ITU-T Workshop on Addressing security challenges on a global scale

6 – 7 December 2010 Geneva, Switzerland

Privacy & security issues for cloud computing services

Heung Youl YOUM, PhD

Vice-chair, ITU-T SG 17

Soonchunhyang University, Korea

Cloud computing definition (NIST)

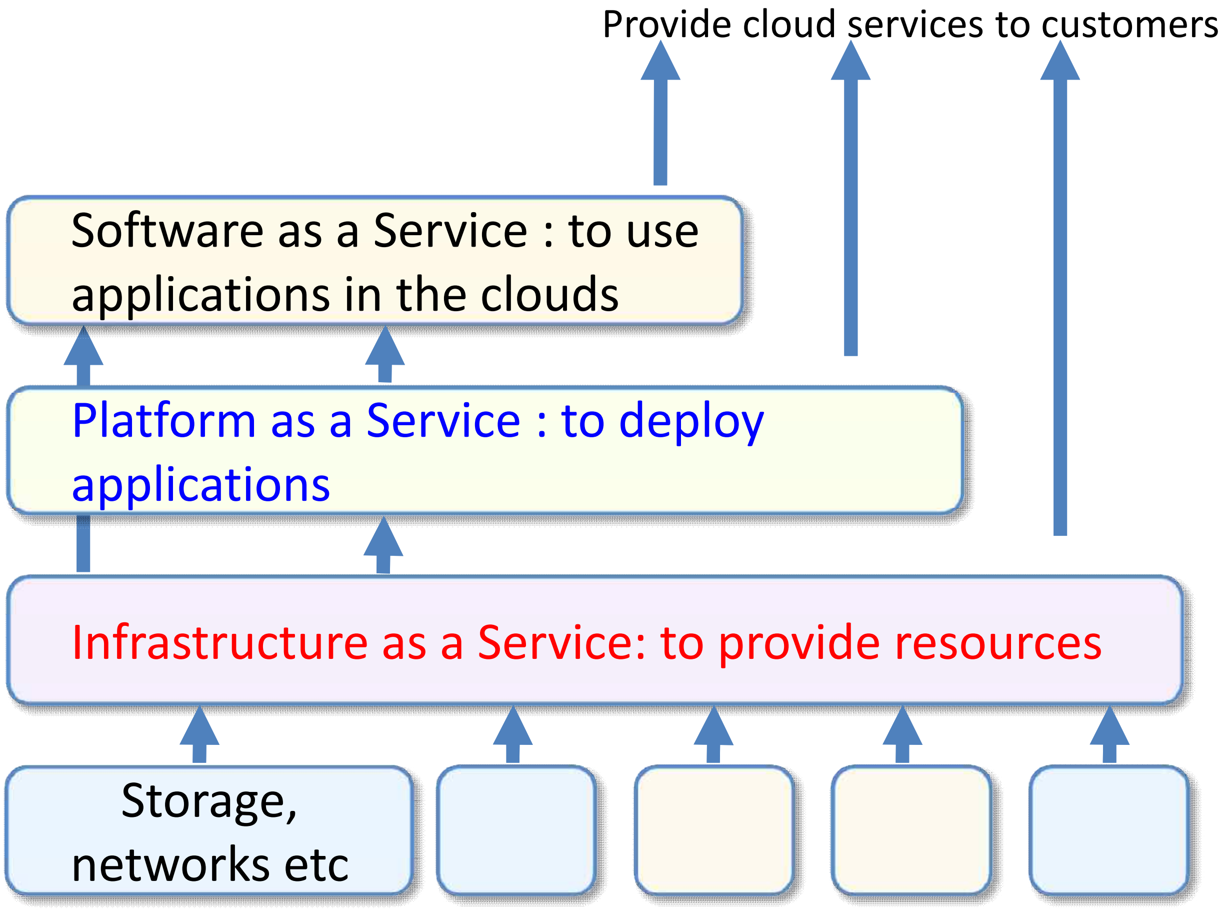
- No unique or globally agreed definition yet,
- (Wikipedia) An Internet-based computing, whereby shared resources, software, and information are provided to computers and other devices on demand, like the electricity grid.
- (Gatner) A style of computing that characterizes a model in which providers deliver a variety of IT-enabled capabilities to consumers
- (NIST) A model for enabling 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 promotes availability and is composed of
  - five essential characteristics (on-demand self service, broad network access, resource pooling, rapid elasticity, measure service),
  - three service models (Software as a service, platform as a service, infrastructure as a service), and
  - four deployment models (private, public, community, hybrid cloud).

Service model

- Cloud Software as a Service (SaaS)
  - The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a web browser (e.g., web-based email).
- Cloud Platform as a Service (PaaS)
  - The capability is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages and tools supported by the provider.
- Cloud Infrastructure as a Service (IaaS)
  - The capability is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications.

Conceptual service models (CSA&NIST)

- According to layer, there are three service models.



