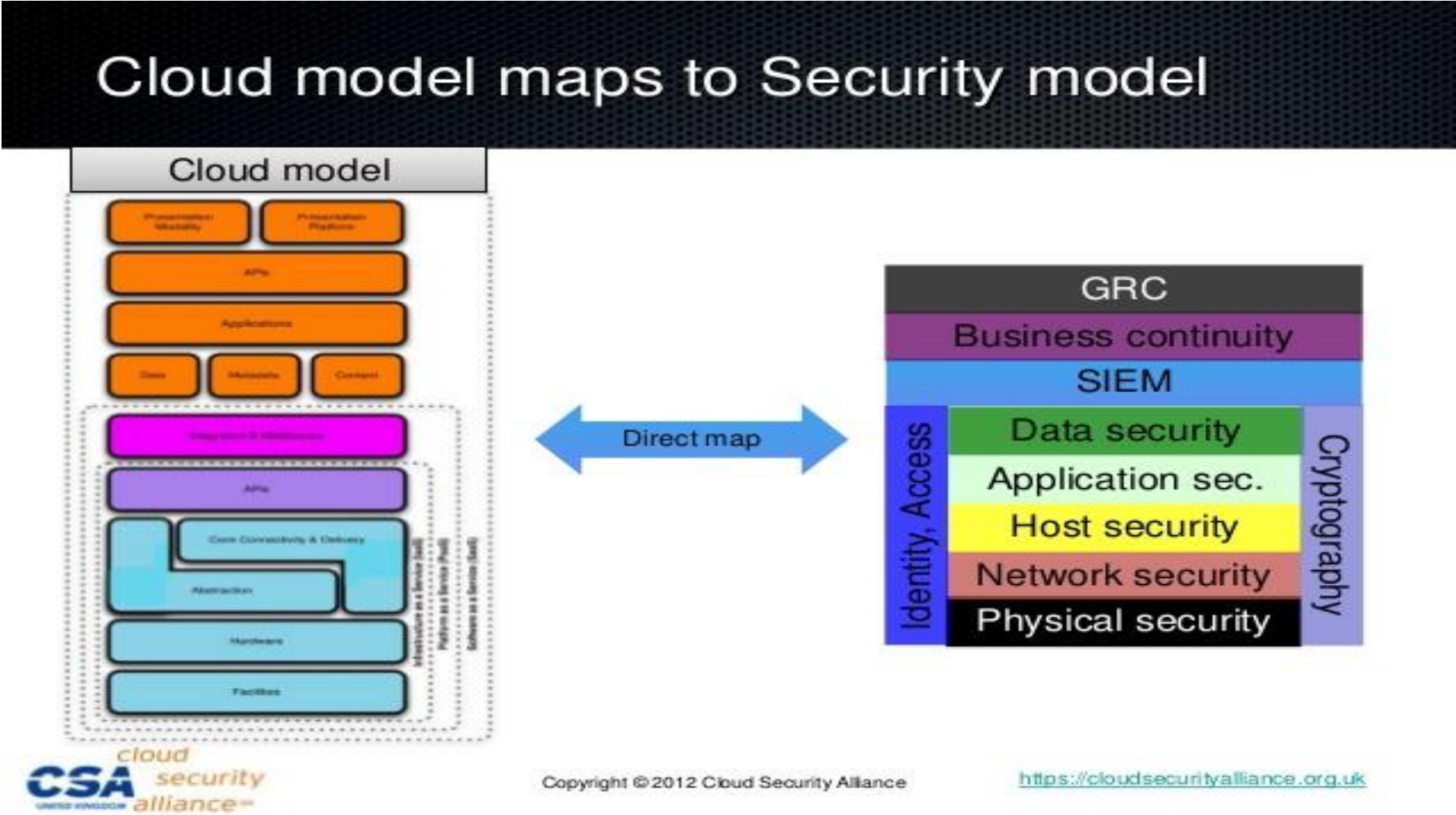
CONTENTS

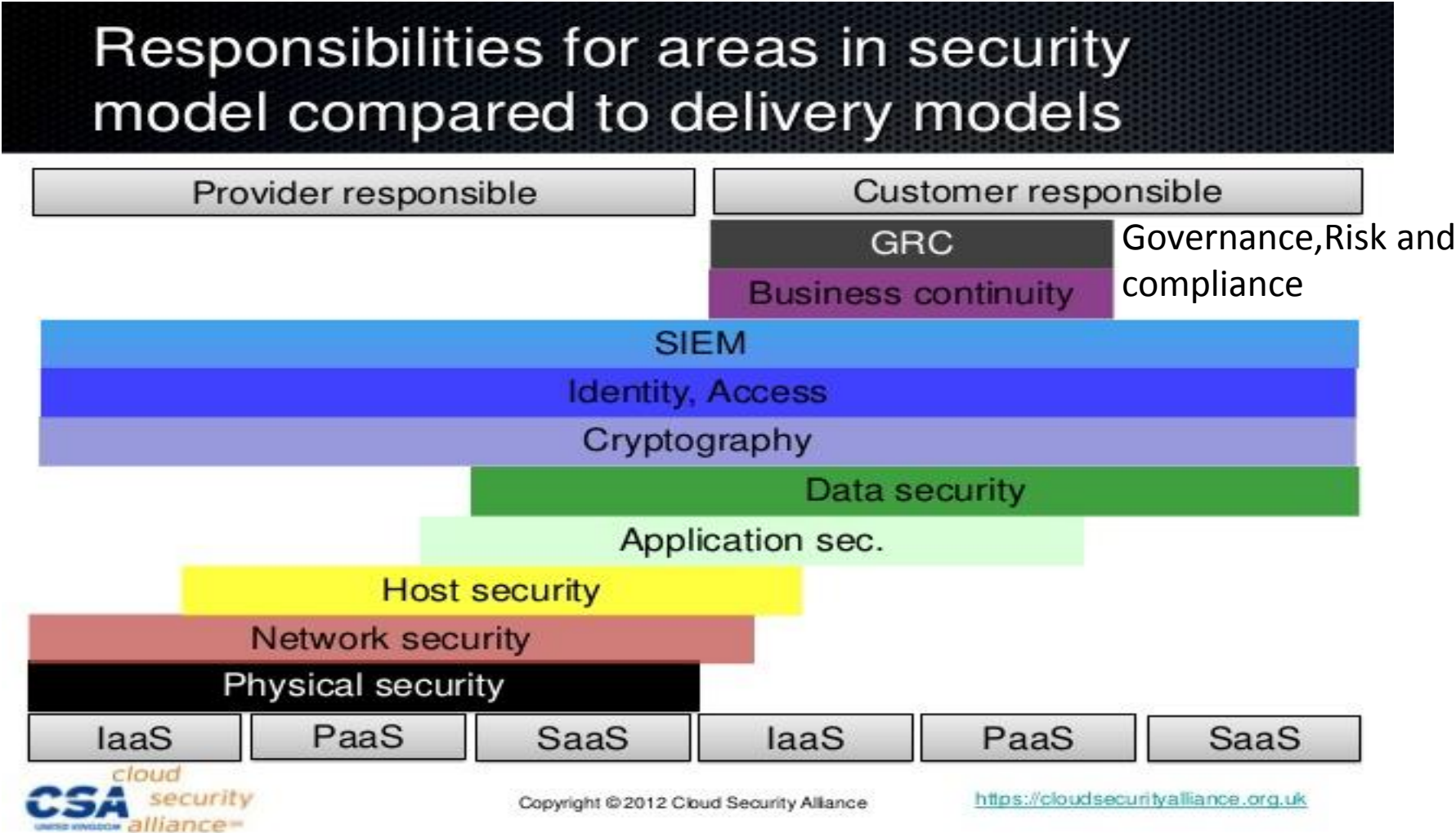
- Security model mapping in cloud model
- Cloud Security models
- Cloud security domains
- Issues of cloud computing security
- Data security and storage



Cloud computing deployment models

| | Infrastructure managed by | Infrastructure owned by | Infrastructure located | Accessible and consumed by |
|-----------------------|--|--|---------------------------------|----------------------------|
| Public | Third party provider | Third party provider | Off-premise | Untrusted |
| Private/ Community | Organisation or 3 rd party provider | Organisation or 3 rd party provider | On-premise or Off-Premise | Trusted |
| Hybrid | Both Organisation & Third party provider | Both Organisation & Third party provider | Both On-Premise & Off-Premise | Trusted & Untrusted |





Cloud Security Domains

Governance

- Governance and Enterprise Risk Management
- Legal Issues: Contracts and Electronic Discovery
- Compliance and Audit
- Information Management and Data Security
- Portability and Interoperability