Provide cloud services to customers

Software as a Service : to use applications in the clouds

Platform as a Service : to deploy applications

Infrastructure as a Service: to provide resources

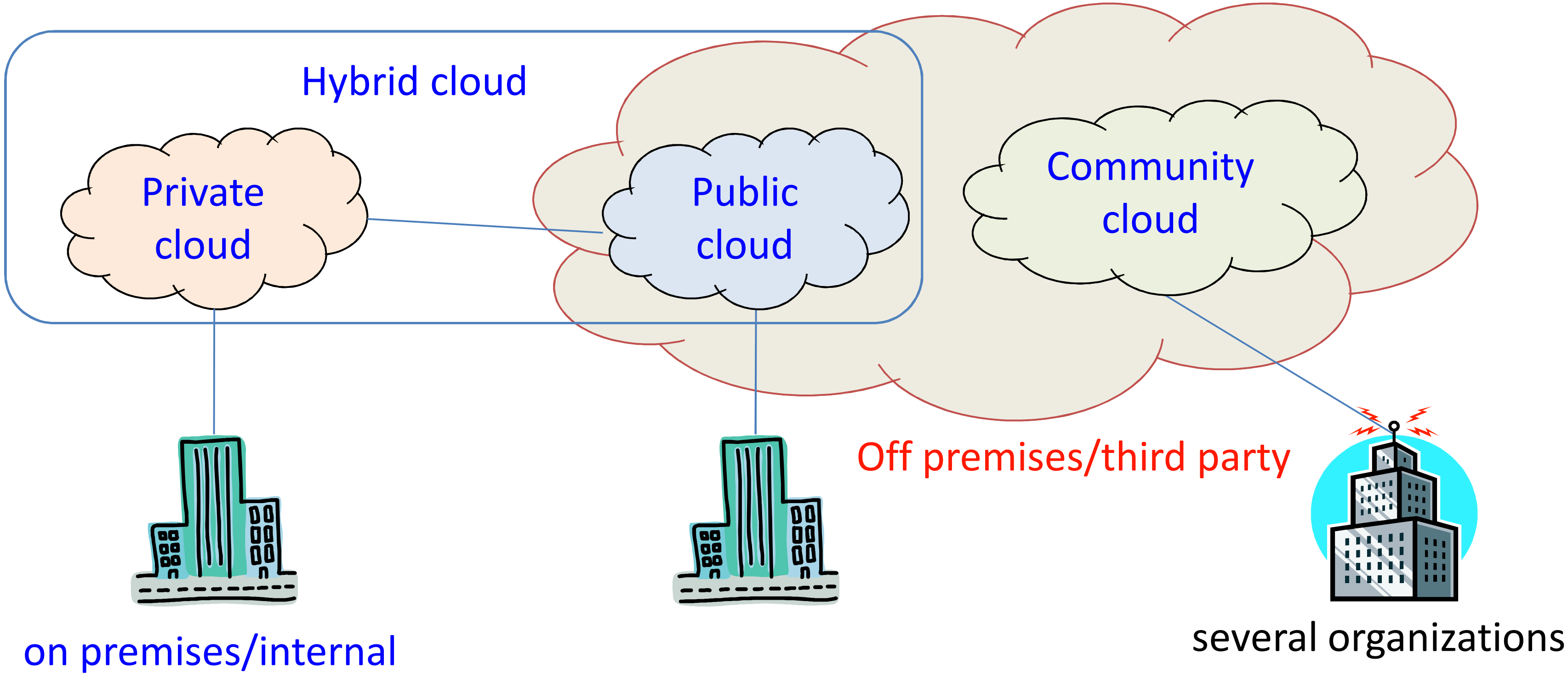
Storage, networks etc

Deployment models

- Private cloud (or internal cloud)
  - The cloud infrastructure is operated solely for an organization. It may be managed by the organization or a third party and may exist on premise or off premise.
- Public Cloud (or external cloud)
  - The cloud infrastructure is made available over the Internet, via web applications/web services, to the general public or a large industry group and is owned by an off-site third-party organization selling cloud services.
- Community cloud
  - The cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be managed by the organizations or a third party and may exist on premise or off premise.
- Hybrid could
  - The cloud infrastructure is a composition of two or more clouds (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load-balancing between clouds).

Conceptual deployment models (CSA&NIST)

- According to deployment location of cloud infra and type of cloud customer, there are four models.



Security advantage of clouds

- Shifting public data to a cloud may reduce the exposure possibility of the internal sensitive data through:
  - Simplification of compliance analysis, and
  - Data held by unbiased party.
- Homogeneous structure of clouds makes security auditing/testing much simpler.
  - Automated security management and safeguards are enabled by a dedicated security team enabling:
  - Real-time detection of system tampering,
  - Possible Reduction of C&A Activities and Advanced honeynet capabilities,
  - On-Demand Security Controls.
- Quick Disaster Recovery through:
  - Fault Tolerance and Reliability
  - Greater Resiliency
  - Low-Cost Disaster Recovery and Data Storage Solutions
  - Rapid Re-Constitution of Services

Security concerns of clouds

- Security concerns originate from loss of control of the customer assets that are stored or maintained by the cloud providers.
- Need to identify the asset(s) in the cloud:
  - Data and applications/functions/process.
- Major security concerns
  - Theft of data/loss of privacy
    - If the asset become widely public & widely distributed.
    - If an employee of our cloud provider accesses the asset.
  - Service disruption/unavailability
    - If the process of function is manipulated by an outsider attacker.
    - If the process or function fails to provide expected results.
    - If the asset is unavailable for a period of time.
  - Damage of data
    - If the info/data may be unexpectedly changed.

Threats for the customer (1/2)

- Trust concern on cloud provider's infrastructure
  - How can customers be sure that their data and application will be treated and maintained in a secure manner, respectively?
- Data loss and leakage
  - The possibility of data compromise, resulting in data loss and leakage, increases in clouds, due to the following reasons which may be unique to cloud:
    - Insufficient authentication, authorization, and audit (AAA) controls;
    - inconsistent use of encryption and software keys;
    - operational failures; risk of association; Incomplete jurisdiction; or
    - Natural or artificial disasters.
- Account hijacking and session hijacking
  - If attackers gain access to customer's credentials, they can eavesdrop on activities and transactions of customers, manipulate data, return falsified information, and redirect clients to illegitimate sites.

Threats for the customer (2/2)

- Lack of Compliance
  - How can the customer be sure regulatory/legal compliance?
  - Cloud providers should enable their customers to comply appropriately with these regulations.
- Loss of business continuity
  - What happens when my Internet provider or cloud provider shut down?
  - Service should be maintained in case of a disaster or an emergency and any data lost will be recovered.
- Loss of business value and reputation
  - How can I be sure that my cloud service provider meets the SLA agreed with customers?

Threats for Service Providers (1/3)

- Abuse and nefarious use of cloud
  - Attackers such as spammers, malicious code authors, and other criminals may use cloud computing to conduct their malicious attacks.
- Insecure Interfaces and APIs
  - Cloud providers provide a set of software interfaces or APIs that customers use to manage and interact with cloud services.
  - These interfaces must be designed to protect against both accidental and malicious attempts to circumvent policy.

Threats for Service Providers (2/3)

- Malicious Insiders
  - Cloud providers may not reveal the followings:
    - how it grants employees access to physical and virtual assets,
    - how it monitors the activities of employees.
  - The access of cloud could enable such an malicious insiders to access to confidential data or gain complete control over the cloud services with little or no risk of detection.
- Shared technology issues
  - Cloud service shares the underlying components that make up this infrastructure (e.g., CPU caches, GPUs, etc.). But, they were not designed to offer strong isolation properties for a multi-tenant architecture.
  - Strong compartmentalization should be employed to ensure that individual customers do not impact the operations of other tenants running on the same cloud provider.

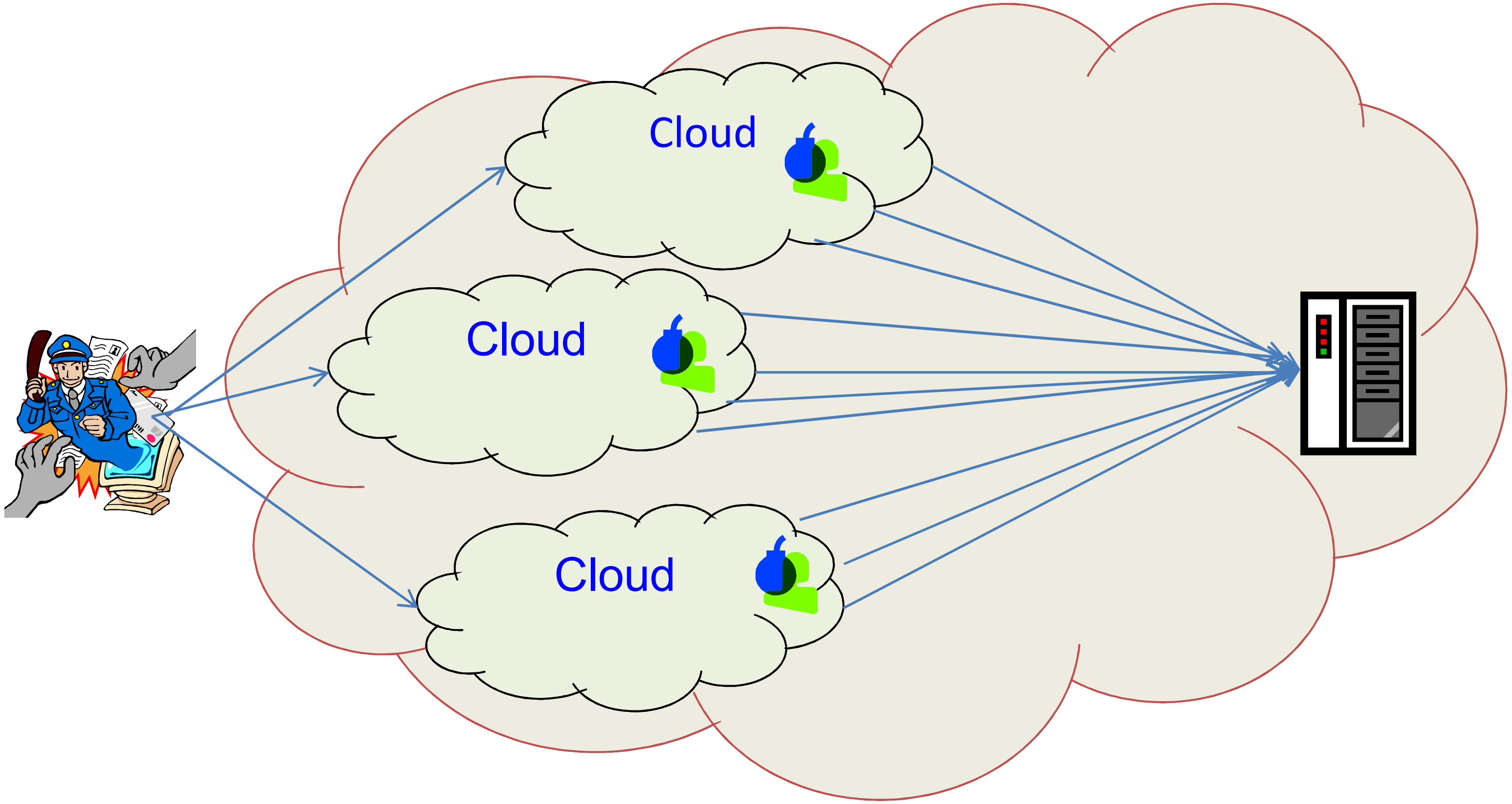
Threats for Service Providers (3/3)