Operational

- Traditional Security, Business Continuity and Disaster Recovery
- Data Center Operations
- Incident Response, Notification and Remediation
- Application Security
- Encryption and Key Management
- Identity and Access Management
- Virtualization
- Security as a Service

Cloud Computing Storage Security Issues:

1. Traditional Security problems.
2. Law Issue.
3. Third party Issue.



Related Research for Storage Security:

1. Authorization:

- Multi-level authorization
- The Face Fuzzy Vault

2. Encryption:

- RSA Encryption
- AES Encryption
- Hybrid Encryption

3. Segmentation:

- Metadata Based Storage Model
- Multi-cloud Architecture Model

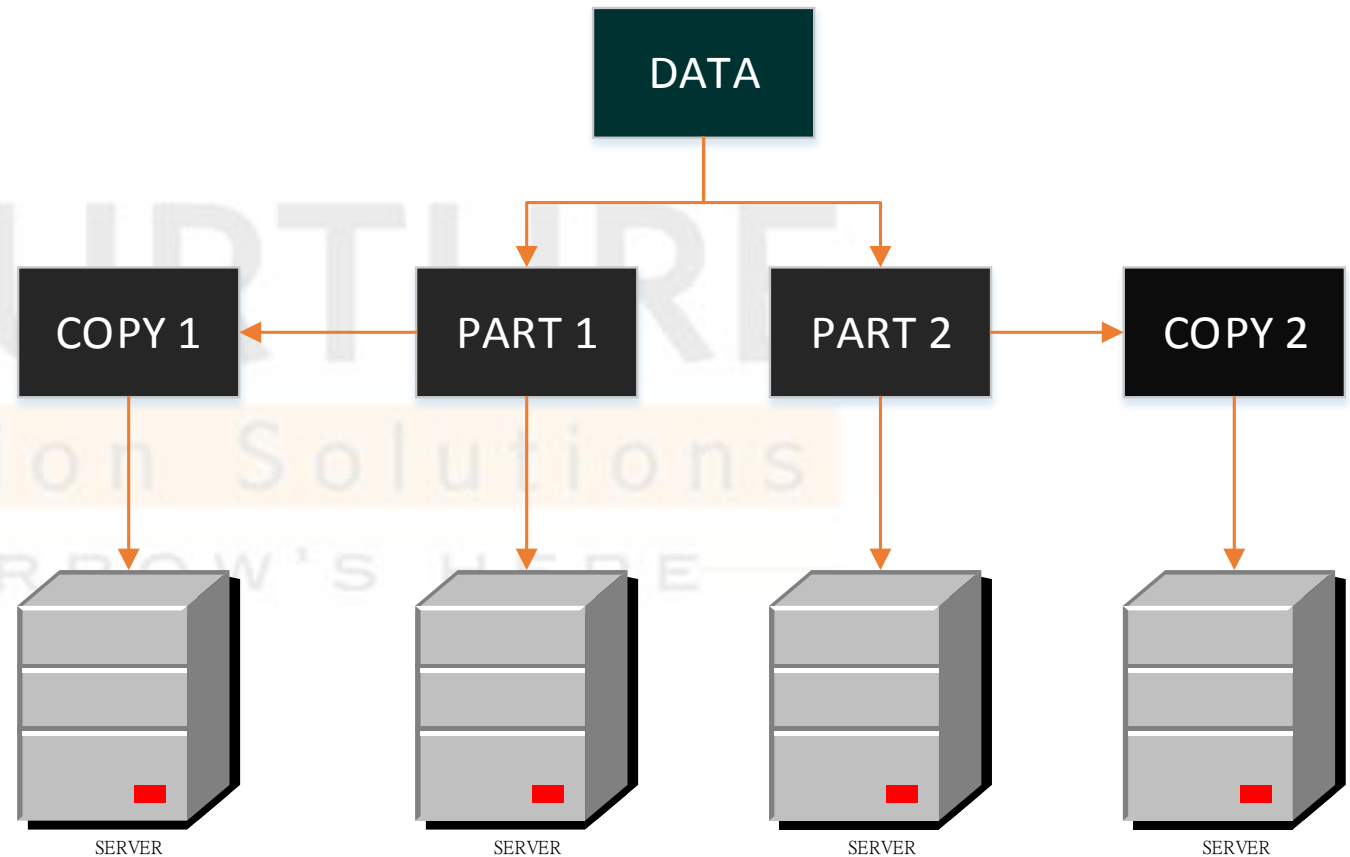


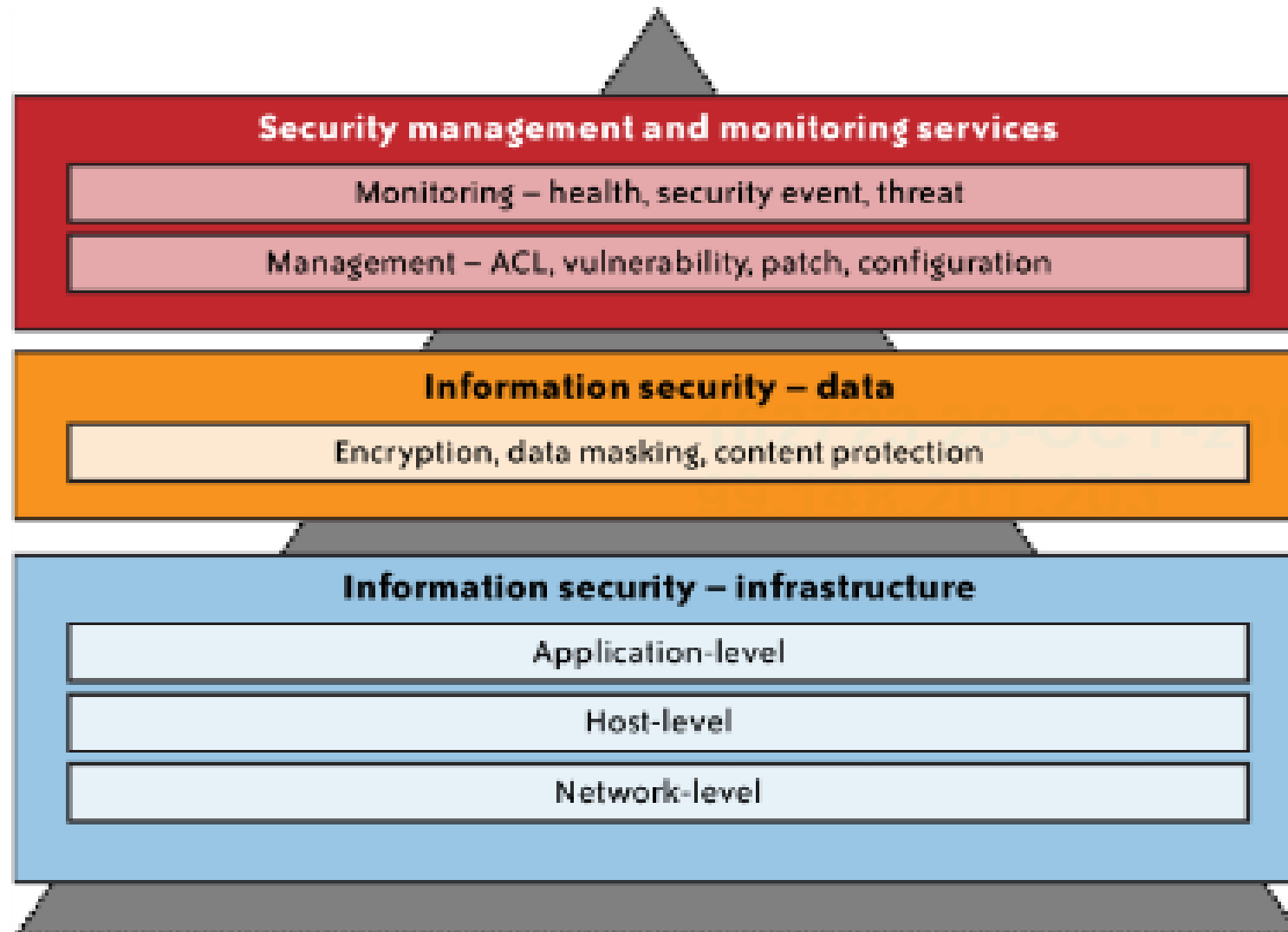
Figure: Segmentation Backup System

Data Security

- Data-in-transit
- Data-at-rest
- Data processing
- Data lineage
- Data provenance
- Data remanence



overview



Data Security and Storage

- Several aspects of data security, including:
 - Data-in-transit
 - Confidentiality + integrity using secured protocol.
 - Confidentiality with non-secured protocol and encryption.
 - Data-at-rest
 - Generally, not encrypted , since data is commingled with other users' data
 - Encryption if it is not associated with applications?
 - But how about indexing and searching?
 - Processing of data, including multitenancy
 - For any application to process data

Data Security and Storage

Data lineage

- Knowing when and where the data was located w/i cloud is important for audit/compliance purposes
- **Example**, Amazon AWS
 - Store <d1, t1, ex1.s3.amazonaws.com>
 - Process <d2, t2, ec2.compute2.amazonaws.com>
 - Restore <d3, t3, ex2.s3.amazonaws.com>

Data provenance

- Computational accuracy (as well as data integrity)

Data Security and Storage

- **Example**, financial calculation: $\text{sum } (((((2*3)*4)/6) - 2) = \2.00 ?
 - How about dollars in different countries?
 - Correct exchange rate?

Data remanence

- Inadvertent disclosure of sensitive information is possible.

What is Privacy?

- The concept of privacy varies widely among (and sometimes within) countries, cultures, and jurisdictions.
- It is shaped by public expectations and legal interpretations; as such, a concise definition is elusive if not impossible.
- Privacy rights or obligations are related to the collection, use, disclosure, storage, and destruction of personal data
- At the end of the day, privacy is about the accountability of organisations to data subjects, as well as the transparency to an organisation's practice around personal information.

What Are the Key Privacy Concerns?

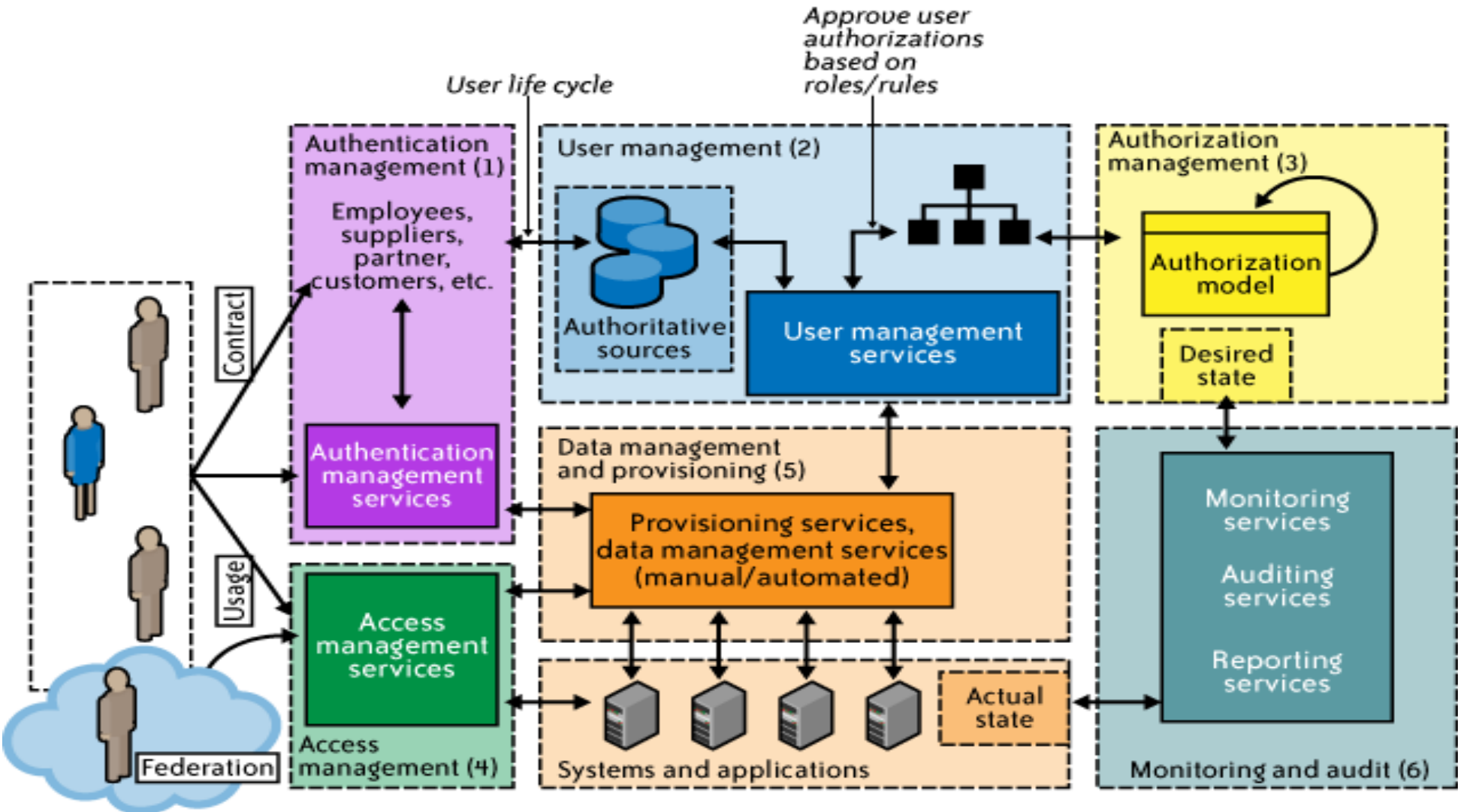
- Typically mix security and privacy
- Some considerations to be aware of:
 - Storage
 - Retention
 - Destruction
 - Auditing, monitoring and risk management
 - Privacy breaches
 - Who is responsible for protecting privacy?

Identity and Access Management

- Traditional trust boundary reinforced by network control
 - VPN, Intrusion detection, intrusion prevention.
- Loss of network control in cloud computing.
- Have to rely on higher-level software controls
 - Application security.
 - User access controls – IAM.

- IAM components
 - Authentication
 - Authorisation
 - Auditing
- IAM processes
 - User management
 - Authentication management
 - Authorisation management
 - Access management – access control
 - Propagation of identity to resources.
 - Monitoring and auditing.

Cloud Security Architecture



IAM standards and specifications

- Avoid duplication of identity, attributes, and credentials and provide a single sign-on user experience
 - SAML(Security Assertion Markup Lang)
- Automatically provision user accounts with cloud services and automate the process of provisioning and de-provisioning
 - SPML (service provisioning markup language).
- Provision user accounts with appropriate privileges and manage entitlements
 - XACML (extensible access control markup language).
- Authorise cloud service X to access my data in cloud service Y without disclosing credentials.
 - Oauth (open authentication).

IAM practice- Identity federation

- Dealing with heterogeneous, dynamic, loosely coupled trust relationships.
- Enabling “Login once, access different systems within the trust boundary”.
 - Single sign-on (SSO).
 - Centralized access control services.
 - Yahoo! OpenID.

When considering Privacy and security

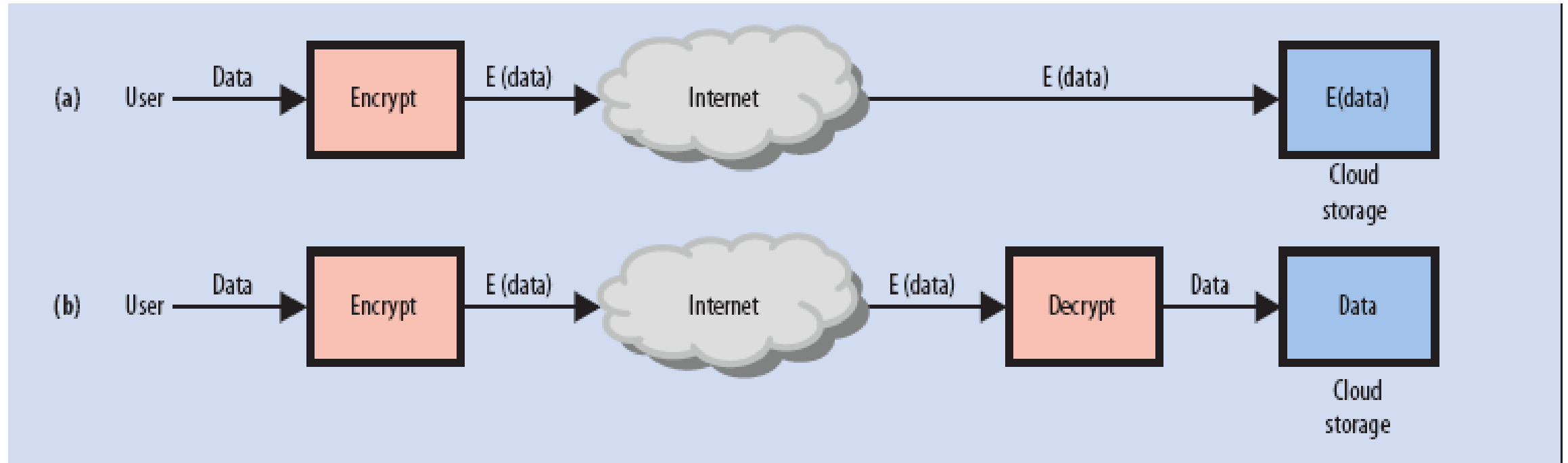


Figure 2. Two encryption scenarios for cloud computing. (a) Data remain encrypted at the cloud storage site, preventing unauthorized access through the Internet; the cloud vendor cannot access the data either. (b) Data are decrypted by the cloud vendor to enable necessary operations on the data.