- Unknown risks
  - One of the advantages of Cloud Computing is the reduction of hardware and software ownership and maintenance to allow companies to focus on their core business strengths.
  - It has clear financial and operational benefits, which must be assessed carefully against the contradictory security concerns — complicated by the fact that cloud deployments are driven by anticipated benefits, by groups who may lose track of the security implications.
- Exposure of data to foreign governments

Examples of abuse of cloud computing

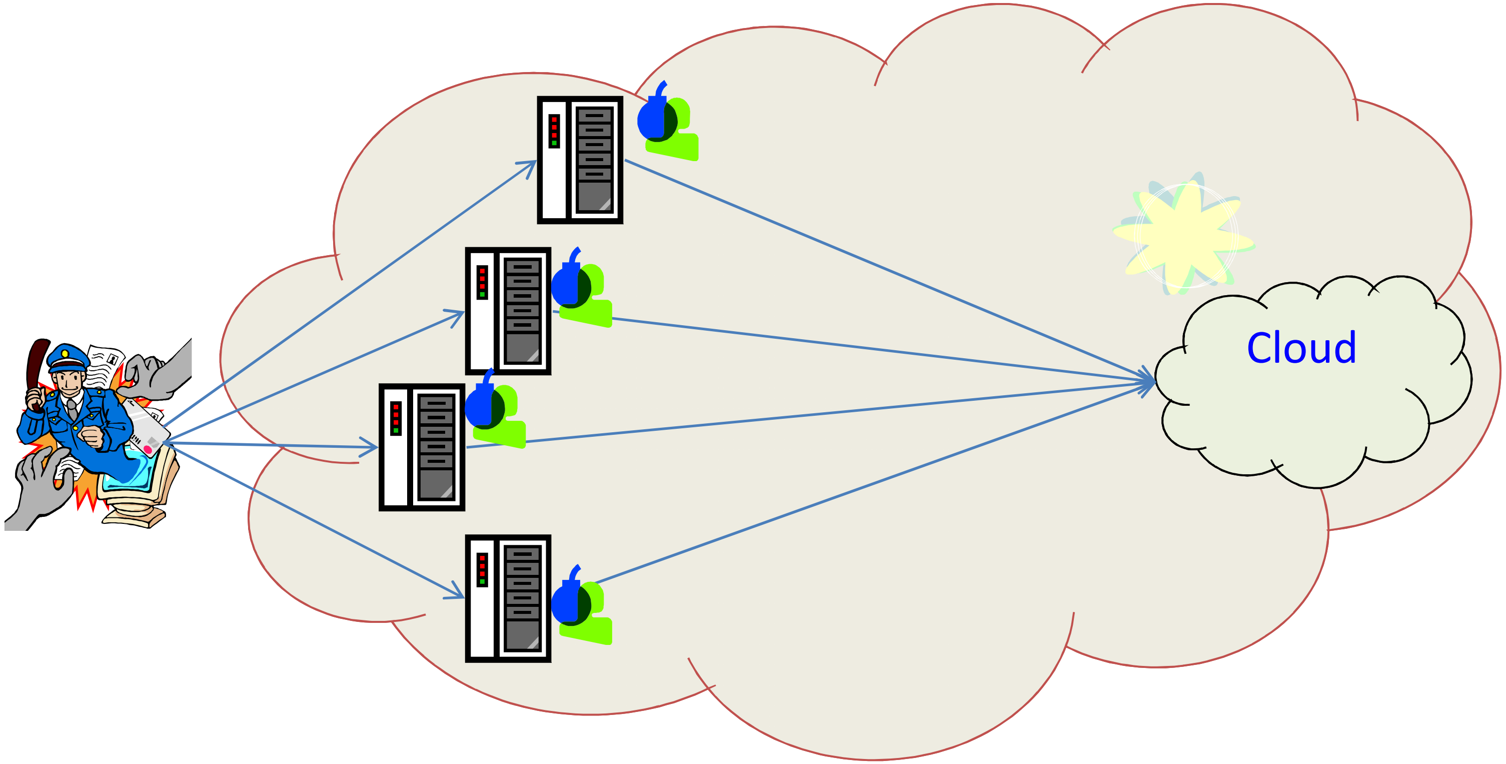
- Denial of service
  - Cloud computing may be used to launch a DoS, DDoS and host C&C server for botnet and malicious code.
- Cryptographic analysis
  - Cloud computing may be used to break someone’s encryption scheme.
- Command & control for botnet
  - Cloud computing may be used to provide an adversary a C&C server to initiate cyber attacks.