When considering Privacy and security

Another possible privacy and security solution is to use a technique called steganography :

- Multimedia content like images and videos have significant redundancy. This makes it possible to hide data in multimedia using steganography.
- Steganography techniques can be used to transform the data before storage so that operations can still be performed on the data.

When considering Privacy and security



(a)



(b)



(c)

Figure A. An example of steganography: images (a) and (c) look identical, but image (c) contains image (b) hidden in it. Applying appropriate transformations to image (c) can obtain image (b).

When considering Privacy and security

Performing encryption or steganography techniques before sending data to the cloud requires some additional processing on the mobile system. So the formula become:


$$\frac{C}{M} \times \left(P_c - \frac{P_d}{F} \right) - P_{tr} \times \frac{D}{B} - P_c \times \frac{C_p}{M},$$

Encryption & key strategies

- On a trusted host, collect the encrypted data, as shown in Figure 3, and decrypt it with the collection agent's private key which stays on that host. Note that in this case, we are in exclusive control of the private key, which the cloud service provider has no view or control over.
- They will discuss this feature of our solution later.

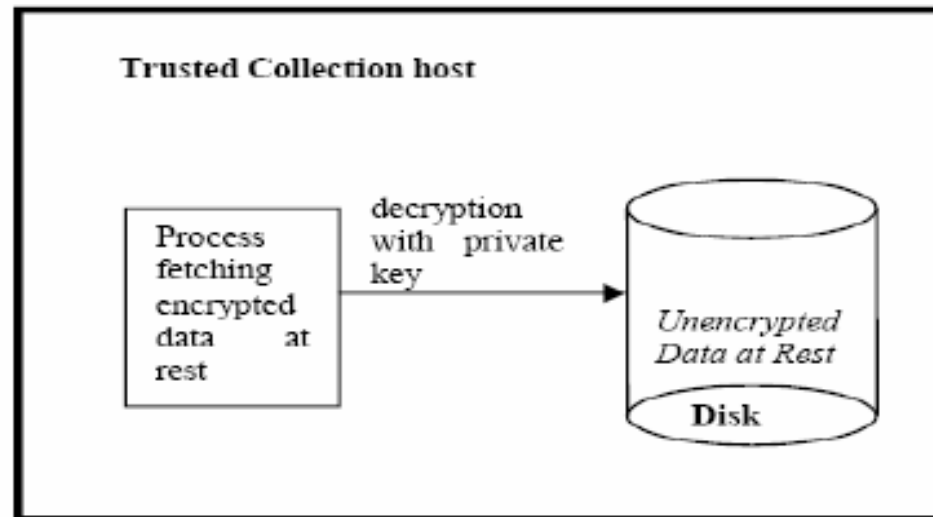
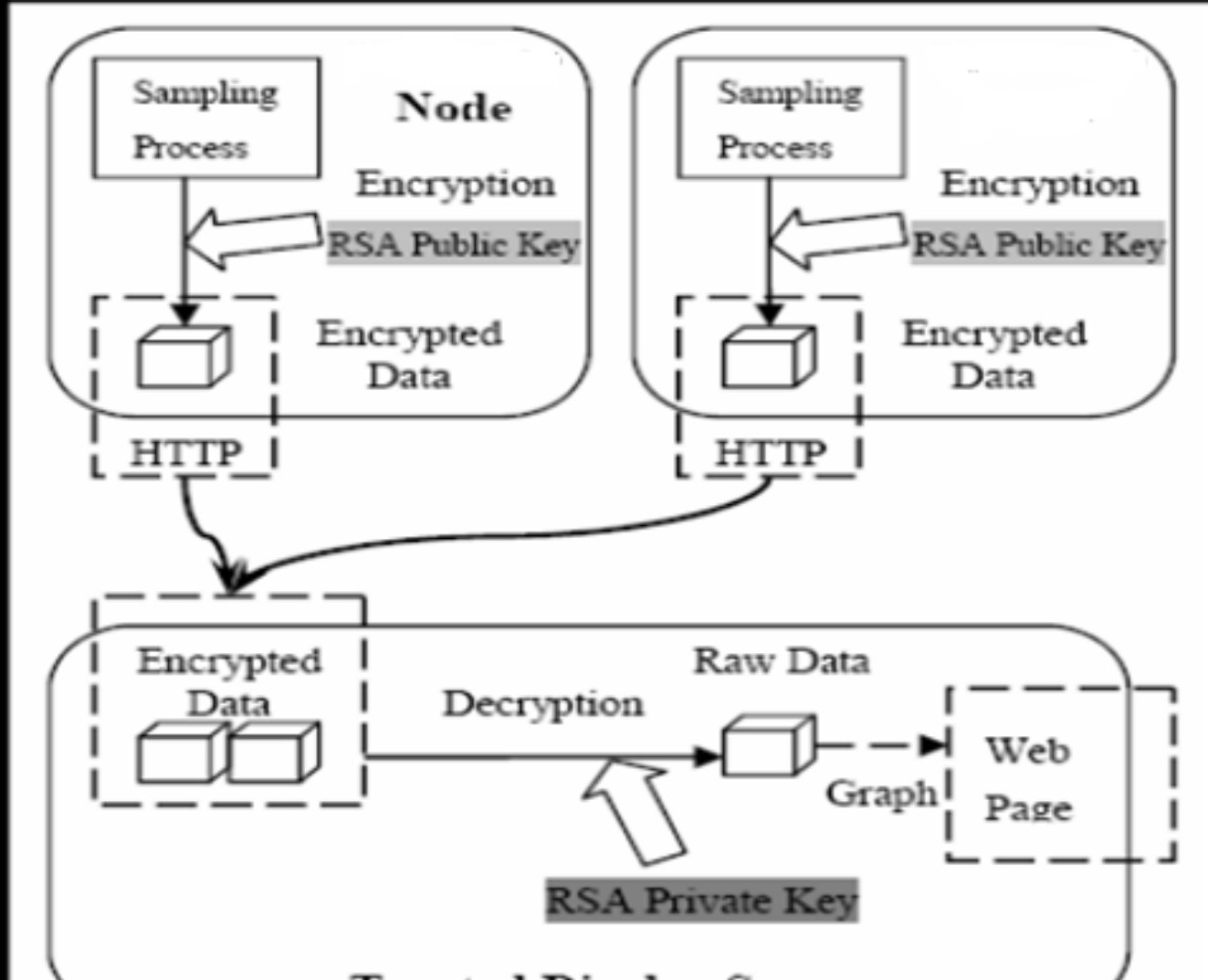


Fig. 3. Process in a Cloud Computing Infrastructure producing Encrypted Data at Rest

Cloud Security Architecture



Cloud Deployment Models

Private cloud

- Single org only, managed by the org or a 3rd party
- On or off premise.

Community cloud

- Shared infrastructure for specific community.
- Several orgs that have shared concerns, managed by org or a 3rd party.

Cloud Deployment Models

- Public cloud
 - Sold to the public, mega-scale infrastructure.
 - available to the general public.
- Hybrid cloud
 - composition of two or more clouds.
 - bound by standard or proprietary technology.

Business Continuity and Recovery Strategies

Hot Site: Fully configured, ready to operate within hours.

Warm Site: Ready to operate within days: no or low power main computer. Does contain disks, network, peripherals.