Conceptual DDoS attack using clouds



- The attacker uses the cloud to launch the DDoS attacks to a specific server.

Conceptual DDoS attack targeted at cloud



- DDoS attacks, causing loss of service availability, could be targeted at Cloud. For example, Twitter was hit with nasty DDoS attacks on August 6 th, 2009.

Requirements from customer's perspective

- Customer should be protected against:
  - trust concern on cloud provider's infrastructure by enforcing security management such as security audit, security policy agreement, security management and presenting the certification by the third party.
  - data loss or leakage by using:
    - encrypting data using key management; availability.
  - Account/session hijacking by using:
    - strong account/identity management;
    - prohibiting the sharing of account credentials between users and services; and
    - Leveraging two-factor authentication techniques where possible.

Requirements from Service providers' perspective (1/3)

- Cloud provider should be protected against:
  - malicious activities such as DDoS, service hijacking and account hijacking by using:
    - comprehensive monitoring of network traffic;
    - employing proactive monitoring to detect unauthorized activity;
    - monitoring public SPAM blacklists for one's own network blocks.
  - insecure interface and API by using:
    - strict Identity management and authentication;
    - implementing strong authentication and access controls;
    - encrypted data transfer; and
    - dependency chain associated with the API.

Requirements from Service provider's perspective (2/3)

- Cloud provider should be protected against :
  - malicious insiders by ensuring that:
    - security management should be appropriately implemented:
    - human resource security requirements be enforced as part of legal contracts; and
    - transparency into overall information security and management practices be provided, as well as compliance reporting.
  - shared technology concerns by ensuring that
    - Virtual machine security of multi-tenancy of data and application should be considered;
    - best practices be implemented for installation/configuration;
    - unauthorized changes/activity be monitored;
    - strong authentication and access control for administrative access and operations and patching and vulnerability remediation be enforced; and
    - vulnerability scanning and configuration audits be conducted.

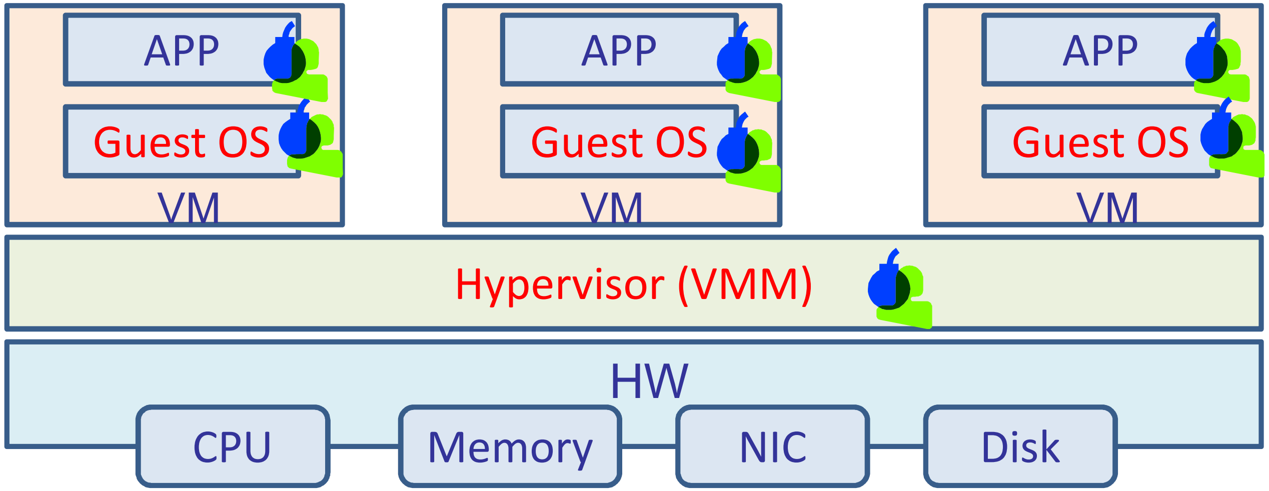
Requirements from Service providers' perspective (3/3)

- Cloud provider should be protected against data against loss or leakage by using:
  - confidentiality and availability mechanisms;
  - implementing strong API access control;
  - encrypting and protecting integrity of data in transit or storage;
  - analyzing data protection at both design and run time;
  - implementing strong key generation, storage and management, and destruction practices; and
  - contractually specifying provider backup and retention strategies.
- Cloud provider should be protected by ensuring that:
  - Certification mechanism should be provided for separate application;
  - Network and perimeter controls should be securely implemented;
  - Contingency planning and disaster recovery should be implemented;
  - Data dispersal and international privacy laws should be assessed.