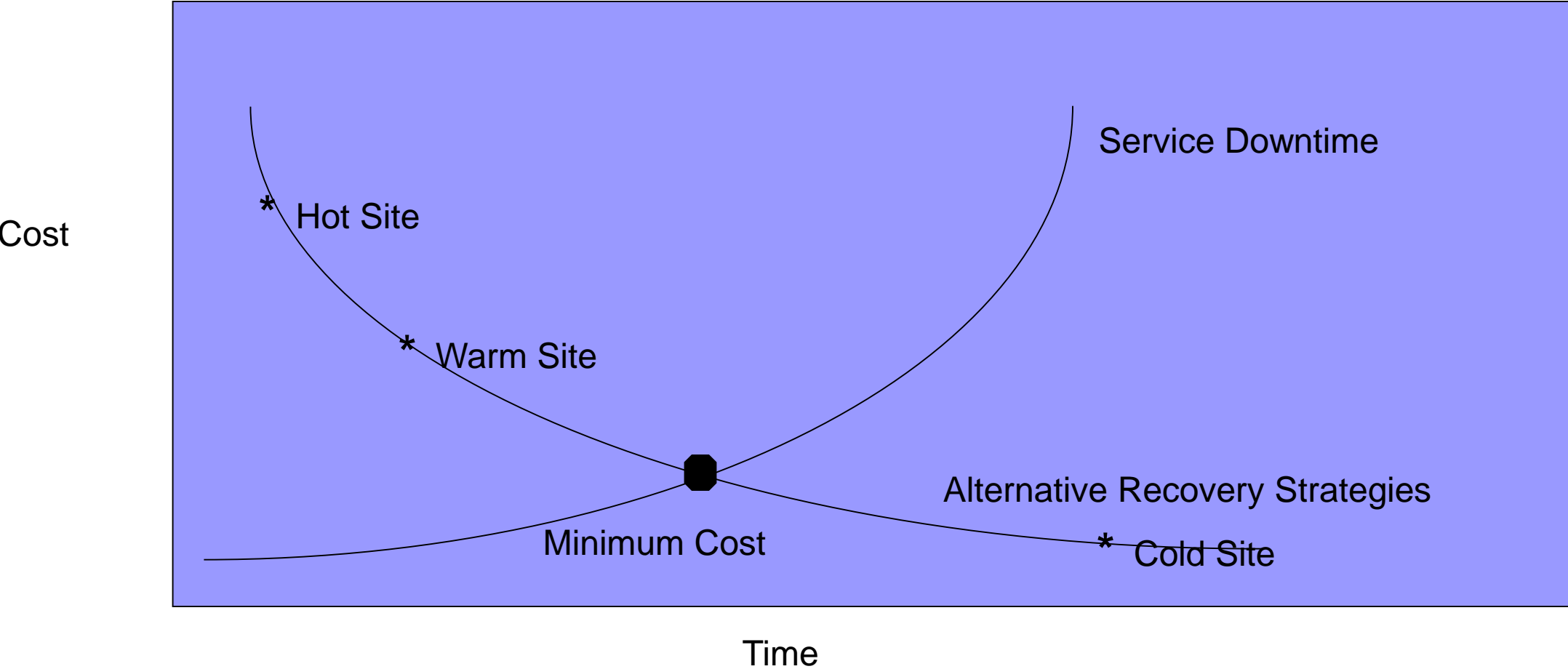
Cold Site: Ready to operate within weeks. Contains electrical wiring, air conditioning, flooring.

Duplicate or Redundant Info. Processing Facility: Standby hot site within the organisation.

Reciprocal Agreement with another organization or division.

Mobile Site: Fully- or partially-configured trailer comes to your site, with microwave or satellite communications.

Disruption vs. Recovery Costs



Hot Site

- Contractual costs include: basic subscription, monthly fee, testing charges, activation costs, and hourly/daily use charges.
- Contractual issues include: other subscriber access, speed of access, configurations, staff assistance, audit and test.
- Hot site is for emergency use – not long term.
- May offer warm or cold site for extended durations.

Reciprocal Agreements

Advantage: Low cost

Problems may include:

- Quick access.
- Compatibility (computer, software).
- Resource availability: computer, network, staff.
- Priority of visitor.
- Security (less a problem if same organisation).
- Testing required.
- Susceptibility to same disasters.
- Length of welcomed stay.

Business Continuity Process

- Perform Business Impact Analysis.
- Prioritize services to support critical business processes.
- Determine alternate processing modes for critical and vital services.
- Develop the Disaster Recovery plan for IS systems recovery.
- Develop BCP for business operations recovery and continuation.
- Test the plans.
- Maintain plans.

The amount of data transactions that are allowed to be lost following a failure depends upon the following points:

1. Recovery Time Objective
2. Recovery Point Objective
3. Service Delivery Objective
4. Maximum Tolerable Outage

Self Assessment Question

1. When the RTO is large, this is associated with:
 - a. Critical applications
 - b. A speedy alternative recovery strategy
 - c. Sensitive or non-sensitive services
 - d. An extensive restoration plan

Self Assessment Question

2. When the RPO is very short, the best solution is:
- a. hot site
 - b. Data mirroring
 - c. A detailed and efficient Disaster Recovery Plan
 - d. An accurate Business Continuity Plan