Virtualization Threats - Malicious

- Virtualization threats
  - Guest OS Infection;
  - Denial of Service;
  - Rouge Virtualized Machine;
  - Virtual-Machine based rootkit;
  - Hypervisor Software Vulnerabilities

- Security of Virtualization
  - VM Security Monitors
  - Patching and Monitoring
  - Hardened Virtual Machine Monitors
  - Best Practices



Security guideline for 13 critical domain [CSA]

- Domain 1: Cloud Computing Architectural Framework
- Domain 2: Governance and Enterprise Risk Management
- Domain 3: Legal and Electronic Discovery
- Domain 4: Compliance and Audit
- Domain 5: Information Lifecycle Management
- Domain 6: Portability and Interoperability
- Domain 7: Traditional Security, Business Continuity, and Disaster Recovery
- Domain 8: Data Center Operations
- Domain 9: Incident Response, Notification, and Remediation
- Domain 10: Application Security
- Domain 11: Encryption and Key Management
- Domain 12: Identity and Access Management
- Domain 13: Virtualization

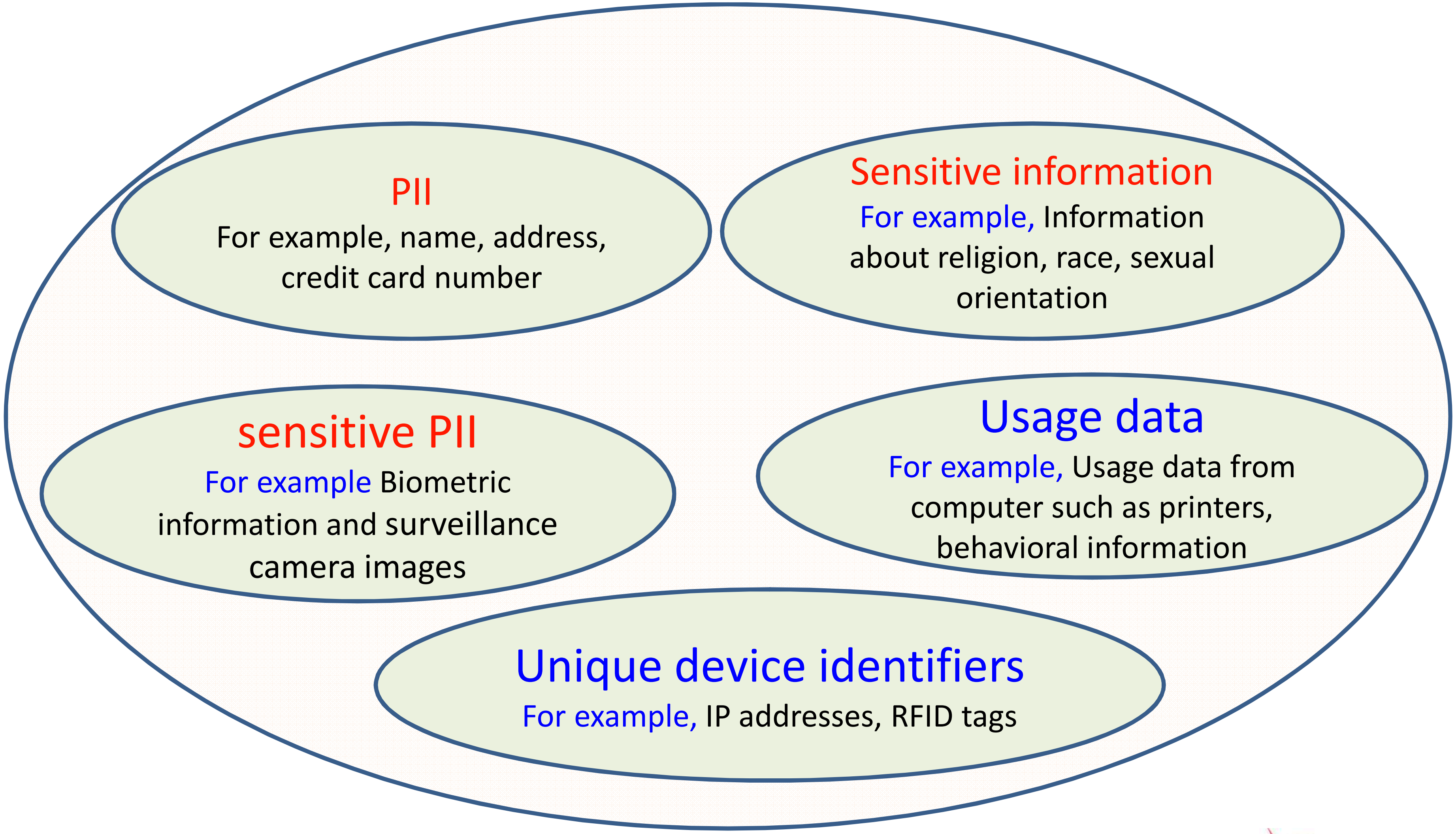
Encryption/ID management domain

- Encryption
  - It is required to encrypt data in transit over the network, at rest, on backup media.
- Key management
  - Key stores should be protected.
  - Access to key stores should be limited to the entities that specifically need the individual keys.
  - Secure backup and recovery should be implemented.
- ID management
  - The secure and timely management of provisioning of users ID should be provided in the cloud.
  - When organizations start to utilize cloud services, it is required to authenticate users in a trustworthy and manageable manner.
  - Various Identity Management plays a vital role in enabling organizations to authenticate their users of cloud services using the organization's chosen identity provider (IdP).

Privacy challenges and Privacy information

- Personal data (personal information) means any information relating to an identified or identifiable individual (data subject). [OECD]
- Privacy challenges
  - It is generally recognized that "the increased commercial use (and value) of PII, the sharing of PII across different legal jurisdictions, and the growing complexity of ICT systems, make it extremely difficult for an organization to ensure privacy and to achieve compliance with various laws and regulations."

Privacy information to be protected



PII

For example, name, address, credit card number

Sensitive information

For example, Information about religion, race, sexual orientation

sensitive PII

For example Biometric information and surveillance camera images

Usage data

For example, Usage data from computer such as printers, behavioral information

Unique device identifiers

For example, IP addresses, RFID tags

Privacy-specific threats

- For the cloud individual customers,
  - Track of personal data: Being forced to be tracked or giving personal data against their will.
  - Lack of data protection and insecure data deletion : The cloud customer (in its role as data controller) have difficulty in effectively checking the data handling practices of the cloud provider and thus being sure that the data is handled in a lawful way. When a request to delete a cloud resource is made, adequate or timely data deletion may also be.
- For the organization providing the cloud service,
  - Non-compliance to enterprise policies and legislations, loss of reputation and credibility.
- For cloud platform implementers,
  - Exposure of sensitive information stored in the platforms, legal liability, loss of credibility, lack of user trust and take-up.
- For providers of application on the top cloud,
  - Legal non-compliance

Key privacy requirements (OECD)

- Notice, openness and transparency
  - Privacy policy should be available to clients regarding what to collect, how to use it, how long to keep it, with whom they share it, any other uses they intend.
- Choice, consent and control
  - Data subject should give their consent to collection, use, and disclosure of their PII.
- Scope/minimization
- Access/accuracy
- Security safeguard
- Compliance
  - Transactions should be compliant to privacy legislations and laws such as data protection law, data retention and cross-border data transfer practices.
- Purpose
- Limiting use – disclosure and retention
  - Data can only be used or disclosed for the purpose for which it was collected.
- Accountability
  - An organization must appoint CPO(Chief Privacy Officer) to ensure that privacy policies and practices are followed, audit function should be present to monitor all data accesses and modification.

Top tips for privacy protection (HP)

- ❑ Minimize personal information such as PII sent to and stored or back-up in the cloud.
- ❑ Protect personal data by technical means in the cloud.
- ❑ Carry out privacy impact assessment before designing clouds.
- ❑ Maximize customer control of personal data in the cloud.
- ❑ Allow customer choice for data process.
- ❑ Specify and limit the purpose of personal data usage.
- ❑ Provide feedback.