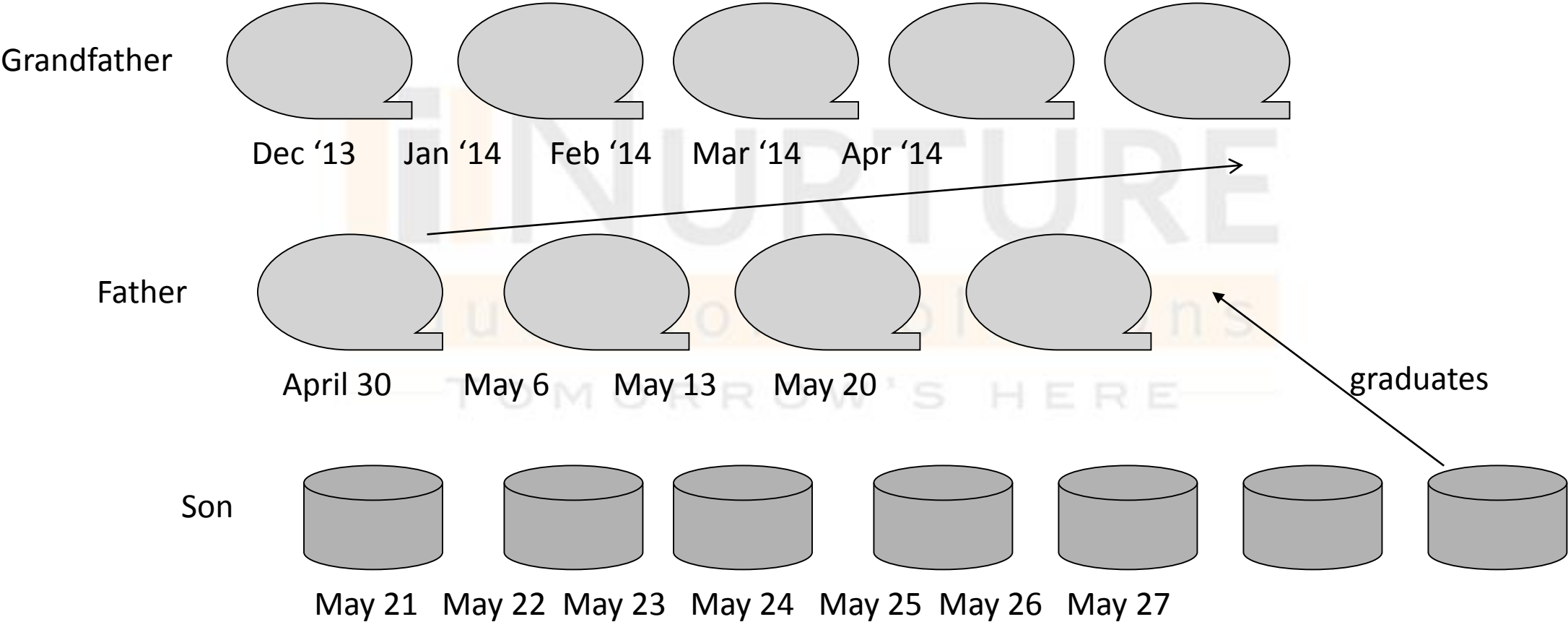
Cloud Security Architecture

Data Storage Protection

Backup Storage



Backup Rotation: Grandfather/Father/Son

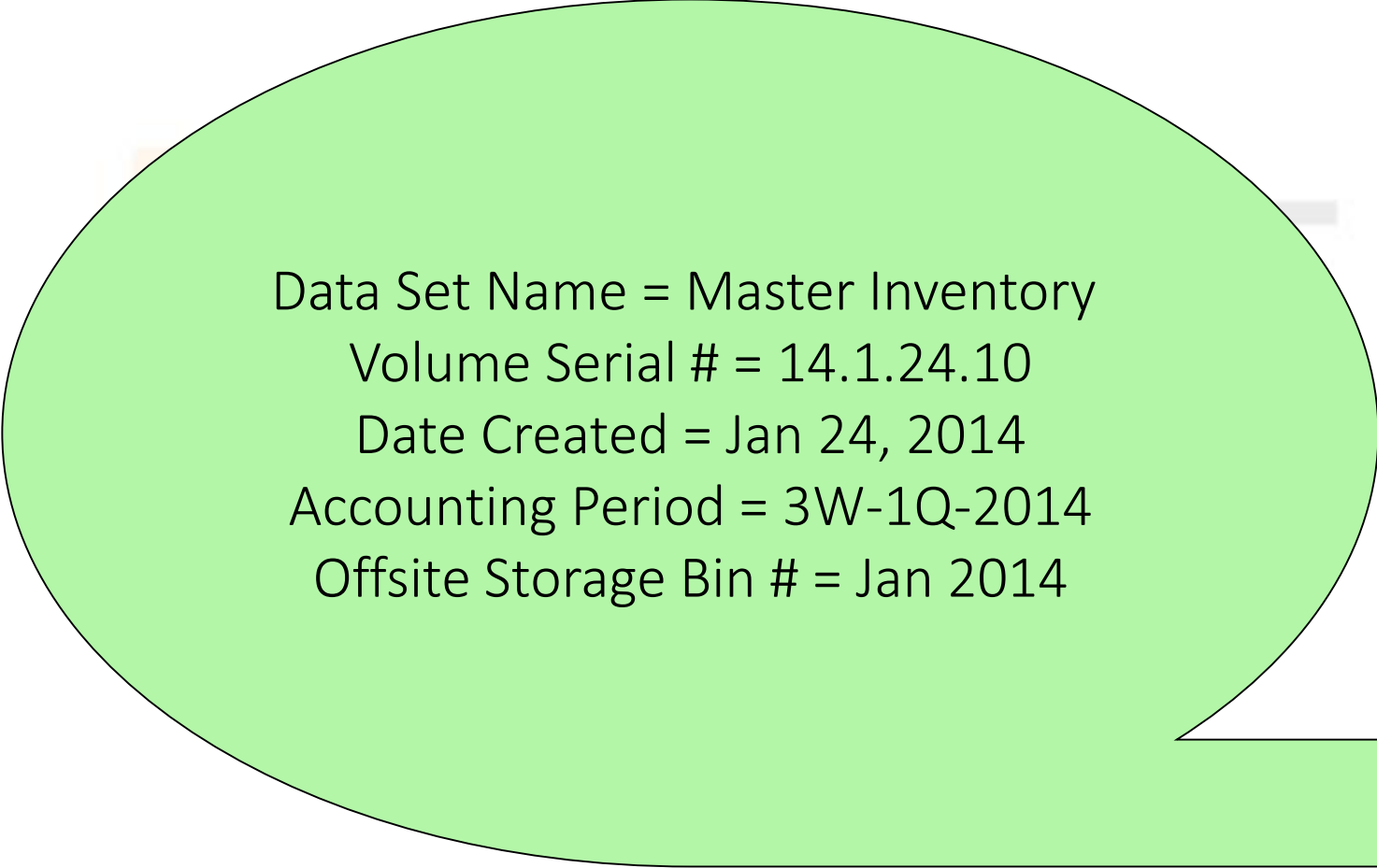


Frequency of backup = daily, 3 generations

Incremental and Differential Backups

| Daily Events | Full | Differential | Incremental |
|----------------------|----------|--------------|-------------|
| Monday: Full Backup | Monday | Monday | Monday |
| Tuesday: A Changes | Tuesday | Saves A | Saves A |
| Wednesday: B Changes | Wed'day | Saves A + B | Saves B |
| Thursday: C Changes | Thursday | Saves A+B+C | Saves C |
| Friday: Full Backup | Friday | Friday | Friday |

Backup Labelling



Data Set Name = Master Inventory
Volume Serial # = 14.1.24.10
Date Created = Jan 24, 2014
Accounting Period = 3W-1Q-2014
Offsite Storage Bin # = Jan 2014

Backup could be disk...

Backup and Offsite Library

- Backups are kept off-site (1 or more).
- Off-site is sufficiently far away (disaster-redundant).
- The library is equally secure as the main site; unlabelled.
- The library has constant environmental control (humidity-, temperature-controlled, UPS, smoke/water detectors, fire extinguishers).
- A detailed inventory of storage media and files is maintained.

Concerns for a BCP/DR Plan

- Evacuation plan: People's lives always take **first priority**.
- Disaster declaration: Who, how, for what?
- Responsibility: Who covers necessary disaster recovery functions.
- Procedures for Disaster Recovery.
- Procedures for Alternate Mode operation.
 - Resource Allocation: During recovery and continued operation.
- Copies of the plan should be off-site.

Disaster Recovery Responsibilities

General Business

- First responder: Evacuation, fire, health.
- Damage Assessment.
- Emergency Management.
- Legal Affairs.
- Transportation/Relocation/Coordination (people, equipment).
- Supplies.
- Salvage.
- Training.

IT-Specific Functions

- Software.
- Application.
- Emergency operations.
- Network recovery.
- Hardware.
- Database/Data Entry.
- Information Security.

Contact information is important!

BCP Documents

| Focus: | IT | Business |
|---------------------|---|--|
| Event Recovery | Disaster Recovery Plan Procedures to recover at alternate site | Business Recovery Plan Recover business after a disaster |
| | IT Contingency Plan: Recovers major application or system | Occupant Emergency Plan: Protect life and assets during physical threat |
| | Cyber Incident Response Plan: Malicious cyber incident | Crisis Communication Plan: Provide status reports to public and personnel |
| Business Continuity | | Business Continuity Plan |
| | | Continuity of Operations Plan Longer duration outages |

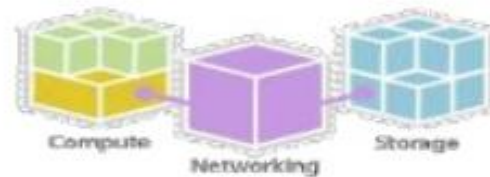
OpenStack Cloud

OpenStack is a community of open source developers, participating organizations and users who are building and running *the* open source cloud operating system.

*“OpenStack is an Infrastructure as a service which is known as a **Cloud Operating System**, that takes resources such as compute, storage, network, virtualization technologies and controls those resources at a data center level”*

“OpenStack’s basic requirement: “Cloud must be simple to implement and massively scalable”

OpenStack Project

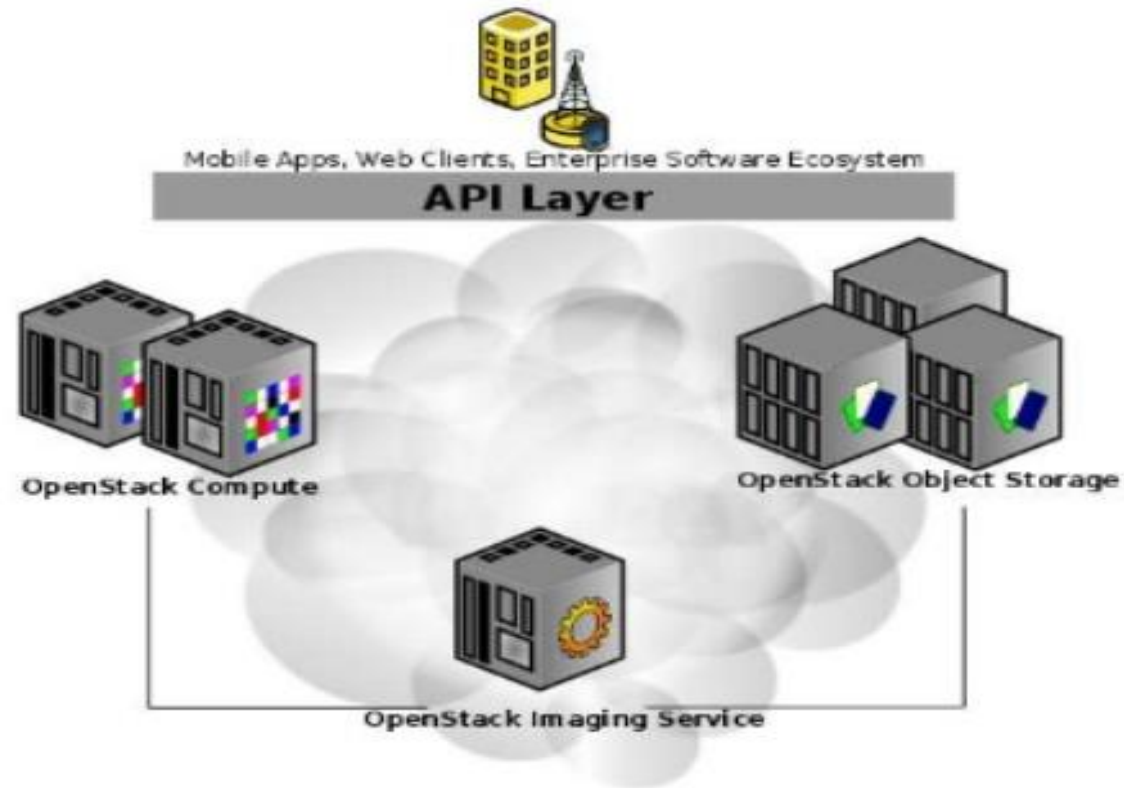


- **OpenStack Compute (Nova):** Provision OpenStack Compute: provision and manage large networks of virtual machines
- **OpenStack Object Store (Swift):** Create petabytes of reliable storage using standard servers
- **OpenStack Image Service (Glance):** Catalog and manage large libraries of server images
- **OpenStack Quantum Service:** provide Network as a service to compute.
- **Other components:** Dashboard, Authentication(Keystone), CLI...