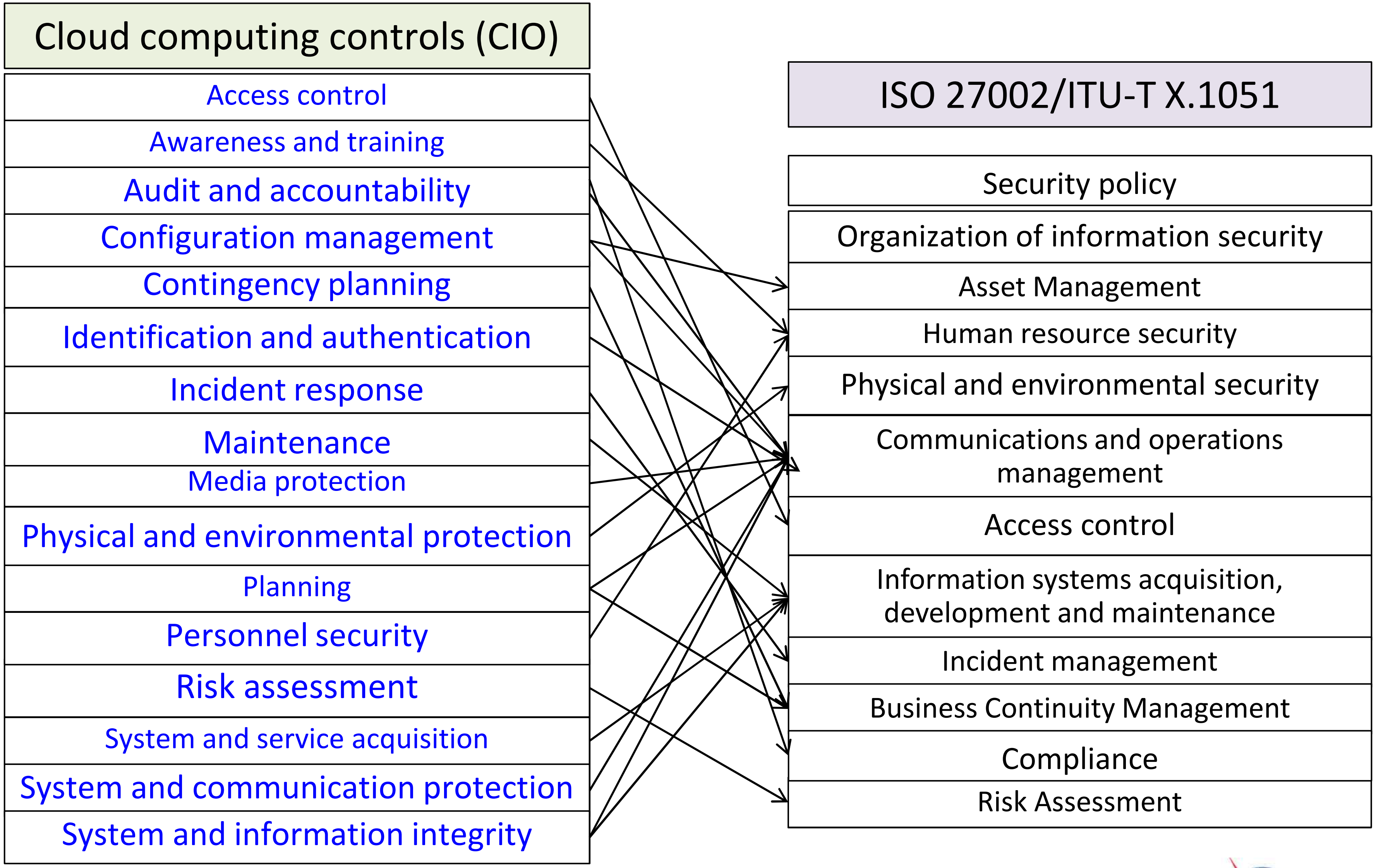
Security countermeasures for clouds

- Technical safeguards
  - Confidentiality and encryption
  - Identification, authentication and access control
  - Data integrity
  - Availability
  - Virtualization security
  - Network and web security
- Security management , physical, and Compliance
  - Information security policy
  - Compliance, audit
  - Incident management
  - Physical & environmental security disaster recovery
  - Business continuity

ISO 27002/ITU-T X.1051

- ISO 27002/ITU-T X.1051 covers the following security controls:
  - Risk Assessment – determining asset vulnerability;
  - Security Policy - management direction;
  - Organization of Information Security - governance of information security;
  - Asset Management - inventory and classification of information assets;
  - Human Resources Security - security aspects for employees joining, moving and leaving an organization;
  - Physical and Environmental Security - protection of the computer facilities;
  - Communications and Operations Management - management of technical security controls;
  - Access Control - restriction of access rights to networks, systems, applications, functions and data;
  - Information systems acquisition, development and maintenance – building security into applications
  - Information security Incident Management - anticipating and responding appropriately to security breaches;
  - Business Continuity Management - protecting, maintaining and recovering business-critical processes and systems; and
  - Compliance - ensuring conformance with information security policies, standards, laws and regulations.

ISMS vs. cloud computing controls[CIO council]



Cloud computing controls (CIO)

Access control

Awareness and training

Audit and accountability

Configuration management

Contingency planning

Identification and authentication

Incident response

Maintenance

Media protection

Physical and environmental protection

Planning

Personnel security

Risk assessment

System and service acquisition

System and communication protection

System and information integrity

ISO 27002/ITU-T X.1051

Security policy

Organization of information security

Asset Management

Human resource security

Physical and environmental security

Communications and operations management

Access control

Information systems acquisition, development and maintenance

Incident management

Business Continuity Management

Compliance

Risk Assessment

Concluding remark

- Need to be aware of various threats in cloud environments:
- Need to provide to ITU-T members cloud computing security standards.
- Recommendations that are not covered by other SDOs should be developed to cover various security aspects for the cloud computing services based on telecommunication by ITU-T SG17, such as:
  - Requirement and functional architectures; Security and privacy guideline for cloud services;
  - Guideline for threats and security requirement of VM;
  - Guideline for secure Interfaces or API;
  - Telecommunication-based cloud ISMS;
  - Key management and encryption; ID management and etc.

References

- CSA, Top Threats to Cloud Computing V1.0, March 2010.
- CIO council, Proposed Security Assessment & Authorization for U.S. Government Cloud Computing, November 2010.
- ENISA, Cloud Computing Benefits, risks and recommendations for information security, November, 2009.
- CSA, Security Guidance for Critical Areas of Focus in Cloud Computing V2.1, December 2009
- Siani Pearson, "Taking Account of Privacy when Designing Cloud Computing Services," HP Labs, Bristol, UK, 2009
- Charles Kolodgy, Virtualization Security –Different Field, Same Game,IDC, 2008
- OECD, OECD guidelines on the protection of privacy and transborder flows of personal data, September 1980
- Marco Casassa Mont, "The Future of Identity in the Cloud: Requirements, Risks & Opportunities," HP Labs, Bristol, UK, 2009