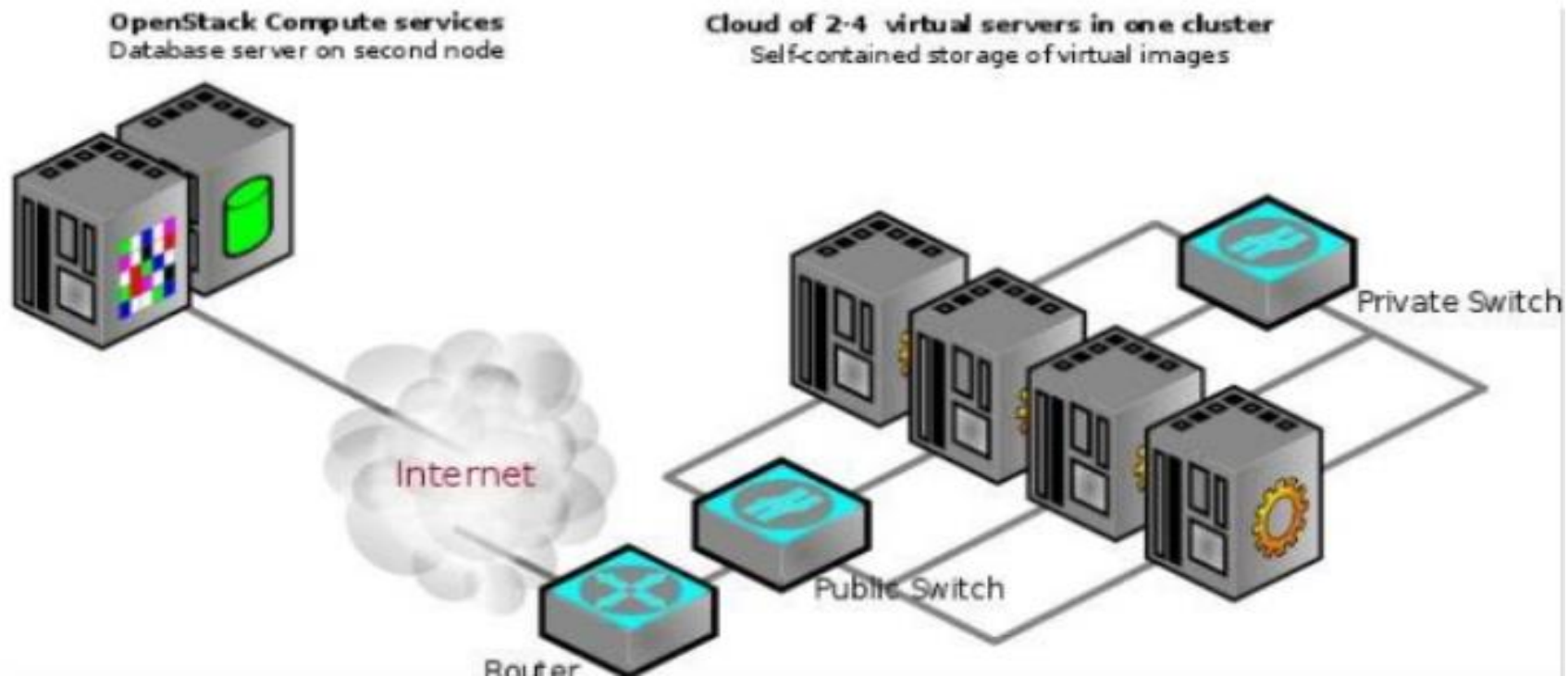
Why OpenStack

- **Control and Flexibility.** Open source platform means you're **never locked to a proprietary vendor**, and modular design can integrate with legacy or third-party technologies to meet your business needs.
- **Industry Standard.** More than 60 leading companies from over a dozen countries are participating in OpenStack, including Cisco, Citrix, Dell, Intel and Microsoft, and **new OpenStack clouds are coming online across the globe.**
- **Proven Software.** Run the same software that today **powers some of the largest public and private clouds in the world.**
- **Compatible and Connected.** Compatibility with public OpenStack clouds means **enterprises are prepared for the future—making it easy to migrate data and applications to public clouds** when conditions are right—based on security policies, economics, and other key business criteria.

Component of OpenStack



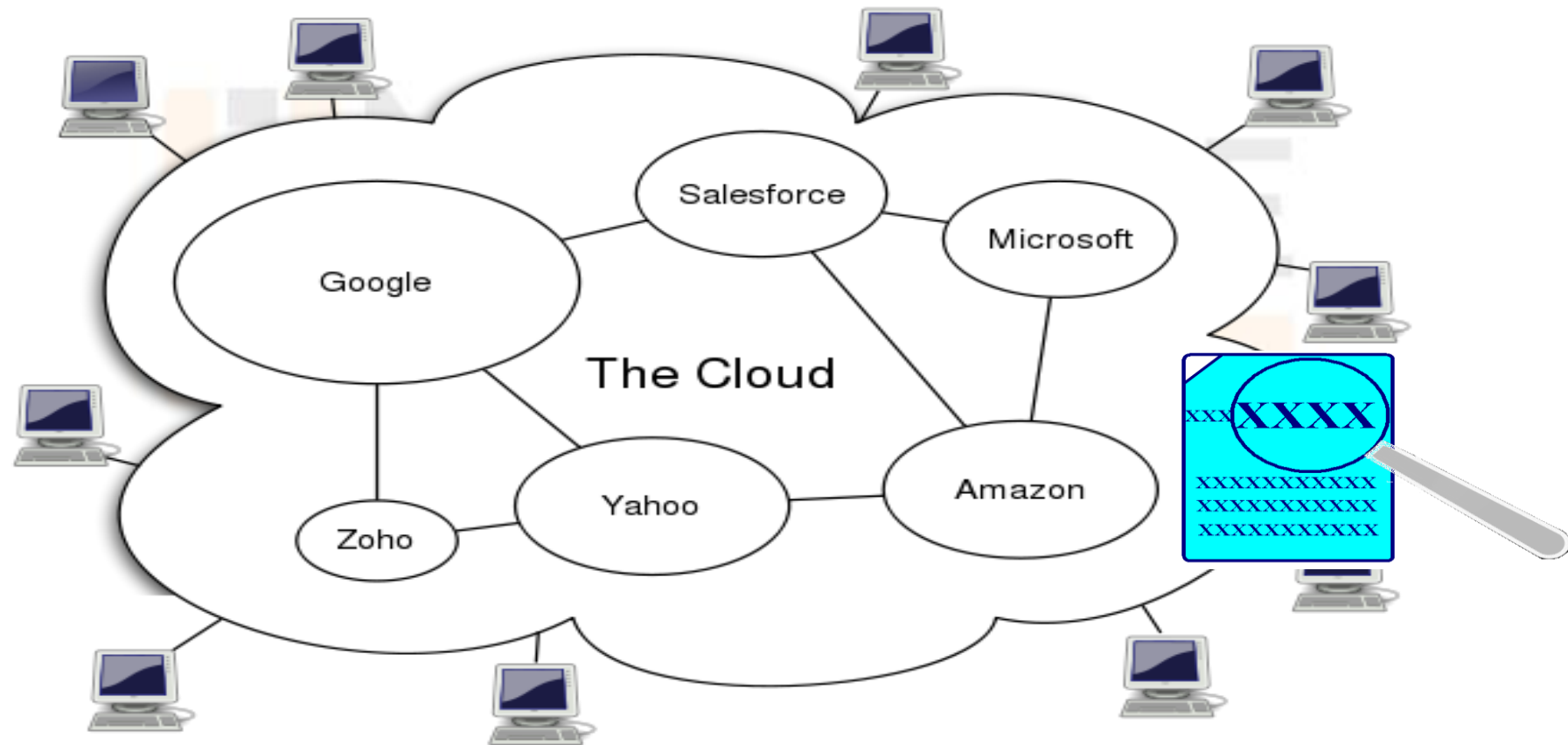
Sample Deployment Architecture of OpenStack



Cloud Forensics

- Cloud forensics is a cross-discipline of cloud computing and digital forensics.
- Cloud forensics is a subset of network forensics. Network forensics deals with forensic investigations of networks.
- Multiple jurisdictions and multi-tenancy are the default settings for cloud forensics, which create additional legal challenges.

Cloud Computing Forensics



Decision Group 2009 Nov.

Basic Concepts of Cloud Forensics

Cloud forensics can have three dimensions:

- Organisational - addresses the structure of the cloud.
- Legal - covers service agreements and other jurisdictional matters.
- Technical - deals with procedures and specialised applications designed to perform forensics recovery and analysis in the cloud.

Basic Concepts of Cloud Forensics

Forensic tool capabilities needed to handle acquiring data from a cloud:

- *Forensic data collection* - must be able to identify, label, record, and acquire data from the cloud.
- *Elastic, static, and live forensics* - must be able to expand and contract their storage capabilities.
- *Evidence segregation* - different businesses and users share the same applications and storage space.
- *Investigations in virtualized environments* - should have the capability to examine virtual systems.

Legal Challenges in Cloud Forensics

- When investigating a cloud system, consider factors involving a CSP's relationship with cloud users
- This section explains
 - A CSP's contract obligations with cloud users.
 - How warrants and subpoenas are applied to CSPs and users?

Self Assessment Question

3. Which of the following service provider provides the least amount of built in security?
- a. SaaS
 - b. PaaS
 - c. IaaS
 - d. All of the above

Answer: c

Self Assessment Question

4. What is the Security Assertion Markup Language used for?
- a. Asserting ownership of a resource
 - b. Managing (setting up, amending and revoking) user or system access entitlements or data
 - c. Exchanging authentication and authorization data
 - d. Defining the security attributes of a system to inquirers
 - e. Writing identity provider programmes

Answer: c

Self Assessment Question

5. Dynamic user provisioning includes everything except:

- a. Evaluating enterprise provisioning tool capabilities
- b. Mapping entitlements between a CSP and the enterprise
- c. Writing custom connectors
- d. Managing users with the CSP management interface
- e. Working with CSP to identify supported mechanisms

Answer: d

Self Assessment Question

6. This is the inclusion of a secret message in otherwise unencrypted text or images.

- a) masquerade
- b) steganography
- c) spoof
- d) eye-in-hand system

Answer: b

Self Assessment Question

7. In password protection, this is a random string of data used to modify a password hash.

- a) sheep-dip
- b) salt
- c) bypass
- d) Dongle

Answer: b

Self Assessment Question

8. This is the encryption algorithm that will begin to supplant the Data Encryption Standard (DES) - and later Triple DES - over the next few years as the new standard encryption algorithm.
- a) Rijndael
 - b) Kerberos
 - c) Blowfish
 - d) IPsec

Answer: a

Self Assessment Question

9. Cryptographic hash function takes an arbitrary block of data and returns

- a) fixed size bit string
- b) variable size bit string
- c) both fixed size bit string and variable size bit string
- d) none of the above

Answer: a

Self Assessment Question

10. An asymmetric-key (or public-key) cipher uses

- a) 1 Key
- b) 2 Key
- c) 3 Key
- d) 4 Key

Answer: b

Self Assessment Question

11. How does Cloud computing change the relationship between provider and customer?

- a) Increased focus on service level agreements (SLAs)
- b) Less compliance to standards
- c) Less focus on service level agreements (SLAs)
- d) More focus on training

Answer: a

Self Assessment Question

12. What is the benefit of storage availability in the Cloud?

- a) Additional storage does not require budget for new large storage devices.
- b) Storage in the Cloud has a higher availability than storage devices in the local area network.
- c) Storage in the Cloud has shorter access times than storage in the local area network.
- d) Storage in the Cloud is easier to protect against intrusion

Answer: a

Self Assessment Question

13. How many types of deployment models are used in cloud?

- a) Public cloud
- b) Private cloud
- c) Community cloud
- d) Hybrid cloud
- e) All of the above

Answer: e

Self Assessment Question

14. In which category of SaaS services does customer relationship management (CRM) software fall?

- a) Consumer services
- b) Communication services
- c) Infrastructure services
- d) Business services

Answer: d

Summary

- The concept of privacy varies widely among (and sometimes within) countries, cultures, and jurisdictions.
- Privacy rights or obligations are related to the collection, use, disclosure, storage, and destruction of personal data
- At the end of the day, privacy is about the accountability of organisations to data subjects, as well as the transparency to an organisation's practice around personal information.
- Contractual costs includes basic subscription, monthly fee, testing charges, activation costs, and hourly/daily use charges.
- Cloud forensics is a subset of network forensics. Network forensics deals with forensic investigations of networks.
- Some business processes are more important than other business processes. Sales is more important in the short term than engineering, and possibly more than the factory. That is why business processes are prioritized.

Assignment

1. Write about the CTP workgroup and its management authority?
2. Name the building blocks of cloud architecture?
3. Define the different layers of cloud architecture?
4. What are the business benefits that can be derived from cloud architecture?
5. What are the phases involved in cloud architecture?
6. List the components needed in cloud architecture?
7. How do you secure your data while transferring on the cloud?

Cloud Security Architecture

Document Links

| Topics | URL | Notes |
|--|---|--|
| Architectural considerations | https://communities.bmc.com/blogs/cloud-n-more/2011/06/01/architectural-considerations-for-cloud-security | This link explains the General issues involving regulatory requirements, standards compliance, security management, information classification and security awareness need s to be maintained |
| Cloud Security Architecture | https://www.infoq.com/articles/cloud-security-architecture-intro | This link explains about the platforms provide basic security features including support for authentication, DoS attack mitigation, firewall policy management, logging, |
| identity management and access control | https://www.imfacademy.com/areasofexpertise/security_management/identity-management-and-access-control.php | This link explains the Identity Management & Access Control initiatives. International Management Forum (IMF) advocates an approach to govern Identity Management & Access Control initiatives |
| autonomic security | https://www.techopedia.com/definition/191/autonomic-computing | This link explains the Autonomic computing is a computer's ability to manage itself automatically through adaptive technologies that further computing capabilities and cut down on the time |
| encryption and key strategies | https://www.rsaconference.com/writable/presentations/file_upload/dsp-w25b.pdf | This link explains the security problems that may exist when the users transport the sensitive data on the network, this paper tries to optimize and |
| secure connection | https://searchcloudsecurity.techtarget.com/tip/Cloud-computing-security-Choosing-a-VPN-type-to-connect-to-the-cloud | This link explains the level-set for the cloud computing security discussion with a general... |
| Privacy in Cloud | http://journals.sagepub.com/doi/full/10.1155/2014/190903 | This link is explains the Data security has consistently been a major issue in information technology. In the cloud computing environment |

Cloud Security Architecture

Video Links

| Topics | URL | Notes |
|--|---|--|
| Architectural considerations | https://www.youtube.com/watch?v=fZ3D6HQRWzs | This video explains the Cloud computing is defined with several deployment models, each of which has specific trade-offs for agencies that are migrating services |
| Cloud Security Architecture | https://www.youtube.com/watch?v=QUZhgEscPOY | This video explains the Basic operating concepts, different types of Operating System and Goals of Operating System. This Video will help you in building up concepts |
| identity management and access control | https://www.youtube.com/watch?v=l0SmnVmr14I | This video will help in understanding AWS Identity and Access Management (IAM) enables you to securely control access to AWS services and resources for your users. Using IAM, you can create and manage AWS users and groups and use permissions to allow and deny their access to AWS resource |
| autonomic security | https://www.youtube.com/watch?v=p7-ICpM8YVo | This video explains the introduction of autonomic security |
| encryption and key strategies | https://www.youtube.com/watch?v=On9NoUwj-Os | This video explains the Protecting sensitive data in the cloud typically requires encryption. Managing the keys used for encryption can be challenging as your sensitive data passes between services and applications. |
| secure connection | https://www.youtube.com/watch?v=LcAPj95KeSA | This video explains how to secure the connection of cloud server |
| Privacy in Cloud | https://www.youtube.com/watch?v=NUT-fuRPm_M | This video explain the security and privacy of cloud computing |

E-Book Links

| Topics | URL |
|--|---|
| Architectural considerations | https://azure.microsoft.com/en-in/campaigns/cloud-application-architecture-guide/ |
| identity management and access control | https://pdfs.semanticscholar.org/f051/551d8983f5f2241ffa82d32c0274261d8972.pdf |
| encryption and key strategies | http://www.iosrjournals.org/iosr-jce/papers/Vol17-issue1/Version-5/H017155360.pdf |
| Privacy in Cloud | https://www.itu.int/dms_pub/itu-t/oth/23/01/T23010000160001PDFE.pdf |